aws

Guía del usuario

Amazon Macie

Amazon Macie: Guía del usuario

Table of Contents

¿Qué es Amazon Macie?

Amazon Macie es un servicio de seguridad de datos que descubre datos confidenciales mediante el machine learning y la coincidencia de patrones, proporciona visibilidad de los riesgos de seguridad de los datos y permite establecer una protección automatizada contra esos riesgos.

Para ayudarle a gestionar la seguridad del patrimonio de datos del Amazon Simple Storage Service (Amazon S3) de su organización, Macie le proporciona un inventario de sus depósitos de uso general de S3 y evalúa y supervisa automáticamente los depósitos para garantizar la seguridad y el control de acceso. Si Macie detecta un posible problema con la seguridad o la privacidad de sus datos, como un bucket de acceso público, Macie genera un resultado para que lo revise y solucione según sea necesario.

Macie también automatiza la detección y la notificación de informes de datos confidenciales para ofrecerle una mejor comprensión de los datos que su organización almacena en Amazon S3. Para detectar datos confidenciales, puede utilizar los criterios y técnicas integrados que proporciona Macie, los criterios personalizados que usted defina o una combinación de ambos. Si Macie detecta datos confidenciales en un objeto de S3, Macie genera un hallazgo para notificarle los datos confidenciales que ha encontrado.

Además de los resultados, Macie proporciona estadísticas e información que ofrecen información sobre el estado de seguridad de sus datos de Amazon S3 y sobre dónde pueden residir los datos confidenciales en su patrimonio de datos. Las estadísticas y la información pueden guiar sus decisiones para llevar a cabo investigaciones más exhaustivas de objetos y depósitos de S3 específicos. Puede revisar y analizar los hallazgos, las estadísticas y otra información mediante la consola de Amazon Macie o la API de Amazon Macie. También puede aprovechar la integración de Macie con Amazon EventBridge AWS Security Hub para monitorear, procesar y corregir los hallazgos mediante el uso de otros servicios, aplicaciones y sistemas.

Temas

Características de Amazon Macie

Estas son algunas de las formas clave en las que Amazon Macie puede ayudarle a descubrir, supervisar y proteger sus datos confidenciales en Amazon S3.

Automatice la detección de datos confidenciales

Con Macie, puede automatizar la detección y la notificación de información confidencial de dos maneras: configurando Macie para realizar un descubrimiento automatizado de información confidencial y creando y ejecutando trabajos de detección de información confidencial. Si Macie detecta datos confidenciales en un objeto de S3, crea un resultado de datos confidenciales para usted. El hallazgo proporciona un informe detallado de los datos confidenciales que Macie detectó.

La detección de datos confidenciales proporciona una amplia visibilidad de dónde pueden residir los datos confidenciales en su patrimonio de datos de Amazon S3. Con esta opción, Macie evalúa continuamente su inventario de buckets de S3 y utiliza técnicas de muestreo para identificar y seleccionar objetos de S3 representativos de sus buckets. A continuación, Macie recupera y analiza los objetos seleccionados, inspeccionándolos en busca de datos confidenciales.

Los trabajos de detección de datos confidenciales proporcionan un análisis más profundo y específico. Con esta opción, puede definir la amplitud y profundidad del análisis: los segmentos de S3 que se van a analizar, la profundidad de muestreo y los criterios personalizados que se derivan de las propiedades de los objetos de S3. También puede configurar un trabajo para que se ejecute solo una vez para el análisis y la evaluación bajo demanda, o de forma periódica para el análisis, la evaluación y el monitoreo periódicos.

Ambas opciones pueden ayudarle a crear y mantener una visión integral de los datos que almacena su organización en Amazon S3 y de cualquier riesgo de seguridad o cumplimiento de esos datos.

Descubra una variedad de tipos de datos confidenciales

Para detectar información confidencial con Macie, puede utilizar criterios y técnicas integradas, como machine learning y coincidencia de patrones, para analizar objetos en buckets de S3. Estos criterios y técnicas, que se denominan identificadores de datos administrados, pueden detectar una lista extensa y creciente de tipos de datos confidenciales en muchos países y regiones, incluidos varios tipos de información de identificación personal (PII), datos financieros y datos de credenciales.

También puede utilizar identificadores de datos personalizados. Un identificador de datos personalizado es un conjunto de criterios que usted define para detectar datos confidenciales: una expresión regular (regex) que define un patrón de texto para coincidir y, opcionalmente, secuencias de caracteres y una regla de proximidad que refina los resultados. Con este tipo de identificador, puede detectar datos confidenciales que reflejen escenarios particulares, propiedad intelectual o datos de propietario. Pueden complementar los identificadores de datos administrados que Macie proporciona.

Para ajustar los análisis, también puede utilizar listas de permisos. Permita que las listas definan texto y patrones de texto específicos que desea que Macie ignore en los objetos de S3. Por lo general, se trata de excepciones a los datos confidenciales en situaciones o entornos específicos, por ejemplo, los nombres de los representantes públicos de la organización, los números de teléfono públicos de la organización o los datos de muestra que la organización utiliza para las pruebas.

Evalúe y supervise los datos para garantizar la seguridad y el control de acceso

Al activar Macie, Macie genera automáticamente y comienza a mantener un inventario completo de sus cubos S3 de uso general. Macie también comienza a evaluar y monitorear los buckets para ofrecer seguridad y control de acceso. Si Macie detecta un posible problema con la seguridad o la privacidad de un bucket, crea un resultado de política para usted.

Además de los resultados específicos, un panel le ofrece una instantánea de las estadísticas agregadas de sus datos de Amazon S3. Esto incluye estadísticas de métricas clave, como la cantidad de depósitos a los que se puede acceder públicamente o que se comparten con otros usuarios. Cuentas de AWS Puedes profundizar en cada estadística para revisar los datos de respaldo.

Macie también proporciona información y estadísticas detalladas para cada uno de los buckets S3 de su inventario. Los datos incluyen un desglose de la configuración de acceso público y cifrado de un bucket, así como el tamaño y la cantidad de objetos que Macie puede analizar para detectar datos confidenciales en el bucket. Puede examinar el inventario u ordenar y filtrar el inventario por determinados campos.

Revise y analice los resultados

En Macie, un hallazgo es un informe detallado de los datos confidenciales que Macie ha detectado en un objeto de S3 o de un posible problema con la seguridad o la privacidad de un depósito de uso general de S3. Cada hallazgo proporciona una clasificación de gravedad,

información sobre el recurso afectado y detalles adicionales, como cuándo y cómo Macie detectó los datos o el problema.

Para revisar, analizar y administrar los resultados, puede utilizar las páginas de Resultados de la consola de Amazon Macie. En estas páginas se enumeran sus resultados y se proporcionan los detalles de los resultados individuales. También ofrecen múltiples opciones para agrupar, filtrar, ordenar y suprimir los resultados. También puede utilizar la API de Amazon Macie para consultar, recuperar y suprimir resultados. Si usa la API, puede pasar los datos a otra aplicación, servicio o sistema para realizar análisis más detallados, almacenarlos a largo plazo o generar informes.

Supervise y procese los resultados con otros servicios y sistemas

Para facilitar la integración con otros servicios y sistemas, Macie publica los resultados en Amazon EventBridge como eventos de búsqueda. EventBridge es un servicio de bus de eventos sin servidor que puede dirigir los datos de los hallazgos a objetivos, como AWS Lambda funciones y temas del Amazon Simple Notification Service (Amazon SNS). Con EventBridge él, puede monitorear y procesar los hallazgos casi en tiempo real como parte de sus flujos de trabajo actuales de seguridad y cumplimiento.

Puede configurar Macie para que también publique los resultados en AWS Security Hub. Security Hub es un servicio que proporciona una visión integral de su postura de seguridad en todo su AWS entorno y le ayuda a comprobar su entorno según los estándares y las mejores prácticas del sector de la seguridad. Con Security Hub, puede supervisar y procesar los resultados de forma sencilla como parte de un análisis más completo del estado de seguridad de la organización en AWS. También puede agregar las conclusiones de varias regiones y Regiones de AWS, a continuación, supervisar y procesar los datos de las conclusiones agregadas de una sola región.

Administre de forma centralizada varias cuentas de Macie

Si su AWS entorno tiene varias cuentas, puede administrar Macie de forma centralizada para las cuentas de su entorno. Puede hacerlo de dos maneras: integrando Macie AWS Organizations o enviando y aceptando invitaciones de membresía en Macie.

En una configuración de cuentas múltiples, un administrador designado de Macie puede realizar determinadas tareas y acceder a determinados ajustes, datos y recursos de Macie para las cuentas que son miembros de la misma organización. Las tareas incluyen revisar la información sobre los grupos de S3 que son propiedad de las cuentas de los miembros, revisar las conclusiones de las políticas para esos grupos e inspeccionar los grupos para detectar datos confidenciales. Si las cuentas están asociadas directamente AWS Organizations, el administrador de Macie también puede habilitar Macie para las cuentas de los miembros de la organización.

Desarrolle y administre los recursos mediante programación

Además de la consola de Amazon Macie, puede interactuar con Macie mediante la API de Amazon Macie. La API de Amazon Macie le proporciona un acceso completo y programático a la configuración, los datos y los recursos de su cuenta de Macie.

Para interactuar con Macie mediante programación, puede enviar solicitudes HTTPS directamente a Macie o utilizar una versión actual de una herramienta de línea de AWS comandos o un SDK. AWS AWS proporciona herramientas y SDK que consisten en bibliotecas y código de muestra para varios lenguajes y plataformas, como Java PowerShell, Go, Python, C++ y.NET.

Acceso a Amazon Macie

Amazon Macie está disponible en la mayoría. Regiones de AWS Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie en la Referencia general de AWS. Para obtener información sobre cómo administrar Regiones de AWS su cuenta Cuenta de AWS, consulte Especificar qué Regiones de AWS cuenta puede usar en la Guía de AWS Account Management referencia.

En cada región, puede trabajar con Macie de cualquiera de las siguientes maneras.

AWS Management Console

AWS Management Console Se trata de una interfaz basada en un navegador que puede utilizar para crear y gestionar AWS recursos. Como parte de esa consola, la consola de Amazon Macie proporciona acceso a su cuenta, datos y recursos de Macie. Puede realizar cualquier tarea de Macie mediante la consola de Macie: revise las estadísticas y otra información sobre sus buckets de S3, cree y ejecute tareas de descubrimiento de datos confidenciales, revise y analice los resultados, etc.

AWS herramientas de línea de comandos

Con las herramientas de línea de AWS comandos, puede emitir comandos en la línea de comandos de su sistema para realizar tareas y AWS tareas de Macie. Usar la línea de comandos puede ser más rápido y práctico que usar la consola. Las herramientas de línea de comandos también son útiles si desea crear scripts que realicen tareas.

AWS proporciona dos conjuntos de herramientas de línea de comandos: el AWS Command Line Interface (AWS CLI) y el AWS Tools for PowerShell. Para obtener información sobre la instalación

y el uso de AWS CLI, consulte la Guía del AWS Command Line Interface usuario. Para obtener información sobre la instalación y el uso de las herramientas PowerShell, consulte la Guía del AWS Tools for PowerShell usuario.

AWS SDK

AWS proporciona SDK que constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas, por ejemplo, Java, Go, Python, C++ y.NET. Los SDK proporcionan un acceso práctico y programático a Macie y a otros. Servicios de AWS También permiten realizar tareas como firmar solicitudes criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre la instalación y el uso de los AWS SDK, consulte Herramientas sobre las que basarse. AWS

API de REST de Amazon Macie

La API de REST de Amazon Macie le proporciona un acceso completo y programático a su cuenta, datos y recursos de Macie. Con esta API, puede enviar solicitudes HTTPS directamente a Macie. Sin embargo, a diferencia de las herramientas de línea de AWS comandos y los SDK, el uso de esta API requiere que tu aplicación gestione detalles de bajo nivel, como la generación de un hash para firmar una solicitud. Para obtener más información acerca de esta API, consulte Referencia de la API de Amazon Macie.

Precios de Amazon Macie

Al igual que con otros AWS productos, no hay contratos ni compromisos mínimos para usar Amazon Macie.

Los precios de Macie se basan en varias dimensiones: evaluar y monitorear los segmentos de S3 para garantizar la seguridad y el control de acceso, monitorear los objetos de S3 para detectar automáticamente datos confidenciales y analizar los objetos de S3 para detectar y reportar datos confidenciales en los objetos. Para obtener más información, consulte Precios de Amazon Macie.

Para ayudarlo a comprender y pronosticar el costo de usar Macie, Macie proporciona los costos de uso estimados de su cuenta. Puede revisar estas estimaciones en la consola de Amazon Macie y acceder a ellas con la API de Amazon Macie. En función de cómo utilice el servicio, podría incurrir en costes adicionales si utiliza otras funciones de Macie Servicios de AWS en combinación con determinadas funciones, como la recuperación de datos de los buckets de Amazon S3 y el uso de la tecnología gestionada por el cliente AWS KMS keys para descifrar objetos para su análisis.

Al activar Macie por primera vez, se inscribirá automáticamente en la versión de prueba Cuenta de AWS gratuita de 30 días de Macie. Esto incluye cuentas individuales habilitadas como parte de una organización en AWS Organizations. Durante la prueba gratuita, el uso de Macie en la versión aplicable para evaluar y monitorizar sus buckets de S3 Región de AWS con fines de seguridad y control de acceso es gratuito. Según la configuración de su cuenta, la prueba gratuita también puede incluir la detección automática de datos confidenciales para sus datos de Amazon S3. La prueba gratuita no incluye la ejecución de trabajos de detección de información confidencial para detectar e informar de información confidencial en objetos de S3.

Para ayudarle a comprender y pronosticar el costo de utilizar Macie una vez finalizada la prueba gratuita, Macie le proporciona una estimación de los costos de uso en función del uso de Macie durante la prueba. Sus datos de uso también indican el tiempo que queda hasta que finalice la prueba gratuita. Puede revisar estos datos en la consola de Amazon Macie y acceder a ellos con la API de Amazon Macie.

Servicios relacionados

Para proteger aún más sus datos, cargas de trabajo y aplicaciones AWS, considere usar lo siguiente Servicios de AWS en combinación con Amazon Macie.

AWS Security Hub

AWS Security Hub le ofrece una visión completa del estado de seguridad de sus AWS recursos y le ayuda a comprobar si su AWS entorno se ajusta a los estándares y las mejores prácticas del sector de la seguridad. Esto lo consigue, en parte, consumiendo, agrupando, organizando y priorizando las conclusiones de seguridad procedentes de varios productos Servicios de AWS (incluido Macie) y de AWS Partner Network (APN) compatibles. Security Hub le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios en todo su AWS entorno.

Para obtener más información sobre Security Hub, consulte la AWS Security Hub Guía del usuario. Para obtener información sobre el uso conjunto de Macie y Security Hub, consulte Integración de Amazon Macie con AWS Security Hub.

Amazon GuardDuty

Amazon GuardDuty es un servicio de supervisión de seguridad que analiza y procesa determinados tipos de AWS registros, como los registros de eventos de AWS CloudTrail datos para Amazon S3 y los registros CloudTrail de eventos de administración. Utiliza fuentes

de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, y el aprendizaje automático para identificar actividades inesperadas y potencialmente no autorizadas y maliciosas en su AWS entorno.

Para obtener más información GuardDuty, consulta la Guía del GuardDuty usuario de Amazon.

Para obtener más información sobre los servicios de AWS seguridad adicionales, consulte Seguridad, identidad y conformidad en AWS.

Introducción a Amazon Macie

En este tutorial, solo se proporciona una introducción a Amazon Macie. Aprenderá a habilitar Macie para suc Cuenta de AWS. También aprenderá a evaluar su postura de seguridad del Amazon Simple Storage Service (Amazon S3) y a configurar los ajustes y recursos clave para detectar y reportar datos confidenciales en sus buckets de S3.

Tareas

Antes de empezar

Cuando se registra en Amazon Web Services (AWS), su cuenta se registra automáticamente para todos los Servicios de AWS, incluido Amazon Macie. Sin embargo, para habilitar y utilizar Macie, primero tiene que configurar permisos que permitan acceder a la consola de Amazon Macie y a las operaciones de la API. Para ello, usted o su AWS administrador pueden utilizar AWS Identity and Access Management (IAM) para adjuntar la política AWS gestionada nombrada `AmazonMacieFullAccess` a su identidad de IAM. Para obtener más información, consulte Políticas administradas por AWS para Amazon Macie.

Paso 1: Habilitar Amazon Macie

Después de configurar los permisos necesarios, puede habilitar Amazon Macie para su Cuenta de AWS. Siga estos pasos para habilitar Macie para su cuenta.

Para habilitar Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee activar y utilizar Macie.

3. En la página de Amazon Macie, seleccione Comenzar.
4. (Opcional) Al activar Macie, Macie crea automáticamente un rol vinculado al servicio que otorga a Macie los permisos necesarios para llamar a otras personas y supervisar los recursos en tu nombre. Servicios de AWS AWS Para revisar la política de permisos de este rol, selecciona Ver los permisos del rol en la consola. Para obtener más información sobre este rol, consulte Roles vinculados a servicios para Amazon Macie.
5. Seleccione Habilitar Macie.

En cuestión de minutos, Macie genera automáticamente y comienza a mantener un inventario completo de sus depósitos de uso general de S3 en la región actual. Macie también comienza a evaluar y monitorear los buckets para ofrecer seguridad y control de acceso. Para obtener más información, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.

En función de la configuración de su cuenta, Macie también comienza a realizar la detección automática de datos confidenciales para sus buckets de S3. Macie comienza a identificar, seleccionar y analizar continuamente los objetos representativos de sus depósitos, inspeccionándolos en busca de datos confidenciales. A medida que avanzan los análisis, Macie proporciona estadísticas y otros resultados que puede revisar, normalmente en un plazo de 48 horas desde la activación de Macie en su cuenta. Puede personalizar los análisis configurando los ajustes de detección automática de datos confidenciales para su cuenta. Para obtener más información, consulte Cómo funciona la detección automatizada de datos confidenciales.

Para revisar las estadísticas agregadas de sus datos de Amazon S3, seleccione Resumen en el panel de navegación de la consola. Para revisar los detalles de los buckets de S3 individuales de su inventario, elija los grupos de buckets de S3 en el panel de navegación. Para mostrar a continuación los detalles de un bucket, elija el bucket. El panel de detalles muestra estadísticas y otra información que proporciona información sobre la seguridad, privacidad y confidencialidad de los datos del bucket. Para obtener más información sobre estos detalles, consulte Revisar el inventario de bucket de S3.

Paso 2: Configurar un repositorio para los resultados de detección de datos confidenciales

Con Amazon Macie, puede detectar datos confidenciales en sus buckets de S3 de dos maneras: configurando Macie para que realice una detección automática de datos confidenciales y ejecutando tareas de detección de datos confidenciales. Un trabajo de detección de datos confidenciales es

un trabajo que se crea para analizar los objetos de los buckets de S3 y determinar si los objetos contienen datos confidenciales.

Macie crea un registro para cada objeto de S3 que analiza cuando usted ejecuta tareas de descubrimiento de datos confidenciales o cuando realiza un descubrimiento automatizado de datos confidenciales. Estos registros, denominados resultados del detección de datos confidenciales, registran detalles sobre el análisis de objetos individuales. Macie también crea resultados de detección de datos confidenciales para objetos que no puede analizar debido a errores o problemas. Los resultados del detección de datos confidenciales le proporcionan registros de análisis que pueden resultar útiles para auditorías o investigaciones sobre la privacidad y la protección de los datos.

Macie almacena los resultados de la detección de datos confidenciales solo durante 90 días. Para acceder a los resultados y permitir su almacenamiento y retención a largo plazo, configure Macie para que almacene los resultados en un bucket de S3. Debe hacerlo en un plazo de 30 días a partir de la activación de Macie. Una vez hecho esto, el bucket puede servir como un repositorio definitivo y a largo plazo para todos sus resultados de detección de datos confidenciales.

Para obtener información sobre cómo configurar este repositorio, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Paso 3: Explorar los resultados de muestra

En Amazon Macie, hay dos categorías de hallazgos: los hallazgos de políticas y los hallazgos de datos confidenciales. Macie crea una constatación de políticas cuando las políticas o la configuración de un segmento de uso general de S3 se modifican de forma que se reduce la seguridad o la privacidad del depósito y de los objetos del mismo. Macie crea un resultado de datos confidenciales cuando detecta datos confidenciales en un objeto de S3. Dentro de cada categoría, hay varios tipos de resultados.

Para explorar y conocer las diferentes categorías y tipos de resultados que proporciona Macie, si lo desea, cree y revise ejemplos de resultados. Los resultados de la muestra utilizan datos de ejemplo y valores de marcador de posición para demostrar los tipos de información que Macie podría incluir en cada tipo de resultado.

Siga estos pasos para crear y revisar los resultados de las muestras.

Para crear y revisar ejemplos de resultados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. En el panel de navegación, seleccione Configuración.
3. En Muestra de resultados, seleccione Generar muestra de resultados. Macie genera una muestra de resultado para cada tipo de resultado respaldado por Macie.
4. En el panel de navegación, seleccione Resultados. La página de Resultados muestra los resultados de su cuenta en la versión actual Región de AWS. Esto incluye los resultados de muestra que creó en el paso anterior.
5. En la página Resultados, localice los resultados cuyo tipo comience por [MUESTRA].
6. Para revisar los detalles de un resultado de muestra en particular, elija el resultado. El panel de detalles muestra los detalles del resultado.

Para obtener más información sobre cada tipo de resultado, consulte Tipos de hallazgos. Para obtener más información sobre cómo crear y revisar ejemplos de resultados, consulte Trabajar con muestras de resultados.

Paso 4: Crear un trabajo para descubrir datos confidenciales

Para detectar y reportar datos confidenciales en buckets de S3, puede ejecutar trabajos de detección de datos confidenciales. Un trabajo de detección de datos confidenciales es un trabajo que se crea para analizar los objetos de los buckets de S3 y determinar si los objetos contienen datos confidenciales. A diferencia del detección automatizado de datos confidenciales, usted define la amplitud y profundidad del análisis. También puede especificar la frecuencia con la que se debe ejecutar un trabajo: una vez o periódicamente de forma programada.

Siga estos pasos para crear un trabajo que se ejecute una vez, inmediatamente después de crearlo, y utilice la configuración predeterminada. Para obtener información sobre cómo crear un trabajo que se ejecute periódicamente o utilice configuraciones personalizadas, consulte Creación de un trabajo de detección de datos confidenciales.

Crear un trabajo de detección de información confidencial

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Trabajos.
3. Seleccione Crear trabajo.
4. Para el paso Elegir buckets S3, seleccione Seleccionar buckets específicos. A continuación, en la tabla, seleccione la casilla de verificación de cada bucket de S3 que desea que el trabajo analice.

La tabla proporciona un inventario completo de los cubos de uso general de S3 actuales. Región de AWS Para encontrar buckets específicos más fácilmente, introduzca los criterios de filtro en el cuadro de filtro situado sobre la tabla. También puede ordenar la tabla si elige un encabezado de columna en la tabla.

5. Cuando termine de seleccionar los buckets, elija Siguiente.
6. Para el paso Revisar los buckets de S3, revise y verifique tus selecciones de buckets y, a continuación, seleccione Siguiente.
7. Para el paso Refinar el alcance, seleccione Trabajo único y, a continuación, selecciona Siguiente.
8. Para el paso Seleccionar identificadores de datos gestionados, seleccione Recomendado. Si lo desea, revise la tabla de identificadores de datos gestionados que recomendamos para los trabajos y, a continuación, seleccione Siguiente.

   Un identificador de datos gestionado es un conjunto de criterios y técnicas integrados que están diseñados para detectar un tipo específico de datos confidenciales, por ejemplo, números de tarjetas de crédito, claves de acceso AWS secretas o números de pasaporte de un país o región determinados. Para obtener más información, consulte Uso de identificadores de datos administrados.
9. Para el paso Seleccionar identificadores de datos personalizados, seleccione Siguiente.

   Un identificador de datos personalizado es un conjunto de criterios que usted define para detectar datos confidenciales: una expresión regular (regex) que define un patrón de texto para coincidir y, opcionalmente, secuencias de caracteres y una regla de proximidad que refina los resultados. Para obtener más información, consulte Creación de identificadores de datos personalizados.
10. Para el paso Seleccionar listas permitidas, elija Siguiente.

    En Amazon Macie, una lista de permitidos especifica un texto o un patrón de texto que Macie debe ignorar al inspeccionar objetos de S3 en busca de datos confidenciales. Por lo general, se trata de excepciones de datos confidenciales para escenarios o entornos particulares. Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.
11. Para el paso Introducir la configuración general, introduzca un nombre y, si lo desea, una descripción del trabajo. A continuación, elija Siguiente.

12. Para el paso Revisar y crear revise los ajustes de configuración del trabajo y verifique que sean correctos.

    También puede revisar el costo total estimado (en USD) de ejecutar el trabajo. La estimación puede ayudarle a determinar si debe ajustar la configuración del trabajo antes de guardarlo. Para obtener más información, consulte Previsión del costo de un trabajo de detección de información confidencial.
13. Cuando termine de revisar y verificar la configuración del trabajo, seleccione Enviar.

Macie comienza inmediatamente a ejecutar el trabajo. Para obtener información sobre cómo supervisar el trabajo, consulte Comprobar el estado de los trabajos de detección de datos confidenciales.

Paso 5: Revisar sus resultados

Amazon Macie supervisa automáticamente los depósitos de uso general de S3 para garantizar la seguridad y el control de acceso, y elabora conclusiones de políticas para informar sobre posibles problemas con la seguridad o la privacidad de los depósitos. Si realiza un trabajo de descubrimiento de datos confidenciales o configura a Macie para que realice una detección automática de datos confidenciales, Macie crea datos confidenciales para informar sobre los datos confidenciales que detecta en los objetos de S3. Para obtener más información sobre los resultados, consulte Análisis de resultados.

Siga estos pasos para revisar sus resultados.

Visualizar los resultados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (resultados). La página de Resultados muestra los resultados de su cuenta en la versión actual Región de AWS.
3. (Opcional) Para filtrar los resultados por criterios específicos, introduce los criterios en el cuadro de filtro situado encima de la tabla.
4. Para ver los detalles de un resultado, elija el título del resultado. El panel de detalles muestra los detalles del resultado.

Para obtener más información, incluido cómo agrupar y filtrar los resultados, consulte Revisión de resultados.

Conceptos y terminología de Amazon Macie

En Amazon Macie, nos basamos en AWS conceptos y terminología comunes y utilizamos estos términos adicionales.

cuenta

Un estándar Cuenta de AWS que contiene sus AWS recursos y las identidades que pueden acceder a esos recursos.

Para usar Macie, inicie sesión AWS con sus Cuenta de AWS credenciales, seleccione el lugar Región de AWS en el que desee usar Macie y, a continuación, habilite Macie para usted Cuenta de AWS en esa región. Para obtener más información, consulte Introducción a Amazon Macie.

Existen tres tipos de cuentas en Macie:

- Cuenta de administrador: este tipo de cuenta administra las cuentas de Macie de una organización. Una organización es un conjunto de cuentas de Macie que se asocian entre sí y se administran de forma centralizada como un grupo de cuentas asociadas en un Región de AWS específico.
- Cuenta de miembro: este tipo de cuenta está asociada y gestionada por la cuenta de administrador de Macie de una organización.
- Cuenta independiente: este tipo de cuenta no es una cuenta de administrador ni de miembro. No forma parte de una organización.

Puedes añadir cuentas de Macie a una organización de dos maneras: integrando Macie con AWS Organizations o enviando y aceptando invitaciones de membresía de Macie. Para obtener más información, consulte Administración de varias cuentas .

cuenta de administrador

En Macie, una cuenta que administra las cuentas de Macie para una organización. Una organización es un conjunto de cuentas de Macie que se asocian entre sí y se administran de forma centralizada como un grupo de cuentas asociadas en un Región de AWS específico.

Los usuarios de una cuenta de administrador de Macie tienen acceso a los datos de inventario de Amazon Simple Storage Service (Amazon S3), a los resultados de políticas y a ciertas

configuraciones y recursos de Macie para todas las cuentas de su organización. El administrador también puede realizar la detección automatizada de datos confidenciales y ejecutar trabajos de detección de datos confidenciales para detectar dichos datos en los buckets de S3 propiedad de las cuentas de miembros. Según cómo se designe una cuenta como cuenta de administrador, es posible que también puedan realizar tareas adicionales para otras cuentas de su organización.

Para obtener más información, consulte Administración de varias cuentas .

lista de permitidos

En Amazon Macie, una lista de permitidos especifica un texto o un patrón de texto que Macie debe ignorar al inspeccionar objetos de S3 en busca de datos confidenciales.

Puede crear dos tipos de listas de permitidos en Macie: un archivo de texto sin formato que enumera palabras específicas y otros tipos de secuencias de caracteres que se van a ignorar o una expresión regular (regex) que define el patrón del texto que se va a ignorar. Si un objeto contiene texto que coincide con una entrada o patrón en una lista de permitidos, Macie no notifica el texto en resultados de datos confidenciales, estadísticas y otros tipos de resultados, incluso si el texto coincide con los criterios de un identificador de datos administrados o un identificador de datos personalizado.

Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

detección automatizada de datos confidenciales

Una serie de actividades de análisis automatizadas que Macie realiza continuamente para identificar y seleccionar objetos representativos de los buckets de S3 e inspeccionar los objetos seleccionados en busca de datos confidenciales.

A medida que avanzan los análisis, Macie crea registros de los datos confidenciales que encuentra (resultados de datos confidenciales) y de los análisis que realiza (resultados del detección de datos confidenciales). Macie también actualiza las estadísticas y otra información que proporciona sobre los datos de Amazon S3.

Para obtener más información, consulte Realización de la detección automatizada de datos confidenciales.

AWS Formato de búsqueda de seguridad (ASFF)

Formato JSON estandarizado para el contenido de las conclusiones publicadas o generadas por AWS Security Hub. El ASFF incluye detalles sobre el origen del problema de seguridad, los recursos afectados y el estado actual del resultado.

Para obtener más información sobre ASFF, consulte Formato de resultados de seguridad (ASFF) de AWS en la Guía del usuario AWS Security Hub . Para obtener información sobre cómo publicar los resultados de Macie en Security Hub, consulte Integración de Amazon Macie con AWS Security Hub.

bytes o tamaño clasificables

En las estadísticas del bucket de S3 que proporciona Macie, el tamaño total de almacenamiento de todos los objetos clasificables de un bucket de S3.

Si el control de versiones está activado para un bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto clasificable del bucket. Si un objeto es un archivo comprimido, este valor no refleja el tamaño real del contenido del archivo después de descomprimirlo.

Para obtener más información, consulte Revisar el inventario de bucket de S3 y Evaluación de la postura de seguridad de Amazon S3.

objeto clasificable

Un objeto de S3 que Macie puede analizar para detectar datos confidenciales.

Al calcular las estadísticas del bucket de S3, Macie determina que un objeto es clasificable según la clase de almacenamiento del objeto y la extensión del nombre del archivo. Un objeto es clasificable si utiliza una clase de almacenamiento Amazon S3 compatible y tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible.

Para obtener más información, consulte Revisar el inventario de bucket de S3 y Evaluación de la postura de seguridad de Amazon S3.

Para la detección de datos confidenciales, Macie determina que un objeto se puede clasificar en función de la clase de almacenamiento, la extensión del nombre de archivo y el contenido del objeto. Un objeto es clasificable si: utiliza una clase de almacenamiento de Amazon S3 compatible, tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido y Macie ha comprobado que puede extraer y analizar datos del objeto.

Para obtener más información, consulte Detección de datos confidenciales y Previsión y supervisión de costos.

identificador de datos personalizado

Un conjunto de criterios que define para detectar información confidencial.

Los criterios consisten en una expresión regular (regex) que define un patrón de texto para que coincida y, opcionalmente, secuencias de caracteres y una regla de proximidad que perfeccionen los resultados. Las secuencias de caracteres pueden ser las siguientes:

- Palabras clave, que son palabras o frases que deben estar cerca del texto que coincida con la expresión regular o
- Ignorar palabras, que son palabras o frases que se excluyen de los resultados.

Además de los criterios de detección, puede definir ajustes de gravedad personalizados para los resultados de datos confidenciales que produzca un identificador de datos personalizado.

Para obtener más información, consulte Creación de identificadores de datos personalizados.

regla de filtro

Conjunto de criterios de filtrado basados en atributos que puede crear y guardar para analizar los resultados en la consola de Amazon Macie. Las reglas de filtrado pueden ayudarlo a realizar un análisis coherente de los resultados que tienen características específicas, como todos los resultados de alta gravedad que reportan un tipo específico de datos confidenciales.

Para obtener más información, consulte Creación y administración de reglas de filtrado para los resultados.

resultado

Un informe detallado de los datos confidenciales que Macie encontró en un objeto de S3 o de un posible problema con la seguridad o la privacidad de un depósito de uso general de S3. Cada resultado proporciona detalles como una clasificación de gravedad, información sobre el recurso afectado y cuándo Macie encontró los datos o el problema.

Macie genera dos categorías de resultados: datos confidenciales, para los datos confidenciales que Macie detecta en los objetos de S3, y resultados de políticas, para posibles problemas que Macie

detecta con la configuración de seguridad y control de acceso de los buckets de S3. Dentro de cada categoría, hay tipos específicos de resultados.

Para obtener más información, consulte Tipos de resultados de Amazon Macie.

evento de resultados

Un EventBridge evento de Amazon que contiene los detalles de un hallazgo de datos confidenciales o de una política.

Macie publica automáticamente las conclusiones sobre datos confidenciales y políticas en Amazon EventBridge como eventos. Un evento es un objeto JSON que se ajusta al EventBridge esquema de los eventos. AWS Puedes usar estos eventos para monitorear, procesar y actuar en función de los resultados mediante el uso de otras aplicaciones, servicios y sistemas.

Para obtener más información, consulte Integración de Amazon Macie con Amazon Eventbridge y Esquema de eventos de Amazon EventBridge para los resultados de Amazon Macie.

trabajo

Consulte el trabajo de detección de datos confidenciales.

identificador de datos administrados

Conjunto de criterios y técnicas integradas diseñados para detectar un tipo específico de datos confidenciales. Algunos ejemplos de datos confidenciales son los números de tarjetas de crédito, las claves de acceso AWS secretas o los números de pasaporte de un país o región en particular. Estos identificadores pueden detectar una lista extensa y creciente de tipos de datos confidenciales en muchos países y regiones.

Para obtener más información, consulte Uso de identificadores de datos administrados.

cuenta de miembro

Una cuenta de Macie administrada por la cuenta de administrador de Macie designada para una organización. Una organización es un conjunto de cuentas de Macie que se asocian entre sí y se administran de forma centralizada como un grupo de cuentas relacionadas en un espacio específico Región de AWS.

Una cuenta puede convertirse en una cuenta de miembro de dos maneras: integrando Macie con la organización de la cuenta AWS Organizations o aceptando una invitación de membresía de Macie.

Si tiene una cuenta de miembro, su administrador de Macie tiene acceso a los datos de inventario de Amazon S3, a los resultados de políticas y a determinados ajustes y recursos de Macie para su cuenta. El administrador también puede realizar la detección automática de datos confidenciales y ejecutar tareas de detección de datos confidenciales para detectar los datos confidenciales en sus buckets de S3. Es posible que también puedan realizar tareas adicionales para su cuenta, en función del modo en que su cuenta se haya convertido en una cuenta de miembro.

Para obtener más información, consulte Administración de varias cuentas .

organización

Conjunto de cuentas de Macie que están asociadas entre sí y que se gestionan de forma centralizada como un grupo de cuentas relacionadas en un ámbito específico. Región de AWS

Cada organización consta de una cuenta de administrador designada de Macie y una o más cuentas de miembros asociadas. La cuenta de administrador puede acceder a determinados ajustes, datos y recursos de Macie para las cuentas de los miembros. Puede crear una organización de dos maneras: integrando Macie con AWS Organizations o enviando y aceptando invitaciones de membresía en Macie.

Para obtener más información, consulte Administración de varias cuentas .

resultado de política

Un informe detallado sobre una posible infracción de la política o un problema con la configuración de seguridad y control de acceso de un segmento de uso general de S3. Los detalles incluyen un índice de gravedad, información sobre el recurso afectado y el momento en que Macie encontró el problema.

Macie genera conclusiones sobre las políticas cuando las políticas o la configuración de un depósito de uso general de S3 se modifican de forma que se reduzca la seguridad o la privacidad del depósito y de sus objetos. Macie genera estos resultados como parte de sus actividades de monitoreo continuo de sus datos de Amazon S3. Macie puede generar varios tipos de conclusiones sobre políticas.

Para obtener más información, consulte Tipos de resultados de Amazon Macie y Supervisión de la seguridad y la privacidad de los datos.

muestra de resultados

Un resultado que utiliza datos de ejemplo y valores de marcador de posición para demostrar el tipo de información que puede contener un resultado.

Para obtener más información, consulte Trabajar con muestras de resultados.

resultado de datos confidenciales

Un informe detallado de información confidencial que Macie encontró en un objeto de S3. Los detalles incluyen un índice de gravedad, información sobre el recurso afectado, el tipo y el número de ocurrencias de los datos confidenciales que ha encontrado Macie y el momento en que ha encontrado los datos confidenciales.

Macie genera datos confidenciales si detecta datos confidenciales en los objetos de S3 que analiza cuando realiza tareas de detección de datos confidenciales o si realiza un detección automatizado de datos confidenciales. Macie puede generar varios tipos de resultados de datos confidenciales.

Para obtener más información, consulte Tipos de resultados de Amazon Macie y Detección de datos confidenciales.

trabajos de detección de datos confidenciales

También se denomina trabajo a una serie de tareas automatizadas de procesamiento y análisis que Macie lleva a cabo para detectar y reportar datos confidenciales en objetos S3. Al crear un trabajo, puede especificar la frecuencia con que desea que el trabajo se ejecute y define el ámbito y la naturaleza del análisis del trabajo.

Cuando se ejecuta un trabajo, Macie genera registros de los datos confidenciales que encuentra (resultados de datos confidenciales) y de los análisis que realiza (resultados del detección de datos confidenciales). Macie también publica los datos de registro en Amazon CloudWatch Logs.

Para obtener más información, consulte Ejecución de trabajos de detección de datos confidenciales.

Resultado de la detección de datos confidenciales

Registro que registra detalles sobre el análisis que Macie realizó en un objeto S3 para determinar si el objeto contiene datos confidenciales. Macie genera y escribe estos registros en archivos JSON

Lines (.jsonl), que cifra y almacena en un bucket de S3 que usted especifique. Los registros siguen un esquema estandarizado.

Cuando realizas un trabajo de detección de datos confidenciales o Macie realiza una detección automatizada de datos confidenciales, Macie crea un resultado de detección de datos confidenciales para cada objeto incluido en el ámbito del análisis. Esto incluye:

- Objetos en los que Macie encuentra datos confidenciales y, por lo tanto, también produce resultados de datos confidenciales.
- Objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no los encuentra.
- Objetos que Macie no puede analizar debido a errores o problemas, como la configuración de los permisos o el uso de un archivo o formato de almacenamiento no compatible.

Para obtener más información, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

cuenta independiente

Una cuenta de Macie que no es una cuenta de administrador ni de miembro en una organización. La cuenta no forma parte de una organización.

resultado suprimido

Un resultado que se archivó automáticamente mediante una regla de supresión. Es decir, Macie cambió automáticamente el estado del resultado a archivado porque el resultado cumplía con los criterios de una regla de supresión cuando Macie generó el resultado.

Para obtener más información, consulte Supresión de hallazgos.

regla de supresión

Conjunto de criterios de filtrado basados en atributos que se crean y guardan para archivar (suprimir) los resultados automáticamente. Las reglas de supresión son útiles en situaciones en las que haya revisado una clase de resultados y no quiere que se le vuelva a notificar sobre ellos.

Si suprimes los resultados con una regla de supresión, Macie seguirá generando resultados que coincidan con los criterios de la regla. Sin embargo, Macie cambia automáticamente el estado de los

resultados a archivado. Esto significa que los resultados no aparecen de forma predeterminada en la consola de Amazon Macie y Macie no los publica en otras consolas Servicios de AWS.

Para obtener más información, consulte Supresión de hallazgos.

bytes o tamaño no clasibicables

En las estadísticas del bucket de S3 que proporciona Macie, el tamaño total de almacenamiento de todos los objetos no clasificables de un bucket de S3.

Si el control de versiones está activado para un bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto no clasificable del bucket. Si un objeto es un archivo comprimido, este valor no refleja el tamaño real del contenido del archivo después de descomprimirlo.

Para obtener más información, consulte Revisar el inventario de bucket de S3 y Evaluación de la postura de seguridad de Amazon S3.

objeto no clasificable

Un objeto S3 que Macie no puede analizar para detectar datos confidenciales.

Al calcular las estadísticas del bucket de S3, Macie determina que un objeto es no clasificable en función de la clase de almacenamiento y la extensión del nombre de archivo del objeto. Un objeto no es clasificable si no utiliza una clase de almacenamiento de Amazon S3 o no tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido.

Para obtener más información, consulte Revisar el inventario de bucket de S3 y Evaluación de la postura de seguridad de Amazon S3.

Para el detección de datos confidenciales, Macie determina que un objeto no se puede clasificar en función de la clase de almacenamiento, la extensión del nombre de archivo y el contenido del objeto. Un objeto no se puede clasificar si: no usa una clase de almacenamiento Amazon S3 compatible, no tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible, o Macie no pudo extraer y analizar datos del objeto. Por ejemplo, el objeto es un archivo con formato incorrecto.

Para obtener más información, consulte Detección de datos confidenciales y Previsión y supervisión de costos.

Supervisión de la seguridad y la privacidad de los datos con Amazon Macie

Cuando habilita Amazon Macie para usted Cuenta de AWS, Macie genera automáticamente y comienza a mantener un inventario completo de sus depósitos de uso general del Amazon Simple Storage Service (Amazon S3) actuales. Región de AWS Macie también comienza a evaluar y monitorear los buckets para ofrecer seguridad y control de acceso. Si Macie detecta un suceso que reduce la seguridad o la privacidad de un depósito, Macie crea una política para que la revises y la corrijas según sea necesario.

Para evaluar y supervisar también los depósitos de S3 para detectar la presencia de datos confidenciales, puede crear y ejecutar tareas de detección de datos confidenciales. Las tareas de detección de datos confidenciales pueden realizar análisis incrementales de los objetos del bucket diaria, semanal o mensualmente. En función de la configuración de su cuenta, también puede configurar Macie para que detecte datos confidenciales de forma automática. La detección automática de datos confidenciales utiliza técnicas de muestreo para identificar, seleccionar y analizar continuamente los objetos representativos de sus buckets. Si Macie detecta datos confidenciales en un objeto de S3, Macie crea un resultado de datos confidenciales para enviarle una notificación sobre los datos confidenciales que Macie ha encontrado. Para obtener más información, consulte Detección de datos confidenciales.

Además de los resultados, Macie ofrece una visibilidad constante de la seguridad y la privacidad de sus datos de Amazon S3. Para evaluar el nivel de seguridad de sus datos y determinar qué medidas tomar, puede utilizar el panel de Resumen de la consola. El panel proporciona un resumen de las estadísticas agregadas de los datos de Amazon S3. Las estadísticas incluyen datos para métricas de seguridad clave, como el número de depósitos de uso general a los que se puede acceder públicamente o que se comparten con otros. Cuentas de AWS El panel también muestra grupos de datos de resultados agregados de su cuenta, por ejemplo, los nombres de 1 a 5 buckets que generaron más resultados durante los siete días anteriores. Puede profundizar en cada estadística para revisar sus datos de respaldo. Si prefiere consultar las estadísticas mediante programación, puede utilizar el GetBucketStatisticsfuncionamiento de la API Amazon Macie.

Para un análisis y una evaluación más exhaustivos, Macie también proporciona información y estadísticas detalladas de los buckets de S3 individuales de su inventario. Esto incluye un desglose de la configuración de acceso público y cifrado de cada bucket, así como el tamaño y la cantidad de objetos que Macie puede analizar para detectar datos confidenciales en el bucket.

El inventario también indica si configuró algún trabajo de detección de datos confidenciales para analizar los objetos de un bucket y, de ser así, cuándo se ejecutó uno de esos trabajos por última vez. Puede buscar, ordenar y filtrar el inventario mediante la consola de Amazon Macie o el DescribeBucketsfuncionamiento de la API de Amazon Macie.

Si es el administrador de Macie de una organización, puede acceder a datos estadísticos y de otro tipo sobre los buckets de S3 que posean las cuentas de sus miembros. También puede acceder a los resultados de las políticas que Macie genera para los depósitos e inspeccionar los depósitos en busca de datos confidenciales. Como administrador de Macie, puede utilizar Macie para evaluar y supervisar el estado general de seguridad de la propiedad de datos de Amazon S3 de su organización. Para obtener más información, consulte Administración de varias cuentas .

Temas

- Cómo supervisa Amazon Macie la seguridad de los datos de Amazon S3
- Evaluación de la postura de seguridad de Amazon S3 con Amazon Macie
- Análisis de la posición de seguridad de Amazon S3 con Amazon Macie
- Permitir a Amazon Macie el acceso a buckets y objetos de S3

Cómo supervisa Amazon Macie la seguridad de los datos de Amazon S3

Cuando habilita Amazon Macie para su cuenta Cuenta de AWS, Macie crea un rol vinculado al servicio AWS Identity and Access Management (IAM) para su cuenta en la cuenta actual. Región de AWS La política de permisos de este rol permite a Macie llamar a otros recursos Servicios de AWS y supervisarlos en su nombre. AWS Al utilizar esta función, Macie genera y mantiene un inventario completo de los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) en la región. Macie también supervisa y evalúa los depósitos para garantizar la seguridad y el control de acceso.

Si es el administrador de Macie de una organización, el inventario incluye datos estadísticos y de otro tipo sobre los depósitos de S3 de su cuenta y de las cuentas de los miembros de su organización. Con estos datos, puede usar Macie para monitorear y evaluar el estado de seguridad de su organización en todo el patrimonio de datos de Amazon S3. Para obtener más información, consulte Administración de varias cuentas .

Temas

Componentes principales

Amazon Macie utiliza una combinación de características y técnicas para proporcionar y mantener datos de inventario sobre los depósitos de uso general de S3, y para supervisar y evaluar los depósitos con fines de seguridad y control de acceso.

Recopilación de metadatos y cálculo de estadísticas

Para generar y mantener los metadatos y las estadísticas de su inventario de buckets, Macie recupera los metadatos de los buckets y los objetos directamente de Amazon S3. Para cada bucket, los metadatos incluyen:

- Información general sobre el depósito, como el nombre del depósito, el nombre del recurso de Amazon (ARN), la fecha de creación, la configuración de cifrado, las etiquetas y el ID de Cuenta de AWS cuenta del propietario del depósito.
- Configuración de permisos a nivel de cuenta que se aplica al bucket, como la configuración de bloqueo del acceso público de la cuenta.
- Configuración de permisos a nivel de bucket para el bucket, como la configuración de bloqueo del acceso público al bucket y la configuración derivada de una política de bucket o de una lista de control de acceso (ACL).
- Configuración de acceso compartido y replicación del depósito, incluida la cuestión de si los datos del depósito se replican o se comparten con personas Cuentas de AWS que no forman parte de su organización.
- Recuentos de objetos y configuración de los objetos del bucket, como el número de objetos del bucket y los desgloses de los recuentos de objetos por tipo de cifrado, tipo de archivo y clase de almacenamiento.

Macie le proporciona esta información directamente. Macie también utiliza la información para calcular estadísticas y proporcionar evaluaciones sobre la seguridad y la privacidad del inventario de buckets en general y de los buckets individuales de su inventario. Por ejemplo, puede encontrar el tamaño total de almacenamiento y el número de buckets de su inventario, el tamaño total del almacenamiento y el número de objetos de esos buckets, y el tamaño total

del almacenamiento y el número de objetos que Macie puede analizar para detectar datos confidenciales en los buckets.

De forma predeterminada, los metadatos y las estadísticas incluyen los datos de cualquier parte del objeto que exista debido a una carga multiparte incompleta. Si actualiza manualmente los metadatos de los objetos de un bucket específico, Macie volverá a calcular las estadísticas del bucket y del inventario general del mismo, y excluirá los datos de las partes del objeto de los valores recalculados. La próxima vez que Macie recupere metadatos de buckets y objetos de Amazon S3 como parte del ciclo de actualización diario, Macie actualizará sus datos de inventario e incluirá de nuevo los datos de las partes del objeto. Para obtener información sobre cuándo recupera Macie los metadatos de los buckets y los objetos, consulte Actualizaciones de datos.

Es importante tener en cuenta que Macie no puede analizar partes de objetos para detectar datos confidenciales. Amazon S3 primero debe terminar de ensamblar las partes en uno o más objetos para que Macie los analice. Para obtener información sobre las cargas multiparte y las partes de objetos, incluido cómo eliminar partes automáticamente según las reglas del ciclo de vida, consulte Carga y copia de objetos mediante la carga multiparte en la Guía del usuario de Amazon Simple Storage Service. Para identificar los buckets que contienen partes de objetos, puede consultar las métricas de carga multiparte incompleta en Lente de almacenamiento de Amazon S3. Para obtener más información, consulte Evaluación de la actividad y el uso en la Guía del usuario de Amazon Simple Storage Service.

Supervisión de la seguridad y la privacidad de los buckets

Para garantizar la precisión de los datos a nivel de bucket de su inventario, Macie supervisa y analiza determinados eventos AWS CloudTrail que pueden producirse en los datos de Amazon S3. Si se produce un evento relevante, Macie actualiza los datos de inventario correspondientes.

Por ejemplo, si habilita la configuración de bloqueo de acceso público para un bucket, Macie actualiza todos los datos sobre la configuración de acceso público del bucket. Del mismo modo, si añade o actualiza la política de un bucket, Macie analizará la política y actualizará los datos relevantes de su inventario.

Macie monitorea y analiza los datos de los siguientes eventos: CloudTrail

- Eventos a nivel de cuenta, y DeletePublicAccessBlock PutPublicAccessBlock
- Eventos a nivel de grupo:CreateBucket,,, DeleteAccountPublicAccessBlock,, DeleteBucket,,DeleteBucketEncryption, DeleteBucketPolicy,, DeleteBucketPublicAccessBlock,DeleteBucketReplication,, DeleteBucketTagging,

PutAccountPublicAccessBlock,,PutBucketAcl, PutBucketEncryption, PutBucketPolicy, y PutBucketPublicAccessBlock PutBucketReplication PutBucketTagging PutBucketVersioning

No puede habilitar la supervisión de CloudTrail eventos adicionales ni deshabilitar la supervisión de ninguno de los eventos anteriores. Para obtener información detallada sobre las operaciones correspondientes de los eventos anteriores, consulte Referencia de la API de Amazon Simple Storage Service.

> **Tip**
>
> Para supervisar los eventos a nivel de objeto, le recomendamos que utilice la función de protección Amazon S3 de Amazon. GuardDuty Esta característica supervisa eventos de datos de Amazon S3 y los analiza en busca de actividades maliciosas y sospechosas. Para obtener más información, consulte la protección de Amazon S3 en Amazon GuardDuty en la Guía del GuardDuty usuario de Amazon.

Evaluación de la seguridad y el control de acceso de los buckets

Para evaluar la seguridad y el control de acceso a nivel de bucket, Macie utiliza un razonamiento automatizado y basado en la lógica para analizar las políticas basadas en los recursos que se aplican a un bucket. Macie también analiza la configuración de permisos a nivel de cuenta y de bucket que se aplica a un bucket. Este análisis tiene en cuenta las políticas de bucket, las ACL a nivel de bucket y la configuración de bloqueo del acceso público a la cuenta y al bucket.

Para las políticas basadas en recursos, Macie utiliza Zelkova. Zelkova es un motor de razonamiento automatizado que traduce las políticas AWS Identity and Access Management (IAM) en declaraciones lógicas y utiliza un conjunto de soluciones lógicas especializadas y de uso general (teorías de los módulos de adaptabilidad) para resolver el problema de decisión. Macie aplica Zelkova repetidamente a una política con consultas cada vez más específicas para caracterizar las clases de comportamientos que permite la política. Para obtener más información sobre la naturaleza de los solucionadores que utiliza Zelkova, consulte Teorías de los módulos de satisfactibilidad.

> **Important**
>
> Para realizar las tareas anteriores para un bucket, el bucket debe ser un bucket de uso general de S3. Macie no supervisa ni analiza los cubos de directorio de S3.

Además, se debe permitir a Macie acceder al depósito. Si la configuración de permisos de un bucket impide que Macie recupere los metadatos del bucket o de sus objetos, Macie solo podrá proporcionar un subconjunto de información sobre el bucket, como el nombre y la fecha de creación del bucket. Macie no puede realizar ningún trabajo adicional para el bucket. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Actualizaciones de datos

Cuando habilita Amazon Macie para usted Cuenta de AWS, Macie recupera los metadatos de sus buckets y objetos de uso general de S3 directamente de Amazon S3. A partir de entonces, Macie recupera automáticamente los metadatos de los cubos y objetos directamente de Amazon S3 a diario como parte de un ciclo de actualización diario.

Macie también recupera los metadatos del bucket directamente de Amazon S3 cuando se da alguno de los casos siguientes:

- Para actualizar los datos de inventario, selecciona refresh () en la consola de Amazon Macie. Puede actualizar los datos con una frecuencia de hasta cinco minutos.
- Envía una DescribeBucketssolicitud a la API de Amazon Macie mediante programación y no ha enviado ninguna DescribeBuckets solicitud en los cinco minutos anteriores.
- Macie detecta un evento relevante. AWS CloudTrail

Macie también puede recuperar los metadatos de objetos más recientes de un bucket específico si decide actualizar esos datos manualmente. Esto puede resultar útil si ha creado un bucket recientemente o ha realizado cambios importantes en los objetos de un bucket durante las últimas 24 horas. Para actualizar manualmente los metadatos de los objetos de un bucket, seleccione actualizar () en la sección Estadísticas de objetos del Panel de detalles del bucket de la página Buckets de S3 de la consola. Esta función está disponible para depósitos que almacenan 30 000 objetos o menos.

Cada vez que Macie recupera los metadatos de un bucket o un objeto, actualiza automáticamente todos los datos relevantes de su inventario. Si Macie detecta diferencias que afectan a la seguridad o la privacidad de un bucket, Macie comienza inmediatamente a evaluar y analizar los cambios.

Cuando se completa el análisis, Macie actualiza los datos relevantes de su inventario. Si alguna diferencia reduce la seguridad o la privacidad de un bucket, Macie crea también los resultados de política apropiados para que los revise y solucione como sea oportuno.

Para determinar cuándo fue la última vez que Macie recuperó los metadatos de un bucket u objeto para su cuenta, consulte el campo Última actualización de la consola. Este campo aparece en el panel de resumen, en la página de depósitos de S3 y en el panel de detalles del depósito de la página de depósitos de S3. (Si utiliza la API de Amazon Macie para consultar datos de inventario, el campo `lastUpdated` proporciona esta información). Si es el administrador de Macie de una organización, el campo Última actualización indica la fecha y hora más antiguas en que Macie recuperó los datos de una cuenta de su organización.

En raras ocasiones, y en determinadas condiciones, la latencia y otros problemas pueden impedir que Macie recupere los metadatos de los buckets y los objetos. También pueden retrasar las notificaciones que recibe Macie sobre los cambios en su inventario de buckets o la configuración de permisos y las políticas de los buckets individuales. Por ejemplo, los problemas de entrega relacionados con CloudTrail los eventos pueden provocar retrasos. Si esto sucede, Macie analiza los datos nuevos y actualizados la próxima vez que realice la actualización diaria, que es dentro de las 24 horas.

Consideraciones adicionales

Cuando utilice Amazon Macie para supervisar y evaluar el nivel de seguridad de sus datos de Amazon S3, tenga en cuenta lo siguiente:

- Los datos de inventario solo se aplican a los depósitos de uso general de S3 en la actualidad Región de AWS. Para acceder a los datos de otras regiones, habilite y use Macie en cada región adicional.
- Si es el administrador de Macie de una organización, solo podrá acceder a los datos de inventario de una cuenta de miembro si Macie está habilitada para esa cuenta en la región actual.
- Si la configuración de permisos de un bucket impide que Macie recupere información sobre el bucket o sus objetos, Macie no podrá evaluar ni supervisar la seguridad y la privacidad de los datos del bucket ni proporcionar información detallada sobre el bucket.

  Para ayudarle a identificar un bucket en ese caso, Macie hace lo siguiente:

  - En su inventario de buckets, Macie muestra un icono de advertencia (⚠) para el bucket. Para ver los detalles del depósito, Macie muestra solo un subconjunto de campos

y datos: el ID de cuenta del Cuenta de AWS propietario del depósito; el nombre del depósito, el nombre del recurso de Amazon (ARN), la fecha de creación y la región; y la fecha y la hora en que Macie recuperó por última vez los metadatos del depósito y del objeto del depósito como parte del ciclo de actualización diario. Si utiliza la API de Amazon Macie para consultar los datos de inventario, Macie proporciona un código y un mensaje de error para el bucket y el valor de la mayoría de las propiedades del bucket es nulo.

- En el panel Resumen, el bucket tiene el valor Desconocido para las estadísticas de Acceso público, Cifrado y Uso compartido. (Si utiliza la API de Amazon Macie para consultar las estadísticas, el bucket tiene un valor de `unknown` para estas estadísticas). Además, Macie excluye el bucket cuando calcula los datos para las estadísticas de Almacenamiento y Objetos.

Para investigar el problema, revise la política y la configuración de permisos del bucket en Amazon S3. Por ejemplo, el bucket puede tener una política de bucket restrictiva. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

- Los datos sobre el acceso y los permisos se limitan a la configuración a nivel de cuenta y de bucket. No refleja la configuración a nivel de objeto que determina el acceso a objetos específicos de un bucket. Por ejemplo, si el acceso público está habilitado para un objeto específico de un bucket, Macie no informa de que el bucket o los objetos del bucket sean de acceso público.

  Para supervisar las operaciones a nivel de objeto e identificar posibles riesgos de seguridad, le recomendamos que utilice la función de protección Amazon S3 de Amazon. GuardDuty Esta característica supervisa eventos de datos de Amazon S3 y los analiza en busca de actividades maliciosas y sospechosas. Para obtener más información, consulte la protección de Amazon S3 en Amazon GuardDuty en la Guía del GuardDuty usuario de Amazon.
- Si actualiza manualmente los metadatos de los objetos de un bucket específico, Macie mostrará temporalmente el informe Desconocido para obtener estadísticas de cifrado aplicables a los objetos. La próxima vez que Macie actualice los datos diariamente (en un plazo de 24 horas), Macie volverá a evaluar los metadatos de cifrado de los objetos y volverá a generar datos cuantitativos para las estadísticas.
- Si actualizas manualmente los metadatos de los objetos de un segmento específico, Macie excluye temporalmente los datos de cualquier parte del objeto que contenga el depósito debido a que las cargas de varias partes están incompletas. La próxima vez que Macie actualice los datos a diario (en un plazo de 24 horas), volverá a calcular los recuentos y los valores del tamaño de almacenamiento de los objetos del bucket e incluirá los datos de las partes en esos cálculos.
- En raras ocasiones, es posible que Macie no pueda determinar si un bucket es de acceso público o compartido, o que necesite cifrar los objetos nuevos en el servidor. Por ejemplo, un problema

temporal podría impedir que Macie recupere y analice los datos necesarios. O bien, es posible que Macie no pueda determinar completamente si una o más declaraciones de política otorgan acceso a una entidad externa. En estos casos, Macie envía un informe Desconocido para las estadísticas y los campos relevantes del inventario. Para investigar estos casos, revise la política y la configuración de permisos del bucket en Amazon S3.

Tenga en cuenta también que Macie solo genera resultados sobre las políticas si se reduce la seguridad o la privacidad de un bucket después de habilitar Macie en su cuenta. Por ejemplo, si inhabilitas la configuración de bloqueo de acceso público de un bucket después de activar Macie, Macie generará un archivo Policy:iamUser/S3 para el bucket. BlockPublicAccessDisabled Sin embargo, si la configuración de bloquear el acceso público estaba deshabilitada en un bucket cuando activaste Macie y sigue estando deshabilitada, Macie no generará ninguna búsqueda de Policy:iamUser/S3 para el bucket. BlockPublicAccessDisabled

Además, cuando Macie evalúa la seguridad y la privacidad de un bucket, no examina los registros de acceso ni analiza los usuarios, las funciones y otras configuraciones relevantes de las cuentas. En su lugar, Macie analiza los datos e informa sobre los ajustes clave que indican posibles riesgos de seguridad. Por ejemplo, si el resultado de una política indica que un bucket es de acceso público, no significa necesariamente que una entidad externa haya accedido al bucket. Del mismo modo, si la conclusión de una política indica que un depósito se comparte con una persona Cuenta de AWS ajena a tu organización, Macie no intentará determinar si este acceso está previsto y es seguro. Por el contrario, estos resultados indican que una entidad externa podría acceder a los datos del bucket, lo que podría suponer un riesgo de seguridad imprevisto.

Evaluación de la postura de seguridad de Amazon S3 con Amazon Macie

Para evaluar el nivel de seguridad de sus datos de Amazon Simple Storage Service (Amazon S3) y determinar qué medidas tomar, puede utilizar el panel de Resumen de la consola de Amazon Macie.

El panel de Resumen proporciona una instantánea de las estadísticas agregadas de sus datos de Amazon S3 en la Región de AWS actual. Las estadísticas incluyen datos para métricas de seguridad clave, como la cantidad de depósitos de uso general a los que se puede acceder públicamente o que se comparten con otros Cuentas de AWS. El panel también muestra grupos de datos de resultados agregados de su cuenta, por ejemplo, los tipos de resultados que tuvieron el mayor número de casos durante los siete días anteriores. Si es el administrador de Macie de una organización, el panel

proporciona estadísticas y datos agregados de todas las cuentas de su organización. Si lo desea, puede filtrar los datos por cuenta.

Para realizar un análisis más profundo, puede desglosar y revisar los datos de respaldo de los elementos individuales del panel de control. También puede revisar y analizar su inventario de cubos de S3 mediante la consola de Amazon Macie, o consultar y analizar los datos de inventario mediante programación mediante el DescribeBucketsfuncionamiento de la API de Amazon Macie.

Temas

Mostrar el panel Resumen

En la consola de Amazon Macie, el panel Resumen proporciona una instantánea de las estadísticas agregadas y los datos de resultados de sus datos de Amazon S3 en la Región de AWS actual. Si prefiere consultar las estadísticas mediante programación, puede utilizar el GetBucketStatisticsfuncionamiento de la API de Amazon Macie.

Para mostrar el panel Resumen

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Resumen. Macie muestra el panel Resumen.
3. Para determinar cuándo fue la última vez que Macie recuperó metadatos de buckets u objetos de Amazon S3 para su cuenta, consulte el campo Última actualización en la parte superior del panel de control. Para obtener más información, consulte Actualizaciones de datos.
4. Para profundizar y revisar los datos de respaldo de un elemento del panel de control, selecciónelo.

Si es el administrador de Macie de una organización, el panel muestra estadísticas y datos agregados de su cuenta y de las cuentas de miembros de la organización. Para filtrar el panel y mostrar los datos solo para una cuenta determinada, especifique el ID de la cuenta en el cuadro Cuenta en la parte superior del panel.

Descripción de los componentes del panel Resumen

En el panel Resumen, las estadísticas y los datos están organizados en varias secciones. En la parte superior del panel, encontrará estadísticas agregadas que indican la cantidad de datos que almacena en Amazon S3 y la cantidad de esos datos que Amazon Macie puede analizar para detectar datos confidenciales. También puede consultar el campo Última actualización para determinar cuándo Macie recuperó por última vez los metadatos de buckets u objetos de Amazon S3 para su cuenta. Las secciones adicionales proporcionan estadísticas y datos de resultados recientes que pueden ayudarlo a evaluar la seguridad, la privacidad y la confidencialidad de sus datos de Amazon S3 en la Región de AWS actual.

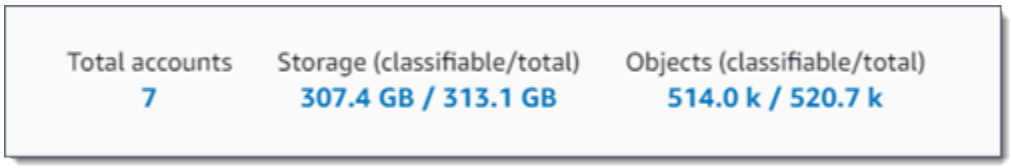
Las estadísticas y los datos están organizados en las siguientes secciones:

Almacenamiento y detección de datos confidenciales | Detección automatizada y problemas de cobertura | Seguridad de los datos | Principales buckets de S3 | Principales tipos de resultados | Resultados de política

Al revisar cada sección, si lo desea, elija un elemento para desglosar y revisar los datos de respaldo. Tenga en cuenta también que el panel de control no incluye datos de los buckets de directorios de S3, solo de los buckets de uso general. Macie no monitorea ni analiza los depósitos de directorios.

Almacenamiento y detección de datos confidenciales

Las estadísticas de la parte superior del panel indican cuántos datos almacena en Amazon S3 y cuántos de esos datos puede analizar Macie para detectar datos confidenciales. Por ejemplo:



En esta sección:

- Total de cuentas: este campo aparece si es el administrador de Macie de una organización o si tiene una cuenta de Macie independiente. Indica el número total de Cuentas de AWS cubos propios en tu inventario de cubos. Si es administrador de Macie, este es el número total de cuentas de Macie que administra para su organización. Si tiene una cuenta Macie independiente, este valor es 1.

Total de buckets de S3: este campo aparece si su cuenta de Macie es miembro de una organización. Indica el número total de cubos de uso general de tu inventario, incluidos los cubos que no almacenan ningún objeto.

- Almacenamiento: estas métricas proporcionan información sobre el tamaño de almacenamiento de los objetos de su inventario de buckets:
  - Clasificable: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar en los buckets.
  - Total: el tamaño total de almacenamiento de todos los objetos de los buckets, incluidos los objetos que Macie no puede analizar.

  Si alguno de los objetos son archivos comprimidos, estos valores no reflejan el tamaño real de esos archivos una vez descomprimidos. Si el control de versiones está habilitado para alguno de los buckets, estos valores se basan en el tamaño de almacenamiento de la última versión de cada objeto de esos buckets.
- Objetos: estas métricas ofrecen información sobre el número de objetos en su inventario de buckets:
  - Clasificable el número total de objetos que Macie puede analizar en los buckets.
  - Total: el número total de objetos de los buckets, incluidos los objetos que Macie no puede analizar.

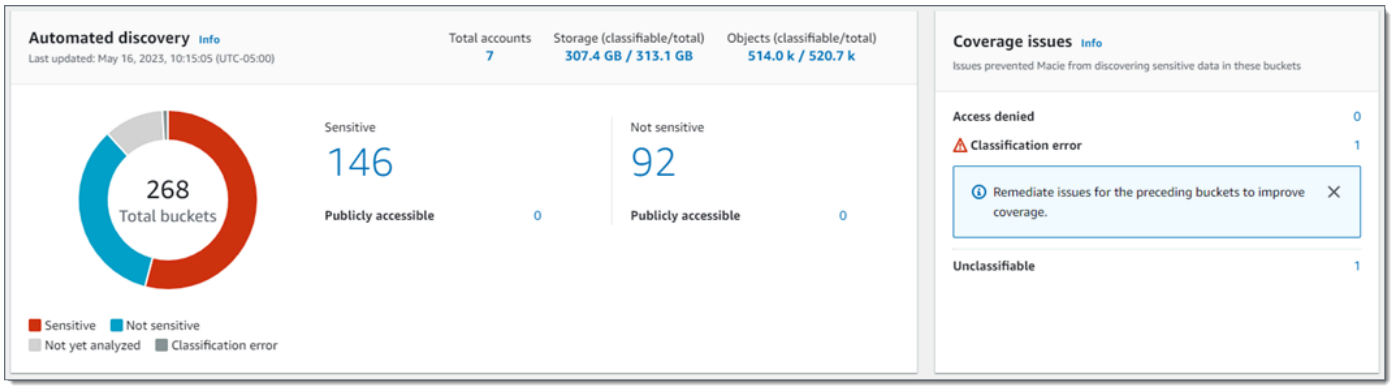
En las estadísticas anteriores, los objetos son clasificables si utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Puede detectar datos confidenciales en los objetos mediante Macie. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

Tenga en cuenta que las estadísticas de Almacenamiento y Objetos no incluyen datos sobre los objetos de los buckets a los que Macie no puede acceder. Por ejemplo, los objetos de los buckets que tienen políticas de bucket restrictivas. Para identificar los buckets que son el caso, puede revisar su inventario de bucket utilizando la tabla de buckets de S3. Si el icono de advertencia (⚠) aparece junto al nombre de un bucket, significa que Macie no puede acceder al bucket.

Detección automatizada y Problemas de cobertura

Si la detección automatizada de datos confidenciales está habilitada en su cuenta, estas secciones aparecen en el panel de control. Las estadísticas de estas secciones recopilan el

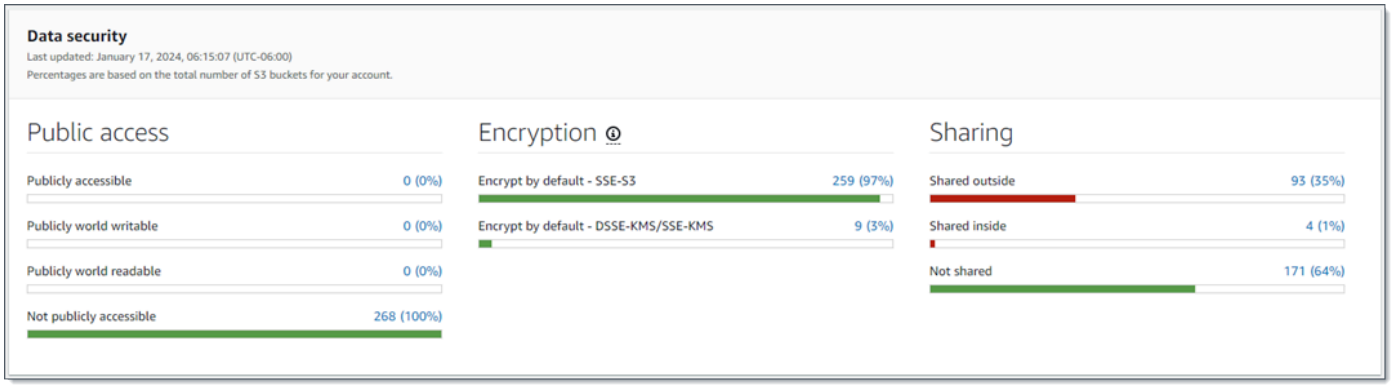
estado y los resultados de las actividades de detección automatizada de datos confidenciales que Macie haya realizado hasta el momento para sus datos de Amazon S3. Por ejemplo:



Para obtener detalles sobre estas estadísticas, consulte Revisión de estadísticas agregadas de confidencialidad de los datos en el panel de resumen.

Seguridad de los datos

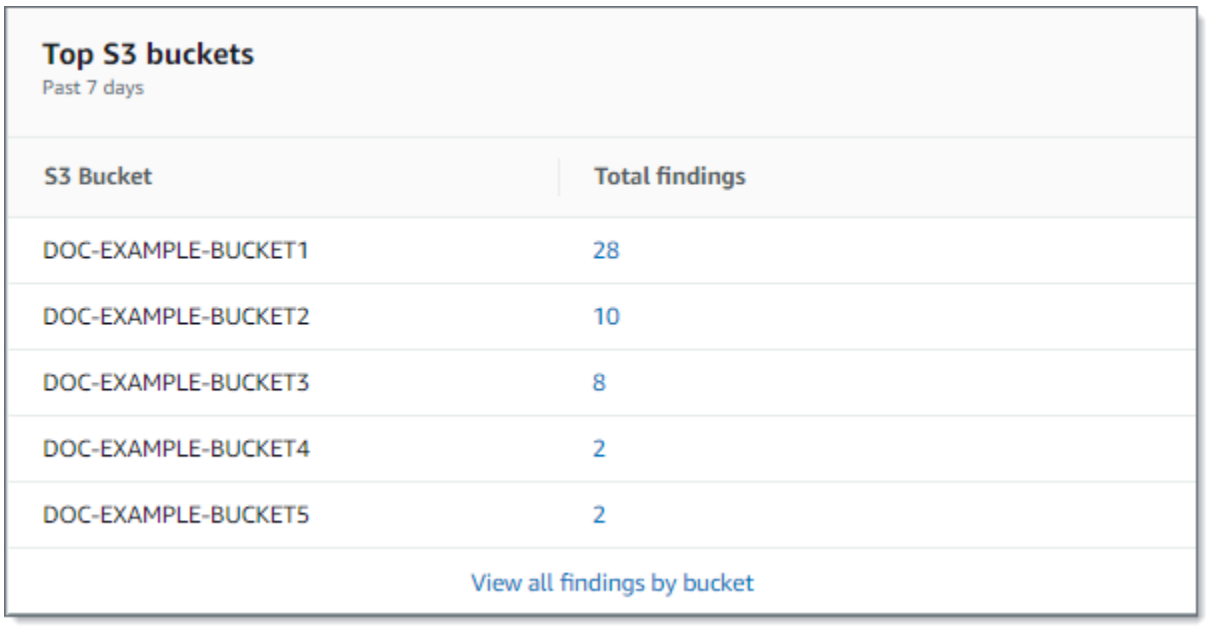
En esta sección se proporcionan estadísticas que indican los posibles riesgos de seguridad y privacidad para sus datos de Amazon S3. Por ejemplo:



Para obtener detalles sobre estas estadísticas, consulte Descripción de las estadísticas de seguridad de los datos en el panel Resumen.

Principales buckets de S3

En esta sección se enumeran los buckets de S3 que generaron la mayor cantidad de resultados de cualquier tipo durante los siete días previos, hasta un total de cinco buckets. También indica el número de resultados que Macie generó para cada bucket. Por ejemplo:

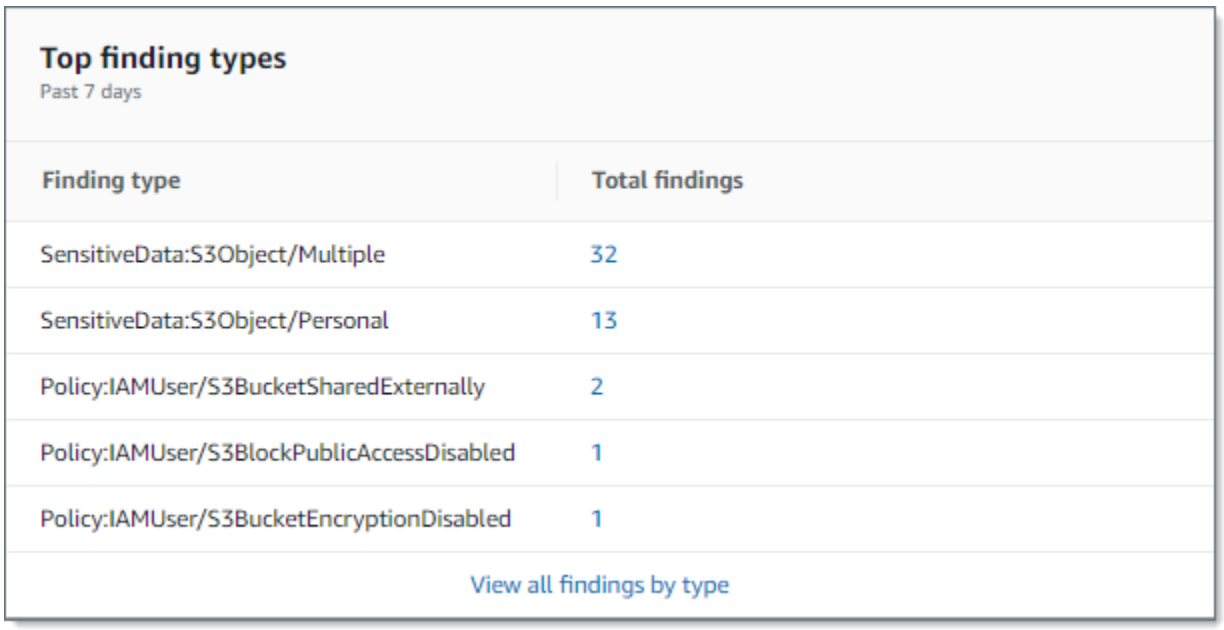


Para mostrar y, si lo desea, profundizar en todos los resultados para un bucket del período de los siete días previos, seleccione el valor en el campo Resultados totales. Para mostrar todos los resultados actuales de todos sus buckets, agrupados por bucket, seleccione Ver todos los resultados por bucket.

Esta sección está vacía si Macie no generó ningún resultado durante los siete días previos. O bien, todos los resultados que se generaron durante los siete días previos se suprimieron mediante una regla de supresión.

Tipos de resultados principales

En esta sección se enumeran los tipos de resultados que tuvieron el mayor número de casos durante los siete días previos, hasta un total de cinco tipos de resultados. También indica el número de resultados que Macie generó para cada tipo. Por ejemplo:



Para mostrar y, si lo desea, profundizar en todos los resultados de un tipo concreto de los siete días previos, seleccione el valor en el campo Resultados totales. Para mostrar todos los resultados actuales, agrupados por tipo de resultado, seleccione Ver todos los resultados por tipo.

Esta sección está vacía si Macie no generó ningún resultado durante los siete días previos. O bien, todos los resultados que se generaron durante los siete días previos se suprimieron mediante una regla de supresión.

Resultados de política

En esta sección se enumeran los resultados de política que Macie generó o actualizó más recientemente, hasta un máximo de diez resultados. Por ejemplo:

Para mostrar los detalles de un resultado en particular, selecciónelo.

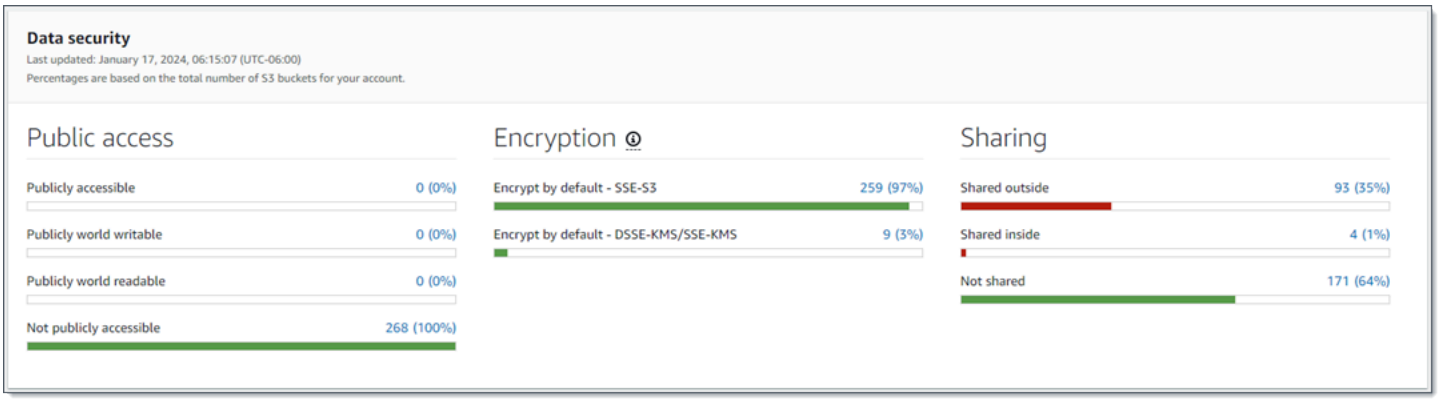
Esta sección estará vacía si Macie no generó ni actualizó ningún resultado de política durante los siete días previos. O bien, todos los resultados de política que se generaron o actualizaron durante los siete días previos se suprimieron mediante una regla de supresión.

Descripción de las estadísticas de seguridad de los datos en el panel Resumen

La sección Seguridad de los datos del panel Resumen ofrece estadísticas que pueden ayudarlo a identificar e investigar posibles riesgos de seguridad y privacidad de sus datos de Amazon S3 en la Región de AWS actual. Por ejemplo, puedes usar estos datos para identificar los depósitos de uso general a los que se puede acceder públicamente o que se comparten con otras personas. Cuentas de AWS

Si su cuenta de Macie es miembro de una organización, las estadísticas de almacenamiento y detección de datos confidenciales que aparecen en la parte superior de esta sección indican cuántos datos almacena en Amazon S3 y cuántos de esos datos puede analizar Macie para detectar datos confidenciales.

Para cualquier tipo de cuenta Macie, las estadísticas adicionales se organizan en tres áreas, tal y como se muestra en la siguiente imagen.



Al revisar cada área, si lo desea, elija un elemento para desglosar y revisar los datos de respaldo. Tenga en cuenta también que las estadísticas no incluyen los datos de los depósitos de directorio de S3, solo los de uso general. Macie no monitorea ni analiza los depósitos de directorios.

Las estadísticas individuales de cada sección son las siguientes.

Public access (Acceso público)

Estas estadísticas indican cuántos buckets de S3 son o no de acceso público:

- De acceso público: el número y porcentaje de buckets que permiten al público general tener acceso de lectura o escritura al bucket.
- De acceso público de escritura: el número y porcentaje de buckets que permiten al público general tener acceso de escritura al bucket.
- De acceso público de lectura: el número y porcentaje de buckets que permiten al público general tener acceso de lectura al bucket.
- De acceso no público: el número y porcentaje de buckets que no permiten al público general tener acceso de lectura o escritura al bucket.

Para calcular cada porcentaje, Macie divide el número de buckets que correspondan entre el número total de buckets de su inventario de buckets.

Para determinar los valores de esta sección, Macie analiza una combinación de configuraciones de niveles de cuentas y de buckets para cada bucket: la configuración de bloqueo de acceso público de la cuenta, la configuración de bloqueo de acceso público del bucket, la política de buckets para ese bucket y la lista de control de acceso (ACL) del bucket. Para obtener información sobre esta configuración, consulte Administración de identidades y accesos en Amazon S3 y Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

En algunos casos, la sección Acceso público también muestra valores correspondientes a Desconocido. Si aparecen esos valores, es que Macie no ha podido evaluar la configuración de acceso público en el número y porcentaje de buckets especificados. Por ejemplo, un problema temporal o la configuración de permisos de los buckets impidieron que Macie recuperara los datos necesarios. O Macie no pudo determinar completamente si una o más instrucciones de política permitían que una entidad externa accediera a los buckets.

Cifrado

Estas estadísticas indican cuántos buckets de S3 están configurados para aplicar determinados tipos de cifrado del lado del servidor a los objetos que se añaden a los buckets:

- Cifrado de forma predeterminada (SSE-S3): número y porcentaje de buckets con configuración de cifrado predeterminada para cifrar objetos nuevos con una clave administrada por Amazon S3. Para estos buckets, los objetos nuevos se cifran automáticamente mediante cifrado SSE-S3.
- Cifrar de forma predeterminada (DSSE-KMS/SSE-KMS): número y porcentaje de depósitos cuya configuración de cifrado predeterminada está configurada para cifrar nuevos objetos con

una clave, ya sea una o una gestionada por el cliente. AWS KMS key Clave administrada de AWS En estos depósitos, los objetos nuevos se cifran automáticamente mediante el cifrado DSSE-KMS o SSE-KMS.

Para calcular cada porcentaje, Macie divide el número de buckets que correspondan entre el número total de buckets de su inventario de buckets.

Para determinar los valores de esta sección, Macie analiza la configuración de cifrado predeterminada de cada bucket. A partir del 5 de enero de 2023, Amazon S3 aplica el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) como el nivel básico de cifrado para cada objeto añadido a un bucket. Si lo desea, puede configurar los ajustes de cifrado predeterminados de un bucket para utilizar el cifrado del lado del servidor con una AWS KMS clave (SSE-KMS) o el cifrado de doble capa del lado del servidor con una clave (DSSE-KMS). AWS KMS Para obtener información sobre las opciones y la configuración de cifrado, consulte Establecer el comportamiento del cifrado predeterminado del servidor para los bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

En algunos casos, la sección Cifrado también muestra valores correspondientes a Desconocido. Si aparecen esos valores, es que Macie no ha podido evaluar la configuración de cifrado en el número y porcentaje de buckets especificados. Por ejemplo, un problema temporal o la configuración de permisos de los buckets impidieron que Macie recuperara los datos necesarios.

Uso compartido

Estas estadísticas indican cuántos buckets de S3 se comparten o no con otras Cuentas de AWS identidades de acceso de CloudFront origen (OAI) o controles de acceso de CloudFront origen (OAC) de Amazon:

- Compartidos de forma externa: la cantidad y el porcentaje de depósitos que se comparten con una o más de las siguientes entidades o con cualquier combinación de las siguientes: una CloudFront OAI, una CloudFront OAC o una cuenta que no pertenece a la misma organización.
- Compartido internamente: número y porcentaje de buckets que se comparten con una o más cuentas de la misma organización. Estos depósitos no se comparten con las OAI ni con CloudFront las OAC.
- No compartidos: la cantidad y el porcentaje de grupos que no se comparten con otras cuentas, CloudFront OAI u OAC. CloudFront

Para calcular cada porcentaje, Macie divide el número de buckets que correspondan entre el número total de buckets de su inventario de buckets.

Para determinar si los buckets se comparten con otros Cuentas de AWS, Macie analiza la política de bucket y la ACL de cada bucket. Además, una organización se define como un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante una invitación de Macie AWS Organizations o por invitación de Macie. Para obtener información sobre las opciones de Amazon S3 para compartir buckets, consulte Administración de identidades y accesos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> En algunos casos, es posible que Macie notifique erróneamente que un bucket está compartido con alguna Cuenta de AWS que no pertenece a la misma organización. Esto puede ocurrir si Macie no puede evaluar completamente la relación entre el elemento `Principal` de la política del bucket y determinadas claves de contexto de condiciones AWS globales o claves de condición de Amazon S3 del elemento `Condition` de la política. Las claves de condición aplicables son:`aws:PrincipalAccount`,`aws:PrincipalArn`,`aws:PrincipalOrgID`,`aws:PrincipalOr` `aws:SourceVpce` `aws:userids3:DataAccessPointAccount`, y. `s3:DataAccessPointArn`
>
> Para determinar si este es el caso de buckets individuales, seleccione la estadística Compartido externamente en el panel de control. En la tabla que aparece, anote el nombre de cada bucket. A continuación, utilice Amazon S3 para revisar la política de cada bucket y determinar si la configuración de acceso compartido es adecuada y segura.

Para determinar si los cubos se comparten con las CloudFront OAI o los OAC, Macie analiza la política de los depósitos de cada grupo. Una CloudFront OAI o una OAC permiten a los usuarios acceder a los objetos de un depósito a través de una o más distribuciones específicas. CloudFront Para obtener información sobre las CloudFront OAI y las OAC, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.

En algunos casos, la sección Compartido también muestra valores correspondientes a Desconocido. Si aparecen estos valores, Macie no ha podido determinar si el número y el porcentaje de cubos especificados se comparten con otras cuentas, CloudFront OAI u OAC. CloudFront Por ejemplo, un problema temporal o la configuración de permisos de los buckets impidieron que Macie recuperara los datos necesarios. O Macie no pudo evaluar completamente las políticas de los buckets o las ACL.

Análisis de la posición de seguridad de Amazon S3 con Amazon Macie

Para ayudarle a realizar un análisis exhaustivo y evaluar el nivel de seguridad de sus datos del Amazon Simple Storage Service (Amazon S3), Amazon Macie mantiene un inventario completo de los depósitos de uso general de S3 en cada uno de los sitios en Región de AWS los que utilice Macie. Para saber cómo Macie mantiene este inventario por usted, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3. Si es el administrador de Macie de una organización, el inventario incluye los datos de los buckets de S3 que sean propiedad de sus cuentas de miembros.

Mediante este inventario, puede revisar el estado de sus datos de Amazon S3 y examinar los detalles y las estadísticas de la configuración de seguridad clave y las métricas que se aplican a los buckets de S3 individuales. Por ejemplo, puede acceder a desgloses de la configuración de acceso público y cifrado de cada bucket, así como al tamaño y número de objetos que Macie puede analizar para detectar datos confidenciales en cada bucket. También puede determinar si configuró algún trabajo de detección de datos confidenciales para analizar objetos en un bucket y, en caso afirmativo, cuándo se ejecutó una de esas tareas más recientemente. Si la detección automática de datos confidenciales está activada para su cuenta, también puede utilizar el inventario para revisar los resultados de las actividades de detección automática de datos confidenciales que Macie ha realizado hasta el momento para su cuenta u organización. Para obtener más información, consulte Detección de datos confidenciales.

Puede examinar y filtrar los datos de inventario utilizando la página de buckets de S3 en la consola de Amazon Macie. También puede acceder a los datos de su inventario mediante programación mediante el DescribeBucketsfuncionamiento de la API Amazon Macie.

Temas

- Revisar el inventario de bucket de S3 con Amazon Macie
- Filtrar el inventario del bucket de S3 con Amazon Macie

Revisar el inventario de bucket de S3 con Amazon Macie

En la consola de Amazon Macie, la página de bucket de S3 proporciona información detallada sobre la seguridad y la privacidad de los datos del Amazon Simple Storage Service (Amazon S3) en el Región de AWS actual. En esta página, puede revisar y analizar un inventario completo de sus cubos de uso general de S3 en la región y revisar información y estadísticas detalladas de los

cubos individuales. Si es el administrador de Macie de una organización, su inventario incluye datos estadísticos y detalles sobre los buckets de S3 que son propiedad de su cuenta y de las cuentas de los miembros de su organización.

La página de bucket de S3 también indica cuándo Macie recuperó por última vez los metadatos de bucket u objetos de Amazon S3 para su cuenta. Puede encontrar esta información en el campo Última actualización de la parte superior de la página. Si es el administrador de Macie de una organización, este campo indica la fecha y hora más antiguas en que Macie recuperó los datos de una cuenta de su organización. Para obtener más información, consulte Actualizaciones de datos.

Tenga en cuenta que los datos y las estadísticas del inventario no incluyen datos sobre los depósitos de directorio de S3, solo los depósitos de uso general. Macie no supervisa ni analiza los depósitos de directorios. Además, la mayoría de los datos de inventario se limitan a los grupos a los que Macie puede acceder desde tu cuenta. Si la configuración de permisos de un bucket impide que Macie recupere la información del bucket o de sus objetos, Macie solo podrá proporcionar un subconjunto de información sobre el bucket. Si este es el caso de un bucket en concreto, Macie mostrará un icono de advertencia (⚠) y un mensaje para el bucket de su inventario. Para los detalles del bucket, Macie muestra solo un subconjunto de campos y datos: el ID de cuenta del Cuenta de AWS propietario del bucket; el nombre del bucket, el Nombre de recurso de Amazon (ARN), la fecha de creación y la región; y el momento en que Macie recuperó por última vez los metadatos del bucket y del objeto del bucket como parte del ciclo de actualización diario. Para investigar el problema, revise la política y la configuración de permisos del bucket en Amazon S3. Por ejemplo, el bucket puede tener una política de bucket restrictiva. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Si prefiere acceder a los datos de inventario y consultarlos mediante programación, puede utilizar el DescribeBucketsfuncionamiento de la API Amazon Macie.

Temas

- Revisar el inventario de bucket de S3
- Revisión de los detalles de los bucket de S3

Revisar el inventario de bucket de S3

La página de buckets S3 de la consola de Amazon Macie proporciona información sobre los buckets S3 de uso general en la actualidad. Región de AWS En esta página, hay una tabla que muestra

información resumida de cada bucket de su inventario. Para personalizar la vista, puede ordenar y filtrar la tabla. Si elige un bucket de la tabla, el panel de detalles muestra información adicional sobre el bucket. Esto incluye detalles y datos estadísticos para la configuración, y las métricas que proporcionan información sobre la seguridad y la privacidad de los datos del bucket. Si lo desea, puede exportar los datos de la tabla a un archivo de valores separados por comas (CSV).

Si su cuenta tiene habilitada la detección automática de datos confidenciales, también tiene la opción de revisar el inventario mediante un mapa térmico interactivo. El mapa proporciona una representación visual e interactiva de la sensibilidad de los datos en todo su patrimonio de datos de Amazon S3. La información adicional recoge los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado para su cuenta u organización. Para obtener información sobre este mapa, consulte Visualización de la confidencialidad de los datos con el mapa de buckets de S3.

Para revisar el inventario de bucket de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3. La página Buckets de S3 muestra su inventario de buckets.

   Si la página muestra un mapa interactivo de su inventario de bucket, seleccione la opción de tabla
   ()
   en la parte superior de la página. Entonces, Macie muestra el número de buckets de su inventario y una tabla con los buckets.
3. En la parte superior de la página, si lo desea, seleccione Actualizar
   ()
   para recuperar los metadatos del bucket más recientes de Amazon S3.

   Si el icono de información
   ()
   aparece junto al nombre de algún bucket, le recomendamos que lo haga. Este icono indica que se creó un bucket durante las últimas 24 horas, posiblemente después de que Macie recuperara por última vez los metadatos del bucket y del objeto de Amazon S3 como parte del ciclo de actualización diario.
4. En la página de bucket de S3, utilice la tabla para revisar un subconjunto de información sobre cada depósito de su inventario:

- Confidencialidad: la puntuación de confidencialidad actual del bucket. Esta columna solo aparece si la detección automatizada de datos confidenciales está habilitada en su cuenta. Para obtener información sobre el rango de puntuaciones de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.
- Bucket: el nombre del bucket.
- Cuenta: El ID de la cuenta para la Cuenta de AWS propietaria del bucket.
- Objetos clasificables: el número total de objetos que Macie puede analizar para detectar datos confidenciales en el bucket.
- Tamaño clasificable: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar para detectar datos confidenciales en el bucket.

  Tenga en cuenta que este valor no refleja el tamaño real de los objetos comprimidos después de descomprimirlos. Además, si el control de versiones está activado para el bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto del bucket.
- Supervisado por el trabajo: si los trabajos de detección de datos confidenciales están configurados para analizar periódicamente los objetos del bucket de forma diaria, semanal o mensual.

  Si el valor de este campo es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.
- Último trabajo ejecutado: si se ha configurado algún trabajo de descubrimiento de datos confidenciales puntual o periódico para analizar los objetos del depósito, este campo indica la fecha y la hora más recientes en las que se empezó a ejecutar uno de esos trabajos. De lo contrario, este campo está vacío.

Los objetos son clasificables si utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Puede detectar datos confidenciales en los objetos mediante Macie. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

5. Para analizar su inventario mediante la tabla, realice alguna de las siguientes acciones:

   - Para ordenar la tabla por un campo específico, elija el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a elegir el encabezado de la columna.

- Para filtrar la tabla y mostrar solo los buckets que tienen un valor específico para un campo, coloque el cursor en el cuadro de filtro y, a continuación, añada una condición de filtro para el campo. Para refinar aún más los resultados, añada condiciones de filtro para campos adicionales. Para obtener más información, consulte Filtrar el inventario de su bucket de S3.

6. Para consultar detalles y estadísticas de un bucket en particular, elija el nombre del bucket en la tabla y consulte el panel de detalles.

> **Tip**
>
> Puede desplazarse y profundizar en muchos de los campos en el panel de detalles del bucket. Para mostrar los buckets que tienen el mismo valor para un campo, elija  en el campo. Para mostrar los buckets que tienen otros valores para un campo, elija  en el campo.

7. Para exportar los datos de la tabla a un archivo CSV, active la casilla de verificación de cada fila que desee exportar o active la casilla del encabezado de la columna de selección para seleccionar todas las filas. A continuación, elija Exportar a CSV en la parte superior de la página. Puede exportar hasta 50 000 filas de la tabla.

Revisión de los detalles de los bucket de S3

En la consola de Amazon Macie, puede usar el panel de detalles de la página de cubos de S3 para revisar las estadísticas y otra información sobre cada uno de los cubos de uso general de su inventario de cubos de S3. Esto incluye detalles y datos estadísticos para la configuración, y las métricas que proporcionan información sobre la seguridad y la privacidad de los datos de un bucket.

Por ejemplo, puede revisar los desgloses de la configuración de acceso público del bucket de S3 y determinar si el bucket está configurado para replicar objetos o se comparte con otros Cuentas de AWS. También puede determinar si hay algún trabajo de detección de datos confidenciales que está configurado para inspeccionar el bucket en busca de datos confidenciales. Si los hay, puede acceder a los detalles del trabajo que se ejecutó más recientemente y, si lo desea, mostrar los resultados que arroje el trabajo.

Si su cuenta tiene habilitada la detección automática de datos confidenciales, también puede usar el panel de detalles para revisar las estadísticas de la detección de datos confidenciales y otra

información sobre los distintos bucket de S3. El panel recoge los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para el bucket. Para obtener más información sobre estos detalles, consulte Revisión de los detalles de confidencialidad de los datos de los buckets S3 individuales.

Para revisar los detalles de un bucket de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3. La página Buckets de S3 muestra su inventario de buckets.
3. En la parte superior de la página, si lo desea, seleccione Actualizar () para recuperar los metadatos del bucket más recientes de Amazon S3.
4. En la tabla o el mapa Buckets de S3, elija el nombre del bucket cuyos detalles desee consultar. El panel de detalles muestra estadísticas y otra información sobre el bucket.

En el panel de detalles, las estadísticas y la información del bucket se organizan en las siguientes secciones principales:

Información general | Estadísticas del objeto | Cifrado del servidor | Detección de datos confidenciales | Acceso público | Replicación | Etiquetas

Al revisar la información de cada sección, puede desplazarse y desglosar en ciertos campos. Para mostrar los buckets que tienen el mismo valor para un campo, elija  en el campo. Para mostrar los buckets que tienen otros valores para un campo, elija  en el campo.

Información general

En esta sección se proporciona información general sobre el depósito, como el nombre del depósito, cuándo se creó y el identificador de cuenta del propietario del Cuenta de AWS depósito. Cabe destacar que el campo Última actualización indica cuándo Macie recuperó por última vez los metadatos del bucket o de los objetos del bucket de Amazon S3.

El campo Acceso compartido indica si el depósito se comparte con otro Cuenta de AWS, con una identidad de acceso de CloudFront origen (OAI) de Amazon o con un control de acceso de CloudFront origen (OAC):

- Externo: el depósito se comparte con una o más de las siguientes opciones o con una combinación de las siguientes: una CloudFront OAI, una CloudFront OAC o una cuenta externa a tu organización (que no forma parte de ella).
- Interno: el bucket se comparte con una o más cuentas que son internas (forman parte) de su organización. No se comparte con una CloudFront OAI ni con una OAC.
- No compartido: el depósito no se comparte con otra cuenta, una CloudFront OAI o una OAC. CloudFront
- Desconocido: Macie no ha podido evaluar la configuración de acceso compartido del bucket.

Para determinar si un bucket se comparte con otro Cuenta de AWS, Macie analiza la política del bucket y la lista de control de acceso (ACL) del bucket. El análisis se limita a la configuración del bucket. No refleja ninguna configuración de objeto para compartir objetos específicos en el bucket. Además, una organización se define como un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante AWS Organizations una invitación de Macie. Para obtener información sobre las opciones de Amazon S3 para compartir buckets, consulte Administración de identidades y accesos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> En algunos casos, Macie podría indicar incorrectamente que un bucket está compartido con una Cuenta de AWS externa a su organización (que no forma parte de ella). Esto puede ocurrir si Macie no puede evaluar completamente la relación entre el elemento `Principal` de la política del bucket y determinadas claves de contexto de condiciones AWS globales o claves de condición de Amazon S3 del elemento `Condition` de la política. Las claves de condición aplicables son:`aws:PrincipalAccount`,`aws:PrincipalArn`,`aws:PrincipalOrgID`,`aws:PrincipalOrgPa` `aws:SourceVpce` `aws:userids3:DataAccessPointAccount`, y. `s3:DataAccessPointArn` Le recomendamos que revise la política del bucket para determinar si este acceso está previsto y es seguro.

Para determinar si un depósito se comparte con una CloudFront OAI o una OAC, Macie analiza la política del depósito. Una CloudFront OAI o una OAC permiten a los usuarios acceder a los objetos de un depósito a través de una o más distribuciones específicas. CloudFront Para obtener más información sobre las CloudFront OAI y las OAC, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.

La sección Información general del panel también incluye el campo Última ejecución de detección automática. Si la detección automática de datos confidenciales está habilitada en su cuenta, este campo indica cuándo Macie analizó por última vez los objetos del bucket mientras realizaba la detección automática para su cuenta. Si la detección automática de datos confidenciales está deshabilitada en su cuenta, aparecerá un guion (—) en este campo.

Estadísticas de objetos

En esta sección se proporciona información sobre los objetos del bucket, empezando por el número total de objetos del bucket (recuento total), el tamaño total de almacenamiento de todos esos objetos (tamaño total de almacenamiento) y el tamaño total de almacenamiento de todos los objetos que son archivos comprimidos (.gz, .gzip o .zip) (tamaño total comprimido). Las estadísticas adicionales de esta sección pueden ayudarle a evaluar la cantidad de datos que Macie puede analizar para detectar datos confidenciales en el bucket.

Si ha creado el bucket recientemente o ha realizado cambios significativos en los objetos del bucket durante las últimas 24 horas, si lo desea, elija actualizar () para recuperar los metadatos más recientes de los objetos del bucket. Macie muestra el icono de información () para ayudarle a determinar si este es el caso. La opción de actualización está disponible si un depósito almacena 30 000 objetos o menos.

Al revisar las estadísticas de esta sección, tenga en cuenta lo siguiente:

- Si el control de versiones está habilitado para el bucket, los valores del tamaño se basan en el tamaño de almacenamiento de la última versión de cada objeto del bucket.
- Si el depósito almacena objetos comprimidos, los valores de tamaño no reflejan el tamaño real de esos objetos una vez descomprimidos.
- Si actualiza los metadatos de los objetos de un bucket, Macie mostrará temporalmente el informe Desconocido para obtener estadísticas de cifrado aplicables a los objetos. Macie volverá a evaluar

y actualizar los datos de estas estadísticas cuando realice la próxima actualización diaria de los metadatos del bucket y del objeto, es decir, en un plazo de 24 horas.

- De forma predeterminada, los recuentos de objetos y los valores de tamaño incluyen los datos de cualquier parte del objeto que contenga el bucket como resultado de cargas incompletas de varias partes. Si actualizas los metadatos del objeto de un bucket, Macie excluye datos de las partes del objeto de los valores recalculados. Cuando Macie realiza la siguiente actualización diaria de los metadatos del bucket y del objeto (en un plazo de 24 horas), recalcula y actualiza los valores de estas estadísticas y vuelve a incluir los datos de las partes del objeto en los valores.

  Tenga en cuenta que Macie no puede analizar partes de objetos para detectar datos confidenciales. Amazon S3 primero debe terminar de ensamblar las partes en uno o más objetos para que Macie los analice. Para obtener información sobre las cargas multiparte y las partes de objetos, incluido cómo eliminar partes automáticamente según las reglas del ciclo de vida, consulte Carga y copia de objetos mediante la carga multiparte en la Guía del usuario de Amazon Simple Storage Service. Para identificar los buckets que contienen partes de objetos, puede consultar las métricas de carga multiparte incompleta en Lente de almacenamiento de Amazon S3. Para obtener más información, consulte Evaluación de la actividad y el uso de almacenamiento en la Guía del usuario de Amazon S3.

Las estadísticas de objetos se organizan de la siguiente manera.

Objetos clasificables

En esta sección se indica el número total de objetos que Macie puede analizar para detectar datos confidenciales y el tamaño total de almacenamiento de esos objetos. Estos objetos utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Puede detectar datos confidenciales en los objetos mediante Macie. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

Objetos no clasificables

En esta sección se indica el número total de objetos que Macie no puede analizar para detectar datos confidenciales y el tamaño total de almacenamiento de esos objetos. Estos objetos no utilizan una clase de almacenamiento de Amazon S3 compatible o no tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido.

Objetos no clasificables: clase de almacenamiento

En esta sección se proporciona un desglose del número y el tamaño de almacenamiento de los objetos que Macie no puede analizar porque no utilizan una clase de almacenamiento compatible con Amazon S3.

Objetos no clasificables: tipo de archivo

En esta sección se proporciona un desglose del número y el tamaño de almacenamiento de los objetos que Macie no puede analizar porque no tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido.

Objetos por tipo de cifrado

En esta sección se proporciona un desglose del número de objetos que utilizan cada tipo de cifrado que admite Amazon S3:

- Proporcionado por el cliente: el número de objetos que están cifrados con una clave proporcionada por el cliente. Estos objetos utilizan el cifrado SSE-C.
- AWS KMS gestionado: el número de objetos que se cifran con una AWS KMS key clave gestionada por el cliente Clave administrada de AWS o una clave gestionada por el cliente. Estos objetos utilizan el cifrado DSSE-KMS o SSE-KMS.
- Amazon S3 gestionado: el número de objetos que se cifran con una clave gestionada por Amazon S3. Estos objetos utilizan el cifrado SSE-S3.
- Sin cifrado: el número de objetos que no están cifrados o que utilizan el cifrado del cliente. (Si un objeto se cifra mediante el cifrado del cliente, Macie no puede acceder a los datos cifrados del objeto ni declararlos).
- Desconocido: el número de objetos para los que Macie no tiene metadatos de cifrado actuales. Esto suele ocurrir si hace poco que ha decidido actualizar manualmente los metadatos de los objetos del bucket. Macie actualizará las estadísticas de cifrado cuando realice la próxima actualización diaria de los metadatos del bucket y del objeto, es decir, en un plazo de 24 horas.

Para obtener información sobre cada tipo de cifrado compatible, consulte Protección de datos con cifrado en la Guía del usuario de Amazon Simple Storage Service.

Cifrado en el servidor

En esta sección se proporciona información sobre la configuración de cifrado del servidor para el bucket.

El campo Cifrado obligatorio por política de bucket indica si la política del bucket requiere el cifrado de los objetos del servidor cuando se añaden objetos al bucket:

- No: el bucket no tiene una política de bucket o la política del bucket no requiere el cifrado del servidor de los objetos nuevos. Si existe una política de bucket, no requiere que PutObjectlas solicitudes incluyan un encabezado de cifrado válido del lado del servidor.
- Sí: la política del bucket exige el cifrado del servidor de los objetos nuevos. Las solicitudes de PutObject del depósito deben incluir un encabezado de cifrado del servidor válido. De lo contrario, Amazon S3 deniega la solicitud.
- Desconocido: Macie no pudo evaluar la política del bucket para determinar si requiere el cifrado del servidor de los objetos nuevos.

Para esta evaluación, los encabezados de cifrado del servidor válidos son: `x-amz-server-side-encryption` con el valor `AES256` o `aws:kms` y `x-amz-server-side-encryption-customer-algorithm` con el valor `AES256`. Para obtener información sobre el uso de políticas de bucket para exigir el cifrado del lado del servidor de los nuevos objetos, consulte Protección de datos con el cifrado del lado del servidor en la Guía del usuario de Amazon Simple Storage Service.

El campo de cifrado predeterminado indica qué algoritmo de cifrado del lado del servidor está configurado para aplicar el depósito de forma predeterminada a los objetos que se añaden al depósito:

- AES256: la configuración de cifrado predeterminada del bucket cifra nuevos objetos con una clave gestionada por Amazon S3. Los objetos nuevos se cifran automáticamente mediante el cifrado SSE-S3.
- aws:kms: la configuración de cifrado predeterminada del depósito está configurada para cifrar nuevos objetos con una clave AWS KMS key, ya sea una Clave administrada de AWS o una gestionada por el cliente. Los objetos nuevos se cifran automáticamente mediante el cifrado SSE-KMS. El AWS KMS keycampo muestra el nombre del recurso de Amazon (ARN) o el identificador único (ID de clave) de la clave que se utiliza.
- aws:kms:dsse: la configuración de cifrado predeterminada del bucket está configurada para cifrar nuevos objetos con una clave AWS KMS key, ya sea una o una gestionada por el cliente. Clave administrada de AWS Los objetos nuevos se cifran automáticamente mediante el cifrado DSSE-KMS. El AWS KMS keycampo muestra el ARN o el ID de clave de la clave que se utiliza.
- Ninguno: la configuración de cifrado predeterminada del bucket no especifica el comportamiento de cifrado del servidor para los objetos nuevos.

A partir del 5 de enero de 2023, Amazon S3 aplica el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) como el nivel básico de cifrado para cada objeto añadido a un bucket. Si lo desea, puede configurar los ajustes de cifrado predeterminados de un depósito para utilizar el cifrado del lado del servidor con una AWS KMS clave (SSE-KMS) o el cifrado de doble capa del lado del servidor con una clave (DSSE-KMS). AWS KMS Para obtener información sobre las opciones y la configuración de cifrado, consulte Establecer el comportamiento del cifrado predeterminado del servidor para los bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Detección de datos confidenciales

Esta sección indica si los trabajos de detección de datos confidenciales están configurados para analizar periódicamente los objetos del bucket de forma diaria, semanal o mensual. Si el valor del campo Supervisado activamente por tarea es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.

Si se ha configurado algún tipo de trabajo de detección de datos confidenciales (ya sea un trabajo periódico o un trabajo único) para inspeccionar el bucket, el campo Último trabajo proporciona el identificador único del que se ha empezado a ejecutar más recientemente. El campo Último trabajo ejecutado indica cuándo comenzó a ejecutarse ese trabajo.

> **Tip**
>
> Para ver todos los datos confidenciales encontrados por el trabajo, seleccione la conexión del campo Último trabajo. En el panel de detalles del trabajo que aparece, seleccione Mostrar resultados en la parte superior del panel y, a continuación, seleccione Mostrar resultados.

Acceso público

En esta sección, se indica si se puede acceder al bucket públicamente. También proporciona un desglose de las distintas configuraciones de la cuenta y del bucket que determinan si este es el caso. El campo Permiso efectivo indica el resultado acumulado de estos ajustes:

- No público: el bucket no está accesible públicamente.
- Público: el bucket está accesible públicamente.

- Desconocido: Macie no ha podido evaluar todas las configuraciones de acceso público del bucket.

Tenga en cuenta que estos datos se limitan a la configuración de la cuenta y del bucket. No refleja la configuración a nivel de objeto que permite el acceso público a objetos específicos de un bucket.

Para obtener más información sobre la configuración de Amazon S3 para administrar el acceso público a los bucket y a los datos de los bucket, consulte Administración de identidad y acceso en Amazon S3 y Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Replicación

En esta sección, el campo Replicado indica si el bucket está configurado para replicar objetos en otros bucket. Si el valor de este campo es Sí, se configuran y habilitan una o más reglas de replicación para el bucket. A continuación, en esta sección también se muestra el ID de cuenta de cada uno de los propietarios de un bucket de destino. Cuenta de AWS

El campo Replicado externamente indica si el depósito está configurado para replicar objetos en depósitos externos a la organización (Cuentas de AWS que no forman parte de ella). Una organización es un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante AWS Organizations una invitación de Macie. Si el valor de este campo es Sí, se configura y activa una regla de replicación para el bucket, y la regla se configura para replicar objetos en un bucket que es propiedad de un usuario externo. Cuenta de AWS

> **Note**
>
> En determinadas condiciones, Macie podría indicar incorrectamente que un depósito está configurado para replicar objetos en un depósito que es propiedad de una persona externa Cuenta de AWS. Esto puede ocurrir si el bucket de destino se creó en una Región de AWS diferente durante las 24 horas anteriores, después de que Macie recuperara los metadatos del bucket y del objeto de Amazon S3 como parte del ciclo de actualización diario.
> Para investigar el problema con Macie, selecciona actualizar
> ()
> para recuperar los metadatos del bucket más recientes de Amazon S3. A continuación, revise la lista de identificadores de la cuenta de esta sección. Para una investigación más profunda, utilice Amazon S3 y revise las reglas de replicación del bucket.

Para obtener información acerca de las opciones y configuraciones de Amazon S3 para replicar objetos de bucket, consulte Replicación de objetos en la Guía del usuario de Amazon Simple Storage Service.

Etiquetas

Si las etiquetas están asociadas al bucket, esta sección aparece en el panel y contiene una lista de dichas etiquetas. Las etiquetas se pueden definir y asignar a determinados tipos de recursos de AWS , incluidos los buckets de S3. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional.

Para obtener información acerca de etiquetar bucket, consulte Uso de etiquetas de buckets de S3 de asignación de costos en la Guía del usuario de Amazon Simple Storage Service.

Filtrar el inventario del bucket de S3 con Amazon Macie

Para identificar los buckets que tienen características específicas y centrarse en ellos, puede filtrar el inventario de buckets de S3 en la consola de Amazon Macie y en las consultas que envíe mediante programación a través de la API de Amazon Macie. Al crear un filtro, utiliza atributos de bucket específicos para definir los criterios para incluir o excluir los buckets de una vista o de los resultados de una consulta. Un atributo de bucket es un campo que almacena metadatos específicos para un bucket.

En Macie, un filtro consta de una o más condiciones. Cada condición, también denominada criterio, consta de tres partes:

- Un campo basado en atributos, como Nombre del bucket, Clave de etiqueta o Definido en el trabajo.
- Un operador, como igual o no igual.
- Uno o varios valores. El tipo y el número de valores dependen del campo y el operador que elija.

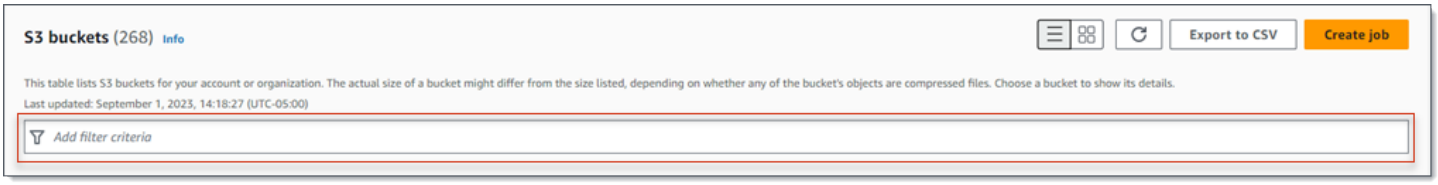
La forma en que defina y aplique las condiciones de filtrado depende de si utiliza la consola de Amazon Macie o la API de Amazon Macie.

Temas

- Filtrar su inventario en la consola de Amazon Macie
- Filtrar el inventario mediante programación con la API Amazon Macie

Filtrar su inventario en la consola de Amazon Macie

Si utiliza la consola de Amazon Macie para filtrar el inventario de buckets de S3, Macie ofrece opciones que le ayudan a elegir campos, operadores y valores para condiciones individuales. Para acceder a estas opciones, utilice el cuadro de filtro de la página Buckets de S3, como se muestra en la siguiente imagen.

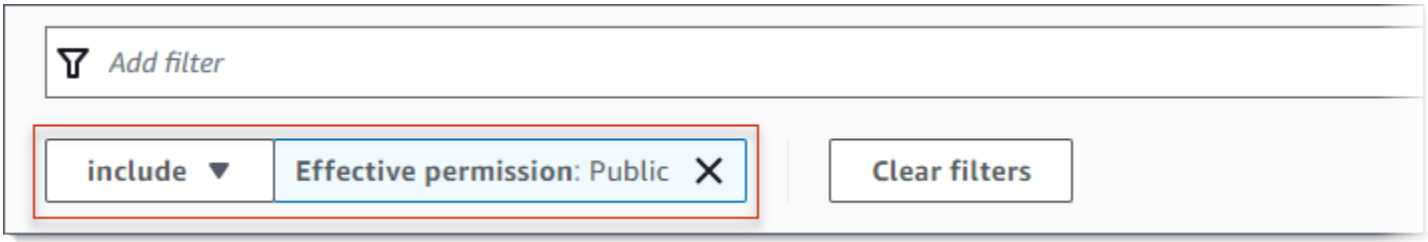


Al colocar el cursor en el cuadro de filtrado, Macie muestra una lista de campos que puede utilizar en las condiciones de filtrado. Los campos están organizados por categorías lógicas. Por ejemplo, la categoría Campos comunes incluye campos que almacenan información general sobre un bucket de S3. Las categorías de Acceso público incluyen campos que almacenan datos sobre los distintos tipos de configuraciones de acceso público que se pueden aplicar a un bucket. Los campos se ordenan alfabéticamente dentro de cada categoría.

Para añadir una condición, comience por elegir un campo de la lista. Para buscar un campo, navegue por la lista completa o introduzca parte del nombre del campo para reducir la lista de campos.

Dependiendo del campo que elija, Macie muestra diferentes opciones. Las opciones reflejan el tipo y la naturaleza del campo que elija. Por ejemplo, si elige el campo Acceso compartido, Macie mostrará una lista de valores entre los que elegir. Si selecciona el campo Nombre del bucket, Macie mostrará un cuadro de texto en el que podrá introducir el nombre del bucket de S3. Sea cual sea el campo que elija, Macie le guiará por los pasos necesarios para añadir una condición que incluya los ajustes necesarios para el campo.

Tras añadir una condición, Macie aplica los criterios de la condición y la añade a un token de filtro en el cuadro de filtrado, como se muestra en la imagen siguiente.



En este ejemplo, la condición está configurada para incluir todos los buckets a los que se puede acceder públicamente y para excluir todos los demás buckets. Devuelve los buckets en los que el valor del campo de Permiso efectivo es igual a Público.

A medida que añada más condiciones, Macie aplicará sus criterios y los mostrará debajo del cuadro de filtrado. Si añade varias condiciones, Macie utiliza la lógica AND (Y) para unir las condiciones y evaluar los criterios de filtrado. Esto significa que un bucket de S3 coincide con los criterios de filtrado solo si coincide con todas las condiciones en el filtro. Puede consultar el área debajo del cuadro de filtrado en cualquier momento para determinar qué criterios has aplicado.

Para filtrar el inventario mediante la consola

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3. La página Buckets de S3 muestra su inventario de buckets.
3. En la parte superior de la página, si lo desea, seleccione Actualizar () para recuperar los metadatos del bucket más recientes de Amazon S3.
4. Coloque el cursor en el cuadro de filtrado y, a continuación, elija el campo que desee utilizar para la condición.
5. Elija o introduzca el tipo de valor adecuado para el campo, teniendo en cuenta los siguientes consejos.

   Fechas, horas e intervalos de tiempo

   Para fechas y horas, utilice los cuadros Desde y Hasta para definir un intervalo de tiempo inclusivo:

   - Para definir un intervalo de tiempo fijo, utilice los cuadros Desde y Hasta para especificar la primera fecha y hora y la última fecha y hora del intervalo, respectivamente.
   - Para definir un intervalo de tiempo relativo que comience en una fecha y hora determinadas y termine en la hora actual, introduzca la fecha y la hora de inicio en los cuadros Desde y elimine el texto de los cuadros Hasta.
   - Para definir un intervalo de tiempo relativo que comience en una fecha y hora determinadas y termine en la hora actual, introduzca la fecha y la hora de inicio en los cuadros Hasta y elimine el texto de los cuadros Desde.

Tenga en cuenta que los valores de hora utilizan la notación de 24 horas. Si utiliza el selector de fechas para elegir fechas, puede refinar los valores introduciendo el texto directamente en los cuadros Desde y Hasta.

Números y rangos numéricos

Para los valores numéricos, utilice los cuadros Desde y Hasta para introducir números enteros que definan un rango numérico inclusivo:

- Para definir un rango numérico fijo, utilice los cuadros Desde y Hasta para especificar los números más bajos y más altos del rango, respectivamente.
- Para definir un rango numérico fijo que se limite a un valor específico, introduzca el valor en los cuadros Desde y Hasta. Por ejemplo, para incluir solo los depósitos S3 que almacenan exactamente 15 objetos, introduzca **15** los campos Desde y Hasta.
- Para definir un rango numérico relativo que comience en un número determinado, introduzca el número en el cuadro Desde y no introduzca ningún texto en el cuadro Hasta.
- Para definir un rango numérico relativo que termine en un número determinado, introduzca el número en el cuadro Hasta y no introduzca ningún texto en el cuadro Desde.

Valores de texto (cadena)

Para este tipo de valor, introduzca un valor completo y válido para el campo. Los valores distinguen entre mayúsculas y minúsculas.

Tenga en cuenta que no puede utilizar un valor parcial ni caracteres comodín en este tipo de valor. La única excepción es el campo Nombre del bucket. Para ese campo, puede especificar un prefijo en lugar de un nombre completo de bucket. Por ejemplo, para buscar todos los buckets de S3 cuyos nombres comiencen por my-S3, introduzca **`my-S3`** como valor de filtrado para el campo Nombre del bucket. Si introduce cualquier otro valor, como **`My-s3`** o **`my*`**, Macie no devolverá los buckets.

6. Cuando termine de añadir un valor al campo, elija Aplicar. Macie aplicará los criterios de filtrado y mostrará la condición en un token de filtrado debajo del cuadro de filtrado.
7. Repita los pasos 4 al 6 para cada condición adicional que desee agregar.
8. Para eliminar una condición, seleccione la X en el token de filtrado para la condición.
9. Para cambiar una condición, elimine la condición seleccionando la X en el token de filtrado para la condición. A continuación, repita los pasos 4 al 6 para añadir una condición con la configuración correcta.

Filtrar el inventario mediante programación con la API Amazon Macie

Para filtrar su inventario de buckets de S3 mediante programación, especifique los criterios de filtrado en las consultas que envíe mediante la DescribeBucketsoperación de la API Amazon Macie. Esta operación devuelve una matriz de objetos. Cada objeto contiene datos estadísticos y otra información sobre un bucket que coincide con los criterios de filtrado.

Para especificar los criterios de filtrado en una consulta, incluya una asignación de las condiciones del filtrado en la solicitud. Para cada condición debe especificar un campo, un operador y uno o varios valores para el campo. El tipo y el número de valores dependen del campo y el operador que elija. Para obtener información sobre los campos, los operadores y los tipos de valores que puede usar en una condición, consulte Fuentes de datos de Amazon S3 en la Referencia de la API de Amazon Macie.

En los siguientes ejemplos, se muestra cómo especificar los criterios de filtrado en las consultas que se envían mediante AWS Command Line Interface (AWS CLI). También puede hacerlo utilizando una versión actual de otra herramienta de línea de AWS comandos o un AWS SDK, o enviando las solicitudes HTTPS directamente a Macie. Para obtener más información sobre AWS las herramientas y los SDK, consulte Herramientas sobre las que construir. AWS

Ejemplos

- Ejemplo 1: buscar buckets por nombre de bucket
- Ejemplo 2: buscar buckets que sean de acceso público
- Ejemplo 3: busca depósitos que almacenen objetos no cifrados
- Ejemplo 4: buscar buckets que no estén supervisados por un trabajo
- Ejemplo 5: buscar buckets que repliquen datos en cuentas externas
- Ejemplo 6: bucar buckets en función de varios criterios

Los ejemplos utilizan el comando describe-buckets. Si un ejemplo se ejecuta correctamente, Macie devuelve una matriz `buckets`. La matriz contiene un objeto para cada depósito que se encuentra en el bloque actual Región de AWS y que coincide con los criterios del filtro. Para ver un ejemplo de esta salida, amplíe la siguiente sección.

Ejemplo de una matriz **`buckets`**

En este ejemplo, la matriz `buckets` proporciona detalles sobre dos buckets que coinciden con los criterios de filtrado especificados en una consulta.

```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
                "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
                "lastJobRunTime": "2021-04-26T14:55:30.270000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2022-12-10T19:11:25.364000+00:00",
            "lastUpdated": "2022-12-13T07:33:06.337000+00:00",
            "objectCount": 13,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 2,
                "s3Managed": 7,
                "unencrypted": 4,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
```

```
                    "blockPublicAcls": true,
                    "blockPublicPolicy": true,
                    "ignorePublicAcls": true,
                    "restrictPublicBuckets": true
                },
                "bucketPolicy": {
                    "allowsPublicReadAccess": false,
                    "allowsPublicWriteAccess": false
                }
            }
        }
    },
    "region": "us-east-1",
    "replicationDetails": {
        "replicated": false,
        "replicatedExternally": false,
        "replicationAccounts": []
    },
    "sensitivityScore": 78,
    "serverSideEncryption": {
        "kmsMasterKeyId": null,
        "type": "NONE"
    },
    "sharedAccess": "NOT_SHARED",
    "sizeInBytes": 4549746,
    "sizeInBytesCompressed": 0,
    "tags": [
        {
            "key": "Division",
            "value": "HR"
        },
        {
            "key": "Team",
            "value": "Recruiting"
        }
    ],
    "unclassifiableObjectCount": {
        "fileType": 0,
        "storageClass": 0,
        "total": 0
    },
    "unclassifiableObjectSizeInBytes": {
        "fileType": 0,
        "storageClass": 0,
```

```
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "FALSE",
                "lastJobId": "188d4f6044d621771ef7d65f2example",
                "lastJobRunTime": "2021-04-09T19:37:11.511000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2022-12-12T19:11:25.364000+00:00",
            "lastUpdated": "2022-12-13T07:33:06.337000+00:00",
            "objectCount": 8,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 0,
                "s3Managed": 8,
                "unencrypted": 0,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
```

```
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
        "region": "us-east-1",
        "replicationDetails": {
            "replicated": false,
            "replicatedExternally": false,
            "replicationAccounts": []
        },
        "sensitivityScore": 95,
        "serverSideEncryption": {
            "kmsMasterKeyId": null,
            "type": "AES256"
        },
        "sharedAccess": "EXTERNAL",
        "sizeInBytes": 175978,
        "sizeInBytesCompressed": 0,
        "tags": [
            {
                "key": "Division",
                "value": "HR"
            },
            {
                "key": "Team",
                "value": "Recruiting"
            }
        ],
        "unclassifiableObjectCount": {
            "fileType": 3,
            "storageClass": 0,
            "total": 3
        },
        "unclassifiableObjectSizeInBytes": {
            "fileType": 2999826,
```

```
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```

Si ningún bucket coincide con los criterios de filtrado, Macie devuelve una matriz `buckets` vacía.

```
{
    "buckets": []
}
```

Ejemplo 1: buscar buckets por nombre de bucket

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de todos los depósitos cuyos nombres comiencen por my-S3 y estén en el valor actual. Región de AWS

Para Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

Donde:

- *bucketName* especifica el nombre JSON del campo Nombre del bucket.
- *prefijo* especifica el operador de prefijo.
- *my-S3* es el valor del campo Nombre del bucket.

Ejemplo 2: buscar buckets que sean de acceso público

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de los depósitos que están en el estado actual Región de AWS y que, en función de una combinación de configuraciones de permisos, son de acceso público.

Para Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":
{\"eq\":[\"PUBLIC\"]}}
```

Donde:

- *publicAccess.effectivePermission* especifica el nombre JSON del campo Permiso efectivo.
- *eq* especifica el operador igual a.
- *PUBLIC* es un valor enumerado para el campo Permiso efectivo.

Ejemplo 3: busca depósitos que almacenen objetos no cifrados

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de los depósitos que se encuentran en la versión actual y que almacenan objetos no cifrados. Región de AWS

Para Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":
{"gte":1}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --
criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

Donde:

- *objectCountByEncryptionType.unencrypted* especifica el nombre JSON del campo Sin cifrado.
- *gte* especifica el operador es mayor o igual a.
- *1* es el valor más bajo de un rango numérico relativo e inclusivo para el campo Sin cifrado.

Ejemplo 4: buscar buckets que no estén supervisados por un trabajo

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de los depósitos que están en el estado actual Región de AWS y que no están asociados a ningún trabajo periódico de descubrimiento de datos confidenciales.

Para Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

Donde:

- *Detalles del trabajo. isMonitoredByJob* especifica el nombre JSON del campo Monitoreado activamente por trabajo.
- *eq* especifica el operador igual a.
- *FALSE* es un valor enumerado para el campo Supervisado activamente por trabajo.

Ejemplo 5: buscar buckets que repliquen datos en cuentas externas

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de los depósitos que están en el estado actual Región de AWS y que están configurados para replicar objetos en otros Cuenta de AWS que no forman parte de la organización.

Para Linux, macOS o Unix:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

Donde:

- *replicationDetails.replicatedExternally* especifica el nombre JSON del campo Replicado externamente.
- *eq* especifica el operador igual a.
- *true* especifica un valor booleano para el campo Replicado externamente.

Ejemplo 6: bucar buckets en función de varios criterios

En este ejemplo, se utiliza el comando describe-buckets para consultar los metadatos de los depósitos que están en el estado actual Región de AWS y que cumplen los siguientes criterios: son de acceso público en función de una combinación de configuraciones de permisos, almacenan objetos no cifrados y no están asociados a ningún trabajo periódico de descubrimiento de datos confidenciales.

Para Linux, macOS o Unix, utilice el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad:

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Para Microsoft Windows, utilice el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad:

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

Donde:

- *publicAccess.effectivePermission* especifica el nombre JSON del campo Permiso en vigor, y:
  - *eq* especifica el operador igual a.
  - *PUBLIC* es un valor enumerado para el campo Permiso efectivo.
- *objectCountByEncryptionType.unencrypted* especifica el nombre JSON del campo Sin cifrado y:

  - *gte* especifica el operador es mayor o igual a.
  - *1* es el valor más bajo de un rango numérico relativo e inclusivo para el campo Sin cifrado.
- *Detalles del trabajo. isMonitoredByJob* especifica el nombre JSON del campo Monitoreado activamente por trabajo y:
  - *eq* especifica el operador igual a.
  - *FALSE* es un valor enumerado para el campo Supervisado activamente por trabajo.

Permitir a Amazon Macie el acceso a buckets y objetos de S3

Cuando habilitas Amazon Macie para ti Cuenta de AWS, Macie crea un rol vinculado a un servicio que otorga a Macie los permisos necesarios para llamar a Amazon Simple Storage Service (Amazon S3) y a otros en tu nombre. Servicios de AWS Un rol vinculado a un servicio simplifica el proceso de configuración de un, Servicio de AWS ya que no es necesario añadir permisos manualmente para que el servicio complete acciones en su nombre. Para obtener más información sobre este tipo de rol, consulte Uso de roles vinculados en la AWS Identity and Access Management Guía del usuario.

La política de permisos del rol vinculado a un servicio de Macie (`AWSServiceRoleForAmazonMacie`) permite a Macie realizar acciones que incluyen la recuperación de información sobre los bucket y objetos de S3 y la recuperación y el análisis de los objetos de los bucket. Si es el administrador de Macie de una organización, la política también permite a Macie llevar a cabo estas acciones en su nombre para las cuentas miembro de su organización.

Macie utiliza estos permisos para realizar tareas como:

- Genere y mantenga un inventario de sus depósitos de uso general de S3
- Ofrecer datos estadísticos y de otro tipo sobre los buckets y los objetos que contienen
- Supervisar y evaluar los buckets para garantizar la seguridad y el control de acceso
- Analizar los objetos de los buckets para detectar datos confidenciales

En la mayoría de los casos, Macie tiene los permisos que necesita para realizar estas tareas. Sin embargo, si un bucket de S3 tiene una política de buckets restrictiva, la política podría impedir que Macie realice algunas o todas estas tareas.

Una política de bucket es una política basada en recursos AWS Identity and Access Management (IAM) que especifica qué acciones puede realizar un principal (usuario, cuenta, servicio u otra

entidad) en un bucket de S3 y las condiciones en las que un principal puede realizar esas acciones. Las acciones y condiciones se pueden aplicar a las operaciones a nivel de bucket, como la recuperación de información sobre un bucket, y a las operaciones a nivel de objeto, como la recuperación de objetos de un bucket.

Las políticas de bucket suelen conceder o restringir el acceso mediante declaraciones y condiciones de `Allow` o `Deny`. Por ejemplo, una política de bucket puede contener una instrucción `Allow` o `Deny` que deniegue el acceso al bucket a menos que se utilicen direcciones IP, puntos de conexión Amazon Virtual Private Cloud (Amazon VPC) o VPC para acceder al bucket. Para obtener más información acerca de la asociación de políticas de buckets de Amazon S3, consulte Uso de políticas de bucket y políticas de usuario y Cómo autoriza Amazon S3 una solicitud en la Guía del usuario de Amazon Simple Storage Service.

Si una política de bucket utiliza una instrucción explícita de `Allow`, la política no impide que Macie recupere información sobre el bucket y sus objetos, ni que recupere objetos del bucket. Esto se debe a que las declaraciones de `Allow` de la política de permisos para el rol vinculado al servicio de Macie otorgan estos permisos.

Sin embargo, si una política de bucket utiliza una instrucción explícita de `Deny` con una o más condiciones, es posible que a Macie no se le permita recuperar información sobre el bucket o los objetos del bucket, ni recuperar los objetos del bucket. Por ejemplo, si una política de bucket deniega explícitamente el acceso desde todas las fuentes excepto desde una dirección IP específica, Macie no podrá analizar los objetos del bucket cuando se ejecute un trabajo de detección de datos confidenciales. Esto se debe a que las políticas de bucket restrictivas tienen prioridad sobre las instrucciones de `Allow` de la política de permisos del rol vinculado a servicios de Macie.

Para permitir que Macie acceda a un bucket de S3 que tenga una política de bucket restrictiva, puede añadir una condición para el rol vinculado al servicio de Macie (`AWSServiceRoleForAmazonMacie`) a la política de bucket. La condición debe impedir que el rol vinculado al servicio de Macie coincida con la restricción `Deny` de la política. Para ello, puede utilizar la `aws:PrincipalArn`clave de contexto de la condición global y el nombre de recurso de Amazon (ARN) del rol vinculado a un servicio de Macie.

Este procedimiento lo guía a través del proceso y pone un ejemplo.

Para añadir la función vinculada al servicio de Macie a una política de buckets

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.

2. En el panel de navegación, elija Buckets.
3. Elija el bucket de S3 al que desea permitir que Macie acceda.
4. En la pestaña Permissions (Permisos), en Bucket policy (Política de bucket), elija Edit (Editar).
5. En el editor de Política del bucket, identifique cada instrucción `Deny` que restrinja el acceso e impida que Macie acceda al bucket o a sus objetos.
6. En cada instrucción de `Deny`, añada una condición que utilice la clave de contexto de la condición global `aws:PrincipalArn` y especifique el ARN de la función vinculada al servicio de Macie para su Cuenta de AWS.

   El valor de la clave de condición debe ser `arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, donde *`123456789012`* es el ID de cuenta de su Cuenta de AWS.

El lugar donde se añada esta instrucción a una política de buckets depende de la estructura, los elementos y las condiciones que la política contenga actualmente. Para obtener más información sobre las estructuras y los elementos compatibles, consulte Políticas y permisos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

El siguiente es un ejemplo de una política de buckets que utiliza una instrucción explícita de `Deny` para restringir el acceso a un bucket de S3 denominado DOC-EXAMPLE-BUCKET. Con la política actual, solo se puede acceder al bucket desde punto de conexión de VPC cuyo ID es `vpce-1a2b3c4d`. Se deniega el acceso desde todos los demás puntos finales de la VPC, incluido el acceso desde Macie y Macie. AWS Management Console

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
```

```
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

Para cambiar esta política y permitir que Macie acceda al bucket de S3 y a los objetos del bucket, podemos añadir una condición que utilice el operador de condición `StringNotLike` y la clave de contexto de la condición global `aws:PrincipalArn`. La condición debe impedir que el rol vinculado al servicio de Macie coincida con la `Deny`restricción.

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
               "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
      }
   ]
}
```

En el ejemplo anterior, el operador de condición `StringNotLike` utiliza la clave de contexto de la condición `aws:PrincipalArn` para especificar el ARN del rol vinculado al servicio de Macie, donde:

- `123456789012`es el identificador de cuenta Cuenta de AWS que permite utilizar Macie para recuperar información sobre el depósito y los objetos del depósito, así como para recuperar objetos del depósito.
- `macie.amazonaws.com` es el identificador de la entidad principal del servicio de Macie.
- El nombre de la función vinculada a servicios para Macie es `AWSServiceRoleForAmazonMacie`

Usamos el operador `StringNotLike` porque la política ya usa un operador `StringNotEquals`. Una política solo puede usar el operador `StringNotEquals` una vez.

Para obtener ejemplos de política adicionales e información detallada sobre cómo administrar el acceso a los recursos Amazon S3, consulte Administración de identidad y acceso en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Detección de datos confidenciales con Amazon Macie

Con Amazon Macie, puede automatizar la detección, el registro y la notificación de información confidencial en su conjunto de datos de Amazon Simple Storage Service (Amazon S3). Puede hacerlo de dos maneras: configurando Macie para que realice el descubrimiento automatizado de datos confidenciales y creando y ejecutando trabajos de descubrimiento de datos confidenciales.

Detección automatizada de datos confidenciales

> La detección de datos confidenciales proporciona una amplia visibilidad de dónde pueden residir los datos confidenciales en su patrimonio de datos de Amazon S3. Con esta opción, Macie evalúa su inventario de buckets de S3 a diario y utiliza técnicas de muestreo para identificar y seleccionar objetos de S3 representativos de sus buckets. A continuación, Macie recupera y analiza los objetos seleccionados, inspeccionándolos en busca de datos confidenciales. Para obtener más información, consulte Realización de la detección automatizada de datos confidenciales.

Trabajos de detección de datos confidenciales

> Los trabajos de detección de datos confidenciales proporcionan un análisis más profundo y específico. Con esta opción, usted define la amplitud y la profundidad del análisis: bucket de S3 específicos que seleccione o buckets que coincidan con criterios específicos. También puede ajustar el ámbito del análisis eligiendo opciones, como los criterios personalizados que se derivan de las propiedades de los objetos de S3. Además, puede configurar un trabajo para que se ejecute solo una vez para el análisis y la evaluación bajo demanda, o de forma periódica para el análisis, la evaluación y la supervisión periódicos. Para obtener más información, consulte Ejecución de trabajos de detección de datos confidenciales.

Con cualquiera de las dos opciones, la detección de datos confidenciales automatizada o los trabajos de detección de datos confidenciales, puede analizar objetos de S3 mediante identificadores de datos administrados que proporciona Macie, identificadores de datos personalizados que usted defina o una combinación de ambos. También puede ajustar el análisis mediante el uso de listas de permitidos.

Identificadores de datos administrados

> Los identificadores de datos administrados son criterios y técnicas integradas diseñados para detectar un tipo específico de datos confidenciales, como números de tarjetas de crédito, claves

de acceso secretas de AWS o números de pasaporte de un país o región en particular. Las técnicas pueden detectar una larga lista de tipos de información confidencial para muchos países y regiones, incluidos datos de credenciales, datos financieros, información de identificación personal (PII). Para obtener más información, consulte Uso de identificadores de datos administrados.

Identificadores de datos personalizados

Un identificador de datos personalizados es un conjunto de criterios personalizados que se definen para detectar información confidencial. Cada identificador de datos personalizados especifíca una expresión regular (regex) que define un patrón de texto para que coincida y, opcionalmente, secuencias de caracteres y una regla de proximidad que perfeccionen los resultados. Puede utilizarlos para detectar datos confidenciales que reflejen escenarios particulares, propiedad intelectual o datos de propietario, por ejemplo, identificaciones de empleados, números de cuentas de clientes o clasificaciones de datos internos. Para obtener más información, consulte Creación de identificadores de datos personalizados.

Listas de permitidos

En Macie, permita que las listas especifiquen el texto y los patrones de texto que deben ignorarse en los objetos de S3, normalmente excepciones a los datos confidenciales en sus escenarios o entornos específicos, por ejemplo, nombres públicos o números de teléfono de su organización, o datos de muestra que su organización utiliza para realizar pruebas. Si Macie encuentra texto que coincide con una entrada o un patrón en una lista de permitidos, Macie no informa la aparición de texto, incluso si el texto coincide con los criterios de un identificador de datos administrados o un identificador de datos personalizado. Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

Cuando Macie analiza un objeto de S3, recupera la última versión del objeto de Amazon S3 y, a continuación, inspecciona el contenido del objeto en busca de datos confidenciales. Macie puede analizar un objeto si se cumple lo siguiente:

- El objeto utiliza un formato de archivo o almacenamiento compatible y se almacena en un depósito de uso general de S3 con una clase de almacenamiento compatible. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.
- Si el objeto está cifrado, asegúrese de que también esté cifrado con una clave que Macie pueda usar. Para obtener más información, consulte Análisis de objetos S3 cifrados.

- Si el objeto está almacenado en un bucket que tiene una política de bucket restrictiva, la política permite a Macie acceder a los objetos del bucket. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Para ayudarle a cumplir y mantener el cumplimiento de sus requisitos de seguridad y privacidad de datos, Macie crea registros de los datos confidenciales que encuentra y de los análisis que realiza: tanto los resultados de datos confidenciales como los resultados de la detección de datos confidenciales. Un resultado de datos confidenciales es un informe detallado de los datos confidenciales que Macie encontró en un objeto de S3. Un resultado de detección de datos confidenciales es un registro de los detalles sobre el análisis de un objeto. Cada tipo de registro sigue un esquema estandarizado, que puede ayudarle a consultarlos, supervisarlos y procesarlos mediante el uso de otras aplicaciones, servicios y sistemas, según sea necesario.

> **Tip**
>
> Aunque Macie está optimizado para Amazon S3, puede usarlo para detectar datos confidenciales en recursos que actualmente almacena en otros lugares. Para ello, puede mover los datos a Amazon S3 de forma temporal o permanente. Por ejemplo, exporte instantáneas Amazon Relational Database Service o Amazon Aurora a Amazon S3 en formato Apache Parquet. O exporte una tabla de Amazon DynamoDB a Amazon S3. A continuación, puede crear un trabajo para analizar los datos en Amazon S3.

Temas

Uso de identificadores de datos administrados en Amazon Macie

Amazon Macie utiliza una combinación de criterios y técnicas, como machine learning y la coincidencia de patrones, para detectar datos confidenciales en objetos de Amazon Simple Storage Service (Amazon S3). Estos criterios y técnicas, que se denominan en su conjunto identificadores de datos administrados, pueden detectar una lista extensa y creciente de tipos de datos confidenciales en muchos países y regiones, incluidos varios tipos de credenciales, datos financieros, información médica personal (PHI) e información de identificación personal (PII). Cada identificador de datos administrado está diseñado para detectar un tipo específico de datos confidenciales, como por ejemplo, AWS clave de acceso secreta, números de tarjetas de crédito, claves de acceso secretas, números de tarjetas de crédito o de pasaporte de un país o región en particular.

Macie puede detectar las siguientes categorías de datos confidenciales mediante identificadores de datos administrados:

- Credenciales, para datos de credenciales como claves privadas y AWS claves de acceso secreto.
- Información financiera, para datos financieros como números de tarjetas de crédito y números de cuentas bancarias.
- Información personal, para la PHI, como los números de seguro médico y de identificación médica, y la PII, como los números de identificación del carné de conducir y los números de pasaporte.

Dentro de cada categoría, Macie puede detectar varios tipos de datos confidenciales. En los temas de esta sección, se enumeran y describen cada tipo y los requisitos pertinentes para detectarlos. Para cada tipo, también se indica el identificador único (ID) del identificador de datos administrados que está diseñado para detectar los datos. Al crear una tarea de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede utilizar estos ID para especificar qué identificadores de datos gestionados desea que Macie utilice cuando analice los objetos de S3.

Para obtener una lista de los identificadores de datos administrados que recomendamos para los trabajos, consulte Identificadores de datos administrados recomendados para trabajos de detección de datos confidenciales. Para ver una lista de los identificadores de datos gestionados que recomendamos y que se utilizan de forma predeterminada para la detección automática de datos confidenciales, consulte Configuración predeterminada para la detección automatizada de datos confidenciales.

Temas

Requisitos de palabras clave para los identificadores de datos gestionados por Amazon Macie

Para detectar ciertos tipos de datos confidenciales mediante identificadores de datos administrados, Amazon Macie requiere que una palabra clave esté cerca de los datos. Si es así para un tipo concreto de datos, en un tema posterior de esta sección se indican los requisitos de palabras clave específicos para esos datos.

Si una palabra clave debe estar cerca de un tipo de datos en particular, normalmente debe estar dentro de los 30 caracteres (ambos incluidos) de los datos. Los requisitos de proximidad adicionales varían en función del tipo de archivo o el formato de almacenamiento de un objeto de Amazon Simple Storage Service (Amazon S3).

Datos estructurados y en columnas

> En el caso de los datos en columnas, una palabra clave debe formar parte del mismo valor o estar en el nombre de la columna o el campo que almacena un valor. Esto es válido para los libros de trabajo de Microsoft Excel, los archivos CSV y los archivos TSV.
>
> Por ejemplo, si el valor de un campo contiene tanto el SSN como un número de nueve dígitos que usa la sintaxis de un número de seguro social (SSN) de EE.UU., Macie puede detectar el SSN en el campo. Del mismo modo, si el nombre de una columna contiene el SSN, Macie puede detectar todos los SSN de la columna. Macie considera que los valores de esa columna están cerca de la palabra clave SSN.

Datos estructurados y basados en registros

> En el caso de los datos basados en registros, una palabra clave debe formar parte del mismo valor o estar en el nombre de un elemento de la ruta al campo o matriz que almacena un valor. Esto es válido para los contenedores de objetos Apache Avro, los archivos Apache Parquet, los archivos JSON y los archivos JSON Lines.
>
> Por ejemplo, si el valor de un campo contiene tanto credenciales como una secuencia de caracteres que utiliza la sintaxis de una clave de acceso secreta de AWS, Macie puede detectar la clave en el campo. Del mismo modo, si la ruta a un campo es `$.credentials.aws.key`,

Macie puede detectar una clave de acceso secreta de AWS en el campo. Macie considera que el valor del campo está cerca de las credenciales de la palabra clave.

Datos no estructurados

No hay requisitos de proximidad adicionales para los archivos de formato de documento portátil de Adobe, los documentos de Microsoft Word, los mensajes de correo electrónico y los archivos de texto no binarios, excepto los archivos CSV, JSON, JSON Lines y TSV. Por lo general, una palabra clave debe estar dentro de los 30 caracteres (ambos incluidos) de los datos. Esto incluye todos los datos estructurados, como las tablas, de estos tipos de archivos.

Las palabras clave no distinguen entre mayúsculas y minúsculas. Además, si una palabra clave contiene un espacio, Macie busca automáticamente las variaciones de palabras clave que no contienen el espacio o que contienen un guion bajo (_) o un guion (-) en lugar del espacio. En ciertos casos, Macie también expande o abrevia una palabra clave para tener en cuenta las variaciones comunes de esa palabra clave.

Para ver una demostración de cómo las palabras clave proporcionan contexto y ayudan a Macie a detectar tipos específicos de datos confidenciales, vea el siguiente vídeo: Cómo Amazon Macie usa palabras clave para detectar datos confidenciales.

Referencia rápida: identificadores de datos administrados por Amazon Macie

En Amazon Macie, un identificador de datos gestionados es un conjunto de criterios y técnicas integrados que están diseñados para detectar un tipo específico de datos confidenciales, por ejemplo, números de tarjetas de crédito, claves de acceso AWS secretas o números de pasaporte de un país o región determinados. Estos identificadores pueden detectar una lista extensa y creciente de tipos de datos confidenciales en muchos países y regiones, incluidos varios tipos de datos de credenciales, información financiera, información médica personal e información de identificación personal (PII).

En la siguiente tabla se enumeran todos los identificadores de datos administrados que Macie proporciona actualmente, organizados por tipo de datos confidenciales. Para cada tipo, se proporciona la siguiente información:

- Categoría de datos confidenciales: especifica la categoría general de datos confidenciales que incluye el tipo: Credenciales, para datos de credenciales, como claves privadas; Información

financiera, para datos financieros, como números de tarjetas de crédito y números de cuentas bancarias; Información personal: PHI para información de salud personal, como números de seguro médico e identificación médica; e información personal: PII para información de identificación personal, como números de identificación del carné de conducir y números de pasaporte

- ID de identificador datos administrados: especifica el identificador único (ID) para uno o más identificadores de datos administrados que están diseñados para detectar los datos. Al crear una tarea de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede utilizar estos ID para especificar qué identificadores de datos gestionados desea que Macie utilice cuando analice los datos. Para obtener una lista de los identificadores de datos administrados que recomendamos para los trabajos, consulte Identificadores de datos administrados recomendados para trabajos de detección de datos confidenciales. Para ver una lista de los identificadores de datos administrados que recomendamos y para la detección automática de datos confidenciales, consulte Configuración predeterminada para la detección automatizada de datos confidenciales.
- Palabra clave obligatoria: especifica si la detección requiere que una palabra clave esté cerca de los datos. Para obtener información sobre cómo Macie utiliza las palabras clave cuando analiza los datos, consulteRequisitos de palabras clave.
- Países y regiones compatibles: especifica para qué países o regiones están diseñados los identificadores de datos administrados compatibles. Si los identificadores de datos administrados no están diseñados para un país o región en particular, este valor es Cualquiera.

Para revisar detalles adicionales sobre los identificadores de datos administrados para un tipo concreto de datos sensibles, elija el tipo.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Clave de acceso secreta de AWS	Credenciales	AWS_CREDENTIALS	Sí	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de cuenta bancaria	Información financiera	BANK_ACCOUNT_NUMBER (para Canadá y EE. UU.),	Sí	Canadá, EE. UU.
Número de cuenta bancaria básico (BBAN)	Información financiera	Según el país o región: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Sí	Alemania, España, Francia, Italia, Reino Unido
Fecha de nacimiento	Información personal: PII	DATE_OF_BIRTH	Sí	Cualquiera
Fecha de caducidad de la tarjeta	Información financiera	CREDIT_CARD_EXPIRATION	Sí	Cualquiera
Datos de banda magnética de tarjetas de crédito	Información financiera	CREDIT_CARD_MAGNETIC_STRIPE	Sí	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de tarjetas de crédito	Información financiera	CREDIT_CARD_NUMBER (para números de tarjetas de crédito próximos a una palabra clave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (para números de tarjetas de crédito que no están cerca de una palabra clave)	Varía	Cualquiera
Código de verificación de tarjeta de crédito	Información financiera	CREDIT_CARD_SECURITY_CODE	Sí	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación del permiso de conducir	Información personal: PII	Según el país o región: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Sí	Australia, Austria, Bélgica, Bulgaria, Canadá, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, India, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía, Eslovaquia, Eslovenia

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, España, Suecia, Reino Unido, Estados Unidos
Número de registro de la Administración para el Control de Drogas (DEA)	Información personal: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sí	EE. UU.
Número de registro electoral	Información personal: PII	UK_ELECTORAL_ROLL_NUMBER	Sí	Reino Unido
Nombre completo	Información personal: PII	NAME	No	Cualquiera, si el nombre utiliza un juego de caracteres latinos

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Coordenadas del sistema de posicionamiento global (GPS)	Información personal: PII	LATITUDE_LONGITUDE	Sí	Cualquiera, si las coordenadas están cerca de una palabra clave en inglés
Clave de API de Google Cloud	Credenciales	GCP_API_KEY	Sí	Cualquiera
Número de reclamación del seguro médico (HICN)	Información personal: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sí	EE. UU.
Número de seguro médico o identificación médica	Información personal: PHI	Según el país o región: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sí	Canadá, UE, Estados Unidos, Finlandia, Francia, Reino Unido

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)	Información personal: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sí	EE. UU.
Encabezado de autorización básica de HTTP	Credenciales	HTTP_BASIC_AUTH_HEADER	No	Cualquiera
Cookie HTTP	Información personal: PII	HTTP_COOKIE	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de cuenta bancaria internacional (IBAN)	Información financiera	Según el país o región: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER,	No	Albania, Andorra, Bosnia-Herzegovina, Brasil, Bulgaria, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, República Dominicana, Egipto, Estonia, Islas Feroe, Finlandia, Francia, Georgia, Alemania, Grecia, Groenlandia, Hungría, Islandia, Irlanda, Italia, Jordania,

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER,		Kosovo, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauricio, Mónaco, Montenegro, Países Bajos, Macedonia del Norte, Polonia, Portugal, San Marino, Senegal, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Timor-Leste, Túnez, Türkiye, Reino Unido, Ucrania,

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (para las Islas Vírgenes Británicas)		Árabe Unido Emiratos, Islas Vírgenes Británicas
Token web JSON (JWT)	Credenciales	JSON_WEB_TOKEN	No	Cualquiera
Dirección postal	Información personal: PII	ADDRESS, BRAZIL_CEP_CODE (para el Código de Endereçamento Postal de Brasil)	Varía	Australia, Brasil, Canadá, Francia, Alemania, Italia, España, Reino Unido, Estados Unidos
Código nacional de medicamento (NDC)	Información personal: PHI	USA_NATIONAL_DRUG_CODE	Sí	EE. UU.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación nacional	Información personal: PII	Según el país o región: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Sí	Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos
Número de seguro nacional (NINO)	Información personal: PII	UK_NATIONAL_INSURANCE_NUMBER	Sí	Reino Unido
Identificador nacional de proveedor (NPI)	Información personal: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sí	EE. UU.
Clave privada de OpenSSH	Credenciales	OPENSSH_PRIVATE_KEY	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de pasaporte	Información personal: PII	Según el país o región: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sí	Alemania, Canadá, España, Estados Unidos, Francia, Italia, Reino Unido
Número de residencia permanente	Información personal: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Sí	Canadá
Clave privada de PGP	Credenciales	PGP_PRIVATE_KEY	No	Cualquiera
Número de teléfono	Información personal: PII	Según el país o región: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Varía	Alemania, Brasil, Canadá, España, Estados Unidos, Francia, Italia, Reino Unido

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Clave privada del estándar de criptografía de clave pública (PKCS)	Credenciales	PKCS	No	Cualquiera
Clave privada PuTTY	Credenciales	PUTTY_PRIVATE_KEY	No	Cualquiera
Número de Seguro Social (SIN)	Información personal: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sí	Canadá
Número de la Seguridad Social (SSN)	Información personal: PII	Según el país o región: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sí	España, Estados Unidos
the section called “Clave de API de Stripe”	Credenciales	STRIPE_CREDENTIALS	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación o referencia del contribuyente	Información personal: PII	Según el país o región: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Sí	Australia, Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos
Identificador de dispositivo único (UDI)	Información personal: PHI	MEDICAL_DEVICE_UDI	Sí	EE. UU.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación de vehículo (VIN)	Información personal: PII	VEHICLE_IDENTIFICATION_NUMBER	Sí	Cualquiera, si el VIN está cerca de una palabra clave en uno de los siguientes idiomas: inglés, francés, alemán, lituano, polaco, portugués, rumano o español

Referencia detallada: identificadores de datos gestionados por Amazon Macie

En Amazon Macie, los identificadores de datos administrados son criterios y técnicas integradas diseñados para detectar tipos específicos de datos confidenciales. Pueden detectar una lista grande y creciente de tipos de datos confidenciales para muchos países y regiones, incluyendo múltiples tipos de datos de credenciales, información financiera e información personal. Cada identificador de datos administrado está diseñado para detectar un tipo específico de datos confidenciales, como por ejemplo, AWS clave de acceso secreta, números de tarjetas de crédito, claves de acceso secretas, números de tarjetas de crédito o de pasaporte de un país o región en particular.

Macie puede detectar las siguientes categorías de datos confidenciales mediante identificadores de datos administrados. Dentro de cada categoría, Macie puede detectar varios tipos de datos

confidenciales. Los temas de esta sección enumeran y describen cada tipo y cualquier requisito relevante para detectar los datos. Para obtener más información sobre los identificadores de datos gestionados para tipos específicos de datos confidenciales, puede examinar los temas por categoría:

- Credenciales: para datos de credenciales, como claves privadas y claves de acceso AWS secretas.
- Información financiera: para datos financieros como números de tarjetas de crédito y números de cuentas bancarias.
- Información personal: PHI: para información de salud personal (PHI), como números de seguro médico e identificación médica.
- Información personal: PII: para información de identificación personal (PII), como los números de identificación del carné de conducir y los números de pasaporte.

O bien, puede elegir un tipo específico de datos confidenciales de la siguiente tabla. En la tabla se enumeran todos los identificadores de datos gestionados que Macie proporciona actualmente, organizados por tipo de datos confidenciales. La tabla también resume los requisitos relevantes para detectar cada tipo.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Clave de acceso secreta de AWS	Credenciales	AWS_CREDENTIALS	Sí	Cualquiera
Número de cuenta bancaria	Información financiera	BANK_ACCOUNT_NUMBER (para Canadá y EE. UU.),	Sí	Canadá, EE. UU.
Número de cuenta bancaria básico (BBAN)	Información financiera	Según el país o región: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BAN	Sí	Alemania, España, Francia, Italia,

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		K_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER		Reino Unido
Fecha de nacimiento	Información personal: PII	DATE_OF_BIRTH	Sí	Cualquiera
Fecha de caducidad de la tarjeta	Información financiera	CREDIT_CARD_EXPIRATION	Sí	Cualquiera
Datos de banda magnética de tarjetas de crédito	Información financiera	CREDIT_CARD_MAGNETIC_STRIPE	Sí	Cualquiera
Número de tarjetas de crédito	Información financiera	CREDIT_CARD_NUMBER (para números de tarjetas de crédito próximos a una palabra clave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (para números de tarjetas de crédito que no están cerca de una palabra clave)	Varía	Cualquiera
Código de verificación de tarjeta de crédito	Información financiera	CREDIT_CARD_SECURITY_CODE	Sí	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación del permiso de conducir	Información personal: PII	Según el país o región: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Sí	Australia, Austria, Bélgica, Bulgaria, Canadá, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, India, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía, Eslovaquia, Eslovenia

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, España, Suecia, Reino Unido, Estados Unidos
Número de registro de la Administración para el Control de Drogas (DEA)	Información personal: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sí	EE. UU.
Número de registro electoral	Información personal: PII	UK_ELECTORAL_ROLL_NUMBER	Sí	Reino Unido
Nombre completo	Información personal: PII	NAME	No	Cualquiera, si el nombre utiliza un juego de caracteres latinos

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Coordenadas del sistema de posicionamiento global (GPS)	Información personal: PII	LATITUDE_LONGITUDE	Sí	Cualquiera, si las coordenadas están cerca de una palabra clave en inglés
Clave de API de Google Cloud	Credenciales	GCP_API_KEY	Sí	Cualquiera
Número de reclamación del seguro médico (HICN)	Información personal: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sí	EE. UU.
Número de seguro médico o identificación médica	Información personal: PHI	Según el país o región: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sí	Canadá, UE, Estados Unidos, Finlandia, Francia, Reino Unido

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)	Información personal: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sí	EE. UU.
Encabezado de autorización básica de HTTP	Credenciales	HTTP_BASIC_AUTH_HEADER	No	Cualquiera
Cookie HTTP	Información personal: PII	HTTP_COOKIE	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de cuenta bancaria internacional (IBAN)	Información financiera	Según el país o región: ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER,	No	Albania, Andorra, Bosnia-Herzegovina, Brasil, Bulgaria, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, República Dominicana, Egipto, Estonia, Islas Feroe, Finlandia, Francia, Georgia, Alemania, Grecia, Groenlandia, Hungría, Islandia, Irlanda, Italia, Jordania,

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER,		Kosovo, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauricio, Mónaco, Montenegro, Países Bajos, Macedonia del Norte, Polonia, Portugal, San Marino, Senegal, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Timor-Leste, Túnez, Türkiye, Reino Unido, Ucrania,

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (para las Islas Vírgenes Británicas)		Árabe Unido Emiratos, Islas Vírgenes Británicas
Token web JSON (JWT)	Credenciales	JSON_WEB_TOKEN	No	Cualquiera
Dirección postal	Información personal: PII	ADDRESS, BRAZIL_CEP_CODE (para el Código de Endereçamento Postal de Brasil)	Varía	Australia, Brasil, Canadá, Francia, Alemania, Italia, España, Reino Unido, Estados Unidos
Código nacional de medicamento (NDC)	Información personal: PHI	USA_NATIONAL_DRUG_CODE	Sí	EE. UU.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación nacional	Información personal: PII	Según el país o región: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Sí	Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos
Número de seguro nacional (NINO)	Información personal: PII	UK_NATIONAL_INSURANCE_NUMBER	Sí	Reino Unido
Identificador nacional de proveedor (NPI)	Información personal: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sí	EE. UU.
Clave privada de OpenSSH	Credenciales	OPENSSH_PRIVATE_KEY	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de pasaporte	Información personal: PII	Según el país o región: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sí	Alemania, Canadá, España, Estados Unidos, Francia, Italia, Reino Unido
Número de residencia permanente	Información personal: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Sí	Canadá
Clave privada de PGP	Credenciales	PGP_PRIVATE_KEY	No	Cualquiera
Número de teléfono	Información personal: PII	Según el país o región: BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Varía	Alemania, Brasil, Canadá, España, Estados Unidos, Francia, Italia, Reino Unido

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Clave privada del estándar de criptografía de clave pública (PKCS)	Credenciales	PKCS	No	Cualquiera
Clave privada PuTTY	Credenciales	PUTTY_PRIVATE_KEY	No	Cualquiera
Número de Seguro Social (SIN)	Información personal: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sí	Canadá
Número de la Seguridad Social (SSN)	Información personal: PII	Según el país o región: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sí	España, Estados Unidos
the section called “Clave de API de Stripe”	Credenciales	STRIPE_CREDENTIALS	No	Cualquiera

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación o referencia del contribuyente	Información personal: PII	Según el país o región: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Sí	Australia, Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos
Identificador de dispositivo único (UDI)	Información personal: PHI	MEDICAL_DEVICE_UDI	Sí	EE. UU.

Tipos de datos confidenciales	Categoría de datos confidenciales	Identificador de datos administrados	Palabra clave necesaria	Países y regiones
Número de identificación de vehículo (VIN)	Información personal: PII	VEHICLE_IDENTIFICATION_NUMBER	Sí	Cualquiera, si el VIN está cerca de una palabra clave en uno de los siguientes idiomas: inglés, francés, alemán, lituano, polaco, portugués, rumano o español

Identificadores de datos administrados para datos de credenciales

Amazon Macie puede detectar distintos tipos de datos de credenciales confidenciales mediante identificadores de datos administrados. Los temas de esta página especifican cada tipo y proporcionan información sobre el identificador de datos administrados que está diseñado para detectar los datos. Cada tema proporciona la siguiente información:

- ID de datos administrados: especifica el identificador único (ID) del identificador de datos administrados que está diseñado para detectar los datos. Al crear una tarea de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede usar este ID para especificar si desea que Macie utilice el identificador de datos gestionados cuando analice los datos.

- Países y regiones compatibles: indica para qué países o regiones está diseñado el identificador de datos gestionados aplicable. Si el identificador de datos gestionados no está diseñado para un país o región en particular, este valor es Cualquiera.
- Palabra clave obligatoria: especifica si la detección requiere que una palabra clave esté cerca de los datos. Si se requiere una palabra clave, el tema también proporciona ejemplos de palabras clave obligatorias. Para obtener información sobre cómo Macie utiliza las palabras clave cuando analiza los datos, consulteRequisitos de palabras clave.
- Comentarios: proporciona todos los detalles relevantes que puedan afectar a la elección del identificador de datos gestionados o a la investigación de los informes de casos de datos confidenciales. Los detalles incluyen información como los estándares admitidos, los requisitos de sintaxis y las excepciones.

Los temas se enumeran en orden alfabético por tipo de datos confidenciales.

Tipos de datos confidenciales

- Clave de acceso secreta de AWS
- Clave de API de Google Cloud
- Encabezado de autorización básica de HTTP
- Token web JSON (JWT)
- Clave privada de OpenSSH
- Clave privada de PGP
- Clave privada del estándar de criptografía de clave pública (PKCS)
- Clave privada PuTTY
- Clave de API de Stripe

Clave de acceso secreta de AWS

ID del Identificador de datos administrados: AWS_CREDENTIALS

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

Comentarios: Macie no informa de la aparición de las siguientes secuencias de caracteres, que se utilizan comúnmente como ejemplos ficticios: `je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` y `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Clave de API de Google Cloud

ID del Identificador de datos administrados: GCP_API_KEY

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Comentarios: Macie solo puede detectar el componente de cadena (`keyString`) de una clave de API de Google Cloud. El soporte no incluye la detección del componente de ID o nombre para mostrar de una clave de API de Google Cloud.

Encabezado de autorización básica de HTTP

ID del Identificador de datos administrados: HTTP_BASIC_AUTH_HEADER

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: la detección requiere un encabezado completo, que incluya el nombre del campo y la directiva del esquema de autenticación, tal como se especifica en el RFC 7617. Por ejemplo: `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` y `Proxy-Authorization: Basic dGVzdDoxMjPCow==`.

Token web JSON (JWT)

ID del Identificador de datos administrados: JSON_WEB_TOKEN

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: Macie puede detectar los Tokens web JSON (JWT) que cumplen los requisitos especificados en el RFC 7519 para las estructuras de firma web JSON (JWS). Los tokens pueden estar firmados o no firmados.

Clave privada de OpenSSH

ID del Identificador de datos administrados: OPENSSH_PRIVATE_KEY

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: ninguno

Clave privada de PGP

ID del Identificador de datos administrados: PGP_PRIVATE_KEY

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: ninguno

Clave privada del estándar de criptografía de clave pública (PKCS)

ID del Identificador de datos administrados: PKCS

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: ninguno

Clave privada PuTTY

ID del Identificador de datos administrados: PUTTY_PRIVATE_KEY

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: Macie puede detectar claves privadas de PuTTY que utilizan los siguientes encabezados y secuencias de encabezados estándar`PuTTY-User-Key-File`:`Encryption`,, `Comment``Public-Lines`, `Private-Lines` y. `Private-MAC` Los valores del encabezado pueden contener caracteres alfanuméricos, guiones () y caracteres de nueva línea (o`-`). `\n` `\r` `Public-Lines`y `Private-Lines` los valores también pueden contener barras diagonales (`/`), signos más () y signos + iguales (). = `Private-MAC`Los valores también pueden contener signos más (+).

Support no incluye la detección de claves privadas con valores de encabezado que contengan otros caracteres, como espacios o guiones bajos (_). Support tampoco incluye la detección de claves privadas que incluyan encabezados personalizados.

Clave de API de Stripe

ID del Identificador de datos administrados: STRIPE_CREDENTIALS

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: Macie no informa de la aparición de las siguientes secuencias de caracteres, que se utilizan comúnmente como ejemplos ficticios: `sk_test_4eC39HqLyjWDarjtT1zdp7dc` y `pk_test_TYooMQauvdEDq54NiTphI7jx`.

Identificadores de datos administrados para información financiera

Obtenga información sobre los tipos de información financiera que Amazon Macie puede detectar mediante identificadores de datos administrados. Los temas de esta página enumeran cada tipo y proporcionan información sobre los identificadores de datos administrados que están diseñados para detectar los datos. Cada tema proporciona la siguiente información.

- ID de identificador datos administrados: especifica el identificador único (ID) para uno o más identificadores de datos administrados que están diseñados para detectar los datos. Al crear un trabajo de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede utilizar estos ID para especificar qué identificadores de datos gestionados desea que Macie utilice cuando analice datos.
- Países y regiones compatibles: indica para qué países o regiones está diseñado el identificador de datos gestionados aplicable. Si los identificadores de datos administrados no están diseñados para un país o región en particular, este valor es Cualquiera.
- Palabra clave obligatoria: especifica si la detección requiere que una palabra clave esté cerca de los datos. Si se requiere una palabra clave, el tema también proporciona ejemplos de palabras clave obligatorias. Para obtener información sobre cómo Macie utiliza las palabras clave cuando analiza los datos, consulteRequisitos de palabras clave.
- Comentarios: proporciona todos los detalles relevantes que puedan afectar a la elección del identificador de datos gestionados o a la investigación de los informes de casos de datos confidenciales. Los detalles incluyen información como los estándares admitidos, los requisitos de sintaxis y las excepciones.

Los temas se enumeran en orden alfabético por tipo de datos confidenciales.

Tipos de datos confidenciales

- Número de cuenta bancaria
- Número de cuenta bancaria básico (BBAN)
- Fecha de caducidad de la tarjeta
- Datos de banda magnética de tarjetas de crédito
- Número de tarjetas de crédito
- Código de verificación de tarjeta de crédito
- Número de cuenta bancaria internacional (IBAN)

Número de cuenta bancaria

Macie puede detectar números de cuentas bancarias canadienses y estadounidenses que consten de secuencias de 9 a 17 dígitos y no contengan espacios.

ID del Identificador de datos administrados:BANK_ACCOUNT_NUMBER

Regiones y países admitidos: Canadá y EE. UU.

Palabra clave necesaria: Sí. Las palabras clave incluyen: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Comentarios: este identificador de datos gestionados está diseñado explícitamente para detectar los números de cuentas bancarias de Canadá y EE. UU. Estos países no utilizan los formatos de número de cuenta bancaria básico (BBAN) o número de cuenta bancaria internacional (IBAN) definidos por la norma internacional ISO para la numeración de cuentas bancarias, tal como se especifica en la norma ISO 13616. Para detectar los números de cuentas bancarias de otros países y regiones, utilice los identificadores de datos gestionados diseñados para esos formatos. Para más información, consulte Número de cuenta bancaria básico (BBAN) y Número de cuenta bancaria internacional (IBAN).

Número de cuenta bancaria básico (BBAN)

Macie puede detectar números de cuentas bancarias básicos (BBAN) que se ajusten a la estructura BBAN definida por la norma internacional ISO para la numeración de cuentas bancarias, tal como se

especifica en la norma ISO 13616. Esto incluye los IBAN que no contienen espacios o que utilizan separadores de espacios o guiones, por ejemplo: `NWBK60161331926819`, `NWBK 6016 1331 9268 19` y `NWBK-6016-1331-9268-19`.

ID identificador de datos gestionados: según el país o la región, FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

Países y regiones compatibles: Francia, Alemania, Italia, España y Reino Unido

Palabra clave necesaria: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Francia	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
Alemania	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzah l, iban, kartennummer, kontonummer, kreditkar tennummer, sepa
Italia	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
España	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account

País o región	Palabras clave
	number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
Reino Unido	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

Comentarios: estos identificadores de datos gestionados también pueden detectar números de cuentas bancarias internacionales (IBAN) que cumplan con la norma ISO 13616. Para obtener más información, consulte Número de cuenta bancaria internacional (IBAN). El identificador de datos gestionados del Reino Unido (UK_BANK_ACCOUNT_NUMBER) también puede detectar los números de cuentas bancarias nacionales del Reino Unido, por ejemplo, `60-16-13 31926819`.

Fecha de caducidad de la tarjeta

ID del Identificador de datos administrados:CREDIT_CARD_EXPIRATION

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: exp d, exp m, exp y, expiration, expiry

Comentarios: Admite la mayoría de formatos de fecha, como todos los dígitos y combinaciones de dígitos y nombres de meses. Los componentes de fecha se pueden separar mediante barras (/) o guiones (-) o palabras clave aplicables. Por ejemplo, Macie puede detectar fechas como `02/26`, `02/2026`, `Feb 2026`, `26-Feb` y `expY=2026, expM=02`.

Datos de banda magnética de tarjetas de crédito

ID del Identificador de datos administrados:CREDIT_CARD_MAGNETIC_STRIPE

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: card data, iso7813, mag, magstripe, stripe, swipe

Comentarios: la compatibilidad incluye las pistas 1 y 2.

Número de tarjetas de crédito

ID del identificador de datos gestionados: CREDIT_CARD_NUMBER para números de tarjetas de crédito próximos a una palabra clave, CREDIT_CARD_NUMBER_(NO_KEYWORD) para números de tarjetas de crédito que no están próximos a una palabra clave

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Varía El identificador de datos CREDIT_CARD_NUMBER gestionados requiere palabras clave. Las palabras clave incluyen: account number, american express, amex, bank card, card, card num, card number, cc #, ccn, check card, credit, credit card#, dankort, debit, debit card, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, union pay, visa. El identificador de datos CREDIT_CARD_NUMBER_(NO_KEYWORD) gestionados no requiere palabras clave.

Comentarios: La detección requiere que los datos estén en una secuencia de 13 a 19 dígitos que siga la fórmula del cheque de Luhn y utilice un prefijo numérico de tarjeta estándar para cualquiera de los siguientes tipos de tarjetas de crédito: American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard y Visa. UnionPay

Macie no informa de la aparición de las siguientes secuencias, que los emisores de tarjetas de crédito se reservan para las pruebas públicas: 122000000000003, 2222405343248877, 2222990905257051, 2223007648726984, 2223577120017656, 30569309025904, 34343434343434, 3528000700000000, 3530111333300000, 3566002020360505, 36148900647913, 36700102000000, 371449635398431, 378282246310005, 378734493671000, 38520000023237, 4012888888881881, 4111111111111111, 4222222222222, 4444333322221111, 4462030000000000, 4484070000000000, 4911830000000, 4917300800000000, 4917610000000000, 4917610000000000003, 5019717010103742, 5105105105105100, 5111010030175156, 5185540810000019, 5200828282828210, 5204230080000017, 5204740009900014, 5420923878724339, 5454545454545454, 5455330760000018, 5506900490000436, 5506900490000444, 5506900510000234, 5506920809243667, 5506922400634930, 5506927427317625, 5553042241984105, 5555553753048194, 5555555555554444, 5610591081018250, 6011000990139424, 6011000400000000, 6011111111111117, 630490017740292441, 630495060000000000, 6331101999990016, 6759649826438453, 6799990100000000019 y 76009244561.

Código de verificación de tarjeta de crédito

ID del Identificador de datos administrados:CREDIT_CARD_SECURITY_CODE

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

Comentarios: ninguno

Número de cuenta bancaria internacional (IBAN)

Macie puede detectar números de cuentas bancarias internacionales (IBAN) que constan de hasta 34 caracteres alfanuméricos, incluidos elementos como el código de país. Más concretamente, Macie puede detectar los IBAN que cumplen con la norma internacional ISO para la numeración de cuentas bancarias, tal como se especifica en la norma ISO 13616. Esto incluye los IBAN que no contienen espacios o que utilizan separadores de espacios o guiones, por ejemplo: `GB29NWBK60161331926819`, `GB29 NWBK 6016 1331 9268 19` y `GB29-NWBK-6016-1331-9268-19`. La detección incluye comprobaciones de validación basadas en el esquema Modulus 97.

ID de identificador de datos gestionados: según el país o la región ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER,

NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (en el caso de las Islas Vírgenes Británicas)

Países y regiones compatibles: Albania, Andorra, Bosnia-Herzegovina, Brasil, Bulgaria, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, República Dominicana, Egipto, Estonia, Islas Feroe, Finlandia, Francia, Georgia, Alemania, Grecia, Groenlandia, Hungría, Islandia, Irlanda, Italia, Jordania, Kosovo, Kosovo, Liechtenstein, Lituania, Malta, Mauritania, Mauricio, Mónaco, Montenegro, Países Bajos, Macedonia del Norte, Polonia, Portugal, San Marino, Senegal, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Timor-Leste, Túnez, Türkiye, Reino Unido, Ucrania, Árabe Unido Emiratos, Islas Vírgenes Británicas

Palabra clave necesaria: No

Comentarios: los identificadores de datos gestionados de Francia, Alemania, Italia, España y el Reino Unido también pueden detectar números básicos de cuentas bancarias (BBAN) que se ajusten a la estructura BBAN definida por la norma ISO 13616, si la secuencia de caracteres está cerca de una palabra clave. Para obtener más información, consulte Número de cuenta bancaria básico (BBAN).

Identificadores de datos administrados para información médica personal (PHI)

Amazon Macie puede detectar distintos tipos de información médica personal (PHI) confidencial mediante identificadores de datos administrados. Los temas de esta página especifican cada tipo y proporcionan información sobre el identificador de datos administrados que está diseñado para detectar los datos. Cada tema proporciona la siguiente información:

- ID de datos administrados: especifica el identificador único (ID) del identificador de datos administrados que está diseñado para detectar los datos. Al crear una tarea de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede usar este ID para especificar si desea que Macie utilice el identificador de datos gestionados cuando analice los datos.

- Países y regiones compatibles: indica para qué países o regiones está diseñado el identificador de datos gestionados aplicable. Si el identificador de datos gestionados no está diseñado para un país o región en particular, este valor es Cualquiera.
- Palabra clave obligatoria: especifica si la detección requiere que una palabra clave esté cerca de los datos. Si se requiere una palabra clave, el tema también proporciona ejemplos de palabras clave obligatorias. Para obtener información sobre cómo Macie utiliza las palabras clave cuando analiza los datos, consulteRequisitos de palabras clave.
- Comentarios: proporciona todos los detalles relevantes que puedan afectar a la elección del identificador de datos gestionados o a la investigación de los informes de casos de datos confidenciales. Los detalles incluyen información como los estándares admitidos, los requisitos de sintaxis y las excepciones.

Los temas se enumeran en orden alfabético por tipo de datos confidenciales.

Tipos de datos confidenciales

Número de registro de la Administración para el Control de Drogas (DEA)

Identificador de datos administrados: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: dea number, dea registration

Comentarios: ninguno

Número de reclamación del seguro médico (HICN)

Identificador de datos administrados: USA_HEALTH_INSURANCE_CLAIM_NUMBER

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

Comentarios: ninguno

Número de seguro médico o identificación médica

El soporte incluye números de tarjetas de seguro médico europeas para la UE y Finlandia, números de seguro médico para Francia, identificadores de beneficiarios de Medicare para los EE. UU., números del NS para el Reino Unido y de médicos personales para Canadá.

ID identificador de datos gestionados: según el país o la región, CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Países y regiones compatibles: Canadá, UE, Finlandia, Francia, Reino Unido y EE. UU.

Se requiere palabra clave: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Canadá	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
UE	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d’assurance maladie, numéro de carte d’assurance, numéro

País o región	Palabras clave
	de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausva kuutuskortti, sairausvakuutusnumero, sjukförsä kring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicher ungsnummer
Finlandia	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskor t, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin , sairausvakuutuskortti, sairausvakuutusnum ero, sjukförsäkring nummer, sjukförsäkringskor t, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
Francia	carte d'assuré social, carte vitale, insurance card
Reino Unido	national health service, NHS
EE. UU.	mbi, medicare beneficiary

Comentarios: ninguno

Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)

Identificador de datos administrados: USA_HEALTHCARE_PROCEDURE_CODE

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: current procedural terminology, hcpcs, healthcare common procedure coding system

Comentarios: ninguno

Código nacional de medicamento (NDC)

Identificador de datos administrados: USA_NATIONAL_DRUG_CODE

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: national drug code, ndc

Comentarios: ninguno

Identificador nacional de proveedor (NPI)

Identificador de datos administrados: USA_NATIONAL_PROVIDER_IDENTIFIER

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: hipaa, n.p.i, national provider, npi

Comentarios: ninguno

Identificador de dispositivo único (UDI)

Identificador de datos administrados: MEDICAL_DEVICE_UDI

Regiones y países admitidos: EE. UU.

Se requiere palabra clave: Sí. Las palabras clave incluyen: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Comentarios: Macie puede detectar identificadores únicos de dispositivos (UDIs) que cumplen con los formatos aprobados por la Administración de Alimentos y Medicamentos de los EE. UU. Esto incluye los formatos estándar definidos por GS1, HIBCC e ICCBBA. El soporte ICCBA es para el estándar ISBT.

Identificadores de datos administrados para la información de identificación personal (PII)

Amazon Macie puede detectar varios tipos de información de identificación personal (PII) e información confidencial mediante identificadores de datos administrados. Los temas de esta página enumeran cada tipo y proporcionan información sobre los identificadores de datos administrados que están diseñados para detectar los datos. Cada tema proporciona la siguiente información.

- ID de identificador datos administrados: especifica el identificador único (ID) para uno o más identificadores de datos administrados que están diseñados para detectar los datos. Al crear un trabajo de detección de datos confidenciales o configurar los ajustes de detección automática de datos confidenciales, puede utilizar estos ID para especificar qué identificadores de datos gestionados desea que Macie utilice cuando analice datos.
- Países y regiones compatibles: indica para qué países o regiones está diseñado el identificador de datos gestionados aplicable. Si los identificadores de datos administrados no están diseñados para un país o región en particular, este valor es Cualquiera.
- Palabra clave obligatoria: especifica si la detección requiere que una palabra clave esté cerca de los datos. Si se requiere una palabra clave, el tema también proporciona ejemplos de palabras clave obligatorias. Para obtener información sobre cómo Macie utiliza las palabras clave cuando analiza los datos, consulteRequisitos de palabras clave.
- Comentarios: proporciona todos los detalles relevantes que puedan afectar a la elección del identificador de datos gestionados o a la investigación de los informes de casos de datos confidenciales. Los detalles incluyen información como los estándares admitidos, los requisitos de sintaxis y las excepciones.

Los temas se enumeran en orden alfabético por tipo de datos confidenciales.

Tipos de datos confidenciales

- Fecha de nacimiento
- Número de identificación del permiso de conducir
- Número de registro electoral
- Nombre completo
- Coordenadas del sistema de posicionamiento global (GPS)
- Cookie HTTP
- Dirección postal
- Número de identificación nacional
- Número de seguro nacional (NINO)
- Número de pasaporte
- Número de residencia permanente
- Número de teléfono

- Número de Seguro Social (SIN)
- Número de la Seguridad Social (SSN)
- Número de identificación o referencia del contribuyente
- Número de identificación de vehículo (VIN)

Fecha de nacimiento

ID del Identificador de datos administrados:DATE_OF_BIRTH

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: Sí. Las palabras clave incluyen: bday, b-day, birth date, birthday, date of birth, dob

Comentarios: Admite la mayoría de formatos de fecha, como todos los dígitos y combinaciones de dígitos y nombres de meses. Los componentes de fecha se pueden separar mediante espacios, barras (/) o guiones (-).

Número de identificación del permiso de conducir

ID identificador de datos gestionados: según el país o la región, AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

Regiones y países admitidos: Alemania, Australia, Austria, Bélgica, Bulgaria, Canadá, Chipre, Croacia, Dinamarca, EE. UU., Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, India, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumanía, Reino Unido, República Checa, Suecia

Palabra clave necesaria: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Australia	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
Austria	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
Bélgica	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
Bulgaria	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
Canadá	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
Croacia	vozačka dozvola

País o región	Palabras clave
Chipre	άδεια οδήγησης
República Checa	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
Dinamarca	kørekort, kørekortnummer
Estonia	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finlandia	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
Francia	permis de conduire
Alemania	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
Grecia	δεια οδήγησης, adeia odigisis
Hungría	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
India	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
Irlanda	ceadúnas tiomána

País o región	Palabras clave
Italia	patente di guida, patente di guida numero, patente guida, patente guida numero
Letonia	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
Lituania	vairuotojo pažymėjimas
Luxemburgo	fahrerlaubnis, führerschäin
Malta	liċenzja tas-sewqan
Países Bajos	permis de conduire, rijbewijs, rijbewijsnummer
Polonia	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
Portugal	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
Rumanía	numărul permisului de conducere, permis de conducere
Eslovaquia	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Eslovenia	vozniško dovoljenje

País o región	Palabras clave
España	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
Suecia	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
Reino Unido	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
EE. UU.	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Comentarios: ninguno

Número de registro electoral

ID del Identificador de datos administrados:UK_ELECTORAL_ROLL_NUMBER

Regiones y países admitidos: Reino Unido

Palabra clave necesaria: Sí. Las palabras clave incluyen: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Comentarios: ninguno

Nombre completo

ID del Identificador de datos administrados:NAME

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: Macie solo puede detectar nombres completos. La compatibilidad se limita a los conjuntos de caracteres latinos.

Coordenadas del sistema de posicionamiento global (GPS)

ID del Identificador de datos administrados:LATITUDE_LONGITUDE

Regiones y países admitidos: Cualquiera, si las coordenadas están cerca de una palabra clave en inglés

Palabra clave necesaria: Sí. Las palabras clave incluyen: coordinate, coordinates, lat long, latitude longitude, position

Comentarios: Macie puede detectar las coordenadas GPS si las coordenadas de latitud y longitud se almacenan como un par y están en formato de grados decimales (DD), por ejemplo `41.948614,-87.655311`. No es compatible con coordenadas en formato de grados y minutos decimales (DDM), como por ejemplo: `41°56.9168'N 87°39.3187'W`; o en formato de grados, minutos y segundos (DMS), como por ejemplo: `41°56'55.0104"N 87°39'19.1196"W`.

Cookie HTTP

ID del Identificador de datos administrados:HTTP_COOKIE

Regiones y países admitidos: Cualquiera

Palabra clave necesaria: No

Comentarios: la detección requiere un encabezado `Cookie` o `Set-Cookie` completo. El encabezado puede incluir uno o más pares de nombre-valor, por ejemplo: `Set-Cookie: id=TWlrZQ` y `Cookie: session=3948; lang=en`.

Dirección postal

ID de identificador de datos gestionados: ADDRESS (para Australia, Canadá, Francia, Alemania, Italia, España, Reino Unido y EE. UU.), BRAZIL_CEP_CODE (para el Código de Endereçamento Postal de Brasil)

Países y regiones compatibles: Australia, Brasil, Canadá, Francia, Alemania, Italia, España, Reino Unido, Estados Unidos

Palabra clave necesaria: Varía El identificador de datos ADDRESS gestionados no requiere palabras clave. El identificador de datos BRAZIL_CEP_CODE gestionados requiere palabras clave. Las palabras clave incluyen: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

Comentarios: Si bien el identificador de datos ADDRESS gestionados no requiere ninguna palabra clave, la detección requiere una dirección que incluya el nombre de una ciudad o un lugar y el código postal o postal correspondiente en un país o región compatibles. El identificador de datos BRAZIL_CEP_CODE gestionados solo puede detectar la parte del Código de Endereçamento Postal (CEP) de una dirección.

Número de identificación nacional

Esto incluye los identificadores del número Aadhar (India), del número de Codice Fiscale (Italia), del documento nacional de identidad (DNI) (España), los códigos del Instituto Nacional de Estadística y Estudios Económicos (INSEE) de Francia, los números del documento nacional de identidad alemán y los números del Registro Geral (RG) (Brasil).

ID identificador de datos gestionados: según el país o la región, BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Países y regiones compatibles: Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos

Palabra clave necesaria: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Brasil	registro geral, rg
Francia	assurance sociale, carte nationale d’identit é, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
Alemania	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
India	aadhaar, aadhar, adhaar, uidai
Italia	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
España	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

Comentarios: ninguno

Número de seguro nacional (NINO)

ID del Identificador de datos administrados:UK_NATIONAL_INSURANCE_NUMBER

Regiones y países admitidos: Reino Unido

Palabra clave necesaria: Sí. Las palabras clave incluyen: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

Comentarios: ninguno

Número de pasaporte

ID identificador de datos gestionados: según el país o la región, CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

Países y regiones compatibles: Canadá, España, Estados Unidos, Francia, Italia, Reino Unido

Palabra clave necesaria: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Canadá	passeport, passeport#, passport, passport#, passportno, passportno#
Francia	numéro de passeport, passeport, passeport #, passeport n °, passeport non
Alemania	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
Italia	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
España	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport

País o región	Palabras clave
Reino Unido	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
EE. UU.	passport, travel document

Comentarios: ninguno

Número de residencia permanente

ID del Identificador de datos administrados:CANADA_NATIONAL_IDENTIFICATION_NUMBER

Regiones y países admitidos: Canadá

Palabra clave necesaria: Sí. Las palabras clave incluyen: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

Comentarios: ninguno

Número de teléfono

ID identificador de datos gestionados: según el país o la región, BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

Países y regiones compatibles: Brasil, Canadá, España, Estados Unidos, Francia, Italia, Reino Unido

Palabra clave necesaria: Varía Si una palabra clave está cerca de los datos, no es necesario que el número incluya un código de país. Las palabras clave incluyen: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Brasil: las palabras clave también incluyen: cel, celular, fone, móvel, número residencial, numero residencial, telefone. Si una palabra clave no está cerca de los datos, el número debe incluir un código de país.

Comentarios: Para Estados Unidos, se admiten los números de teléfono gratuitos.

Número de Seguro Social (SIN)

ID del Identificador de datos administrados:CANADA_SOCIAL_INSURANCE_NUMBER

Regiones y países admitidos: Canadá

Palabra clave necesaria: Sí. Las palabras clave incluyen: canadian id, numéro d'assurance sociale, sin, social insurance number

Comentarios: ninguno

Número de la Seguridad Social (SSN)

ID identificador de datos administrados: según el país o la región, SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Regiones y países admitidos: España, EE. UU.

Palabra clave necesaria: Sí. Para España, las palabras clave incluyen: número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Para EE. UU., las palabras clave incluyen: social security, ss#, ssn.

Comentarios: ninguno

Número de identificación o referencia del contribuyente

El soporte incluye: números CIF, NIE y NIF para España; números CNPJ y CPF para Brasil; números Codice Fiscale para Italia; ITIN para EE. UU.; PAN para India; números Steueridentifikationsnummer para Alemania; TFN para Australia; TIN para Francia; y números TRN y UTR para el Reino Unido.

ID identificador de datos gestionados: según el país o la región, AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Países y regiones compatibles: Australia, Brasil, Francia, Alemania, India, Italia, España, Reino Unido, Estados Unidos

Palabra clave necesaria: Sí. En la siguiente tabla se enumeran las palabras clave que Macie reconoce para países y regiones específicos.

País o región	Palabras clave
Australia	tax file number, tfn

País o región	Palabras clave
Brasil	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
Francia	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
Alemania	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
India	e-pan, pan card, pan number, permanent account number
Italia	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
España	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
Reino Unido	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
EE. UU.	número de identificación tributaria individual (ITIN)

Comentarios: ninguno

Número de identificación de vehículo (VIN)

ID del Identificador de datos administrados:VEHICLE_IDENTIFICATION_NUMBER

Países y regiones compatibles: Cualquiera, si el VIN está cerca de una palabra clave en uno de los siguientes idiomas: inglés, francés, alemán, lituano, polaco, portugués, rumano o español

Palabra clave necesaria: Sí. Las palabras clave incluyen: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

Comentarios: Macie puede detectar VIN que constan de una secuencia de 17 caracteres y cumplen con las normas ISO 3779 y 3780. Estos estándares fueron diseñados para su uso en todo el mundo.

Creación de identificadores de datos personalizados en Amazon Macie

Un identificador de datos personalizado es un conjunto de criterios que se definen para detectar datos confidenciales en objetos de Amazon Simple Storage Service (Amazon S3). Los criterios consisten en una expresión regular (regex) que define un patrón de texto para que coincida y, opcionalmente, secuencias de caracteres y una regla de proximidad que perfeccionen los resultados.

Con identificadores de datos personalizados, puede definir criterios de detección que reflejen escenarios particulares de su organización, propiedad intelectual o datos de propietario, por ejemplo, identificaciones de empleados, números de cuentas de clientes o clasificaciones de datos internas. Si configura trabajos de descubrimiento de datos confidenciales o el descubrimiento automatizado de datos confidenciales para usar estos identificadores, puede analizar los objetos de S3 de una manera que complemente los identificadores de datos administrados que proporciona Amazon Macie.

Además de los criterios de detección, puede definir ajustes de gravedad personalizados para los resultados de datos confidenciales que genere un identificador de datos personalizado. De forma predeterminada, Macie asigna la gravedad media a todos los resultados que produce un identificador de datos personalizado; la gravedad no cambia en función del número de apariciones de texto que coincidan con los criterios de detección de un identificador de datos personalizado. Al definir una

configuración de gravedad personalizada, puede especificar qué gravedad asignar en función del número de apariciones de texto que coincidan con los criterios.

Temas

Definir los criterios de detección para los identificadores de datos personalizados

Cuando crea un identificador de datos personalizado, especifica una expresión regular (regex) que define un patrón de texto para que coincida con objetos de S3. Macie admite un subconjunto de la sintaxis de patrones de expresiones regulares proporcionado por la biblioteca de expresiones regulares compatibles con Perl (PCRE). Para obtener más información, consulte Compatibilidad de experiones regulares más adelante en este tema.

También puede especificar secuencias de caracteres, como palabras y frases, y una regla de proximidad para refinar los resultados.

Palabras clave

Son secuencias de caracteres que deben estar cerca del texto que coincida con el patrón de expresiones regulares. Los requisitos de proximidad varían según el formato de almacenamiento o el tipo de archivo del objeto S3:

- En el caso de los datos estructurados y en columnas, Macie incluye un resultado si el texto coincide con el patrón de expresiones regulares y hay una palabra clave en el nombre del campo o la columna que almacena el texto, o si el texto va precedido por una palabra clave del mismo valor de campo o celda y dentro de la distancia máxima de coincidencia de dicha palabra clave. Esto es válido para los libros de trabajo de Microsoft Excel, los archivos CSV y los archivos TSV.
- En el caso de los datos estructurados y basados en registros, Macie incluye un resultado si el texto coincide con el patrón de expresiones regulares y el texto se encuentra dentro de la distancia máxima de coincidencia de una palabra clave. La palabra clave puede estar en el

nombre de un elemento de la ruta al campo o matriz que almacena el texto, o puede preceder y formar parte del mismo valor en el campo o matriz que almacena el texto. Esto es válido para los contenedores de objetos Apache Avro, los archivos Apache Parquet, los archivos JSON y los archivos JSON Lines.

- En el caso de los datos no estructurados, Macie incluye un resultado si el texto coincide con el patrón de expresiones regulares y va precedido por una palabra clave dentro de la distancia máxima de coincidencia de la misma. Esto es válido para los archivos de formato de documento portátil de Adobe, los documentos de Microsoft Word, los mensajes de correo electrónico y los archivos de texto no binarios distintos de los archivos CSV, JSON, JSON Lines y TSV. Esto incluye todos los datos estructurados, como las tablas, de estos tipos de archivos.

Puede especificar hasta 50 palabras clave. Cada palabra clave puede contener entre 3 y 90 caracteres UTF-8. Las palabras clave no distinguen entre mayúsculas y minúsculas.

Distancia máxima de coincidencia

Se trata de una regla de proximidad basada en caracteres para las palabras clave. Macie usa esta configuración para determinar si una palabra clave precede al texto que coincide con el patrón de expresiones regulares. La configuración define el número máximo de caracteres que puede existir entre el final de una palabra clave y el final del texto que coincide con el patrón de expresiones regulares. Si el texto coincide con el patrón de expresiones regulares, si aparece después de al menos una palabra clave completa y dentro de la distancia especificada de la palabra clave, Macie lo incluye en los resultados. De lo contrario, Macie la excluye de los resultados.

Puede especificar una distancia de 1 a 300 caracteres. La distancia por defecto es de 50 caracteres. Para obtener los mejores resultados, esta distancia debe ser mayor que el número mínimo de caracteres de texto que la expresión regular está diseñada para detectar. Si solo una parte del texto está dentro de la distancia máxima de coincidencia de una palabra clave, Macie no la incluye en los resultados.

Ignorar palabras

Son secuencias de caracteres que se excluyen de los resultados. Si el texto coincide con el patrón de regex, pero contiene una palabra ignorada, Macie no la incluye en los resultados.

Puede especificar hasta 10 palabras ignoradas. Cada palabra ignorada puede contener entre 4 y 90 caracteres UTF-8. Las palabras ignoradas distinguen mayúsculas de minúsculas.

Por ejemplo, muchas empresas tienen una sintaxis específica para las identificaciones de los empleados. Una de estas sintaxis podría ser: una letra mayúscula que indique si el empleado es empleado a tiempo completo (F) o a tiempo parcial (P), seguida de un guión (-) y una secuencia de ocho dígitos que identifica al empleado. Algunos ejemplos son: F-12345678, para un empleado a tiempo completo, y P-87654321, para un empleado a tiempo parcial.

Si crea un identificador de datos personalizado para detectar las identificaciones de los empleados que utilizan esta sintaxis, puede utilizar la siguiente expresión regular: `[A-Z]-\d{8}`. Para afinar el análisis y evitar los falsos positivos, también puedes configurar el identificador de datos personalizado para que utilice las palabras clave empleado e ID de empleado y una distancia máxima de coincidencia de 20 caracteres. Con estos criterios, los resultados incluyen texto que coincida con la expresión regular solo si el texto aparece después de la palabra clave empleado o identificador de empleado y todo el texto aparece dentro de los 20 caracteres de una de esas palabras clave.

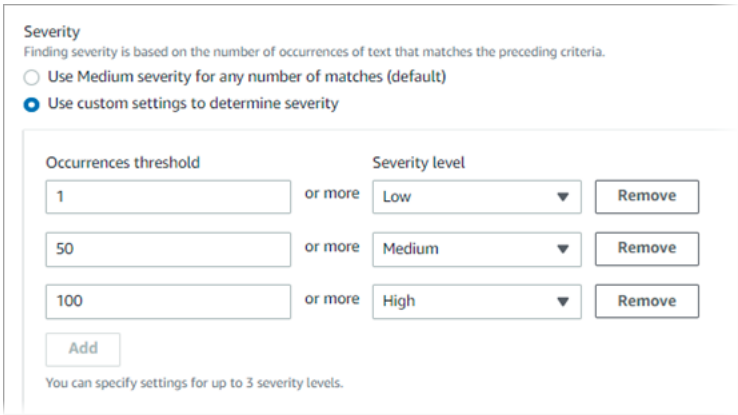
Para ver una demostración de cómo las palabras clave pueden ayudarle a encontrar datos confidenciales y evitar falsos positivos, vea el siguiente vídeo: Cómo Amazon Macie utiliza las palabras clave para descubrir datos confidenciales.

Definir la configuración de búsqueda del nivel de gravedad para los identificadores de los resultados

Al crear un identificador de datos personalizado, también puede definir una configuración de gravedad personalizada para los datos confidenciales que produzca el identificador. De forma predeterminada, Macie asigna la gravedad media a todos los resultados que produce un identificador de datos personalizado; si un objeto S3 contiene al menos una aparición de texto que coincide con los criterios de detección de un identificador de datos personalizado, Macie asigna automáticamente la gravedad media al resultado encontrado.

Con la configuración de gravedad personalizada, puede especificar qué gravedad desea asignar en función del número de apariciones de texto que coincidan con los criterios de detección del identificador de datos personalizado. Para ello, defina umbrales de incidencia para hasta tres niveles de gravedad: bajo (menos grave), medio y alto (más grave). Un umbral de ocurrencias es el número mínimo de coincidencias que deben existir en un objeto de S3 para producir un resultado con la gravedad especificada. Si especifica más de un umbral, los umbrales deben estar en orden ascendente según la gravedad, pasando de bajo a alto.

Por ejemplo, la imagen siguiente muestra la configuración de gravedad de un identificador de datos personalizado que especifica tres umbrales de incidencia, uno para cada nivel de gravedad compatible con Macie.



En la siguiente tabla se indica la gravedad de los resultados que produce el identificador de datos personalizado.

Umbral de aparición	Nivel de gravedad	Resultado
1	Baja	Si un objeto de S3 contiene entre 1 y 49 apariciones de texto que coinciden con los criterios de detección, la gravedad del resultado encontrado es baja.
50	Media	Si un objeto S3 contiene entre 50 y 99 apariciones de texto que coinciden con los criterios de detección, la gravedad del resultado encontrado es media.
100	Alta	Si un objeto S3 contiene 100 o más apariciones de texto que coinciden con los criterios de detección, la gravedad del resultado encontrado es alta.

También puede usar la configuración de gravedad para especificar si se debe crear o no un resultado. Si un objeto S3 contiene menos ocurrencias que el umbral más bajo, Macie no crea ningún resultado.

Creación de identificadores de datos personalizados

Siga estos pasos para crear un identificador de datos personalizado mediante la consola de Amazon Macie. Para crear un identificador de datos personalizado mediante programación, utilice la operación CreateCustomDataIdentifier de la API de Amazon Macie.

Para crear un identificador de datos personalizado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Configuración, elija Identificadores de datos personalizados.
3. Seleccione Crear.
4. En Nombre, introduzca un nombre único para el identificador de datos personalizado. El nombre puede contener hasta 128 caracteres.

   Evite incluir información confidencial en el nombre. Es posible que otros usuarios de su cuenta puedan ver el nombre, en función de las acciones que puedan llevar a cabo en Amazon Macie.
5. (Opcional) En Descripción, introduzca una breve descripción del identificador de datos personalizado. La descripción puede contener hasta 512 caracteres.

   Evite incluir información confidencial en la descripción. Es posible que otros usuarios de su cuenta puedan ver la descripción, en función de las acciones que puedan llevar a cabo en Macie.
6. En Expresión regular, introduzca la expresión regular (regex) que define el patrón de texto que debe coincidir. La expresión regular puede contener hasta 512 caracteres. Para obtener información sobre la sintaxis y las restricciones compatibles, consulte Compatibilidad de experiones regulares más adelante en esta sección.
7. (Opcional) En el caso de las palabras clave, introduzca hasta 50 secuencias de caracteres (separadas por comas) para definir un texto específico que debe estar cerca del texto que coincida con el patrón de expresiones regulares. Cada palabra clave puede contener entre 3 y 90 caracteres UTF-8. Las palabras clave no distinguen entre mayúsculas y minúsculas.

   Macie incluye una aparición en los resultados sólo si el texto coincide con el patrón de expresiones regulares y el texto se encuentra dentro de la distancia máxima de coincidencia de una de estas palabras clave, como se ha explicado en el tema anterior.

8. (Opcional) En Ignorar palabras, introduzca hasta 10 secuencias de caracteres (separadas por comas) que definan un texto específico para excluirlo de los resultados. Cada palabra ignorada puede contener entre 4 y 90 caracteres UTF-8. Las palabras ignoradas distinguen mayúsculas de minúsculas.

   Macie excluye una aparición de los resultados si el texto coincide con el patrón de expresiones regulares pero contiene una de estas palabras para omitir.
9. (Opcional) En Distancia de coincidencia máxima, introduzca el número máximo de caracteres que puede existir entre el final de una palabra clave y el final del texto que coincide con el patrón de regex. La distancia puede ser de 1 a 300 caracteres. La distancia por defecto es de 50 caracteres.

   Macie incluye una aparición en los resultados sólo si el texto coincide con el patrón de expresiones regulares y el texto se encuentra dentro de esta distancia de una palabra clave completa, como se ha explicado en el tema anterior.
10. En Gravedad, elija cómo quiere que Macie asigne la gravedad a los resultados de datos confidenciales que produzca el identificador de datos personalizado:

    - Para asignar automáticamente la gravedad media a todos los resultados, seleccione Utilizar una gravedad media para cualquier número de coincidencias (opción predeterminada). Con esta opción, Macie asigna automáticamente la gravedad media a un resultado si el objeto de S3 afectado contiene una o más apariciones de texto que coinciden con los criterios de detección.
    - Para asignar la gravedad en función de los umbrales de aparición que especifique, elija Usar una configuración personalizada para determinar la gravedad. A continuación, utilice las opciones Umbral de ocurrencias y Nivel de gravedad para especificar el número mínimo de coincidencias que deben existir en un objeto de S3 para obtener un resultado con la gravedad seleccionada.

      Por ejemplo, para asignar la gravedad alta a un resultado que muestre 100 o más apariciones de texto que coincidan con los criterios de detección, introdúzca **`100`** en el cuadro Umbral de ocurrencias y, a continuación, seleccione alta en la lista de niveles de gravedad.

      Puede especificar hasta tres umbrales de incidencia, uno para cada nivel de gravedad que admita Macie: bajo (para los menos graves), medio o alto (para los más graves). Si especifica más de uno, los umbrales deben estar en orden ascendente según la gravedad, pasando de bajo a alto. Si un objeto de S3 contiene menos apariciones que el umbral más bajo especificado, Macie no crea ningún resultado.

11. (Opcional) En el caso de las etiquetas, elija Añadir etiqueta y, a continuación, introduzca hasta 50 etiquetas para asignarlas al identificador de datos personalizado.

    Una Etiqueta es una etiqueta que se define y se asigna a determinados tipos de recursos de AWS. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

12. (Opcional) En Evaluar, introduzca hasta 1000 caracteres en el cuadro de Datos de muestra y, a continuación, elija Probar para probar los criterios de detección. Macie evalúa los datos de la muestra e informa del número de apariciones de texto que coinciden con los criterios. Puede repetir este paso tantas veces como desee para refinar y optimizar los criterios.

    > **Note**
    >
    > Le recomendamos encarecidamente que pruebe y ajuste los criterios de detección antes de guardar el identificador de datos personalizado. Dado que los identificadores de datos personalizados se utilizan en los trabajos de detección de información confidencial, no puede editar un identificador de datos personalizado después de guardarlo. Esto ayuda a garantizar que tiene un historial inmutable de resultados de datos confidenciales y resultados de detección para las auditorías o investigaciones de privacidad y protección de datos que lleve a cabo.

13. Cuando haya terminado, elija Enviar.

Macie comprueba la configuración y verifica que puede compilar la expresión regular. Si hay algún problema con alguna de las configuraciones o con la expresión regular, se produce un error que indica la naturaleza del problema. Una vez solucionados los problemas, puede guardar el identificador de datos personalizado.

Soporte de expresiones regulares en identificadores de datos personalizados

Macie admite un subconjunto de la sintaxis de patrones de expresiones regulares proporcionado por la biblioteca de expresiones regulares compatibles con Perl (PCRE). De las construcciones que proporciona la biblioteca PCRE, Macie no admite los siguientes elementos de patrón:

- Referencias inversas
- Capturar grupos
- Patrones condicionales
- Código incrustado
- Indicadores de patrones globales, como `/i`, `/m` y `/x`
- Patrones recursivos
- Afirmaciones positivas y negativas de ancho cero retrospectivas y prospectivas, como `?=`, `?!`, `?<=` y `?<!`

Para crear patrones de expresiones regulares efectivos para identificadores de datos personalizados, ten en cuenta también los siguientes consejos y recomendaciones:

- Anclajes: utilice anclajes (`^` o `$`) solo si espera que el patrón aparezca al principio o al final de un archivo, no al principio o al final de una línea.
- Repeticiones acotadas: por motivos de rendimiento, Macie limita el tamaño de los grupos de repeticiones acotadas. Por ejemplo, `\d{100,1000}` no se compilará en Macie. Para aproximarse a esta funcionalidad, puede utilizar una repetición abierta, como `\d{100,}`.
- Indistinción entre mayúsculas y minúsculas: para hacer que partes de un patrón no distingan mayúsculas de minúsculas, puede usar la construcción `(?i)` en lugar de la bandera `/i`.
- Rendimiento: no es necesario optimizar los prefijos o las alternancias manualmente. Por ejemplo, cambiar `/hello|hi|hey/` a `/h(?:ello|i|ey)/` no mejorará el rendimiento.
- Comodín: por motivos de rendimiento, Macie limita el número de comodines que se repiten. Por ejemplo, `a*b*a*` no se compilará en Macie.

Para protegerse de expresiones mal formadas o de larga duración, Macie comprueba automáticamente los patrones de expresiones regulares comparándolos con una colección de textos de muestra.

Definición de excepciones de datos confidenciales con las listas de permitidos de Amazon Macie

Con las listas de permitidos en Amazon Macie, puede definir texto específico y patrones de texto que desea que Macie ignore cuando inspeccione objetos de Amazon Simple Storage Service (Amazon

S3) en busca de datos confidenciales. Se trata normalmente de excepciones de datos confidenciales para sus escenarios o entornos particulares. Si los datos coinciden con un texto o un patrón de texto de una lista de permitidos, Macie no informa de ellos, aunque coincidan con los criterios de un identificador de datos administrados o un identificador de datos personalizados. Mediante el uso de listas de permitidos, puede refinar el análisis de los datos de Amazon S3 y reducir el ruido.

Puede crear y utilizar dos tipos de listas de permitidos en Macie:

- Texto predefinido: para este tipo de lista, se especifican determinadas secuencias de caracteres que deben ignorarse; por ejemplo, los nombres de los representantes públicos de su organización, números de teléfono concretos o datos de muestra específicos que su organización utiliza para realizar pruebas. Si usa este tipo de lista, Macie ignora el texto que coincida exactamente con una entrada de la lista.

  Este tipo de lista de permitidos es útil si desea especificar palabras, frases y otros tipos de secuencias de caracteres que no son confidenciales, no es probable que cambien y que no se adhieren necesariamente a un patrón común.
- Expresión regular: para este tipo de lista, se especifica una expresión regular (regex) que define un patrón de texto que se debe ignorar; por ejemplo, números de teléfono públicos de su organización, direcciones de correo electrónico del dominio de su organización o datos de muestra con patrones que su organización utiliza para realizar pruebas. Si utiliza este tipo de lista, Macie ignora el texto que coincide completamente con el patrón definido por la lista.

  Este tipo de lista de permitidos es útil si quiere especificar texto que no es confidencial pero que varía o es probable que cambie, al tiempo que se adhiere a un patrón común.

Después de crear una lista de permitidos, puede crear y configurar trabajos de detección de datos confidenciales para utilizarla, o añadirla a su configuración automática de detección de datos confidenciales. Macie utilizará la lista cuando analice los datos. Si Macie encuentra texto que coincide con una entrada o un patrón de una lista de permitidos, Macie no informa de esa aparición de texto en los hallazgos de datos confidenciales, estadísticas y otros tipos de resultados.

Puede crear y utilizar listas de permitidos en todos los Regiones de AWS en los que Macie está disponible actualmente, excepto en la región de Asia-Pacífico (Osaka).

Temas

- Requisitos y opciones de listas de permitidos en Amazon Macie
- Creación y administración de listas de permitidos en Amazon Macie

Requisitos y opciones de listas de permitidos en Amazon Macie

En Amazon Macie, puede utilizar listas de permitidos para especificar texto o patrones de texto que desea que Macie ignore cuando inspeccione objetos de Amazon Simple Storage Service (Amazon S3) en busca de datos confidenciales. Macie ofrece opciones para dos tipos de listas de permitidos, texto predefinido y expresiones regulares.

Una lista de texto predefinido es útil si desea que Macie ignore palabras, frases y otros tipos de secuencias de caracteres específicos que no considera confidenciales. Algunos ejemplos son los nombres de los representantes públicos de su organización, números de teléfono concretos o datos de muestra específicos que su organización utiliza para las pruebas. Si Macie encuentra texto que coincide con los criterios de un identificador de datos gestionado o personalizado y el texto también coincide con una entrada de una lista de permitidos, Macie no informa de esa aparición de texto en las búsquedas de datos confidenciales, las estadísticas y otros tipos de resultados.

Una expresión regular (regex) es útil si desea que Macie ignore el texto que varía o que es probable que cambie y que, al mismo tiempo, sigue un patrón común. La regex especifica un patrón de texto que debe ignorarse. Algunos ejemplos son los números de teléfono públicos de su organización, las direcciones de correo electrónico del dominio de su organización o los datos de muestra de patrones que su organización utiliza para realizar pruebas. Si Macie encuentra texto que coincide con los criterios de un identificador de datos gestionado o personalizado y el texto también coincide con un patrón de expresiones regulares en una lista de permitidos, Macie no informa de esa aparición de texto en las búsquedas de datos confidenciales, las estadísticas y otros tipos de resultados.

Puede crear y usar ambos tipos de listas de permitidos en todos los Regiones de AWS lugares en los que Macie esté disponible actualmente, excepto en la región de Asia Pacífico (Osaka). Cuando cree y gestione listas de permitidos, tenga en cuenta las siguientes opciones y requisitos. Tenga en cuenta también que las entradas de listas de permitidos y los patrones regex para direcciones de correo no son compatibles.

Temas

- Soporte y recomendaciones sobre la sintaxis
- Ejemplos

Opciones y requisitos para las listas de texto predefinidas

Para este tipo de lista de permitidos, se proporciona un archivo de texto plano delimitado por líneas que enumera las secuencias de caracteres específicas que se deben ignorar. Las entradas de la lista suelen ser palabras, frases y otros tipos de secuencias de caracteres que no se consideran confidenciales, que no es probable que cambien y que no se adhieren necesariamente a un patrón específico. Si utiliza este tipo de lista, Amazon Macie no informa de las apariciones de texto que coincidan exactamente con una entrada de la lista. Macie trata cada entrada de la lista como un valor literal de cadena.

Para utilizar este tipo de lista de permitidos, empiece por crear la lista en un editor de texto y guárdela como archivo de texto sin formato. A continuación, sube la lista a un depósito de uso general de S3. Asegúrese también de que la configuración de almacenamiento y cifrado del depósito y del objeto permita a Macie recuperar y descifrar la lista. A continuación, cree y configure los ajustes de la lista en Macie.

Después de configurar los ajustes en Macie, le recomendamos que pruebe la lista de permitidos con un conjunto de datos pequeño y representativo de su cuenta u organización. Para probar una lista, puede crear un trabajo único y configurarlo para que utilice la lista además de los identificadores de datos administrados y los identificadores de datos personalizados que suele utilizar para analizar los datos. A continuación, puede revisar los resultados del trabajo: resultados de datos confidenciales, resultados de detección de datos confidenciales o ambos. Si los resultados del trabajo difieren de lo que espera, puede cambiar y probar la lista hasta que los resultados sean los esperados.

Cuando termine de configurar y probar una lista de permitidos, puede crear y configurar trabajos adicionales para utilizarla, o añadirla a su configuración automática de detección de datos confidenciales de su cuenta. Cuando esos trabajos comienzan a ejecutarse o se inicia el siguiente ciclo de análisis de detección automatizado, Macie recupera la última versión de la lista de Amazon S3 y la almacena en la memoria temporal. Luego, Macie utiliza esta copia temporal de la lista cuando inspecciona los objetos de S3 en busca de datos confidenciales. Cuando finaliza la ejecución de un trabajo o el ciclo de análisis, Macie borra permanentemente de la memoria su copia de la lista. La lista no persiste en Macie. Solo persisten en Macie los ajustes de la lista.

> **Important**
>
> Dado que las listas de texto predefinido no persisten en Macie, es importante comprobar periódicamente el estado de las listas de permitidos. Si Macie no puede recuperar o analizar una lista para cuya utilización se ha configurado un trabajo o una detección automatizada, Macie no utilizará la lista. Esto podría provocar resultados inesperados, como resultados de datos confidenciales para el texto que especificó en la lista.

Temas

- Requisitos de sintaxis
- Requisitos de almacenamiento
- Requisitos de cifrado y descifrado
- Recomendaciones y consideraciones de diseño

Requisitos de sintaxis

Cuando cree este tipo de lista de permitidos, tenga en cuenta los siguientes requisitos para el archivo de la lista:

- La lista debe almacenarse como un archivo de texto plano (`text/plain`), como un archivo .txt, .text o .plain.
- La lista debe utilizar saltos de línea para separar las entradas individuales. Por ejemplo:

```
Akua Mansa
John Doe
Martha Rivera
425-555-0100
425-555-0101
425-555-0102
```

  Macie trata cada línea como una entrada única y distinta de la lista. El archivo también puede contener líneas en blanco para mejorar la legibilidad. Macie omite las líneas en blanco cuando analiza el archivo.
- Cada entrada puede contener entre 1 y 90 caracteres UTF-8.
- Cada entrada debe ser una coincidencia completa y exacta para que el texto sea ignorado. Macie no admite el uso de caracteres comodín ni valores parciales para las entradas. Macie trata cada

entrada como un valor literal de cadena. Las coincidencias no distinguen entre mayúsculas y minúsculas.

- El archivo puede contener entre 1 y 100 000 entradas.
- El tamaño total del archivo no puede superar los 35 MB.

Requisitos de almacenamiento

A medida que añada y administre listas de permitidos en Amazon S3, tenga en cuenta los siguientes requisitos y recomendaciones de almacenamiento:

- Soporte regional: la lista de personas permitidas debe almacenarse en un depósito que se encuentre en el mismo Región de AWS lugar que tu cuenta de Macie. Macie no puede acceder a una lista de permitidos si está almacenada en otra región.
- Propiedad de un grupo: una lista de personas permitidas debe almacenarse en un grupo que sea de tu Cuenta de AWS propiedad. Si desea que otras cuentas utilicen la misma lista de permitidos, considere la posibilidad de crear una regla de replicación de Amazon S3 para replicar la lista en los buckets propiedad de esas cuentas. Para obtener información acerca de cómo replicar objetos de S3, consulte Replicación de objetos en la Guía del usuario de Amazon Simple Storage Service.

  Además, tu identidad AWS Identity and Access Management (IAM) debe tener acceso de lectura al depósito y al objeto que almacenan la lista. De lo contrario, no podrá crear o actualizar la configuración de la lista ni comprobar su estado mediante Macie.
- Tipos y clases de almacenamiento: una lista de objetos permitidos debe almacenarse en un depósito de uso general, no en un depósito de directorios. Además, debe almacenarse con una de las siguientes clases de almacenamiento: redundancia reducida (RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Standard o S3 Standard-IA.
- Políticas de bucket: si guardas una lista de permitidos en un bucket que tiene una política de bucket restrictiva, asegúrate de que la política permita a Macie recuperar la lista. Para ello, puede añadir una condición para la función vinculada al servicio de Macie a la política de bucket. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

  Asegúrese también de que la política permita que su identidad de IAM tenga acceso de lectura al bucket. De lo contrario, no podrá crear o actualizar la configuración de la lista ni comprobar su estado mediante Macie.

- Rutas de objetos: si almacena más de una lista de permitidos en Amazon S3, la ruta de objetos de cada lista debe ser única. En otras palabras, cada lista de permitidos debe almacenarse por separado como su propio objeto de S3.
- Control de versiones: cuando añada una lista de permitidos a un bucket, le recomendamos que también active el control de versiones del bucket. A continuación, puede utilizar los valores de fecha y hora para correlacionar las versiones de la lista con los resultados de los trabajos de detección de datos confidenciales y los ciclos automatizados de detección de datos confidenciales que utilizan la lista. Esto puede ayudarle en las auditorías o investigaciones sobre protección y privacidad de datos que realice.
- Bloqueo de objetos: para evitar que una lista de objetos permitidos se elimine o sobrescriba durante un período de tiempo determinado o indefinidamente, puedes habilitar el bloqueo de objetos para el depósito que almacena la lista. Activar esta opción no impide que Macie acceda a la lista. Para obtener información sobre este ajuste, consulte Usar Bloqueo de objetos de S3 en la Guía del usuario de Amazon Simple Storage Service.

Requisitos de cifrado y descifrado

Si cifra una lista de permitidos en Amazon S3, la política de permisos de la función vinculada al servicio de Macie suele conceder a Macie los permisos que necesita para descifrar la lista. Sin embargo, esto depende del tipo de cifrado utilizado:

- Si una lista se cifra mediante el cifrado del lado del servidor con una clave gestionada por Amazon S3 (SSE-S3), Macie puede descifrar la lista. La función vinculada al servicio para su cuenta de Macie concede a Macie los permisos que necesita.
- Si una lista se cifra mediante un cifrado del lado del servidor con un cifrado AWS gestionado AWS KMS key (DSSE-KMS o SSE-KMS), Macie puede descifrar la lista. La función vinculada al servicio para su cuenta de Macie concede a Macie los permisos que necesita.
- Si una lista se cifra mediante un cifrado del lado del servidor gestionado por el cliente AWS KMS key (DSSE-KMS o SSE-KMS), Macie solo podrá descifrar la lista si usted permite que Macie utilice la clave. Para obtener información sobre como hacer esto, consulte Permitir a Macie utilizar un sistema gestionado por clientes AWS KMS key.

> **Note**
>
> Puede cifrar una lista con un cliente gestionado en un almacén de claves externo. AWS KMS key Sin embargo, es posible que la clave sea más lenta y menos fiable que una clave que se gestione íntegramente dentro de AWS KMS. Si la latencia o un problema de

disponibilidad impiden a Macie descifrar la lista, Macie no utiliza la lista cuando analiza objetos de S3. Esto podría provocar resultados inesperados, como resultados de datos confidenciales para el texto que especificó en la lista. Para reducir este riesgo, considere la posibilidad de almacenar la lista en un bucket de S3 que esté configurado para utilizar la clave como clave de bucket de S3.
Para obtener información sobre el uso de claves de KMS en almacenes de claves externos, consulte Almacenes de claves externos en la AWS Key Management Service Guía para desarrolladores. Para obtener más información sobre el uso de claves de Bucket de S3, consulte Reducción del costo de SSE-KMS con las claves de bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

- Si una lista está cifrada mediante cifrado del lado del servidor con una clave proporcionada por el cliente (SSE-C) o cifrado del cliente, Macie no puede descifrar la lista. Considere utilizar en su lugar el cifrado SSE-S3, DSSE-KMS o SSE-KMS.

Si una lista está cifrada con una clave KMS AWS administrada o una clave KMS administrada por el cliente, su identidad AWS Identity and Access Management (IAM) también debe poder usar la clave. De lo contrario, no podrá crear o actualizar la configuración de la lista ni comprobar su estado mediante Macie. Para saber cómo comprobar o cambiar los permisos de una clave KMS, consulte Políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

Para obtener información detallada sobre las opciones de cifrado de los datos de Amazon S3, consulte Protección de datos con cifrado en la Guía del usuario de Amazon Simple Storage Service.

Recomendaciones y consideraciones de diseño

En general, Macie trata cada entrada de una lista de permitidos como un valor literal de cadena. Es decir, Macie ignora cada aparición de texto que coincida exactamente con una entrada completa de una lista de permitidos. Las coincidencias no distinguen entre mayúsculas y minúsculas.

Sin embargo, Macie utiliza las entradas como parte de un marco más amplio de extracción y análisis de datos. El marco incluye funciones de machine learning y concordancia de patrones que tienen en cuenta dimensiones como las variaciones gramaticales y sintácticas y, en muchos casos, la proximidad de palabras clave. El marco también determina el tipo de archivo o el formato de almacenamiento de un objeto de S3. Por lo tanto, tenga en cuenta las siguientes consideraciones y recomendaciones a la hora de añadir y gestionar las entradas de una lista de permitidos.

Prepárese para diferentes tipos de archivos y formatos de almacenamiento

En el caso de los datos no estructurados, como el texto de un archivo en formato de documento portátil de Adobe (.pdf), Macie ignora el texto que coincide exactamente con una entrada completa de una lista de permitidos, incluido el texto que abarca varias líneas o páginas.

En el caso de los datos estructurados, como los datos en columnas de un archivo CSV o los datos basados en registros de un archivo JSON, Macie ignora el texto que coincide exactamente con una entrada completa de una lista de permitidos si todo el texto está almacenado en un único campo, celda o matriz. Este requisito no se aplica a los datos estructurados almacenados en un archivo no estructurado, como una tabla en un archivo .pdf.

Por ejemplo, considere el siguiente contenido en un archivo CSV:

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

Si `Akua Mansa` y `John Doe` son entradas de una lista de permitidos, Macie ignora esos nombres en el archivo CSV. El texto completo de cada entrada de la lista se guarda en un único campo `Name`.

Por el contrario, considere un archivo CSV que contenga las siguientes columnas y campos:

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

Si `Akua Mansa` y `John Doe` son entradas de una lista de permitidos, Macie no ignora esos nombres en el archivo CSV. Ninguno de los campos del archivo CSV contiene el texto completo de una entrada de la lista de permitidos.

Incluya las variantes más comunes

Añada entradas para variaciones comunes de datos numéricos, nombres propios, términos y secuencias de caracteres alfanuméricos. Por ejemplo, si añade nombres o frases que contengan solo un espacio entre palabras, añada también variaciones que incluyan dos espacios entre palabras. Del mismo modo, añada palabras y frases que contengan y no contengan caracteres especiales, y considere la posibilidad de incluir variaciones sintácticas y semánticas comunes.

Para el número de teléfono estadounidense 425-555-0100, por ejemplo, podría añadir estas entradas a una lista de permitidos:

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

Para la fecha del 1 de febrero de 2022, en un contexto multinacional, podría añadir entradas que incluyan variaciones sintácticas comunes para el inglés y el francés, incluidas las variaciones que incluyen y no incluyen caracteres especiales:

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

Para los nombres de personas, incluya entradas para las distintas formas de un nombre que no considere confidenciales. Por ejemplo, incluya: el nombre seguido del apellido; el apellido seguido del nombre, el nombre y el apellido separados por un espacio; el nombre y el apellido separados por dos espacios; y apodos.

Para el nombre Martha Rivera, por ejemplo, podría añadir:

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

Si desea ignorar variaciones de un nombre específico que contiene muchas partes, cree una lista de permitidos que utilice una expresión regular en su lugar. Por ejemplo, para el nombre Dra. Martha Lyda Rivera, PhD, podría utilizar la siguiente expresión regular: `^(Dr. )?Martha \s(Lyda|L\.)?\s?Rivera,?( PhD)?$`.

Opciones y requisitos de las expresiones regulares en las listas de permitidos

Para este tipo de lista, se especifica una expresión regular (regex) que define un patrón de texto que se debe ignorar; por ejemplo, números de teléfono públicos de su organización, direcciones de correo electrónico del dominio de su organización o datos de muestra con patrones que su organización utiliza para realizar pruebas. La regex define un patrón común para un tipo específico de datos que usted no considera confidenciales. Si usa este tipo de lista de permitidos, Amazon Macie no informa de los resultados de texto que coincidan exactamente con el patrón especificado. A diferencia de una lista de permitidos que especifica el texto predefinido que debe ignorarse, usted crea y almacena la expresión regular y el resto de la configuración de la lista en Macie.

Al crear o actualizar este tipo de lista de permitidos, puede probar la expresión regular de la lista con datos de muestra antes de guardarla. Le recomendamos que lo haga con varios conjuntos de datos de muestra. Si crea una expresión regular demasiado general, Macie podría ignorar las apariciones de texto que considere confidenciales. Si la expresión regular es demasiado específica, Macie podría ignorar las apariciones de texto que no considere confidenciales. Para protegerse contra expresiones malformadas o de larga duración, Macie también compila y comprueba automáticamente la expresión regular contra una colección de texto de muestra, y le notifica los problemas que debe resolver.

Para realizar pruebas adicionales, le recomendamos que también pruebe la expresión regular de la lista con un conjunto de datos pequeño y representativo de su cuenta u organización. Para ello, puede crear un trabajo único y configurarlo para que utilice la lista además de los identificadores de datos administrados y los identificadores de datos personalizados que suele utilizar para analizar los datos. A continuación, puede revisar los resultados del trabajo: resultados de datos confidenciales, resultados de detección de datos confidenciales o ambos. Si los resultados del trabajo difieren de lo que espera, puede cambiar y probar la expresión regular hasta que los resultados sean los esperados.

Cuando configure y pruebe una lista de permitidos, puede crear y configurar trabajos adicionales para utilizarla, o añadirla a su configuración automática de detección de datos confidenciales de su cuenta. Cuando se ejecutan esos trabajos o Macie realiza una detección automática para tu cuenta, Macie utiliza la última versión de la expresión regular de la lista para analizar los datos.

Temas

- Soporte y recomendaciones sobre la sintaxis
- Ejemplos

Soporte y recomendaciones sobre la sintaxis

Una lista de permitidos puede especificar una expresión regular (regex) que contenga hasta 512 caracteres. Macie admite un subconjunto de la sintaxis de patrones de expresiones regulares proporcionado por la biblioteca de expresiones regulares compatibles con Perl (PCRE). De las construcciones que proporciona la biblioteca PCRE, Macie no admite los siguientes elementos de patrón:

- Referencias inversas
- Capturar grupos
- Patrones condicionales
- Código incrustado
- Indicadores de patrones globales, como `/i`, `/m` y `/x`
- Patrones recursivos
- Afirmaciones positivas y negativas de ancho cero retrospectivas y prospectivas, como `?=`, `?!`, `?<=` y `?<!`

Para crear patrones de expresiones regulares eficaces para las listas de permitidos, tenga en cuenta también los siguientes consejos y recomendaciones:

- Anclajes: utilice anclajes (`^` o `$`) solo si espera que el patrón aparezca al principio o al final de un archivo, no al principio o al final de una línea.
- Repeticiones acotadas: por motivos de rendimiento, Macie limita el tamaño de los grupos de repeticiones acotadas. Por ejemplo, `\d{100,1000}` no se compilará en Macie. Para aproximarse a esta funcionalidad, puede utilizar una repetición abierta, como `\d{100,}`.
- Indistinción entre mayúsculas y minúsculas: para hacer que partes de un patrón no distingan mayúsculas de minúsculas, puede usar el constructo `(?i)` en lugar de la bandera `/i`.
- Rendimiento: no es necesario optimizar los prefijos o las alternancias manualmente. Por ejemplo, cambiar `/hello|hi|hey/` a `/h(?:ello|i|ey)/` no mejorará el rendimiento.
- Comodín: por motivos de rendimiento, Macie limita el número de comodines que se repiten. Por ejemplo, `a*b*a*` no se compilará en Macie.
- Alternancia: para especificar más de un patrón en una única lista de permitidos, puede utilizar el operador de alternancia (`|`) para concatenar los patrones. Si lo hace, Macie utiliza la lógica OR para combinar los patrones y formar uno nuevo. Por ejemplo, si especifica `(apple|orange)`, Macie reconoce tanto manzana como naranja como coincidencia e ignora las apariciones de

ambas palabras. Si concatena patrones, asegúrese de limitar la longitud total de la expresión concatenada a 512 caracteres o menos.

Por último, cuando desarrolle la expresión regular, diséñela para que se adapte a distintos tipos de archivos y formatos de almacenamiento. Macie utiliza la regex como parte de un marco más amplio de extracción y análisis de datos. El marco determina el tipo de archivo o el formato de almacenamiento de un objeto de S3. En el caso de los datos estructurados, como los datos en columnas de un archivo CSV o los datos basados en registros de un archivo JSON, Macie ignora el texto que coincide completamente con el patrón solo si todo el texto está almacenado en un único campo, celda o matriz. Este requisito no se aplica a los datos estructurados almacenados en un archivo no estructurado, como una tabla en un archivo Adobe Portable Document Format (.pdf). En el caso de los datos no estructurados, como el texto de un archivo .pdf, Macie ignora el texto que coincide completamente con el patrón, incluido el texto que abarca varias líneas o páginas.

Ejemplos

Los siguientes ejemplos muestran patrones de expresiones regulares válidos para algunos escenarios comunes.

Direcciones de correo electrónico

Si utiliza un identificador de datos personalizados para detectar direcciones de correo electrónico, puede ignorar las direcciones de correo electrónico que no considere confidenciales, como las direcciones de correo electrónico de su organización.

Para ignorar las direcciones de correo electrónico de un determinado dominio de segundo y primer nivel, puede utilizar este patrón:

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

Donde *example* es el nombre del dominio de segundo nivel y *com* es el dominio de primer nivel. En este caso, Macie hace coincidir e ignora direcciones como johndoe@example.com y john.doe@example.com.

Para ignorar las direcciones de correo electrónico de un dominio concreto en cualquier dominio de nivel superior genérico (gTLD), como .com o .gov, puede utilizar este patrón:

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

Donde *example* es el nombre del dominio. En este caso, Macie hace coincidir e ignora direcciones como johndoe@example.com, john.doe@example.gov y johndoe@example.edu.

Para ignorar las direcciones de correo electrónico de un dominio concreto en cualquier dominio de nivel superior de código de país (gTLD), como .com o .gov, puede utilizar este patrón:

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

Donde *example* es el nombre del dominio y *ca* y *au* son ccTLD específicos que hay que ignorar. En este caso, Macie hace coincidir e ignora direcciones como johndoe@example.ca y john.doe@example.au.

Para ignorar las direcciones de correo electrónico que corresponden a un dominio y gTLD concretos e incluir dominios de tercer y cuarto nivel, puede utilizar este patrón:

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

Donde *example* es el nombre del dominio y *com* es el gTLD. En este caso, Macie hace coincidir e ignora direcciones como johndoe@www.example.com y john.doe@www.team.example.com.

Números de teléfono

Macie proporciona identificadores de datos administrados que pueden detectar números de teléfono de varios países y regiones. Para ignorar determinados números de teléfono, como los números gratuitos o los números de teléfono públicos de su organización, puede utilizar patrones como los siguientes.

Para ignorar los números de teléfono estadounidenses gratuitos que utilizan el prefijo 800 y tienen el formato (800) ###-####:

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

Para ignorar los números de teléfono estadounidenses gratuitos que utilizan el prefijo 888 y tienen el formato (888) ###-####:

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

Para ignorar los números de teléfono franceses de 10 dígitos que incluyen el prefijo 33 y tienen el formato +33 ## ## ## ## ##:

```
^\+33 \d( \d\d){4}$
```

Para ignorar los números de teléfono de EE. UU. y Canadá que utilizan determinados prefijos y códigos de área, no incluyen prefijo de país y tienen el formato (###) ###-####:

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

Donde *123* es el prefijo y *555* es el código de centralita.

Para ignorar los números de teléfono de EE. UU. y Canadá que utilizan determinados prefijos y códigos de área, incluyen prefijo de país y tienen el formato +1 (###) ###-####:

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

Donde *123* es el prefijo y *555* es el código de centralita.

Creación y administración de listas de permitidos en Amazon Macie

En Amazon Macie, una lista de permitidos define un texto específico o un patrón de texto que debe ignorar Macie al inspeccionar objetos de Amazon Simple Storage Service (Amazon S3) en busca de datos confidenciales. Si los datos coinciden con una entrada o un patrón en una lista de permitidos, Macie no informa los datos en resultados de datos confidenciales, estadísticas u otros tipos de resultados, incluso si el texto coincide con los criterios de un identificador de datos administrado o un identificador de datos personalizado.

Puede crear y administrar los siguientes tipos de listas de permitidos en Macie.

Texto predefinido

Use este tipo de lista para especificar palabras, frases y otros tipos de secuencias de caracteres específicas que no son confidenciales, no es probable que cambien y que no se adhieren a un patrón común necesariamente. Algunos ejemplos son los nombres de los representantes públicos de su organización, números de teléfono específicos y datos de muestra específicos que su organización utiliza para las pruebas. Si usa este tipo de lista, Macie ignora el texto que coincida exactamente con una entrada de la lista.

Para este tipo de lista, se crea un archivo de texto sin formato delimitado por líneas en el que se muestra el texto específico que se debe ignorar. A continuación, se ignora el archivo en un bucket de S3 y configura los ajustes para que Macie acceda a la lista del bucket. A continuación, puede crear y configurar trabajos de detección de datos confidenciales para usar la lista o añadir la lista a la configuración automática de detección de datos confidenciales de su cuenta. Cuando cada trabajo comienza a ejecutarse o se inicia el siguiente ciclo de análisis de detección automatizado, Macie recupera la última versión de la lista de Amazon S3. Luego, Macie usa esa versión de la lista cuando inspecciona los objetos de S3 en busca de datos confidenciales. Si Macie encuentra

texto que coincida exactamente con una entrada de la lista, Macie no informa de la aparición del texto como datos confidenciales.

Expresión regular

Use este tipo de lista para especificar una expresión regular (regex) que defina el patrón de texto que se va a ignorar. Algunos ejemplos son los números de teléfono públicos de su organización, las direcciones de correo electrónico del dominio de su organización y los datos de muestra modelados que su organización utiliza para las pruebas. Si usa este tipo de lista, Macie ignora el texto que coincide completamente con el patrón de expresión regular definido por la lista.

Para este tipo de lista, debe crear una expresión regular que defina un patrón común para el texto que no es confidencial, pero que varía o es probable que cambie. A diferencia de una lista de texto predefinido, se crea y almacena la expresión regular y el resto de la configuración de la lista en Macie. A continuación, puede crear y configurar trabajos de detección de datos confidenciales para usar la lista o añadir la lista a la configuración automática de detección de datos confidenciales de su cuenta. Cuando se ejecutan esos trabajos o Macie realiza una detección automática para tu cuenta, Macie utiliza la última versión de la expresión regular de la lista para analizar los datos. Si Macie encuentra texto que coincida exactamente con el patrón definido por la lista, Macie no informa de la aparición del texto como datos confidenciales.

Para ver los requisitos detallados, las recomendaciones y los ejemplos de cada tipo de lista, consulte Requisitos y opciones de listas de permitidos. Puede crear hasta 10 listas de permisos para su cuenta en cada una de las admitidas Región de AWS, hasta cinco listas de permisos que especifiquen texto predefinido y hasta cinco listas de permisos que especifiquen expresiones regulares. Puede crear y utilizar listas de personas permitidas en todos los Regiones de AWS lugares en los que Macie esté disponible actualmente, excepto en la región de Asia Pacífico (Osaka).

Para crear y gestionar listas de permitidos, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. En los siguientes temas se explica cómo hacerlo. En el caso de la API, los temas incluyen ejemplos de cómo realizar estas tareas mediante la AWS Command Line Interface (AWS CLI). También puede realizar estas tareas utilizando una versión actual de otra herramienta de línea de AWS comandos o un AWS SDK, o enviando las solicitudes HTTPS directamente a Macie. Para obtener información sobre AWS las herramientas y los SDK, consulte Herramientas sobre las que construir. AWS

Temas

- Crear listas de permitidos

- Comprobación del estado de las listas de permitidos
- Cambiar las listas de permitidos
- Eliminar listas de permitidos

Crear listas de permitidos

La forma de crear una lista de permitidos en Amazon Macie depende del tipo de lista que desee crear. Una lista de permitidos puede ser un archivo que incluye texto predefinido para ignorarlo, o puede ser una expresión regular (regex) que define un patrón de texto que se debe ignorar. Elija la sección para el tipo de lista que desea crear.

Texto predefinido

Antes de crear este tipo de lista de permitidos en Macie, siga estos pasos:

1. Con un editor de texto, cree un archivo de texto sin formato delimitado por líneas que enumere el texto específico que desee ignorar, por ejemplo, un archivo .txt, .text o .plain. Para obtener más información, consulte Requisitos de sintaxis para las listas de texto predefinidas.
2. Cargue el archivo en un depósito de uso general de S3 y anote el nombre del depósito y del objeto. Deberá introducir estos nombres cuando haga los ajustes en Macie.
3. Asegúrese de que la configuración del bucket y el objeto de S3 les permita a Macie y a usted recuperar la lista del bucket. Para obtener más información, consulte Requisitos de almacenamiento para las listas de texto predefinido.
4. Si cifró el objeto de S3, asegúrese de que también esté cifrado con una clave que pueda usted y Macie puedan usar. Para obtener más información, consulte Requisitos de cifrado y descifrado para listas de texto predefinido.

Tras realizar estos pasos, estará listo para hacer los ajustes de la lista en Macie. Puede hacer los ajustes mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

Para hacer los ajustes para una lista de permitidos mediante la consola de Amazon Macie, siga los pasos siguientes.

Para hacer los ajustes de la lista de permitidos en Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. En el panel de navegación, en Configuración, seleccione Listas de permitidos.
3. En la página Listas de permitidos, seleccione Crear.
4. En Seleccione un tipo de lista, elija Texto predefinido.
5. En Configuración de lista, utilice las siguientes opciones para introducir ajustes adicionales para la lista de permitidos:

   - En Nombre, ingrese el nombre de la lista. El nombre puede contener hasta 128 caracteres.
   - En Descripción, escriba una breve descripción de la lista. La descripción puede contener hasta 512 caracteres.
   - Para el nombre del depósito de S3, introduzca el nombre del depósito que almacena la lista.

     En Amazon S3, puede encontrar este valor en el campo Nombre de las propiedades del bucket. Este valor distingue entre mayúsculas y minúsculas. Además, no utilice caracteres comodín ni valores parciales al ingresar el nombre.
   - Para el nombre del objeto de S3, introduzca el nombre del objeto de S3 que almacena la lista.

     En Amazon S3, puede encontrar este valor en el campo Clave de las propiedades del objeto. Si el nombre contiene una ruta, asegúrese de incluir la ruta completa al introducir el nombre, por ejemplo **`allowlists/macie/mylist.txt`**. Este valor distingue entre mayúsculas y minúsculas. Además, no utilice caracteres comodín ni valores parciales al ingresar el nombre.
6. (Opcional) En Etiquetas, seleccione Añadir etiqueta y, a continuación, introduzca hasta 50 etiquetas para asignarlas a la lista de permitidos.

   Una etiqueta es una etiqueta que se define y se asigna a determinados tipos de AWS recursos. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.
7. Cuando haya terminado, elija Create (Crear).

Macie comprueba la configuración de la lista. Macie también comprueba que puede recuperar la lista de Amazon S3 y analizar su contenido. Si se ha producido un error, Macie muestra un mensaje que describe el error. Para obtener información detallada que puede ayudarle a

solucionar el error, consulte Opciones y requisitos para las listas de texto predefinidas. Tras corregir los errores, puede guardar la configuración de la lista.

API

Para configurar los ajustes de la lista de permitidos mediante programación, utilice el CreateAllowListfuncionamiento de la API Amazon Macie y especifique los valores adecuados para los parámetros necesarios.

Para el parámetro `criteria`, utilice un objeto `s3WordsList` para especificar el nombre del bucket de S3 (`bucketName`) y el nombre del objeto de S3 (`objectKey`) que almacena la lista. Para determinar el nombre del bucket, consulte el campo `Name` de Amazon S3. Para determinar el nombre del objeto, consulte el campo `Key` de Amazon S3. Tenga en cuenta que estos valores distinguen entre mayúsculas y minúsculas. Además, no utilice caracteres comodín ni valores parciales cuando especifique estos nombres.

Para configurar los ajustes mediante el AWS CLI, ejecute el create-allow-listcomando y especifique los valores adecuados para los parámetros necesarios. Los siguientes ejemplos muestran cómo configurar los ajustes de una lista de permitidos que se almacena en un bucket de S3 denominado *DOC-EXAMPLE-BUCKET*. El nombre del objeto S3 que almacena la lista es *allowlists/macie/mylist.txt*.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de continuación de línea de barra invertida (\) para mejorar la legibilidad.

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

Al enviar la solicitud, Macie comprueba la configuración de la lista. Macie también comprueba que puede recuperar la lista de Amazon S3 y analizar su contenido. Si se produce un error, su solicitud fallará y Macie devolverá un mensaje que describe el error. Para obtener información detallada que puede ayudarle a solucionar el error, consulte Opciones y requisitos para las listas de texto predefinidas.

Si Macie puede recuperar y analizar la lista, la solicitud se realizará correctamente y verá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
}
```

Dónde `arn` es el nombre de recurso de Amazon (ARN) de la lista de permitidos que se creó y `id` es el identificador único de la lista.

Una vez guardada la configuración de la lista, puede crear y configurar trabajos de detección de datos confidenciales para utilizarla, o bien añadir la lista a su configuración automática de detección de datos confidenciales. Cada vez que esos trabajos comienzan a ejecutarse o se inicia un ciclo de análisis de descubrimiento automatizado, Macie recupera la última versión de la lista de Amazon S3. Luego, Macie usa esa versión de la lista cuando analiza los datos.

Expresión regular

Cuando crea una lista de permitidos que especifica una expresión regular (regex), define la expresión regular y todos los demás ajustes de la lista directamente en Macie. Macie admite un subconjunto de la sintaxis de patrones de expresiones regulares proporcionado por la biblioteca de expresiones regulares compatibles con Perl (PCRE). Para obtener más información, consulte Soporte y recomendaciones sobre la sintaxis.

Puede crear este tipo de lista mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para crear una lista de permitidos mediante la consola de Amazon Macie.

Para crear una lista de permitidos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Configuración, seleccione Listas de permitidos.
3. En la página Listas de permitidos, seleccione Crear.
4. En Seleccione un tipo de lista, elija Expresión regular.
5. En Configuración de lista, utilice las siguientes opciones para introducir ajustes adicionales para la lista de permitidos:
   - En Nombre, ingrese el nombre de la lista. El nombre puede contener hasta 128 caracteres.
   - En Descripción, escriba una breve descripción de la lista. La descripción puede contener hasta 512 caracteres.
   - Para la Expresión regular, ingrese la expresión regular que define el patrón de texto que se debe omitir. La expresión regular puede contener hasta 512 caracteres.
6. (Opcional) Para Evaluar, introduzca hasta 1000 caracteres en el cuadro Datos de muestra y, a continuación, elija Probar para comprobar la expresión regular. Macie evalúa los datos de muestra e informa del número de apariciones del texto que coincide con la expresión regular. Puede repetir este paso tantas veces como desee para refinar y optimizar la expresión regular.

   > **Note**
   >
   > Le recomendamos que pruebe y refine la expresión regular con varios conjuntos de datos de muestra. Si crea una expresión regular demasiado general, Macie podría ignorar las apariciones de texto que considere confidenciales. Si la expresión regular es demasiado específica, Macie podría ignorar las apariciones de texto que no considere confidenciales.

7. (Opcional) En Etiquetas, seleccione Añadir etiqueta y, a continuación, introduzca hasta 50 etiquetas para asignarlas a la lista de permitidos.

   Una etiqueta es una etiqueta que se define y se asigna a determinados tipos de AWS recursos. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

8. Cuando haya terminado, elija Create (Crear).

Macie comprueba la configuración de la lista. Macie también prueba la expresión regular para comprobar que puede compilar la expresión. Si se ha producido un error, Macie muestra un mensaje que describe el error. Para obtener información detallada que puede ayudarle a solucionar el error, consulte Opciones y requisitos de las expresiones regulares en las listas de permitidos. Tras corregir los errores, puede guardar la lista de permitidos.

API

Antes de crear este tipo de lista de permitidos en Macie, le recomendamos que pruebe y refine la expresión regular con varios conjuntos de datos de muestra. Si crea una expresión regular demasiado general, Macie podría ignorar las apariciones de texto que considere confidenciales. Si la expresión regular es demasiado específica, Macie podría ignorar las apariciones de texto que no considere confidenciales.

Para probar una expresión con Macie, puede utilizar la TestCustomDataIdentifieroperación de la API de Amazon Macie o, para ello, ejecutar AWS CLItest-custom-data-identifierel comando. Macie usa el mismo código subyacente para compilar expresiones con el fin de permitir listas e identificadores de datos personalizados. Si prueba una expresión de este modo, asegúrese de especificar valores únicamente para los parámetros `regex` y `sampleText`. De lo contrario, verá resultados inexactos.

Cuando esté listo para crear este tipo de lista de permitidos, utilice la CreateAllowListoperación de la API de Amazon Macie y especifique los valores adecuados para los parámetros necesarios. Para el parámetro `criteria`, utilice el campo `regex` para especificar la expresión regular que define el patrón de texto que se debe omitir. La expresión puede contener hasta 512 caracteres.

Para crear este tipo de lista mediante el AWS CLI, ejecute el create-allow-listcomando y especifique los valores adecuados para los parámetros necesarios. En los siguientes ejemplos se crea una lista de permitidos denominada *`my_allow_list`*. La expresión regular está diseñada para ignorar todas las direcciones de correo electrónico que un identificador de datos personalizado podría detectar para el dominio `example.com`.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de continuación de línea de barra invertida (\) para mejorar la legibilidad.

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
```

```
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

Al enviar la solicitud, Macie comprueba la configuración de la lista. Macie también prueba la expresión regular para comprobar que puede compilar la expresión. Si se produce un error, la solicitud fallará y Macie devolverá un mensaje que describe el error. Para obtener información detallada que puede ayudarle a solucionar el error, consulte Opciones y requisitos de las expresiones regulares en las listas de permitidos.

Si Macie puede compilar la expresión, la solicitud se realizará correctamente y verá un resultado similar al siguiente:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Dónde `arn` es el nombre de recurso de Amazon (ARN) de la lista de permitidos que se creó y `id` es el identificador único de la lista.

Tras guardar la lista, puede crear y configurar trabajos de detección de datos confidenciales para utilizarla o añadirla a su configuración automática de detección de datos confidenciales. Cuando se ejecutan esos trabajos o Macie realiza una detección automática para tu cuenta, Macie utiliza la última versión de la expresión regular de la lista para analizar los datos.

Comprobación del estado de las listas de permitidos

Es importante comprobar el estado de las listas de permitidos de forma periódica. De lo contrario, los errores podrían provocar que Amazon Macie produzca resultados de análisis inesperados, como resultados de datos confidenciales para el texto que especificó en una lista de permitidos.

Si configura un trabajo de detección de datos confidenciales para que utilice una lista de permitidos y Macie no puede acceder a la lista o utilizarla cuando el trabajo comience a ejecutarse, el trabajo seguirá ejecutándose. Sin embargo, Macie no usa la lista cuando analiza los objetos de S3. Del mismo modo, si se inicia un ciclo de análisis para la detección automática de datos confidenciales y Macie no puede acceder a una lista de permitidos específica ni utilizarla, el análisis continúa pero Macie no lo utiliza.

Es poco probable que se produzcan errores en una lista de permitidos que especifique una expresión regular (regex). Esto se debe en parte a que Macie prueba automáticamente la expresión regular al crear o actualizar la configuración de la lista. Además, debe almacenar la expresión regular y el resto de la configuración de la lista en Macie.

Sin embargo, pueden producirse errores en una lista de permitidos que especifica texto predefinido, en parte porque se guarda la lista en Amazon S3 en lugar de en Macie. Las causas comunes de errores son:

- Se elimina el bucket o el objeto de S3.
- Se cambia el nombre del bucket u objeto de S3 y la configuración de la lista en Macie no especifica el nuevo nombre.
- Se cambia la configuración de permisos del bucket de S3 y Macie pierde el acceso al bucket y al objeto.
- La configuración de cifrado del bucket de S3 ha cambiado y Macie no puede descifrar el objeto que almacena la lista.
- Se cambia la política de la clave de cifrado y Macie pierde el acceso a la clave. Macie no puede descifrar el objeto S3 que almacena la lista.

> **Important**
>
> Dado que estos errores afectan a los resultados de sus análisis, le recomendamos que compruebe periódicamente el estado de las listas de personas permitidas. Le recomendamos que también lo haga si cambia los permisos o la configuración de cifrado de un bucket de S3 que almacena una lista de permitidos, o si cambia la política de una clave AWS Key Management Service (AWS KMS) que se utiliza para cifrar una lista.

Puede revisar el estado de sus listas de permitidos mediante la consola de Amazon Macie o la API de Amazon Macie. Para obtener información detallada que puede ayudarle a solucionar errores que sucedan, consulte Opciones y requisitos para las listas de texto predefinidas.

Console

Siga estos pasos para revisar el estado de sus listas de permitidos mediante la consola de Amazon Macie.

Para revisar el estado de sus listas de permitidos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Configuración, seleccione Listas de permitidos.
3. En la página Listas de permitidos, seleccione actualizar ().
   Macie comprueba la configuración de todas las listas de permitidos y actualiza el campo Estado para indicar el estado actual de cada lista.

   Si una lista especifica una expresión regular, su estado suele ser Correcto. Esto significa que Macie puede compilar la expresión. Si una lista especifica texto predefinido, su estado puede ser alguno de los siguientes valores.

   OK (Correcto)

   Macie puede recuperar y analizar el contenido de la lista.

   Acceso denegado

   A Macie no se le permite acceder al objeto S3 que almacena la lista. Amazon S3 denegó la solicitud para recuperar el objeto. Una lista también puede tener este estado si el objeto está cifrado con un cliente gestionado por un cliente AWS KMS key que Macie no puede utilizar.

   Para tratar este error, revise la política de bucket y otra configuración de permisos para el bucket y el objeto. Asegúrese de que Macie pueda acceder al objeto y recuperarlo. Si el objeto está cifrado con una clave AWS KMS gestionada por un cliente, revise también la política de claves y asegúrese de que Macie pueda usar la clave.

Error

Se produjo un error transitorio o interno cuando Macie intentó recuperar o analizar el contenido de la lista. Una lista de permitidos también puede tener este estado si está cifrada con un cifrado al que Amazon S3 y Macie no pueden acceder ni usar.

Para solucionar este error, espere unos minutos y, a continuación, seleccione actualizar () de nuevo. Si el estado sigue siendo Error, compruebe la configuración de cifrado del objeto de S3. Asegúrese de que el objeto esté cifrado con una clave a la que Amazon S3 y Macie puedan acceder y usar.

El objeto está vacío

Macie puede recuperar la lista de Amazon S3, pero la lista no tiene ningún contenido.

Para solucionar este error, descargue el objeto de Amazon S3 y asegúrese de que contiene las entradas correctas. Si las entradas son correctas, revise la configuración de la lista en Macie. Asegúrese de que los nombres de los buckets y objetos especificados sean correctos.

No se ha encontrado el objeto

La lista no existe en Amazon S3.

Para solucionar este error, revise la configuración de la lista en Macie. Asegúrese de que los nombres de los buckets y objetos especificados sean correctos.

Cuota excedida

Macie puede acceder a la lista en Amazon S3. Sin embargo, el número de entradas de la lista o el tamaño de almacenamiento de la lista superan la cuota de una lista de permitidos.

Para solucionar este error, divida la lista en varios archivos. Asegúrese de que cada archivo contenga menos de 100 000 entradas. Asegúrese también de que el tamaño de cada archivo sea inferior a 35 MB. A continuación, cargue cada archivo en Amazon S3. Al terminar, ha los ajustes de la lista de permitidos en Macie para cada archivo. Puede tener hasta cinco listas de texto predefinido en cada Región de AWS compatible.

Solicitudes restringidas

Amazon S3 limitó la solicitud para recuperar la lista.

Para solucionar este error, espere unos minutos y, a continuación, seleccione actualizar () de nuevo.

Acceso de usuario denegado

Amazon S3 denegó la solicitud para recuperar el objeto. Si el objeto especificado existe, no puedes acceder a él o está cifrado con una AWS KMS clave que no puedes usar.

Para solucionar este error, póngase en contacto con el AWS administrador para asegurarse de que la configuración de la lista especifique los nombres correctos del depósito y del objeto y de que tenga acceso de lectura al depósito y al objeto. Si el objeto está cifrado, asegúrese de que también esté cifrado con una clave que pueda usar.

4. Para revisar la configuración y el estado de una lista específica, elija el nombre de la lista.

API

Para comprobar el estado de una lista de permitidos mediante programación, utilice la GetAllowListoperación de la API de Amazon Macie o, para ello, ejecute AWS CLI el comando. get-allow-list

Para el parámetro `id`, especifique el identificador único de la lista de permitidos cuyo estado desea comprobar. Para obtener este identificador, puede usar la operación. ListAllowLists La operación ListAllowLists recupera información sobre todas las listas de permitidos de la cuenta. Si utiliza el AWS CLI, puede ejecutar el list-allow-listscomando para recuperar esta información.

Al enviar una solicitud GetAllowList, Macie comprueba todos los ajustes de la lista de permitidos. Si la configuración especifica una expresión regular (regex), Macie comprueba que puede compilar la expresión. Si la configuración especifica una lista de texto predefinido, Macie comprueba que puede recuperar y analizar la lista.

A continuación, Macie devuelve un objeto `GetAllowListResponse` que proporciona los detalles de la lista de permitidos. En el objeto `GetAllowListResponse`, el objeto `status` indica el estado actual de la lista: un código de estado (`code`) y, según el código de estado, una breve descripción del estado de la lista (`description`).

Si la lista de permitidos especifica una expresión regular, el código de estado suele ser 0K y no hay una descripción asociada. Esto significa que Macie compiló la expresión con éxito.

Si la lista de permitidos especifica un texto predefinido, el código de estado varía en función de los resultados de la prueba:

- Si Macie recuperó y analizó la lista correctamente, el código de estado es 0K y no hay ninguna descripción asociada.
- Si un error ha impedido a Macie recuperar o analizar la lista, el código de estado y la descripción indican la naturaleza del error que se ha producido.

Para obtener una lista de los posibles códigos de estado y una descripción de cada uno de ellos, consulte la AllowListStatusreferencia de la API de Amazon Macie.

Cambiar las listas de permitidos

Después de crear una lista de permitidos, puede cambiar la mayoría de los ajustes de la lista en Amazon Macie. Por ejemplo, puede cambiar el nombre y la descripción de la lista, y puede añadir y editar las etiquetas de la lista. La única configuración que no puede cambiar es el tipo de lista. Por ejemplo, si una lista de permitidos existente especifica una expresión regular, no puede cambiar su tipo a texto predefinido.

Si una lista de permitidos especifica texto predefinido, también puede cambiar las entradas de la lista. Para ello, actualice el archivo que contiene las entradas y, a continuación, cargue la nueva versión del archivo en Amazon S3. La próxima vez que Macie se prepare para usar la lista, recuperará la última versión del archivo de Amazon S3. Cuando cargue el nuevo archivo, asegúrese de guardarlo en el mismo bucket y objeto de S3. O bien, si cambia el nombre del bucket o del objeto, asegúrse de actualizar la configuración de la lista en Macie.

Puede cambiar la configuración de una lista de permitidios mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

Para cambiar la configuración de una lista de permitidos mediante la consola de Amazon Macie, siga los pasos siguientes.

Para cambiar una lista de permitidos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Configuración, seleccione Listas de permitidos.
3. En la página Listas de permitidos, elija el nombre de la lista de permitidos que desea cambiar. Se abre la página de listas de permitidos y muestra la configuración actual de la lista.
4. Para asignar o editar las etiquetas de la lista de permitidos, en la sección Etiquetas, elija Administrar etiquetas. A continuación, cambie las etiquetas según sea necesario. Cuando termine, elija Save (Guardar).
5. Para cambiar otros ajustes de la lista de permitidos, seleccione Editar en la sección Ajustes de la lista. A continuación, cambie la configuración como desee:

   - Nombre: ingrese un nombre nuevo para la lista. El nombre puede contener hasta 128 caracteres.
   - Descripción: introduzca una nueva descripción de la lista. La descripción puede contener hasta 512 caracteres.
   - Si la lista de permitidos especifica un texto predefinido:
     - Nombre del bucket de S3: introduzca el nombre del bucket que actualmente almacena la lista.

       En Amazon S3, puede encontrar este valor en el campo Nombre de las propiedades del bucket. Este valor distingue entre mayúsculas y minúsculas. Además, no utilice caracteres comodín ni valores parciales al ingresar el nombre.
     - Nombre del objeto S3: introduzca el nombre del objeto S3 que actualmente almacena la lista.

       En Amazon S3, puede encontrar este valor en el campo Clave de las propiedades del objeto. Si el nombre contiene una ruta, asegúrese de incluir la ruta completa al introducir el nombre, por ejemplo **`allowlists/macie/mylist.txt`**. Este valor distingue entre mayúsculas y minúsculas. Además, no utilice caracteres comodín ni valores parciales al ingresar el nombre.
   - Si la lista de permitidos especifica una expresión regular (regex), introduzca una nueva expresión regular en el cuadro Expresión regular. La expresión regular puede contener hasta 512 caracteres.

Después de introducir la nueva expresión regular, si lo desea, pruébela. Para ello, introduzca hasta 1000 caracteres en el cuadro Datos de muestra y, a continuación, seleccione Probar. Macie evalúa los datos de muestra e informa del número de apariciones del texto que coincide con la expresión regular. Puede repetir este paso tantas veces como desee para refinar y optimizar la expresión regular antes de guardar los cambios.

Cuando termine con los cambios a la configuración, elija Guardar.

Macie comprueba la configuración de la lista. Para una lista de texto predefinido, Macie también comprueba que puede recuperar la lista de Amazon S3 y analizar su contenido. Para una expresión regular, Macie también verifica que puede compilar la expresión. Si se ha producido un error, Macie muestra un mensaje que describe el error. Para obtener información detallada que puede ayudarle a solucionar el error, consulte Requisitos y opciones de listas de permitidos. Después de corregir los errores, puede guardar los cambios.

API

Para cambiar una lista de permitidos mediante programación, utilice la UpdateAllowListoperación de la API de Amazon Macie o, para ello, ejecute AWS CLI el comando. update-allow-list En su solicitud, utilice los parámetros admitidos con el fin de especificar un nuevo valor para cada configuración que desee cambiar. Tenga en cuenta que los parámetros `criteria`, `id` y `name` son obligatorios. Si no desea cambiar el valor de un parámetro obligatorio, especifique el valor actual del parámetro.

Por ejemplo, el siguiente comando cambia el nombre y la descripción de una lista de permitidos existente. El ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

Donde:

- *km2d4y22hp6rv05example* es el identificador único de la lista.
- *my_allow_list-email es el* nuevo nombre de la lista.

- *`[a-z]@example.com`* es el criterio de la lista, una expresión regular.
- *`Omite todas las direcciones de correo electrónico del dominio example.com`*, es la nueva descripción de la lista.

Al enviar la solicitud, Macie comprueba la configuración de la lista. Si la lista especifica texto predefinido, esto incluye verificar que Macie puede recuperar la lista de Amazon S3 y analizar su contenido. Si la lista especifica una expresión regular, esto incluye comprobar que Macie puede compilar la expresión.

Si se produce un error cuando Macie prueba la configuración, su solicitud fallará y Macie devolverá un mensaje que describe el error. Para obtener información detallada que puede ayudarle a solucionar el error, consulte Requisitos y opciones de listas de permitidos. Si la solicitud falla por otro motivo, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Si su solicitud tiene éxito, Macie actualiza la configuración de la lista y recibirá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Dónde `arn` es el nombre de recurso de Amazon (ARN) de la lista de permitidos que se actualizó y `id` es el identificador único de la lista.

Eliminar listas de permitidos

Al eliminar una lista de permitidos en Amazon Macie, se eliminan permanentemente todas las configuraciones de la lista. Estas configuraciones no se pueden recuperar después de eliminarlas. Si la configuración especifica una lista de texto predefinido que almacena en Amazon S3, Macie no elimina el objeto S3 que almacena la lista. Solo se eliminan las configuracines de Macie.

Si configura los trabajos de detección de datos confidenciales para que utilicen una lista de permitidos y, posteriormente, elimina la lista, los trabajos se ejecutarán según lo programado. Sin embargo, los resultados de su trabajo, tanto los resultados de datos confidenciales como los resultados de la detección de datos confidenciales, pueden incluir texto que especificó previamente

en una lista de permitidos. Del mismo modo, si configura la detección automática de datos confidenciales para utilizar una lista y, posteriormente, la elimina, continuarán los ciclos de análisis diarios. Sin embargo, los resultados de datos confidenciales, las estadísticas u otros tipos de resultados pueden incluir texto que especificó previamente en una lista de permitidos.

Antes de eliminar una lista de permitidos, le recomendamos que revise su inventario de tareas para identificar los trabajos que utilizan la lista y que están programados para ejecutarse en el futuro. En el inventario, el panel de detalles indica si un trabajo está configurado para usar alguna lista de permitidos y, de ser así, cuáles. Además, compruebe la configuración de detección automática de datos confidenciales. Puede que decida que es mejor cambiar una lista en lugar de eliminarla.

Como medida de seguridad adicional, Macie comprueba la configuración de todos sus trabajos cuando intenta eliminar una lista de permitidos. Si ha configurado trabajos para usar la lista y alguno de esos trabajos tiene un estado distinto de Completado o Cancelado, Macie no eliminará la lista a menos que usted proporcione una confirmación adicional.

Puede eliminar una lista de permitidos mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para eliminar una regla de filtrado mediante la consola de Amazon Macie.

Para eliminar una lista de permitidos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Configuración, seleccione Listas de permitidos.
3. En la página Listas de permitidos, seleccione la casilla de la lista de permitidos que desea eliminar.
4. En el menú Actions (Acciones), elija Delete (Eliminar).
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Delete (Eliminar).

API

Para eliminar una lista de permitidos mediante programación, utilice la DeleteAllowListoperación de la API Amazon Macie. Para el parámetro `id`, especifique el identificador único de la lista de permitidos que desee eliminar. Puede obtener este identificador mediante la operación. ListAllowLists La operación ListAllowLists recupera información sobre todas las listas de

permitidos de la cuenta. Si utiliza el AWS CLI, puede ejecutar el list-allow-listscomando para recuperar esta información.

Para el parámetro `ignoreJobChecks`, especifique si desea forzar la eliminación de la lista, incluso si los trabajos de detección de datos confidenciales están configurados para usar la lista:

- Si especifica `false`, Macie comprobará la configuración de todos los trabajos que tengan un estado distinto de `COMPLETE` o `CANCELLED`. Si ninguno de esos trabajos está configurado para usar la lista, Macie lo borra permanentemente. Si alguno de esos trabajos está configurado para usar la lista, Macie rechazará su solicitud y devolverá un error HTTP 400 (`ValidationException`). El mensaje de error indica el número de trabajos aplicables para un máximo de 200 trabajos.
- Si especifica `true`, Macie eliminará la lista de forma permanente sin comprobar la configuración de ninguno de sus trabajos.

Para eliminar una lista de permitidos mediante el AWS CLI, ejecute el delete-allow-listcomando. Por ejemplo:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

Donde *nkr81bmtu2542yyexample* es el identificador único de la lista de permitidos que se pueden eliminar.

Si la solicitud se realiza correctamente, Macie devuelve una respuesta HTTP 200 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Si la lista de permitidos especificaba un texto predefinido, si lo desea, puede eliminar el objeto de S3 que almacena la lista. Sin embargo, conservar este objeto puede ayudar a garantizar que tiene un historial inmutable de resultados de datos confidenciales y resultados de detección para las auditorías o investigaciones de privacidad y protección de datos.

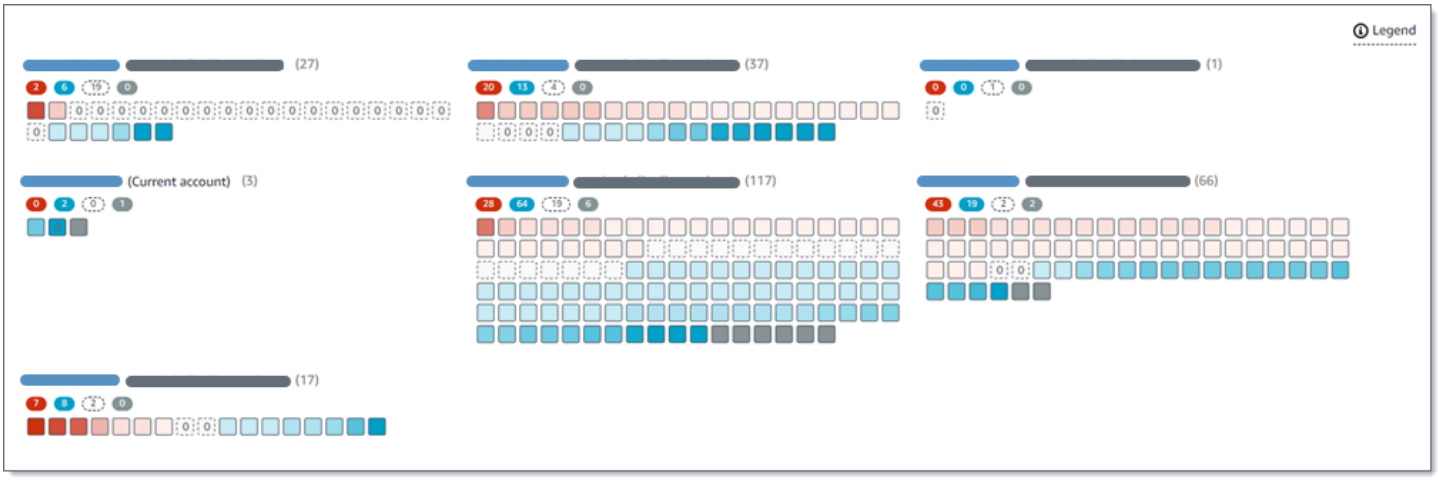
Realización de la detección automatizada de datos confidenciales con Amazon Macie

Para obtener una amplia visibilidad de dónde pueden residir los datos confidenciales en su patrimonio de datos de Amazon Simple Storage Service (Amazon S3), configure Amazon Macie para que realice la detección automática de datos confidenciales para su cuenta u organización. Gracias a la detección automática de datos confidenciales, Macie evalúa continuamente su inventario de buckets de S3 y utiliza técnicas de muestreo para identificar y seleccionar los objetos de S3 representativos de sus buckets. A continuación, Macie recupera y analiza los objetos seleccionados, inspeccionándolos en busca de datos confidenciales.

De forma predeterminada, Macie analiza los objetos de S3 mediante el conjunto de identificadores de datos administrados que recomendamos para la detección automatizada de datos confidenciales. Puede personalizar los análisis configurando Macie para que utilice determinados identificadores de datos administrados, identificadores de datos personalizados y listas de permitidos cuando realice la detección automatizada de datos confidenciales para su cuenta u organización. Además, Macie selecciona y analiza automáticamente los objetos de todos sus cubos S3 de uso general. Si eres el administrador de Macie de una organización, esto incluye los objetos de los depósitos que son propiedad de tus cuentas de miembros. Puede ajustar el alcance de los análisis excluyendo grupos específicos, por ejemplo, los grupos que suelen almacenar datos de registro. AWS

A medida que el análisis avanza día a día, Macie genera registros de los datos confidenciales que encuentra y de los análisis que realiza: los hallazgos de datos confidenciales, que registran los datos confidenciales que Macie encuentra en objetos S3 individuales, y los resultados de descubrimiento de datos confidenciales, que registran detalles sobre el análisis de objetos S3 individuales. Macie también actualiza las estadísticas, los datos de inventario y demás información que proporcione sobre sus datos de Amazon S3.

Por ejemplo, un mapa térmico interactivo de la consola ofrece una representación visual de la confidencialidad de datos de todo su patrimonio de datos:



Estas características están diseñadas para ayudarlo a evaluar la confidencialidad de los datos en todo su patrimonio de datos de Amazon S3 y a profundizar para investigar y evaluar cuentas, depósitos y objetos individuales. También pueden ayudarlo a determinar dónde realizar un análisis más profundo e inmediato mediante la ejecución de trabajos de detección de datos confidenciales. Junto con la información que Macie proporciona sobre la seguridad y la privacidad de sus datos de Amazon S3, también puede usar estas características para identificar los casos en los que podría ser necesaria una solución inmediata, por ejemplo, un bucket de acceso público en el que Macie encontró datos confidenciales.

Para configurar y utilizar la detección automatizada de datos confidenciales, su cuenta debe ser una cuenta de Macie independiente o la cuenta de administrador de Macie de una organización.

Temas

- Cómo funciona la detección automatizada de datos confidenciales
- Configuración de la detección de datos confidenciales automatizada para su cuenta
- Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales
- Evaluación de cobertura de detección de datos confidenciales automatizada
- Revisión de las estadísticas y los resultados de la detección automatizada de datos confidenciales
- Puntuación de confidencialidad para buckets de S3
- Configuración predeterminada para la detección automatizada de datos confidenciales

Cómo funciona la detección automatizada de datos confidenciales

Cuando habilita Amazon Macie para su cuenta Cuenta de AWS, Macie crea un rol vinculado al servicio AWS Identity and Access Management (IAM) para su cuenta en la cuenta actual. Región de

AWS La política de permisos de este rol permite a Macie llamar a otros recursos Servicios de AWS y supervisarlos en su nombre. AWS Al utilizar esta función, Macie genera y mantiene un inventario completo de los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) en la región. El inventario incluye información sobre cada uno de sus depósitos de S3 y los objetos incluidos en ellos. Si eres el administrador de Macie de una organización, el inventario incluye información sobre los depósitos que son propiedad de las cuentas de tus miembros. Para obtener más información, consulte Administración de varias cuentas .

Si está habilitada la detección automatizada de datos confidenciales en su cuenta de Macie, Macie evalúa los datos del inventario a diario para identificar los objetos de S3 que son aptos para la detección automatizada. Como parte de la evaluación, Macie también selecciona una muestra de objetos representativos para analizarlos. A continuación, Macie recupera y analiza la versión más reciente de cada objeto seleccionado de Amazon S3 e inspecciona cada objeto en busca de datos confidenciales.

A medida que el análisis avanza cada día, Macie actualiza las estadísticas, los datos de inventario y otra información que proporciona sobre sus datos de Amazon S3. Macie también genera registros de los datos confidenciales que encuentra y de los análisis que realiza. Los datos resultantes proporcionan información sobre dónde Macie encontró datos confidenciales en su patrimonio de datos de Amazon S3, abarcando todos los depósitos de uso general de S3 que Macie monitorea y analiza para su cuenta. Los datos pueden ayudarlo a evaluar la seguridad y la privacidad de sus datos, determinar dónde realizar una investigación más profunda e identificar los casos en los que es necesario remediarlos.

Para ver una breve demostración de cómo funciona la detección automatizada de datos confidenciales, vea el siguiente vídeo: Descripción general de la detección automatizada de datos de Amazon Macie.

Para configurar y utilizar la detección automatizada de datos confidenciales, su cuenta debe ser una cuenta de Macie independiente o la cuenta de administrador de Macie de una organización.

Temas

- Componentes principales
- Consideraciones

Componentes principales

Amazon Macie utiliza una combinación de características y técnicas para realizar la detección automatizada de datos confidenciales para sus datos de Amazon S3. Estos funcionan junto con las características y técnicas que Macie utiliza para ayudarlo a monitorear sus datos de Amazon S3 con fines de seguridad y control de acceso.

Selección de objetos de S3 para analizarlos

A diario, Macie evalúa los datos de inventario de Amazon S3 para identificar los objetos de S3 que pueden analizarse mediante la detección automatizada de datos confidenciales. Si es el administrador de Macie de una organización, esto incluye los datos de inventario de los buckets de S3 que sean propiedad de sus cuentas de miembros.

Como parte de la evaluación, Macie utiliza técnicas de muestreo para seleccionar objetos S3 representativos para analizarlos. Las técnicas definen grupos de objetos que tienen metadatos similares y es probable que tengan un contenido similar. Los grupos se basan en dimensiones como el nombre del bucket, el prefijo, la clase de almacenamiento, la extensión del nombre del archivo y la fecha de la última modificación. A continuación, Macie selecciona un conjunto representativo de muestras de cada grupo, recupera la última versión de cada objeto seleccionado de Amazon S3 y analiza cada objeto seleccionado para determinar si el objeto contiene datos confidenciales. Cuando se completa el análisis, Macie descarta su copia del objeto.

La estrategia de muestreo prioriza los análisis distribuidos. En general, utiliza un enfoque centrado en la amplitud de datos de Amazon S3. Cada día, se selecciona un conjunto representativo de objetos de S3 de entre tantos grupos de uso general como sea posible en función del tamaño total de almacenamiento de todos los objetos clasificables de su patrimonio de datos de Amazon S3. Por ejemplo, si Macie ya ha analizado y encontrado datos confidenciales en los objetos de un depósito y aún no ha analizado los objetos de otro depósito, este último grupo tiene mayor prioridad en el análisis. Con este enfoque, obtendrá una visión amplia de la confidencialidad de sus datos S3 de Amazon con mayor rapidez. Según el tamaño de su patrimonio de datos, los resultados del análisis pueden empezar a aparecer en un plazo de 48 horas a partir de la activación de la detección automatizada de datos confidenciales para su cuenta.

La estrategia de muestreo también prioriza el análisis de distintos tipos de objetos de S3 y de objetos que se hayan creado o modificado recientemente. No se garantiza que ninguna muestra de un solo objeto sea concluyente. Por lo tanto, el análisis de un conjunto diverso de objetos

puede proporcionar una mejor visión de los tipos y la cantidad de datos confidenciales que puede contener un bucket de S3. Además, la priorización de los objetos nuevos o modificados recientemente ayuda a que el análisis se adapte a los cambios en el inventario de buckets. Por ejemplo, si los objetos se crean o modifican después de un análisis anterior, esos objetos tienen mayor prioridad para los análisis posteriores. Por el contrario, si un objeto se analizó previamente y no ha cambiado desde ese análisis, Macie no vuelve a analizarlo. Este enfoque le ayuda a establecer las líneas base de confidencialidad para los buckets S3 individuales. Luego, a medida que avanzan los análisis continuos e incrementales de su cuenta, las evaluaciones de confidencialidad de los grupos individuales pueden ser cada vez más profundas y detalladas a un ritmo predecible.

Definir el alcance de los análisis

De forma predeterminada, Macie incluye todos los depósitos de uso general de S3 que supervisa y analiza para su cuenta cuando evalúa los datos de inventario y selecciona los objetos de S3 para analizarlos. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro.

Puede excluir grupos de S3 específicos de los análisis. Por ejemplo, es posible que prefiera excluir los depósitos que suelen almacenar datos de AWS registro, como los registros de eventos. AWS CloudTrail Para excluir un bucket, puede cambiar la configuración de detección automatizada de datos confidenciales de su cuenta o del bucket. Si lo hace, Macie comenzará a excluir el bucket cuando comience el siguiente ciclo diario de evaluación y análisis. Puede excluir hasta 1000 buckets de los análisis.

Si excluyes un bucket de S3, puedes volver a incluirlo posteriormente. Para ello, vuelva a cambiar la configuración de detección automatizada de datos confidenciales de su cuenta o del bucket. Luego, Macie comienza a incluir el bucket cuando comienza el siguiente ciclo diario de evaluación y análisis.

Determinar qué tipos de datos confidenciales detectar e informar

De forma predeterminada, Macie inspecciona los objetos de S3 mediante el conjunto de identificadores de datos gestionados que recomendamos para la detección automatizada de datos confidenciales. Para obtener una lista de identificadores, consulte Configuración predeterminada para la detección automatizada de datos confidenciales.

Puede personalizar los análisis para que se centren en tipos específicos de datos confidenciales. Para ello, cambie la configuración de detección automatizada de datos confidenciales de su cuenta de cualquiera de estas formas:

- Añadir o eliminar un identificador de datos administrados. Un identificador de datos administrados es un conjunto basado en técnicas y criterios que están diseñados para detectar un tipo específico de datos confidenciales, como números de tarjetas de crédito, claves de acceso secretas de AWS o números de pasaporte de un país o región en particular. Para obtener más información, consulte Uso de identificadores de datos administrados.
- Añadir o eliminar posteriormente un identificador de datos personalizado. Un identificador de datos personalizado es un conjunto de criterios personalizados que se definen para detectar información confidencial. Con los identificadores de datos personalizados, puede detectar datos confidenciales que reflejen escenarios particulares de la organización, propiedad intelectual o datos de propietario, como identificaciones de empleados, números de cuenta de clientes o clasificaciones de datos internos. Para obtener más información, consulte Creación de identificadores de datos personalizados.
- Añadir o eliminar posteriormente listas de permitidos: En Macie, una lista de permisos especifiquen el texto y los patrones de texto que deben ignorarse en los objetos de S3, normalmente excepciones a los datos confidenciales en sus escenarios o entornos específicos, por ejemplo, nombres públicos o números de teléfono de su organización, o datos de muestra que su organización utiliza para realizar pruebas. Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

Si cambia la configuración, Macie aplicará los cambios cuando comience el siguiente ciclo de análisis diario.

También puede ajustar la configuración a nivel de bucket para determinar si se incluyen tipos específicos de datos confidenciales en las evaluaciones de la confidencialidad de un bucket. Para saber cómo hacerlo, consulte Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales.

Calcular las puntuaciones de confidencialidad

De forma predeterminada, Macie calcula automáticamente una puntuación de sensibilidad para cada segmento de uso general de S3 que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro.

En Macie, una puntuación de confidencialidad es una medida cuantitativa de la intersección de dos dimensiones principales: la cantidad de datos confidenciales que Macie ha encontrado en un bucket y la cantidad de datos que Macie ha analizado en un bucket. La puntuación de confidencialidad de un bucket determina qué etiqueta de confidencialidad asigna Macie al bucket. Una etiqueta de confidencialidad es una representación cualitativa de la puntuación

de confidencialidad de un bucket, por ejemplo, Confidencial No confidencial y Aún no se ha analizado. Para obtener más información sobre el rango de puntuaciones y etiquetas de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.

> **Important**
>
> La puntuación de confidencialidad y la etiqueta de un bucket de S3 no implican ni indican de otro modo la criticidad o importancia que el bucket o los objetos del bucket puedan tener para su organización. Por el contrario, su objetivo es proporcionar puntos de referencia que puedan ayudarlo a identificar y monitorear los posibles riesgos de seguridad.

Cuando habilita inicialmente la detección automatizada de datos confidenciales en su cuenta, Macie asigna automáticamente una puntuación de confidencialidad de 50 y la etiqueta Aún no se ha analizado a cada bucket de S3. La excepción son los buckets vacíos. Un depósito vacío es un depósito que no almacena ningún objeto o que todos los objetos del depósito contienen cero (0) bytes de datos. Si este es el caso de un bucket, Macie le asigna una puntuación de 1 y le asigna la etiqueta No confidencial.

A medida que avanza la detección automatizada de su cuenta, Macie actualiza las puntuaciones de confidencialidad y las etiquetas para reflejar los resultados de los análisis. Por ejemplo:

- Si Macie no encuentra datos confidenciales en un objeto, reduce la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto, aumenta la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto que se ha modificado posteriormente, elimina las detecciones de datos confidenciales del objeto de la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto y los elimina posteriormente, elimina las detecciones de datos confidenciales del objeto de la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.

Puede ajustar la configuración de la puntuación de confidencialidad de cada segmento S3 incluyendo o excluyendo tipos específicos de datos confidenciales de la puntuación de un

segmento. Puede anular la puntuación calculada de un bucket y asignar manualmente la puntuación máxima (100) al bucket. Si asigna la puntuación máxima, la casilla se etiquetará como Confidencial. Para obtener más información, consulte Gestión de la detección automatizada de buckets de S3 individuales.

Generar metadatos, estadísticas y resultados

Si su cuenta tiene habilitada la detección automática de datos confidenciales, Macie generará y conservará automáticamente datos de inventario adicionales, estadísticas y otra información sobre los depósitos de uso general de S3 que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro.

La información adicional recoge los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para su cuenta. También complementa otra información que Macie proporciona sobre sus datos de Amazon S3, como la configuración de acceso público y acceso compartido para buckets individuales. La información adicional incluye lo siguiente:

- Estadísticas agregadas de confidencialidad de los datos, como el número total de grupos en los que Macie ha encontrado datos confidenciales y cuántos de esos grupos son de acceso público.
- Una representación visual e interactiva de la confidencialidad de los datos en todo su patrimonio de datos de Amazon S3.
- Detalles a nivel de bucket que indican el estado actual de los análisis, como una lista de los objetos que Macie ha analizado en un bucket, los tipos de datos confidenciales que Macie ha encontrado en un bucket y el número de apariciones de cada tipo de datos confidenciales que ha encontrado Macie.

Para obtener más información, consulte Revisión de las estadísticas y los resultados de la detección automatizada de datos confidenciales.

La información adicional también incluye estadísticas y detalles que pueden ayudarle a evaluar y supervisar la cobertura de sus datos de Amazon S3. Puede comprobar el estado de los análisis de su patrimonio de datos en general y de los buckets de S3 individuales de su inventario de buckets. También puede identificar los problemas que impidieron que Macie analizara objetos en buckets específicos. Si soluciona los problemas, puede aumentar la cobertura de sus datos de Amazon S3 durante los ciclos de análisis posteriores. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatizada.

Macie recalcula y actualiza automáticamente esta información mientras detecta automáticamente los datos confidenciales de su cuenta. Por ejemplo, si Macie encuentra datos confidenciales en un objeto que posteriormente se modifican o eliminan, Macie actualiza los metadatos del bucket correspondiente: elimina el objeto de la lista de objetos analizados; elimina las apariciones de datos confidenciales que Macie encontró en el objeto; recalcula la puntuación de confidencialidad, si la puntuación se calcula automáticamente; y actualiza la etiqueta de confidencialidad según sea necesario para reflejar la nueva puntuación.

Además de los metadatos y las estadísticas, Macie produce registros de los datos confidenciales que encuentra y los análisis que realiza: hallazgos de datos confidenciales, que informan de los datos confidenciales que Macie encuentra en objetos S3 individuales, y resultados de descubrimiento de datos confidenciales, que registran detalles sobre el análisis de objetos S3 individuales.

Consideraciones

Al utilizar Amazon Macie para realizar la detección automatizada de datos confidenciales para sus datos de Amazon S3, tenga en cuenta lo siguiente:

- Su configuración de detección automática solo se aplica a los datos actuales. Región de AWS En consecuencia, los análisis y los datos resultantes se aplican únicamente a los depósitos y objetos de uso general de S3 en la región actual. Para realizar la detección automatizada y acceder a los datos resultantes en regiones adicionales, habilite y configure la detección automatizada en cada región adicional.
- Si es el administrador de Macie de una organización:
  - Solo puede realizar la detección automatizada de una cuenta de miembro si Macie está habilitada para la cuenta en la región actual. Las cuentas de los miembros no pueden realizar la detección automatizada de sus propias cuentas.
  - Las cuentas de los miembros no pueden acceder a la configuración de detección automatizada que se aplica a sus grupos de S3. Solo el administrador de Macie puede acceder a estos ajustes.
  - Las cuentas de los miembros no pueden acceder a datos confidenciales, estadísticas de detección ni a otros resultados que Macie proporciona directamente a sus grupos de S3. Por ejemplo, la cuenta de un miembro no puede usar la consola de Amazon Macie para revisar las puntuaciones de confidencialidad de sus buckets de S3. Solo el administrador de Macie puede acceder a estos datos.

- Si la configuración de permisos de un bucket de S3 impide que Macie recupere información sobre el bucket o los objetos del bucket o acceda a ellos, Macie no podrá realizar la detección automatizada del bucket. Macie solo puede proporcionar un subconjunto de información sobre el bucket, como el ID de cuenta del propietario del bucket, el nombre del bucket y la fecha en Cuenta de AWS que Macie recuperó por última vez los metadatos del bucket y del objeto del bucket como parte del ciclo de actualización diario. En su inventario de buckets, la puntuación de confidencialidad de estos buckets es 50 y su etiqueta de confidencialidad es Aún no se ha analizado.

  Para identificar rápidamente los buckets de S3 en estos casos, consulte sus datos de cobertura de detección automatizada. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatizada. Para investigar el problema de un bucket en particular, revise la política y la configuración de permisos del bucket en Amazon S3. Por ejemplo, el bucket puede tener una política de bucket restrictiva. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.
- Para poder seleccionarse y analizarse, un objeto de S3 debe estar almacenado en un depósito de uso general y debe ser clasificable. Un objeto clasificable utiliza una clase de almacenamiento de Amazon S3 compatible y tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.
- Si un objeto de S3 está cifrado, Macie solo puede analizarlo si está cifrado con una clave a la que Macie pueda acceder y que pueda usar. Para obtener más información, consulte Análisis de objetos S3 cifrados. Para identificar los casos en los que la configuración de cifrado impidió que Macie analizara uno o más objetos de un bucket, consulte sus datos de cobertura de detección automatizada. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatizada.

Configuración de la detección de datos confidenciales automatizada para su cuenta

Con la detección automática de datos confidenciales, Amazon Macie selecciona continuamente objetos de muestra de sus depósitos de uso general del Amazon Simple Storage Service (Amazon S3) y los analiza para determinar si contienen datos confidenciales. Si es el administrador de Macie de una organización, esto incluye los objetos de los buckets de S3 que sean propiedad de sus cuentas de miembros. A medida que el análisis avanza cada día, Macie actualiza las estadísticas,

los datos de inventario y otra información que proporciona sobre sus datos de Amazon S3. Macie también genera registros de los datos confidenciales que encuentra y de los análisis que realiza.

Para configurar y utilizar la detección automatizada de datos confidenciales, su cuenta debe ser una cuenta de Macie independiente o la cuenta de administrador de Macie de una organización. Si tiene una cuenta de miembro y desea realizar la detección automatizada de sus buckets de S3, póngase en contacto con el administrador de Macie de su organización. Para obtener más información, consulte Administración de varias cuentas .

Temas

Al activar, configurar o deshabilitar la detección automática de datos confidenciales en su cuenta, los cambios se aplicarán únicamente a la cuenta actual. Región de AWS Para realizar los mismos cambios en regiones adicionales, repita los pasos correspondientes en cada región adicional.

Antes de empezar

Antes de configurar la detección de datos confidenciales automatizada para su cuenta, compruebe que dispone de los permisos que necesita. Compruebe también que ha configurado un repositorio para los resultados de la detección de datos confidenciales.

Para verificar tus permisos, usa AWS Identity and Access Management (IAM) para revisar las políticas de IAM asociadas a tu identidad de IAM. A continuación, compare la información de esas políticas con la siguiente lista de acciones que debe estar autorizado a realizar:

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`

La primera acción le permite acceder a su cuenta de Amazon Macie. La segunda acción le permite cambiar los ajustes de configuración de la detección de datos confidenciales automatizada de su cuenta. Esto incluye habilitar y deshabilitar la configuración. Si lo desea, compruebe que también está autorizado a realizar la acción `macie2:GetAutomatedDiscoveryConfiguration`.

Esta acción le permite recuperar los valores de configuración actuales y el estado actual de la configuración.

Además de verificar sus permisos, compruebe que ha configurado un repositorio para almacenar los resultados de la detección de datos confidenciales. Un resultado de detección de datos confidenciales es un registro de los detalles sobre el análisis de un objeto. Macie crea un resultado de detección de datos confidenciales para cada objeto de S3 que analiza mientras realiza la detección de datos confidenciales automatizada. Esto incluye objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no produce resultados de datos confidenciales y objetos que Macie no puede analizar debido a problemas o errores. Si Macie encuentra datos confidenciales en un objeto, el resultado de la detección de datos confidenciales incluirá los datos del resultado correspondiente. También contiene información adicional. Estos resultados le proporcionan registros de análisis que pueden ser útiles para las auditorías o investigaciones sobre la privacidad y la protección de los datos.

Macie almacena los resultados de la detección de datos confidenciales solo durante 90 días. Para acceder a los resultados y permitir su almacenamiento y retención a largo plazo, configure Macie para que almacene los resultados en un bucket de S3. El bucket puede servir como un repositorio definitivo y a largo plazo para todos sus resultados de detección de datos confidenciales.

Para comprobar que ha configurado este repositorio para su cuenta, seleccione Resultados de la detección en el panel de navegación de la consola de Amazon Macie. Si prefiere hacerlo mediante programación, utilice el GetClassificationExportConfigurationfuncionamiento de la API Amazon Macie. Para obtener información sobre cómo configurar este repositorio, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Si ha configurado el repositorio, Macie crea una carpeta denominada automated-sensitive-data-discovery en el repositorio cuando la detección de datos confidenciales automatizada esté habilitada inicialmente en su cuenta. Esta carpeta almacena los resultados de la detección de datos confidenciales que Macie crea mientras realiza la detección automática de su cuenta.

Habilitación de la detección de datos confidenciales automatizada para su cuenta

Cuando habilita la detección de datos confidenciales automatizada en su cuenta, Amazon Macie comienza a evaluar los datos de inventario de Amazon S3 y a realizar otras actividades de detección automatizada para su cuenta en la Región de AWS actual. Según el tamaño del patrimonio de datos de Amazon S3, las estadísticas de detección de datos confidenciales y otros resultados pueden empezar a aparecer en un plazo de 48 horas tras habilitar la detección automatizada para su cuenta.

Siga estos pasos para habilitar la detección de datos confidenciales automatizada para su cuenta mediante la consola de Amazon Macie. Para habilitar el descubrimiento automatizado mediante programación, utilice el UpdateAutomatedDiscoveryConfigurationfuncionamiento de la API Amazon Macie.

Para habilitar la detección de datos confidenciales automatizada para su cuenta

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee habilitar la detección automática de datos confidenciales.
3. En el panel de navegación, en Configuración, elija Detección automatizada.
4. En la lista Estado, elija Habilitado.
5. Cuando se le pida que confirme, elija Enable (Habilitar).

Tras activar la detección de datos confidenciales automatizada, revise y configure los ajustes para refinar los análisis que Macie realizará posteriormente.

Configuración de los ajustes de detección de datos confidenciales automatizada para su cuenta

Si la detección de datos confidenciales automatizada está habilitada para su cuenta, puede ajustar la configuración de detección automatizada de su cuenta para refinar los análisis que realiza Amazon Macie. Esta configuración especifica qué buckets de S3 desea incluir en los análisis. También especifican los tipos y las ocurrencias de datos confidenciales que desea que Macie detecte y notifique: los identificadores de datos administrados, los identificadores de datos personalizados y las listas de permisos que se pueden utilizar al analizar los objetos de S3.

De forma predeterminada, Macie realiza la detección automática de datos confidenciales para todos los depósitos de uso general de S3 que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro. Puede excluir buckets específicos de los análisis. Por ejemplo, puede excluir los depósitos que suelen almacenar datos de AWS registro, como AWS CloudTrail los registros de eventos. Si excluye un bucket, puede volver a incluirlo posteriormente.

Además, Macie analiza los objetos de S3 utilizando únicamente el conjunto de identificadores de datos administrados que recomendamos para la detección de datos confidenciales automatizada. Macie no utiliza identificadores de datos personalizados ni permite listas que usted haya definido.

Para personalizar los análisis, puede configurar Macie para que utilice listas de permisos específicas, identificadores de datos personalizados e identificadores de datos administrados.

En las siguientes secciones se proporciona información adicional sobre cada tipo de configuración y se explica cómo cambiar una configuración mediante la consola Amazon Macie. Elija una sección para obtener más información. Para revisar o cambiar la configuración mediante programación, puede utilizar las siguientes operaciones de la API de Amazon Macie UpdateClassificationScope: para especificar qué buckets de S3 debe excluir de los análisis UpdateSensitivityInspectionTemplatey para especificar qué listas de permisos, identificadores de datos personalizados e identificadores de datos gestionados utilizar.

Si cambia una configuración, Macie aplicará su cambio cuando comience el siguiente ciclo de evaluación y análisis para la detección de datos confidenciales automatizada, normalmente en un plazo de 24 horas.

Excluir o incluir buckets de S3 en los análisis

De forma predeterminada, Macie realiza la detección automática de datos confidenciales para todos los depósitos de uso general de S3 que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro. Para ajustar el ámbito, puede excluir hasta 1000 buckets de los análisis.

Si excluye un bucket de S3, Macie dejará de analizar los objetos del bucket cuando realice la detección de datos confidenciales automatizada de su cuenta. Las estadísticas y los detalles de detección de datos confidenciales existentes sobre el bucket persisten; por ejemplo, la puntuación de confidencialidad actual del bucket permanece inalterada. Después de excluir un bucket, puede volver a incluirlo posteriormente.

Para excluir o incluir buckets S3 específicos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee excluir o incluir grupos de S3 específicos en los análisis de detección automatizados.
3. En el panel de navegación, en Configuración, elija Detección automatizada. Aparece la página Detección de datos confidenciales automatizada y muestra su configuración actual. En esa página, la sección de buckets de S3 muestra los buckets de S3 que están actualmente excluidos o indica que todos los buckets están incluidos actualmente.
4. En la sección Buckets de S3, elija Editar.

5. Realice una de las siguientes acciones siguientes:

   - Para excluir uno o más buckets de S3, seleccione Agregar buckets a la lista de exclusión. A continuación, en la tabla de buckets de S3, seleccione la casilla de verificación de cada bucket que desee excluir. En la tabla se muestran todos los grupos de uso general de su cuenta en la región actual.
   - Para incluir uno o más buckets de S3 que excluyó anteriormente, seleccione Eliminar buckets de la lista de exclusión. A continuación, en la tabla de buckets de S3, seleccione la casilla de verificación de cada bucket que desee incluir. En la tabla se enumeran todos los buckets que actualmente están excluidos de la detección de datos confidenciales automatizada.

   Para encontrar buckets específicos con mayor facilidad, introduzca los criterios de búsqueda en el cuadro de búsqueda situado encima de la tabla. También puede ordenar la tabla por nombre de bucket.
6. Cuando termine de seleccionar los buckets, elija Agregar o Eliminar, según la opción que haya elegido en el paso anterior.

Agregar o eliminar los identificadores de datos administrados de los análisis

Un identificador de datos gestionados es un conjunto de criterios y técnicas integrados que están diseñados para detectar un tipo específico de datos confidenciales, por ejemplo, números de tarjetas de crédito, claves de acceso AWS secretas o números de pasaporte de un país o región determinados. De forma predeterminada, Macie analiza los objetos de S3 mediante el conjunto de identificadores de datos administrados que recomendamos para la detección automatizada de datos confidenciales. Para revisar la lista de identificadores incluidos en este conjunto, consulte Configuración predeterminada para la detección automatizada de datos confidenciales.

Puede personalizar los análisis para que se centren en tipos específicos de datos confidenciales: añada identificadores de datos administrados para los tipos de datos confidenciales que desee que Macie detecte y notifique, y elimine los identificadores de datos administrados para los tipos de datos confidenciales que no desee que Macie detecte y notifique. Si elimina un identificador de datos administrados, el cambio no afectará a las estadísticas ni a los detalles de detección de datos confidenciales existentes en sus buckets de S3. Por ejemplo, si eliminas el identificador de datos gestionados que detecta las claves de acceso AWS secretas y Macie detectó previamente ese tipo de datos confidenciales en un depósito, Macie seguirá informando de esas detecciones en el depósito.

> **Tip**
>
> En lugar de eliminar un identificador de datos administrados de los análisis posteriores de todos los buckets de S3, puede excluir ese tipo de detección de la puntuación de confidencialidad de determinados buckets. Para obtener más información, consulte Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales.

Agregar o eliminar identificadores de datos administrados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee añadir o eliminar los identificadores de datos gestionados de los análisis de detección automatizados.
3. En el panel de navegación, en Configuración, elija Detección automatizada. En la página Detección de datos confidenciales automatizada, la sección Identificadores de datos administrados muestra su configuración actual, organizada en dos pestañas:

   - Se ha agregado al valor predeterminado: en esta pestaña se muestran los identificadores de datos administrados que ha añadido de forma explícita. Macie utiliza estos identificadores de datos administrados además de los que están en el conjunto predeterminado y usted no los ha eliminado de forma explícita.
   - Se ha eliminado del valor predeterminado: en esta pestaña se muestran los identificadores de datos administrados que ha eliminado de forma explícita. Macie no utiliza estos identificadores de datos administrados.
4. En la sección Identificadores de datos administrados, seleccione Editar.
5. Realice uno de los siguientes procedimientos:

   - Para añadir uno o más identificadores de datos administrados, seleccione la pestaña Se ha agregado al valor predeterminado. A continuación, en la tabla, seleccione la casilla de verificación de cada identificador de datos administrados que desee agregar. Si una casilla de verificación ya está seleccionada, ya ha agregado ese identificador.
   - Para eliminar uno o más identificadores de datos administrados, seleccione la pestaña Se ha eliminado del valor predeterminado. A continuación, en la tabla, seleccione la casilla de verificación de cada identificador de datos administrados que desee eliminar. Si una casilla de verificación ya está seleccionada, ya ha eliminado ese identificador.

En cada pestaña, la tabla muestra una lista de todos los identificadores de datos administrados que Macie proporciona actualmente. En la tabla, el ID de cada identificador de datos administrados describe el tipo de datos confidenciales que el identificador está diseñado para detectar, por ejemplo, USA_PASSPORT_NUMBER para los números de pasaporte estadounidenses. Para encontrar más fácilmente identificadores de datos administrados específicos, introduzca los criterios de búsqueda en el cuadro de búsqueda situado encima de la tabla. Puede ordenar las filas de la tabla si elige un encabezado de columna. Para obtener más información sobre cada identificador, consulte Uso de identificadores de datos administrados.

6. Cuando termine, elija Save (Guardar).

Agregar o eliminar identificadores de datos personalizados de los análisis

Un identificador de datos personalizado es un conjunto de criterios que se definen para detectar información confidencial. Los criterios consisten en una expresión regular (regex) que define un patrón de texto para que coincida y, opcionalmente, secuencias de caracteres y una regla de proximidad que perfeccionen los resultados. Para obtener más información, consulte Creación de identificadores de datos personalizados.

De forma predeterminada, Amazon Macie no utiliza identificadores de datos personalizados cuando realiza la detección de datos confidenciales automatizada. Si desea que Macie utilice identificadores de datos personalizados específicos, puede añadirlos a los análisis. A continuación, Macie utiliza los identificadores de datos personalizados además de los identificadores de datos administrados que también haya configurado para que utilice Macie.

Si añade un identificador de datos personalizado a los análisis, podrá eliminarlo posteriormente. El cambio no afectará a las estadísticas ni a los detalles de detección de datos confidenciales existentes en sus buckets de S3. Por ejemplo, si elimina un identificador de datos personalizado que anteriormente producía detecciones para un bucket, Macie seguirá informando de esas detecciones para el bucket. Sin embargo, considere la posibilidad de excluir ese tipo de detección de la puntuación de confidencialidad para buckets específicos en lugar de eliminar el identificador de los análisis posteriores de todos los buckets. Para obtener más información, consulte Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales.

Agregar o eliminar identificadores de datos personalizados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee añadir o eliminar los identificadores de datos personalizados de los análisis de descubrimiento automatizados.
3. En el panel de navegación, en Configuración, elija Detección automatizada. Aparece la página Detección de datos confidenciales automatizada y muestra su configuración actual. En esa página, la sección Identificadores de datos personalizados muestra los identificadores de datos personalizados que ha agregado o indica que no ha seleccionado ningún identificador de datos personalizado para su detección automatizada.
4. En la sección Identificadores de datos administrados, seleccione Editar.
5. Realice uno de los siguientes procedimientos:

   - Agregue uno o más identificadores de datos personalizados, seleccione la casilla de verificación de cada identificador de datos personalizado que desee agregar. Si una casilla de verificación ya está seleccionada, ya ha agregado ese identificador.
   - Para eliminar uno o más identificadores de datos personalizados, desactive la casilla de verificación de cada identificador de datos personalizado que desee eliminar. Si una casilla de verificación ya está desactivada, Macie no utiliza actualmente ese identificador al realizar la detección automatizada.

   > **Tip**
   >
   > Para revisar o probar la configuración de un identificador de datos personalizado antes de añadirlo o eliminarlo, elija el icono de enlace () junto al nombre del identificador. Macie abre una página que muestra la configuración del identificador.
   >
   > También puede usar esta página para probar el identificador con datos de muestra. Para ello, introduzca hasta 1000 caracteres en el cuadro Datos de muestra y, a continuación, seleccione Prueba. Macie evalúa los datos de la muestra mediante el identificador y, a continuación, indica el número de coincidencias.

6. Cuando termine, elija Save (Guardar).

Añadir o elimine las listas de los análisis

En Amazon Macie, una lista de permitidos define un texto específico o un patrón de texto que debe ignorar Macie al inspeccionar objetos de S3 en busca de datos confidenciales. Si el texto coincide con una entrada o un patrón de una lista de permitidos, Macie no lo registra, aunque el texto coincida con los criterios de un identificador de datos gestionado o personalizado. Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

De forma predeterminada, Macie no utiliza listas cuando realiza la detección de datos confidenciales automatizada. Si quiere que Macie utilice listas de permisos específicas, puede añadirlas a los análisis. Si añade una lista de permitidos a los análisis, podrá eliminarla posteriormente.

Añadir o eliminar listas de permitidos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee añadir o eliminar las listas de usuarios permitidos en los análisis de detección automatizados.
3. En el panel de navegación, en Configuración, elija Detección automatizada. Aparece la página Detección de datos confidenciales automatizada y muestra su configuración actual. En esa página, la sección Listas de permitidos indica qué listas de permitidos ha agregado o indica que no ha seleccionado ninguna lista de permitidos para su detección automatizada.
4. En la sección Listas de permitidos elija Editar.
5. Realice uno de los siguientes procedimientos:

   - Agregar una o más listas de permisos. seleccione la casilla de verificación de cada lista de permisos. Si una casilla de verificación ya está seleccionada, ya ha agregado esa lista.
   - Para agregar una o más listas de permitidos, desactive la casilla de verificación de cada lista de permitidos que desee eliminar. Si una casilla de verificación ya está desactivada, Macie no utiliza actualmente ese identificador al realizar la detección automatizada.

> **Tip**
>
> Para revisar la configuración de una lista de permitidos antes de añadirla o eliminarla, seleccione el icono de enlace ( )

situado junto al nombre de la lista. Macie abre una página que muestra la configuración de la lista.

6. Cuando termine, elija Save (Guardar).

Desactivación de la detección de datos confidenciales automatizada en su cuenta

Puede desactivar la detección de datos confidenciales automatizada de su cuenta en cualquier momento. Si desactiva la detección de datos confidenciales automatizada, Macie dejará de realizar todas las actividades de detección automatizada en su cuenta antes de que comience el siguiente ciclo de evaluación y análisis, normalmente en un plazo de 24 horas. Además, perderá el acceso a todos los datos estadísticos, de inventario y demás información que Macie produjo y proporcionó directamente mientras realizaba esas actividades. Por ejemplo, su inventario de cubos de S3 ya no incluye puntuaciones de sensibilidad ni visualizaciones, ni analiza las estadísticas y los detalles de los grupos individuales.

Puede seguir accediendo a los resultados de datos confidenciales que Macie ha obtenido mientras realizaba la detección automatizada de su cuenta. Macie guarda sus resultados durante 90 días. Además, los datos que ha almacenado o publicado en otros sitios Servicios de AWS permanecen intactos y no se ven afectados, como los resultados de descubrimiento de datos confidenciales en Amazon S3 y los eventos de búsqueda en Amazon EventBridge.

Si desactiva la detección de datos confidenciales automatizada de su cuenta, puede activarla de nuevo. A continuación, Macie reanudará todas las actividades de detección automatizada de su cuenta. Si lo vuelve a habilitar en 30 días, volverá a tener acceso a todos los datos estadísticos, de inventario y demás información que Macie produjo previamente y proporcionó directamente mientras realizaba esas actividades. Si no lo vuelve a activar en un plazo de 30 días, Macie eliminará de forma permanente los datos estadísticos y demás información que anteriormente generaba y proporcionaba directamente.

Siga estos pasos para deshabilitar la detección de datos confidenciales automatizada para su cuenta mediante la consola de Amazon Macie. Para deshabilitar la detección automática mediante programación, utilice el UpdateAutomatedDiscoveryConfigurationfuncionamiento de la API Amazon Macie.

Para desactivar la detección de datos confidenciales automatizada en su cuenta

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee deshabilitar la detección automática de datos confidenciales.
3. En el panel de navegación, en Configuración, elija Detección automatizada.
4. En la sección Estado, elija Deshabilitada.
5. Cuando se le indique que confirme, elija Disable (Desactivar).

Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales

A medida que revise y evalúe las estadísticas y los resultados de la detección automatizada de datos confidenciales, podrá ajustar la puntuación de confidencialidad y otros ajustes para los buckets individuales de Amazon Simple Storage Service (Amazon S3). Al ajustar esta configuración, puede ajustar con precisión las evaluaciones de confidencialidad de su patrimonio de datos de Amazon S3 en general y de los buckets específicos que contiene. También puede capturar los resultados de las investigaciones que realice para buckets específicos.

Puede ajustar la configuración de detección automatizada de datos confidenciales para un bucket de S3 de las siguientes maneras.

Asignar puntuación de confidencialidad

De forma predeterminada, Amazon Macie calcula automáticamente la puntuación de confidencialidad de un bucket. La puntuación se basa principalmente en la cantidad de datos confidenciales que Macie ha encontrado en un bucket y en la cantidad de datos que Macie ha analizado en un bucket. Para obtener más información, consulte Puntuación de confidencialidad para buckets de S3.

Puede anular la puntuación calculada de un bucket y asignar manualmente la puntuación máxima (100), con lo que también se aplica la etiqueta de Confidencialidad al bucket. Si lo hace, Macie seguirá realizando la detección automatizada del bucket. Sin embargo, los análisis posteriores no afectan a la puntuación del bucket. Para volver a calcular la puntuación automáticamente, vuelva a cambiar la configuración.

Excluya o incluya tipos de datos confidenciales específicos en la puntuación de confidencialidad

Si se calcula automáticamente, la puntuación de confidencialidad de un bucket se basa en parte en la cantidad de datos confidenciales que Macie ha encontrado en el bucket. Esto se debe principalmente a la naturaleza y el número de tipos de datos confidenciales que Macie ha

encontrado en el bucket y al número de veces que aparece cada tipo. De forma predeterminada, Macie incluye las apariciones de todos los tipos de datos confidenciales al calcular la puntuación de confidencialidad de un bucket.

Puede ajustar el cálculo excluyendo o incluyendo tipos específicos de datos confidenciales en la puntuación de un segmento. Por ejemplo, si Macie detectó direcciones postales en un bucket y usted determina que esto es aceptable, puede excluir todas las direcciones postales que aparezcan en la puntuación del bucket. Si excluye un tipo de datos confidenciales, Macie seguirá inspeccionando el bucket en busca de ese tipo de datos e informando de los casos que encuentre. Sin embargo, esas ocurrencias no afectan a la puntuación calculada por el grupo. Para volver a incluir un tipo de datos confidenciales en el almacén calculado, vuelva a cambiar la configuración.

Excluya o incluya el bucket en los análisis posteriores

De forma predeterminada, Macie realiza la detección automática de todos los depósitos de uso general que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro. Puede excluir buckets específicos de los análisis. Por ejemplo, puede excluir los depósitos que suelen almacenar datos de AWS registro, como AWS CloudTrail los registros de eventos.

Si excluye un bucket, las estadísticas de detección de datos confidenciales existentes y los detalles del bucket persisten; por ejemplo, la puntuación de confidencialidad actual del bucket permanece inalterada. Sin embargo, Macie deja de analizar los objetos del bucket cuando realiza una detección automatizada para su cuenta. Después de excluir un bucket, puede volver a incluirlo posteriormente.

Si cambia una configuración que afecta a la puntuación de confidencialidad de un bucket de S3, Macie empezará inmediatamente a recalcular y actualizar las estadísticas de detección de datos confidenciales relevantes y demás información que proporcione sobre sus datos de Amazon S3. Por ejemplo, si asigna la máxima puntuación a un bucket, Macie incrementará el número de buckets Confidenciales en las estadísticas agregadas de su cuenta.

Siga estos pasos para cambiar una configuración mediante la consola Amazon Macie. Para cambiar una configuración mediante programación, puede utilizar las siguientes operaciones de la API de Amazon Macie UpdateResourceProfile:, para asignar una puntuación de sensibilidad a un segmento UpdateResourceProfileDetections;, para excluir o incluir posteriormente tipos de datos confidenciales en la puntuación de un segmento; y UpdateClassificationScope, para excluir o incluir un segmento en los análisis posteriores.

Para cambiar la configuración de la detección de datos confidenciales de un bucket de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3.
3. En la página de buckets de S3, elija el bucket de S3 cuya configuración desee cambiar. Puede elegir el bucket mediante la vista de tabla () o el mapa interactivo ().
4. En la página de detalles, realice alguna de las siguientes acciones:

   - Para anular la puntuación calculada y asignar manualmente una puntuación de confidencialidad al bucket, active Asignar puntuación máxima ().
     Esto cambia la puntuación del bucket a 100 y se aplica la etiqueta de confidencial al bucket.

     Para asignar una puntuación que Macie calcule automáticamente, desactive Asignar puntuación máxima ().
   - Para excluir el bucket de los análisis posteriores, active Excluir de la detección automatizada ().

     Si anteriormente excluyó el bucket de los análisis, desactive Excluir de la detección automatizada () para volver a incluirlo.
   - Para excluir o incluir la aparición de tipos específicos de datos confidenciales en la puntuación de confidencialidad del bucket, seleccione la pestaña Confidencialidad. En la tabla de Detecciones, active la casilla del tipo de datos confidenciales que desee excluir o incluir. A continuación, en el menú Acciones, elija Excluir de la puntuación para excluir el tipo o elija Incluir en la puntuación para incluir el tipo.

     En la tabla, el campo Tipo de datos confidenciales especifica el identificador (ID) único del identificador de datos administrados que detectó los datos o el nombre del identificador de datos personalizado que detectó los datos. El ID de un identificador de datos administrados describe el tipo de datos confidenciales que el identificador está diseñado para detectar; por

ejemplo, USA_PASSPORT_NUMBER para los números de pasaporte estadounidenses. Para obtener más información sobre cada identificador de datos administrados, consulte. Uso de identificadores de datos administrados

Si ha cambiado una configuración que afecta a la puntuación de sensibilidad del depósito de S3, Macie empezará inmediatamente a volver a calcular y actualizar las estadísticas de detección de datos confidenciales pertinentes y otra información sobre el depósito.

Evaluación de cobertura de detección de datos confidenciales automatizada

A medida que avanza la detección de datos confidenciales automatizada para su cuenta, Amazon Macie proporciona estadísticas y detalles para ayudarle a evaluar y supervisar la cobertura de su patrimonio de datos de Amazon Simple Storage Service (Amazon S3). Con estos datos, puede comprobar el estado de detección de datos confidenciales automatizada para el patrimonio de datos en general y de los buckets de S3 individuales de su inventario de buckets. También puede identificar los problemas que impidieron que Macie analizara objetos en buckets específicos. Si soluciona los problemas, puede aumentar la cobertura de sus datos de Amazon S3 durante los ciclos de análisis posteriores.

Los datos de cobertura proporcionan una instantánea del estado actual de la detección automática de datos confidenciales para sus depósitos de uso general de S3 en la actualidad Región de AWS. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro. Para cada bucket, los datos indican si se produjeron problemas cuando Macie intentó analizar los objetos del bucket. Si se produjeron problemas, los datos indican la naturaleza de cada problema y, en algunos casos, el número de casos. Los datos se actualizan a medida que avanza la detección de datos confidenciales automatizada en su cuenta cada día. Si Macie analiza o intenta analizar uno o más objetos de un bucket durante un ciclo de análisis diario, Macie actualiza la cobertura y otros datos para reflejar los resultados.

En el caso de determinados tipos de problemas, puede revisar los datos en conjunto de todos los segmentos de uso general de S3 y, si lo desea, profundizar en ellos para obtener detalles adicionales sobre cada uno de ellos. Por ejemplo, los datos de cobertura pueden ayudarte a identificar rápidamente todos los buckets a los que Macie no puede acceder desde su cuenta. Los datos de cobertura también indican los problemas a nivel de objeto que se han producido. Estos problemas, denominados errores de clasificación, impidieron que Macie analizara objetos específicos de un bucket. Por ejemplo, puedes determinar cuántos objetos no pudo analizar Macie en un depósito porque los objetos están cifrados con una clave AWS Key Management Service (AWS KMS) que ya no está disponible.

Si utiliza la consola de Amazon Macie para revisar los datos de cobertura, la vista de los datos incluye un asesoramiento de corrección para solucionar cada tipo de problema. Los temas siguientes de esta sección también proporcionan un asesoramiento de corrección para cada tipo.

Temas

Revisión de datos de cobertura de detección de datos confidenciales automatizada

Para revisar y evaluar la detección de datos confidenciales automatizada de su cuenta, puede utilizar la consola Amazon Macie o la API de Amazon Macie. Tanto la consola como la API proporcionan datos que indican el estado actual de los análisis de los buckets de uso general de Amazon Simple Storage Service (Amazon S3) en ese momento. Región de AWS Los datos incluyen información sobre los problemas que crean lagunas en los análisis:

- Buckets a los que Macie no puede acceder. Macie no puede analizar ningún objeto de estos buckets porque la configuración de permisos de los buckets impide que Macie acceda a los buckets y a los objetos de los buckets.
- Cubos que no almacenan ningún objeto clasificable. Macie no puede analizar ningún objeto de estos buckets porque todos los objetos utilizan clases de almacenamiento de Amazon S3 que Macie no admite o tienen extensiones de nombre de archivo para formatos de archivo o almacenamiento que Macie no admite.
- Cubos que Macie aún no ha podido analizar debido a errores de clasificación a nivel de objeto. Macie intentó analizar uno o más objetos de estos buckets. Sin embargo, Macie no pudo analizar los objetos debido a problemas con la configuración de los permisos a nivel de objeto, el contenido de los objetos o las cuotas.

Los datos de cobertura se actualizan a medida que avanza la detección de datos confidenciales automatizada para su cuenta cada día. Si es el administrador de Macie de una organización, los datos incluyen información de los buckets de S3 que sean propiedad de sus cuentas de miembros.

> **Note**
>
> Los datos de cobertura no incluyen explícitamente los resultados de los trabajos de detección de datos confidenciales que haya creado y ejecutado. Sin embargo, si corrige los problemas de cobertura que afectan a los resultados de la detección de datos confidenciales automatizada, es probable que también aumente la cobertura de los trabajos de detección de datos confidenciales que ejecute posteriormente. Para evaluar la cobertura de un trabajo, revise las estadísticas y los resultados del trabajo. Si los eventos de registro u otros resultados indican problemas de cobertura, el asesoramiento de corrección que aparece más adelante en esta sección puede ayudarle a solucionar algunos de los problemas.

Para revisar los datos de cobertura de detección de datos confidenciales automatizada

Puede usar la consola de Amazon Macie o la API de Amazon Macie para revisar los datos de cobertura de su cuenta u organización. En la consola, una sola página ofrece una vista unificada de los datos de cobertura de todos los segmentos de uso general de S3, incluido un resumen de los problemas que se han producido recientemente en cada uno de ellos. La página también ofrece opciones para revisar grupos de datos por tipo de problema. Para realizar un seguimiento de la investigación de problemas en buckets específicos, puede exportar los datos de la página a un archivo de valores separados por comas (CSV).

Console

Siga estos pasos para revisar los datos de cobertura de detección de datos confidenciales automatizada mediante la consola de Amazon Macie.

Para revisar los datos de cobertura

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Cobertura de recursos.
3. En la página Cobertura de recursos, seleccione la pestaña correspondiente al tipo de datos de cobertura que desea revisar:

   - Todos: muestra todos los depósitos que Macie monitorea y analiza para tu cuenta.

Para cada bucket, el campo Problemas indica si los problemas impidieron que Macie analizara los objetos del bucket. Si el valor de este campo es Ninguno, Macie ha analizado al menos uno de los objetos del bucket o no ha intentado analizar ninguno de los objetos del bucket todavía. Si hay problemas, este campo indica la naturaleza de los problemas y cómo solucionarlos. En el caso de los errores de clasificación a nivel de objeto, también puede indicar (entre paréntesis) el número de ocurrencias del error.

- Acceso denegado: muestra los depósitos a los que Macie no puede acceder. La configuración de permisos de estos buckets impide que Macie acceda a los buckets y a los objetos de los buckets. Por lo tanto, Macie no puede analizar ningún objeto de estos buckets.
- Error de clasificación: muestra los grupos que Macie aún no ha analizado debido a errores de clasificación a nivel de objeto (problemas con la configuración de los permisos, el contenido de los objetos o las cuotas) a nivel de objeto.

  Para cada bucket, el campo Problemas indica la naturaleza de cada tipo de error que se ha producido y ha impedido a Macie analizar un objeto del bucket. También indica cómo corregir cada tipo de error. Dependiendo del error, también puede indicar (entre paréntesis) el número de ocurrencias del error.
- Inclasificable: enumera los cubos que Macie no puede analizar porque no almacenan ningún objeto clasificable. Todos los objetos de estos buckets utilizan clases de almacenamiento de Amazon S3 no compatibles o tienen extensiones de nombre de archivo para formatos de archivo o almacenamiento no compatibles. Por lo tanto, Macie no puede analizar ningún objeto de estos buckets.

4. Para profundizar y revisar los datos de respaldo de un depósito, elija el nombre del depósito. A continuación, consulte el panel de detalles del bucket para ver las estadísticas y otra información sobre el bucket.
5. Para exportar la tabla a un archivo CSV, seleccione Exportar a CSV en la parte superior de la página. El archivo CSV resultante contiene un subconjunto de metadatos para cada depósito de la tabla, hasta un máximo de 50 000 cubos. El archivo incluye un campo Problemas de cobertura. El valor de este campo indica si los problemas impidieron a Macie analizar los objetos del bucket y, de ser así, la naturaleza de los problemas.

API

Para revisar los datos de cobertura mediante programación, especifique los criterios de filtrado en las consultas que envíe mediante la DescribeBucketsoperación de la API Amazon Macie. Esta operación devuelve una matriz de objetos. Cada objeto contiene datos estadísticos y otra información sobre un depósito de uso general de S3 que coincide con los criterios del filtro.

En los criterios de filtro, incluya una condición para el tipo de datos de cobertura que desee revisar:

- Para identificar los buckets a los que Macie no puede acceder debido a la configuración de permisos de los buckets, incluye una condición en la que el valor del campo`errorCode` sea igual a `ACCESS_DENIED`.
- Para identificar los buckets a los que Macie puede acceder y que aún no ha analizado, incluye las condiciones en las que el valor del campo `sensitivityScore` sea igual a `50` y el valor del campo `errorCode` no sea igual a `ACCESS_DENIED`.
- Para identificar los buckets que Macie no puede analizar porque todos los objetos de los buckets utilizan clases o formatos de almacenamiento no compatibles, incluya condiciones en las que el valor del campo `classifiableSizeInBytes` sea igual a `0` y el valor del campo `sizeInBytes` sea mayor que `0`.
- Para identificar los grupos en los que Macie ha analizado al menos un objeto, incluya condiciones en las que el valor del campo `sensitivityScore` esté comprendido entre 1 y 99, pero no sea igual a `50`. Para incluir también los buckets en los que se asignó manualmente la puntuación máxima, el rango debe estar comprendido entre 1 y 100.
- Para identificar los buckets que Macie aún no ha analizado debido a errores de clasificación a nivel de objeto, incluye una condición en la que el valor del campo `sensitivityScore` sea igual a `-1`. Para, a continuación, revisar un desglose de los tipos y la cantidad de errores que se produjeron en un depósito en particular, utilice la GetResourceProfileoperación.

Si utiliza AWS Command Line Interface (AWS CLI), especifique los criterios de filtro en las consultas que envíe ejecutando el comando describe-buckets. Para revisar un desglose de los tipos y la cantidad de errores que se produjeron en un bucket de S3 concreto, si los hubo, ejecute el get-resource-profilecomando.

Por ejemplo, los siguientes AWS CLI comandos utilizan criterios de filtrado para recuperar los detalles de todos los buckets de S3 a los que Macie no puede acceder debido a la configuración de permisos de los buckets.

Este ejemplo está preparado para Unix, Linux y macOS:

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Este ejemplo tiene el formato de Microsoft Windows.

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

Si la solicitud se realiza correctamente, Macie devuelve una `buckets` matriz. La matriz contiene un objeto para cada depósito de S3 que se encuentra en el actual Región de AWS y que coincide con los criterios del filtro.

Si ningún bucket de S3 coincide con los criterios del filtro, Macie devuelve una matriz `buckets` vacía.

```
{
    "buckets": []
}
```

Para obtener más información sobre cómo especificar los criterios de filtro en las consultas, incluidos ejemplos de criterios comunes, consulte Filtrar el inventario de su bucket de S3.

Solución de los problemas de cobertura para la detección de datos confidenciales automatizada

Amazon Macie informa de varios tipos de problemas que reducen la cobertura de la detección de datos confidenciales automatizada de los datos de Amazon Simple Storage Service (Amazon S3). La siguiente información puede ayudarle a investigar y solucionar estos problemas.

Tipos y detalles de los problemas

- Acceso denegado
- Error de clasificación: contenido no válido
- Error de clasificación: cifrado no válido
- Error de clasificación: clave KMS no válida
- Error de clasificación: permiso denegado
- No clasificable

> **Tip**
>
> Para investigar los errores de clasificación a nivel de objeto de un bucket de S3, comience por revisar la lista de muestras de objetos del bucket. Esta lista indica los objetos que Macie analizó o intentó analizar en el bucket, para un máximo de 100 objetos.
> Para revisar la lista en la consola de Amazon Macie, elija el bucket en la página de buckets de S3 y, a continuación, elija la pestaña Muestras de objetos en el panel de detalles del bucket. Para revisar la lista mediante programación, utilice el ListResourceProfileArtifactsfuncionamiento de la API Amazon Macie. Si el estado del análisis de un objeto es Omitido (`SKIPPED`), es posible que el objeto haya provocado el error.

Acceso denegado

La configuración de permisos del bucket impide que Macie acceda al bucket y a los objetos del bucket. Macie no puede analizar ningún objeto de este bucket.

Detalles

La causa más común de este tipo de problemas es una política de bucket restrictiva. Una política de bucket es una política basada en recursos AWS Identity and Access Management (IAM) que especifica qué acciones puede realizar un principal (usuario, cuenta, servicio u otra entidad) en un bucket de S3 y las condiciones en las que un principal puede realizar esas acciones. Una política de bucket restrictiva utiliza instrucciones explícitas `Allow` o `Deny` restrictivas que conceden o restringen el acceso a los datos de un bucket en función de condiciones específicas. Por ejemplo, una política de bucket puede contener una instrucción `Allow` o `Deny` que deniegue el acceso a un bucket a menos que se utilicen direcciones IP de origen específicas para acceder al bucket.

Si la política de bucket de un bucket de S3 contiene una instrucción `Deny` explícita con una o más condiciones, es posible que a Macie no se le permita recuperar y analizar los objetos del bucket para detectar datos confidenciales. Macie solo puede proporcionar un subconjunto de información sobre el bucket, como el nombre y la fecha de creación del bucket.

Asesoramiento de corrección

Para solucionar este problema, actualice la política del bucket para el bucket de S3. Asegúrese de que la política permita a Macie acceder al bucket y a los objetos del bucket. Para permitir este acceso, añada a la política una condición para el rol vinculado al servicio de Macie (`AWSServiceRoleForAmazonMacie`). La condición debe impedir que el rol vinculado al servicio

de Macie coincida con la restricción `Deny` de la política. Para ello, puede utilizar la clave de contexto de la condición global `aws:PrincipalArn` y el nombre de recurso de Amazon (ARN) del rol vinculado al servicio de Macie para su cuenta.

Si actualiza la política del bucket y Macie obtiene acceso al bucket de S3, Macie detectará el cambio. Cuando esto sucede, Macie actualizará las estadísticas, los datos de inventario y demás información que proporcione sobre sus datos de Amazon S3. Además, los objetos del bucket tendrán mayor prioridad para el análisis durante un ciclo de análisis posterior.

Referencia adicional

Para obtener más información sobre cómo actualizar una política de bucket de S3 para permitir que Macie acceda a un bucket, consulte Permitir a Amazon Macie el acceso a buckets y objetos de S3. Para obtener más información acerca de la asociación de políticas a buckets, consulte las políticas de bucket y de usuario y cómo Amazon S3 autoriza una solicitud en el manual del usuario de Amazon Simple Storage.

Error de clasificación: contenido no válido

Este tipo de error de clasificación se produce si Macie intenta analizar un objeto de un bucket de S3 y el objeto tiene un formato incorrecto o contiene contenido que supera la cuota de detección de datos confidenciales. Macie no puede analizar el objeto.

Detalles

Este error suele producirse porque un objeto S3 es un archivo con formato incorrecto o dañado. En consecuencia, Macie no puede analizar todos los datos del archivo.

Este error también puede producirse si el análisis de un objeto de S3 supera la cuota de detección de datos confidenciales de un archivo individual. Por ejemplo, el tamaño de almacenamiento del objeto supera la cuota de tamaño para ese tipo de archivo.

En cualquier caso, Macie no puede completar el análisis del objeto S3 y el estado del análisis del objeto es Omitido (`SKIPPED`).

Asesoramiento de corrección

Para investigar este error, descargue el objeto de S3 y compruebe el formato y el contenido del archivo. Evalúe también el contenido del archivo comparándolo con las cuotas de Macie para la detección de datos confidenciales.

Si no corrige este error, Macie intentará analizar otros objetos del bucket de S3. Si Macie analiza otro objeto correctamente, actualizará los datos de cobertura y demás información que proporcione sobre el bucket.

Referencia adicional

Para obtener una lista de las cuotas de detección de datos confidenciales, incluidas las cuotas para determinados tipos de archivos, consulteCuotas de Amazon Macie. Para obtener información sobre cómo Macie actualiza las puntuaciones de sensibilidad y otra información que proporciona sobre los buckets de S3, consulte Cómo funciona la detección automatizada de datos confidenciales.

Error de clasificación: cifrado no válido

Este tipo de error de clasificación se produce si Macie intenta analizar un objeto de un bucket de S3 y el objeto está cifrado con una clave proporcionada por el cliente. El objeto utiliza el cifrado SSE-C, lo que significa que Macie no puede recuperar ni analizar el objeto.

Detalles

Amazon S3 admite varias opciones de cifrado para los objetos S3. En la mayoría de estas opciones, Macie puede descifrar un objeto mediante el rol vinculado al servicio de Macie de su cuenta. Sin embargo, esto depende del tipo de cifrado utilizado.

Para que Macie pueda descifrar un objeto de S3, el objeto debe estar cifrado con una clave a la que Macie pueda acceder y que Macie pueda usar. Si un objeto está cifrado con una clave proporcionada por el cliente, Macie no puede proporcionar el material clave necesario para recuperar el objeto de Amazon S3. En consecuencia, Macie no puede analizar el objeto y el estado del análisis del objeto es Omitido (`SKIPPED`).

Asesoramiento de corrección

Para corregir este error, cifre los objetos S3 con claves administradas o claves AWS Key Management Service (AWS KMS) de Amazon S3. Si prefiere usar AWS KMS claves, las claves pueden ser claves de KMS AWS administradas o claves de KMS administradas por el cliente que Macie puede usar.

Para cifrar los objetos de S3 existentes con claves a las que Macie pueda acceder y utilizar, puede cambiar la configuración de cifrado de los objetos. Para cifrar objetos nuevos con claves a las que Macie pueda acceder y utilizar, cambie la configuración de cifrado predeterminada del

bucket de S3. Asegúrese también de que la política del bucket no exija que los objetos nuevos se cifren con una clave proporcionada por el cliente.

Si no corrige este error, Macie intentará analizar otros objetos del bucket de S3. Si Macie analiza otro objeto correctamente, actualizará los datos de cobertura y demás información que proporcione sobre el bucket.

Referencia adicional

Para obtener información sobre los requisitos y las opciones para usar Macie para analizar objetos de S3 cifrados, consulte Análisis de objetos de Amazon S3 cifrados con Amazon Macie. Para obtener información sobre las opciones de cifrado y la configuración de los buckets de S3, consulte la protección de los datos con cifrado y la configuración del comportamiento de cifrado del servidor para los buckets de S3 predeterminado en la guía del usuario de Amazon Simple Storage Service.

Error de clasificación: clave KMS no válida

Este tipo de error de clasificación se produce si Macie intenta analizar un objeto de un bucket de S3 y el objeto se cifra con una clave AWS Key Management Service (AWS KMS) que ya no está disponible. Macie no puede recuperar y analizar el objeto.

Detalles

AWS KMS ofrece opciones para deshabilitar y eliminar las opciones gestionadas por el cliente. AWS KMS keys Si un objeto de S3 está cifrado con una clave KMS desactivada, cuya eliminación está programada o ya se ha eliminado, Macie no podrá recuperar ni descifrar el objeto. En consecuencia, Macie no puede analizar el objeto y el estado del análisis del objeto es Omitido (`SKIPPED`). Para que Macie pueda analizar un objeto cifrado, el objeto debe estar cifrado con una clave a la que Macie pueda acceder y que Macie pueda usar.

Asesoramiento de corrección

Para corregir este error, vuelva a activar o cancele la eliminación programada de la AWS KMS key aplicable, dependiendo del estado actual de la clave. Si la clave correspondiente ya se ha eliminado, este error no se puede corregir.

Para determinar cuál se AWS KMS key utilizó para cifrar un objeto de S3, puede empezar por utilizar Macie para revisar la configuración de cifrado del lado del servidor para el bucket de S3. Si la configuración de cifrado predeterminada del bucket está configurada para utilizar una clave

KMS, los detalles del bucket indican qué clave se utiliza. A continuación, puede comprobar el estado de esa clave. Como alternativa, puede utilizar Amazon S3 para revisar la configuración de cifrado del bucket y los objetos individuales del bucket.

Si no corrige este error, Macie intentará analizar otros objetos del bucket de S3. Si Macie analiza otro objeto correctamente, actualizará los datos de cobertura y demás información que proporcione sobre el bucket.

Referencia adicional

Para obtener información sobre el uso de Macie para revisar la configuración de cifrado del lado del servidor de un bucket de S3, consulte Revisión de los detalles de los bucket de S3. Para obtener información sobre cómo volver a habilitar o cancelar la eliminación programada de un elemento AWS KMS key, consulte Habilitar y deshabilitar claves y Programar y cancelar la eliminación de claves en la Guía para desarrolladores.AWS Key Management Service

Error de clasificación: permiso denegado

Este tipo de error de clasificación se produce si Macie intenta analizar un objeto de un bucket de S3 y Macie no puede recuperarlo ni descifrarlo debido a la configuración de permisos del objeto o a la configuración de permisos de la clave que se utilizó para cifrar el objeto. Macie no puede recuperar y analizar el objeto.

Detalles

Este error suele producirse porque un objeto de S3 está cifrado con una clave AWS Key Management Service (AWS KMS) administrada por el cliente que Macie no puede utilizar. Si un objeto se cifra con una clave gestionada por el cliente AWS KMS key, la política de la clave debe permitir a Macie descifrar los datos mediante la clave.

Este error también puede producirse si la configuración de permisos de Amazon S3 impide que Macie recupere un objeto de S3. La política de bucket para el bucket de S3 puede restringir el acceso a objetos de bucket específicos o permitir que solo determinadas entidades principales (usuarios, cuentas, servicios u otras entidades) accedan a los objetos. O bien, la lista de control de acceso (ACL) de un objeto puede restringir el acceso a ese objeto. En consecuencia, es posible que a Macie no se le permita acceder al objeto.

Para cualquiera de los casos precedentes, Macie no puede recuperar y analizar el objeto y el estado del análisis del objeto es Omitido (`SKIPPED`).

Asesoramiento de corrección

Para corregir este error, determine si el objeto de S3 está cifrado con una AWS KMS key administrada por el cliente. Si es así, asegúrese de que la política de claves permita al rol vinculado al servicio de Macie (`AWSServiceRoleForAmazonMacie`) para descifrar los datos con la clave. La forma en que se permita este acceso depende de si la cuenta propietaria AWS KMS key también es propietaria del depósito de S3 que almacena el objeto. Si la misma cuenta es propietaria de la clave KMS y del bucket, el usuario de la cuenta debe actualizar la política de claves. Si una cuenta es propietaria de la clave KMS y otra cuenta es propietaria del bucket, el usuario de la cuenta propietaria de la clave debe permitir el acceso entre cuentas a la clave.

> **Tip**
>
> Puedes generar automáticamente una lista de todos los clientes gestionados a los AWS KMS keys que Macie necesita acceder para analizar los objetos de los depósitos de S3 de tu cuenta. Para ello, ejecute el script AWS KMS Permission Analyzer, que está disponible en el repositorio de Amazon Macie Scripts en. GitHub El script también puede generar un script adicional de comandos AWS Command Line Interface (AWS CLI). Si lo desea, puede ejecutar esos comandos para actualizar las políticas y los ajustes de configuración necesarios para las claves de KMS que especifique.

Si a Macie ya se le permite usar el objeto correspondiente AWS KMS key o si el objeto S3 no está cifrado con una clave KMS gestionada por el cliente, asegúrese de que la política del bucket permita a Macie acceder al objeto. Compruebe también que la ACL del objeto permite a Macie leer los datos y metadatos del objeto.

Para la política de bucket, puede permitir este acceso añadiendo una condición para el rol vinculado al servicio de Macie a la política. La condición debe impedir que el rol vinculado al servicio de Macie coincida con la restricción `Deny` de la política. Para ello, puede utilizar la clave de contexto de la condición global `aws:PrincipalArn` y el nombre de recurso de Amazon (ARN) del rol vinculado al servicio de Macie para su cuenta.

En el caso de la ACL del objeto, puedes permitir este acceso si trabajas con el propietario del objeto para que te añada Cuenta de AWS como cesionario con `READ` los permisos para el objeto. A continuación, Macie puede utilizar el rol vinculado al servicio de su cuenta para recuperar y analizar el objeto. Considere también la posibilidad de cambiar la configuración de propiedad

del objeto para el bucket. Puede usar esta configuración para deshabilitar las ACL de todos los objetos del bucket y conceder permisos de propiedad a la cuenta propietaria del bucket.

Si no corrige este error, Macie intentará analizar otros objetos del bucket de S3. Si Macie analiza otro objeto correctamente, actualizará los datos de cobertura y demás información que proporcione sobre el bucket.

Referencia adicional

Para obtener más información sobre cómo permitir que Macie descifre datos con una AWS KMS key administrada por el cliente, consulte Permitir que Amazon Macie utilice un sistema gestionado por el cliente AWS KMS key. Para obtener información sobre cómo actualizar una política de bucket de S3 para permitir que Macie acceda a un bucket, consulte Permitir a Amazon Macie el acceso a buckets y objetos de S3.

Para obtener información sobre cómo modificar una política de claves, consulte Cambiar una política de claves en la AWS Key Management Service Guía para desarrolladores. Para obtener información sobre el uso del cifrado de objetos S3 gestionado AWS KMS keys por el cliente, consulte Uso del cifrado del lado del servidor con AWS KMS claves en la Guía del usuario de Amazon Simple Storage Service.

Para obtener más información acerca del uso de políticas de buckets para controlar el acceso a buckets de S3, consulte Uso de políticas de bucket y políticas de usuario y Cómo Amazon S3 autoriza una petición en la Guía del usuario de Amazon Simple Storage Service. Para obtener información sobre el uso de las ACL o la configuración de propiedad de los objetos para controlar el acceso a los objetos de S3, consulte Administración del acceso con las ACL y Control de la propiedad de los objetos y deshabilitación de las ACL de su bucket en la Guía del usuario de Amazon Simple Storage Service.

No clasificable

Este problema indica que todos los objetos de un bucket de S3 se almacenan utilizando clases de almacenamiento de Amazon S3 no compatibles o formatos de archivo o almacenamiento no compatibles. Macie no puede analizar ningún objeto del bucket.

Detalles

Para poder ser seleccionado y analizado, un objeto de S3 debe utilizar una clase de almacenamiento de Amazon S3 compatible con Macie. El objeto también debe tener una extensión de nombre de archivo para un archivo o formato de almacenamiento que Macie admita.

Si un objeto no cumple estos criterios, se trata como un objeto no clasificable. Macie no intenta extraer ni analizar los datos en objetos no clasificables.

Si todos los objetos de un bucket de S3 son objetos no clasificables, el bucket total es un bucket no clasificable. Macie no puede realizar una detección de datos confidenciales automatizada para el bucket.

Asesoramiento de corrección

Para solucionar este problema, revise las reglas de configuración del ciclo de vida y otros ajustes que determinan qué clases de almacenamiento se utilizan para almacenar objetos en el bucket de S3. Considere la posibilidad de ajustar esa configuración para utilizar las clases de almacenamiento compatibles con Macie. También puede cambiar la clase de almacenamiento de los objetos existentes en el bucket.

Evalúa también los formatos de archivo y de almacenamiento de los objetos existentes en el bucket de S3. Para analizar los objetos, considere la posibilidad de transferir los datos, de forma temporal o permanente, a objetos nuevos que utilicen un formato compatible.

Si se añaden objetos al bucket de S3 y utilizan una clase y un formato de almacenamiento compatibles, Macie los detectará la próxima vez que evalúe el inventario del bucket. Cuando esto suceda, Macie dejará de informar de que el bucket no clasificable en las estadísticas, los datos de cobertura y otra información que proporciona sobre sus datos de Amazon S3. Además, los nuevos objetos tendrán mayor prioridad para el análisis durante un ciclo de análisis posterior.

Referencia adicional

Para obtener información sobre las clases de almacenamiento de Amazon S3 y los formatos de archivo y almacenamiento compatibles con Macie, consulteClases y formatos de almacenamiento compatibles con Amazon Macie. Para obtener información sobre las reglas de configuración del ciclo de vida y las opciones de clases de almacenamiento que ofrece Amazon S3, consulte Administración del ciclo de vida del almacenamiento y Uso de las clases de almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Revisión de las estadísticas y los resultados de la detección automatizada de datos confidenciales

Cuando se habilita la detección automática de datos confidenciales en su cuenta, Amazon Macie genera y mantiene automáticamente datos de inventario adicionales, estadísticas y otra información sobre los depósitos de uso general del Amazon Simple Storage Service (Amazon S3) que supervisa

y analiza para su cuenta. Si es el administrador de Macie de una organización, esto incluye los buckets de S3 que son propiedad de sus cuentas de miembro.

La información adicional recoge los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para su cuenta. También complementa otra información que Macie proporciona sobre sus datos de Amazon S3, como la configuración de acceso público y acceso compartido para buckets de S3 individuales. Además de los metadatos y las estadísticas, Macie genera registros de los datos confidenciales que encuentra y de los análisis que realiza (tanto los datos confidenciales como los resultados del descubrimiento de datos confidenciales).

A medida que la detección automatizada de datos confidenciales analiza el progreso de su cuenta, las siguientes funciones y datos pueden ayudarle a revisar y evaluar los resultados:

- Panel de resumen: proporciona estadísticas agregadas del patrimonio de datos de Amazon S3. Las estadísticas incluyen datos de métricas clave, como el número total de buckets en los que Macie ha encontrado datos confidenciales y cuántos de esos grupos son de acceso público. También informan de problemas que afectan a la cobertura de sus datos de Amazon S3.
- Mapa de calor de buckets de S3: proporciona una representación visual interactiva de la confidencialidad de los datos en todo el patrimonio de datos, agrupados por Cuenta de AWS. Para cada cuenta, el mapa incluye estadísticas de confidencialidad agregadas y utiliza colores para indicar la puntuación de confidencialidad actual de cada segmento que posee la cuenta. El mapa también utiliza símbolos para ayudarle a identificar los buckets que son de acceso público, los que Macie no puede analizar, etc.
- Tabla de buckets de S3: proporciona información resumida de cada uno de los buckets de S3 de su inventario. Para cada bucket, la tabla incluye datos como el nombre del bucket y la puntuación de confidencialidad actual, la cantidad de objetos que Macie puede analizar en el bucket y si ha configurado algún trabajo de detección de datos confidenciales para analizar periódicamente los objetos del bucket. Puede exportar los datos de la tabla a un archivo de valores separados por comas (CSV).
- Panel de detalles: proporciona detalles y estadísticas de un segmento de S3 que elija en la tabla o el mapa de calor. Los detalles incluyen una lista de los objetos que Macie ha analizado en el bucket y un desglose de los tipos y el número de apariciones de datos confidenciales que Macie ha encontrado en el bucket. También puede usar el panel para administrar la configuración de detección automática de un depósito.
- Resultados de datos confidenciales: proporciona informes detallados de los datos confidenciales que Macie encuentra en objetos S3 individuales. Los detalles incluyen cuándo ha encontrado

Macie los datos confidenciales y los tipos y el número de ocurrencias de los datos confidenciales que ha encontrado Macie. Los detalles también incluyen información sobre el bucket y el objeto de S3 afectados, incluida la configuración de acceso público del bucket y la fecha en que se modificó el objeto por última vez.

- Resultados de la detección de datos confidenciales: proporciona registros del análisis que Macie realiza para objetos S3 individuales. Esto incluye objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no produce resultados de datos confidenciales y objetos que Macie no puede analizar debido a problemas o errores.

Con estos datos, puede evaluar la confidencialidad de los datos en todo su patrimonio de datos de Amazon S3 y profundizar para evaluar e investigar los buckets y objetos individuales de S3. Junto con la información que Macie proporciona sobre la seguridad y la privacidad de sus datos de Amazon S3, también puede identificar los casos en los que podría ser necesaria una solución inmediata, por ejemplo, un bucket de acceso público en el que Macie encontró datos confidenciales.

Los datos adicionales pueden ayudarlo a evaluar y monitorear la cobertura de su patrimonio de datos de Amazon S3. Con los datos de cobertura, puede comprobar el estado de los análisis de su patrimonio de datos en general y de los buckets de S3 individuales de su inventario de buckets. También puede identificar los problemas que impidieron que Macie analizara objetos en buckets específicos. Si soluciona los problemas, puede aumentar la cobertura de sus datos de Amazon S3 durante los ciclos de análisis posteriores. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatizada.

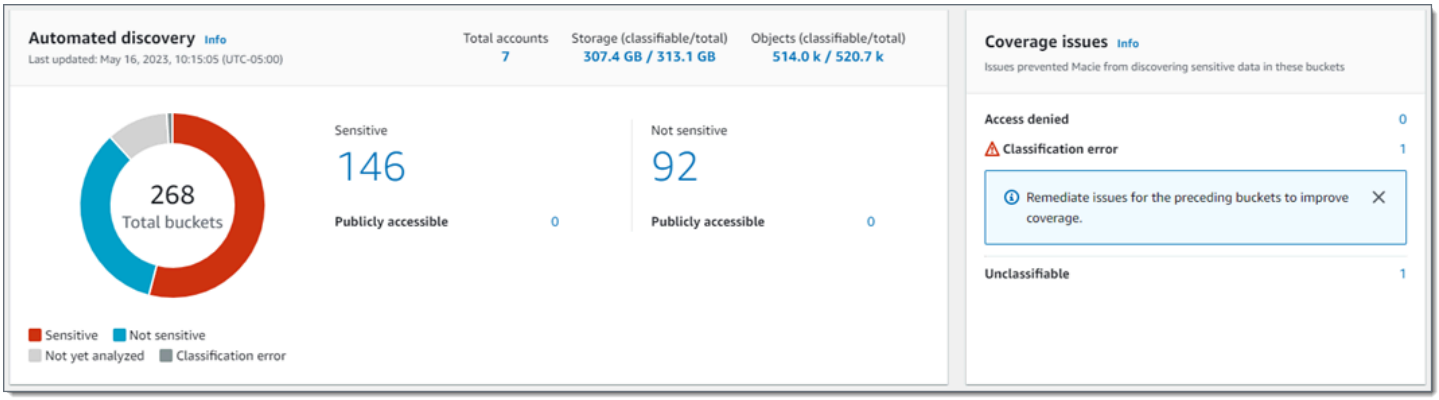
Temas

Revisión de estadísticas agregadas de confidencialidad de los datos en el panel de resumen

En la consola de Amazon Macie, el panel de Resumen proporciona una instantánea de las estadísticas agregadas y los datos de resultados de sus datos de Amazon Simple Storage Service (Amazon S3) en el Región de AWS actual. Está diseñado para ayudarle a evaluar la seguridad general de sus datos de Amazon S3.

Las estadísticas del panel de control incluyen datos sobre métricas de seguridad clave, como la cantidad de depósitos de uso general de S3 a los que se puede acceder públicamente o que se comparten con otros Cuentas de AWS usuarios. El panel también muestra grupos de datos de hallazgos agregados de su cuenta, por ejemplo, los grupos que generaron más hallazgos durante los siete días anteriores. Si es el administrador de Macie de una organización, el panel proporciona estadísticas y datos agregados de todas las cuentas de su organización. Si lo desea, puede filtrar los datos por cuenta.

Si la detección automatizada de datos confidenciales está habilitada en su cuenta, el panel de Resumen incluye estadísticas de detección automatizada de datos confidenciales. Las estadísticas recopilan el estado y los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para sus datos de Amazon S3. Por ejemplo:



Las estadísticas de la sección Descubrimiento automatizado proporcionan una instantánea del estado actual y los resultados de las actividades automatizadas de descubrimiento de datos confidenciales. Los datos no incluyen los resultados de los trabajos de descubrimiento de datos confidenciales que haya creado y ejecutado.

Las estadísticas de la sección Problemas de cobertura indican si los problemas impiden que Macie analice los objetos en buckets de S3 individuales. Estas estadísticas no incluyen de forma explícita los datos de los trabajos de descubrimiento de datos confidenciales que usted haya creado y

ejecutado. Sin embargo, si corrige los problemas de cobertura que afectan a los resultados de la detección automática de datos confidenciales, es probable que también aumente la cobertura de los trabajos que ejecute posteriormente.

Temas

Mostrar el panel Resumen

Siga estos pasos para mostrar el panel Resumen en la consola de Amazon Macie.
Si prefiere consultar las estadísticas mediante programación, puede utilizar el GetBucketStatisticsfuncionamiento de la API de Amazon Macie.

Para mostrar el panel Resumen

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Resumen. Macie muestra el panel Resumen.
3. Para profundizar y revisar los datos de respaldo de un elemento del panel de control, selecciónelo.

Si es el administrador de Macie de una organización, el panel muestra estadísticas y datos agregados de su cuenta y de las cuentas de miembros de la organización. Para filtrar el panel y mostrar los datos solo para una cuenta determinada, especifique el ID de cuenta en el cuadro Cuenta en la parte superior del panel..

Conozca las estadísticas de detección automatizada de datos confidenciales en el panel Resumen

El panel Resumen de la consola de Amazon Macie incluye estadísticas agregadas que pueden ayudarle a supervisar la detección automatizada de datos confidenciales para sus datos de Amazon S3. Por ejemplo, puede utilizar las estadísticas del panel de control para determinar rápidamente en cuántos buckets de S3 Amazon Macie ha encontrado datos confidenciales y cuántos de esos buckets son de acceso público. El panel proporciona una instantánea del estado actual y los resultados de los análisis de sus datos de Amazon S3 en la actualidad Región de AWS.

También puede utilizar las estadísticas del panel para evaluar la cobertura de sus datos de Amazon S3 e identificar los problemas que impiden que Macie analice los objetos en buckets de S3

individuales. Por ejemplo, puede determinar a cuántos buckets no puede acceder Macie para su cuenta.

En el panel, las estadísticas de detección automatizada de datos confidenciales se organizan principalmente en las siguientes secciones:

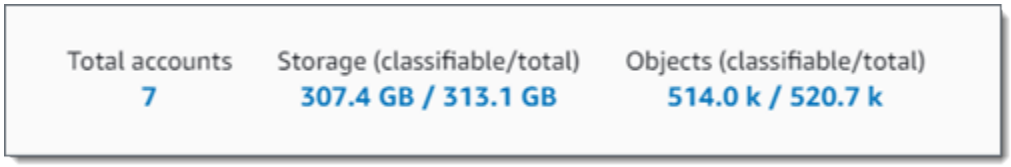
- Almacenamiento y detección de datos confidenciales
- Detección automatizada
- Problemas de cobertura

Al revisar cada sección, si lo desea, elija un elemento para desglosar y revisar los datos de respaldo. Tenga en cuenta también que el panel de control no incluye datos de los buckets de directorios de S3, solo de los buckets de uso general. Macie no monitorea ni analiza los depósitos de directorios.

Las estadísticas individuales de cada sección son las siguientes. Para obtener información sobre las estadísticas de otras secciones del panel Resumen, consulte Descripción de los componentes del panel Resumen.

Almacenamiento y detección de datos confidenciales

En la parte superior de la sección Detección automatizada, encontrará estadísticas que indican la cantidad de datos que almacena en Amazon S3 y la cantidad de esos datos que Macie puede analizar para detectar datos confidenciales. Por ejemplo:



En esta sección:

- Total de cuentas: el número total de grupos Cuentas de AWS que poseen en tu inventario de cubos. Si es el administrador de Macie de una organización, este es el número total de cuentas de Macie que administra para su organización. Si tiene una cuenta Macie independiente, este valor es 1.
- Almacenamiento: estas métricas proporcionan información sobre el tamaño de almacenamiento de los objetos de su inventario de buckets:
  - Clasificable: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar en los buckets.

- Total: el tamaño total de almacenamiento de todos los objetos de los buckets, incluidos los objetos que Macie no puede analizar.

Si alguno de los objetos son archivos comprimidos, estos valores no reflejan el tamaño real de esos archivos una vez descomprimidos. Si el control de versiones está habilitado para alguno de los buckets, estos valores se basan en el tamaño de almacenamiento de la última versión de cada objeto de esos buckets.

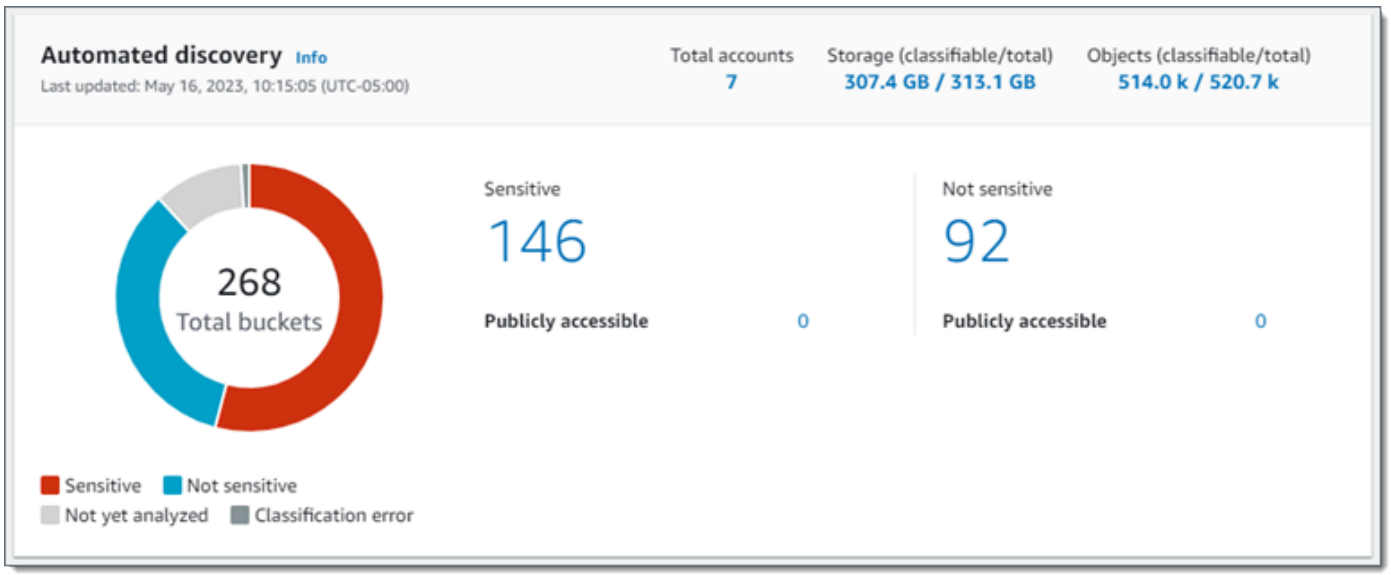
- Objetos: estas métricas ofrecen información sobre el número de objetos en su inventario de buckets:
  - Clasificable el número total de objetos que Macie puede analizar en los buckets.
  - Total: el número total de objetos de los buckets, incluidos los objetos que Macie no puede analizar.

En las estadísticas anteriores, los objetos son clasificables si utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Puede detectar datos confidenciales en los objetos mediante Macie. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

Tenga en cuenta que las estadísticas de Almacenamiento y Objetos no incluyen datos sobre los objetos de los buckets a los que Macie no puede acceder. Para identificar los grupos en los que este es el caso, seleccione la estadística de Acceso denegado en la sección Problemas de cobertura del panel.

Detección automatizada

Las estadísticas recopilan el estado y los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para sus datos de Amazon S3. Por ejemplo:



Las estadísticas individuales de esta sección son las siguientes.

Total de buckets

El gráfico de anillos indica el número total de cubos en tu inventario de cubos. El gráfico agrupa los buckets en categorías en función de la puntuación de confidencialidad actual de cada uno de ellos:

- Confidencial (rojo): el número total de buckets cuya puntuación de confidencialidad oscila entre 51 y 100.
- No confidencial (azul): el número total de buckets cuya puntuación de confidencialidad oscila entre 1 y 49.
- Aún no se ha analizado (gris claro): el número total de buckets cuya puntuación de confidencialidad es 50.
- Error de clasificación (gris oscuro): número total de buckets cuya puntuación de confidencialidad es -1.

Para obtener más información sobre el rango de puntuaciones y etiquetas de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.

Para revisar las estadísticas adicionales de un grupo, coloque el cursor sobre el grupo:

- Buckets: el número total de buckets
- Accesible públicamente: el número total de compartimentos que permiten al público en general tener acceso de lectura o escritura al bucket.

- Bytes clasificables: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar en los buckets. Estos objetos utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.
- Total de bytes: el tamaño total de almacenamiento de todos los buckets.

En las estadísticas anteriores, los valores del tamaño de almacenamiento se basan en el tamaño de almacenamiento de la última versión de cada objeto de los buckets. Si alguno de los objetos son archivos comprimidos, estos valores no reflejan el tamaño real de esos archivos una vez descomprimidos.

Confidencial

Esta área indica el número total de cubos que actualmente tienen una puntuación de sensibilidad que va de 51 a 100. Dentro de este grupo, el término Acceso público indica el número total de buckets que también permiten al público en general tener acceso de lectura o escritura al bucket.

No confidencial

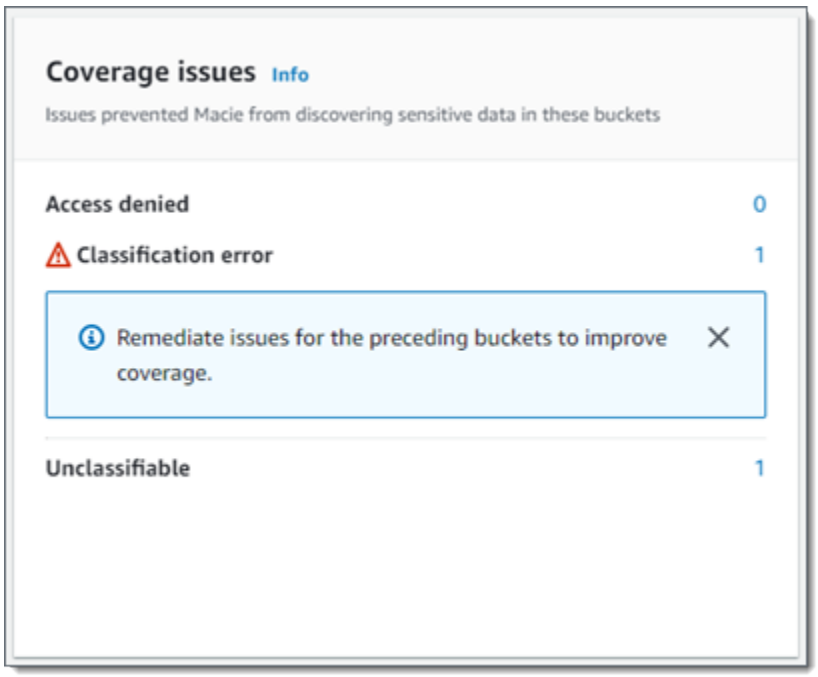
Esta área indica el número total de cubos que actualmente tienen una puntuación de sensibilidad que va de 1 a 49. Dentro de este grupo, el término Acceso público indica el número total de buckets que también permiten al público en general tener acceso de lectura o escritura al bucket.

Para determinar y calcular los valores de las estadísticas de Acceso público, Macie analiza una combinación de ajustes a nivel de cuenta y de bucket para cada grupo, como la configuración de bloqueo del acceso público para la cuenta y el bucket, y la política del bucket para el grupo. Para obtener más información, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.

Tenga en cuenta que las estadísticas de la sección Descubrimiento automatizado no incluyen los resultados de los trabajos de descubrimiento de datos confidenciales que haya creado y ejecutado.

Problemas de cobertura

Estas estadísticas indican si ciertos tipos de problemas impiden que Macie analice los objetos de los buckets S3 individuales. Por ejemplo:



En esta sección:

- Acceso denegado: el número total de buckets a los que Macie no puede acceder. Macie no puede analizar ningún objeto de estos buckets. La configuración de permisos de los buckets impide que Macie acceda a los buckets y a los objetos de los buckets.
- Error de clasificación: el número total de buckets que Macie aún no ha analizado debido a errores de clasificación a nivel de objeto. Macie intentó analizar uno o más objetos de estos buckets. Sin embargo, Macie no pudo analizar los objetos debido a problemas con la configuración de los permisos a nivel de objeto, el contenido de los objetos o las cuotas.
- No clasificable: el número total de buckets que no almacenan ningún objeto clasificable. Macie no puede analizar ningún objeto de estos buckets. Todos los objetos utilizan clases de almacenamiento de Amazon S3 que Macie no admite o tienen extensiones de nombre de archivo para formatos de archivo o almacenamiento que Macie no admite.

Elija el valor de una estadística para mostrar detalles adicionales y, según proceda, una guía de corrección. Si soluciona los problemas de acceso y los errores de clasificación, puede aumentar la cobertura de sus datos de Amazon S3 durante los ciclos de análisis posteriores. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatizada.

Tenga en cuenta que las estadísticas de la sección Problemas de cobertura no incluyen de forma explícita los datos de los trabajos de descubrimiento de datos confidenciales que haya creado y ejecutado. Sin embargo, si corrige los problemas de cobertura que afectan a los resultados de la

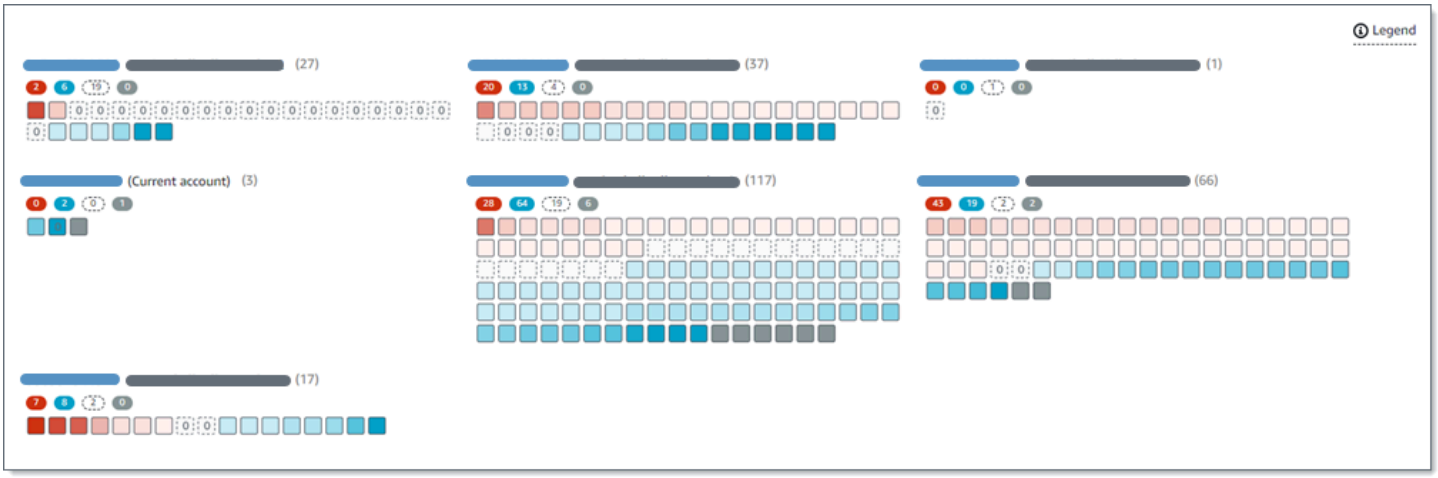
detección automática de datos confidenciales, es probable que también aumente la cobertura de los trabajos que ejecute posteriormente.

Para obtener información sobre otras secciones del panel de Resumen, consulteDescripción de los componentes del panel Resumen.

Visualización de la confidencialidad de los datos con el mapa de buckets de S3

En la consola de Amazon Macie, el mapa de calor de los buckets S3 proporciona una representación visual interactiva de la confidencialidad de los datos en todo el patrimonio de datos de Amazon Simple Storage Service (Amazon S3) en el estado actual. Región de AWS La información adicional recoge los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para su cuenta.

Si es el administrador de Macie de una organización, el mapa incluye los resultados de los segmentos de S3 que son propiedad de sus cuentas de miembros. Los datos se agrupan Cuenta de AWS y ordenan por ID de cuenta. Por ejemplo:



Cada página del mapa muestra los datos de hasta 99 cuentas o 1000 buckets, en función del tamaño de la organización o del patrimonio de datos de Amazon S3.

Para mostrar el mapa, elija Buckets de S3 en el panel de navegación de la consola. Luego, elija mapa
( )
en la parte superior de la página. El mapa solo está disponible si la detección automatizada de datos confidenciales está habilitada actualmente en su cuenta. No incluye los resultados de los trabajos de detección de datos confidenciales que haya creado y ejecutado.

Temas

Interpretación de los datos del mapa de buckets de S3

En el mapa de cubos de S3, cada cuadrado representa un grupo de uso general de S3 en tu inventario de cubos. El color de un cuadrado representa la puntuación de confidencialidad actual de un bucket, que mide la intersección de dos dimensiones principales: la cantidad de datos confidenciales que Macie ha encontrado en el bucket y la cantidad de datos que Macie ha analizado en el bucket. La intensidad del tono del color representa el lugar en el que se sitúa la puntuación de un bucket en un rango de valores de confidencialidad de datos, como se muestra en la siguiente imagen.

En general, puede interpretar la intensidad del color y el matiz de la siguiente manera:

- Azul: si la puntuación de confidencialidad actual de un bucket va de 1 a 49, el cuadrado del bucket es azul y la etiqueta de confidencialidad del bucket es No confidencial. La intensidad del tono azul refleja el número de objetos únicos que Macie ha analizado en el bucket en relación con el número total de objetos únicos del bucket. Un tono más oscuro indica una puntuación de confidencialidad más baja.
- Sin color: si la puntuación de confidencialidad actual de un bucket es 50, el cuadrado del bucket no está coloreado y la etiqueta de confidencialidad del bucket no se ha analizado aún. Además, el cuadrado tiene un borde discontinuo.
- Rojo: si la puntuación de confidencialidad actual de un bucket oscila entre 51 y 100, el cuadrado del bucket es rojo y la etiqueta de confidencialidad del bucket es Confidencial. La intensidad del tono rojo refleja la cantidad de datos confidenciales que Macie ha encontrado en el bucket. Un tono más oscuro indica una puntuación de confidencialidad más alta.
- Gris: si la puntuación de confidencialidad actual de un bucket es -1, el cuadrado del bucket es de color gris oscuro y la etiqueta de confidencialidad del bucket es un error de clasificación. La intensidad del tono no varía.

Para obtener más información sobre el rango de puntuaciones y etiquetas de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.

En el mapa, el cuadrado de un bucket S3 también puede contener un símbolo. El símbolo indica un error, un problema u otro tipo de consideración que podría afectar a la evaluación de la confidencialidad de un bucket. Un símbolo también puede indicar un posible problema con la seguridad del bucket; por ejemplo, el bucket es de acceso público. En la siguiente tabla se enumeran los símbolos que Macie utiliza para avisarle de estos casos.

Símbolo	Definición	Descripción
	Acceso denegado	A Macie no se le permite acceder al bucket ni a los objetos del bucket. En consecuencia, Macie no puede analizar ningún objeto del bucket. Este problema suele producirse porque un bucket tiene una política de bucket restrictiva. Para obtener información acerca de cómo resolver este problema, consulte Permitir a Macie el acceso a buckets y objetos de S3.
	Publicly accessible (Accesible públicamente)	El público en general tiene acceso de lectura o escritura al bucket. Para determinar esto, Macie analiza una combinación de ajustes a nivel de cuenta y de bucket para cada grupo, como la configuración de bloqueo del acceso público para la cuenta y el bucket, y la política

Símbolo	Definición	Descripción
		del bucket para el bucket. Para obtener más informaci ón, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.
	No clasificable	Macie no puede analizar ningún objeto del bucket. Todos los objetos del bucket utilizan clases de almacenam iento de Amazon S3 que Macie no admite o tienen extensiones de nombre de archivo para formatos de archivo o almacenamiento que Macie no admite. Para que Macie pueda analizar un objeto, el objeto debe utilizar una clase de almacenamiento compatibl e y tener una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.
	Cero bytes	El depósito no almacena ningún objeto para que Macie lo analice. El bucket está vacío o todos los objetos del bucket contienen cero (0) bytes de datos.

Interactúa con el mapa de buckets de S3

Al revisar el mapa de buckets de S3, podrá interactuar con él de diferentes maneras para revelar y evaluar datos y detalles adicionales de cuentas y buckets individuales. Siga estos pasos para mostrar el mapa en la consola de Amazon Macie e interactuar con las diversas características que ofrece el mapa.

Para interactuar con el mapa de buckets de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3. La página de buckets de S3 muestra un mapa de su inventario de buckets. Si la página muestra su inventario en formato tabular, seleccione map () en la parte superior de la página.
3. En la parte superior de la página, si lo desea, seleccione Actualizar () para recuperar los metadatos del bucket más recientes de Amazon S3.
4. En el mapa de buckets de S3, realice una de las siguientes acciones:

   - Para determinar cuántos cubos tienen una etiqueta de sensibilidad específica, consulta las insignias de colores que hay justo debajo de la identificación. Cuenta de AWS Las insignias muestran el recuento total de buckets, desglosado por etiqueta de confidencialidad.

     Por ejemplo, la insignia roja indica el número total de buckets que son propiedad de la cuenta y que tienen la etiqueta de Confidencial. La puntuación de confidencialidad de estos buckets oscila entre 51 y 100. La insignia azul indica el número total de buckets que son propiedad de la cuenta y que tienen la etiqueta de No confidencial. La puntuación de confidencialidad de estos buckets oscila entre 1 y 49.
   - Para revisar un subconjunto de información sobre un bucket, coloca el cursor sobre el cuadrado del bucket. En una ventana emergente se muestra el nombre del bucket y la puntuación de confidencialidad actual.

     La ventana emergente también muestra el número total de objetos que Macie puede analizar en el bucket y el tamaño total de almacenamiento de la última versión de esos objetos. Estos objetos son clasificables. Los objetos son clasificables si utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo

o formato de almacenamiento admitido. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

- Para filtrar el mapa y mostrar solo los buckets que tienen un valor específico para un campo, coloque el cursor en el cuadro de filtro y, a continuación, añada una condición de filtro para el campo. Macie aplica los criterios de la condición y muestra la condición debajo del cuadro de filtro. Para refinar aún más los resultados, añada condiciones de filtro para campos adicionales. Para obtener más información, consulte Filtrar el inventario de su bucket de S3.
- Para desglosar y mostrar solo los grupos que pertenecen a una cuenta en particular, elija el ID de cuenta de la cuenta. Macie abre una nueva pestaña que filtra y muestra los datos únicamente de esa cuenta.

5. Para revisar todas las estadísticas de detección de datos confidenciales y otra información que Macie proporciona sobre un segmento en particular, seleccione el cuadrado del bucket y, a continuación, consulte el panel de detalles. Para obtener más información, consulte Revisión de los detalles de confidencialidad de los datos de los buckets S3 individuales.

> **Tip**
>
> En la pestaña Detalles del bucket del panel, puede desplazarse y profundizar en muchos de los campos. Para mostrar los buckets que tienen el mismo valor para un campo, elija
>
> en el campo. Para mostrar los buckets que tienen otros valores para un campo, elija
>
> en el campo.

Evaluación de la confidencialidad de los datos con la tabla de buckets S3

En la consola de Amazon Macie, la tabla de buckets S3 muestra información resumida sobre cada uno de los buckets de uso general de Amazon Simple Storage Service (Amazon S3) actuales. Región de AWS Si es el administrador de Macie de una organización, esto incluye información sobre los depósitos que poseen las cuentas de sus miembros. Si prefiere acceder a los datos mediante programación, puede utilizar el DescribeBucketsfuncionamiento de la API de Amazon Macie.

En la consola, puede ordenar y filtrar la tabla para personalizar la vista. Si lo desea, puede exportar los datos de la tabla a un archivo de valores separados por comas (CSV). Si elige un bucket de S3 en la tabla, el panel de detalles muestra información adicional sobre el bucket. Esto incluye detalles y estadísticas que recopilan los resultados de las actividades de detección automatizada de datos

confidenciales que Macie ha realizado para el bucket hasta el momento. También incluye datos para la configuración y las métricas que proporcionan información sobre la seguridad y la privacidad de los datos del bucket. Además de revisar los detalles de un bucket, puede usar el panel de detalles para ajustar la configuración de detección automatizada de datos confidenciales del bucket. Para saber cómo hacerlo, consulte Gestión de la detección automatizada de datos confidenciales para buckets S3 individuales.

Para evaluar la confidencialidad de los datos mediante la tabla de buckets de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3.
3. En la página de buckets de S3, elija tabla
   ()
   en la parte superior de la página. Macie muestra el número de buckets de su inventario y una tabla con los buckets.
4. En la parte superior de la página, si lo desea, seleccione Actualizar
   ()
   para recuperar los metadatos del bucket más recientes de Amazon S3.

   Si el icono de información
   ()
   aparece junto al nombre de algún bucket, le recomendamos que lo haga. Este icono indica que se creó un bucket durante las últimas 24 horas, posiblemente después de que Macie recuperara por última vez los metadatos del bucket y del objeto de Amazon S3 como parte del ciclo de actualización diario.
5. En la tabla de buckets de S3, consulte la información resumida sobre cada uno de los buckets de su inventario:

   - Confidencialidad: la puntuación de confidencialidad actual del bucket. Para obtener información sobre el rango de puntuaciones de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.
   - Bucket: el nombre del bucket.
   - Cuenta: el ID de cuenta del propietario del Cuenta de AWS depósito.
   - Objetos clasificables: el número total de objetos que Macie puede analizar para detectar datos confidenciales en el bucket.

- Tamaño clasificable: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar para detectar datos confidenciales en el bucket.

  Este valor no refleja el tamaño real de los objetos comprimidos después de descomprimirlos. Además, si el control de versiones está activado para el bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto del bucket.
- Supervisado por el trabajo: si los trabajos de detección de datos confidenciales están configurados para analizar periódicamente los objetos del bucket de forma diaria, semanal o mensual.

  Si el valor de este campo es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.
- Último trabajo ejecutado: si se ha configurado algún trabajo puntual o periódico de descubrimiento de datos confidenciales para analizar los objetos del depósito, este campo indica la fecha y hora más recientes en las que se empezó a ejecutar uno de esos trabajos. De lo contrario, este campo está vacío.

Los objetos son clasificables si utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Puede detectar datos confidenciales en los objetos mediante Macie. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.

6. Para analizar su inventario mediante la tabla, realice alguna de las siguientes acciones:

   - Para ordenar la tabla por un campo específico, elija el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a elegir el encabezado de la columna.
   - Para filtrar la tabla y mostrar solo los buckets que tienen un valor específico para un campo, coloque el cursor en el cuadro de filtro y, a continuación, añada una condición de filtro para el campo. Macie aplica los criterios de la condición y muestra la condición debajo del cuadro de filtro. Para refinar aún más los resultados, añada condiciones de filtro para campos adicionales. Para obtener más información, consulte Filtrar el inventario de su bucket de S3.
   - Para consultar detalles y estadísticas de un bucket en particular, elija el nombre del bucket en la tabla y consulte el panel de detalles. Para obtener más información, consulte Revisión de los detalles del bucket de S3.

> **Tip**
>
> En la pestaña Detalles del bucket del panel, puede desplazarse y profundizar en muchos de los campos. Para mostrar los buckets que tienen el mismo valor para un campo, elija  en el campo. Para mostrar los buckets que tienen otros valores para un campo, elija  en el campo.

7. Para exportar los datos de la tabla a un archivo CSV, active la casilla de verificación de cada fila que desee exportar o active la casilla del encabezado de la columna de selección para seleccionar todas las filas. A continuación, elija Exportar a CSV en la parte superior de la página. Puede exportar hasta 50 000 filas de la tabla.
8. Para realizar un análisis más profundo e inmediato de los objetos de uno o más buckets, active la casilla de verificación de cada grupo y, a continuación, elija Crear trabajo. Para obtener más información, consulte Creación de un trabajo de detección de datos confidenciales.

Revisión de los detalles de confidencialidad de los datos de los buckets S3 individuales

En la consola de Amazon Macie, puede utilizar el panel de detalles de la página de cubos S3 para revisar las estadísticas y otra información sobre cada depósito de uso general de Amazon Simple Storage Service (Amazon S3) que Macie supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, incluirá los buckets que son propiedad de las cuentas miembro.

Las estadísticas y la información incluyen detalles que proporcionan información sobre la seguridad y la privacidad de los datos de un bucket de S3. Si su cuenta tiene habilitada la detección automatizada de datos confidenciales, también se recopilan los resultados de las actividades de detección automatizada de datos confidenciales que Macie ha realizado hasta ahora para un bucket. Por ejemplo, puede encontrar una lista de objetos que Macie ha analizado en un bucket y un desglose de los tipos y el número de apariciones de datos confidenciales que Macie ha encontrado en un bucket. Tenga en cuenta que los datos no incluyen los resultados de los trabajos de detección de datos confidenciales que haya creado y ejecutado.

Macie recalcula y actualiza automáticamente estas estadísticas y detalles mientras detecta automáticamente los datos confidenciales de su cuenta. Por ejemplo:

- Si Macie no encuentra datos confidenciales en un objeto de S3, reduce la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario. Macie también añade el objeto a la lista de objetos que analiza en el bucket.
- Si Macie encuentra datos confidenciales en un objeto de S3, Macie añade esas apariciones al desglose de los tipos de datos confidenciales que Macie ha encontrado en el bucket. Macie también aumenta la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario. Además, Macie añade el objeto a la lista de objetos que analiza en el bucket. Estas tareas se suman a la creación de un resultado de datos confidenciales para el objeto.
- Si Macie encuentra datos confidenciales en un objeto de S3 que posteriormente se modifican o eliminan, Macie elimina las incidencias de datos confidenciales de ese objeto del desglose de tipos de datos confidenciales del bucket. Macie también reduce la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario. Además, Macie elimina el objeto de la lista de objetos que ha analizado en el bucket.
- Si Macie intenta analizar un objeto de S3 pero un problema o error se lo impide, Macie añade el objeto a la lista de objetos que ha analizado en el bucket e indica que no ha podido analizarlo.

Además de revisar las estadísticas y los detalles, puede usar el panel para ajustar la configuración de detección automatizada de datos confidenciales de un bucket de S3. Por ejemplo, puede incluir o excluir tipos específicos de datos confidenciales de la puntuación de un segmento. Para obtener más información, consulte Gestión de la detección automatizada de buckets de S3 individuales.

Para revisar los detalles de confidencialidad de datos de un bucket de S3

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, elija Buckets de S3. La página Buckets de S3 muestra un mapa interactivo de su inventario de buckets. Si lo prefiere, elija tabla () en la parte superior de la página para mostrar el inventario en formato tabular.
3. En el mapa o la tabla Buckets de S3, elija el nombre del bucket de S3 cuyos detalles desee consultar. El panel de detalles muestra estadísticas y otra información sobre el bucket.

En la parte superior del panel se muestra información general sobre el depósito: el nombre del depósito y el identificador de cuenta del propietario del Cuenta de AWS depósito. También ofrece opciones para cambiar determinadas configuraciones de detección automatizada de datos confidenciales para el bucket. Los ajustes e información adicionales sobre el bucket se organizan en las siguientes pestañas:

- Confidencialidad
- Detalles del bucket
- Muestras de objetos
- Detección de datos confidenciales

Los ajustes individuales y la información de cada pestaña son los siguientes.

Confidencialidad

Esta pestaña muestra la puntuación de confidencialidad actual del bucket, que va de -1 a 100. Para obtener información sobre el rango de puntuaciones de confidencialidad que define Macie, consulte Puntuación de confidencialidad para buckets de S3.

La pestaña también proporciona un desglose de los tipos de datos confidenciales que Macie ha encontrado en los objetos del bucket y el número de veces que aparecen cada tipo:

- Tipo de datos confidenciales: el identificador único (ID) del identificador de datos administrados que ha detectado los datos o el nombre del identificador de datos personalizado que ha detectado los datos.

  El ID de un identificador de datos administrados describe el tipo de datos confidenciales que el identificador está diseñado para detectar; por ejemplo, USA_PASSPORT_NUMBER para los números de pasaporte estadounidenses. Para obtener más información sobre cada identificador de datos administrados, consulte. Uso de identificadores de datos administrados
- Recuento: el número total de apariciones de los datos que detectó el identificador de datos administrado o personalizado.
- Estado de la puntuación: especifica si las apariciones de los datos se incluyen o excluyen de la puntuación de confidencialidad del bucket.

  Si ha configurado Macie para que calcule la puntuación del bucket automáticamente, puede ajustar el cálculo incluyendo o excluyendo tipos específicos de datos confidenciales de la puntuación del bucket: seleccione la casilla de verificación del identificador de datos que desee

incluir o excluir y, a continuación, elija la opción que desee en el menú Acciones. Para obtener más información, consulte Gestión de la detección automatizada de buckets de S3 individuales.

Si Macie no ha encontrado datos confidenciales en los objetos que el bucket almacena actualmente, en esta sección se muestra el mensaje No se encontraron detecciones.

Tenga en cuenta que la pestaña Confidencialidad no incluye los datos de los objetos que Macie analizó y que posteriormente se modificaron o eliminaron. Si los objetos se modifican o eliminan de un bucket después de analizarlos, Macie recalcula y actualiza automáticamente las estadísticas y los datos correspondientes para excluir los objetos.

Detalles del bucket

Esta pestaña proporciona detalles sobre la configuración del bucket, incluida la configuración de seguridad y privacidad de los datos. Por ejemplo, puede revisar los desgloses de la configuración de acceso público del bucket y determinar si el bucket replica objetos o se comparte con otros Cuentas de AWS.

Cabe destacar que el campo Última actualización indica cuándo Macie recuperó por última vez los metadatos del bucket o de los objetos del bucket de Amazon S3. El campo Última ejecución de detección automatizada indica cuándo Macie analizó por última vez los objetos del bucket mientras realizaba una detección automatizada.

La pestaña también proporciona estadísticas a nivel de objeto que pueden ayudarle a evaluar la cantidad de datos que Macie puede analizar en el bucket. También indica si algún trabajo de detección de datos confidenciales está configurado para analizar los objetos del bucket. Si los hay, puede acceder a los detalles del trabajo que se ejecutó más recientemente y, si lo desea, mostrar los resultados que arroje el trabajo.

Para obtener más información sobre la información de esta pestaña, consulte Revisión de los detalles de los bucket de S3.

Muestras de objetos

En esta pestaña se enumeran los objetos que Macie ha analizado en el bucket mientras realizaba la detección automatizada de datos confidenciales. Si lo desea, elija el nombre de un objeto para abrir la consola de Amazon S3 y mostrar las propiedades del objeto.

La lista incluye datos de hasta 100 objetos. La lista se rellena en función del valor del campo Confidencialidad del objeto: Confidencial, seguido de No confidencial, seguido de los objetos que Macie no ha podido analizar.

En la lista, el campo Confidencialidad del objeto indica si Macie encontró datos confidenciales en un objeto:

- Confidencial: Macie encontró al menos una aparición de datos confidenciales en el objeto.
- No confidencial: Macie no encontró datos confidenciales en el objeto.
- – (guión): Macie no pudo completar el análisis del objeto debido a un problema o error.

El campo Resultados de clasificación indica si Macie pudo analizar un objeto:

- Completado: Macie completó el análisis del objeto.
- Parcial: Macie analizó solo un subconjunto de datos del objeto debido a un problema o error. Por ejemplo, el objeto es un archivo comprimido que contiene archivos en un formato no compatible.
- Omitido: Macie no pudo analizar ningún dato del objeto debido a un problema o error. Por ejemplo, el objeto está cifrado con una clave que Macie no puede usar.

Tenga en cuenta que la lista no incluye los objetos que se modificaron o eliminaron después de que Macie los analizara o intentara analizarlos. Macie elimina automáticamente un objeto de la lista si el objeto se modifica o elimina posteriormente.

Detección de datos confidenciales

Esta pestaña proporciona estadísticas agregadas y automatizadas de detección de datos confidenciales para el bucket:

- Bytes analizados: la cantidad total de datos, en bytes, que Macie ha analizado en el bucket.
- Tamaño clasificable: el tamaño total de almacenamiento de todos los objetos que Macie puede analizar en el bucket. Estos objetos utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Para obtener más información, consulte Clases y formatos de almacenamiento compatibles.
- Detecciones totales: el número total de apariciones de datos confidenciales que Macie ha encontrado en el bucket. Esto incluye las incidencias que actualmente están suprimidas por la configuración de la puntuación de confidencialidad del bucket.

El gráfico Objetos analizados indica el número total de objetos que Macie ha analizado en el bucket. También proporciona una representación visual del número de objetos en los que Macie encontró o no encontró datos confidenciales. La leyenda que aparece debajo del gráfico muestra un desglose de estos resultados:

- Objetos confidenciales (rojo): el número total de objetos en los que Macie encontró al menos una aparición de datos confidenciales.
- Objetos no confidenciales (azul): el número total de objetos en los que Macie no encontró datos confidenciales.
- Objetos omitidos (gris oscuro): el número total de objetos que Macie no pudo analizar debido a un problema o error.

El área situada debajo de la leyenda del gráfico muestra un desglose de los casos en los que Macie no pudo analizar los objetos debido a ciertos tipos de problemas de permisos o errores criptográficos:

- Omitido: cifrado no válido: número total de objetos cifrados con las claves proporcionadas por el cliente. Macie no puede acceder a estas claves.
- Omitido: KMS no válido: número total de objetos cifrados con claves AWS Key Management Service (AWS KMS) que ya no están disponibles. Estos objetos se cifran con las AWS KMS keys que estaban deshabilitadas, están programadas para su eliminación o se eliminaron. Macie no puede usar estas claves.
- Omitido: permiso denegado: el número total de objetos a los que Macie no puede acceder debido a la configuración de permisos del objeto o a la configuración de permisos de la clave que se utilizó para cifrar el objeto.

Para obtener más información sobre estos y otros tipos de problemas y errores que pueden producirse, consulte. Solución de los problemas de cobertura para la detección de datos confidenciales automatizada Si soluciona los problemas y los errores, puede aumentar la cobertura de los datos del depósito durante los ciclos de análisis posteriores.

Las estadísticas de la pestaña Detección de datos confidenciales no incluyen los datos de los objetos que se modificaron o eliminaron después de que Macie los analizara o intentara analizarlos. Si los objetos se modifican o eliminan de un bucket después de que Macie los analice o intente analizarlos, Macie recalcula automáticamente estas estadísticas para excluir los objetos.

Análisis de resultados de datos confidenciales obtenidos mediante la detección automatizada

Al realizar una detección automatizada de datos confidenciales, Amazon Macie crea un resultado de datos confidenciales para cada objeto de Amazon Simple Storage Service (Amazon S3) en el que encuentra datos confidenciales. Un resultado de datos confidenciales es un informe detallado de los

datos confidenciales que Macie encontró en un objeto de S3. Cada resultado de datos confidenciales proporciona una clasificación de gravedad y detalles como:

- La fecha y hora en que Macie encontró los datos confidenciales.
- La categoría y los tipos de datos confidenciales que encontró Macie.
- El número de apariciones de cada tipo de datos confidenciales que Macie encontró.
- Cómo descubrió Macie los datos confidenciales, la detección automatizada de datos confidenciales o un trabajo de detección de datos confidenciales.
- El nombre, la configuración de acceso público, el tipo de cifrado y otra información sobre el bucket y el objeto de S3 afectados.

Según el tipo de archivo o el formato de almacenamiento del objeto S3 afectado, los detalles también pueden incluir la ubicación de hasta 15 apariciones de los datos confidenciales que Macie encontró. Los resultados de datos confidenciales no incluyen los datos confidenciales que encontró Macie. En cambio, proporciona información que puede utilizar para investigar y corregir más a fondo, según sea necesario.

Macie almacena sus datos confidenciales durante 90 días. Puede acceder a ellos mediante la consola de Amazon Macie o la API de Amazon Macie. También puede supervisar y procesar los resultados mediante otras aplicaciones, servicios y sistemas. Para obtener más información, consulte Análisis de resultados.

Para analizar los resultados generados por la detección automatizada de datos confidenciales

Para identificar y analizar los datos confidenciales que Macie crea mientras realiza la detección automatizada de datos confidenciales para su cuenta, puede filtrar sus resultados. Con los filtros, puede utilizar atributos específicos de los resultados para crear vistas y consultas personalizadas. Puede utilizar la consola de Amazon Macie para filtrar resultados o enviar consultas mediante programación mediante la API de Amazon Macie.

Console

Siga estos pasos para identificar y analizar los resultados mediante la consola de Amazon Macie.

Para analizar los resultados generados por la detección automatizada

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Resultados.

3. (Opcional) Para mostrar los resultados que fueron suprimidos por una regla de supresión, cambie la configuración del Estado del resultado. Seleccione Todos para mostrar los resultados suprimidos y no suprimidos, o bien seleccione Archivado para mostrar solo los resultados suprimidos. Para volver a ocultar los resultados suprimidos, seleccione Actual.
4. Coloque el cursor en el cuadro Criterios de filtro. En la lista de campos que aparece, seleccione Tipo de origen.

   Este campo especifica cómo Macie encontró los datos confidenciales que dieron lugar a un resultado, a la detección automatizada de datos confidenciales o a un trabajo de detección de datos confidenciales. Para encontrar este campo en la lista de campos de filtro, puede examinar la lista completa o introducir parte del nombre del campo para reducir la lista de campos.
5. Seleccione AUTOMATED_SENSITIVE_DATA_DISCOVERY como valor del campo y, a continuación, elija Aplicar. Macie aplica los criterios de filtro y añade la condición a un token de filtro en el cuadro Criterios de filtro.
6. (Opcional) Para refinar los resultados, añada condiciones de filtro para campos adicionales, por ejemplo, Creado en para el intervalo de tiempo en el que se creó un resultado, nombre de bucket S3 para el nombre del bucket afectado o Tipo de detección de datos confidenciales para el tipo de dato confidencial que se detectó y produjo un resultado. Para obtener más información, consulte Filtro de resultados.

Si desea volver a utilizar este conjunto de condiciones posteriormente, puede guardarlo como regla de filtro. Para ello, seleccione Guardar regla en el cuadro Criterios de filtro. Ingrese un nombre y, opcionalmente, una descripción para la regla. Cuando termine, elija Save (Guardar).

API

Para identificar y analizar los resultados mediante programación, especifique los criterios de filtrado en las consultas que envíe mediante la GetFindingStatisticsoperación ListFindingso de la API Amazon Macie. La operación ListFindings devuelve una matriz de identificadores de resultados, un identificador por cada resultado que coincida con los criterios de filtrado. A continuación, puede utilizar esos identificadores para recuperar los detalles de cada resultado. La operación GetFindingStatistics devuelve datos estadísticos agregados sobre todos los resultados que coinciden con los criterios de filtro, agrupados por un campo que especifique en la solicitud. Para obtener más información sobre cómo filtrar los resultados mediante programación, consulte. Filtro de resultados

En los criterios de filtro, incluya una condición para el campo `originType`. Este campo especifica cómo Macie encontró los datos confidenciales que dieron lugar a un resultado, a la detección automatizada de datos confidenciales o a un trabajo de detección de datos confidenciales. El valor de este campo es `AUTOMATED_SENSITIVE_DATA_DISCOVERY` si se produjo un resultados al realizar una detección automatizada.

Para identificar y analizar los resultados mediante el comando AWS Command Line Interface (AWS CLI), ejecute el comando o list-findings. get-finding-statistics En los siguientes ejemplos, se utiliza el comando list-findings para recuperar los identificadores de búsqueda de todos los resultados de alta gravedad generados por la detección automatizada de datos confidenciales en la Región de AWS actual.

Para Linux, macOS o Unix, utilice el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Para Microsoft Windows, utilice el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

Donde:

- `classificationDetails.originType` especifica el nombre JSON del campo Tipo de origen y:
  - `eq` especifica el operador igual.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY` es un valor enumerado para el campo.
- *`severity.description`* especifica el nombre JSON del campo Gravedad y:
  - *`eq`* especifica el operador igual.
  - *`High`* es un valor enumerado para el campo.

Si el comando se ejecuta correctamente, Macie devuelve una matriz `findingIds`. La matriz indica el identificador único de cada resultado que coincide con los criterios de filtro, como se muestra en el siguiente ejemplo.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Si ningún resultado coincide con los criterios del filtro, Macie devuelve una matriz `findingIds` vacía.

```
{
    "findingIds": []
}
```

Acceso a los resultados de detección de datos confidenciales producidos por la detección automatizada

Amazon Macie crea un registro de análisis para cada objeto de Amazon Simple Storage Service (Amazon S3) que seleccione para el análisis y, al mismo tiempo, realiza una detección automatizada de datos confidenciales para su cuenta u organización. Estos registros, denominados resultados de la detección de datos confidenciales, registran detalles sobre el análisis que Macie realiza en objetos S3 individuales. Esto incluye objetos en los que Macie no detecta datos confidenciales y, por lo tanto, no produce resultados y objetos que Macie no puede analizar debido a errores o problemas como la configuración de permisos o el uso de un archivo o formato de almacenamiento no compatible.

Si Macie detecta datos confidenciales en un objeto de S3, el resultado de la detección de datos confidenciales incluye datos del resultado correspondiente. También proporciona información adicional, como la ubicación de hasta 1000 apariciones de cada tipo de datos confidenciales que Macie encontró en el objeto. Por ejemplo:

- El número de columna y fila de una celda o campo de un libro de Microsoft Excel, un archivo CSV o un archivo TSV

- La ruta a un campo o matriz en un archivo JSON o líneas JSON
- El número de línea de una línea de un archivo de texto no binario que no sea un archivo CSV, JSON, líneas JSON o TSV, por ejemplo, un archivo HTML, TXT o XML
- El número de página de una página de un archivo en formato de documento portátil (PDF) de Adobe
- El índice de registro y la ruta a un campo de un registro en un contenedor de objetos de Apache Avro o un archivo de Apache Parquet

Si el objeto S3 afectado es un archivo de almacenamiento, como un archivo .tar o .zip, el resultado de la detección de datos confidenciales también proporciona datos de ubicación detallados para la aparición de datos confidenciales en archivos individuales que Macie extrae del archivo. Macie no incluye esta información en los resultados de datos confidenciales para los archivos archivados. Para informar sobre los datos de ubicación, los resultados de la detección de datos confidenciales utilizan un esquema JSON estandarizado.

Un resultado de detección de datos confidenciales no incluye los datos confidenciales que encontró Macie. En cambio, le proporciona un registro de análisis que puede resultar útil para auditorías o investigaciones sobre la privacidad y la protección de los datos.

Macie almacena los resultados de la detección de datos confidenciales durante 90 días. No puede acceder a ellos directamente en la consola de Amazon Macie ni con la API de Amazon Macie. En cambio, usted configura Macie para que los cifre y almacene en un bucket de S3. El bucket puede servir como un repositorio definitivo y a largo plazo para todos sus resultados de detección de datos confidenciales. A continuación, si lo desea, puede acceder a los resultados de ese repositorio y consultarlos.

Para determinar dónde se encuentra este repositorio para su cuenta, elija Resultados de la detección en el panel de navegación de la consola de Amazon Macie. Para hacerlo mediante programación, utilice la GetClassificationExportConfigurationoperación de la API Amazon Macie. Si no ha configurado este repositorio para su cuenta, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales para obtener información sobre cómo hacerlo.

Tras configurar Macie para almacenar los resultados de la detección de datos confidenciales en un bucket de S3, Macie escribe los resultados en archivos JSON Lines (.jsonl), cifra y añade esos archivos al bucket como archivos GNU Zip (.gz). Para la detección automática de datos confidenciales, Macie añade los archivos a una carpeta cuyo nombre automated-sensitive-data-discoveryaparece en el depósito.

Al igual que en el caso de los resultados de datos confidenciales, los resultados de la detección de datos confidenciales siguen un esquema estandarizado. De forma opcional, esto puede ayudarle a consultarlos, supervisarlos y procesarlos mediante otras aplicaciones, servicios y sistemas.

> **Tip**
>
> Para ver un ejemplo detallado e instructivo de cómo puede consultar y utilizar los resultados del descubrimiento de datos confidenciales para analizar e informar sobre los posibles riesgos de seguridad de los datos, consulte la entrada del blog Cómo consultar y visualizar los resultados del descubrimiento de datos confidenciales de Macie con Amazon Athena y QuickSight Amazon AWS en el blog de seguridad.
> Para ver ejemplos de consultas de Athena que puede utilizar para analizar los resultados del descubrimiento de datos confidenciales, visite el repositorio de Amazon Macie Results Analytics en. GitHub Este repositorio también proporciona instrucciones para configurar Athena para recuperar y descifrar los resultados, y scripts para crear tablas para los resultados.

Puntuación de confidencialidad para buckets de S3

Si la detección automática de datos confidenciales está habilitada para su cuenta, Amazon Macie calcula y asigna automáticamente una puntuación de sensibilidad a cada depósito de uso general de Amazon Simple Storage Service (Amazon S3) que supervisa y analiza para su cuenta. Una puntuación de confidencialidad es una representación cuantitativa de la cantidad de datos confidenciales que puede contener un bucket de S3. En función de esa puntuación, Macie también asigna una etiqueta de confidencialidad a cada bucket. Una etiqueta de confidencialidad es una representación cualitativa de la puntuación de confidencialidad de un bucket. Estos valores pueden servir como puntos de referencia para determinar dónde pueden residir los datos confidenciales en su patrimonio de datos de Amazon S3 e identificar y supervisar los posibles riesgos de seguridad de esos datos.

De forma predeterminada, la puntuación de confidencialidad y la etiqueta de un bucket de S3 reflejan los resultados de las actividades automatizadas de detección de datos confidenciales que Macie ha realizado hasta ahora para ese bucket. No reflejan los resultados de los trabajos de detección de datos confidenciales que haya creado y ejecutado. Además, ni la puntuación ni la etiqueta implican ni indican de otro modo la criticidad o importancia que un bucket o los objetos de un bucket pueden tener para su organización. Puede anular la puntuación calculada de un bucket

y asignar manualmente la puntuación máxima (100), con lo que también se aplica la etiqueta de confidencialidad al bucket.

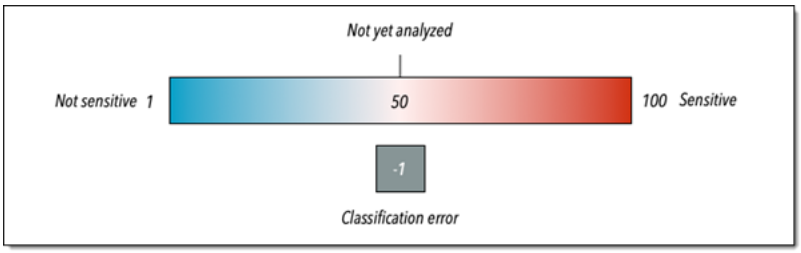
Temas

Dimensiones y rangos de puntuación de confidencialidad

Si la calcula Amazon Macie, la puntuación de confidencialidad de un bucket S3 es una medida cuantitativa de la intersección de dos dimensiones principales:

- La cantidad de datos confidenciales que Macie ha encontrado en el bucket. Esto se debe principalmente a la naturaleza y el número de tipos de datos confidenciales que Macie ha encontrado en el bucket y al número de veces que aparece cada tipo.
- La cantidad de datos que Macie ha analizado en el bucket. Esto se debe principalmente al número de objetos únicos que Macie ha analizado en el bucket en relación con el número total de objetos únicos del bucket.

La puntuación de confidencialidad de un bucket de S3 determina qué etiqueta de confidencialidad asigna Macie al bucket. La etiqueta de confidencialidad es una representación cualitativa de la puntuación, por ejemplo: Confidencial o No confidencial. En la consola de Amazon Macie, la puntuación de confidencialidad de un bucket también determina qué color utiliza Macie para representar el bucket en las visualizaciones de datos, como se muestra en la siguiente imagen.



Las puntuaciones de confidencialidad oscilan entre -1 y 100, tal y como se describe en la siguiente tabla. Para evaluar las entradas de la puntuación de un bucket de S3, puede consultar las estadísticas de detección de datos confidenciales y otros detalles que Macie proporcione sobre el bucket.

Puntuación de confidenc ialidad	Etiqueta de confidencialidad	Información adicional
-1	Clasificación de errores	Macie aún no ha analizado ninguno de los objetos del bucket debido a errores de clasificación a nivel de objeto: problemas con la configura ción de los permisos, el contenido de los objetos o las cuotas a nivel de objeto. Cuando Macie intentó analizar uno o más objetos del bucket, se produjeron errores. Por ejemplo, un objeto es un archivo con un formato incorrecto o un objeto está cifrado con una clave a la que Macie no puede acceder o que no puede utilizar. Los datos de cobertura del bucket pueden ayudarle a investiga r y corregir los errores. Para obtener más información, consulte Evaluación de cobertura de detección de datos confidenciales automatiz ada. Macie seguirá intentando analizar los objetos del bucket. Si Macie analiza un objeto correctamente, actualizará la puntuación de confidenc ialidad y la etiqueta del bucket

Puntuación de confidencialidad	Etiqueta de confidencialidad	Información adicional
		para reflejar los resultados del análisis.
Del 1 al 49	No confidencial	En este rango, una puntuación más alta, como 49, indica que Macie ha analizado relativamente pocos objetos del bucket. Una puntuación más baja, como 1, indica que Macie ha analizado muchos objetos del bucket (en relación con el número total de objetos del bucket) y ha detectado relativamente pocos tipos y casos de datos confidenciales en esos objetos. Una puntuación de 1 también puede indicar que el depósito no almacena ningún objeto o que todos los objetos del depósito contienen cero (0) bytes de datos. Las estadísticas de los objetos incluidas en los detalles del bucket pueden ayudarle a determinar si este es el caso. Para obtener más información, consulte Revisión de los detalles del bucket de S3.

Puntuación de confidenc ialidad	Etiqueta de confidencialidad	Información adicional
50	Aún no se ha analizado	Macie aún no ha intentado analizar ni analizado ninguno de los objetos del bucket. Macie asigna automátic amente esta puntuación a un bucket cuando activa por primera vez la detección automática en su cuenta o cuando se añade un bucket a su inventario de buckets. Una puntuación de 50 también puede indicar que la configura ción de permisos del bucket impide que Macie acceda al bucket o a los objetos del bucket. Por lo general, esto se debe a una política de bucket restrictiva. Los detalles del bucket pueden ayudarle a determinar si este es el caso, ya que Macie solo puede proporcionar un subconjun to de información sobre el bucket. Para obtener informaci ón acerca de cómo resolver este problema, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Puntuación de confidencialidad	Etiqueta de confidencialidad	Información adicional
51 a 99	Confidencial	En este rango, una puntuación más alta, como 99, indica que Macie ha analizado muchos objetos del bucket (en relación con el número total de objetos del bucket) y ha detectado muchos tipos y apariciones de datos confidenciales en esos objetos. Una puntuación más baja, como 51, indica que Macie ha analizado un número moderado de objetos del bucket (en relación con el número total de objetos del bucket) y ha detectado al menos algunos tipos y apariciones de datos confidenciales en esos objetos.
100	Confidencial	La puntuación se asignó manualmente al bucket y prevaleció sobre la puntuación calculada. Macie no asigna esta puntuación a los buckets.

Monitorización de las puntuaciones de confidencialidad

Cuando habilita inicialmente la detección automatizada de datos confidenciales en su cuenta, Amazon Macie asigna automáticamente una puntuación de confidencialidad de 50 a cada bucket de S3. Macie también asigna esta puntuación a un bucket cuando este se añade a su inventario de buckets. En función de esa puntuación, la etiqueta de confidencialidad de cada bucket es Aún no se ha analizado. La excepción es un depósito vacío, que es un depósito que no almacena ningún

objeto o que todos los objetos del depósito contienen cero (0) bytes de datos. Si este es el caso de un bucket, Macie le asigna una puntuación de 1 al bucket y le asigna la etiqueta No confidencial.

A medida que avanza la detección automatizada de su cuenta, Macie actualiza las puntuaciones de confidencialidad y las etiquetas de los buckets de S3 para reflejar los resultados de los análisis. Por ejemplo:

- Si Macie no encuentra datos confidenciales en un objeto, reduce la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto, aumenta la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto que se ha modificado posteriormente, elimina las detecciones de datos confidenciales del objeto de la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si Macie encuentra datos confidenciales en un objeto y los elimina posteriormente, elimina las detecciones de datos confidenciales del objeto de la puntuación de confidencialidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si se añade un objeto a un bucket que antes estaba vacío y Macie encuentra datos confidenciales en el objeto, Macie aumenta la puntuación de sensibilidad del bucket y actualiza la etiqueta de confidencialidad del bucket según sea necesario.
- Si la configuración de permisos de un bucket impide a Macie recuperar información sobre el bucket o los objetos del bucket o acceder a ellos, Macie cambia la puntuación de confidencialidad del depósito a 50 y cambia la etiqueta de confidencialidad del bucket a Aún no se ha analizado.

Según el tamaño de su patrimonio de datos que almacena en Amazon S3, los resultados del análisis pueden empezar a aparecer en un plazo de 48 horas a partir de la activación de la detección automatizada de datos confidenciales para su cuenta.

Puede ajustar la configuración de la puntuación de confidencialidad de su cuenta, lo que cambia la configuración para los análisis posteriores de todos sus buckets de S3. También puede ajustar la configuración de los buckets de S3 individuales. En cuanto a la configuración a nivel de cuenta, puede empezar a incluir o excluir de los análisis listas de permisos específicas, identificadores de datos personalizados o identificadores de datos gestionados específicos. Puede excluir buckets específicos de los análisis. Para obtener más información, consulte Establecer la configuración de detección automatizada de su cuenta.

Para ajustar la configuración de puntuación de un segmento de S3 concreto, puede incluir o excluir tipos específicos de datos confidenciales de la puntuación del depósito. También puede especificar si desea asignar una puntuación calculada automáticamente al bucket. Para obtener más información, consulte Gestión de la detección automatizada de buckets de S3 individuales.

Configuración predeterminada para la detección automatizada de datos confidenciales

Si la detección automática de datos confidenciales está habilitada para su cuenta, Amazon Macie selecciona y analiza automáticamente los objetos de muestra de todos los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) que supervisa y analiza para su cuenta. Si es el administrador de Macie de una organización, esto incluye los buckets de S3 que son propiedad de sus cuentas de miembro. Para afinar el alcance de los análisis, puede excluir buckets específicos de la detección automatizada de datos confidenciales. Puede hacerlo de dos maneras: cambiando la configuración de detección automatizada de datos confidenciales de su cuenta y cambiando la configuración de detección automatizada de datos confidenciales para buckets individuales.

De forma predeterminada, Macie analiza los objetos de S3 utilizando únicamente el conjunto de identificadores de datos gestionados que recomendamos para la detección automatizada de datos confidenciales. Macie no utiliza ningún identificador de datos personalizado ni permite listas que usted haya definido. Para personalizar los análisis, puede configurar Macie para que utilice identificadores de datos gestionados específicos, identificadores de datos personalizados y listas de permisos. Para ello, puede cambiar la configuración de detección automatizada de datos confidenciales de su cuenta.

Temas

- Identificadores de datos administrados predeterminados para la detección automatizada de datos confidenciales
- Actualiza la configuración predeterminada para la detección automatizada de datos confidenciales

Identificadores de datos administrados predeterminados para la detección automatizada de datos confidenciales

De forma predeterminada, Amazon Macie analiza los objetos de S3 utilizando únicamente el conjunto de identificadores de datos gestionados que recomendamos para la detección automatizada de datos confidenciales. Este conjunto predeterminado de identificadores de datos administrados está diseñado para detectar categorías y tipos comunes de datos confidenciales. Según nuestras

investigaciones, puede detectar categorías y tipos generales de datos confidenciales y, al mismo tiempo, optimizar los resultados de la detección automatizada al reducir el ruido.

El conjunto predeterminado es dinámico. A medida que publicamos nuevos identificadores de datos gestionados, los añadimos al conjunto predeterminado si es probable que puedan optimizar aún más los resultados de la detección automatizada de datos confidenciales. Con el tiempo, también podríamos añadir o eliminar del conjunto los identificadores de datos administrados existentes. La eliminación de un identificador de datos gestionados no afecta a las estadísticas ni a los detalles de detección de datos confidenciales existentes en sus buckets de S3. Por ejemplo, si eliminamos el identificador de datos gestionados de un tipo de datos confidenciales que Macie detectó anteriormente en un bucket, Macie seguirá informando de esas detecciones en el bucket. Si añadimos o eliminamos un identificador de datos gestionados del conjunto predeterminado, actualizamos esta página para indicar la naturaleza y el momento del cambio. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos.

En los siguientes temas, se enumeran los identificadores de datos gestionados que se encuentran actualmente en el conjunto predeterminado, organizados por categoría y tipo de datos confidenciales. Especifican el identificador (ID) único de cada identificador de datos administrados del conjunto. Este ID describe el tipo de datos confidenciales que un identificador de datos gestionados está diseñado para detectar, por ejemplo: `PGP_PRIVATE_KEY` para las claves privadas de PGP y `USA_PASSPORT_NUMBER` para los números de pasaportes estadounidenses. Si cambia la configuración de detección automatizada de datos confidenciales de su cuenta, puede usar este ID para excluir explícitamente un identificador de datos gestionados de los análisis posteriores.

Temas

- Credenciales
- Información financiera
- Información de identificación personal (PII)

Para obtener más información sobre identificadores de datos administrados específicos o una lista completa de todos los identificadores de datos administrados que Macie proporciona actualmente, consulte Uso de identificadores de datos administrados.

Credenciales

Para detectar la aparición de datos de credenciales en los objetos de S3, Macie utiliza los siguientes identificadores de datos gestionados de forma predeterminada.

Tipos de datos confidenciales	Identificador de datos administrados
AWS clave de acceso secreta	`AWS_CREDENTIALS`
Encabezado de autorización básica de HTTP	`HTTP_BASIC_AUTH_HEADER`
Clave privada de OpenSSH	`OPENSSH_PRIVATE_KEY`
Clave privada de PGP	`PGP_PRIVATE_KEY`
Clave privada del estándar de criptografía de clave pública (PKCS)	`PKCS`
Clave privada PuTTY	`PUTTY_PRIVATE_KEY`

Información financiera

Para detectar la aparición de información financiera en los objetos de S3, Macie utiliza los siguientes identificadores de datos gestionados de forma predeterminada.

Tipos de datos confidenciales	Identificador de datos administrados
Datos de banda magnética de tarjetas de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Número de tarjetas de crédito	`CREDIT_CARD_NUMBER` (para números de tarjetas de crédito próximos a una palabra clave)

Información de identificación personal (PII)

Para detectar la aparición de información de identificación personal (PII) en objetos de S3, Macie utiliza de forma predeterminada los siguientes identificadores de datos administrados.

Tipos de datos confidenciales	Identificador de datos administrados
Número de identificación del permiso de conducir	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (para EE. UU.), `UK_DRIVERS_LICENSE`
Número de registro electoral	`UK_ELECTORAL_ROLL_NUMBER`
Número de identificación nacional	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Número de seguro nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Número de pasaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Número de Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número de la Seguridad Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`
Número de identificación o referencia del contribuyente	`AUSTRALIA_TAX_FILE_NUMBER`, `BRAZIL_CPF_NUMBER`, `FRANCE_TAX_IDENTIFICATION_NUMBER`, `GERMANY_TAX_IDENTIFICATION_NUMBER`, `SPAIN_NIE_NUMBER`, `SPAIN_NIF_NUMBER`, `SPAIN_TAX_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Actualiza la configuración predeterminada para la detección automatizada de datos confidenciales

En la siguiente tabla se describen los cambios en la configuración que Amazon Macie utiliza de forma predeterminada para la detección automatizada de datos confidenciales. Para obtener alertas automáticas sobre cambios, suscríbase a la fuente RSS en la página de historial de documentos de Macie.

Cambio	Descripción	Fecha
Se implementó un nuevo conjunto dinámico de identific adores de datos administrados predeterminados	Las nuevas configuraciones de detección automatizada de datos confidenciales ahora se basan en un conjunto dinámico predeterminado de identificadores de datos gestionados. Si habilita la detección automatizada de datos confidenciales por primera vez en esta fecha o después, la configuración se basará en el conjunto dinámico. Si habilitó la detección automatizada de datos confidenciales por primera vez antes de esta fecha, la configuración se basará en un conjunto diferente de identific adores de datos gestionados. Para obtener más informaci ón, consulte las notas al pie después de esta tabla.	2 de agosto de 2023

Cambio	Descripción	Fecha
Disponibilidad general	Versión inicial de la detección automatizada de datos confidenciales.	28 de noviembre de 2022

Si habilitó inicialmente la detección automatizada de datos confidenciales en su cuenta antes del 2 de agosto de 2023, su configuración no se basa en el conjunto dinámico de identificadores de datos gestionados predeterminados. En cambio, su configuración se basa en un conjunto estático de identificadores de datos gestionados que definimos para la versión inicial de la detección automatizada de datos confidenciales, tal y como se indica en la siguiente tabla.

Para determinar cuándo habilitó inicialmente la detección automatizada de datos confidenciales para la cuenta, seleccione Detección automatizada en el panel de navegación de la consola de Amazon Macie y, a continuación, consulte la fecha de activación en la sección Estado. Para hacerlo mediante programación, utilice la GetAutomatedDiscoveryConfigurationoperación de la API de Amazon Macie y consulte el valor del campo. `firstEnabledAt` Si la fecha es anterior al 2 de agosto de 2023 y desea empezar a utilizar el conjunto dinámico de identificadores de datos gestionados predeterminados, póngase en contacto con nosotros para obtener ayuda. AWS Support

En la siguiente tabla se enumeran todos los identificadores de datos administrados que se encuentran en el conjunto estático. La tabla se ordena primero por categoría de datos confidenciales y, después, por tipo de datos confidenciales. Para obtener más información sobre identificadores de datos gestionados específicos, consulte Uso de identificadores de datos administrados.

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Credenciales	AWS clave de acceso secreta	`AWS_CREDENTIALS`
Credenciales	Encabezado de autorización básica de HTTP	`HTTP_BASIC_AUTH_HEADER`
Credenciales	Clave privada de OpenSSH	`OPENSSH_PRIVATE_KEY`
Credenciales	Clave privada de PGP	`PGP_PRIVATE_KEY`

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Credenciales	Clave privada del estándar de criptografía de clave pública (PKCS)	PKCS
Credenciales	Clave privada PuTTY	PUTTY_PRIVATE_KEY
Información financiera	Número de cuenta bancaria	BANK_ACCOUNT_NUMBER (para números de cuentas bancarias de Canadá y EE. UU.), FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
Información financiera	Fecha de caducidad de la tarjeta	CREDIT_CARD_EXPIRATION
Información financiera	Datos de banda magnética de tarjetas de crédito	CREDIT_CARD_MAGNETIC_STRIPE
Información financiera	Número de tarjetas de crédito	CREDIT_CARD_NUMBER (para números de tarjetas de crédito próximos a una palabra clave)
Información financiera	Código de verificación de tarjeta de crédito	CREDIT_CARD_SECURITY_CODE
Información personal: información médica personal (PHI)	Número de registro de la Administración para el Control de Drogas (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Información personal: PHI	Número de reclamación del seguro médico (HICN)	`USA_HEALTH_INSURANCE_CLAIM_NUMBER`
Información personal: PHI	Número de seguro médico o identificación médica	`CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER`
Información personal: PHI	Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Información personal: PHI	Código nacional de medicamento (NDC)	`USA_NATIONAL_DRUG_CODE`
Información personal: PHI	Identificador nacional de proveedores (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Información personal: PHI	Identificador único de dispositivo (UDI)	`MEDICAL_DEVICE_UDI`
Información personal: información de identificación personal (PII)	Fecha de nacimiento	`DATE_OF_BIRTH`

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Información personal: PII	Número de identificación del permiso de conducir	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (para EE. UU.), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE,

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
		NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Información personal: PII	Número de registro electoral	UK_ELECTORAL_ROLL_NUMBER
Información personal: PII	Nombre completo	NAME
Información personal: PII	Coordenadas del sistema de posicionamiento global (GPS)	LATITUDE_LONGITUDE
Información personal: PII	Dirección postal	ADDRESS, BRAZIL_CEP_CODE
Información personal: PII	Número de identificación nacional	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Información personal: PII	Número de seguro nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Información personal: PII	Número de pasaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Información personal: PII	Número de residencia permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Información personal: PII	Número de teléfono	`BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (para Canadá y EE. UU.), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Información personal: PII	Número de Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Información personal: PII	Número de la Seguridad Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Categoría de datos confidenciales	Tipos de datos confidenciales	Identificador de datos administrados
Información personal: PII	Número de identificación o referencia del contribuyente	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Información personal: PII	Número de identificación de vehículo (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Ejecución de trabajos de detección de datos confidenciales en Amazon Macie

Con Amazon Macie, puede crear y ejecutar trabajos de descubrimiento de datos confidenciales para automatizar la detección, el registro y la notificación de datos confidenciales en los depósitos de uso general de Amazon Simple Storage Service (Amazon S3). Un trabajo de detección de datos confidenciales es una serie de tareas automatizadas de procesamiento y análisis que Macie realiza para detectar y reportar datos confidenciales en objetos de Amazon S3. Cada trabajo proporciona informes detallados de los datos confidenciales que Macie encuentra y de los análisis que realiza. Al crear y ejecutar trabajos, puede crear y mantener una visión integral de los datos que almacena su organización en Amazon S3 y de cualquier riesgo de seguridad o de conformidad de datos.

Para ayudarlo a atender y mantener el cumplimiento de sus requisitos de seguridad y privacidad de datos, Macie ofrece varias opciones para programar y definir el alcance de un trabajo. Puede configurar un trabajo para que se ejecute solo una vez para el análisis y la evaluación bajo demanda, o de forma recurrente para el análisis periódico, la evaluación y la supervisión. Usted define la amplitud y la profundidad del análisis: buckets de S3 específicos que seleccione o bucket que coincidan con criterios específicos. Si lo desea, puede refinar el alcance de ese análisis seleccionando opciones adicionales. Las opciones incluyen criterios personalizados de inclusión y exclusión que se derivan de las propiedades de los objetos de S3, como las etiquetas, los prefijos y la fecha en que se modificó un objeto por última vez.

Para cada trabajo, también debe especificar los tipos de datos confidenciales que desea que Macie detecte y notifique. Puede configurar un trabajo para que utilice los identificadores de datos administrados que proporciona Macie, los identificadores de datos personalizados que usted defina o una combinación de ambos. Al seleccionar identificadores de datos gestionados y personalizados específicos para un trabajo, puede personalizar el análisis para que se centre en tipos específicos de datos confidenciales. Para ajustar el análisis, también puede configurar un trabajo para que utilice las listas de permisos que usted defina. Las listas de permisos especifican el texto y los patrones de texto que desea que Macie ignore, normalmente excepciones de datos confidenciales para los escenarios o entornos particulares de su organización.

Cada trabajo genera registros de los datos confidenciales que Macie encuentra y de los análisis que realiza Macie: los resultados de datos confidenciales y los resultados de la detección de datos confidenciales. Un resultado de datos confidenciales es un informe detallado de los datos confidenciales que Macie encontró en un objeto de S3. Un resultado de detección de datos confidenciales es un registro de los detalles sobre el análisis de un objeto S3. Macie crea un resultado de detección de datos confidenciales para cada objeto que usted configure un trabajo para analizar. Esto incluye objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no produce resultados de datos confidenciales y objetos que Macie no puede analizar debido a problemas o errores. Cada tipo de registro sigue un esquema estandarizado, que puede ayudarle a consultar, supervisar y procesar los registros para cumplir con sus requisitos de seguridad y conformidad.

Temas

- Monitoreo de trabajos de detección de información confidencial con los Registros de Amazon CloudWatch.
- Administración de trabajos de detección de datos confidenciales
- Previsión y supervisión de los costos de los trabajos de detección de datos confidenciales
- Identificadores de datos administrados recomendados para trabajos de detección de datos confidenciales

Opciones de alcance para trabajos de detección de datos confidenciales

Con los trabajos de detección de información confidencial, se define el alcance de los datos de Amazon Simple Storage Service (Amazon S3) que Amazon Macie analiza para detectar y notificar los datos confidenciales. Para ayudarle a hacerlo, Macie ofrece varias opciones específicas para cada trabajo que puede elegir al crear y configurar un trabajo.

Opciones de alcance

- Buckets de S3
- Incluir objetos de S3 existentes
- Profundidad de muestreo
- Criterios de objeto de S3

Buckets de S3

Cuando crea un trabajo de descubrimiento de datos confidenciales, especifica qué depósitos de S3 almacenan los objetos que desea que Macie analice cuando se ejecute el trabajo. Puede hacerlo de dos maneras: seleccionando depósitos de S3 específicos de su inventario de depósitos o especificando criterios personalizados que se derivan de las propiedades de los depósitos de S3.

Selecciona buckets S3 específicos

> Con esta opción, selecciona de forma explícita cada depósito de S3 para analizarlo. Luego, cuando se ejecuta el trabajo, analiza los objetos solo en los buckets que seleccione. Si configura un trabajo para que se ejecute periódicamente de forma diaria, semanal o mensual, el trabajo analiza los objetos de esos mismos cubos cada vez que se ejecuta.

Esta configuración resulta útil en los casos en los que desee realizar un análisis específico de un conjunto de datos específico. Esto le proporciona un control preciso y predecible sobre los buckets que analiza un trabajo.

Especifique los criterios del bucket de S3

Con esta opción, se definen los criterios de tiempo de ejecución que determinan qué buckets de S3 analizar. Los criterios consisten en una o más condiciones que se derivan de las propiedades del bucket, como las etiquetas y la configuración del acceso público. Cuando se ejecuta el trabajo, identifica los buckets que coinciden con sus criterios y analiza los objetos de esos buckets. Si configura un trabajo para que se ejecute periódicamente, el trabajo lo hará cada vez que se ejecute. En consecuencia, el trabajo puede analizar los objetos de distintos buckets cada vez que se ejecute, en función de los cambios en el inventario de bucket y de los criterios que defina.

Esta configuración resulta útil en los casos en los que desea que el alcance del análisis se adapte dinámicamente a los cambios en el inventario de depósitos. Si configura un trabajo para que utilice los criterios de los buckets y se ejecute periódicamente, el trabajo identifica automáticamente los nuevos buckets que cumplen los criterios y los inspecciona para detectar datos confidenciales.

En los temas de esta sección, se proporcionan detalles adicionales acerca de cada opción.

Temas

Selección de buckets de S3 específicos

Si elige seleccionar de forma explícita cada uno de los cubos de S3 que desee analizar en un trabajo, Macie le proporcionará un inventario completo de los depósitos de uso general actuales. Región de AWS A continuación, puede revisar su inventario y seleccionar los buckets que desee. Para saber cómo Macie mantiene este inventario por usted, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.

Si es el administrador de Macie de una organización, el inventario incluye buckets que son propiedad de las cuentas de miembros de su organización. Puede seleccionar hasta 1000 de estos buckets, que abarquen hasta 1000 cuentas.

Para ayudarle a seleccionar buckets, el inventario proporciona detalles y estadísticas para cada bucket. Esto incluye la cantidad de datos que el trabajo puede analizar en cada depósito: los objetos clasificables son objetos que utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un formato de archivo o almacenamiento compatible. El inventario también indica si algún trabajo existente está configurado para analizar los objetos de un bucket. Estos detalles pueden ayudarle a estimar la amplitud de un trabajo y a afinar sus selecciones de buckets.

En la tabla de inventario:

- Confidencialidad: indica la puntuación de confidencialidad actual de un bucket, si la detección automática de datos confidenciales está habilitada en su cuenta.
- Objetos clasificables es el número total de objetos que el trabajo puede analizar en el bucket.
- Tamaño clasificable es el tamaño total de almacenamiento de todos los objetos que el trabajo puede analizar en el bucket.

  Si un depósito almacena objetos comprimidos, este valor no refleja el tamaño real de esos objetos una vez descomprimidos. Si el control de versiones está activado para el bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto del bucket.
- Supervisado por el trabajo: indica si los trabajos de detección de datos confidenciales están configurados para analizar periódicamente los objetos del bucket de forma diaria, semanal o mensual.

  Si el valor de este campo es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.
- Última ejecución de un trabajo: si los trabajos periódicos o únicos existentes están configurados para analizar los objetos de un bucket, este campo indica la fecha y la hora más recientes en que se inició la ejecución de uno de esos trabajos. De lo contrario, este campo está vacío.

Si el icono de información
()
aparece junto a los nombres de los buckets de la tabla, le recomendamos que recupere los metadatos de bucket más recientes de Amazon S3. Para ello, seleccione actualizar
()
encima de la tabla. Este icono indica que se creó un bucket durante las últimas 24 horas,

posiblemente después de que Macie recuperara por última vez los metadatos del bucket y del objeto de Amazon S3 como parte del ciclo de actualización diario. Para obtener más información, consulte Actualizaciones de datos.

Si el icono de advertencia
(⚠)
aparece junto al nombre de un bucket, significa que Macie no puede acceder a los objetos del bucket. Esto significa que el trabajo no podrá analizar los objetos del bucket. Para investigar el problema, revise la política y la configuración de permisos del bucket en Amazon S3. Por ejemplo, el bucket puede tener una política de bucket restrictiva. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Para personalizar su vista del inventario y encontrar buckets específicos con mayor facilidad, puede filtrar la tabla introduciendo los criterios de filtrado en el cuadro de filtro. La siguiente tabla muestra algunos ejemplos.

Para mostrar los buckets que...	Aplicar este filtro...
Son propiedad de una cuenta específica	ID de cuenta = *el identificador de 12 dígitos de la cuenta*
Accesible públicamente	Permiso efectivo = Público
No se incluyen en ningún trabajo periódico	Supervisados activamente por trabajo = Falso
No se incluyen en ningún trabajo periódico o único	Definidos en el trabajo = Falso
Tienen una clave de etiqueta concreta*	Clave de etiqueta = *la clave de etiqueta*
Tienen un valor de etiqueta especifico*	Valor de etiqueta = *el valor de etiqueta*
Almacene objetos no cifrados (u objetos que utilicen cifrado del lado del cliente)	El recuento de objetos mediante cifrado está Sin encriptar y Desde = 1

* Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Debe especificar un valor completo y válido para el campo. No puede especificar valores parciales ni utilizar caracteres comodín.

Para mostrar los detalles de un bucket, elija el nombre del bucket y consulte el panel de detalles. Desde allí, también puede hacer lo siguiente:

- Desplácese y profundice en ciertos campos eligiendo una lupa para el campo. Elija
  
  para mostrar los buckets con el mismo valor o elija
  
  para mostrar los buckets con otros valores.
- Recupere los metadatos más recientes de los objetos del bucket. Esto puede resultar útil si ha creado un bucket recientemente o ha realizado cambios importantes en los objetos de un bucket durante las últimas 24 horas. Para recuperar los datos, seleccione actualizar () en la sección de estadísticas de objetos del panel. Esta opción está disponible para depósitos que almacenan 30 000 objetos o menos.

Especificar los criterios de los buckets de S3

Si decide especificar los criterios del bucket para un trabajo, Macie ofrece opciones para definir y probar los criterios. Estos son criterios de tiempo de ejecución que determinan qué depósitos de S3 almacenan los objetos que se van a analizar. Cada vez que se ejecuta el trabajo, identifica los depósitos de uso general que coinciden con sus criterios y, a continuación, analiza los objetos de los cubos correspondientes. Si es el administrador de Macie de una organización, el inventario incluye datos estadísticos y de otro tipo sobre los buckets de S3 que son propiedad de su cuenta y de las cuentas de miembros de su organización.

Definición de los criterios de bucket

Los criterios consisten en una o más condiciones que se derivan de las propiedades del bucket de S3. Cada condición, también denominada criterio, consta de las siguientes partes:

- Un campo basado en una propiedad, como el ID de cuenta o el permiso efectivo.
- Un operador, como igual a (`eq`) o no igual a(`neq`).
- Uno o varios valores.
- Una declaración de inclusión o exclusión que indica si se deben analizar (incluir) u omitir (excluir) los cubos que coincidan con la condición.

Si especifica más de un valor para un campo, Macie utiliza la lógica OR para unir los valores. Si especifica más de una condición para los criterios, Macie utiliza la lógica AND para unir las condiciones. Además, las condiciones de exclusión tienen prioridad sobre las condiciones de inclusión. Por ejemplo, si incluye buckets de acceso público y excluye los que tienen etiquetas específicas, el trabajo analiza los objetos de cualquier bucket de acceso público, a menos que el bucket tenga una de las etiquetas especificadas.

Puede definir condiciones que se deriven de cualquiera de los siguientes campos basados en propiedades de los objetos de S3.

ID de cuenta

El identificador (ID) único del propietario Cuenta de AWS de un bucket. Para especificar varios valores para este campo, introduzca el ID de cada cuenta y separe cada entrada con una coma.

Macie no admite el uso de caracteres comodín ni valores parciales para las entradas.

Nombre del bucket

Nombre del bucket de. Este campo se correlaciona con el campo Nombre, no con el campo Nombre de recurso de Amazon (ARN), en Amazon S3. Para especificar varios valores para este campo, introduzca el ID de cada bucket y separe cada entrada con una coma.

Tenga en cuenta que los valores distinguen entre mayúsculas y minúsculas. Además, Macie no admite el uso de valores parciales o caracteres comodín en este tipo de condición.

Permisos efectivos

Especifica si un bucket es accesible públicamente. Puede elegir uno o varios de los siguientes valores para este campo:

- No público: el público en general no tiene acceso de lectura ni escritura al bucket.
- Público: el público en general tiene acceso de lectura o escritura al bucket.
- Desconocido: Macie no ha podido evaluar la configuración de acceso público del bucket.

Para determinar los valores de esta sección, Macie analiza una combinación de configuraciones de niveles de cuentas y de buckets para cada bucket: la configuración de bloqueo de acceso público de la cuenta, la configuración de bloqueo de acceso público del bucket, la política de buckets para ese bucket y la lista de control de acceso (ACL) del bucket.

Acceso compartido

Especifica si un bucket se comparte con otro Cuenta de AWS, con una identidad de acceso de CloudFront origen (OAI) de Amazon o con un control de acceso de CloudFront origen (OAC). Puede elegir uno o varios de los siguientes valores para este campo:

- Externo: el depósito se comparte con una o más de las siguientes opciones, o con una combinación de las siguientes: una CloudFront OAI, una CloudFront OAC o una cuenta externa a tu organización (que no forma parte de ella).
- Interno: el bucket se comparte con una o más cuentas que son internas (forman parte) de su organización. No se comparte con una CloudFront OAI ni con una OAC.
- No compartido: el depósito no se comparte con otra cuenta, una CloudFront OAI o una OAC. CloudFront
- Desconocido: Macie no ha podido evaluar la configuración de acceso compartido del bucket.

Para determinar si un bucket se comparte con otro Cuenta de AWS, Macie analiza la política del bucket y la ACL del bucket. Además, una organización se define como un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante AWS Organizations una invitación de Macie. Para obtener información sobre las opciones de Amazon S3 para compartir buckets, consulte Administración de identidades y accesos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Para determinar si un bucket se comparte con una CloudFront OAI o una OAC, Macie analiza la política del bucket. Una CloudFront OAI o una OAC permiten a los usuarios acceder a los objetos de un depósito a través de una o más distribuciones específicas. CloudFront Para obtener información sobre las CloudFront OAI y las OAC, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFront desarrolladores de Amazon.

Etiquetas

Las etiquetas que están asociadas al bucket. Las etiquetas son etiquetas que puede definir y asignar a determinados tipos de AWS recursos, incluidos los buckets de S3. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Para obtener más información acerca del etiquetado de buckets de S3, consulte Uso de etiquetas de asignación de costos de buckets de S3 en la Guía del usuario de Amazon Simple Storage Service.

Para un trabajo de detección de datos confidenciales, puede usar este tipo de condición para incluir o excluir los buckets que tengan una clave de etiqueta específica, un valor de etiqueta específico o una clave de etiqueta y un valor de etiqueta específicos (como un par). Por ejemplo:

- Si especifica **`Project`** como clave de etiqueta y no especifica ningún valor de etiqueta para una condición, cualquier bucket que contenga la clave de etiqueta del proyecto cumplirá los criterios de la condición, independientemente de los valores de etiqueta asociados a esa clave de etiqueta.
- Si especifica **`Development`** y **`Test`** como valores de etiqueta y no especifica ninguna clave de etiqueta para una condición, cualquier bucket que contenga el valor de etiqueta **`Development`** o **`Test`** cumple los criterios de la condición, independientemente de los valores de etiqueta asociados a esas claves de etiqueta.

Para especificar varias claves de etiqueta en una condición, introduzca cada clave de etiqueta en el campo Clave y separe cada entrada con una coma. Para especificar varios valores de etiqueta en una condición, introduzca cada clave de etiqueta en el campo Valor y separe cada entrada con una coma.

Las claves y los valores de las etiquetas no distinguen entre mayúsculas y minúsculas. Además, Macie no admite el uso de valores parciales o caracteres comodín en este tipo de condiciones.

Probar los criterios de buckets

Mientras define los criterios del bucket, puede probar y refinar los criterios previsualizando los resultados. Para ello, expanda la sección Vista previa de los resultados de los criterios que aparece debajo de los criterios en la consola. En esta sección se muestra una tabla de los depósitos de uso general de S3 que actualmente cumplen los criterios.

Esto incluye la cantidad de datos que un trabajo puede analizar en cada bucket: los objetos clasificables son objetos que utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un formato de archivo o almacenamiento compatible. El inventario también indica si algún trabajo existente está configurado para analizar los objetos de un bucket.

En la tabla:

- Confidencialidad: indica la puntuación de confidencialidad actual de un bucket, si la detección automática de datos confidenciales está habilitada en su cuenta.
- Objetos clasificables es el número total de objetos que el trabajo puede analizar en el bucket.
- Tamaño clasificable es el tamaño total de almacenamiento de todos los objetos que el trabajo puede analizar en el bucket.

Si un depósito almacena objetos comprimidos, este valor no refleja el tamaño real de esos objetos una vez descomprimidos. Si el control de versiones está activado para el bucket, este valor se basa en el tamaño de almacenamiento de la última versión de cada objeto del bucket.

- Supervisado por el trabajo: indica si los trabajos de detección de datos confidenciales están configurados para analizar periódicamente los objetos del bucket de forma diaria, semanal o mensual.

  Si el valor de este campo es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.

Si el icono de advertencia
(⚠)
aparece junto al nombre de un bucket, significa que Macie no puede acceder al bucket. Esto significa que el trabajo no podrá analizar los objetos del bucket. Para investigar el problema, revise la política y la configuración de permisos del bucket en Amazon S3. Por ejemplo, el bucket puede tener una política de bucket restrictiva. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Para refinar los criterios del bucket para el trabajo, use las opciones de filtro para añadir, cambiar o eliminar condiciones de los criterios. A continuación, Macie actualizará la tabla para reflejar los cambios.

Incluir objetos de S3 existentes

Puede utilizar los trabajos de detección de datos confidenciales para realizar un análisis continuo e incremental de los objetos en los buckets de S3. Si configura un trabajo para que se ejecute periódicamente, Macie lo hará automáticamente: cada ejecución analiza solo los objetos que se crearon o modificaron después de la ejecución anterior. Con la opción Incluir objetos existentes, puede elegir el punto de partida para el primer incremento:

- Seleccione esta casilla de verificación para analizar todos los objetos existentes inmediatamente después de crear el trabajo.
- Para esperar y analizar solo los objetos creados o modificados después de crear el trabajo y antes de la primera ejecución, desactive la casilla de verificación de esta opción.

Desactivar esta casilla de verificación resulta útil en los casos en los que ya ha analizado los datos y desea seguir analizándolos periódicamente. Por ejemplo, si ha utilizado anteriormente otro servicio o aplicación para clasificar los datos y ha empezado a utilizar Macie recientemente, puede utilizar esta opción para garantizar el descubrimiento y la clasificación de forma continua de los datos sin incurrir en costos innecesarios ni duplicar los datos de clasificación.

Cada ejecución posterior del trabajo periódico analiza solo los objetos creados o modificados después de la ejecución anterior.

Tanto para los trabajos periódicos como para los únicos, también puede configurar un trabajo para analizar solo los objetos que se creen o modifiquen antes o después de un tiempo determinado o durante un intervalo de tiempo determinado. Para ello, añada criterios de objeto que utilicen la fecha de la última modificación de los objetos.

Profundidad de muestreo

Con esta opción, usted especifica el porcentaje de objetos S3 aptos que desea que analice un trabajo de descubrimiento de datos confidenciales. Los objetos aptos son objetos que: utilizan una clase de almacenamiento de Amazon S3 compatible, tienen una extensión de nombre de archivo para un formato de archivo o almacenamiento compatible y cumplen otros criterios que especifique para el trabajo.

Si este valor es menor que el 100 %, Macie selecciona de forma aleatoria los objetos que se van a analizar, hasta el porcentaje especificado y analiza todos los datos de esos objetos. Por ejemplo, si configura un trabajo para analizar 10 000 objetos y especifica una profundidad de muestreo del 20%, Macie analiza aproximadamente 2000 objetos aptos y seleccionados al azar cuando se ejecuta el trabajo.

Reducir la profundidad de muestreo de un trabajo puede reducir el costo y la duración del trabajo. Resulta útil en los casos en los que los datos de los objetos son muy coherentes y se desea determinar si un depósito de S3, en lugar de cada objeto, almacena datos confidenciales.

Tenga en cuenta que esta opción controla el porcentaje de objetos que se analizan, no el porcentaje de bytes que se analizan. Si introduce una profundidad de muestreo inferior al 100%, Macie analiza todos los datos de cada objeto seleccionado, no ese porcentaje de los datos de cada objeto seleccionado.

Criterios de objeto de S3

Para ajustar el alcance de un trabajo de detección de datos confidenciales, también puede definir criterios personalizados que determinen qué objetos de S3 Macie incluye o excluye del análisis de un trabajo. Estos criterios se componen de una o más condiciones que se derivan de las propiedades de los objetos de S3: Las condiciones se aplican a los objetos de todos los depósitos de S3 para los que configure un trabajo para analizarlos. Si un depósito almacena varias versiones de un objeto, las condiciones se aplican a la última versión del objeto.

Si añade varias condiciones, Macie utiliza la lógica AND para unir las condiciones. Además, las condiciones de exclusión tienen prioridad sobre las condiciones de inclusión. Por ejemplo, si incluye objetos que tienen la extensión de nombre de archivo .pdf y excluye los objetos que pesan más de 5 MB, el trabajo analiza cualquier objeto que tenga la extensión de nombre de archivo .pdf, a menos que el objeto supere los 5 MB.

Puede definir condiciones que se deriven de cualquiera de las siguientes propiedades de los objetos de S3.

Extensión de nombre de archivo

Esto se correlaciona con la extensión del nombre de archivo de un objeto de S3. Puede usar este tipo de condición para incluir o excluir objetos según el tipo de archivo. Para hacerlo con varios tipos de archivos, introduzca la extensión del nombre de archivo de cada tipo y separe cada entrada con una coma, por ejemplo: **`docx,pdf,xlsx`**. Si introduce varias extensiones de nombre de archivo como valores para una condición, Macie utiliza la lógica OR para unir los valores.

Tenga en cuenta que los valores distinguen entre mayúsculas y minúsculas. Además, Macie no admite el uso de valores parciales o caracteres comodín en este tipo de condición.

Para obtener información sobre los tipos de archivos que Macie puede analizar, consulte Formatos de archivo y almacenamiento compatibles.

Última modificación

Esto se correlaciona con el campo Última modificación de Amazon S3. En Amazon S3, este campo almacena la fecha y la hora en que se creó o se modificó por última vez un objeto de S3, la que sea más reciente.

En el caso de un trabajo de detección de datos confidenciales, esta condición puede ser una fecha específica, una fecha y hora específicas o un intervalo de tiempo exclusivo:

- Para analizar los objetos que se modificaron por última vez después de una fecha y hora determinadas, introduzca los valores en los campos Desde.
- Para analizar los objetos que se modificaron por última vez después de una fecha y hora determinadas, introduzca los valores en los campos Hasta.
- Para analizar los objetos que se modificaron por última vez durante un intervalo de tiempo determinado, utilice los campos Desde para introducir los valores de la primera fecha o fecha y hora en el intervalo de tiempo. Utilice los campos Hasta para introducir los valores de la última fecha o fecha y hora del intervalo de tiempo.
- Para analizar los objetos que se modificaron por última vez durante un día determinado, introduzca la fecha en el campo Desde. Introduzca la fecha del día siguiente en el campo Hasta la fecha. A continuación, compruebe que ambos campos de hora estén en blanco. (Macie trata un campo de tiempo en blanco como `00:00:00`.) Por ejemplo, para analizar los objetos que se modificaron el 9 de agosto de 2023, introduzca **`2023/08/09`** en el campo Fecha desde, escriba **`2023/08/10`** en el campo Fecha hasta y no introduzca ningún valor en ninguno de los campos de tiempo.

Introduzca cualquier valor de hora en el horario universal coordinado (UTC) y utilice la notación de 24 horas.

Prefix

Esto se correlaciona con el campo Clave de Amazon S3. En Amazon S3, este campo almacena el nombre de un objeto de S3, incluido el prefijo del objeto. Un prefijo es similar a la ruta de un directorio dentro de un bucket. Permite agrupar objetos similares en un bucket, de forma similar a cuando se almacenan archivos similares en una carpeta de un sistema de archivos. Para obtener más información acerca de los prefijos y carpetas en Amazon S3, consulte Organizar objetos en la consola de Amazon S3 utilizando carpetas en la guía del usuario de Amazon Simple Storage Service.

Puede usar este tipo de condición para incluir o excluir objetos cuyas claves (nombres) comiencen por un valor determinado. Por ejemplo, para excluir todos los objetos cuya clave comience por AWSLogs, introdúzcala **`AWSLogs`** como valor para una condición de prefijo y, a continuación, elija Excluir.

Si introduce varios prefijos como valores para una condición, Macie utiliza la lógica OR para unir los valores. Por ejemplo, si introduce **`AWSLogs1`** y **`AWSLogs2`** como valores para una condición, cualquier objeto cuya clave comience por AWSLogs1 o AWSLogs2 coincidirá con los criterios de la condición.

Cuando introduzca un valor para una condición de Prefijo, tenga en cuenta lo siguiente:

- Los valores distinguen entre mayúsculas y minúsculas.
- Macie no admite el uso de caracteres comodín en estos valores.
- En Amazon S3, la clave de un objeto no incluye el nombre del depósito que almacena el objeto. Por este motivo, no especifique los nombres de los buckets en estos valores.
- Si un prefijo incluye un delimitador, inclúyalo en el valor. Por ejemplo, introduzca **`AWSLogs/eventlogs`** para definir una condición para todos los objetos cuya clave comience por AWSLogs/eventlogs. Macie admite el delimitador predeterminado de Amazon S3, que es una barra (/), y los delimitadores personalizados.

Tenga en cuenta también que un objeto cumple con los criterios de una condición solo si la clave del objeto coincide exactamente con el valor que ha introducido, empezando por el primer carácter de la clave del objeto. Además, Macie aplica una condición al valor Clave completo de un objeto, incluido el nombre de archivo del objeto.

Por ejemplo, si la clave de un objeto es AWSLogs/eventlogs/testlog.csv y se introduce alguno de los siguientes valores para una condición, el objeto coincide con los criterios de la condición:

- **`AWSLogs`**
- **`AWSLogs/event`**
- **`AWSLogs/eventlogs/`**
- **`AWSLogs/eventlogs/testlog`**
- **`AWSLogs/eventlogs/testlog.csv`**

Sin embargo, si lo introduce***`eventlogs`***, el objeto no cumple los criterios: el valor de la condición no incluye la primera parte de la clave,AWSLogs/. Del mismo modo, si introduce **`awslogs`**, el objeto no cumple los criterios debido a las diferencias en el uso de mayúsculas y minúsculas.

Tamaño del almacenamiento

Esto se correlaciona con el campo Tamaño de Amazon S3. En Amazon S3, este campo indica el tamaño total de almacenamiento de un objeto de S3. Si un objeto es un archivo comprimido, este valor no refleja el tamaño real del archivo después de descomprimirlo.

Puede usar este tipo de condición para incluir o excluir objetos que sean más pequeños que un tamaño determinado, más grandes que un tamaño determinado o que estén dentro de un rango de tamaño determinado. Macie aplica este tipo de condición a todos los tipos de objetos, incluidos

los archivos comprimidos o archivados y los archivos que contienen. Para obtener información sobre las restricciones basadas en el tamaño para cada formato compatible, consulte Cuotas de Amazon Macie.

Etiquetas

Las etiquetas asociadas a un objeto de S3. Las etiquetas son etiquetas que se pueden definir y asignar a determinados tipos de AWS recursos, incluidos los objetos de S3. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Para obtener información sobre el etiquetado de objetos de S3, consulte Categorización del almacenamiento mediante etiquetas en la Guía del usuario de Amazon Simple Storage Service.

Para un trabajo de detección de datos confidenciales, puede usar este tipo de condición para incluir o excluir objetos que tengan una etiqueta específica. Puede ser una clave de etiqueta específica o una clave de etiqueta y un valor de etiqueta específicos (como par). Si introduce varias extensiones de nombre de archivo como valores para una condición, Macie utiliza la lógica OR para unir los valores. Por ejemplo, si especifica **`Project1`** y **`Project2`** como claves de etiqueta para una condición, cualquier objeto que tenga la clave de etiqueta Project1 o Project2 cumplirá los criterios de la condición.

Las claves y los valores de las etiquetas no distinguen entre mayúsculas y minúsculas. Además, Macie no admite el uso de valores parciales o caracteres comodín en este tipo de condición.

Creación de un trabajo de detección de datos confidenciales

Con Amazon Macie, puede crear y ejecutar trabajos de descubrimiento de datos confidenciales para automatizar la detección, el registro y la notificación de datos confidenciales en los depósitos de uso general de Amazon Simple Storage Service (Amazon S3). Un trabajo de detección de datos confidenciales es una serie de tareas automatizadas de procesamiento y análisis que Macie realiza para detectar y reportar datos confidenciales en objetos de Amazon S3. A medida que avanza el análisis, Macie proporciona informes detallados sobre los datos confidenciales que encuentra y los análisis que realiza: los resultados de datos confidenciales, que muestran los datos confidenciales que Macie encuentra en objetos S3 individuales, y los resultados de detección de datos confidenciales, que registran detalles sobre el análisis de objetos S3 individuales. Para obtener más información, consulte Revisión de estadísticas y resultados de un trabajo.

Al crear un trabajo, empieza por especificar qué depósitos de S3 almacenan los objetos que desea que Macie analice cuando se ejecute el trabajo: depósitos específicos que usted selecciona o depósitos que cumplen criterios específicos. A continuación, especifique la frecuencia de

ejecución del trabajo: una vez o periódicamente, a diario, semanal o mensualmente. También puede elegir opciones para mejorar el alcance del análisis del trabajo. Las opciones incluyen criterios personalizados que se derivan de las propiedades de los objetos de S3, como las etiquetas, los prefijos y la fecha en que se modificó un objeto por última vez.

Tras definir el cronograma y el alcance del trabajo, debe especificar qué identificadores de datos gestionados e identificadores de datos personalizados utilizar:

- Un identificador de datos gestionados es un conjunto de criterios y técnicas integrados que están diseñados para detectar un tipo específico de datos confidenciales, por ejemplo, números de tarjetas de crédito, claves de acceso AWS secretas o números de pasaporte de un país o región determinados. Estos identificadores pueden detectar una lista extensa y creciente de tipos de datos confidenciales en muchos países y regiones, incluidos varios tipos de datos de credenciales, información financiera e información de identificación personal (PII). Para obtener más información, consulte Uso de identificadores de datos administrados.
- Un identificador de datos personalizado es un conjunto de criterios que se define para detectar información confidencial. Con los identificadores de datos personalizados, puede detectar datos confidenciales que reflejen escenarios particulares, propiedad intelectual o datos de propietario, por ejemplo, identificaciones de empleados, números de cuentas de clientes o clasificaciones de datos internos. Pueden complementar los identificadores de datos administrados que Macie proporciona. Para obtener más información, consulte Creación de identificadores de datos personalizados.

A continuación, puede seleccionar, si lo desea, permitir el uso de listas. Una lista de permitidos especifica el texto o un patrón de texto que usted quiere que Macie ignore, normalmente excepciones de datos confidenciales para sus escenarios o entornos particulares, por ejemplo, nombres públicos o números de teléfono de su organización o datos de muestra que su organización utiliza para las pruebas. Para obtener más información, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

Cuando termine de elegir estas opciones, estará listo para introducir la configuración general del trabajo, como el nombre y la descripción del trabajo. A continuación, puede revisar y guardar el trabajo.

Tareas

- Antes de empezar
- Paso 1: Elegir buckets S3

- Paso 2: Revisión de las selecciones o criterios de bucket de S3
- Paso 3: Definir el cronograma y mejorar el alcance
- Paso 4: Seleccione los identificadores de datos gestionados
- Paso 5: Seleccione identificadores de datos personalizados
- Paso 6: Selección de listas de permitidos
- Paso 7: Introducir configuración general
- Paso 4: revisar y crear

Antes de empezar

Antes de crear un trabajo, es una buena idea seguir los siguientes pasos:

- Compruebe que haya configurado un repositorio para los resultados de la detección de datos confidenciales. Para ello, seleccione Resultados de la detección en el panel de navegación de la consola de Amazon Macie. Para obtener más información sobre estos ajustes, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.
- Cree los identificadores de datos personalizados que desee que utilice el trabajo. Para saber cómo hacerlo, consulte Creación de identificadores de datos personalizados.
- Cree las listas de permisos que desee que utilice el trabajo. Para saber cómo hacerlo, consulte Creación y administración de listas de permitidos.
- Si desea analizar los objetos de S3 que están cifrados, asegúrese de que Macie puede acceder a las claves de cifrado adecuadas y utilizarlas. Para obtener más información, consulte Análisis de objetos S3 cifrados.
- Si quiere analizar los objetos de un bucket de S3 que tiene una política de bucket restrictiva, asegúrese de que Macie puede acceder a los objetos. Para obtener más información, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Si hace esto antes de crear un trabajo, agiliza la creación del trabajo y ayuda a garantizar que el trabajo puede analizar los datos que desea.

Paso 1: Elegir buckets S3

Al crear un trabajo, el primer paso consiste en especificar qué depósitos de S3 almacenan los objetos que desea que Macie analice cuando se ejecute el trabajo. Dispone de dos opciones para hacerlo:

- Seleccione depósitos específicos: con esta opción, selecciona de forma explícita cada uno de los depósitos de S3 que desee analizar. Luego, cuando se ejecuta el trabajo, analiza los objetos solo en los buckets que seleccione.
- Especificar los criterios de los depósitos: con esta opción, se definen los criterios de tiempo de ejecución que determinan los depósitos de S3 que se van a analizar. Los criterios consisten en una o más condiciones que se derivan de las propiedades del bucket. A continuación, cuando se ejecuta el trabajo, identifica los buckets que coinciden con sus criterios y analiza los objetos de esos buckets.

Para obtener información detallada sobre estas opciones, consulte Opciones de ámbito para trabajos.

Las siguientes secciones proporcionan instrucciones para elegir y configurar cada opción. Elija la sección para la opción que desee.

Seleccionar buckets específicos

Si eliges seleccionar de forma explícita cada uno de los cubos de S3 que deseas analizar, Macie te proporcionará un inventario completo de los depósitos de uso general actuales. Región de AWS A continuación, puede utilizar este inventario para seleccionar uno o más cubos para el trabajo. Para obtener más información sobre este inventario, consulte Selección de buckets de S3 específicos.

Si es el administrador de Macie de una organización, el inventario incluye buckets que son propiedad de las cuentas de miembros de su organización. Puede seleccionar hasta 1000 de estos buckets, que abarquen hasta 1000 cuentas.

Para seleccionar cubos S3 específicos para el trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Trabajos.
3. Seleccione Crear trabajo.
4. En la página Elegir buckets de S3, seleccione Seleccionar buckets específicos. Macie muestra una tabla con todos los grupos de uso general de su cuenta en la región actual.
5. En la sección Seleccionar buckets de S3, si lo desea, elija refrescar () para recuperar los metadatos de bucket más recientes de Amazon S3.

Si el icono de información
(ⓘ)
aparece junto al nombre de algún bucket, le recomendamos que lo haga. Este icono indica que se creó un bucket durante las últimas 24 horas, posiblemente después de que Macie recuperara por última vez los metadatos del bucket y del objeto de Amazon S3 como parte del ciclo de actualización diario.

6. En la tabla, active la casilla de verificación de cada bucket de que desea que el trabajo analice.

> **Tip**
>
> - Para encontrar buckets específicos más fácilmente, introduzca los criterios de filtro en el cuadro de filtro situado sobre la tabla. Puede ordenar las filas de la tabla si elige un encabezado de columna.
> - Para determinar si ya ha configurado un trabajo para analizar periódicamente los objetos de un bucket, consulte el campo Supervisado por trabajo. Si el valor de un campo es Sí, el bucket se incluye explícitamente en un trabajo periódico o el bucket ha cumplido los criterios de un trabajo periódico en las últimas 24 horas. Además, el estado de al menos uno de esos trabajos no es Cancelado. Macie actualiza estos datos a diario.
> - Para determinar cuándo fue la última vez que un trabajo periódico o único existente analizó los objetos de un bucket, consulte el campo Último trabajo ejecutado. Para obtener información adicional sobre ese trabajo, consulte los detalles del bucket.
> - Para mostrar los detalles de un bucket, elija el nombre del bucket. Además de la información relacionada con el trabajo, el panel de detalles proporciona estadísticas y otra información sobre el bucket, como la configuración de acceso público del bucket. Para obtener más información sobre esto, consulte Revisar el inventario de bucket de S3.

7. Cuando termine de seleccionar los buckets, elija Siguiente.

En el siguiente paso, revisará y verificará las selecciones.

Especificar los criterios del bucket

Si decide especificar los criterios de tiempo de ejecución que determinan qué depósitos de S3 analizar, Macie ofrece opciones que le ayudarán a elegir campos, operadores y valores para las

condiciones individuales de los criterios. Para más información sobre estas opciones, consulte Especificar los criterios de los buckets de S3.

Para especificar los criterios del bucket de S3 para el trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Trabajos.
3. Seleccione Crear trabajo.
4. En la página Elegir buckets de S3, elija Especificar los criterios del bucket.
5. En Especificar los criterios del bucket, haga lo siguiente para añadir una condición a los criterios:

   a. Coloque el cursor en el cuadro Criterios de filtrado y, a continuación, elija la propiedad del bucket que desee utilizar para la condición.

   b. En el primer cuadro, elija un operador para la condición: Igual o No igual.

   c. En el cuadro siguiente, introduzca uno o más valores para la propiedad.

      Según el tipo y la naturaleza de la propiedad del bucket, Macie muestra diferentes opciones para introducir valores. Por ejemplo, si elige la propiedad de Permiso efectivo, Macie mostrará una lista de valores entre los que elegir. Si selecciona la propiedad ID de cuenta, Macie mostrará un cuadro de texto en el que podrá introducir uno o varios ID de Cuenta de AWS . Para introducir varios valores en un cuadro de texto, introduzca cada valor y separe cada entrada con una coma.

   d. Seleccione Apply. Macie añade la condición y la muestra debajo del cuadro de filtro.

      De forma predeterminada, Macie añade la condición con una sentencia include. Esto significa que el trabajo está configurado para analizar (incluir) objetos en buckets que coincidan con la condición. Para omitir (excluir) los buckets que coincidan con la condición, elija Incluir para la condición y, a continuación, elija Excluir.

   e. Repita los pasos anteriores para cada condición adicional que desee agregar a los criterios.
6. Para probar sus criterios, amplíe la sección Vista previa de los resultados de los criterios. En esta sección se muestra una tabla de grupos de uso general que actualmente cumplen con los criterios.
7. Para mejorar los criterios, lleve a cabo alguna de las siguientes acciones:

   - Para eliminar una condición, elija X para la condición .

- Para cambiar una condición, elimine la condición eligiendo X para la condición A continuación, añada una condición que tenga la configuración correcta.
- Para eliminar todas las condiciones, seleccione Borrar filtros.

Macie actualiza los resultados de la tabla de criterios para reflejar sus cambios.

8. Cuando termine de especificar los criterios del bucket, seleccione Siguiente.

En el siguiente paso, revisará y verificará sus criterios.

Paso 2: Revisión de las selecciones o criterios de bucket de S3

Para este paso, compruebe que ha elegido la configuración correcta en el paso anterior:

- Revise sus selecciones de buckets: si seleccionó buckets de S3 específicos para el trabajo, revise la tabla de buckets y cambie sus selecciones de buckets según sea necesario. La tabla proporciona información sobre el alcance y el costo proyectados del análisis del trabajo. Los datos se basan en el tamaño y los tipos de objetos que se almacenan actualmente en un bucket.

  En la tabla de este paso, el campo Costo estimado indica el costo total estimado (en dólares estadounidenses) del análisis de objetos de un bucket de S3. Cada estimación refleja la cantidad proyectada de datos sin comprimir que el trabajo analizará en un bucket. Si algún objeto es un archivo comprimido o archivado, la estimación supone que los archivos utilizan una relación de compresión de 3:1, y que el trabajo puede analizar todos los archivos extraídos. Para obtener más información, consulte Previsión y supervisión de costos.
- Revise los criterios del bucket: si especificó los criterios del bucket para el trabajo, revise cada condición de los criterios. Para cambiar los criterios, elija Anterior y, a continuación, utilice las opciones de filtro del paso anterior para introducir los criterios correctos. Cuando haya terminado, elija Siguiente.

Cuando termine de revisar y verificar la configuración, elija Siguiente.

Paso 3: Definir el cronograma y mejorar el alcance

Para este paso, especifique la frecuencia con la que desea que el trabajo se ejecute: una vez o periódicamente, a diario, semanal o mensualmente. También puede elegir opciones para mejorar el alcance del análisis del trabajo. Para obtener más información sobre estas opciones, consulte Opciones de ámbito para trabajos.

Paso 3: Definir el cronograma y mejorar el alcance

1. En la página Ajustar el ámbito, especifique la frecuencia con la que desea que se ejecute el trabajo:

   - Para ejecutar el trabajo solo una vez, inmediatamente después de terminar de crearlo, elija Trabajo único.
   - Para ejecutar el trabajo periódicamente de forma recurrente, elija Trabajo programado. En Frecuencia de actualización, elija si desea ejecutar el trabajo de forma diaria, semanal o mensual. A continuación, utilice la opción Incluir objetos existentes para definir el alcance de la primera ejecución del trabajo:
     - Seleccione esta casilla de verificación para analizar todos los objetos existentes y aptos inmediatamente después de crear el trabajo. Cada ejecución posterior del trabajo periódico analiza solo los objetos creados o modificados después de la ejecución anterior.
     - Desactive esta casilla de verificación para omitir el análisis de los objetos existentes. La primera ejecución analiza solo los objetos que se crean o se modifican después de terminar la creación del trabajo. Cada ejecución posterior del trabajo periódico analiza solo los objetos creados o modificados después de la ejecución anterior.

       Desactivar esta casilla de verificación resulta útil en los casos en los que ya ha analizado los datos y desea seguir analizándolos periódicamente. Por ejemplo, si ha utilizado anteriormente otro servicio o aplicación para clasificar los datos y ha empezado a utilizar Macie recientemente, puede utilizar esta opción para garantizar el descubrimiento y la clasificación de forma continua de los datos sin incurrir en costos innecesarios ni duplicar los datos de clasificación.
2. (Opcional) Para especificar el porcentaje de objetos que desea analizar en el trabajo, introduzca el porcentaje en el cuadro Profundidad de muestreo.

   Si este valor es menor que el 100 %, Macie selecciona de forma aleatoria los objetos que se van a analizar, hasta el porcentaje especificado y analiza todos los datos de esos objetos. El valor predeterminado es 100 %.
3. (Opcional) Para añadir criterios específicos que determinen qué objetos de S3 se incluyen o excluyen del análisis del trabajo, amplíe la sección Configuración adicional y, a continuación, introduzca los criterios. Estos criterios se componen de condiciones individuales que se derivan de las propiedades de los objetos:

- Para analizar (incluir) los objetos que cumplen una condición específica, introduzca el tipo y el valor de la condición y, a continuación, elija Incluir.
- Para omitir (excluir) los objetos que cumplen una condición específica, introduzca el tipo y el valor de la condición y, a continuación, elija Excluir.

Repita este paso para cada condición de inclusión o exclusión que desee.

Si introduce varias condiciones, cualquier condición de exclusión tendrá prioridad sobre las condiciones de inclusión. Por ejemplo, si incluye objetos que tienen la extensión de nombre de archivo .pdf y excluye los objetos que pesan más de 5 MB, el trabajo analiza cualquier objeto que tenga la extensión de nombre de archivo .pdf, a menos que el objeto supere los 5 MB.

4. Cuando haya terminado, elija Siguiente.

Paso 4: Seleccione los identificadores de datos gestionados

Para este paso, especifique qué identificadores de datos administrados desea que el trabajo utilice cuando analice objetos de S3. Dispone de dos opciones para hacerlo:

- Utilice la configuración recomendada: con esta opción, el trabajo analiza los objetos de S3 mediante el conjunto de identificadores de datos gestionados que recomendamos para los trabajos. Este conjunto está diseñado para detectar categorías y tipos comunes de datos confidenciales. Para revisar una lista de los identificadores de datos gestionados que se encuentran actualmente en el conjunto, consulte Identificadores de datos administrados recomendados para trabajos. Actualizamos esa lista cada vez que añadimos o eliminamos un identificador de datos gestionados del conjunto.
- Utilice la configuración recomendada: con esta opción, el trabajo analiza los objetos de S3 mediante el conjunto de identificadores de datos gestionados que rseleccione. Pueden ser todos o solo algunos de los identificadores de datos gestionados que están disponibles actualmente. También puede configurar el trabajo para que no utilice ningún identificador de datos gestionados. En su lugar, el trabajo solo puede usar los identificadores de datos personalizados que seleccione en el siguiente paso. Para revisar una lista de los identificadores de datos gestionados que están disponibles actualmente, consulte. Referencia rápida: identificadores de datos administrados por Amazon Macie Actualizamos esa lista cada vez que publicamos un nuevo identificador de datos gestionados.

Al elegir cualquiera de las dos opciones, Macie muestra una tabla de identificadores de datos gestionados. En la tabla, el campo de Tipo de datos confidenciales especifica el identificador único (ID) de un identificador de datos administrados. Este identificador describe el tipo de datos confidenciales que el identificador de datos gestionados está diseñado para detectar, por ejemplo: USA_PASSPORT_NUMBER para los números de pasaporte estadounidenses, CREDIT_CARD_NUMBER para los números de tarjetas de crédito y PGP_PRIVATE_KEY para las claves privadas PGP. Para encontrar identificadores específicos con mayor rapidez, puede ordenar y filtrar la tabla por categoría o tipo de datos confidenciales.

Para seleccionar identificadores de datos administrados para el trabajo

1. En la página Seleccionar identificadores de datos gestionados, en Opciones de identificadores de datos gestionados, realice una de las siguientes acciones:

   - Para usar el conjunto de identificadores de datos gestionados que recomendamos para los trabajos, seleccione Recomendado.

     Si elige esta opción y ha configurado el trabajo para que se ejecute más de una vez, cada ejecución utilizará automáticamente todos los identificadores de datos gestionados incluidos en el conjunto recomendado cuando se inicie la ejecución. Esto incluye los nuevos identificadores de datos gestionados que publicamos y añadimos al conjunto. Excluye los identificadores de datos gestionados que eliminamos del conjunto y que ya no recomendamos para los trabajos.
   - Para usar solo los identificadores de datos administrados específicos que seleccione, elija Personalizado y, a continuación, elija Usar identificadores de datos administrados específicos. A continuación, en la tabla, active la casilla de verificación de cada identificador de datos administrados que desee que el trabajo utilice.

     Si elige esta opción y ha configurado el trabajo para que se ejecute más de una vez, cada ejecución utilizará únicamente los identificadores de datos gestionados que seleccione. En otras palabras, el trabajo utiliza estos mismos identificadores de datos gestionados cada vez que se ejecuta.
   - Para utilizar todos los identificadores de datos gestionados que Macie proporciona actualmente, seleccione Personalizado y, a continuación, elija Utilizar identificadores de datos gestionados específicos. A continuación, en la tabla, active la casilla de verificación situada en el encabezado de la columna de selección para seleccionar todas las filas.

Si elige esta opción y ha configurado el trabajo para que se ejecute más de una vez, cada ejecución utilizará únicamente los identificadores de datos gestionados que seleccione. En otras palabras, el trabajo utiliza estos mismos identificadores de datos gestionados cada vez que se ejecuta.

- Para no utilizar ningún identificador de datos gestionado y utilizar únicamente identificadores de datos personalizados, seleccione Personalizado y, a continuación, seleccione No utilizar ningún identificador de datos gestionado. A continuación, en el siguiente paso, seleccione los identificadores de datos personalizados que quiere usar.

2. Cuando haya terminado, elija Siguiente.

Paso 5: Seleccione identificadores de datos personalizados

Para este paso, de forma opcional seleccione los identificadores de datos personalizados que desea que el trabajo utilice cuando analice datos. El trabajo utilizará los identificadores seleccionados además de los identificadores de datos administrados que desee que utilice el trabajo. Para obtener más información sobre los identificadores de datos personalizados, consulte Creación de identificadores de datos personalizados.

Para seleccionar identificadores de datos personalizados para el trabajo

1. En la página Seleccionar identificadores de datos personalizados, active la casilla de verificación de cada identificador de datos personalizado que desee que utilice el trabajo. Puede seleccionar hasta 30 identificadores de datos personalizados.

> **Tip**
>
> Para revisar o probar un identificador de datos personalizado antes de seleccionarlo, elija el icono de conexión () junto al nombre del identificador. Macie abre una página que muestra la configuración del identificador.
>
> También puede usar esta página para probar el identificador con datos de muestra. Para ello, introduzca hasta 1000 caracteres en el cuadro Datos de muestra y, a continuación, seleccione Prueba. Macie evalúa los datos de la muestra mediante el identificador y, a continuación, indica el número de coincidencias.

2. Cuando termine de seleccionar los identificadores de datos personalizados, elija Siguiente.

Paso 6: Selección de listas de permitidos

Para este paso, seleccione las listas de permisos que desea que el trabajo utilice cuando analice objetos de S3. Para obtener más información acerca de seleccionar listas, consulte Definición de excepciones de datos confidenciales con las listas de permitidos.

Para seleccionar listas de permisos para el trabajo

1. En la página Seleccionar listas de permitidos, active la casilla de verificación de cada lista de permitidos que desee que el trabajo utilice. Puede seleccionar hasta 10 listas.

> **Tip**
>
> Para revisar la configuración de una lista de permitidos antes de seleccionarla, elija el icono de conexión
> ( )
> junto al nombre de la lista. Macie abre una página que muestra la configuración de la lista.
> Si la lista especifica una expresión regular (regex), también puede usar esta página para probar la expresión regular con datos de ejemplo. Para ello, introduzca hasta 1000 caracteres en el cuadro Datos de muestra y, a continuación, seleccione Prueba. Macie evalúa los datos de la muestra mediante el identificador y, a continuación, informa el número de coincidencias.

2. Cuando termine de seleccionar las listas permitidas, elija Siguiente.

Paso 7: Introducir configuración general

Para este paso, especifique un nombre y, opcionalmente, una descripción del trabajo. También puede asignar etiquetas al trabajo. Una etiqueta es una etiqueta que se define y se asigna a determinados tipos de AWS recursos. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

Para introducir la configuración general del trabajo

1. En la página Introducir la configuración general, introduzca un nombre para el trabajo en el cuadro Nombre del trabajo. El nombre puede contener hasta 500 caracteres.
2. (Opcional) En Descripción de imagen, introduzca una breve descripción del trabajo. La descripción puede contener hasta 200 caracteres.
3. (Opcional) En Etiquetas, seleccione Añadir etiqueta y, a continuación, introduzca hasta 50 etiquetas para asignarlas a la lista de permitidos.
4. Cuando haya terminado, elija Siguiente.

Paso 4: revisar y crear

En este último paso, revise los ajustes de configuración del trabajo y verifique que son correctos. Este es un paso importante. Tras crear un trabajo, no puede cambiar ninguna de estas opciones. Esto ayuda a garantizar que tiene un historial inmutable de resultados de datos confidenciales y resultados de detección para las auditorías o investigaciones de privacidad y protección de datos que lleve a cabo.

También puede revisar el costo estimado (en dólares estadounidenses) de ejecutar el trabajo una vez y cambiar la configuración del trabajo según sea necesario. Si especificó los criterios de bucket para el trabajo, la estimación se basa en el tamaño y los tipos de objetos de hasta 500 buckets que cumplen actualmente los criterios y en la cantidad de esos datos que puede analizar el trabajo. Si especificó los criterios de bucket para el trabajo, la estimación se basa en el tamaño y los tipos de objetos de hasta 500 buckets que cumplen actualmente los criterios y en la cantidad de esos datos que puede analizar el trabajo. Para obtener más información sobre esto, consulte Previsión y supervisión de costos.

Revise y cree la VM.

1. En la página Revisar y crear, revise cada configuración y compruebe que es correcta. Para cambiar una configuración, elija Editar para la configuración y, a continuación, escriba la configuración adecuada. También puede usar las pestañas de navegación para ir a la página que contiene una configuración.
2. Cuando termine de verificar la configuración, seleccione Enviar para crear y guardar el trabajo. Macie comprueba la configuración y le notifica los problemas que debe solucionar.

> **Note**
>
> Si no ha configurado un repositorio para sus resultados de detección de datos confidenciales, Macie muestra una advertencia y no guarda el trabajo. Para solucionar este problema, seleccione Configurar en la sección Repositorio de resultados de detección de datos confidenciales. A continuación, introduzca las opciones de configuración para el repositorio. Para saber cómo hacerlo, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales. Tras introducir la configuración, vuelva a la página Revisar y crear y, a continuación, seleccione refrescar () en la sección de Resultados del repositorio de datos confidenciales de la página. Aunque no lo recomendamos, puede anular temporalmente el requisito de repositorio y guardar el trabajo. Si lo hace, corre el riesgo de perder los resultados de detección derivados del trabajo; Macie retendrá los resultados solo durante 90 días. Para anular temporalmente el requisito, active la casilla de la verificación de la opción de anulación.

3. Si Macie le notifica los problemas que debe solucionar, solucione los problemas y, a continuación, vuelva a seleccionar Enviar para crear y guardar el trabajo.

Si ha configurado el trabajo para que se ejecute una vez, diariamente o en el día actual de la semana o el mes, comienza inmediatamente a ejecutar el trabajo. De lo contrario, se prepara para ejecutar el trabajo el día especificado de la semana o el mes. Para supervisar el trabajo, puede comprobar el estado del trabajo.

Revisión de estadísticas y resultados para trabajos de detección de datos confidenciales

Cuando ejecuta un trabajo de detección de datos confidenciales, Amazon Macie calcula e informa automáticamente determinados datos estadísticos para el trabajo. Por ejemplo, Macie informa el número de veces que se ha ejecutado el trabajo y el número aproximado de objetos de Amazon Simple Storage Service (Amazon S3) que el trabajo aún no ha procesado durante su ejecución actual. Macie también produce varios tipos de resultados para el trabajo: eventos de registro, resultados de datos confidenciales y resultados de detección de datos confidenciales.

Temas

- Tipos de resultados para trabajos de detección de datos confidenciales

- Revisión de las estadísticas y los resultados de un trabajo de detección de datos confidenciales

Tipos de resultados para trabajos de detección de datos confidenciales

A medida que avanza un trabajo de detección de datos confidenciales, Amazon Macie produce los siguientes tipos de resultados para el trabajo.

evento de registro

Se trata de un registro de un evento que se produjo mientras se ejecutaba el trabajo. Macie registra y publica automáticamente los datos de determinados eventos en los Registros de Amazon CloudWatch. Los datos de estos registros proporcionan un registro de los cambios en el progreso o el estado del trabajo, como la fecha y la hora exactas en que el trabajo comenzó o dejó de ejecutarse. Los datos también proporcionan detalles sobre cualquier error a nivel de cuenta o de bucket que se haya producido durante la ejecución del trabajo.

Los eventos de registro pueden ayudarle a supervisar un trabajo y a solucionar cualquier problema que haya impedido que el trabajo analice los datos que desea. Si un trabajo utiliza criterios de tiempo de ejecución para determinar qué bucket de S3 analizar, el evento de registro también puede ayudarle a determinar si los buckets de S3 cumplían los criterios cuando se ejecutó el trabajo.

Puede acceder a los eventos de registro mediante la consola de Amazon CloudWatch o la API de Registros de Amazon CloudWatch. Para ayudarle a navegar hasta el evento de registro de un trabajo, la consola de Amazon Macie proporciona un enlace a ellos. Para obtener más información, consulte Monitoreo de trabajos.

Resultados de datos confidenciales

Este es un informe de información confidencial que Macie encontró en un objeto de S3. Cada resultado proporciona una clasificación de gravedad y detalles como:

- La fecha y hora en que Macie encontró los datos confidenciales.
- La categoría y los tipos de datos confidenciales que encontró Macie.
- El número de apariciones de cada tipo de datos confidenciales que Macie encontró.
- El identificador único del trabajo de detección de datos confidenciales que produjo el resultado.
- El nombre, la configuración de acceso público, el tipo de cifrado y otra información sobre el bucket y el objeto de S3 afectados.

Según el tipo de archivo o el formato de almacenamiento del objeto S3 afectado, los detalles también pueden incluir la ubicación de hasta 15 apariciones de los datos confidenciales que Macie encontró. Para informar sobre los datos de ubicación, los resultados del descubrimiento de datos confidenciales utilizan un esquema JSON estandarizado.

Los resultados de datos confidenciales no incluyen los datos confidenciales que encontró Macie. En cambio, proporciona información que puede utilizar para investigar y corregir más a fondo, según sea necesario.

Macie almacena los resultados de datos confidenciales durante 90 días. Puede acceder a ellos mediante la consola de Amazon Macie o la API de Amazon Macie. Puede también supervisarlos y procesarlos mediante otras aplicaciones, servicios y sistemas. Para obtener más información, consulte Análisis de resultados.

Resultado de la detección de datos confidenciales

Este es un registro de detalles sobre el análisis de un objeto de S3. Macie crea automáticamente un resultado de detección de datos confidenciales para cada objeto que usted configure de un trabajo para analizar. Esto incluye objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no produce datos confidenciales y objetos que Macie no puede analizar debido a errores o problemas como la configuración de permisos o el uso de un archivo o formato de almacenamiento no compatible.

Si Macie encuentra datos confidenciales en un objeto de S3, el resultado de detección de datos confidenciales incluirá los datos del resultado correspondiente. También proporciona información adicional, como la ubicación de hasta 1000 apariciones de cada tipo de datos confidenciales que Macie encontró en el objeto. Por ejemplo:

- El número de columna y fila de una celda o campo de un libro de Microsoft Excel, un archivo CSV o un archivo TSV
- La ruta a un campo o matriz en un archivo JSON o líneas JSON
- El número de línea de una línea de un archivo de texto no binario que no sea un archivo CSV, JSON, líneas JSON o TSV, por ejemplo, un archivo HTML, TXT o XML
- El número de página de una página de un archivo en formato de documento portátil (PDF) de Adobe
- El índice de registro y la ruta a un campo de un registro en un contenedor de objetos de Apache Avro o un archivo de Apache Parquet

Si el objeto S3 afectado es un archivo de almacenamiento, como un archivo .tar o .zip, el resultado de la detección de datos confidenciales también proporciona datos de ubicación

detallados para la aparición de datos confidenciales en archivos individuales que Macie extrae del archivo. Macie no incluye esta información en los resultados de datos confidenciales para los archivos archivados. Para informar sobre los datos de ubicación, los resultados de la detección de datos confidenciales utilizan un esquema JSON estandarizado.

Un resultado de detección de datos confidenciales no incluye los datos confidenciales que encontró Macie. En cambio, le proporciona un registro de análisis que puede resultar útil para auditorías o investigaciones sobre la privacidad y la protección de los datos.

Macie almacena los resultados de la detección de datos confidenciales durante 90 días. No puede acceder a ellos directamente en la consola de Amazon Macie ni con la API de Amazon Macie. En cambio, usted configura Macie para que los cifre y almacene en un bucket de S3. El bucket puede servir como un repositorio definitivo y a largo plazo para todos sus resultados de detección de datos confidenciales. A continuación, si lo desea, puede acceder a los resultados de ese repositorio y consultarlos. Para obtener información sobre cómo configurar estos ajustes, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Tras configurar los ajustes, Macie graba los resultados de detección de datos confidenciales en archivos líneas JSON (.jsonl), los cifra y los añade al bucket de S3 como archivos GNU Zip (.gz). Para ayudarle a navegar hasta los resultados, la consola de Amazon Macie proporciona enlaces a los mismos.

Tanto los resultados de datos confidenciales como los de detección de datos confidenciales siguen esquemas estandarizados. De forma opcional, esto puede ayudarle a consultarlos, supervisarlos y procesarlos mediante otras aplicaciones, servicios y sistemas.

> **Tip**
>
> Para ver un ejemplo detallado e instructivo de cómo puede consultar y utilizar los resultados de la detección de datos confidenciales para analizar e informar sobre los posibles riesgos de seguridad de los datos, consulte la entrada del blog Cómo consultar y visualizar los resultados de la detección de datos confidenciales de Macie con Amazon Athena y Amazon QuickSight en el AWSBlog de seguridad.
> Para ver ejemplos de consultas de Amazon Athena que puede usar para analizar los resultados de la detección de datos confidenciales, visite el repositorio de Amazon Macie Results Analytics en GitHub. Este repositorio también proporciona instrucciones para

configurar Athena para recuperar y descifrar los resultados, y scripts para crear tablas para los resultados.

Revisión de las estadísticas y los resultados de un trabajo de detección de datos confidenciales

Para revisar las estadísticas y los resultados de los trabajos individuales de detección de datos confidenciales, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Siga estos pasos para revisar las estadísticas y los resultados de un trabajo mediante la consola.

Para acceder a las estadísticas de procesamiento de un trabajo mediante programación, utilice la operación DescribeClassificationJob de la API Amazon Macie. Para acceder mediante programación a los resultados generados por un trabajo, utilice la operación ListFindings de la API Amazon Macie y especifique el identificador único del trabajo en una condición de filtro para el campo `classificationDetails.jobId`. Para saber cómo hacerlo, consulte Crear y aplicar filtros a los resultados. A continuación, utilice la operación GetFindings para recuperar los detalles de esos resultados.

Revisión de estadísticas y resultados de un trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Jobs (Trabajos).
3. En la página Trabajos, elija el nombre del trabajo cuyas estadísticas y resultados desee revisar. El panel de detalles muestra las estadísticas, la configuración y otra información sobre el trabajo.
4. En la página de detalles, realice alguna de las siguientes acciones:

   - Para revisar las estadísticas de procesamiento del trabajo, consulte la sección Estadísticas del panel. En esta sección se muestran estadísticas como el número de veces que se ha ejecutado el trabajo y el número aproximado de objetos que el trabajo aún no ha procesado durante su ejecución actual.
   - Para revisar los eventos de registro del trabajo, elija Mostrar resultados en la parte superior del panel y, a continuación, elija Mostrar registros de CloudWatch. Macie abre la consola Amazon CloudWatch y muestra una tabla con los eventos de registro que Macie publicó para el trabajo.
   - Para revisar todos los datos confidenciales encontrados en el trabajo, seleccione Mostrar resultados en la parte superior del panel y, a continuación, elija Mostrar resultados. Macie abre

la página de Resultados y muestra todos los resultados del trabajo. Para consultar los detalles de un resultado, elija el resultado y consulte el panel de detalles.

> **Tip**
>
> En el panel de detalles de búsqueda, puede utilizar el enlace del campo Ubicación detallada del resultado para navegar hasta el resultado de detección de datos confidenciales correspondiente en Amazon S3:
>
> - Si el resultado se refiere a un archivo comprimido o a un archivo comprimido de gran tamaño, el enlace muestra la carpeta que contiene los resultados de detección del archivo. Un archivo comprimido o comprimido es grande si genera más de 100 resultados de detección.
> - Si el resultado se refiere a un archivo pequeño o a un archivo comprimido, el enlace muestra el archivo que contiene los resultados de detección del archivo. Un archivo o archivo comprimido es pequeño si genera 100 o menos resultados de detección.
> - Si el resultado se refiere a otro tipo de archivo, el enlace muestra el archivo que contiene los resultados de detección del archivo.

- Para revisar todos los datos confidenciales encontrados en el trabajo, elija Mostrar resultados en la parte superior del panel y, a continuación, elija Mostrar resultados. Macie abre la consola de Amazon S3 y muestra la carpeta que contiene todos los resultados de detección. Esta opción solo está disponible tras configurar Macie para almacenar los resultados de detección de datos confidenciales en un bucket de S3.

Monitoreo de trabajos de detección de información confidencial con los Registros de Amazon CloudWatch.

Además de monitorear el estado general de un trabajo de detección de datos confidenciales, puede monitorear y analizar eventos específicos que se producen a medida que avanza un trabajo. Para ello, utilice datos de registro prácticamente en tiempo real que Amazon Macie publica automáticamente en los Registros de Amazon CloudWatch. Los datos de estos registros proporcionan un registro de los cambios en el progreso o el estado de un trabajo, como la fecha y la hora exactas en que un trabajo comenzó a ejecutarse, se detuvo o terminó de ejecutarse.

Los datos de registro también proporcionan detalles sobre cualquier error a nivel de cuenta o de bucket que se produzca durante la ejecución de un trabajo. Por ejemplo, si la configuración de

permisos de un bucket de S3 impide que un trabajo analice los objetos del bucket, Macie registra un evento. El evento indica cuándo se produjo el error e identifica tanto el bucket afectado como la cuenta propietaria del bucket. Los datos de este tipo de eventos pueden ayudarle a identificar, investigar y abordar los errores que impiden que Macie analice los datos que desea.

Con los Registros de Amazon CloudWatch, puede monitorizar, almacenar y obtener acceso a los archivos de registro de varios sistemas, aplicaciones y Servicios de AWS, incluido Macie. También puede consultar y analizar los datos de registro y configurar los Registros CloudWatch para que le notifiquen cuando se produzcan determinados eventos o se alcancen los umbrales. Los Registros de CloudWatch también ofrecen características para archivar datos de registro y exportarlos a Amazon S3. Para obtener más información acerca de los Registros de CloudWatch, consulte la Guía del usuario de los Registros de Amazon CloudWatch.

Temas

Cómo funciona el registro para trabajos de detección de datos confidenciales

Cuando comience a ejecutar trabajos de detección de datos confidenciales, Macie creará y configurará automáticamente los recursos adecuados en los Registros de Amazon CloudWatch para eventos de registro de todos sus trabajos en la Región de AWS actual. A continuación, Macie publica automáticamente los datos de los eventos en esos recursos cuando se ejecutan sus trabajos. La política de permisos del rol vinculado al servicio de Macie para tu cuenta permite a Macie realizar estas tareas en tu nombre. No necesita tomar ninguna medida para crear o configurar recursos en los Registros de CloudWatch ni para datos de eventos de registro de sus trabajos.

En CloudWatch Logs, los registros se organizan en grupos de registro. Cada grupo de registros contiene flujos de registros. Cada flujo de registro contiene eventos de registro. El propósito general de cada uno de estos recursos es el siguiente:

- Un grupo de registro es un conjunto de flujos de registro que comparten la misma configuración de retención, supervisión y control de acceso; por ejemplo, la recopilación de registros para todos sus trabajos de detección de datos confidenciales.

- Un flujo de registro es una secuencia de eventos de registro que comparten el mismo origen, por ejemplo, un trabajo de detección de datos confidenciales individual.
- Un evento de registro es un registro de una actividad registrada por una aplicación o un recurso, por ejemplo, un evento individual que Macie registró y publicó para un trabajo concreto de detección de datos confidenciales.

Macie publica los eventos de todos sus trabajos de detección de datos confidenciales en un grupo de registro y cada trabajo tiene un flujo de registro único en ese grupo de registro. El grupo de registros tiene el prefijo y el nombre siguientes:

```
/aws/macie/classificationjobs
```

Si este grupo de registros ya existe, Macie lo utiliza para almacenar los eventos de registro de sus trabajos. Esto puede resultar útil si su organización utiliza la configuración automática, como AWS CloudFormation, para crear grupos de registro con periodos de retención de registro predefinidos, configuración de cifrado, etiquetas, filtros de métricas, etc. para eventos de trabajo.

Si este grupo de registros no existe, Macie lo crea con la configuración predeterminada que los Registros CloudWatch usan para los nuevos grupos de registros. La configuración incluye un período de retención de registros de Nunca caduca, lo que significa que los Registros CloudWatch almacenan los registros de forma indefinida. Utilice la consola de Amazon CloudWatch Logs o la API de Registros de Amazon CloudWatch para modificar el periodo de retención del grupo de registro. Para obtener más información, consulte Trabajar con grupos de registros y flujos de registros en la Guía del usuario de Registros de Amazon CloudWatch.

Dentro de este grupo de registros, Macie crea un flujo de registro único para cada trabajo que ejecute, la primera vez que se ejecute el trabajo. El nombre del flujo de registro es el identificador único del trabajo, por ejemplo `85a55dc0fa6ed0be5939d0408example`, en el siguiente formato.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Cada flujo de registro contiene todos los eventos de registro que Macie registró y publicó para el trabajo correspondiente. En el caso de los trabajos periódicos, eso incluye los eventos de todas las ejecuciones del trabajo. Si elimina el flujo de registro de un trabajo periódico, Macie volverá a crear el flujo la próxima vez que se ejecute el trabajo. Si elimina el flujo de registro de un trabajo único, no podrá restaurarlo.

Tenga en cuenta que el registro está habilitado de forma predeterminada para todos sus trabajos. No puede inhabilitarlo ni impedir de ningún otro modo que Macie publique eventos de trabajo en los Registros CloudWatch. Si no desea almacenar los registros, puede reducir el período de retención del grupo de registros a tan solo un día. Al final del período de retención, los Registros CloudWatch eliminan automáticamente los datos de eventos caducados del grupo de registros.

Revisión de registros para trabajos de detección de datos confidenciales

Puede revisar los registros de sus trabajos de detección de datos confidenciales mediante la consola de Amazon CloudWatch o la API de Registros de Amazon CloudWatch. Tanto la consola como la API ofrecen características diseñadas para ayudarle a revisar y analizar los datos de registro. Puede utilizar estas funciones para trabajar con flujos de registro y eventos para sus trabajos del mismo modo que lo haría con cualquier otro tipo de datos de registro en los Registros CloudWatch.

Por ejemplo, puede buscar y filtrar datos agregados para identificar tipos específicos de eventos que se produjeron en todos sus trabajos durante un intervalo de tiempo específico. O bien, puede realizar una revisión específica de todos los eventos que se produjeron en un trabajo concreto. Los Registros CloudWatch también ofrecen opciones para supervisar los datos de registro, definir filtros de métricas y crear alarmas personalizadas.

> **Tip**
>
> Para acceder a los eventos de registro de un trabajo concreto mediante la consola de Amazon Macie, haga lo siguiente: En la página Trabajos, elija el nombre del trabajo. En la parte superior del panel de detalles, selecciona Mostrar resultados y, a continuación, selecciona Mostrar registros de CloudWatch. Macie abre la consola Amazon CloudWatch y muestra una tabla de eventos de registro del trabajo.

Para revisar los registros de sus trabajos (consola de Amazon CloudWatch)

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que ha solicitado los trabajos para los que desea revisar los registros.
3. En el panel de navegación, elija Logs (Registros) y, luego, Log groups (Grupos de registros).
4. En la página Grupos de registros, elija el grupo de registros /aws/macie/classificationjobs. Los Registros CloudWatch muestran una tabla de flujo de registros de los trabajos que ha ejecutado.

Hay un flujo único para cada trabajo. El nombre de cada flujo se correlaciona con el identificador único de un trabajo.

5. En Flujos de registro, realice una de las acciones siguientes:

   - Para revisar los eventos de registro de un trabajo en particular, elija el flujo de registro del trabajo. Para encontrar el flujo más fácilmente, introduzca el identificador único del trabajo en el cuadro de filtro situado encima de la tabla. Tras elegir el flujo de registro, los Registros CloudWatch muestran una tabla de eventos de registro para el trabajo.
   - Para revisar los eventos de registro de todos sus trabajos, elija Buscar en todos los flujos de registro. Los Registros CloudWatch muestran una tabla de eventos de registro para todos sus trabajos.

6. (Opcional) En el cuadro de filtro situado encima de la tabla, introduzca términos, frases o valores que especifiquen las características de los eventos específicos que desee revisar. Para obtener más información sobre la búsqueda de datos de registro, consulte Búsqueda de datos de registro mediante patrones de filtro en la Guía del usuario de Amazon CloudWatch Logs.
7. Para revisar los detalles de un evento de registro específico, elija la flecha derecha ( ) en la fila del evento. Los Registros CloudWatch muestran los detalles del evento en formato JSON.

A medida que se familiarice con los datos de los eventos de registro, también podrá realizar tareas como crear filtros de métricas que conviertan los datos de registro en métricas numéricas de CloudWatch y crear alarmas personalizadas que le faciliten identificar eventos de registro específicos y responder a ellos. Para obtener más información, consulte la Guía del usuario de Registros de Amazon CloudWatch.

Esquema de eventos de registro para trabajos de detección de datos confidenciales

Cada evento de registro de un trabajo de detección de datos confidenciales es un objeto JSON que se ajusta al esquema de eventos de los Registros de Amazon CloudWatch y contiene un conjunto estándar de campos. Algunos tipos de eventos tienen campos adicionales que proporcionan información que resulta especialmente útil para ese tipo de eventos. Por ejemplo, los eventos relacionados con errores a nivel de cuenta incluyen el identificador de cuenta del Cuenta de AWS afectado. Los eventos de errores de nivel de bucket incluyen el nombre del bucket de S3 afectado. Para obtener una lista detallada de los eventos de trabajo que Macie publica en los Registros CloudWatch, consulte Tipos de eventos de registro para trabajos.

En el siguiente ejemplo se muestra el esquema de eventos de registro para trabajos de detección de datos confidenciales. En este ejemplo, el evento informa que Macie no ha podido analizar ningún objeto de un bucket de S3 porque Amazon S3 ha denegado el acceso al bucket.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

En el ejemplo anterior, Macie intentó enumerar los objetos del bucket mediante la operación ListObjectsV2 de la API de Amazon S3. Cuando Macie envió la solicitud a Amazon S3, Amazon S3 denegó el acceso al bucket.

Los siguientes campos son comunes a todos los eventos de registro de los trabajos de detección de datos confidenciales:

- `adminAccountId`: el identificador único de Cuenta de AWS que creó la tarea.
- `jobId`: el identificador único del trabajo.
- `eventType`: el tipo de evento que se produjo. Para obtener una lista completa de los valores posibles y una descripción de cada uno de ellos, consulte Tipos de eventos de registro para trabajos.
- `occurredAt`: la fecha y hora, en tiempo universal coordinado (UTC) y formato ISO 8601 extendido, cuando se produjo el evento.
- `description`: una descripción breve del evento.
- `jobName`: el nombre personalizado del trabajo.

Según el tipo y la naturaleza del evento, un evento de registro también puede contener los siguientes campos:

- `affectedAccount`: el identificador único del Cuenta de AWS propietario del recurso afectado.
- `affectedResource`: un objeto que proporciona detalles sobre el recurso afectado. En el objeto, el campo `type` especifica un campo que almacena metadatos sobre un recurso. El campo `value` especifica el valor del campo (`type`).
- `operation`: la operación que Macie intentó realizar y provocó el error.
- `runDate`: la fecha y hora, en tiempo universal coordinado (UTC) y formato ISO 8601 extendido, cuando se inició el trabajo o la ejecución de trabajos correspondiente.

Tipos de eventos de registro para trabajos de detección de datos confidenciales

Macie publica los eventos de registro para tres categorías de eventos:

- Eventos de estado del trabajo, que registran los cambios en el estado o el progreso de un trabajo o de una ejecución de un trabajo.
- Eventos de error a nivel de cuenta, que registran los errores que impidieron a Macie analizar los datos de Amazon S3 para un Cuenta de AWS específico.
- Eventos de error a nivel de bucket, que registran los errores que impidieron a Macie analizar los datos de un bucket de S3 específico.

En los temas de esta sección, se enumeran y describen los tipos de eventos que publica Macie para cada categoría.

Temas

Eventos de estado del trabajo

Un evento de estado del trabajo registra un cambio en el estado o el progreso de un trabajo o de una ejecución de un trabajo. En el caso de los trabajos periódicos, Macie registra y publica estos eventos tanto para el trabajo en general como para las ejecuciones individuales. Para obtener más

información sobre cómo determinar el estado de un trabajo, consulte Comprobación del estado de los trabajos de detección de datos confidenciales.

En el siguiente ejemplo, se utilizan datos de muestra para mostrar la estructura y la naturaleza de los campos de un evento de estado del trabajo. En este ejemplo, un evento `SCHEDULED_RUN_COMPLETED` indica que la ejecución programada de un trabajo periódico ha terminado de ejecutarse. La ejecución comenzó el 14 de abril de 2021 a las 17:09:30 UTC, tal y como se indica en el campo `runDate`. La carrera finalizó el 14 de abril de 2021 a las 17:16:30 UTC, según lo indicado por el campo `occurredAt`.

```
{
    "adminAccountId": "123456789012",
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

En la siguiente tabla se enumeran y describen los tipos de eventos de estado de trabajo que Macie registra y publica en los Registros CloudWatch. La columna Tipo de evento indica el nombre de cada evento tal como aparece en el campo `eventType` de un evento. La columna Descripción proporciona una breve descripción del evento tal como aparece en el campo `description` de un evento. La Información adicional proporciona información sobre el tipo de trabajo al que se aplica el evento. La tabla se ordena primero por el orden cronológico general en el que pueden producirse los eventos y, después, en orden alfabético ascendente por tipo de evento.

Tipo de evento	Descripción	Información adicional
JOB_CREATED	Se creó un trabajo.	Se aplica a trabajos puntuales y periódicos.
ONE_TIME_JOB_STARTED	El trabajo empezó a ejecutarse.	Se aplica solo a trabajos únicos.

Tipo de evento	Descripción	Información adicional
SCHEDULED_RUN_STARTED	La ejecución de la tarea programada comenzó a ejecutarse.	Se aplica solo a trabajos periódicos. Para registrar el inicio de un trabajo único, Macie publica un evento ONE_TIME_JOB_STARTED, no este tipo de eventos.
BUCKET_MATCHED_THE_CRITERIA	El bucket afectado coincidía con los criterios del bucket especificados para el trabajo.	Se aplica a trabajos puntuales y periódicos que utilizan criterios de bucket de tiempo de ejecución para determinar qué buckets de S3 analizar. El objeto `affectedResource` especifica el nombre del bucket que coincidió con los criterios y que se incluyó en el análisis del trabajo.
NO_BUCKETS_MATCHED_THE_CRITERIA	El trabajo comenzó a ejecutarse, pero actualmente ningún bucket coincide con los criterios de bucket especificados para el trabajo. El trabajo no analizaba ningún dato.	Se aplica a trabajos puntuales y periódicos que utilizan criterios de bucket de tiempo de ejecución para determinar qué buckets de S3 analizar.
SCHEDULED_RUN_COMPLETED	La ejecución de la tarea programada terminó de ejecutarse.	Se aplica solo a trabajos periódicos. Para registrar la finalización de un trabajo único, Macie publica un evento JOB_COMPLETED, no este tipo de eventos.

Tipo de evento	Descripción	Información adicional
JOB_PAUSED_BY_USER	Un usuario ha pausado el trabajo.	Se aplica a los trabajos puntuales y periódicos que se detuvieron temporalmente (en pausa).
JOB_RESUMED_BY_USER	Un usuario reanudó el trabajo.	Se aplica a los trabajos puntuales y periódicos que se detuvieron temporalmente (en pausa) y se reanudaron posteriormente.
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	Macie ha pausado el trabajo. Completion of the job would exceed a monthly quota for the affected account.	Se aplica a los trabajos puntuales y periódicos que Macie interrumpió temporalmente (en pausa). Macie detiene automáticamente un trabajo cuando el procesamiento adicional realizado por el trabajo o la ejecución de un trabajo supera la cuota mensual de detección de datos confidenciales de una o más cuentas para las que el trabajo analiza datos. Para evitar este problema, considere la posibilidad de aumentar la cuota de las cuentas afectadas.

Tipo de evento	Descripción	Información adicional
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	Un usuario reanudó el trabajo. Se suprimió la cuota de servicio mensual para la cuenta afectada.	Se aplica a los trabajos puntuales y periódicos que se detuvieron temporalmente (en pausa). Si Macie detuvo automáticamente un trabajo único, lo reanudará automáticamente cuando comience el mes siguiente o aumentará la cuota mensual de descubrimiento de datos confidenciales para todas las cuentas afectadas, lo que ocurra primero. Si Macie detuvo automáticamente un trabajo periódico, lo reanudará automáticamente cuando esté previsto que comience la siguiente ejecución o comience el mes siguiente, lo que ocurra primero.

Tipo de evento	Descripción	Información adicional
JOB_CANCELLED	El trabajo se ha cancelado.	Se aplica a los trabajos puntuales y periódicos que suspendió permanentemente (canceló) o, en el caso de los trabajos puntuales, que se detuvieron y no se reanudaron en un plazo de 30 días. Si suspende o inhabilita Macie, este tipo de evento también se aplica a los trabajos que estaban activos o en pausa cuando suspendió o inhabilitó Macie. Macie cancela automáticamente sus trabajos en un Región de AWS si suspende o inhabilita Macie en la Región.
JOB_COMPLETED	El trabajo terminó de ejecutarse.	Se aplica solo a trabajos únicos. Para registrar la finalización de un trabajo ejecutado para un trabajo periódico, Macie publica un evento SCHEDULED_RUN_COMPLETED, no este tipo de evento.

Eventos de error a nivel de cuenta

Un evento de error a nivel de cuenta registra un error que impedía a Macie analizar los objetos de los bucket de S3 que son propiedad de un Cuenta de AWS específico. El campo `affectedAccount` de cada evento especifica el ID de cuenta de esa cuenta.

En el siguiente ejemplo, se utilizan datos de ejemplo para mostrar la estructura y la naturaleza de los campos en un evento de error a nivel de cuenta. En este ejemplo, un evento `ACCOUNT_ACCESS_DENIED` indica que Macie no ha podido analizar los objetos de ningún bucket de S3 que sea propiedad de la cuenta `444455556666`.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn't have permission to access S3 bucket data for the
 affected account.",
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

En la siguiente tabla se enumeran y describen los tipos de eventos de error a nivel de cuenta que Macie registra y publica en los Registros CloudWatch. La columna Tipo de evento indica el nombre de cada evento tal como aparece en el campo `eventType` de un evento. La columna Descripción proporciona una breve descripción del evento tal como aparece en el campo `description` de un evento. La columna de Información adicional proporciona todos los consejos aplicables para investigar o solucionar el error que se ha producido. La tabla está ordenada alfabéticamente en orden ascendente por tipo de evento.

Tipo de evento	Descripción	Información adicional
ACCOUNT_ACCESS_DENIED	Macie no tiene permiso para acceder a los datos del bucket de S3 de la cuenta afectada.	Esto suele ocurrir porque los buckets que son propiedad de la cuenta tienen políticas de buckets restrictivas. Para obtener información acerca de cómo resolver este problema, consulte Permitir a Macie el acceso a buckets y objetos de S3.

Tipo de evento	Descripción	Información adicional
		El valor del campo `operation` del evento puede ayudarle a determinar qué configuración de permisos impidió que Macie accediera a los datos de S3 de la cuenta. Este campo indica la operación de Amazon S3 que Macie intentó realizar cuando se produjo el error.
ACCOUNT_DISABLED	El trabajo omitió los recursos que son propiedad de la cuenta afectada. Se ha desactivado Macie para la cuenta.	Para solucionar este problema, vuelva a habilitar Macie para la cuenta en el mismo Región de AWS.
ACCOUNT_DISASSOCIATED	El trabajo omitió los recursos que son propiedad de la cuenta afectada. La cuenta ya no está asociada a su cuenta de administrador de Macie como cuenta de miembro.	Esto ocurre si, como administrador de Macie para una organización, configura un trabajo para analizar los datos de una cuenta de miembro asociada y, posteriormente, la cuenta de miembro se elimina de su organización. Para solucionar este problema, vuelva a asociar la cuenta afectada a su cuenta de administrador de Macie como cuenta de miembro. Para obtener más información, consulte Administración de varias cuentas .

Tipo de evento	Descripción	Información adicional
ACCOUNT_ISOLATED	El trabajo omitió los recursos que son propiedad de la cuenta afectada. Cuenta de AWS estaba aislado.	–
ACCOUNT_REGION_DISABLED	El trabajo omitió los recursos que son propiedad de la cuenta afectada. El Cuenta de AWS no está activo en la Región de AWS actual.	–
ACCOUNT_SUSPENDED	Se canceló el trabajo o se omitieron los recursos que son propiedad de la cuenta afectada. Macie fue suspendido para la cuenta.	Si la cuenta especificada es su propia cuenta, Macie canceló automáticamente el trabajo cuando suspendió Macie en la misma Región. Para solucionar el problema, vuelva a activar Macie en la Región. Si la cuenta especificada es una cuenta de miembro, vuelva a habilitar Macie para esa cuenta en la misma Región.
ACCOUNT_TERMINATED	El trabajo omitió los recursos que son propiedad de la cuenta afectada. Cuenta de AWS se canceló.	–

Eventos de error a nivel de bucket

Un evento de error a nivel de bucket registra un error que impedía a Macie analizar los objetos de un bucket de S3 específico. El `affectedAccount` campo de cada evento especifica el ID de la cuenta para el Cuenta de AWS propietario del bucket. El objeto `affectedResource` de cada evento especifica el nombre del bucket.

En el siguiente ejemplo, se utilizan datos de ejemplo para mostrar la estructura y la naturaleza de los campos en un evento de error a nivel de bucket. En este ejemplo, un evento `BUCKET_ACCESS_DENIED` indica que Macie no pudo analizar ningún objeto del bucket de S3 denominado. `DOC-EXAMPLE-BUCKET` Cuando Macie intentó enumerar los objetos del bucket mediante la operación ListObjectsV2 de la API de Amazon S3, Amazon S3 denegó el acceso al bucket.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

En la siguiente tabla se enumeran y describen los tipos de eventos de error a nivel de bucket que Macie registra y publica en CloudWatch Logs. La columna Tipo de evento indica el nombre de cada evento tal como aparece en el campo `eventType` de un evento. La columna Descripción proporciona una breve descripción del evento tal como aparece en el campo `description` de un evento. La columna de Información adicional proporciona todos los consejos aplicables para investigar o solucionar el error que se ha producido. La tabla está ordenada alfabéticamente en orden ascendente por tipo de evento.

Tipo de evento	Descripción	Información adicional

Tipo de evento	Descripción	Información adicional
BUCKET_ACCESS_DENIED	Macie no tiene permiso para acceder al bucket de S3 afectado.	Esto suele ocurrir porque un bucket tiene una política de bucket restrictiva. Para obtener información acerca de cómo resolver este problema, consulte Permitir a Macie el acceso a buckets y objetos de S3. El valor del campo `operation` del evento puede ayudarle a determinar qué configuración de permisos impidió que Macie accediera al bucket Este campo indica la operación de Amazon S3 que Macie intentó realizar cuando se produjo el error.

Tipo de evento	Descripción	Información adicional
BUCKET_DETAILS_UNAVAILABLE	Un problema temporal impidió que Macie recuperara detalles sobre el bucket y los objetos del bucket.	Esto ocurre si un problema transitorio impide que Macie recupere los metadatos del bucket y del objeto que necesita para analizar los objetos de un bucket. Por ejemplo, se produjo una excepción de Amazon S3 cuando Macie intentó comprobar que tenía permiso para acceder al bucket. Para solucionar el problema de un trabajo único, considere la posibilidad de crear y ejecutar un nuevo trabajo único para analizar los objetos del bucket. En el caso de un trabajo programado, Macie intentará recuperar los metadatos de nuevo durante la siguiente ejecución del trabajo.
BUCKET_DOES_NOT_EXIST	El bucket de S3 afectado ya no existe.	Esto suele ocurrir porque se ha eliminado un bucket.
BUCKET_IN_DIFFERENT_REGION	El bucket de S3 afectado se trasladó a otro Región de AWS.	–

Tipo de evento	Descripción	Información adicional
BUCKET_OWNER_CHANGED	El propietario del bucket de S3 afectado ha cambiado. Macie ya no tiene permiso para acceder al bucket.	Esto suele ocurrir si la propiedad de un bucket se transfiere a un Cuenta de AWS que no forma parte de su organización. El campo `affectedAccount` del evento indica el ID de cuenta de la cuenta que anteriormente era propietaria del bucket.

Administración de trabajos de detección de datos confidenciales

Para ayudarle a administrar sus trabajos de detección de datos confidenciales, Amazon Macie proporciona un inventario completo de sus trabajos en cada Región de AWS. Con este inventario, puede administrar sus trabajos como una única colección y acceder a los ajustes de configuración, el estado y las estadísticas de procesamiento de trabajos individuales. También puede acceder a los hallazgos de datos confidenciales y otros resultados que produjo cada trabajo.

Además de estas tareas, puede crear variaciones personalizadas de trabajos individuales: copie un trabajo existente, ajuste la configuración de la copia y, a continuación, guarde la copia como un nuevo trabajo. Esto puede ser útil en los casos en los que desee analizar diferentes conjuntos de datos de la misma manera, o el mismo conjunto de datos de diferentes maneras. En caso de que desee ajustar los ajustes de configuración de un trabajo existente, cancele el trabajo existente, cópielo y, a continuación, ajuste y guarde la copia como un nuevo trabajo.

Temas

- Evaluación del inventario de trabajos de detección de datos confidenciales
- Revisión de los ajustes de configuración de los trabajos de detección de datos confidenciales
- Comprobación del estado de los trabajos de detección de datos confidenciales
- Pausar, reanudar o cancelar los trabajos de detección de datos confidenciales
- Copiar trabajos de detección de datos confidenciales

Evaluación del inventario de trabajos de detección de datos confidenciales

La página Trabajos de la consola de Amazon Macie proporciona información sobre todos los trabajos de detección de datos confidenciales de su cuenta en el Región de AWS actual. Para cada trabajo, la tabla muestra información resumida que incluye: el estado actual del trabajo; si el trabajo se ejecuta de forma programada o periódica y si el trabajo analiza un número específico de buckets de S3 o analiza los buckets de S3 que coinciden con los criterios de tiempo de ejecución. Si selecciona un trabajo en la tabla, el panel de detalles muestra los ajustes de configuración y otra información sobre el trabajo.

Para revisar el inventario de trabajos

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Trabajos. Se abre la página Trabajos y muestra el número de trabajos de su inventario y una tabla de dichos trabajos.
3. Para encontrar un trabajo específico con mayor rapidez, realice alguna de las siguientes acciones:

   - Para ordenar la tabla por un campo específico, haga clic en el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a hacer clic en el encabezado de la columna.
   - Para mostrar solo los trabajos que tienen un valor específico para un campo, coloque el cursor en el cuadro de filtro. En el menú que aparece, seleccione el campo que desea utilizar para el filtro e introduzca el valor del filtro. A continuación, elija Aplicar.
   - Para ocultar los trabajos que tienen un valor específico para un campo, coloque el cursor en el cuadro de filtro. En el menú que aparece, seleccione el campo que desea utilizar para el filtro e introduzca el valor del filtro. A continuación, elija Aplicar. En el cuadro de filtro, seleccione el icono de igual () para el filtro. Esto cambia el operador del filtro de igual a no igual ().
   - Para eliminar un filtro, seleccione el icono de eliminar filtro () del filtro que desee eliminar.
4. Para revisar los ajustes de configuración y otros detalles de un trabajo concreto, seleccione el nombre del trabajo en la tabla y, a continuación, consulte el panel de detalles.

Revisión de los ajustes de configuración de los trabajos de detección de datos confidenciales

En la consola de Amazon Macie, puede utilizar el panel de detalles de la página Trabajos para revisar los ajustes de configuración y otra información sobre trabajos individuales de detección de datos confidenciales. Por ejemplo, puede revisar una lista de los buckets de S3 que un trabajo está configurado para analizar y qué identificadores de datos administrados utiliza un trabajo para analizar objetos en esos buckets.

> **Note**
>
> No puede cambiar ningún ajuste de configuración de un trabajo existente. Esto ayuda a garantizar que tiene un historial inmutable de resultados de datos confidenciales y resultados de detección para las auditorías o investigaciones de privacidad y protección de datos que lleve a cabo. Si desea cambiar un trabajo existente, cancele el trabajo. A continuación, copie el trabajo, configure la copia para que utilice los ajustes que desee y guarde la copia como un nuevo trabajo.
>
> Si hace esto, también debe tomar medidas para asegurarse de que el nuevo trabajo no vuelva a analizar los datos existentes de la misma manera. Para ello, anote la fecha y la hora en que canceló el trabajo existente. A continuación, configure el ámbito del nuevo trabajo para que solo incluya los objetos que se creen o modifiquen después de cancelar el trabajo original. Por ejemplo, utilice los criterios de objeto para añadir una condición de exclusión Última modificación que especifique la fecha y hora en que se canceló el trabajo original.

Para revisar los ajustes de configuración de un trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Trabajos.
3. En la página Trabajos, seleccione el nombre del trabajo cuya configuración desea revisar.
   El panel de detalles muestra los ajustes de configuración y otra información sobre el trabajo. Dependiendo de la configuración del trabajo, el panel contiene las siguientes secciones.

   Información general

   En esta sección se proporciona información general sobre el trabajo, por ejemplo, el nombre de recurso de Amazon (ARN) del trabajo, cuándo comenzó a ejecutarse el trabajo

más recientemente y el estado actual del trabajo. Si ha puesto en pausa el trabajo, en esta sección también se indica cuándo se pausó el trabajo y cuándo el trabajo o la última ejecución del trabajo expiró o expirará si no lo reanuda.

Estadísticas

En esta sección se muestran las estadísticas de procesamiento del trabajo, como el número de veces que se ha ejecutado el trabajo y el número aproximado de objetos que el trabajo aún no ha procesado durante su ejecución actual.

Ámbito

En esta sección se indica la frecuencia con la que se ejecuta el trabajo. También muestra los ajustes que precisan el alcance del trabajo, por ejemplo, la profundidad de muestreo y cualquier criterio de objeto que incluya o excluya objetos de S3 del análisis del trabajo.

Buckets de S3

Esta sección aparece en el panel si el trabajo está configurado para analizar los buckets que seleccionó explícitamente al crear el trabajo. Indica el número de Cuentas de AWS para los que el trabajo está configurado para analizar datos. También indica el número de buckets que el trabajo está configurado para analizar y los nombres de esos buckets (agrupados por cuenta).

Para mostrar la lista completa de cuentas y buckets en formato JSON, seleccione el número en el campo Total de buckets.

Criterios de buckets de S3

Esta sección aparece en el panel si el trabajo utiliza criterios de tiempo de ejecución para determinar qué buckets analizar. Enumera los criterios que el trabajo está configurado para utilizar.

Para mostrar los criterios en formato JSON, seleccione Detalles y, a continuación, seleccione la pestaña Criterios en la ventana que aparece.

Para revisar una tabla de buckets que coincidan actualmente con los criterios, seleccione Detalles y, a continuación, seleccione la pestaña Buckets coincidentes en la ventana que aparece. Si lo desea, seleccione Actualizar () para recuperar los datos más recientes.

> **Tip**
>
> Si el trabajo ya se ha ejecutado, también puede determinar si alguno de los buckets coincidía con los criterios cuando se ejecutó el trabajo y, en caso afirmativo, los nombres de dichos buckets. Para ello, revise los eventos de registro del trabajo: seleccione Mostrar resultados en la parte superior del panel y, a continuación, seleccione Mostrar registros de CloudWatch. Macie abre la consola Amazon CloudWatch y muestra una tabla de eventos de registro del trabajo. Los eventos incluyen un `BUCKET_MATCHED_THE_CRITERIA` evento para cada bucket que coincida con los criterios y se haya incluido en el análisis del trabajo. Para obtener más información, consulte Monitoreo de trabajos.

Identificadores de datos personalizados

Esta sección aparece en el panel si el trabajo está configurado para utilizar uno o varios identificadores de datos personalizados. Especifica los nombres de esos identificadores de datos personalizados.

Listas de permitidos

Esta sección aparece en el panel si el trabajo está configurado para utilizar una o varias listas de permitidos. Especifica los nombres de esas listas. Para revisar la configuración y el estado de una lista, seleccione el icono de enlace ( ) junto al nombre de la lista.

Identificadores de datos administrados

En esta sección se indican los identificadores de datos administrados que el trabajo está configurado para utilizar. Esto viene determinado por el tipo de selección de identificadores de datos administrados para el trabajo:

- Recomendado: utilice los identificadores de datos administrados que se encuentran en el conjunto recomendado cuando se ejecute el trabajo.
- Incluir seleccionados: utilice solo los identificadores de datos administrados que aparecen en la sección Selecciones.
- Incluir todo: utilice todos los identificadores de datos administrados que estén disponibles cuando se ejecute el trabajo.

- Excluir seleccionados: utilice todos los identificadores de datos administrados que estén disponibles cuando se ejecute el trabajo, excepto los que aparezcan en la sección Selecciones.
- Excluir todo: no utilice ningún identificador de datos administrados. Utilice solo los identificadores de datos personalizados especificados.

Para revisar estos ajustes en formato JSON, seleccione Detalles.

Etiquetas

Esta sección aparece en el panel si hay etiquetas asociadas al trabajo. Enumera dichas etiquetas.

Una Etiqueta es una etiqueta que se define y se asigna a determinados tipos de recursos de AWS. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

4. Para revisar y guardar la configuración del trabajo en formato JSON, seleccione el identificador único del trabajo (ID del trabajo) en la parte superior del panel y, a continuación, seleccione Descargar.

Comprobación del estado de los trabajos de detección de datos confidenciales

Cuando se crea un trabajo de detección de datos confidenciales, su estado inicial es Activo (en ejecución) o Activo (en reposo), en función del tipo de trabajo y de la programación. A continuación, la tarea pasa por otros estados, que puede supervisar a medida que avanza.

> **Tip**
>
> Además de monitorear el estado general de un trabajo, puede monitorear eventos específicos que se producen a medida que avanza un trabajo. Para ello, utilice datos de registro que Macie publica automáticamente en los Registros de Amazon CloudWatch. Los datos de proporcionan un registro de cambios del estado de un trabajo y detalles sobre cualquier error a nivel de cuenta o de bucket que se haya producido durante la ejecución del trabajo. Para obtener más información, consulte Monitoreo de trabajos.

Para comprobar el estado de un trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Jobs (Trabajos).
3. En la página Trabajos, localice el trabajo cuyo estado desee comprobar. El campo Estado indica el estado actual del trabajo.

   Activo (en reposo)

   En el caso de un trabajo periódico, la ejecución anterior se ha completado y la siguiente ejecución programada está pendiente. Este valor no se aplica a los trabajos que se realizan una sola vez.

   Activo (en ejecución)

   Si es un trabajo único, está en curso. En el caso de un trabajo periódico, hay una ejecución programada en curso.

   Cancelado

   Cualquier tipo de trabajo, que se ha detenido permanentemente (cancelado).

   Un trabajo tiene este estado si lo ha cancelado de forma explícita o, si es un trabajo único, lo pausó y no lo ha reanudado en un plazo de 30 días. Un trabajo también puede tener este estado si anteriormente suspendió Macie en la Región de AWS actual.

   Completado

   En el caso de un trabajo único, se ejecutó correctamente y ahora está completo. Este valor no se aplica a los trabajos periódicos. En cambio, el estado de un trabajo periódico cambia a Activo (en reposo) cuando cada ejecución se completa correctamente.

   En pausa (por Macie)

   Cualquier tipo de trabajo que Macie ha detenido temporalmente (lo puso en pausa).

   Un trabajo tiene este estado si al completarlo o ejecutarlo se supera la cuota de detección de datos confidenciales mensual de su cuenta. Cuando esto ocurre, Macie detiene automáticamente el trabajo. Macie lo reanuda automáticamente cuando comience el siguiente mes natural (y se restablezca la cuota mensual de su cuenta) o usted aumente la cuota de su cuenta.

Si usted administra Macie en una organización y ha configurado la tarea para analizar los datos de las cuentas de los miembros, la tarea también puede tener este estado si la finalización o ejecución de una tarea supera la cuota mensual de detección de datos confidenciales de la cuenta de un miembro.

Si se está ejecutando un trabajo y el análisis de los objetos aptos alcanza esta cuota para una cuenta de miembro, el trabajo deja de analizar los objetos que son propiedad de la cuenta. Cuando el trabajo termina de analizar los objetos de todas las demás cuentas que no han alcanzado la cuota, Macie detiene automáticamente el trabajo. Si se trata de un trabajo único, Macie reanudará automáticamente el trabajo cuando comience el siguiente mes natural o se aumente la cuota para todas las cuentas afectadas, lo que ocurra primero. Si se trata de un trabajo periódico, Macie lo reanudará automáticamente cuando esté previsto que comience la siguiente ejecución o cuando comience el siguiente mes natural, lo que ocurra primero. Si una ejecución programada comienza antes de que comience el siguiente mes natural o si se aumenta la cuota para una cuenta afectada, el trabajo no analiza los objetos que son propiedad de la cuenta.

En pausa (por usuario)

Cualquier tipo de trabajo que ha detenido temporalmente (lo puso en pausa).

Si pausa un trabajo único y no lo reanuda en 30 días, el trabajo vence y Macie lo cancela. Si pausa un trabajo periódico mientras está en ejecución activa y no lo reanuda en 30 días, la ejecución de la tarea caducará y Macie la cancelará. Para comprobar la fecha de caducidad de un trabajo o ejecución de un trabajo pausado, elija el nombre del trabajo en la tabla y, a continuación, consulte el campo Vencimiento en la sección del panel Detalles de estado.

Si un trabajo está cancelado o en pausa, puede consultar los detalles del trabajo para determinar si el trabajo comenzó a ejecutarse o, en el caso de un trabajo periódico, se ejecutó al menos una vez antes de cancelarse o pausarse. Para ello, elija el nombre del trabajo en la tabla y, a continuación, consulte el panel de detalles. En el panel, el campo Número de ejecuciones indica el número de veces que se ha ejecutado el trabajo. El campo Última hora de ejecución indica la fecha y hora más recientes en las que el trabajo comenzó a ejecutarse.

Según el estado actual del trabajo, si lo desea, puede pausarlo, reanudarlo o cancelarlo.

Pausar, reanudar o cancelar los trabajos de detección de datos confidenciales

Después de crear un trabajo de detección de datos confidenciales, puede pausarlo temporalmente o cancelarlo permanentemente. Cuando pausa un trabajo que se está ejecutando activamente, Macie comienza inmediatamente a pausar todas las tareas de procesamiento del trabajo. Cuando cancela un trabajo que se está ejecutando activamente, Macie comienza inmediatamente a detener todas las tareas de procesamiento del trabajo. No puede reanudar ni reiniciar un trabajo después de cancelarse.

Si pausa un trabajo único, puede reanudarlo en un plazo de 30 días. Cuando reanuda el trabajo, Macie reanuda inmediatamente el procesamiento desde el punto en el que lo pausó; no lo reinicia desde el principio. Si no reanuda un trabajo único después de 30 días de ponerlo en pausa, el trabajo vence y Macie lo cancela.

Si pausa un trabajo periódico, puede reanudarlo en cualquier momento. Si reanuda un trabajo periódico y estaba en reposo cuando lo puso en pausa, Macie lo reanudará según la programación y los otros ajustes de configuración que eligió al crear el trabajo. Si reanuda un trabajo periódico y se estaba ejecutando activamente, la forma en que Macie reanude el trabajo depende del momento:

- Si reanuda el trabajo antes de que pasen 30 días de ponerlo en pausa, Macie reanuda inmediatamente la última ejecución programada desde el punto en el que lo pausó; no la reinicia desde el principio.
- Si no reanuda el trabajo en un plazo de 30 días a partir de la pausa, la última ejecución programada caducará y Macie cancelará todas las tareas de procesamiento restantes de la ejecución. Cuando posteriormente reanuda el trabajo, Macie lo reanudará según la programación y los otros ajustes de configuración que eligió al crear el trabajo.

Para ayudarle a determinar cuándo caducará un trabajo en pausa o en ejecución, Macie añade una fecha de caducidad a los detalles del trabajo mientras está en pausa. Para comprobar esta fecha, elija el nombre del trabajo en la página Trabajos y, a continuación, consulte el campo Vencimiento en la sección del panel Detalles de estado. Además, le notificamos aproximadamente siete días antes de que caduque el trabajo o la ejecución. Le notificaremos de nuevo cuando el trabajo o la ejecución caduque y se cancele. Para notificarlo, le enviamos un correo electrónico a la dirección asociada con su Cuenta de AWS. También creamos eventos AWS Health y eventos de Amazon CloudWatch para su cuenta.

Para pausar, reanudar o cancelar un trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Jobs (Trabajos).
3. En la página Trabajos, active la casilla de verificación del trabajo que desee pausar, reanudar o cancelar y, a continuación, realice una de las siguientes acciones en el menú Acciones:
   - Para pausar el trabajo temporalmente, seleccione Pausar. Esta opción solo está disponible si el estado actual del trabajo es Activo (en reposo), Activo (en ejecución) o En pausa (por Macie).
   - Para reanudar el trabajo, seleccione Reanudar. Esta opción solo está disponible si el estado actual del trabajo es En pausa (por usuario).
   - Para cancelar el trabajo permanentemente, elija Cancelar. Si elige esta opción, no podrá reanudar ni reiniciar el trabajo posteriormente.

Copiar trabajos de detección de datos confidenciales

Para crear rápidamente un nuevo trabajo de detección de datos confidenciales similar a uno existente, puede crear una copia del trabajo, editar la configuración de la copia y, a continuación, guardar la copia como un trabajo nuevo. Esto puede resultar útil en los casos en los que desee crear una variante personalizada de un trabajo existente. En caso de que desee cambiar los ajustes de configuración de un trabajo existente, puede cancelarlo y después copiar, cambiar y guardar los ajustes como un nuevo trabajo.

Para copiar un trabajo

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Jobs (Trabajos).
3. Active la casilla de verificación del trabajo que desea copiar.
4. En el menú Acciones, elija Copiar en uno nuevo.
5. Siga los pasos de la consola para revisar y ajustar la configuración de la copia del trabajo. Para el paso Ajustar el ámbito, considere la posibilidad de elegir opciones que impidan que el trabajo vuelva a analizar los datos existentes de la misma manera:
   - Para un trabajo único, utilice criterios de objeto para incluir solo los objetos que se hayan creado o modificado después de un tiempo determinado. Por ejemplo, si va a crear la copia de

un trabajo que ha cancelado, añada una condición de última modificación que especifique la fecha y la hora en que canceló el trabajo existente.

- Para un trabajo periódico, desactive la casilla de verificación Incluir objetos existentes. Si hace esto, la primera ejecución del trabajo analiza solo los objetos que se crean o se modifican después de la creación del trabajo y antes de su primera ejecución. También puede utilizar criterios de objeto para excluir los objetos que se modificaron por última vez antes de una fecha y hora determinadas.

Para obtener más información sobre este y otros pasos, consulte Creación de un trabajo de detección de datos confidenciales.

6. Cuando termine, seleccione Enviar para guardar la copia como un trabajo nuevo.

Previsión y supervisión de los costos de los trabajos de detección de datos confidenciales

Los precios de Amazon Macie se basan en parte en la cantidad de datos que se analizan al ejecutar tareas de detección de datos confidenciales. Para pronosticar y monitorear los costos estimados de ejecutar trabajos de detección de datos confidenciales, puede revisar las estimaciones de costos que Macie proporciona al crear un trabajo y después de comenzar a ejecutarlo.

Para revisar y supervisar sus costos reales, puede utilizarAWS Billing and Cost Management. AWS Billing and Cost Management proporciona características diseñadas para ayudarlo a realizar un seguimiento y analizar los costos de su cuenta u organización y a administrar los presupuestos de su cuenta u organización. Servicios de AWS También proporciona características que pueden ayudarlo a pronosticar los costos de uso en función de los datos históricos. Para obtener más información, consulte la AWS Billing Guía del usuario.

Para obtener información detallada acerca de los precios de Macie, consulte Precios de Amazon Macie.

Temas

- Previsión del costo de un trabajo de detección de información confidencial
- Monitoreo de los costos estimados de los trabajos de detección de datos confidenciales

Previsión del costo de un trabajo de detección de información confidencial

Al crear un trabajo de detección de datos confidenciales, Amazon Macie puede calcular y mostrar los costos estimados durante dos pasos clave del proceso de creación del trabajo: al revisar la tabla de buckets de S3 que ha seleccionado para el trabajo (paso 2) y al revisar todos los ajustes del trabajo (paso 8). Estos cálculos pueden ayudarle a determinar si debe ajustar la configuración del trabajo antes de guardarlo. La disponibilidad y la naturaleza de los cálculos dependen de la configuración que elija para el trabajo.

Revisar los costos estimados de los buckets individuales (paso 2)

Si selecciona explícitamente bucket individuales para analizar un trabajo, puede revisar el costo estimado del análisis de los objetos de cada uno de esos buckets. Macie muestra estos cálculos durante el paso 2 del proceso de creación de empleo, cuando revisas sus selecciones de buckets. En la tabla de este paso, el campo Costo estimado indica el costo total estimado (en dólares estadounidenses) de ejecutar el trabajo una vez para analizar los objetos de un bucket.

Cada cálculo refleja la cantidad proyectada de datos sin comprimir que el trabajo analizará en un bucket, en función del tamaño y los tipos de objetos que están almacenados actualmente en el bucket. La estimación también refleja los precios de Macie para el actual Región de AWS.

Solo los objetos clasificables se incluyen en el cálculo de costos de un bucket. Un objeto clasificable es un objeto S3 que utiliza una clase de almacenamiento Amazon S3 compatible y tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible. Si algún objeto clasificable es un archivo comprimido o archivado, el cálculo supone que los archivos utilizan una relación de compresión de 3:1, y que el trabajo puede analizar todos los archivos extraídos.

Revisar el costo total estimado de un trabajo (paso 8)

Si crea un trabajo único o crea y configura un trabajo periódico para incluir los objetos S3 existentes, Macie calcula y muestra el costo total estimado del trabajo durante el último paso del proceso de creación del trabajo. Puede revisar este cálculo mientras revisa y verifica todos los ajustes que seleccionó para el trabajo.

Este cálculo indica el costo total proyectado (en dólares estadounidenses) de ejecutar el trabajo una vez en la región actual. El cálculo refleja la cantidad proyectada de datos sin comprimir que analizará el trabajo. Se basa en el tamaño y los tipos de objetos que se almacenan actualmente en los buckets que usted seleccionó explícitamente para el trabajo o en un máximo de 500

buckets que actualmente coinciden con los criterios de bucket que especificó para el trabajo, en función de la configuración del trabajo.

Tenga en cuenta que este cálculo no refleja ninguna opción que haya seleccionado para refinar y reducir el alcance del trabajo, por ejemplo, una profundidad de muestreo más baja o criterios que excluyan determinados objetos S3 del trabajo. Tampoco refleja su cuota mensual de detección de datos confidenciales, lo que podría limitar el alcance y el costo del análisis del trabajo, ni los descuentos que puedan aplicarse a su cuenta.

Además del costo total estimado del trabajo, el cálculo proporciona datos añadidos que ofrecen información sobre el alcance y el costo proyectados del trabajo:

- Tamaño indican el tamaño total de almacenamiento de los objetos que el trabajo puede y no puede analizar.
- Recuento de objetos indican el nbúmero total de objetos que el trabajo puede y no puede analizar.

En estos valores, un objeto Clasificable es un objeto S3 que utiliza una clase de almacenamiento Amazon S3 compatible y tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento compatible. En el cálculo de costos solo se incluyen los objetos clasificables. Un objeto no clasificable es un objeto que no utiliza una clase de almacenamiento de compatible o no tiene una extensión de nombre de archivo para un archivo o formato de almacenamiento admitido. Estos objetos no están incluidos en el cálculo de costos.

El cálculo proporciona datos añadidos adicionales para los objetos de S3 que son archivos comprimidos o archivados. El valor Comprimido indica el tamaño total de almacenamiento de los objetos que utilizan una clase de almacenamiento de Amazon S3 compatible y tienen una extensión de nombre de archivo para un tipo de archivo comprimido o de archivado admitido. El valor Sin comprimir indica el tamaño aproximado de estos objetos si están descomprimidos, en función de una relación de compresión específica. Estos datos son relevantes debido a la forma en que Macie analiza los archivos comprimidos y archivados.

Cuando Macie analiza un archivo comprimido o archivado, inspecciona tanto el archivo completo como su contenido. Para revisar el contenido del archivo, Macie los descomprime y, a continuación, inspecciona cada archivo extraído que utiliza un formato compatible. Por lo tanto, la cantidad real de datos que analiza un trabajo depende de:

- Si un archivo utiliza compresión y, de ser así, la relación de compresión que utiliza.
- El número, el tamaño y el formato de los archivos extraídos.

Por defecto, Macie asume lo siguiente al calcular los cálculos de costos de un trabajo:

- Todos los archivos comprimidos y archivados utilizan una relación de compresión de 3:1.
- Todos los archivos extraídos utilizan un formato de archivo o almacenamiento compatible.

Estas suposiciones pueden dar como resultado un cálculo de mayor tamaño para el alcance de los datos que se analizarán en el trabajo y, en consecuencia, un cálculo de costos mayor para el trabajo.

Puede volver a calcular el costo total estimado del trabajo en función de una relación de compresión diferente. Para ello, elija la relación en la lista Elegir una relación de compresión estimada de la sección Costo estimado. A continuación, Macie actualiza el cálculo para que coincida con su selección.

Para obtener más información acerca de cómo calcula Macie los costos estimados, consulteEntender cómo se calculan los costos estimados de uso.

Monitoreo de los costos estimados de los trabajos de detección de datos confidenciales

Si ya está realizando tareas de detección de datos confidenciales, la página de Uso de la consola de Amazon Macie puede ayudarle a supervisar el costo estimado de esas tareas. La página muestra los costos estimados (en dólares estadounidenses) de usar Macie en el Región de AWS actual durante el mes natural en curso. Para obtener información sobre cómo Macie realiza estos cálculos, consulte Entender cómo se calculan los costos estimados de uso.

Para revisar los costos estimados de los trabajos de ejecución

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector de Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea revisar los costos estimados.
3. En el panel de navegación, seleccione Uso.
4. En la página Uso, consulte el desglose de los costos estimados de su cuenta. El elemento Trabajos de detección de datos confidenciales indica el costo total estimado de los trabajos que ha realizado hasta ahora durante el mes en curso en la región actual.

   Si es el administrador de Macie de una organización, la sección Costos estimados muestra los costos estimados para su organización en general durante el mes en curso en la región actual. Para mostrar el costo total estimado de los trabajos que se ejecutaron para una cuenta

específica, elija la cuenta de la tabla. A continuación, la sección de Costos estimados muestra un desglose de los costos estimados de la cuenta, incluido el costo estimado de los trabajos que se ejecutaron. Para mostrar estos datos para otra cuenta, seleccione la cuenta en la tabla. Para borrar la selección de su cuenta, elija X junto al ID de la cuenta.

Para revisar y monitorear sus costos reales, use AWS Billing and Cost Management.

Identificadores de datos administrados recomendados para trabajos de detección de datos confidenciales

Para optimizar los resultados de sus trabajos de detección de datos confidenciales, puede configurar los trabajos individuales para que utilicen automáticamente el conjunto de identificadores de datos administrados que recomendamos para los trabajos. Un identificador de datos administrados es un conjunto de criterios y técnicas integrados que están diseñados para detectar un tipo específico de datos confidenciales, por ejemplo, números de tarjetas de crédito, claves de acceso secretas AWS o números de pasaporte para un país o región en particular.

El conjunto recomendado de identificadores de datos administrados está diseñado para detectar categorías y tipos comunes de datos confidenciales. Según nuestras investigaciones, puede detectar categorías y tipos generales de datos confidenciales y, al mismo tiempo, optimizar los resultados de su trabajo al reducir el ruido. A medida que publicamos nuevos identificadores de datos administrados, los añadimos a este conjunto si es probable que puedan optimizar aún más los resultados de su trabajo. Con el tiempo, también podríamos añadir o eliminar del conjunto los identificadores de datos administrados existentes. Si añadimos o eliminamos un identificador de datos administrados del conjunto recomendado, actualizamos esta página para indicar la naturaleza y el momento del cambio. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Macie.

Al crear un trabajo de detección de datos confidenciales, debe especificar qué identificadores de datos administrados desea que el trabajo utilice para analizar los objetos de los buckets de Amazon Simple Storage Service (Amazon S3). Para configurar un trabajo para que utilice el conjunto recomendado de identificadores de datos administrados, elija la opción Recomendado al crear el trabajo. A continuación, el trabajo utilizará automáticamente todos los identificadores de datos administrados que estén en el conjunto recomendado cuando el trabajo comience a ejecutarse. Si configura un trabajo para que se ejecute más de una vez, cada ejecución utilizará automáticamente todos los identificadores de datos administrados que estén en el conjunto recomendado cuando comience la ejecución.

En los temas siguientes se enumeran los identificadores de datos administrados que se encuentran actualmente en el conjunto recomendado, organizados por categoría y tipo de datos confidenciales. Especifican el identificador (ID) único de cada identificador de datos administrados del conjunto. Este ID describe el tipo de datos confidenciales que un identificador de datos gestionados está diseñado para detectar, por ejemplo: `PGP_PRIVATE_KEY` para las claves privadas de PGP y `USA_PASSPORT_NUMBER` para los números de pasaportes estadounidenses.

Temas

Para obtener más información sobre identificadores de datos administrados específicos o una lista completa de todos los identificadores de datos administrados que Macie proporciona actualmente, consulte Uso de identificadores de datos administrados.

Credenciales

Para detectar la aparición de datos de credenciales en los objetos de S3, el conjunto recomendado utiliza los siguientes identificadores de datos administrados.

Tipos de datos confidenciales	Identificador de datos administrados
Clave de acceso secreta de AWS	`AWS_CREDENTIALS`
Encabezado de autorización básica de HTTP	`HTTP_BASIC_AUTH_HEADER`
Clave privada de OpenSSH	`OPENSSH_PRIVATE_KEY`
Clave privada de PGP	`PGP_PRIVATE_KEY`
Clave privada del estándar de criptografía de clave pública (PKCS)	`PKCS`
Clave privada PuTTY	`PUTTY_PRIVATE_KEY`

Información financiera

Para detectar la aparición de información financiera en los objetos de S3, el conjunto recomendado utiliza los siguientes identificadores de datos administrados.

Tipos de datos confidenciales	Identificador de datos administrados
Datos de banda magnética de tarjetas de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Número de tarjetas de crédito	`CREDIT_CARD_NUMBER` (para números de tarjetas de crédito próximos a una palabra clave)

Información de identificación personal (PII)

Para detectar la aparición de información de identificación personal (PII) en los objetos de S3, el conjunto recomendado utiliza los siguientes identificadores de datos administrados.

Tipos de datos confidenciales	Identificador de datos administrados
Número de identificación del permiso de conducir	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (para EE. UU.), `UK_DRIVERS_LICENSE`
Número de registro electoral	`UK_ELECTORAL_ROLL_NUMBER`
Número de identificación nacional	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Número de seguro nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Número de pasaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PAS`

Tipos de datos confidenciales	Identificador de datos administrados
	`SPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER`
Número de Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número de la Seguridad Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER`
Número de identificación o referencia del contribuyente	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Actualizaciones del conjunto recomendado

En la siguiente tabla se describen los cambios en el conjunto de identificadores de datos administrados que recomendamos para los trabajos de detección de datos confidenciales. Para obtener alertas automáticas sobre cambios, suscríbase a la fuente RSS en la página de historial de documentos de Macie.

Cambio	Descripción	Fecha
Disponibilidad general	Versión inicial de la serie recomendada.	27 de junio de 2023

Análisis de objetos de Amazon S3 cifrados con Amazon Macie

Cuando habilitas Amazon Macie para ti Cuenta de AWS, Macie crea un rol vinculado a un servicio que otorga a Macie los permisos necesarios para llamar a Amazon Simple Storage Service (Amazon

S3) y a otros en tu nombre. Servicios de AWS Un rol vinculado a un servicio simplifica el proceso de configuración de un, Servicio de AWS ya que no es necesario añadir permisos manualmente para que el servicio complete acciones en su nombre. Para obtener más información sobre este tipo de rol, consulte Uso de roles vinculados en la AWS Identity and Access Management Guía del usuario.

La política de permisos del rol vinculado a un servicio de Macie (`AWSServiceRoleForAmazonMacie`) permite a Macie realizar acciones que incluyen la recuperación de información sobre los buckets y objetos de S3 y la recuperación y el análisis de los objetos de los bucket de S3. Si su cuenta es la cuenta de administrador de Macie de una organización, la política también permite a Macie llevar a cabo estas acciones en su nombre para las cuentas miembro de su organización.

Si cifra un objeto de S3, la política de permisos de la función vinculada al servicio de Macie suele conceder a Macie los permisos que necesita para descifrar la lista. Sin embargo, esto depende del tipo de cifrado utilizado. También puede depender de si Macie puede utilizar la clave de cifrado adecuada.

Temas

- Opciones de cifrado para objetos de Amazon S3
- Permitir que Amazon Macie utilice un sistema gestionado por el cliente AWS KMS key

Opciones de cifrado para objetos de Amazon S3

Amazon S3 admite varias opciones de cifrado para los objetos S3. En la mayoría de estas opciones, Amazon Macie puede descifrar un objeto mediante el rol vinculado al servicio de Macie de su cuenta. Sin embargo, esto depende del tipo de cifrado utilizado para desencriptar un objeto.

Cifrado del servidor con claves administradas por Amazon S3 (SSE-S3)

> Si un objeto se cifra mediante el cifrado del lado del servidor con una clave gestionada por Amazon S3 (SSE-S3), Macie puede descifrar el objeto.
>
> Para obtener información sobre este tipo de cifrado, consulte Uso del cifrado del lado del servidor con claves administradas por Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Cifrado del lado del servidor con (DSSE-KMS y SSE-KMS) AWS KMS keys

Si un objeto se cifra mediante un cifrado de doble capa del lado del servidor o un cifrado del lado del servidor con un cifrado AWS gestionado AWS KMS key (DSSE-KMS o SSE-KMS), Macie puede descifrar el objeto.

Si un objeto se cifra mediante un cifrado de doble capa del lado del servidor o un cifrado del lado del servidor gestionado por el cliente AWS KMS key (DSSE-KMS o SSE-KMS), Macie solo podrá descifrar el objeto si usted permite que Macie utilice la clave. Este es el caso de los objetos que se cifran con claves KMS gestionadas íntegramente desde un almacén de claves externo y claves KMS gestionadas íntegramente. AWS KMS Si a Macie no se le permite usar la clave KMS correspondiente, Macie solo puede almacenar los metadatos del objeto y generar informes al respecto.

Para obtener más información sobre estos tipos de cifrado, consulte Uso del cifrado de doble capa del lado del servidor AWS KMS keys y Uso del cifrado del lado del servidor con en AWS KMS keys la Guía del usuario de Amazon Simple Storage Service.

> **Tip**
>
> Puede generar automáticamente una lista de todos los clientes gestionados a los AWS KMS keys que Macie necesita acceder para analizar los objetos de los depósitos de S3 para su cuenta. Para ello, ejecute el script AWS KMS Permission Analyzer, que está disponible en el repositorio de Amazon Macie Scripts en. GitHub El script también puede generar un script adicional de comandos AWS Command Line Interface (AWS CLI). Si lo desea, puede ejecutar esos comandos para actualizar las políticas y los ajustes de configuración necesarios para las claves de KMS que especifique.

Cifrado en el servidor con claves proporcionadas por el cliente (SSE-C)

Si un objeto se cifra mediante un cifrado del lado del servidor con una clave proporcionada por el cliente (SSE-C), Macie no podrá descifrar el objeto. Macie solo puede almacenar y reportar metadatos para el objeto.

Para obtener más información sobre este tipo de cifrado, consulte Uso del cifrado del lado del servidor con claves en la Guía del usuario de Amazon Simple Storage Service.

Cifrado del cliente

Si un objeto se cifra mediante un cifrado del cliente, Macie puede descifrar el objeto. Macie solo puede almacenar y reportar metadatos para el objeto. Por ejemplo, Macie puede indicar el tamaño del objeto y las etiquetas asociadas al mismo.

Para obtener más información sobre este tipo de cifrado en el contexto de Amazon S3, consulte Protección de datos mediante el cifrado del cliente en la Guía del usuario de Amazon Simple Storage Service.

Puede filtrar su inventario de buckets en Macie para determinar qué buckets de S3 contienen objetos que utilizan determinados tipos de cifrado. También puede determinar qué buckets utilizan determinados tipos de cifrado del lado del servidor de forma predeterminada al almacenar objetos nuevos. La siguiente tabla proporciona ejemplos de filtros que puede aplicar a su inventario de cubos para encontrar esta información.

Para mostrar los buckets que...	Aplicar este filtro...
Almacenan objetos que utilizan el cifrado SSE-C	El recuento de objetos por cifrado es proporcionado por el cliente y desde = 1
Almacene los objetos que utilizan el cifrado DSSE-KMS o SSE-KMS	Se AWS KMS administra el recuento de objetos mediante cifrado y From = 1
Almacenan objetos que utilizan el cifrado SSE-S3	El recuento de objetos por cifrado está gestionado por Amazon S3 y From = 1
Almacenan objetos que utilizan el cifrado del cliente (o no están cifrados)	El recuento de objetos mediante cifrado está Sin encriptar y Desde = 1
Cifre los objetos nuevos de forma predeterminada mediante el cifrado DSSE-KMS	Cifrado predeterminado = aws:kms:dsse
Cifre los objetos nuevos de forma predeterminada mediante el cifrado SSE-KMS	Cifrado predeterminado = aws:kms
Cifre los objetos nuevos de forma predeterminada mediante el cifrado SSE-S3	Cifrado predeterminado = AES256

Si un depósito está configurado para cifrar objetos nuevos de forma predeterminada mediante el cifrado DSSE-KMS o SSE-KMS, también puede determinar cuál se utiliza. AWS KMS key Para ello, elija el bucket en la página de buckets de S3. En el panel de detalles del depósito, en Cifrado del lado del servidor, consulta el campo. AWS KMS key Este campo muestra el nombre de recurso de Amazon (ARN) o identificador único (ID de clave) de la clave.

Permitir que Amazon Macie utilice un sistema gestionado por el cliente AWS KMS key

Si un objeto de Amazon S3 se cifra mediante un cifrado de doble capa del lado del servidor o un cifrado del lado del servidor gestionado por el cliente AWS KMS key (DSSE-KMS o SSE-KMS), Amazon Macie solo podrá descifrar el objeto si se le permite usar la clave. La forma de proporcionar este acceso depende de si la cuenta propietaria de la clave también es propietaria del bucket de S3 que almacena el objeto:

- Si el bucket AWS KMS key y el bucket son propiedad de la misma cuenta, el usuario de la cuenta debe actualizar la política de la clave.
- Si una cuenta es propietaria del depósito AWS KMS key y otra cuenta es propietaria del depósito, el usuario de la cuenta propietaria de la clave debe permitir el acceso a la clave entre cuentas.

En este tema se describe cómo realizar estas tareas y se proporcionan ejemplos para ambos escenarios. Para obtener más información sobre cómo permitir el acceso a la versión gestionada por el cliente AWS KMS keys, consulta Autenticación y control de acceso AWS KMS en la Guía para AWS Key Management Service desarrolladores.

Permitir el acceso de la misma cuenta a una clave administrada por el cliente

Si la misma cuenta es propietaria del bucket S3 AWS KMS key y del bucket, el usuario de la cuenta tiene que añadir un extracto a la política de la clave. La instrucción adicional debe permitir que el rol vinculado a un servicio de Macie de la cuenta utilice la clave para descifrar los datos. Para obtener información sobre cómo modificar una política de claves, consulte Modificación de una política de claves en la AWS Key Management Service Guía del desarrollador.

En la declaración:

- El `Principal` elemento debe especificar el nombre de recurso de Amazon (ARN) de la función vinculada al servicio de Macie para la cuenta propietaria del bucket de S3 y del AWS KMS key bucket.

Si la cuenta es opcional Región de AWS, el ARN también debe incluir el código de región correspondiente a la región. Por ejemplo, si la cuenta se encuentra en la región de Medio Oriente (Baréin) y tiene el código de región me-south-1, el elemento `Principal` debe especificar `arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, en el que *123456789012* es el identificador de la cuenta. Para obtener una lista de todos los códigos de región de las regiones en las que Macie se encuentra disponible actualmente, consulte Puntos de conexión y cuotas de Amazon Macie en la Referencia general de AWS.

- La matriz `Action` debe especificar la acción `kms:Decrypt`. Esta es la única AWS KMS acción que Macie debe poder realizar para descifrar un objeto S3 cifrado con la clave.

A continuación, se muestra un ejemplo de la instrucción que se debe agregar a la política de una AWS KMS key.

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

En el ejemplo anterior:

- El campo `AWS` del elemento `Principal` especifica el ARN del rol vinculado al servicio de Macie (`AWSServiceRoleForAmazonMacie`) de la cuenta. Permite que el rol vinculado al servicio Macie realice la acción especificada en la declaración de política. *123456789012* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario de la clave de KMS y del bucket de S3.
- La matriz `Action` especifica la acción que el rol vinculado a un servicio de Macie puede llevar a cabo con la clave de KMS: descifrar el texto cifrado que se cifró con la clave.

El lugar donde se añada esta declaración a una política de claves depende de la estructura y los elementos que la política contenga actualmente. Cuando añada la instrucción a la política, asegúrese de que la sintaxis sea válida. Las políticas de claves utilizan formato JSON. Esto significa que también hay que añadir una coma antes o después de la declaración, en función de dónde se añada la declaración a la política.

Permitir el acceso entre cuentas a una clave gestionada por el cliente

Si una cuenta es propietaria del depósito AWS KMS key (propietario de la clave) y otra cuenta es propietaria del depósito de S3 (propietario del depósito), el propietario de la clave debe proporcionar al propietario del depósito acceso multicuenta a la clave de KMS. Para ello, el propietario de la clave primero se asegura de que la política de claves permita al propietario del bucket usar la clave y crear una concesión para ella. A continuación, el propietario del bucket crea una concesión para la clave. Una concesión es un instrumento de política que permite a los principales AWS utilizar claves KMS en operaciones criptográficas si se cumplen las condiciones especificadas por la subvención. En este caso, la concesión delega los permisos pertinentes en el rol vinculado a un servicio de Macie de la cuenta del propietario del bucket.

Para obtener información sobre cómo modificar una política de claves, consulte Modificación de una política de claves en la AWS Key Management Service Guía del desarrollador. Para obtener más información sobre las Concesiones en AWS KMS, consulte Subvenciones en la AWS Key Management Service Guía para desarrolladores.

Paso 1: actualización de la política de claves

En la política de claves, el propietario de la clave debe asegurarse de que esta incluya dos instrucciones:

- La primera declaración permite al propietario del bucket utilizar la clave para descifrar los datos.
- La segunda instrucción permite al propietario del bucket crear una concesión para el rol vinculado a un servicio de Macie de la cuenta (del propietario del bucket).

En la primera declaración, el elemento `Principal` debe especificar el ARN de la cuenta del propietario del bucket. La matriz `Action` debe especificar la acción `kms:Decrypt`. Esta es la única AWS KMS acción que Macie debe poder realizar para descifrar un objeto cifrado con la clave. A continuación, se muestra un ejemplo de esta instrucción en la política de una AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to use the key",
```

```
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

En el ejemplo anterior:

- El campo `AWS` del elemento `Principal` especifica el ARN de la cuenta del propietario del bucket (*111122223333*). Permite al propietario del bucket realizar la acción especificada en la declaración de la política. *111122223333* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del bucket.
- La matriz `Action` especifica la acción que el propietario del bucket puede llevar a cabo mediante la clave de KMS: descifrar el texto cifrado con la clave.

La segunda declaración de la política de claves permite al propietario del bucket crear una subvención para el rol vinculado al servicio de Macie para su cuenta. En esta declaración, el elemento `Principal` debe especificar el ARN de la cuenta del propietario del bucket. La matriz `Action` debe especificar la acción `kms:CreateGrant`. Un `Condition` elemento puede filtrar el acceso a la `kms:CreateGrant` acción especificada en la declaración. A continuación, se muestra un ejemplo de esta instrucción en la política de una AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
```

```
        }
    }
}
```

En el ejemplo anterior:

- El campo `AWS` del elemento `Principal` especifica el ARN de la cuenta del propietario del bucket (*111122223333*). Permite al propietario del bucket realizar la acción especificada en la declaración de la política. *111122223333* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del bucket.
- La `Action` matriz especifica la acción que el propietario del bucket puede realizar en la clave de KMS: crear una concesión para la clave.
- El elemento `Condition` utiliza el `StringEquals` operador de condición y la `kms:GranteePrincipal` clave de condición para filtrar el acceso a la acción especificada por la declaración de directiva. En este caso, el propietario del bucket puede crear una concesión solo para la `GranteePrincipal` especificada, que es el ARN del rol vinculado a un servicio de Macie de su cuenta. En ese ARN, *111122223333* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del bucket.

  Si la cuenta del propietario del bucket es opcional Región de AWS, incluye también el código de región correspondiente en el ARN de la función vinculada al servicio de Macie. Por ejemplo, si la cuenta se encuentra en la región de Medio Oriente (Baréin), que tiene el código de región me-south-1, sustituya `macie.amazonaws.com` por `macie.me-south-1.amazonaws.com` en el ARN. Para obtener una lista de todos los códigos de región de las regiones en las que Macie se encuentra disponible actualmente, consulte Puntos de conexión y cuotas de Amazon Macie en la Referencia general de AWS.

Cuando el propietario de la clave añade estas declaraciones a la política de claves, depende de la estructura y los elementos que la directiva contenga actualmente. Cuando el propietario de la clave agregue las instrucciones, debe asegurarse de que la sintaxis sea válida. Las políticas de claves utilizan el formato JSON. Esto significa que el propietario de la clave también debe agregar una coma antes o después de cada instrucción, en función de dónde agregue la instrucción a la política.

Paso 2: creación de una concesión

Una vez que el propietario de la clave actualice la política de claves según sea necesario, el propietario del bucket debe crear una concesión para la clave. La concesión delega los permisos pertinentes al rol vinculado al servicio de Macie para su cuenta (del propietario del bucket). Antes

de que el propietario del bucket cree la concesión, debe comprobar que está autorizado a realizar la acción `kms:CreateGrant` en su cuenta. Esta acción le permite agregar una concesión a una AWS KMS key existente administrada por el cliente.

Para crear la concesión, el propietario del bucket puede utilizar el funcionamiento de la CreateGrantAPI. AWS Key Management Service Cuando el propietario del bucket cree la concesión, debe especificar los siguientes valores para los parámetros necesarios:

- `KeyId`: el ARN de la clave de KMS. Para el acceso entre cuentas a una clave KMS, este valor debe ser un ARN. No puede ser una clave de ID.
- `GranteePrincipal`: el ARN del rol vinculado a un servicio de Macie (`AWSServiceRoleForAmazonMacie`) de su cuenta. Este valor debe ser `arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, donde *`111122223333`* es el ID de la cuenta del propietario del bucket.

  Si la cuenta se encuentra en una región opcional, el ARN debe incluir el código de región apropiado. Por ejemplo, si la cuenta está en la región Medio Oriente (Baréin), que tiene el código de región me-south-1, el ARN debe ser `arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, donde *`111122223333`* es el ID de la cuenta del propietario del bucket.
- `Operations`— La acción AWS KMS de descifrar (`Decrypt`). Esta es la única AWS KMS acción que Macie debe poder realizar para descifrar un objeto que está cifrado con la clave KMS.

Para crear una concesión para una clave KMS gestionada por el cliente mediante AWS Command Line Interface (AWS CLI), ejecuta el comando create-grant. El siguiente ejemplo muestra cómo. El ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

Donde:

- `key-id` especifica el ARN de la clave KMS a la que se va a aplicar la concesión.

- `grantee-principal` especifica el ARN del rol vinculado a un servicio de Macie de la cuenta que puede llevar a cabo la operación especificada en la concesión. Este valor debe coincidir con el ARN especificado en la condición `kms:GranteePrincipal` de la segunda instrucción de la política de claves.
- `operations` especifica la acción que la concesión permite llevar a cabo a la entidad principal especificada: descifrar el texto cifrado que se cifró con la clave de KMS.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Donde `GrantToken` es una cadena única, no secreta, de longitud variable, codificada en base64 que representa la concesión que se creó y `GrantId` es el identificador único de la concesión.

Almacenamiento y retención de los resultados de detección de datos confidenciales con Amazon Macie

Cuando ejecuta un trabajo de detección de datos confidenciales o Amazon Macie realiza una detección automatizado de datos confidenciales, Macie crea un registro de análisis para cada objeto de Amazon Simple Storage Service (Amazon S3) que se incluye en el ámbito del análisis. Estos registros, denominados resultados de la detección de datos confidenciales, registran detalles sobre el análisis que Macie realiza en objetos S3 individuales. Esto incluye objetos en los que Macie no detecta datos confidenciales y, por lo tanto, no produce resultados, y objetos que Macie no puede analizar debido a errores o problemas. Si Macie detecta datos sensibles en un objeto, el registro incluye los datos del hallazgo correspondiente, así como información adicional. Los resultados del detección de datos confidenciales le proporcionan registros de análisis que pueden resultar útiles para auditorías o investigaciones sobre la privacidad y la protección de los datos.

Macie almacena los resultados de la detección de datos confidenciales solo durante 90 días. Para acceder a sus resultados y permitir su almacenamiento y conservación a largo plazo, configure Macie para que cifre los resultados con una clave AWS Key Management Service (AWS KMS) y los almacene en un bucket de S3. El bucket puede servir como un repositorio definitivo y a largo plazo para todos sus resultados de detección de datos confidenciales. A continuación, si lo desea, puede acceder a los resultados de ese repositorio y consultarlos.

Este tema le guía a través del proceso de uso del AWS Management Console para configurar un repositorio para los resultados del descubrimiento de datos confidenciales. La configuración es una combinación de un depósito AWS KMS key que cifra los resultados, un depósito de uso general de S3 que almacena los resultados y los ajustes de Macie que indican qué clave y depósito utilizar. Si prefiere configurar los ajustes de Macie mediante programación, puede utilizar el PutClassificationExportConfigurationfuncionamiento de la API de Amazon Macie.

Al configurar los ajustes en Macie, sus elecciones se aplica únicamente a la Región de AWS actual. Si usted es el administrador de Macie para una organización, sus opciones se aplican solo a su cuenta. No se aplican a ninguna cuenta de miembro asociada.

Si utiliza Macie en varias ocasiones Regiones de AWS, configure los ajustes del repositorio para cada región en la que utilice Macie. De forma opcional, puede almacenar los resultados de la detección de información confidencial de varias regiones en el mismo bucket de S3. Sin embargo, tenga en cuenta los siguientes requisitos:

- Para almacenar los resultados de una región que esté AWS habilitada de forma predeterminada Cuentas de AWS, como la región EE.UU. Este (Virginia del Norte), debe elegir un segmento de una región que esté habilitada de forma predeterminada. Los resultados no se pueden almacenar en un bucket de una región opcional (región que está deshabilitada de forma predeterminada).
- Para almacenar los resultados de una región opcional, como la región Medio Oriente (Baréin), debe elegir un bucket de una región que esté habilitada de forma predeterminada. Los resultados no se pueden almacenar en un bucket de una región opcional diferente.

Para determinar si una región está habilitada de forma predeterminada, consulte Regiones y puntos de conexión en la Guía del usuario de AWS Identity and Access Management . Además de los requisitos anteriores, considere también si desea recuperar muestras de datos confidenciales de los que Macie informa en sus hallazgos individuales. Para recuperar muestras de datos confidenciales de un objeto S3 afectado, todos los siguientes recursos y datos deben almacenarse en la misma región: el objeto afectado, el hallazgo correspondiente y el resultado del descubrimiento de los datos confidenciales correspondientes.

Tareas

- Información general
- Paso 1: Verificar sus permisos
- Paso 2: Configurar en AWS KMS key
- Paso 3: Elegir un bucket de S3

Información general

Amazon Macie crea automáticamente un resultado de detección de datos confidenciales para cada objeto de Amazon S3 que analiza o intenta analizar cuando usted ejecuta un trabajo de detección de datos confidenciales o cuando Macie lleva a cabo una detección automatizada de datos confidenciales para su cuenta u organización. Esto incluye:

- Los objetos en los que Macie detecta datos confidenciales y, por lo tanto, también producen resultados de datos confidenciales.
- Los objetos en los que Macie no detecta datos confidenciales y, por lo tanto, también producen resultados de datos confidenciales.
- Objetos que Macie no puede analizar debido a errores o problemas, como la configuración de los permisos o el uso de un archivo o formato de almacenamiento no compatible.

Si Macie encuentra datos confidenciales en un objeto, el resultado de la detección de datos confidenciales incluirá los datos del resultado correspondiente. También proporciona información adicional, como la ubicación de hasta 1000 apariciones de cada tipo de datos confidenciales que Macie encontró en el objeto. Por ejemplo:

- El número de columna y fila de una celda o campo de un libro de Microsoft Excel, un archivo CSV o un archivo TSV
- La ruta a un campo o matriz en un archivo JSON o líneas JSON
- El número de línea de una línea de un archivo de texto no binario que no sea un archivo CSV, JSON, líneas JSON o TSV, por ejemplo, un archivo HTML, TXT o XML
- El número de página de una página de un archivo en formato de documento portátil (PDF) de Adobe
- El índice de registro y la ruta a un campo de un registro en un contenedor de objetos de Apache Avro o un archivo de Apache Parquet

Si el objeto S3 afectado es un archivo de almacenamiento, como un archivo .tar o .zip, el resultado de la detección de datos confidenciales también proporciona datos de ubicación detallados para la aparición de datos confidenciales en archivos individuales que Macie extrae del archivo. Macie no incluye esta información en los resultados de datos confidenciales para los archivos archivados. Para informar sobre los datos de ubicación, los resultados de la detección de datos confidenciales utilizan un esquema JSON estandarizado.

Un resultado de detección de datos confidenciales no incluye los datos confidenciales que encontró Macie. En su lugar, le proporciona un registro de análisis que puede ser útil para auditorías o investigaciones.

Macie almacena los resultados de la detección de datos confidenciales durante 90 días. No puede acceder a ellos directamente en la consola de Amazon Macie ni con la API de Amazon Macie. En su lugar, siga los pasos de este tema para configurar Macie de forma que cifre los resultados con la AWS KMS key que usted especifique y almacene los resultados en un depósito de uso general de S3 que también especifique. A continuación, Macie escribe los resultados en archivos de líneas JSON (.jsonl), agrega los archivos al bucket como archivos GNU Zip (.gz) y cifra los datos mediante el cifrado SSE-KMS. A partir del 8 de noviembre de 2023, Macie también firma los objetos S3 resultantes con un código de autenticación de mensajes (HMAC) basado en Hash. AWS KMS key

Cuando configure Macie para que almacene los resultados de la detección de datos confidenciales en un bucket de S3, puede usar el bucket como un repositorio definitivo y a largo plazo para los resultados. A continuación, si lo desea, puede acceder a los resultados de ese repositorio y consultarlos.

> **Tip**
>
> Para ver un ejemplo detallado e instructivo de cómo puede consultar y utilizar los resultados del descubrimiento de datos confidenciales para analizar e informar sobre los posibles riesgos de seguridad de los datos, consulte la entrada del blog Cómo consultar y visualizar los resultados del descubrimiento de datos confidenciales de Macie con Amazon Athena y QuickSight Amazon AWS en el blog de seguridad.
>
> Para ver ejemplos de consultas de Amazon Athena que puede utilizar para analizar los resultados del descubrimiento de datos confidenciales, visite el repositorio de Amazon Macie Results Analytics en. GitHub Este repositorio también proporciona instrucciones para configurar Athena para recuperar y descifrar los resultados, y scripts para crear tablas para los resultados.

Paso 1: Verificar sus permisos

Antes de configurar un repositorio para los resultados de la detección de datos confidenciales, compruebe que dispone de los permisos necesarios para cifrar y almacenar los resultados. Para verificar sus permisos, utilice AWS Identity and Access Management (IAM) para revisar las políticas

de IAM asociadas a su identidad de IAM. A continuación, compare la información de esas directivas con la siguiente lista de acciones que debe poder realizar para configurar el repositorio.

Amazon Macie

Para Macie, verifique que se le permite realizar la siguiente acción:

`macie2:PutClassificationExportConfiguration`

Esta acción le permite añadir o cambiar la configuración del repositorio en Macie.

Amazon S3

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

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Estas acciones le permiten acceder a un depósito de uso general de S3 y configurarlo, que puede servir como repositorio.

AWS KMS

Para usar la consola de Amazon Macie para añadir o cambiar la configuración del repositorio, verifique también que se le permita realizar las siguientes acciones AWS KMS :

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

Estas acciones le permiten extraer y mostrar información sobre la AWS KMS keys de su cuenta. A continuación, puede elegir una de estas claves para cifrar los resultados de la detección de datos confidenciales.

Si planea crear uno nuevo AWS KMS key para cifrar los datos, también debe poder realizar las siguientes acciones: `kms:CreateKeykms:GetKeyPolicy`, y`kms:PutKeyPolicy`.

Si no está autorizado a realizar las acciones necesarias, pida ayuda a su AWS administrador antes de continuar con el siguiente paso.

Paso 2: Configurar en AWS KMS key

Tras verificar sus permisos, determine cuáles AWS KMS key desea que Macie utilice para cifrar los resultados de la detección de datos confidenciales. La clave debe ser una clave KMS de cifrado simétrico y administrada por el cliente que esté habilitada en el Región de AWS mismo lugar que el depósito de S3 en el que desea almacenar los resultados.

La clave puede ser una existente AWS KMS key de su propia cuenta o una existente AWS KMS key que sea propiedad de otra cuenta. Si quiere utilizar una clave de KMS nueva, cree la clave antes de continuar. Si desea utilizar una clave ya existente que es propiedad de otra cuenta, obtenga el nombre de recurso de Amazon (ARN) de la clave. Deberá ingresar este ARN cuando configure los ajustes del repositorio en Macie. Para obtener información sobre cómo crear y revisar la configuración de las claves de KMS, consulte Administración de claves en la AWS Key Management Service Guía para desarrolladores.

> **Note**
>
> La clave puede estar AWS KMS key en un almacén de claves externo. Sin embargo, es posible que la clave sea más lenta y menos fiable que una clave que se gestione íntegramente dentro de AWS KMS. Puede reducir este riesgo almacenando los resultados de la detección de información confidencial en un bucket de S3 que esté configurado para utilizar la clave como una bucket de S3. De este modo, se reduce la cantidad de solicitudes de AWS KMS que se deben realizar para cifrar los resultados de la detección de datos confidenciales.
>
> Para obtener información sobre el uso de claves de KMS en almacenes de claves externos, consulte Almacenes de claves externos en la AWS Key Management Service Guía para desarrolladores. Para obtener más información sobre el uso de claves de Bucket de S3, consulte Reducción del costo de SSE-KMS con las claves de bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Después de determinar qué clave de KMS quiere que utilice Macie, dé permiso a Macie para que utilice la clave. De lo contrario, Macie no podrá cifrar ni almacenar los resultados en el repositorio. Para dar permiso a Macie para usar la clave, actualiza la política de claves de la clave. Para obtener información detallada sobre las políticas clave y la administración del acceso a las claves de

KMS, consulte la Política de claves en AWS KMS la AWS Key Management Service Guía para desarrolladores.

Actualización de la política de claves

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. Elija la clave que quiera que Macie utilice para cifrar los resultados de la detección de datos confidenciales.
4. En la pestaña Política de claves, elija Editar.
5. Copie la siguiente declaración en el portapapeles y, a continuación, agréguela a la política:

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
         },
         "ArnLike": {
             "aws:SourceArn": [
                 "arn:aws:macie2:Region:111122223333:export-configuration:*",
                 "arn:aws:macie2:Region:111122223333:classification-job/*"
             ]
         }
    }
}
```

Cuando añada la instrucción a la política, asegúrese de que la sintaxis sea válida. Las políticas utilizan formato JSON. Esto significa que también debe añadir una coma antes o después de la declaración, dependiendo de dónde añada la declaración a la directiva. Si añade la instrucción

como la última instrucción de la política, inserte la coma después del corchete de cierre de la sección anterior. Si lo añade como la primera declaración o entre dos declaraciones existentes, añada una coma después de la llave de cierre para la declaración.

6. Actualice la declaración con los valores correctos para su entorno:

   - En los campos `Condition`, sustituya los valores de los marcadores de posición, donde:
     - *`111122223333`* es el identificador de la cuenta. Cuenta de AWS
     - La *`región`* es Región de AWS en la que utilizas Macie y quieres permitir que Macie utilice la clave.

       Si utilizas Macie en varias regiones y quieres permitir que Macie utilice la clave en otras regiones, añade `aws:SourceArn` condiciones para cada región adicional. Por ejemplo:

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
           "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
           "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
           "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
       ]
       ```

       De forma alternativa, puede permitir a Macie utilizar la clave en todas las regiones. Para ello, sustituya el valor del marcador de posición por el carácter comodín (*). Por ejemplo:

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:*:111122223333:export-configuration:*",
           "arn:aws:macie2:*:111122223333:classification-job/*"
       ]
       ```

   - Si utiliza Macie en una región opcional, agregue el código de región correspondiente al valor del campo `Service`. Por ejemplo, si está usando Macie en la región de Medio Oriente (Baréin), que tiene el código de región me-sur-1, reemplace `macie.amazonaws.com` con `macie.me-south-1.amazonaws.com`. Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie cuotas en la Referencia general de AWS.

   Tenga en cuenta que los campos `Condition` utilizan dos claves de condición globales de IAM:

- aws: SourceAccount — Esta condición permite a Macie realizar las acciones especificadas solo para tu cuenta. Más específicamente, determina qué cuenta puede realizar las acciones especificadas para los recursos y acciones especificados por la condición `aws:SourceArn`.

  Para permitir que Macie realice las acciones especificadas para cuentas adicionales, añada el ID de cuenta para cada cuenta adicional a esta condición. Por ejemplo:

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

- aws: SourceArn — Esta condición impide que otras personas Servicios de AWS realicen las acciones especificadas. También impide que Macie utilice la clave mientras realiza otras acciones en su cuenta. En otras palabras, permite a Macie cifrar objetos de S3 con la clave solo si se trata de resultados de detección de datos confidenciales y únicamente si esos resultados corresponden a una detección de datos confidenciales automatizada o a trabajos de detección de datos confidenciales creados por la cuenta especificada en la región especificada.

  Para permitir que Macie lleve a cabo las acciones especificadas para cuentas adicionales, añada los ARN de cada cuenta adicional a esta condición. Por ejemplo:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
      "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
  ]
  ```

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

  Estas condiciones ayudan a evitar que Macie sea utilizado como un ayudante confuso durante las transacciones con AWS KMS. Aunque no lo recomendamos, puede eliminar estas condiciones de la declaración.

7. Cuando termine de añadir y actualizar la declaración, seleccione Guardar cambios.

Paso 3: Elegir un bucket de S3

Tras comprobar sus permisos y configurarlos AWS KMS key, podrá especificar qué depósito de S3 quiere utilizar como repositorio para los resultados de su descubrimiento de datos confidenciales. Dispone de dos opciones para hacerlo:

- Utilice un nuevo depósito de S3 creado por Macie: si elige esta opción, Macie creará automáticamente un nuevo depósito de S3 de uso general en el actual Región de AWS para los resultados de su descubrimiento. Macie también aplica una política de bucket al bucket. La política permite a Macie añadir objetos al bucket. También requiere que los objetos estén cifrados con la AWS KMS key que especifique, mediante el cifrado SSE-KMS. Para revisar la política, seleccione Ver política en la consola de Amazon Macie después de especificar un nombre para el bucket y la clave de KMS que se va a utilizar.
- Utilice un bucket de S3 existente que haya creado: si prefiere almacenar los resultados de su detección en un bucket de S3 concreto que haya creado, cree el bucket antes de continuar. El depósito debe ser un depósito de uso general. Además, la configuración y la política del depósito deben permitir a Macie añadir objetos al depósito. En este tema se explica qué ajustes se deben comprobar y cómo actualizar la política. También proporciona ejemplos de las declaraciones que se deben añadir a la política.

Las siguientes secciones proporcionan instrucciones para cada opción. Elija la sección para la opción que desee.

Usa un nuevo bucket de S3 creado por Macie

Si prefiere utilizar un nuevo bucket de S3 que Macie cree para usted, el último paso del proceso consiste en configurar los ajustes del repositorio en Macie.

Para configurar los ajustes del repositorio en Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Ajustes, seleccione Resultados de la detección.
3. En Repositorio de resultados de detección de datos confidenciales, seleccione Crear bucket.
4. En el cuadro de diálogo Crear un bucket escriba un nombre para el bucket.

   El nombre debe ser único en todos los buckets de S3. Los nombres de bucket pueden consistir únicamente de letras minúsculas, números, puntos (.) y guiones (-). Para conocer los requisitos

de nomenclatura adicionales, consulte Reglas de nomenclatura de buckets en la Guía del usuario de Amazon Simple Storage Service.

5. Expanda la sección Advanced (Configuración avanzada).
6. (Opcional) Para especificar un prefijo que se utilizará en la ruta a una ubicación del bucket, introdúzcalo en el cuadro de prefijo del resultado de la detección de datos.

   Al introducir un valor, Macie actualiza el ejemplo situado debajo del cuadro para mostrar la ruta a la ubicación del bucket en la que almacenará los resultados de la detección.
7. En Bloquear todo el acceso público, elija Sí para activar todos los ajustes de bloqueo de acceso público del bucket.

   Para obtener información sobre estos ajustes, consulte Bloquear el acceso público a su almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
8. En Configuración del cifrado, especifique la AWS KMS key que Macie tiene que utilizar para cifrar los resultados:

   - Para usar una clave de su propia cuenta, elija Seleccionar una clave de su cuenta. Luego, en la lista AWS KMS key, seleccione la clave que desea usar. La lista muestra las claves KMS de cifrado simétrico administradas por el cliente para su cuenta.
   - Para usar una clave que pertenezca a otra cuenta, seleccione Ingrese el ARN de una clave de otra cuenta. A continuación, en el cuadro AWS KMS key ARN, introduzca el nombre de recurso de Amazon (ARN) de la clave de que se debe utilizar, por ejemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.
9. Cuando termine con la configuración, elija Guardar.

   Macie comprueba la configuración para verificar que es correcta. Si alguna configuración es incorrecta, Macie muestra un mensaje de error que lo ayuda a solucionar el problema.

Tras guardar la configuración del repositorio, Macie añade al mismo los resultados de detección existentes de los 90 días anteriores. Macie también comienza a añadir nuevos resultados de detección al repositorio.

Utilice un bucket de S3 existente que ya haya creado

Si prefiere almacenar los resultados de la detección de datos confidenciales en un bucket de S3 concreto que debe crear, cree y configure el bucket antes de configurar los ajustes del repositorio en Macie. Al crear el bucket, tenga en cuenta los siguientes requisitos:

- La cubeta debe ser de uso general. No puede ser un depósito de directorios.
- Si habilita el bloqueo de objetos para el bucket, debe deshabilitar la configuración de retención predeterminada para esa característica. De lo contrario, Macie no podrá añadir los resultados de la detección al bucket. Para obtener más información, consulte Funcionamiento de Object Lock de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
- Para almacenar los resultados de descubrimiento de una región que está habilitada de forma predeterminada Cuentas de AWS, como la región EE.UU. Este (Virginia del Norte), el depósito debe estar en una región que esté habilitada de forma predeterminada. Los resultados no se pueden almacenar en un bucket de una región opcional (región que está deshabilitada de forma predeterminada).
- Para almacenar los resultados de la detección de una región opcional, como la región Medio Oriente (Baréin), el bucket debe estar en esa misma región o en una región que esté habilitada de forma predeterminada. Los resultados no se pueden almacenar en un bucket de una región opcional diferente.

Para determinar si una región está habilitada de forma predeterminada, consulte Regiones y puntos de conexión en la Guía del usuario de AWS Identity and Access Management .

Tras crear el bucket, actualice la política del bucket para que Macie pueda extraer información sobre el bucket y añadir objetos al bucket. A continuación, puede configurar los ajustes del repositorio en Macie.

Para actualizar la política de bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el bucket en el que desea almacenar sus resultados de detección.
3. Elija la pestaña Permisos.
4. Elija Editar en la sección Política de bucket.
5. Copie el siguiente ejemplo de política en su portapapeles:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. Pegue la política de ejemplo en el editor de políticas de Bucket de la consola de Amazon S3.
7. Actualice la política de ejemplo con los valores correctos para su entorno:

   - En la declaración opcional que niega los encabezados de cifrado incorrectos:
     - *myBucketName*Sustitúyalo por el nombre del depósito.
     - En `StringNotEquals` esta condición, sustituya *arn:AWS:KMS:Region:111122223333:key/KMS KeyId* por el nombre de recurso de Amazon (ARN) del que se utilizará para cifrar los resultados del descubrimiento. AWS KMS key
   - En todas las demás sentencias, sustituya los valores de los marcadores de posición, donde:
     - *myBucketName*es el nombre del depósito.
     - *111122223333* es el identificador de la cuenta. Cuenta de AWS
     - *Región* es aquella Región de AWS en la que utiliza Macie y quiere permitir que Macie añada los resultados de las detecciones al bucket.

       Si utiliza Macie en varias regiones y quiere permitir que Macie añada resultados al bucket de regiones adicionales, añada `aws:SourceArn` condiciones para cada región adicional. Por ejemplo:

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
           "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
           "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
           "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
       ]
       ```

       Como alternativa, puede permitir que Macie añada resultados al bucket para todas las regiones en las que utilice Macie. Para ello, sustituya el valor del marcador de posición por el carácter comodín (*). Por ejemplo:

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:*:111122223333:export-configuration:*",
           "arn:aws:macie2:*:111122223333:classification-job/*"
       ]
       ```
   - Si está utilizando Macie en una región opcional, agregue el código de región correspondiente al valor del campo `Service` en cada instrucción que especifique la entidad principal del servicio de Macie. Por ejemplo, si utiliza Macie en la región de Medio Oriente (Baréin), que

tiene el código de región me-south-1, sustituya `macie.amazonaws.com` por `macie.me-south-1.amazonaws.com` en cada afirmación aplicable. Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie cuotas en la Referencia general de AWS.

Tenga en cuenta que la política de ejemplo incluye instrucciones que permiten a Macie determinar en qué región reside el bucket (`GetBucketLocation`) y agregar objetos al bucket (`PutObject`). Estas declaraciones definen condiciones que utilizan dos claves de condición globales de IAM:

- aws: SourceAccount — Esta condición permite a Macie añadir los resultados del descubrimiento de datos confidenciales al depósito solo para su cuenta. Impide que Macie añada los resultados de detección de otras cuentas al bucket. Más específicamente, la condición especifica qué cuenta puede usar el bucket para los recursos y las acciones especificados en la `aws:SourceArn` condición.

  Para almacenar los resultados de cuentas adicionales en el bucket, añada el identificador de cada cuenta adicional a esta condición. Por ejemplo:

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

- aws: SourceArn — Esta condición restringe el acceso al depósito en función del origen de los objetos que se van a añadir al depósito. Impide que otras Servicios de AWS personas añadan objetos al depósito. También evita que Macie añada objetos al bucket mientras realiza otras acciones en su cuenta. Más concretamente, la condición permite a Macie agregar objetos al bucket solo si se trata de resultados de detección de datos confidenciales y únicamente si esos resultados corresponden a una detección de datos confidenciales automatizada o a trabajos de detección de datos confidenciales creados por la cuenta especificada en la región especificada.

  Para permitir que Macie lleve a cabo las acciones especificadas para cuentas adicionales, añada los ARN de cada cuenta adicional a esta condición. Por ejemplo:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
      "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
  ```

```
]
```

Las cuentas especificadas en las condiciones `aws:SourceAccount` y `aws:SourceArn` deben coincidir.

Ambas condiciones ayudan a evitar que Macie sea utilizado como un ayudante confuso durante las transacciones con Amazon S3. Aunque no lo recomendamos, puedes eliminar estas condiciones de la política del bucket.

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

Ahora, puede configurar los ajustes del repositorio en Macie.

Configuración de los ajustes del repositorio en Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, en Ajustes, seleccione Resultados de la detección.
3. En Repositorio para ver los resultados de la detección de datos confidenciales, elija Bucket existente.
4. En Elegir un bucket, seleccione el bucket en el que desea almacenar los resultados de la detección.
5. (Opcional) Para especificar un prefijo para usarlo en la ruta a una ubicación del bucket, amplíe la sección Avanzadas. Luego, para el Prefijo de resultado de detección de datos, introduzca el prefijo que va a usar.

   Al introducir un valor, Macie actualiza el ejemplo situado debajo del cuadro para mostrar la ruta a la ubicación del bucket en la que almacenará los resultados de la detección.
6. En Configuración del cifrado, especifique la AWS KMS key que Macie tiene que utilizar para cifrar los resultados:

   - Para usar una clave de su propia cuenta, elija Seleccionar una clave de su cuenta. Luego, en la lista AWS KMS key, seleccione la clave que desea usar. La lista muestra las claves KMS de cifrado simétrico administradas por el cliente para su cuenta.
   - Para usar una clave que pertenezca a otra cuenta, seleccione Ingrese el ARN de una clave de otra cuenta. A continuación, en el cuadro AWS KMS key ARN, introduzca el ARN de la clave que se va a utilizar, como por ejemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.

7. Cuando termine con la configuración, elija Guardar.

   Macie comprueba la configuración para verificar que es correcta. Si alguna configuración es incorrecta, Macie muestra un mensaje de error que lo ayuda a solucionar el problema.

Tras guardar la configuración del repositorio, Macie añade al mismo los resultados de detección existentes de los 90 días anteriores. Macie también comienza a añadir nuevos resultados de detección al repositorio.

> **Note**
>
> Si posteriormente cambia la configuración de Prefijo de resultados de detección de datos, actualice también la política de buckets en Amazon S3. Las instrucciones de política que especifican la ruta anterior deben especificar la nueva ruta. De lo contrario, Macie no podrá agregar los resultados de la detección al bucket.

> **Tip**
>
> Para reducir los costes de cifrado del lado del servidor, configure también el depósito de S3 para que utilice una clave de depósito de S3 y especifique la AWS KMS key que haya configurado para cifrar los resultados de la detección de datos confidenciales. El uso de una clave de depósito de S3 reduce el número de llamadas AWS KMS, lo que puede reducir los costes de las AWS KMS solicitudes. Si la clave de KMS se encuentra en un almacén de claves externo, el uso de una clave de bucket de S3 también puede minimizar el impacto en el rendimiento de usar una clave. Para obtener más información, consulte Reducción del costo de SSE-KMS con las claves de bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Clases y formatos de almacenamiento compatibles con Amazon Macie

Para ayudarle a detectar datos confidenciales en su patrimonio de datos de Amazon Simple Storage Service (Amazon S3), Amazon Macie es compatible con la mayoría de las clases de almacenamiento de Amazon S3 y con una amplia variedad de formatos de archivos y almacenamiento. Esta

compatibilidad se aplica al uso de identificadores de datos administrados y al uso de identificadores de datos personalizados para analizar objetos de S3.

Para que Macie analice un objeto de S3, el objeto debe almacenarse en un bucket de uso general de Amazon S3 mediante una clase de almacenamiento compatible. El objeto también debe utilizar un archivo o un formato de almacenamiento compatible. En los temas de esta sección se enumeran las clases de almacenamiento y los formatos de archivo y almacenamiento que Macie admite actualmente.

> **Tip**
>
> Aunque Macie está optimizado para Amazon S3, puede usarlo para detectar datos confidenciales en recursos que actualmente almacena en otros lugares. Para ello, puede mover los datos a Amazon S3 de forma temporal o permanente. Por ejemplo, exporte instantáneas Amazon Relational Database Service o Amazon Aurora a Amazon S3 en formato Apache Parquet. O exporte una tabla de Amazon DynamoDB a Amazon S3. A continuación, puede crear un trabajo de detección de datos confidenciales para analizar los datos en Amazon S3.

Temas

Clases de almacenamiento compatbles de Amazon S3

Para la detección de datos confidenciales, Amazon Macie admite las siguientes clases de almacenamiento de Amazon S3:

- Redundancia reducida (RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 One Zone-Infrequent Access (S3 One Zone-IA)
- S3 Standard
- S3 Standard-Infrequent Access (S3 Standard-IA)

Macie no analiza objetos de S3 que utilizan otras clases de almacenamiento de Amazon S3, como S3 Glacier Deep Archive o S3 Express One Zone. Además, Macie no analiza los objetos que están almacenados en los depósitos de directorio de S3.

Si configura un trabajo de detección de datos confidenciales para analizar objetos de S3 que no utilizan una clase de almacenamiento de Amazon S3 compatible, Macie omite esos objetos cuando se ejecuta el trabajo. Macie no intenta extraer ni analizar los datos de los objetos: los trata como objetos no clasificables. Un objeto no clasificables es un objeto que no utiliza una clase de almacenamiento de compatible o un archivo o formato de almacenamiento compatible. Macie analiza solo aquellos objetos que utilizan una clase, archivo o formato de almacenamiento compatibles.

Igualmente, si se configura Macie para que realice la detección automática de datos confidenciales, los objetos no clasificables no podrán seleccionarse ni analizarse. Macie selecciona solo los objetos que utilizan una clase de almacenamiento Amazon S3, un archivo o formato de almacenamiento compatibles.

Para identificar los depósitos de S3 que almacenan objetos inclasificables, puede filtrar el inventario de depósitos de S3. Para cada bucket del inventario, hay campos que indican el número y el tamaño total de almacenamiento de los objetos no clasificables del depósito.

Para obtener información detallada sobre las clases de almacenamiento que ofrece Amazon S3, consulte Uso de las clases de almacenamiento de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Formatos de archivo y almacenamiento compatibles

Cuando Amazon Macie analiza un objeto de S3, recupera la última versión del objeto de Amazon S3 y luego realiza una inspección profunda de los contenidos del objeto. Esta inspección tiene en cuenta el formato de archivo o almacenamiento de los datos. Macie puede analizar los datos en muchos formatos diferentes, incluidos los formatos de compresión y archivo más utilizados.

Cuando Macie analiza los datos de un archivo comprimido o archivado, Macie inspecciona tanto el archivo completo como su contenido. Para revisar el contenido del archivo, Macie los descomprime y, a continuación, inspecciona cada archivo extraído que utiliza un formato compatible. Macie puede hacer esto para un máximo de 1 000 000 de archivos y hasta una profundidad anidada de 10 niveles. Para obtener información sobre las cuotas adicionales que se aplican a la detección de datos confidenciales, consulte Cuotas de Amazon Macie.

En la siguiente tabla se enumeran y describen los tipos de archivos y formatos de almacenamiento que Macie puede analizar para detectar datos confidenciales. Para cada tipo compatible, la tabla también muestra las extensiones de nombre de archivo aplicables.

Tipo de archivo o almacenamiento	Descripción	Extensiones de nombre de archivo
Big data	Contenedores de objetos Apache Avro y archivos de Apache Parquet	.avro, .parquet
Compresión o archivo	Archivos comprimidos GNU Zip, TAR y ZIP	.gz, .gzip, .tar, .zip
Documento	Archivos de formato de documento portátil de Adobe, libros de trabajo de Microsoft Excel y documentos de Microsoft Word	.doc, .docx, .pdf, .xls, .xlsx
Mensaje de correo electrónico	Archivos de correo electrónico cuyo contenido cumpla los requisitos especificados en una RFC del IETF para los mensajes de correo electrónico, como la RFC 2822	.eml
Texto	Archivos de texto no binarios, como archivos de valores separados por comas (CSV), archivos de lenguaje de marcado de hipertexto (HTML), archivos de notación de JavaScript objetos (JSON), archivos de líneas JSON, documentos de texto sin formato, archivos de valores separados por tabulaciones	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, . y otros (según el tipo de archivo de texto no binario)

Tipo de archivo o almacenamiento	Descripción	Extensiones de nombre de archivo
	(TSV) y archivos de lenguaje de marcado extensible (XML)	

Macie no analiza los datos de las imágenes ni del audio, el vídeo ni otros tipos de contenido multimedia.

Si configura un trabajo de detección de datos confidenciales para analizar los objetos de S3 que no utilizan un formato de archivo o almacenamiento compatible, Macie omite esos objetos cuando se ejecuta el trabajo. Macie no intenta extraer ni analizar los datos de los objetos: los trata como objetos no clasificables. Un objeto no clasificable es un objeto que no utiliza una clase de almacenamiento de Amazon S3 compatible ni un archivo o formato de almacenamiento compatible. Macie analiza solo aquellos objetos que utilizan una clase, archivo o formato de almacenamiento compatibles.

Igualmente, si se configura Macie para que realice la detección automática de datos confidenciales, los objetos no clasificables no podrán seleccionarse ni analizarse. Macie selecciona solo los objetos que utilizan una clase de almacenamiento Amazon S3, un archivo o formato de almacenamiento compatibles.

Para identificar los depósitos de S3 que almacenan objetos inclasificables, puede filtrar el inventario de depósitos de S3. Para cada bucket del inventario, hay campos que indican el número y el tamaño total de almacenamiento de los objetos no clasificables del depósito.

Análisis de los resultados de Amazon Macie

Amazon Macie genera resultados cuando detecta posibles infracciones de políticas o problemas con la seguridad o la privacidad de sus depósitos de uso general de Amazon Simple Storage Service (Amazon S3) o detecta datos confidenciales en objetos de S3. Un resultado es un informe detallado de un posible problema de o información confidencial que Macie encontró. Cada resultado proporciona una clasificación de gravedad, información sobre el recurso afectado y detalles adicionales, como cuándo y cómo Macie detectó el problema o los datos. Macie almacena sus resultados de política y datos confidenciales durante 90 días.

Puede revisar, analizar y administrar resultados de las siguientes formas.

consola de Amazon Macie

En las páginas de Resultados de la consola de Amazon Macie se enumeran sus resultados y se proporciona información detallada sobre los resultados individuales. Estas páginas también ofrecen opciones para agrupar, filtrar y ordenar los resultados, así como para crear y gestionar reglas de supresión. Para agilizar su análisis de los resultados, puede crear y utilizar reglas de supresión.

Amazon Macie API

Con la API de Amazon Macie, puede consultar y recuperar datos de hallazgos mediante una herramienta de línea de AWS comandos o un AWS SDK, o bien enviando solicitudes HTTPS directamente a Macie. Para consultar los datos, debe enviar una solicitud a la API de Amazon Macie y utilizar los parámetros compatibles para especificar los resultados que desea recuperar. Después de enviar la consulta, devuelve los resultados de la consulta en una respuesta JSON. A continuación, puede transferir los resultados a otro servicio o aplicación para un análisis más exhaustivo, para su almacenamiento a largo plazo o para la generación de informes. Para obtener más información, consulte la Referencia de las API de Amazon Macie.

Amazon EventBridge

Para respaldar aún más la integración con otros servicios y sistemas, como los sistemas de monitoreo o gestión de eventos, Macie publica los resultados en Amazon EventBridge como eventos. EventBridge, anteriormente Amazon CloudWatch Events, es un servicio de bus de eventos sin servidor que puede ofrecer un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y, por ejemplo, Servicios de AWS Macie. Puede dirigir esos datos a destinos como AWS Lambda funciones, temas de Amazon

Simple Notification Service y transmisiones de Amazon Kinesis para un procesamiento adicional y automatizado. El uso de EventBridge también ayuda a garantizar la retención a largo plazo de los datos de los hallazgos. Para obtener más información EventBridge, consulta la Guía del EventBridge usuario de Amazon.

Macie publica automáticamente los eventos EventBridge para obtener nuevos hallazgos. También publica los eventos automáticamente para que se repitan posteriormente los resultados de las políticas existentes. Como los datos de los hallazgos están estructurados como EventBridge eventos, puede monitorear, analizar y actuar en consecuencia con mayor facilidad mediante el uso de otros servicios y herramientas. Por ejemplo, puede utilizarlos EventBridge para enviar automáticamente tipos específicos de nuevos hallazgos a una AWS Lambda función que, a su vez, procese y envíe los datos a su sistema de gestión de incidentes y eventos de seguridad (SIEM). Si integra las Notificaciones de usuarios de AWS con Macie, también puede usar los eventos para recibir notificaciones automáticas de los resultados a través de los canales de entrega que especifique. Para obtener información sobre el uso de EventBridge eventos para monitorear y procesar los hallazgos, consulteIntegración de Amazon Macie con Amazon Eventbridge.

AWS Security Hub

Para obtener un análisis adicional y más amplio de la postura de seguridad de su organización, también puede publicar los resultados en AWS Security Hub. Security Hub es un servicio que recopila datos de seguridad de las soluciones de AWS Partner Network seguridad compatibles Servicios de AWS y las soluciones de seguridad compatibles para proporcionarle una visión integral del estado de seguridad en todo su AWS entorno. Security Hub le permite comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener más información sobre Security Hub, consulte la AWS Security Hub Guía del usuario. Para obtener más información sobre el uso del Centro de seguridad para supervisar y procesar los resultados, consulte Integración de Amazon Macie con AWS Security Hub.

Además de las conclusiones, Macie crea resultados de detección de datos confidenciales para los objetos de S3 que analiza para detectar datos confidenciales. Un resultado de detección de datos confidenciales es un registro de los detalles sobre el análisis de un objeto. Esto incluye objetos en los que Macie no encuentra datos confidenciales y, por lo tanto, no produce resultados y objetos que Macie no puede analizar debido a problemas o errores. Los resultados del detección de datos confidenciales le proporcionan registros de análisis que pueden resultar útiles para auditorías o investigaciones sobre la privacidad y la protección de los datos. No puede acceder a los resultados de detección de datos confidenciales directamente en la consola de Amazon Macie ni con la API de

Amazon Macie. En su lugar, configura Macie para almacenar los resultados en un bucket de S3. A continuación, si lo desea, puede acceder a los resultados de ese bucket y consultarlos. Para saber cómo configurar Macie para almacenar los resultados, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Temas

Tipos de resultados de Amazon Macie

Amazon Macie ofrece dos categorías de resultados: resultados de políticas y datos confidenciales. La constatación de una política es un informe detallado sobre una posible infracción de la política o un problema con la seguridad o la privacidad de un depósito de uso general de Amazon Simple Storage Service (Amazon S3). Macie genera conclusiones sobre las políticas como parte de sus actividades continuas para evaluar y supervisar sus segmentos de uso general en materia de seguridad y control de acceso. Un resultado de datos confidenciales es un informe detallado de los datos confidenciales que Macie encontró en un objeto de S3. Macie recopila datos confidenciales como parte de las actividades que lleva a cabo cuando realiza tareas de descubrimiento de datos confidenciales o realiza el descubrimiento automatizado de datos confidenciales.

Dentro de cada categoría, hay tipos específicos. El tipo de resultado proporciona información sobre la naturaleza del problema o de los datos confidenciales encontrados por Macie. Los detalles de un resultado proporcionan una clasificación de gravedad, información sobre el recurso afectado y detalles adicionales, como cuándo y cómo Macie detectó el problema o los datos confidenciales. La gravedad y los detalles de cada resultado varían según el tipo y la naturaleza del resultado.

Temas

> **Tip**
>
> Para obtener información sobre los distintos tipos de resultados que proporciona Macie, puede generar ejemplos de resultados. Los resultados de los ejemplos utilizan datos de ejemplo y valores de marcador de posición para demostrar los tipos de información que puede contener cada tipo de resultado.

Tipos de resultados de políticas

Amazon Macie genera una constatación de política cuando las políticas o la configuración de un depósito de uso general de S3 se modifican de forma que se reduce la seguridad o la privacidad del depósito y de los objetos del depósito. Para obtener más información sobre cómo Macie detecta estos cambios, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.

Macie genera un resultado de políticas solo si el cambio se produce después de activar Macie para su Cuenta de AWS. Por ejemplo, si la configuración de bloquear el acceso público está deshabilitada para un bucket de S3 después de activar Macie, Macie generará un comando BlockPublicAccessDisabledpolicy:IAMuser/S3 para el bucket. Si la configuración de bloqueo de acceso público estaba deshabilitada para un bucket cuando activaste Macie y sigue inhabilitada, Macie no generará ningún comando Polic:iamUser/S3 buscando el bucket. BlockPublicAccessDisabled

Si Macie detecta una ocurrencia posterior a un resultado de política existente, Macie actualiza el resultado existente añadiendo detalles sobre la ocurrencia posterior e incrementando el recuento de ocurrencias. Macie guarda los resultados de políticas durante 90 días.

Macie puede generar los siguientes tipos de conclusiones políticas para un bucket de uso general de S3.

Policy:IAMUser/S3BlockPublicAccessDisabled

Todas las configuraciones de acceso público en bloque a nivel de bucket para el bucket. El acceso al bucket se controla mediante la configuración de bloqueo de acceso público de la cuenta, las listas de control de acceso (ACL) y la política del bucket.

Para obtener más información sobre la configuración del bloqueo de acceso público de los buckets de S3, consulte Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3 en la Guía del usuario de Amazon Simple Storage Service.

Policy:IAMUser/S3BucketEncryptionDisabled

La configuración de cifrado predeterminada del bucket se restableció al comportamiento de cifrado predeterminado de Amazon S3, que consiste en cifrar los nuevos objetos automáticamente con una clave gestionada por Amazon S3.

A partir del 5 de enero de 2023, Amazon S3 aplica el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) como el nivel básico de cifrado para cada objeto añadido a un bucket. Si lo desea, puede configurar los ajustes de cifrado predeterminados de un bucket para utilizar el cifrado del lado del servidor con una AWS KMS clave (SSE-KMS) o el cifrado de doble capa del lado del servidor con una clave (DSSE-KMS). AWS KMS Para obtener información sobre las opciones y la configuración de cifrado para buckets de S3, consulte Establecer el comportamiento del cifrado predeterminado del servidor para los bucket de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Si Macie generó este tipo de resultado antes del 5 de enero de 2023, el resultado indica que la configuración de cifrado predeterminada estaba deshabilitada para el bucket afectado. Esto significaba que la configuración del bucket no especificaba el comportamiento de cifrado predeterminado del lado del servidor para los objetos nuevos. Amazon S3 ya no admite la capacidad de deshabilitar la configuración de cifrado predeterminada de un bucket.

Policy:IAMUser/S3BucketPublic

Se modificó la política de ACL o bucket del bucket para permitir el acceso de usuarios anónimos o de todas las identidades autenticadas (IAM). AWS Identity and Access Management

Para obtener información sobre las políticas de ACL y políticas de buckets, consulte Administración de identidades y accesos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Policy:IAMUser/S3BucketReplicatedExternally

La replicación se habilitó y configuró para replicar los objetos del depósito en un Cuenta de AWS depósito externo a la organización (no parte de ella). Una organización es un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante AWS Organizations una invitación de Macie.

En determinadas condiciones, Macie podría generar este tipo de búsqueda para un depósito que no esté configurado para replicar objetos en un depósito externo. Cuenta de AWS Esto puede ocurrir si el bucket de destino se creó en un lugar diferente Región de AWS durante las 24 horas anteriores, después de que Macie recuperara los metadatos del bucket y del objeto de

Amazon S3 como parte del ciclo de actualización diario. Para investigar el resultado, comience por actualizar los datos de su inventario. A continuación, revise los detalles del bucket. Los detalles indican si el bucket está configurado para replicar objetos en otros buckets. Si el bucket está configurado para ello, los detalles incluyen el ID de cuenta de cada cuenta propietaria de un bucket de destino.

Para obtener información acerca de las configuraciones de replicar de los buckets de S3, consulte Replicación de objetos en la Guía del usuario de Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedExternally

Se modificó la política de ACL o bucket del bucket para permitir que el bucket se comparta con una entidad externa a la organización (Cuenta de AWS que no forme parte de ella). Una organización es un conjunto de cuentas de Macie que se administran de forma centralizada como un grupo de cuentas relacionadas mediante AWS Organizations una invitación de Macie.

En algunos casos, Macie podría generar este tipo de resultado para un bucket que no se comparta con una cuenta de AWS externa. Esto puede ocurrir si Macie no puede evaluar completamente la relación entre el elemento `Principal` de la política del bucket y determinadas claves de contexto de condiciones AWS globales o claves de condición de Amazon S3 del elemento `Condition` de la política. Las claves de condición aplicables son: `aws:PrincipalAccountaws:PrincipalArn`,`aws:PrincipalOrgID`,`aws:PrincipalOrgPaths`,,`a` `aws:SourceVpce` `aws:userids3:DataAccessPointAccount`, y. `s3:DataAccessPointArn` Le recomendamos que revise la política del bucket para determinar si este acceso está previsto y es seguro.

Para obtener información sobre las políticas de ACL y políticas de buckets, consulte Administración de identidades y accesos en Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedWithCloudFront

La política del depósito se modificó para permitir que el depósito se comparta con una identidad de acceso al CloudFront origen (OAI) de Amazon, un control de acceso al CloudFront origen (OAC) o con una CloudFront OAI y una OAC a la vez. CloudFront Una CloudFront OAI o una OAC permiten a los usuarios acceder a los objetos de un bucket a través de una o más distribuciones específicas. CloudFront

Para obtener más información sobre las CloudFront OAI y las OAC, consulte Restringir el acceso a un origen de Amazon S3 en la Guía para CloudFrontdesarrolladores de Amazon.

> **Note**
>
> En algunos casos, Macie genera una búsqueda Policy:iamUser/S3 en lugar de una BucketSharedExternally búsqueda Policy:iamUser/S3 para un bucket. BucketSharedWithCloudFront Estos casos son:
>
> - El depósito se comparte con una entidad externa a tu organización, además de con una OAI o una Cuenta de AWS OAC. CloudFront
> - La política del bucket especifica un ID de usuario canónico, en lugar del nombre de recurso de Amazon (ARN), de una OAI. CloudFront
>
> Esto produce un resultado de política de mayor gravedad para el bucket.

Tipos de resultado de datos confidenciales

Macie genera un resultado de datos confidenciales cuando detecta datos confidenciales en un objeto de S3 que analiza para detectar datos confidenciales. Esto incluye los análisis que Macie realiza cuando realizas un trabajo de descubrimiento de datos confidenciales o cuando realiza un descubrimiento automatizado de datos confidenciales.

Por ejemplo, si crea y ejecuta un trabajo de descubrimiento de datos confidenciales y Macie detecta números de cuentas bancarias en un objeto S3, Macie genera un resultado financiero o un objeto S3Object/Financial para SensitiveData el objeto. Del mismo modo, si Macie detecta números de cuentas bancarias en un objeto de S3 y los analiza durante un ciclo automatizado de descubrimiento de datos confidenciales, Macie genera un resultado de tipo :S3Object/Financial para el objeto. SensitiveData

Si Macie detecta datos confidenciales en el mismo objeto de S3 durante una ejecución posterior de un trabajo o un ciclo de detección automatizado de datos confidenciales, Macie genera un nuevo resultado de d atos confidenciales para el objeto. Los resultados de datos confidenciales, a diferencia de los resultados de políticas, se tratan todos como nuevos (únicos). Macie almacena los resultados de datos confidenciales durante 90 días.

Macie puede generar los siguientes tipos de resultados de datos confidenciales para un objeto de S3.

SensitiveData:S3Object/Credentials

El objeto contiene datos de credenciales confidenciales, como AWS claves de acceso secretas o claves privadas.

SensitiveData:S3Object/CustomIdentifier

El objeto contiene texto que coincide con los criterios de detección de uno o más identificadores de datos personalizados. El objeto puede contener más de un tipo de datos confidenciales.

SensitiveData:S3Object/Financial

El objeto contiene información financiera confidencial, como números de cuentas bancarias o números de tarjetas de crédito.

SensitiveData:S3Object/Multiple

El objeto contiene más de una categoría de datos confidenciales: cualquier combinación de datos de credenciales, información financiera, información personal o texto que coincida con los criterios de detección de uno o más identificadores de datos personalizados.

SensitiveData:S3Object/Personal

El objeto contiene información personal confidencial: información de identificación personal (PII), como números de pasaporte o números de identificación del carné de conducir, información de salud personal (PHI), como números de seguro médico o de identificación médica, o una combinación de PII y PHI.

Para obtener información acerca de los tipos de datos confidenciales que Macie puede detectar mediante técnicas y criterios integrados, consulteUso de identificadores de datos administrados. Para obtener información sobre los tipos de objetos S3 que Macie puede analizar, consulte Clases y formatos de almacenamiento compatibles.

Trabajar con muestras de resultados en Amazon Macie

Para explorar y obtener información sobre los diferentes tipos de resultados que Amazon Macie puede generar, puede crear ejemplos de resultados. Los resultados de los ejemplos utilizan datos de ejemplo y valores de marcador de posición para demostrar los tipos de información que puede contener cada tipo de resultado.

Por ejemplo, el resultado de muestra de Policy:IAMUser/S3BucketPublic contiene detalles sobre un bucket de Amazon Simple Storage Service (Amazon S3) ficticio. Los detalles del resultado

incluyen datos de ejemplo sobre un actor y una acción que modificó la lista de control de acceso (ACL) del bucket y lo hizo accesible al público. Del mismo modo, el resultado de la muestra SensitiveData:S3Object/Multiple contiene detalles sobre un libro de trabajo ficticio de Microsoft Excel. Los detalles del resultado incluyen datos de ejemplo sobre los tipos y la ubicación de los datos confidenciales en el libro de trabajo.

Además de familiarizarse con la información que pueden contener los distintos tipos de resultados, puede utilizar ejemplos de resultados para probar la integración con otras aplicaciones, servicios y sistemas. Según las normas de supresión de su cuenta, Macie puede publicar ejemplos de resultados en Amazon EventBridge como eventos. Al usar los datos de ejemplo en los resultados de las muestras, puede desarrollar y probar soluciones automatizadas para monitorear y procesar estos eventos. En función de la configuración de publicación de su cuenta, Macie también puede publicar ejemplos de resultados en. AWS Security Hub Esto significa que también puede usar ejemplos de resultados para desarrollar y probar soluciones para monitorear y procesar los resultadosde Macie en Security Hub. Para obtener información sobre la publicación de los resultados en estos servicios, consulte Seguimiento y procesamiento de los hallazgos.

Temas

Generar resultados de muestra

Puede crear resultados de muestra mediante la consola de Amazon Macie o la API de Amazon Macie. Si utiliza la consola, Macie genera automáticamente un resultado de muestra para cada tipo de resultado compatible con Macie. Si utiliza la API, puede crear una muestra para cada tipo o solo para algunos tipos que especifique.

Console

Siga estos pasos para crear resultados de muestra mediante la consola de Amazon Macie.

Para crear resultados de muestra

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Settings (Configuración).
3. En Sample findings, seleccione Generate sample findings.

API

Para crear resultados de muestra mediante programación, utilice la operación CreateSampleFindings de la API de Amazon Macie. Cuando envíe su solicitud, si lo desea, utilice el parámetro `findingTypes` para especificar únicamente determinados tipos de resultados de muestra que desee crear. Para crear automáticamente muestras de todos los tipos, no incluya este parámetro en la solicitud.

Para crear resultados de muestra mediante AWS Command Line Interface (AWS CLI), ejecute el comando create-sample-findings. Para crear automáticamente muestras de todos los tipos, no incluya el parámetro `finding-types`. Para crear muestras de solo ciertos tipos de resultados, incluya este parámetro y especifique los tipos de resultados de muestra que desee crear. Por ejemplo:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

Mientras que *`SensitiveData:S3Object/Multiple`* es un tipo de resultado de datos confidenciales para crear y *`Policy:IAMUser/S3BucketPublic`* es un tipo de resultado de política para crear.

Si el comando se ejecuta correctamente, Macie devuelve una respuesta vacía.

Revisión de resultados de muestra

Para ayudarle a identificar los resultados de muestra que ha creado, Macie establece el valor del campo Muestra de cada resultado de muestra en Verdadero. Además, el nombre del bucket de S3 afectado es el mismo para todos los resultados de la muestra: macie-sample-finding-bucket. Si revisa los resultados de las muestras mediante las páginas de resultados de la consola Amazon Macie, Macie también mostrará el prefijo [SAMPLE] en el campo Tipo de resultado para cada resultado de muestra.

Console

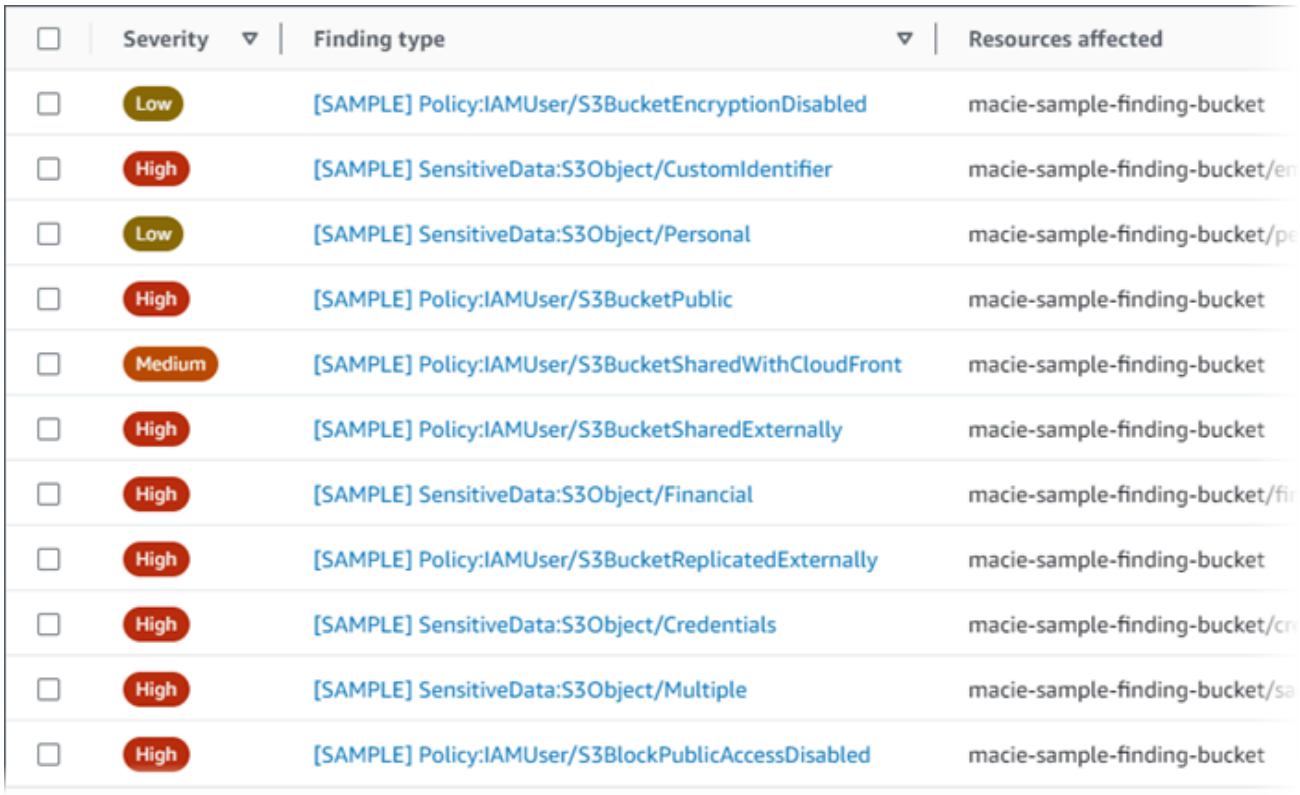
Siga estos pasos para crear resultados de muestra mediante la consola de Amazon Macie.

Para revisar resultados de muestra

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. En el panel de navegación, seleccione Resultados.
3. En la página Resultados, realice alguna de las siguientes acciones:

   - En la columna Tipo de resultado, localice los resultados cuyo tipo comience por [SAMPLE], como se muestra en la imagen siguiente.



   - Al utilizar el cuadro Criterios de filtro situado encima de la tabla, filtre la tabla para que muestre solo los resultados de la muestra. Para ello, coloque el cursor en el cuadro. En la lista de campos que aparece, selecciona Muestra. Elija Habilitada y, a continuación, elija Aplicar. Esto añade la siguiente condición de filtro a la tabla:

4. Para revisar los detalles de un resultado de muestra específico, selecciónelo. El panel de detalles muestra información sobre el resultado.

También puede descargar y guardar los detalles de uno o más ejemplos de resultados en un archivo JSON. Para ello, seleccione la casilla de verificación de cada resultado de muestra que desee descargar y guardar. A continuación, seleccione Exportar (JSON) en el menú Acciones de la parte superior de la página Resultados. En la ventana que aparece, seleccione Descargar.

Para obtener descripciones detalladas de los campos de JSON que puede incluir un resultado, consulte Resultados en la referencia de la API de Amazon Macie.

API

Para revisar los resultados de las muestras mediante programación, utilice primero la operación ListFindings de la API de Amazon Macie para recuperar el identificador único (`findingId`) de cada resultadode muestra que haya creado. A continuación, utilice la operación GetFindings para recuperar los detalles de esos resultados.

Al enviar la solicitud ListFindings, puede especificar los criterios de filtro para incluir solo los resultados de una muestra en los resultados. Para ello, añada una condición de filtro en la que el valor para el campo `sample` sea `true`. Si utiliza el AWS CLI, ejecute el comando list-findings y utilice el `finding-criteria` parámetro para especificar la condición del filtro. Por ejemplo:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":
[\"true\"]}}}
```

Si la solicitud se realiza correctamente, Macie devuelve una `findingIds` matriz. La matriz muestra el identificador único de cada ejemplo encontrado para su cuenta en la Región de AWS actual.

A continuación, para recuperar los detalles de los resultados de la muestra, especifique estos identificadores únicos en una solicitud GetFindings o, para la AWS CLI, cuando ejecute el comando get-findings.

Supresión de resultados

Al igual que otros resultados, Macie almacena los resultados de las muestras durante 90 días. Cuando termine de revisar y experimentar con las muestras, si lo desea, puede archivarlas creando una regla de supresión. Si lo hace, los resultados de las muestras dejarán de aparecer de forma predeterminada en la consola y su estado cambiará a archivado.

Para archivar los resultados de muestras mediante la consola de Amazon Macie, configure la regla para archivar los resultados en los que el valor del campo Muestra sea Verdadero. Para archivar los resultados de muestras mediante la API de Amazon Macie, configure la regla para archivar los resultados en los que el valor del campo `sample` sea `true`.

Revisión de resultados de la consola de Amazon Macie

Amazon Macie supervisa su AWS entorno y genera conclusiones sobre las políticas cuando detecta posibles infracciones de las políticas o problemas con la seguridad o la privacidad de sus depósitos de uso general de Amazon Simple Storage Service (Amazon S3). Macie genera resultados confidenciales cuando detecta datos confidenciales en objetos de S3. Macie almacena sus resultados de política y datos confidenciales durante 90 días.

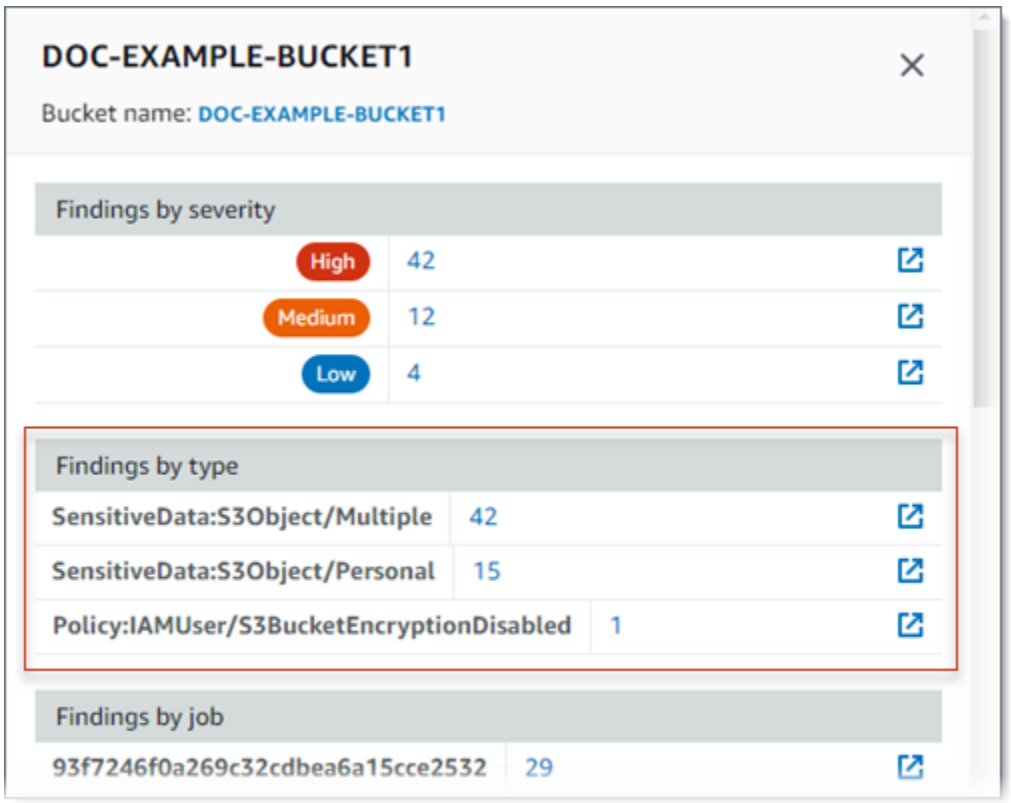
Cada resultado especifica un tipo de resultado y una calificación de gravedad. Los detalles adicionales incluyen información sobre el recurso afectado y cuándo y cómo Macie descubrió el problema o datos confidenciales informados por el resultado. La gravedad y los detalles de cada resultado varían según el tipo y la naturaleza del resultado.

Con la consola de Amazon Macie, puede revisar y analizar los resultados y acceder a los detalles de los resultados individuales. También puede exportar uno o más resultados a un archivo JSON. Para ayudarle a optimizar su análisis, la consola ofrece varias opciones para crear vistas personalizadas de los resultados.

Utilice agrupaciones predefinidas

Utilice páginas específicas para revisar los resultados agrupados por criterios, como el bucket de S3 afectado, el tipo de resultado o el trabajo de descubrimiento de datos confidenciales. En estas páginas, puede revisar las estadísticas agregadas de cada grupo, como el recuento de resultados por gravedad. También puede profundizar para revisar los detalles de los resultados individuales de un grupo y aplicar filtros para afinar su análisis.

Por ejemplo, si agrupa todos los resultados por bucket de S3 y observa que un bucket en particular ha infringido una política, podrá determinar rápidamente si también hay datos confidenciales relacionados con ese bucket. Para ello, seleccione Por bucket en el panel de navegación (en Resultados) y, a continuación, seleccione el grupo. En el panel de detalles que aparece, la sección Resultados por tipo enumera los tipos de resultados que se aplican al bucket, como se muestra en la siguiente imagen.

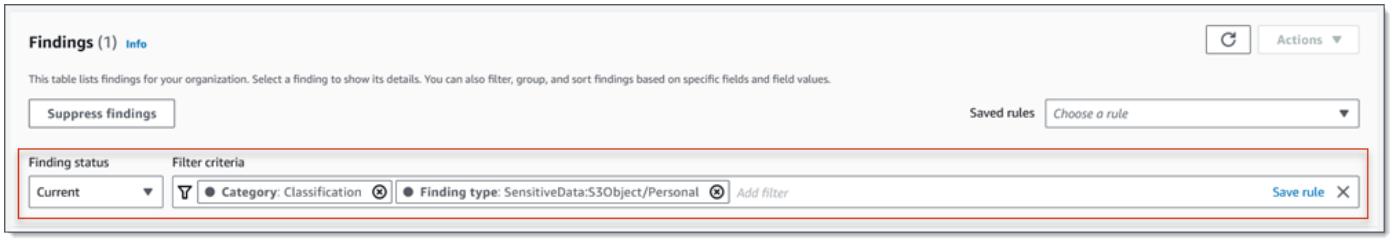


Para investigar un tipo específico, seleccione el número del tipo. Macie muestra una tabla con todos los resultados que coinciden con el tipo seleccionado y que se aplican al segmento S3. Para refinar los resultados, filtre la tabla.

Cree y aplique filtros

Utilice atributos de resultados específicos para incluir o excluir determinados resultados de una tabla de resultados. Un atributo de resultado es un campo que almacena datos específicos de un resultado, como el tipo de resultado, la gravedad o el nombre del bucket de S3 afectado. Si filtra una tabla, puede identificar más fácilmente los resultados que tienen características específicas. A continuación, puede profundizar para revisar los detalles de esos resultados.

Por ejemplo, para revisar todos sus resultados de datos confidenciales, añada criterios de filtro para el campo Categoría. Para refinar los resultados e incluir solo un tipo específico de búsqueda de datos confidenciales, añada criterios de filtro para el campo Tipo de resultado. Por ejemplo:



Para revisar los detalles de un resultado concreto, selecciónelo. El panel de detalles muestra información sobre el resultado.

También puede ordenar los resultados de manera ascendente o descendente por ciertos campos. Para ello, haga clic en el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a hacer clic en el encabezado de la columna.

Para revisar los resultados en la consola

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (resultados). La página de hallazgos muestra los hallazgos que Macie creó o actualizó para tu cuenta en el estado actual Región de AWS durante los últimos 90 días. De forma predeterminada, esto no incluye los resultados que se suprimieron mediante una regla de supresión.
3. Para dinamizar y revisar los resultados por un grupo lógico predefinido, seleccione Por bucket, Por tipo o Por trabajo en el panel de navegación (bajo Resultados). A continuación, seleccione un elemento en la tabla. En el panel de detalles, elija la conexión para el campo en el que se va a dinamizar.
4. Para filtrar los resultados según criterios específicos, utilice las opciones de filtro que se encuentran encima de la tabla:

   - Para mostrar los resultados que se suprimieron mediante una regla de supresión, utilice el menú Estado del resultado. Seleccione Todos para mostrar los resultados suprimidos y no suprimidos, o bien seleccione Archivado para mostrar solo los resultados suprimidos. Para volver a ocultar los resultados suprimidos, seleccione Actual.
   - Para mostrar solo los resultados que tienen un atributo específico, utilice el cuadro Criterios de filtro. Coloque el cursor en el cuadro y añada una condición de filtro para el atributo. Para refinar aún más los resultados, añada condiciones para atributos adicionales. Para, a continuación, eliminar una condición, pulse el icono de eliminación de la condición () correspondiente a la condición que desee eliminar.

   Para obtener más información sobre cómo filtrar resultados, consulte Crear y aplicar filtros a los resultados.

5. Para ordenar los resultados por un campo específico, haga clic en el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a hacer clic en el encabezado de la columna.
6. Para revisar los detalles de un resultado específico, selecciónelo. El panel de detalles muestra información sobre el resultado.

> **Tip**
>
> Puede usar el panel de detalles para desplazarse y profundizar en ciertos campos. Para mostrar los resultados que tienen el mismo valor para un campo, seleccione
>
> 
>
> en el campo. O bien, seleccione
>
> 
>
> para mostrar los resultados que tengan otros valores para el campo.
> Con respecto a un resultado de datos confidenciales, también puede utilizar el panel de detalles para investigar los datos confidenciales que Macie encontró en el objeto de S3 afectado:
>
> - Para localizar casos de un tipo específico de datos confidenciales, seleccione la conexión numérico del campo correspondiente a ese tipo de datos. Macie muestra información (en formato JSON) sobre dónde encontró Macie los datos. Para obtener más información, consulte Localización de los datos confidenciales.
> - Para recuperar ejemplos de los datos confidenciales que Macie encontró, seleccione Revisar en el campo Mostrar ejemplos. Para obtener más información, consulte Recuperación de muestras de datos confidenciales.
> - Para navegar hasta el resultado de detección de datos confidenciales correspondiente, seleccione la conexión en el campo Ubicación detallada del resultado. Macie abre la consola de Amazon S3 y muestra el archivo o la carpeta que contiene el resultado de la detección. Para obtener más información, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

También puede descargar y guardar los detalles de uno o más resultados en un archivo JSON. Para ello, seleccione la casilla de verificación de cada resultado que desee descargar y guardar. A continuación, seleccione Exportar (JSON) en el menú Acciones de la parte superior de la página

Resultados. En la ventana que aparece, seleccione Descargar. Para obtener descripciones detalladas de los campos de JSON que puede incluir un resultado, consulte Resultados en la referencia de la API de Amazon Macie.

Filtro de resultados de Amazon Macie

Para realizar análisis específicos y analizar los resultados de manera más eficiente, puede filtrar los resultados de Amazon Macie. Con los filtros, puede crear vistas y consultas personalizadas para los resultados, lo que le puede ayudar a identificar y centrarse en los resultados que tengan características específicas. Utilice la consola de Amazon Macie para filtrar los resultados o envíe consultas mediante programación con la API de Amazon Macie.

Al crear un filtro, se utilizan atributos específicos de los resultados para definir criterios que permitan incluir o excluir resultados de una vista o de los resultados de una consulta. Un atributo de resultado es un campo que almacena datos específicos de un resultado, como el tipo de resultado, la gravedad o el nombre del bucket de S3 afectado.

En Macie, un filtro consta de una o más condiciones. Cada condición, también denominada criterio, consta de tres partes:

- Un campo basado en atributos, como la Gravedad o el Tipo de resultado.
- Un operador, como igual o no igual.
- Uno o varios valores. El tipo y el número de valores dependen del campo y el operador que elija.

Si crea un filtro que desee volver a utilizar, puede guardarlo como regla de filtro. Una regla de filtro es un conjunto de criterios de filtro que usted crea y guarda para volver a aplicarlos al revisar los resultados en la consola de Amazon Macie.

También puede guardar un filtro como regla de supresión. Una regla de supresión es un conjunto de criterios de filtro que se crean y guardan para archivar automáticamente los resultados que coincidan con los criterios de la regla. Para obtener más información sobre las reglas de supresión, consulte Supresión de hallazgos.

Temas

- Fundamentos del filtrado de resultados
- Crear y aplicar filtros a los resultados
- Creación y administración de reglas de filtrado para los resultados

- Campos para filtrar los resultados

Fundamentos del filtrado de resultados

Cuando cree un filtro, tenga presentes las siguientes características y directrices. Tenga en cuenta también que los resultados filtrados se limitan a los 90 días anteriores y a la Región de AWS actual. Amazon Macie almacena sus resultados solo durante 90 días en cada Región de AWS.

Temas

- Uso de varias condiciones en un filtro
- Especificar valores para los campos
- Especificar varios valores para un campo
- Uso de operadores en condiciones

Uso de varias condiciones en un filtro

Un filtro puede incluir una o varias condiciones. Cada condición, también denominada criterio, consta de tres partes:

- Un campo basado en atributos, como la Gravedad o el Tipo de resultado. Para obtener una lista de campos que puede utilizar, consulte Campos para filtrar los resultados.
- Un operador, como igual o no igual. Para obtener una lista de operadores que puede utilizar, consulte Uso de operadores en condiciones.
- Uno o varios valores. El tipo y el número de valores dependen del campo y el operador que elija.

Si un filtro contiene varias condiciones, Macie utiliza el operador lógico AND para unir las condiciones y evaluar los criterios del filtro. Esto significa que un resultado coincide con los criterios del filtro solo si coincide con todas las condiciones del filtro.

Por ejemplo, si agrega una condición para incluir solo los resultados de alta gravedad y agrega otra condición para incluir solo los resultados de datos confidenciales, Macie devolverá todos los resultados de datos confidenciales de alta gravedad. En otras palabras, Macie excluye todos los resultados de políticas y todos los resultados de datos confidenciales de gravedad media y baja.

Puede usar un campo solo una vez en un filtro. Sin embargo, puede especificar varios valores para varios campos.

Por ejemplo, si una condición utiliza el campo Gravedad para incluir únicamente los resultados de alta gravedad, no podrá utilizar el campo Gravedad en otra condición para incluir los de gravedad media o baja. En su lugar, especifique varios valores para la condición existente o utilice un operador diferente para la condición existente. Por ejemplo, para incluir todos los resultados de gravedad media y alta, añada una condición de Gravedad igual a Media, Alta o añada una condición de Gravedad no igual a Baja.

Especificar valores para los campos

Al especificar un valor para un campo, el valor debe ajustarse al tipo de datos subyacente del campo. Según el campo, puede especificar uno de los siguientes tipos de valores.

Matriz de texto (cadenas)

Especifica una lista de valores de texto (cadena) para un campo. Cada cadena se correlaciona con un valor predefinido o existente de un campo; por ejemplo, Alto para el campo Gravedad, SensitiveData:s3Object/Financial para el campo Tipo de resultado o el nombre de un bucket de S3 para el campo nombre del bucket de S3.

Si utiliza una matriz, tenga en cuenta lo siguiente:

- Estos valores distinguen entre mayúsculas y minúsculas.
- No puede especificar valores parciales ni utilizar caracteres comodín en los valores. Debe especificar un valor completo y válido para el campo.

Por ejemplo, para filtrar los resultados de un bucket de S3 denominado my-S3-bucket, introduzca **`my-S3-bucket`** como el valor del campo nombre del bucket de S3. Si introduce cualquier otro valor, como **`my-s3-bucket`** o **`my-S3`**, Macie no devolverá los resultados del bucket.

Para obtener una lista de valores válidos para cada campo, consulte Campos para filtrar los resultados.

Puede especificar hasta 50 valores en una matriz. La forma de especificar los valores depende de si utiliza la consola de Amazon Macie o la API de Amazon Macie, como se explica en Especificar varios valores para un campo.

Booleano

Especifica uno de los dos valores mutuamente excluyentes de un campo.

Si utiliza la consola Amazon Macie para especificar este tipo de valor, la consola proporciona una lista de valores entre los que puede elegir. Si utiliza la API de Amazon Macie, especifique `true` o `false` para el valor.

Fecha/hora (e intervalos de tiempo)

Especifica una fecha y hora absolutas para un campo. Si especifica este tipo de valor, debe especificar una fecha y una hora.

En la consola Amazon Macie, los valores de fecha y hora están en la zona horaria local y utilizan una notación de 24 horas. En todos los demás contextos, estos valores están en hora universal coordinada (UTC) y en formato ISO 8601 extendido, por ejemplo `2020-09-01T14:31:13Z` para las 2:31:13 PM UTC del 1 de septiembre de 2020.

Si un campo almacena un valor de fecha y hora, puede usarlo para definir un intervalo de tiempo fijo o relativo. Por ejemplo, puede incluir solo los resultados que se crearon entre dos fechas y horas específicas, o solo los resultados que se crearon antes o después de una fecha y hora específicas. La forma en que defina un intervalo de tiempo, depende de si utiliza la consola de Amazon Macie o la API de Amazon Macie.

- En la consola, utilice un selector de fechas o introduzca el texto directamente en los cuadros Desde y Hasta.
- Con la API, defina un intervalo de tiempo fijo añadiendo una condición que especifique la primera fecha y hora del intervalo y añada otra condición que especifique la última fecha y hora del intervalo. Si lo hace, Macie utilizará el operador lógico AND para unir las condiciones. Para definir un intervalo de tiempo relativo, añada una condición que especifique la primera o la última fecha y hora del intervalo. Especifique los valores como marcas de tiempo de Unix en milisegundos, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

En la consola, los intervalos de tiempo son inclusivos. Con la API, los intervalos de tiempo pueden ser inclusivos o exclusivos, según el operador que elija.

Número (y rangos numéricos)

Especifica un entero largo para un campo.

Si un campo almacena un valor numérico, puede usarlo para definir un intervalo numérico fijo o relativo. Por ejemplo, puede incluir solo los resultados que informan de entre 50 y 90 casos de datos confidenciales en un objeto de S3. La forma en que defina un intervalo de tiempo, depende de si utiliza la consola de Amazon Macie o la API de Amazon Macie.

- En la consola, utilice las casillas Desde y Hasta para introducir los números más bajos y más altos del intervalo, respectivamente.
- Con la API, defina un intervalo de tiempo fijo añadiendo una condición que especifique el primer número del intervalo y, añada otra condición que especifique el último número del intervalo. Si lo hace, Macie utilizará el operador lógico AND para unir las condiciones. Para definir un intervalo numérico relativo, añada una condición que especifique el número más bajo o más alto del intervalo.

En la consola, los intervalos numéricos son inclusivos. Con la API, los intervalos numéricos pueden ser inclusivos o exclusivos, según el operador que elija.

Texto (cadena)

Especifica un único valor de texto (cadena) para un campo. La cadena se correlaciona con un valor predefinido o existente para un campo, por ejemplo, Alto para el campo Gravedad, el nombre de un bucket de S3 para el campo nombre del bucket de S3 o el identificador único de un trabajo de detección de datos confidenciales para el campo ID de trabajo.

Si especifica una sola cadena de texto, tenga en cuenta lo siguiente:

- Estos valores distinguen entre mayúsculas y minúsculas.
- No puede utilizar valores parciales ni caracteres comodín en los valores. Debe especificar un valor completo y válido para el campo.

Por ejemplo, para filtrar los resultados de un bucket de S3 denominado my-S3-bucket, introduzca **`my-S3-bucket`** como el valor del campo nombre del bucket de S3. Si introduce cualquier otro valor, como **`my-s3-bucket`** o **`my-S3`**, Macie no devolverá los resultados del bucket.

Para obtener una lista de valores válidos para cada campo, consulte Campos para filtrar los resultados.

Especificar varios valores para un campo

Con determinados campos y operadores, puede especificar varios valores para un campo. Si lo hace, Macie utiliza el operador lógico OR para unir los valores y evaluar los criterios del filtro. Esto significa que un resultado coincide con los criterios si tiene alguno de los valores del campo.

Por ejemplo, si añade una condición para incluir los resultados en los que el valor del campo Tipo de resultado es igual a SensitiveData:S3Object/Financial, SensitiveData:S3Object/Personal, Macie

devuelve resultados de datos confidenciales de los objetos de S3 que contienen solo información financiera y de los objetos de S3 que contienen solo información personal. En otras palabras, Macie excluye todos los resultados de políticas. Macie también excluye todos los resultados de datos confidenciales en el caso de los objetos que contienen otros tipos de datos confidenciales o varios tipos de datos confidenciales.

La excepción son las condiciones que utilizan el operador eqExactMatch. Para este operador, Macie usa el operador lógico AND para unir los valores y evaluar los criterios del filtro. Esto significa que un resultado coincide con los criterios solo si tiene todos los valores del campo y solo esos valores del campo. Para obtener más información sobre este operador, consulte Uso de operadores en condiciones.

La forma de especificar varios valores para un campo depende de si utiliza la API de Amazon Macie o la consola de Amazon Macie. Con la API, se utiliza una matriz que enumera los valores.

En la consola, normalmente se eligen los valores de una lista. Sin embargo, para algunos campos, debe agregar una condición distinta para cada valor. Por ejemplo, para incluir los resultados de los datos que Macie detectó mediante determinados identificadores de datos personalizados, haga lo siguiente:

1. Coloque el cursor en el cuadro Criterios del filtro y, a continuación, elija el campo Nombre del identificador de datos personalizado. Introduzca el nombre de un identificador de datos personalizado y, a continuación, seleccione Aplicar.
2. Repita el paso anterior para cada identificador de datos personalizado adicional que desee especificar para el filtro.

Para obtener una lista de los campos para los que necesita hacer esto, consulte Campos para filtrar los resultados.

Uso de operadores en condiciones

Puede utilizar los siguientes tipos de operadores en condiciones individuales.

Igual (eq)

> Coincide con (=) cualquier valor especificado para el campo. Puede usar el operador igual a con los siguientes tipos de valores: matriz de texto (cadenas), booleano, fecha/hora, número y texto (cadena).

Para muchos campos, puede usar este operador y especificar hasta 50 valores para el campo. Si lo hace, Macie utiliza el operador lógico OR para unir los valores. Esto significa que un resultado coincide con los criterios si tiene alguno de los valores especificados para el campo.

Por ejemplo:

- Para incluir resultados que notifiquen casos de información financiera, información personal o información tanto financiera como personal, añada una condición que utilice el campo Categoría de datos confidenciales y este operador, y especifique Información financiera e Información personal como valores del campo.
- Para incluir los resultados que notifiquen casos de números de tarjetas de crédito, direcciones postales o tanto números de tarjetas de crédito como direcciones postales, añada una condición al campo Tipo de detección de datos confidenciales, utilice este operador y especifique CREDIT_CARD_NUMBER y ADDRESScomo valores del campo.

Si usa la API de Amazon Macie para definir una condición que utilice este operador con un valor de fecha y hora, especifique el valor como una marca de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

Igual a coincidencia exacta (eqExactMatch)

Coincide exclusivamente con todos los valores especificados para el campo. Puede utilizar el operador igual a coincidencia exacta con un conjunto selecto de campos.

Si utiliza este operador y especifica varios valores para un campo, Macie utilizará el operador lógico AND para unir los valores. Esto significa que un resultado coincide con los criterios solo si tiene todos los valores especificados para el campo y solo esos valores para el campo. Puede especificar hasta 50 valores para el campo.

Por ejemplo:

- Para incluir los resultados que notifiquen casos de números de tarjetas de crédito y ningún otro tipo de datos confidenciales, añada una condición al campo Tipo de detección de datos confidenciales, utilice este operador y especifique CREDIT_CARD_NUMBER como único valor para el campo.
- Para incluir los resultados que notifiquen casos de números de tarjetas de crédito y direcciones postales (y ningún otro tipo de datos confidenciales), añada una condición al campo Tipo de detección de datos confidenciales, utilice este operador y especifique CREDIT_CARD_NUMBER y ADDRESS como valores para el campo.

Como Macie utiliza el operador lógico AND para unir los valores de un campo, no puede utilizar este operador junto con ningún otro operador para el mismo campo. En otras palabras, si utiliza el operador igual a coincidencia exacta con un campo en una condición, tendrá que usarlo en todas las demás condiciones que utlicen el mismo campo.

Al igual que otros operadores, puede usar el operador igual a coincidencia exacta en más de una condición de un filtro. Si lo hace, Macie utiliza el operador lógico AND para unir las condiciones y evaluar el filtro. Esto significa que un resultado coincide con los criterios del filtro solo si tiene todos los valores especificados por todas las condiciones del filtro.

Por ejemplo, para incluir los resultados que se crearon después de un tiempo determinado, notificar casos de números de tarjetas de crédito y no notificar ningún otro tipo de datos confidenciales, haga lo siguiente:

1. Agregue una condición que utilice el campo Creado en, utilice el operador mayor que y especifique la fecha y la hora de inicio para el filtro.
2. Agregue otra condición que utilice el campo Tipo de detección de datos confidenciales, utilice el operador igual a coincidencia exacta y especifique CREDIT_CARD_NUMBERcomo único valor para el campo.

Puede utilizar el operador igual a coincidencia exacta con los siguientes campos:

- Identificador de datos personalizado (`customDataIdentifiers.detections.arn`)
- Nombre de identificador de datos personalizado (`customDataIdentifiers.detections.name`)
- Tecla de etiqueta de bucket de S3 (`resourcesAffected.s3Bucket.tags.key`)
- Valor de la etiqueta del bucket de S3 (`resourcesAffected.s3Bucket.tags.value`)
- Clave de la etiqueta del objeto de S3 (`resourcesAffected.s3Object.tags.key`)
- Valor de la etiqueta de objeto de S3 (`resourcesAffected.s3Object.tags.value`)
- Tipo de detección de datos confidenciales (`sensitiveData.detections.type`)
- Categoría de datos confidenciales (`sensitiveData.category`)

En la lista anterior, el nombre entre paréntesis utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie.

Mayor que (gt)

Es mayor que (**>**) el valor especificado para el campo. Puede usar el operador mayor que con valores numéricos y de fecha y hora.

Por ejemplo, para incluir solo los resultados que notifiquen más de 90 casos de datos confidenciales en un objeto de S3, añada una condición que utilice el campo Recuento total de datos confidenciales y este operador, y especifique 90 como valor para el campo. Para hacerlo en la consola Amazon Macie, introduzca **91** en el cuadro Desde, no introduzca ningún valor en el cuadro Hasta y a continuación, seleccione Aplicar. Las comparaciones numéricas y basadas en el tiempo están incluidas en la consola.

Si utiliza la API de Amazon Macie para definir un intervalo de tiempo que utilice este operador, tendrá que especificar los valores de fecha y hora como marcas de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

Mayor o igual que (gte)

Es mayor o igual que (**>=**) el valor especificado para el campo. Puede utilizar el operador mayor o igual que con valores numéricos y de fecha y hora.

Por ejemplo, para incluir solo los resultados que notifiquen 90 o más casos de datos confidenciales en un objeto de S3, añada una condición que utilice el campo Recuento total de datos confidenciales y este operador, y especifique 90 como valor para el campo. Para hacerlo en la consola Amazon Macie, introduzca **90** en el cuadro Desde, no introduzca ningún valor en el cuadro Hasta y a continuación, seleccione Aplicar.

Si utiliza la API de Amazon Macie para definir un intervalo de tiempo que utilice este operador, tendrá que especificar los valores de fecha y hora como marcas de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

Menor que (lt)

Es menor que (**<**) el valor especificado para el campo. Puede usar el operador menor que con valores numéricos y de fecha y hora.

Por ejemplo, para incluir solo los resultados que notifiquen menos de 90 casos de datos confidenciales en un objeto de S3, añada una condición que utilice el campo Recuento total de datos confidenciales y este operador, y especifique 90 como valor para el campo. Para hacerlo en la consola Amazon Macie, introduzca **89** en el cuadro Hasta, no introduzca ningún valor en el cuadro Desde y a continuación, seleccione Aplicar. Las comparaciones numéricas y basadas en el tiempo están incluidas en la consola.

Si utiliza la API de Amazon Macie para definir un intervalo de tiempo que utilice este operador, tendrá que especificar los valores de fecha y hora como marcas de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

Menor o igual que (lte)

Es menor o igual que (**<=**) el valor especificado para el campo. Puede utilizar el operador menor o igual que con valores numéricos y de fecha y hora.

Por ejemplo, para incluir solo los resultados que notifiquen 90 o menos casos de datos confidenciales en un objeto de S3, añada una condición que utilice el campo Recuento total de datos confidenciales y este operador, y especifique 90 como valor para el campo. Para hacerlo en la consola Amazon Macie, introduzca **`90`** en el cuadro Hasta, no introduzca ningún valor en el cuadro Desde y a continuación, seleccione Aplicar.

Si utiliza la API de Amazon Macie para definir un intervalo de tiempo que utilice este operador, tendrá que especificar los valores de fecha y hora como marcas de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

No igual a (neq)

No coincide (≠) con ningún valor especificado para el campo. Puede usar el operador no igual a con los siguientes tipos de valores: matriz de texto (cadenas), booleano, fecha/hora, número y texto (cadena).

Para muchos campos, puede usar este operador y especificar hasta 50 valores para el campo. Si lo hace, Macie utiliza el operador lógico OR para unir los valores. Esto significa que un resultado coincide con los criterios si no tiene ninguno de los valores especificados para el campo.

Por ejemplo:

- Para excluir los resultados que notifiquen casos de información financiera, información personal o información tanto financiera como personal, añada una condición que utilice el campo Categoría de datos confidenciales y este operador, y especifique Información financiera e Información personal como valores del campo.
- Para excluir los resultados que notifiquen casos de números de tarjetas de crédito, añada una condición al campo Tipo de detección de datos confidenciales, utilice este operador y especifique CREDIT_CARD_NUMBER como valor del campo.
- Para excluir los resultados que indiquen casos de números de tarjetas de crédito, direcciones postales o tanto números de tarjetas de crédito como direcciones postales, añada una condición al campo Tipo de detección de datos confidenciales, utilice este operador y especifique CREDIT_CARD_NUMBER y ADDRESScomo valores del campo.

Si usa la API de Amazon Macie para definir una condición que utilice este operador con un valor de fecha y hora, especifique el valor como una marca de tiempo de Unix en milisegundos, por ejemplo, `1604616572653` para las 22:49:32 UTC del 5 de noviembre de 2020.

Crear y aplicar filtros a los resultados

Para identificar y centrarse en los resultados que tienen características específicas, puede filtrar los resultados en la consola de Amazon Macie y en las consultas que envíe mediante programación mediante la API de Amazon Macie. Al crear un filtro, se utilizan atributos específicos de los resultados para definir criterios que permitan incluir o excluir resultados de una vista o de los resultados de una consulta. Un atributo de resultado es un campo que almacena datos específicos de un resultado, como el tipo de resultado, la gravedad o el nombre del bucket de S3 afectado.

En Macie, un filtro consta de una o más condiciones. Cada condición, también denominada criterio, consta de tres partes:

- Un campo basado en atributos, como la Gravedad o el Tipo de resultado.
- Un operador, como igual o no igual.
- Uno o varios valores. El tipo y el número de valores dependen del campo y el operador que elija.

La forma en que defina y aplique las condiciones de filtrado depende de si utiliza la consola de Amazon Macie o la API de Amazon Macie.

Temas

Filtrar resultados en la consola de Amazon Macie

Si utiliza la consola de Amazon Macie para filtrar los resultados, Macie ofrece opciones que le ayudan a elegir campos, operadores y valores para condiciones individuales. Para acceder a estas opciones, utilice los ajustes de filtrado de las páginas de Resultados, como se muestra en la siguiente imagen.

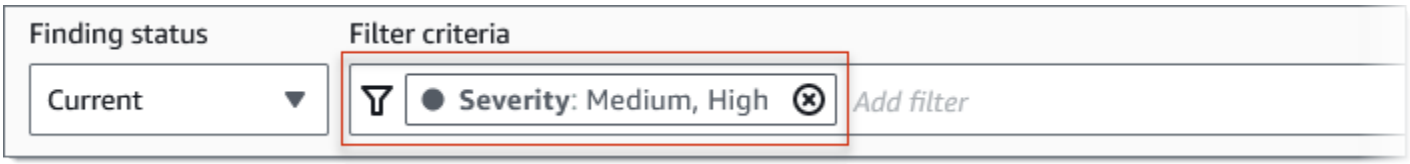
Mediante el menú Estado de los resultados, puede especificar si desea incluir los resultados que fueron suprimidos (archivados automáticamente) por una regla de supresión. Mediante el cuadro Criterios de filtrado, puede introducir las condiciones del filtrado.

Al colocar el cursor en el cuadro Criterios de filtrado, Macie muestra una lista de campos que puede utilizar en las condiciones de filtrado. Los campos están organizados por categorías lógicas. Por ejemplo, la categoría Campos comunes incluye los campos que se aplican a cualquier tipo de resultado y la categoría Classification fields (Campos de clasificación) incluye los campos que se aplican solo a los resultados de datos confidenciales. Los campos se ordenan alfabéticamente dentro de cada categoría.

Para añadir una condición, comience por elegir un campo de la lista. Para buscar un campo, navegue por la lista completa o introduzca parte del nombre del campo para reducir la lista de campos.

Dependiendo del campo que elija, Macie muestra diferentes opciones. Las opciones reflejan el tipo y la naturaleza del campo que elija. Por ejemplo, si selecciona el campo Gravedad, Macie mostrará una lista de valores entre los que elegir: Bajo, Medio y Alto. Si selecciona el campo Nombre del bucket S3, Macie mostrará un cuadro de texto en el que podrá introducir el nombre del bucket. Sea cual sea el campo que elija, Macie le guiará por los pasos necesarios para añadir una condición que incluya los ajustes necesarios para el campo.

Tras añadir una condición, Macie aplica los criterios de la condición y la añade a un token de filtro en el cuadro Criterios del filtro, como se muestra en la imagen siguiente.



En este ejemplo, la condición está configurada para incluir todos los resultados de gravedad media y alta, y excluir todos los resultados de gravedad baja. Devuelve los resultados en los que el valor del campo Gravedad es es igual a Medio o Alto.

> **Tip**
>
> En muchos campos, puede cambiar el operador de una condición de es igual a a no es igual a seleccionando el icono de igualdad (●) en el token de filtrado de la condición. Si lo hace, Macie cambia el operador a no es igual a y muestra el icono de no es igual a (⊘) en el token. Para volver a cambiar al operador es igual a, seleccione el icono no es igual a.

A medida que añada más condiciones, Macie aplicará sus criterios y los añadirá a los símbolos del cuadro Criterios del filtro. Puede consultar el cuadro en cualquier momento para determinar qué criterios has aplicado. Para eliminar una condición, seleccione el icono de eliminación de la condición (⊗) en el token para la condición.

Para filtrar resultados usando la consola

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Hallazgos).
3. (Opcional) Para repasar primero los resultados por un grupo lógico predefinido y revisarlos, seleccione Por bucket, Por tipo o Por trabajo en el panel de navegación (en Resultados). A continuación, seleccione un elemento en la tabla. En el panel de detalles, elija el enlace para el campo en el que se va a dinamizar.
4. (Opcional) Para mostrar los resultados que fueron suprimidos por una regla de supresión, cambie la configuración del Estado de filtrado. Seleccione Archivado para mostrar solo los resultados suprimidos o seleccione Todos para mostrar los resultados suprimidos y no suprimidos. Para ocultar los resultados suprimidos, seleccione Actual.
5. Para añadir una condición de filtrado:
   a. Coloque el cursor en el cuadro Criterios de filtrado y, a continuación, elija el campo que desee utilizar para la condición. Para obtener más información sobre los campos que puede utilizar, consulte Campos para filtrar los resultados.
   b. Introduzca el tipo de valor adecuado para el campo. Para obtener información sobre los distintos tipos de valores, consulte Especificar valores para los campos.

Matriz de texto (cadenas)

Para este tipo de valores, Macie suele proporcionar una lista de valores entre los que elegir. Si este es el caso, seleccione cada valor que desee usar en la condición.

Si Macie no proporciona una lista de valores, introduzca un valor completo y válido para el campo. Para especificar valores adicionales para el campo, elija Aplicar y, a continuación, añada otra condición para cada valor adicional.

Tenga en cuenta que los valores distinguen entre mayúsculas y minúsculas. Además, no puede utilizar valores parciales ni caracteres comodín en los valores. Por ejemplo, para filtrar los resultados de un bucket de S3 denominado my-S3-bucket, introduzca **`my-S3-bucket`** como el valor del campo nombre del bucket de S3. Si introduce cualquier otro valor, como **`my-s3-bucket`** o **`my-S3`**, Macie no devolverá los resultados del bucket.

Booleano

Para este tipo de valores, Macie proporciona una lista de valores entre los que elegir. Seleccione el valor que desea utilizar en la condición.

Fecha/hora (intervalos de tiempo)

Para este tipo de valor, utilice los cuadros Desde y Hasta para definir un intervalo de tiempo inclusivo:

- Para definir un intervalo de tiempo fijo, utilice los cuadros Desde y Hasta para especificar la primera fecha y hora y la última fecha y hora del intervalo, respectivamente.
- Para definir un intervalo de tiempo relativo que comience en una fecha y hora determinadas y termine en la hora actual, introduzca la fecha y la hora de inicio en los cuadros Desde y elimine el texto de los cuadros Hasta.
- Para definir un intervalo de tiempo relativo que termine en una fecha y hora determinadas, introduzca la fecha y la hora de término en los cuadros Hasta y elimine el texto de los cuadros Desde.

Tenga en cuenta que los valores de hora utilizan la notación de 24 horas. Si utiliza el selector de fechas para elegir fechas, puede refinar los valores introduciendo el texto directamente en los cuadros Desde y Hasta.

Número (rangos numéricos)

Para este tipo de valor, utilice los cuadros Desde y Hasta para introducir uno o más números enteros que definan un rango numérico inclusivo, fijo o relativo.

Valores de texto (cadena)

Para este tipo de valor, introduzca un valor completo y válido para el campo.

Tenga en cuenta que los valores distinguen entre mayúsculas y minúsculas. Además, no puede utilizar valores parciales ni caracteres comodín en los valores. Por ejemplo, para filtrar los resultados de un bucket de S3 denominado my-S3-bucket, introduzca **`my-S3-bucket`** como el valor del campo nombre del bucket de S3. Si introduce cualquier otro valor, como **`my-s3-bucket`** o **`my-S3`**, Macie no devolverá los resultados del bucket.

c. Cuando termine de añadir valores al campo, elija Aplicar. Macie aplica los criterios de filtro y añade la condición a un token de filtro en el cuadro de Criterios de filtro.

6. Repita el paso 5 para cada condición adicional que desee agregar.
7. Para eliminar una condición, pulse el icono de eliminación de la condición (⊗) en el token de filtrado para la condición.
8. Para cambiar una condición, elimine la condición pulsando el icono de eliminación de la condición (⊗) en el token de filtrado para la condición. A continuación, repita el paso 5 para añadir una condición con la configuración correcta.

Si desea volver a utilizar este conjunto de condiciones posteriormente, puede guardar el conjunto como una regla de filtrado. Para ello, seleccione Guardar regla en el cuadro Criterios del filtro. Ingrese un nombre y, opcionalmente, una descripción para la regla. Cuando termine, elija Save (Guardar).

Filtrar los resultados mediante programación con la API Amazon Macie

Para filtrar resultados mediante programación, especifique los criterios de filtrado en las consultas que envíe mediante la operación ListFindings o GetFindingStatistics de la API de Amazon Macie. La operación ListFindings devuelve una matriz de identificadores de resultados, un identificador por cada resultado que coincida con los criterios de filtrado. La operación GetFindingStatistics devuelve

datos estadísticos agregados sobre todos los resultados que coinciden con los criterios de filtro, agrupados por un campo que especifique en la solicitud.

Tenga en cuenta que las operaciones ListFindings y GetFindingStatistics son diferentes de las operaciones que se utilizan para suprimir los resultados. A diferencia de las operaciones de supresión, que también especifican los criterios de filtrado, las operaciones ListFindings y GetFindingStatistics solo consultan los datos de los resultados. No llevan a cabo ninguna acción sobre los resultados que coinciden con los criterios de filtro. Para suprimir los resultados, utilice la operación CreateFindingsFilter de la API de Amazon Macie.

Para especificar los criterios de filtrado en una consulta, incluya una asignación de las condiciones del filtrado en la solicitud. Para cada condición debe especificar un campo, un operador y uno o varios valores para el campo. El tipo y el número de valores dependen del campo y el operador que elija. Para obtener información sobre los campos, los operadores y los tipos de valores que puede usar en una condición, consulte Campos para filtrar los resultados, Uso de operadores en condiciones y Especificar valores para los campos.

En los siguientes ejemplos, se muestra cómo especificar los criterios de filtrado en las consultas que se envían mediante AWS Command Line Interface(AWS CLI). También puede realizar esto utilizando una versión actual de otra herramienta de línea de comandos AWS o un SDK AWS, o enviando solicitudes HTTPS directamente a Macie. Para obtener más información sobre las herramientas y los SDK de AWS, consulte Herramientas para crear en .AWS

Ejemplos

- Ejemplo 1: filtrado de los resultados en función de la gravedad
- Ejemplo 2: filtrado de los resultados en función de la categoría de datos confidenciales
- Ejemplo 3: Filtrado de los resultados en función de un intervalo de tiempo fijo
- Ejemplo 4: Filtrado de los resultados en función del estado de supresión
- Ejemplo 5: Filtrado de los resultados en función de varios campos y tipos de valores

Los ejemplos utilizan el comando list-findings. Si un ejemplo se ejecuta correctamente, Macie devuelve una matriz `findingIds`. La matriz indica el identificador único de cada resultado que coincide con los criterios de filtro, como se muestra en el siguiente ejemplo.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
```

```
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Si ningún resultado coincide con los criterios del filtro, Macie devuelve una matriz `findingIds` vacía.

```
{
    "findingIds": []
}
```

Ejemplo 1: filtrado de los resultados en función de la gravedad

En este ejemplo, se utiliza el comando list-findings para recuperar los identificadores de búsqueda de todos los resultados de gravedad alta y media del presente Región de AWS.

Para Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

Donde:

- *severity.description* especifica el nombre JSON del campo Gravedad.
- *eq* especifica el operador es igual a.
- *Alto* y *Medio* son una matriz de valores enumerados para el campo Gravedad.

Ejemplo 2: filtrado de los resultados en función de la categoría de datos confidenciales

En este ejemplo, se utiliza el comando list-findings para recuperar los identificadores de resultados de todos los resultados de datos confidenciales encontrados en la región actual y para informar sobre la aparición de información financiera (y no de otras categorías de datos confidenciales) en los objetos de S3.

Para Linux, macOS o Unix, utilice el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Para Microsoft Windows, utilice el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

Donde:

- *ClassificationDetails.result.SensitiveData.category* especifica el nombre en JSON del campo Categoría de datos confidenciales.
- *eqExactMatch* especifica el operador es igual a coincidencia exacta.
- *FINANCIAL_INFORMATION* es un valor enumerado para el campo Categoría de datos confidenciales.

Ejemplo 3: Filtrado de los resultados en función de un intervalo de tiempo fijo

En este ejemplo, se utiliza el comando list-findings para recuperar los identificadores de resultados de todos los resultados que se encuentren en la región actual y que se hayan creado entre las 07:00 UTC del 5 de octubre de 2020 y las 07:00 UTC del 5 de noviembre de 2020 (ambos inclusive).

Para Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

Donde:

- *CreatedAt* especifica el nombre JSON del campo Creado en.
- *gte* especifica el operador es mayor o igual a.
- *1601881200000* es la primera fecha y hora (como marca de tiempo de Unix en milisegundos) del intervalo de tiempo.
- *gte* especifica el operador es menor o igual a.
- *1604559600000* es la última fecha y hora (como marca de tiempo de Unix en milisegundos) del intervalo de tiempo.

Ejemplo 4: Filtrado de los resultados en función del estado de supresión

En este ejemplo, se utiliza el comando list-findings para recuperar los identificadores de resultados de todos los resultados que se encuentran en la región actual y que fueron suprimidos (archivados automáticamente) por una regla de supresión.

Para Linux, macOS o Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Para Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

Donde:

- *archived* especifica el nombre JSON del campo Archivado.
- *eq* especifica el operador es igual a.
- *true* es un valor booleano para el campo Archivado.

Ejemplo 5: Filtrado de los resultados en función de varios campos y tipos de valores

En este ejemplo, se utiliza el comando list-findings para recuperar los identificadores de resultados de todos los resultados de datos confidenciales que se encuentren en la región actual y que cumplan los siguientes criterios: se crearon entre las 07:00 UTC del 5 de octubre de 2020 y las 07:00

UTC del 5 de noviembre de 2020 (exclusivamente); notifican la aparición de datos financieros y ninguna otra categoría de datos confidenciales en objetos de S3; y no se suprimieron (archivaron automáticamente) mediante una regla de supresión.

Para Linux, macOS o Unix, utilice el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Para Microsoft Windows, utilice el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

Donde:

- *createdAt* especifica el nombre JSON del campo Creado en, y:
  - *gt* especifica el operador es mayor o igual a.
  - *1601881200000* es la primera fecha y hora (como marca de tiempo de Unix en milisegundos) del intervalo de tiempo.
  - *lt* especifica el operador es menor o igual a.
  - *1604559600000* es la última fecha y hora (como marca de tiempo de Unix en milisegundos) del intervalo de tiempo.
- *ClassificationDetails.result.sensitiveData.category* especifica el nombre en JSON del campo Categoría de datos confidenciales, y
  - *eqExactMatch* especifica el operador es igual a coincidencia exacta.
  - *FINANCIAL_INFORMATION* es un valor enumerado para el campo.
- *archivado* especifica el nombre JSON del campo Archivado, y:
  - *eq* especifica el operador es igual a.
  - *false* es un valor booleano para el campo.

Creación y administración de reglas de filtrado para los resultados

Una regla del filtro es un conjunto de criterios de filtrado que usted crea y guarda para volver a usarlos al revisar los resultados en la consola de Amazon Macie. Las reglas de filtrado pueden ayudarle a realizar un análisis coherente de los resultados que tienen características específicas. Por ejemplo, puede crear una regla de filtrado para analizar todos los resultados de políticas de alta gravedad para los buckets de S3 que contienen objetos no cifrados, y otra regla de filtrado para analizar todos los resultados de datos confidenciales de alta gravedad que informen sobre tipos específicos de datos confidenciales.

Tenga en cuenta que las reglas de filtrado son diferentes de las reglas de supresión. Una regla de supresión es un conjunto de criterios de filtro que se crean y guardan para archivar automáticamente los resultados que coincidan con los criterios de la regla. Aunque ambos tipos de reglas almacenan y aplican criterios de filtrado, una regla de filtrado no realiza ninguna acción en relación con los resultados que coinciden con los criterios de la regla. En su lugar, una regla de filtrado solo determina qué resultados aparecen en la consola después de aplicar la regla. Para obtener más información sobre las reglas de supresión, consulte Supresión de hallazgos.

Para crear y gestionar reglas de filtrado, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. En los siguientes temas se explica cómo hacerlo. En el caso de la API, los temas incluyen ejemplos de cómo realizar estas tareas mediante el AWS Command Line Interface (AWS CLI). También puede realizar estas tareas utilizando una versión actual de otra herramienta de línea de comandos AWS o un SDK AWS, o enviando solicitudes HTTPS directamente a Macie. Para obtener más información sobre las herramientas y los SDK de AWS, consulte Herramientas para crear en .AWS

Temas

Creación de reglas de filtrado

Al crear una regla de filtrado, se especifican los criterios de filtrado, un nombre y, si lo desea, una descripción de la regla. Puede crear una regla de filtrado mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

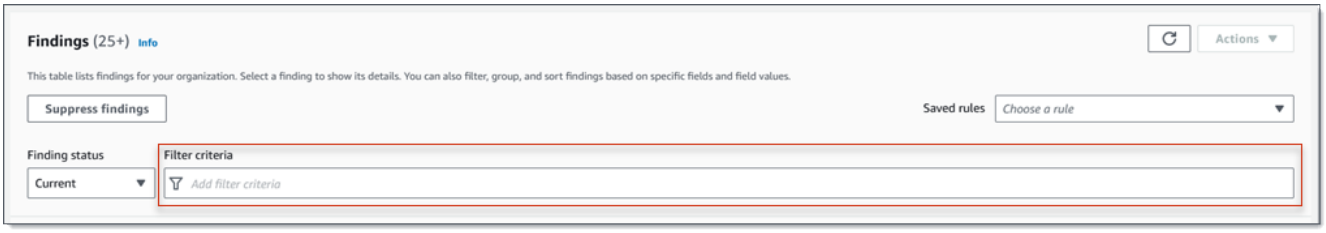
Siga estos pasos para crear una regla de filtrado mediante la consola de Amazon Macie.

Para crear una regla de filtrado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Resultados).

> **Tip**
>
> Para usar una regla de filtrado existente como punto de partida, elija la regla de la lista de Saved rules (Reglas guardadas).
> También puede simplificar la creación de una regla primero centrándose y profundizando en los resultados por un grupo lógico predefinido. Si lo hace, Macie crea y aplica automáticamente las condiciones de filtrado adecuadas, lo que puede ser un punto de partida útil para crear una regla. Para ello, elija Por bucket, Por tipo o Por trabajo en el panel de navegación (en Resultados) y, a continuación, elija un elemento de la tabla. En el panel de detalles, elija el enlace para el campo en el que se va a dinamizar.

3. En el cuadro Criterios del filtro, añada condiciones que definan los criterios de filtrado de la regla.



Para aprender cómo agregar condiciones de filtrado, consulte Crear y aplicar filtros a los resultados.

4. Cuando termine de definir los criterios de filtrado para la regla, seleccione Guardar regla en el cuadro Criterios del filtro.

5. Bajo Regla de filtrado ingrese un nombre y, opcionalmente, una descripción de la regla.
6. Seleccione Save (Guardar).

API

Para crear una regla de filtrado mediante programación, utilice la operación CreateFindingsFilter de la API de Amazon Macie y especifique los valores adecuados para los parámetros necesarios:

- Para el parámetro `action`, especifique `NOOP` para asegurarse de que Macie no suprima (archive automáticamente) los resultados que coincidan con los criterios de la regla.
- Para el parámetro `criterion`, especifique un mapa de condiciones que defina los criterios de filtrado de la regla.

  En el mapa, cada condición debe especificar un campo, un operador y uno o varios valores para el campo. El tipo y el número de valores dependen del campo y el operador que elija. Para obtener información sobre los campos, los operadores y los tipos de valores que puede usar en una condición, consulte Campos para filtrar los resultados, Uso de operadores en condiciones y Especificar valores para los campos.

Para crear una regla de filtrado mediante AWS CLI, ejecute el comando create-findings-filter y especifique los valores adecuados para los parámetros necesarios. En los siguientes ejemplos, se crea una regla de filtrado que devuelve todos los datos confidenciales encontrados en el Región de AWS actual y muestra las apariciones de información personal (y no de otras categorías de datos confidenciales) en los objetos de S3.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de continuación de línea de barra invertida (\) para mejorar la legibilidad.

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
```

```
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

Donde:

- *my_filter_rule* es el nombre personalizado de la regla.
- `criterion` es un mapa de las condiciones de filtro de la regla:
  - *ClassificationDetails.result.SensitiveData.category* es el nombre en JSON del campo categoría de datos confidenciales.
  - *eqExactMatch* especifica el operador es igual a coincidencia exacta.
  - *PERSONAL_INFORMATION* es un valor enumerado para el campo Categoría de datos confidenciales.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Dónde `arn` es el nombre de recurso de Amazon (ARN) de la regla de filtrado que se creó y `id` es el identificador único de la regla.

Para ver ejemplos adicionales de criterios de filtrado, consulte Filtrar los resultados mediante programación con la API Amazon Macie.

Aplicar reglas de filtrado

Cuando aplica una regla de filtrado, Amazon Macie utiliza los criterios de la regla para determinar qué resultados debe incluir o excluir de la vista de resultados en la consola. Macie también muestra los criterios para ayudarle a determinar qué criterios ha aplicado.

Tenga en cuenta que las reglas de filtrado están diseñadas para usarse con la consola Amazon Macie. No puede utilizarlos directamente en consultas que envíe mediante programación a través de la API de Amazon Macie. Sin embargo, si utiliza la API para consultar los resultados, puede recuperar los criterios de filtrado de una regla mediante la operación GetFindingsFilter. A continuación, puede añadir los criterios a la consulta. Para obtener información sobre cómo especificar los criterios de filtrado en una consulta, consulte Crear y aplicar filtros a los resultados.

Siga estos pasos para filtrar los resultados en la consola mediante la aplicación de una regla de filtrado.

Para aplicar una regla de filtrado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Resultados).
3. En la lista Reglas guardadas, elija la regla de filtrado que desea aplicar. Macie aplica los criterios de la regla y los muestra en el cuadro Criterios del filtro.
4. (Opcional) Para afinar los criterios, utilice el cuadro Criterios del filtro si desea añadir o eliminar condiciones de filtrado. Si lo hace, los cambios no afectarán a la configuración de la regla. Macie no guardará ninguno de sus cambios a menos que los guarde explícitamente como una nueva regla.
5. Para aplicar una regla de filtrado diferente, repita el paso 3.

Tras aplicar una regla de filtrado, puede eliminar rápidamente todos sus criterios de filtrado de la vista seleccionando la X en el cuadro Criterios del filtro.

Cambiar las reglas de filtrado

Puede cambiar la configuración de una regla de filtrado en cualquier momento mediante la consola de Amazon Macie o la API de Amazon Macie. También puede asignar y administrar etiquetas para la regla.

Una Etiqueta es una etiqueta que se define y se asigna a determinados tipos de recursos de AWS. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

Console

Para cambiar la configuración para una regla de filtrado existente mediante la consola de Amazon Macie, siga los pasos siguientes.

Para cambiar una regla de filtrado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Resultados).
3. En la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla de filtrado que desee cambiar.
4. Realice uno de los siguientes procedimientos:
   - Para cambiar los criterios de filtrado de la regla, utilice el cuadro Criterios del filtro para introducir las condiciones de los criterios que desee. Para saber cómo hacerlo, consulte Crear y aplicar filtros a los resultados.
   - Para cambiar el nombre de la regla, introduzca un nombre nuevo en el cuadro Nombre bajo la Regla de filtrado.
   - Para cambiar la descripción de la regla, introduzca una nueva descripción en el cuadro Descripción bajo la Regla del filtro.
   - Para asignar, revisar o editar las etiquetas de la regla, seleccione Administrar etiquetas bajo la Regla del filtro. A continuación, revise y cambie las etiquetas según sea necesario. Una regla puede tener hasta 50 etiquetas.
5. Cuando termine de realizar los cambios, seleccione Save (Guardar).

API

Para cambiar una regla de filtrado mediante programación, utilice la operación UpdateFindingsFilter de la API de Amazon Macie. Cuando envíe su solicitud, utilice los

parámetros admitidos con el fin de especificar un nuevo valor para cada configuración que desee cambiar.

Para el parámetro `id`, especifique el identificador único de la regla que desee cambiar. Puede obtener este identificador mediante la operación ListFindingsFilter para recuperar una lista de las reglas de filtrado y supresión de su cuenta. Si utiliza AWS CLI, ejecute el comando list-findings-filters para recuperar esta lista.

Para cambiar una regla de filtrado mediante AWS CLI, ejecute el comando update-findings-filter, utilice los parámetros compatibles y especifique un nuevo valor para cada configuración que desee cambiar. Por ejemplo, el siguiente comando cambia el nombre de una regla de filtrado existente.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

Donde:

- *9b2b4508-aa2f-4940-b347-d1451example* es el identificador único de la regla.
- *personal_information_only* es el nuevo nombre de la regla.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Donde `arn` es el nombre de recurso de Amazon (ARN) de la regla que se ha modificado y `id` es el identificador único de la regla.

Del mismo modo, en el siguiente ejemplo se convierte una regla de supresión en una regla de filtrado cambiando el valor del parámetro `action` de `ARCHIVE` a `NOOP`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

Donde:

- *8a1c3508-aa2f-4940-b347-d1451example* es el identificador único de la regla.
- *NOOP* es la nueva acción que Macie debe realizar en función de los resultados que coincidan con los criterios de la regla: no realizar ninguna acción (no suprimir los resultados).

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Donde `arn` es el nombre de recurso de Amazon (ARN) de la regla que se ha modificado y `id` es el identificador único de la regla.

Eliminar reglas de filtrado

Puede eliminar una regla de filtrado en cualquier momento mediante la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para eliminar una regla de filtrado mediante la consola de Amazon Macie.

Para eliminar una regla de filtrado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Resultados).
3. En la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla de filtrado que desee eliminar.
4. En Regla del filtro, seleccione Eliminar.

API

Para eliminar una regla de filtrado mediante programación, utilice la operación DeleteFindingsFilter de la API de Amazon Macie. Para el parámetro `id`, especifique el

identificador único de la regla de filtrado que desea eliminar. Puede obtener este identificador mediante la operación ListFindingsFilter para recuperar una lista de las reglas de filtrado y supresión de su cuenta. Si utiliza AWS CLI, ejecute el comando list-findings-filters para recuperar esta lista.

Para eliminar una regla de filtrado mediante AWS CLI, ejecute el comando delete-findings-filter. Por ejemplo:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

Donde *9b2b4508-aa2f-4940-b347-d1451example* es el identificador único de la regla de filtrado a eliminar.

Si el comando se ejecuta correctamente, Macie devuelve una respuesta HTTP 200 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Campos para filtrar los resultados

Para ayudarlo a analizar los resultados de manera más eficiente, la consola de Amazon Macie y la API de Amazon Macie proporcionan acceso a varios conjuntos de campos para filtrar los resultados:

- Campos comunes: estos campos almacenan datos que se aplican a cualquier tipo de resultado. Se correlacionan con los atributos comunes de los resultados, como la gravedad, el tipo de resultado y el identificador de búsqueda.
- Campos de recursos afectados: estos campos almacenan datos sobre los recursos a los que se aplica un resultado, como el nombre, las etiquetas y la configuración de cifrado de un bucket u objeto de S3 afectado.
- Campos de política: estos campos almacenan datos específicos de los resultados de la política, como la acción que produjo un resultado y la entidad que realizó la acción.
- Campos de clasificación de datos confidenciales: estos campos almacenan datos específicos de los resultados de datos confidenciales, como la categoría y los tipos de datos confidenciales que Macie encontró en un objeto S3 afectado.

Un filtro puede usar una combinación de campos de cualquiera de los conjuntos anteriores.

En los temas de esta sección, se enumeran y describen los campos individuales que puede usar para filtrar los resultados. Para obtener más información sobre estos campos, incluida cualquier relación entre los campos, consulte Resultados en la referencia de la API de Amazon Macie.

Temas

Campos comunes

En la siguiente tabla se enumeran y describen los campos que puede utilizar para filtrar los resultados en función de los atributos de resultados comunes. Estos campos almacenan datos que se aplican a cualquier tipo de resultado.

En la tabla, la columna Campo indica el nombre del campo de la consola de Amazon Macie. La columna campo JSON utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie. La columna Descripción proporciona una breve descripción de los datos que almacena el campo e indica los requisitos para los valores de filtrado. La tabla se ordena alfabéticamente de manera ascendente por campo y, a continuación, por campo JSON.

Campo	Campo JSON	Descripción
Identificador* de cuenta	`accountId`	El identificador único para el Cuenta de AWS al que se aplica el resultado. Normalmente esta es la cuenta propietaria del recurso afectado.
—	`archived`	Un valor booleano que especifica si una regla de supresión suprimió (archivó automáticamente) el resultado .

Campo	Campo JSON	Descripción
		Para usar este campo en un filtro de la consola, seleccione una opción en el menú Estado del resultado: Archivado (solo suprimido), Actual (solo sin suprimir) o Todos (tanto suprimido como no suprimido).
Categoría	`category`	La categoría del resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. En la API, los valores válidos son: `CLASSIFICATION`, para un resultado de datos confidenciales y, `POLICY`, para un resultado de políticas.
—	`count`	El número total de ocurrencias del resultado. Para los resultados de datos confidenciales, este valor es siempre 1. Todos los resultados de datos confidenciales se consideran únicos. Este campo no está disponible como opción de filtrado en la consola. Con la API, puede usar este campo para definir un rango numérico para un filtrado.

Campo	Campo JSON	Descripción
Creado en	`createdAt`	La fecha y la hora en que Macie creó el resultado. Puede usar este campo para definir un rango de tiempo para un filtrado.
Identificador* del resultado	`id`	Un identificador único para el resultado. Se trata de una cadena aleatoria que Macie genera y asigna a un resultado cuando lo crea.
Tipo de resultado*	`type`	El tipo de resultado, por ejemplo, `SensitiveData:S3Object/Personal` o `Policy:IAMUser/S3BucketPublic`. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos en la API, consulte FindingTypela referencia de la API de Amazon Macie.
Región	`region`	El Región de AWS donde Macie creó el resultado, por ejemplo, `us-east-1` o `ca-central-1`.

Campo	Campo JSON	Descripción
Muestra	`sample`	Un valor booleano que especifica si el resultado es un resultado de muestra. Un resultado de muestra es un resultado que utiliza datos de ejemplo y valores de marcador de posición para demostrar lo que puede contener un resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro.
Gravedad	`severity.description`	La representación cualitativa de la gravedad del resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. En la API, los valores válidos son `Low`, `Medium` y `High`.

Campo	Campo JSON	Descripción
Actualizado a las	`updatedAt`	La fecha y hora de la última actualización del resultado. En el caso de los resultados de datos confidenciales, este valor es el mismo que el del campo Creado a las. Todos los resultados de datos confidenciales se consideran nuevos (únicos). Puede usar este campo para definir un rango de tiempo para un filtrado.

* Para especificar varios valores para este campo en la consola, añada una condición que utilice el campo y especifique un valor distinto para el filtro y, a continuación, repita ese paso para cada valor adicional. Para hacerlo con la API, utilice una matriz que muestre los valores que se van a utilizar para el filtrado.

Campos de recursos afectados

En los temas siguientes se enumeran y describen los campos que puede usar para filtrar los resultados en función del recurso al que se aplica un resultado. Los temas están organizados por tipo de recurso.

Temas

- Bucket de S3
- Objeto de S3

Bucket de S3

En la siguiente tabla se enumeran y describen los campos que puede usar para filtrar los resultados en función de las características del bucket de S3 al que se aplica un resultado.

En la tabla, la columna Campo indica el nombre del campo de la consola de Amazon Macie. La columna campo JSON utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie. (Los nombres de campo JSON más largos utilizan la secuencia de caracteres de nueva línea (\n) para mejorar la legibilidad). La columna Descripción proporciona una breve descripción de los datos que almacena el campo e indica los requisitos para los valores de filtrado. La tabla se ordena alfabéticamente de manera ascendente por campo y, a continuación, por campo JSON.

Campo	Campo JSON	Descripción
—	`resourcesAffected.s3Bucket.createdAt`	La fecha y la hora en que se creó el bucket afectado o los cambios más recientes, como las modificaciones en la política del bucket afectado, se realizaron por última vez en el bucket afectado. Este campo no está disponible como opción de filtrado en la consola. Con la API, puedes usar este campo para definir un rango de tiempo para un filtrado.
Cifrado predeterminado para los buckets de S3	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	El algoritmo de cifrado del lado del servidor que se utiliza de forma predeterminada para cifrar los objetos que se añaden al depósito afectado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos para

Campo	Campo JSON	Descripción
		la API, consulte la referencia EncryptionTypede la API de Amazon Macie.
Identificadores de clave KMS de cifrado de buckets de S3*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	El Nombre de recurso de Amazon (ARN) o el identificador único (Identificador de clave) del AWS KMS key que se utiliza de forma predeterminada para cifrar los objetos que se añaden al bucket afectado.
La política de buckets de S3 exige el cifrado de buckets	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	Especifica si la política de bucket del bucket afectado requiere el cifrado de los objetos en el servidor cuando se añaden objetos al bucket. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos en la API, consulte S3Bucket en la referencia de la API de Amazon Macie.
Nombre del bucket de S3*	`resourcesAffected.s3Bucket.name`	El nombre completo del bucket afectado.

Campo	Campo JSON	Descripción
Nombre visible del propietario del bucket de S3*	`resourcesAffected.s3Bucket.owner.displayName`	El nombre para mostrar del usuario AWS propietario del bucket afectado.
Permiso de acceso público al bucket S3	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	Especifica si el bucket afectado es de acceso público en función de una combinación de ajustes de permisos que se aplican al bucket. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos para la API, consulte la referencia BucketPublicAccessde la API de Amazon Macie.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		Un valor booleano que especifica si Amazon S3 bloquea las listas de control de acceso público (ACL) para el bucket afectado y los objetos del bucket. Se trata de una configuración de bloqueo de acceso público a nivel de cuenta para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Un valor booleano que especifica si Amazon S3 bloquea las políticas de buckets públicos para el bucket afectado. Se trata de una configuración de bloqueo de acceso público a nivel de cuenta para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Un valor booleano que especifica si Amazon S3 omite las ACL públicas para el bucket afectado y los objetos en el bucket. Se trata de una configuración de bloqueo de acceso público a nivel de cuenta para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Un valor booleano que especifica si Amazon S3 restringe las políticas de buckets públicos para el bucket afectado. Se trata de una configuración de bloqueo de acceso público a nivel de cuenta para el bucket. Este campo no está disponible como opción de filtrado en la consola.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	Un valor booleano que especifica si las ACL a nivel de bucket del bucket afectado otorgan al público en general permisos de acceso de lectura para el bucket. Este campo no está disponible como opción de filtrado en la consola.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	Un valor booleano que especifica si las ACL a nivel de bucket del bucket afectado otorga al público en general permisos de acceso de escritura para el bucket. Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicAcls`
		Un valor booleano que especifica si Amazon S3 bloquea las ACL públicas para el bucket afectado y los objetos en el bucket. Se trata de una configuración de bloqueo de acceso público a nivel de bucket para un bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Un valor booleano que especifica si Amazon S3 bloquea las políticas de buckets públicos para el bucket afectado. Se trata de una configuración de bloqueo de acceso público a nivel de bucket para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Un valor booleano que especifica si Amazon S3 omite las ACL públicas para el bucket afectado y los objetos en el bucket. Se trata de una configuración de bloqueo de acceso público a nivel de bucket para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`
		Un valor booleano que especifica si Amazon S3 restringe las políticas de buckets públicos para el bucket afectado. Se trata de una configuración de bloqueo de acceso público a nivel de bucket para el bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`
		Un valor booleano que especifica si la política del bucket afectado permite que el público en general tenga acceso de lectura al bucket.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	Un valor booleano que especifica si la política del bucket afectado permite que el público en general tenga acceso de escritura al bucket. Este campo no está disponible como opción de filtrado en la consola.
Clave de la etiqueta del bucket de S3*	`resourcesAffected.s3Bucket.tags.key`	Una clave de etiqueta asociada al bucket afectado.
Valor de la etiqueta del bucket de S3*	`resourcesAffected.s3Bucket.tags.value`	Un valor de etiqueta asociado al bucket afectado.

* Para especificar varios valores para este campo en la consola, añada una condición que utilice el campo y especifique un valor distinto para el filtro y, a continuación, repita ese paso para cada valor adicional. Para hacerlo con la API, utilice una matriz que muestre los valores que se van a utilizar para el filtrado.

Objeto de S3

En la siguiente tabla se enumeran y describen los campos que se pueden usar para filtrar los resultados en función de las características del objeto de S3 al que se aplica un resultado.

En la tabla, la columna Campo indica el nombre del campo de la consola de Amazon Macie. La columna campo JSON utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie. La columna Descripción proporciona una breve descripción de los datos que almacena el campo e indica los requisitos para los valores de filtrado. La tabla se ordena alfabéticamente de manera ascendente por campo y, a continuación, por campo JSON.

Campo	Campo JSON	Descripción

Campo	Campo JSON	Descripción
Identificador de clave KMS de cifrado del objeto de S3*	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	El Nombre de recurso de Amazon (ARN) o el identificador único (Identificador de clave) del AWS KMS key que se utiliza para cifrar el objeto afectado.
Tipo de cifrado de objetos de S3	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	El algoritmo de cifrado del lado del servidor que se utilizó para cifrar el objeto afectado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos para la API, consulte la referencia EncryptionTypede la API de Amazon Macie.
—	`resourcesAffected.s3Object.extension`	La extensión del nombre de archivo del objeto afectado. En el caso de los objetos que no tienen una extensión de nombre de archivo, especifíque "" como valor para el filtrado. Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
—	`resourcesAffected.s3Object.lastModified`	La fecha y la hora en que se creó o modificó por última vez el objeto afectado, lo que sea más reciente. Este campo no está disponible como opción de filtrado en la consola. Con la API, puedes usar este campo para definir un rango de tiempo para un filtrado.
Una clave del objeto de S3*	`resourcesAffected.s3Object.key`	El nombre completo (clave) del objeto afectado, incluido el prefijo del objeto, si corresponde.
—	`resourcesAffected.s3Object.path`	La ruta completa al objeto afectado, incluidos el nombre del bucket afectado y el nombre del objeto (clave). Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
Acceso público al objeto de S3	`resourcesAffected.s3Object.publicAccess`	Un valor booleano que especifica si el bucket afectado es de acceso público en función de una combinación de ajustes de permisos que se aplican al objeto. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro.
Clave de etiqueta del objeto de S3*	`resourcesAffected.s3Object.tags.key`	Una clave de etiqueta asociada al objeto afectado.
Valor de etiqueta del objeto de S3*	`resourcesAffected.s3Object.tags.value`	Un valor de etiqueta asociado al objetob afectado.

* Para especificar varios valores para este campo en la consola, añada una condición que utilice el campo y especifique un valor distinto para el filtro y, a continuación, repita ese paso para cada valor adicional. Para hacerlo con la API, utilice una matriz que muestre los valores que se van a utilizar para el filtrado.

Campos de política

En la siguiente tabla, se enumeran y describen los campos que puede usar para filtrar los resultados de políticas. Estos campos almacenan datos específicos de los resultados de las políticas.

En la tabla, la columna Campo indica el nombre del campo de la consola de Amazon Macie. La columna campo JSON utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie. (Los nombres de campo JSON más largos utilizan la secuencia de caracteres de nueva línea (\n) para mejorar la legibilidad). La columna Descripción proporciona una breve descripción de los datos que almacena el campo

e indica los requisitos para los valores de filtrado. La tabla se ordena alfabéticamente de manera ascendente por campo y, a continuación, por campo JSON.

Campo	Campo JSON	Descripción
Tipo de acción	`policyDetails.action.actionType`	El tipo de acción que produjo el resultado. El único valor válido para este campo es `AWS_API_CALL` .
Nombre de llamado de la API*	`policyDetails.action.apiCallDetails.api`	El nombre de la operación que se invocó más recientemente y produjo el resultado, por ejemplo, `PutBucketPublicAccessBlock` .
Nombre de servicio de la API*	`policyDetails.action.apiCallDetails.apiServiceName`	La URL del Servicio de AWS que proporciona la operación que se invocó y produjo el resultado, por ejemplo, `s3.amazonaws.com` .
—	`policyDetails.action.apiCallDetails.firstSeen`	La primera fecha y hora en que se invocó una operación y se produjo el resultado. Este campo no está disponible como opción de filtrado en la consola. Con la API, puedes usar este campo para definir un rango de tiempo para un filtrado.
—	`policyDetails.action.apiCallDetails.lastSeen`	La fecha y hora más recientes en las que se invocó la operación especificada (nombre de llamado de la

Campo	Campo JSON	Descripción
		API o `api`) y se produjo el resultado. Este campo no está disponibl e como opción de filtrado en la consola. Con la API, puedes usar este campo para definir un rango de tiempo para un filtrado.
—	`policyDetails.acto r.domainDetails.do mainName`	El nombre de dominio del dispositivo que se utilizó para realizar la acción. Este campo no está disponibl e como opción de filtrado en la consola.
IP de la ciudad*	`policyDetails.acto r.ipAddressDetails .ipCity.name`	El nombre de la ciudad de origen de la dirección IP del dispositivo que se utilizó para realizar la acción.
IP del país*	`policyDetails.acto r.ipAddressDetails .ipCountry.name`	El nombre del país de origen de la dirección IP del dispositi vo que se utilizó para realizar la acción, por ejemplo, `United States`.

Campo	Campo JSON	Descripción
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	El número de sistema autónomo (ASN) del sistema autónomo que incluía la dirección IP del dispositivo que se utilizó para realizar la acción. Este campo no está disponible como opción de filtrado en la consola.
ASN org propietario de la IP*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	El identificador de la organización asociado a la ASN del sistema autónomo que incluía la dirección IP del dispositivo que se utilizó para realizar la acción.
ISP propietario de la IP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	El nombre del proveedor de servicios de Internet (ISP) propietario de la dirección IP del dispositivo que se utilizó para realizar la acción.
Dirección IP V4*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	La dirección del Protocolo de Internet versión 4 (IPv4) del dispositivo que se utilizó para realizar la acción.

Campo	Campo JSON	Descripción
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación de `AssumeRole` de la API AWS STS, el identificador de clave de acceso AWS que identifica las credenciales. Este campo no está disponible como opción de filtrado en la consola.
Identificador de cuenta del rol asumido de identidad del usuario*	`policyDetails.actor.userIdentity.assumedRole.accountId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación de `AssumeRole` de la API AWS STS, el identificador único para el Cuenta de AWS propietario de la entidad que se utilizó para obtener las credenciales.
Identificador principal del rol asumido de identidad del usuario*	`policyDetails.actor.userIdentity.assumedRole.principalId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `AssumeRole` de la API de AWS STS, el identificador único de la entidad que se utilizó para obtener las credenciales.

Campo	Campo JSON	Descripción
ARN de sesión del rol asumido de identidad del usuario*	`policyDetails.actor.userIdentity.assumedRole.arn`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `AssumeRole` de la API AWS STSel Nombre de recurso de Amazon (ARN) de la cuenta de origen, el usuario de IAM, o el rol que se utilizó para obtener las credenciales.

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `AssumeRole` de la API AWS STS, el origen de las credenciales de seguridad temporales, por ejemplo, `Root`, `IAMUser`, o `Role`.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `AssumeRole` de la API AWS STS, el nombre o alias del usuario o rol que emitió la sesión. Tenga en cuenta que este valor es nulo si las credenciales se obtuvieron de una cuenta raíz que no tiene un alias. Este campo no está disponible como opción de filtrado en la consola.
Identificador de usuario de la cuenta AWS de la identidad del usuario*	`policyDetails.actor.userIdentity.awsAccount.accountId`	Para una acción realizada con las credenciales de otra Cuenta de AWS, el identificador único de la cuenta.
Identificador principal de la cuenta AWS de identidad del usuario*	`policyDetails.actor.userIdentity.awsAccount.principalId`	Para una acción realizada con las credenciales de otra Cuenta de AWS, el identificador único para la entidad que realizó la acción.
El servicio AWS de identidad de usuario invocado por	`policyDetails.actor.userIdentity.awsService.invokedBy`	En el caso de una acción realizada por una cuenta que pertenece a un Servicio de AWS, el nombre del servicio.

Campo	Campo JSON	Descripción
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación de `GetFederationToken` de la API AWS STS, el identificador de clave de acceso AWS que identifica las credenciales. Este campo no está disponible como opción de filtrado en la consola.
ARN de sesión de la federación de identidad del usuario*	`policyDetails.actor.userIdentity.federatedUser.arn`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `GetFederationToken` de la API AWS STS, el ARN de la entidad que se utilizó para obtener las credenciales.
Identificador de cuenta de usuario de la federación de identidades del usuario*	`policyDetails.actor.userIdentity.federatedUser.accountId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación de `GetFederationToken` de la API AWS STS, el identificador único para el Cuenta de AWS propietario de la entidad que se utilizó para obtener las credenciales.

Campo	Campo JSON	Descripción
Identificador principal de la federación de identidades del usuario*	`policyDetails.actor.userIdentity.federatedUser.principalId`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `GetFederationToken` de la API de AWS STS, el identificador único de la entidad que se utilizó para obtener las credenciales.

—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n`
	
	`sessionIssuer.type`
		En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `GetFederationToken` de la API AWS STS, el origen de las credenciales de seguridad temporales, por ejemplo, `Root`, `IAMUser`, o `Role`.
		
		Este campo no está disponible como opción de filtrado en la consola.

Campo	Campo JSON	Descripción
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	En el caso de una acción realizada con credenciales de seguridad temporales que se obtuvieron mediante la operación `GetFederationToken` de la API AWS STS, el nombre o alias del usuario o rol que emitió la sesión. Tenga en cuenta que este valor es nulo si las credenciales se obtuvieron de una cuenta raíz que no tiene un alias. Este campo no está disponible como opción de filtrado en la consola.
Identificador de cuenta de IAM de la identidad del usuario*	`policyDetails.actor.userIdentity.iamUser.accountId`	Para una acción realizada con las credenciales de un usuario de IAM, el identificador único del Cuenta de AWS que está asociado con el usuario de IAM que realizó la acción.
Identificador principal de IAM de la identidad del usuario*	`policyDetails.actor.userIdentity.iamUser.principalId`	Para una acción realizada con las credenciales del usuario de IAM, el identificador único del usuario de IAM que realizó la acción.

Campo	Campo JSON	Descripción
Nombre de usuario de IAM de la identidad del usuario*	`policyDetails.actor.userIdentity.iamUser.userName`	Para una acción realizada con las credenciales de un usuario de IAM, el nombre de usuario del usuario de IAM que realizó la acción.
Identificador de cuenta raíz de la identidad del usuario*	`policyDetails.actor.userIdentity.root.accountId`	Para una acción realizada con las credenciales de su Cuenta de AWS, el identificador único de la cuenta.
Identificador principal raíz de la identidad del usuario*	`policyDetails.actor.userIdentity.root.principalId`	Para una acción realizada con las credenciales de su Cuenta de AWS, el identificador único de la entidad que realizó la acción.
Tipo de identidad de usuario	`policyDetails.actor.userIdentity.type`	El tipo de entidad que realizó la acción que produjo el resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos para la API, consulte la referencia UserIdentityTypede la API de Amazon Macie.

* Para especificar varios valores para este campo en la consola, añada una condición que utilice el campo y especifique un valor distinto para el filtro y, a continuación, repita ese paso para cada valor adicional. Para hacerlo con la API, utilice una matriz que muestre los valores que se van a utilizar para el filtrado.

Campos de clasificación de información confidencial

En la siguiente tabla, se enumeran y describen los campos que puede usar para filtrar los resultados de información confidencial. Estos campos almacenan datos específicos de los resultados de información confidencial.

En la tabla, la columna Campo indica el nombre del campo de la consola de Amazon Macie. La columna campo JSON utiliza la notación de puntos para indicar el nombre del campo en las representaciones JSON de los resultados y en la API de Amazon Macie. La columna Descripción proporciona una breve descripción de los datos que almacena el campo e indica los requisitos para los valores de filtrado. La tabla se ordena alfabéticamente de manera ascendente por campo y, a continuación, por campo JSON.

Campo	Campo JSON	Descripción
ID del identificador de datos personalizado*	`classificationDetails.result.customDataIdentifiers.detections.arn`	El identificador único para el identificador de datos personalizado que detectó los datos y produjo el resultado.
Nombre del identificador de datos personalizado*	`classificationDetails.result.customDataIdentifiers.detections.name`	El nombre del identificador de datos personalizado que detectó los datos y produjo el resultado.
Recuento total del identificador de datos personalizados	`classificationDetails.result.customDataIdentifiers.detections.count`	El número total de apariciones de datos detectados por los identificadores de datos personalizados y que produjeron el resultado. Puede usar este campo para definir un rango numérico para un filtrado.
Identificador de trabajo*	`classificationDetails.jobId`	El identificador único del trabajo de detección de

Campo	Campo JSON	Descripción
		información confidencial que produjo el resultado.
Tipo de origen	`classificationDetails.originType`	Cómo encontró Macie los datos confidenciales que produjeron el resultado: `AUTOMATED_SENSITIVE_DATA_DISCOVERY` o `SENSITIVE_DATA_DISCOVERY_JOB` .
—	`classificationDetails.result.mimeType`	El tipo de contenido, en formato MIME, al que se aplica el resultado, por ejemplo, `text/csv` para un archivo CSV o `application/pdf` para un archivo con el formato documento portátil de Adobe. Este campo no está disponible como opción de filtrado en la consola.
—	`classificationDetails.result.sizeClassified`	El tamaño total de almacenamiento, en bytes, del objeto de S3 al que se aplica el resultado. Este campo no está disponible como opción de filtrado en la consola. Con la API, puede usar este campo para definir un rango numérico para un filtrado.

Campo	Campo JSON	Descripción
Código de estado del resultado*	`classificationDetails.result.status.code`	El estado actual del resultado. Los valores válidos son: • `COMPLETE`: Macie completó el análisis del objeto. • `PARTIAL`: Macie analizó solo un subconjunto de los datos del objeto. Por ejemplo, el objeto es un archivo comprimido que contiene archivos en un formato no compatible. • `SKIPPED`: Macie no pudo analizar el objeto. Por ejemplo, el objeto es un archivo con formato incorrecto.
Categoría de datos confidenciales	`classificationDetails.result.sensitiveData.category`	La categoría de datos confidenciales que se detectaron y produjeron el resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. En la API, los valores válidos son `CREDENTIALS` , `FINANCIAL_INFORMATION` y `PERSONAL_INFORMATION` .

Campo	Campo JSON	Descripción
Tipo de detección de datos confidenciales	`classificationDetails.result.sensitiveData.detections.type`	El tipo de datos confidenciales que se detectaron y produjeron el resultado. La consola proporciona una lista de valores entre los que elegir al añadir este campo a un filtro. Para obtener una lista de valores válidos para la consola y la API, consulte Tipos de detección de datos confidenciales.
Recuento total de datos confidenciales	`classificationDetails.result.sensitiveData.detections.count`	El número total de apariciones de los datos confidenciales que se detectaron y produjeron el resultado. Puede usar este campo para definir un rango numérico para un filtrado.

* Para especificar varios valores para este campo en la consola, añada una condición que utilice el campo y especifique un valor distinto para el filtro y, a continuación, repita ese paso para cada valor adicional. Para hacerlo con la API, utilice una matriz que muestre los valores que se van a utilizar para el filtrado.

Tipos de detección de datos confidenciales

En los temas siguientes se enumeran los valores que puede especificar para el campo Tipo de detección de datos confidenciales de un filtrado. (El nombre JSON de este campo es `classificationDetails.result.sensitiveData.detections.type`). Los temas están organizados por categorías de datos confidenciales que Macie puede detectar mediante identificadores de datos administrados.

Categorías

- Credenciales
- Información financiera
- Información personal: información médica personal (PHI)
- Información personal: información de identificación personal (PII)

Para obtener más información sobre el identificador de datos gestionados para un tipo específico de datos confidenciales, consulte Referencia detallada: identificadores de datos gestionados por Amazon Macie.

Credenciales

Puede especificar los siguientes valores para filtrar los resultados que notifican la aparición de datos de credenciales en objetos de S3.

Tipos de datos confidenciales	Valor del filtrado
Clave de acceso secreta de AWS	`AWS_CREDENTIALS`
Clave de API de Google Cloud	`GCP_API_KEY`
Encabezado de autorización básica de HTTP	`HTTP_BASIC_AUTH_HEADER`
Token web JSON (JWT)	`JSON_WEB_TOKEN`
Clave privada de OpenSSH	`OPENSSH_PRIVATE_KEY`
Clave privada de PGP	`PGP_PRIVATE_KEY`
Clave privada del estándar de criptografía de clave pública (PKCS)	`PKCS`
Clave privada PuTTY	`PUTTY_PRIVATE_KEY`
Clave de API de Stripe	`STRIPE_CREDENTIALS`

Información financiera

Puede especificar los siguientes valores para filtrar los resultados que notifican la aparición de información financiera en los objetos de S3.

Tipos de datos confidenciales	Valor del filtrado
Número de cuenta bancaria	`BANK_ACCOUNT_NUMBER` (para Canadá y EE. UU.)
Número de cuenta bancaria básico (BBAN)	Según el país o región: `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Fecha de caducidad de la tarjeta	`CREDIT_CARD_EXPIRATION`
Datos de banda magnética de tarjetas de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Número de tarjetas de crédito	`CREDIT_CARD_NUMBER` (para números de tarjetas de crédito próximos a una palabra clave), `CREDIT_CARD_NUMBER_(NO_KEYWORD)` (para números de tarjetas de crédito que no están cerca de una palabra clave)
Código de verificación de tarjeta de crédito	`CREDIT_CARD_SECURITY_CODE`
Número de cuenta bancaria internacional (IBAN)	Según el país o región: `ALBANIA_BANK_ACCOUNT_NUMBER`, `ANDORRA_BANK_ACCOUNT_NUMBER`, `BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER`, `BRAZIL_BANK_ACCOUNT_NUMBER`, `BULGARIA_BANK_ACCOUNT_NUMBER`, `COSTA_RICA_BANK_ACCOUNT_NUMBER`, `CROATIA_BANK_ACCOUNT_NUMBER`, `CYPRUS_BANK_ACCOUNT_NUMBER`, `CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER`, `DENMARK_BANK_ACCOUNT_NUMBER`, `DOMINICAN`

Tipos de datos confidenciales	Valor del filtrado
	_REPUBLIC_BANK_ACCOUNT_NUMB ER, EGYPT_BANK_ACCOUNT_NUM BER, ESTONIA_BANK_ACCOUNT_NUMBER , FAROE_ISLANDS_BANK_ACCOU NT_NUMBER, FINLAND_BANK_AC COUNT_NUMBER, FRANCE_BANK_ACCOUN T_NUMBER, GEORGIA_BANK_ACC OUNT_NUMBER, GERMANY_BANK_ACCOU NT_NUMBER, GREECE_BANK_ACC OUNT_NUMBER, GREENLAND_BANK_ACC OUNT_NUMBER, HUNGARY_BANK_ ACCOUNT_NUMBER, ICELAND_B ANK_ACCOUNT_NUMBER, IRELAN D_BANK_ACCOUNT_NUMBER, ITALY_BAN K_ACCOUNT_NUMBER, JORDAN_B ANK_ACCOUNT_NUMBER, KOSOVO_BA NK_ACCOUNT_NUMBER, LIECHTE NSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER , MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_N UMBER, NETHERLANDS_BANK_AC COUNT_NUMBER, NORTH_MACEDO NIA_BANK_ACCOUNT_NUMBER, P OLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER,

Tipos de datos confidenciales	Valor del filtrado
	SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (para las Islas Vírgenes Británicas)

Información personal: información médica personal (PHI)

Puede especificar los siguientes valores para filtrar los resultados que notifican la aparición de información médica personal (PHI) en objetos de S3.

Tipos de datos confidenciales	Valor del filtrado
Número de registro de la Administración para el Control de Drogas (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Número de reclamación del seguro médico (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Número de seguro médico o identificación médica	Según el país o región: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Tipos de datos confidenciales	Valor del filtrado
Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Código nacional de medicamento (NDC)	`USA_NATIONAL_DRUG_CODE`
Identificador nacional de proveedores (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Identificador de dispositivo único (UDI)	`MEDICAL_DEVICE_UDI`

Información personal: información de identificación personal (PII)

Puede especificar los siguientes valores para filtrar los resultados que notifican la aparición de información de identificación personal (PII) en los objetos de S3.

Tipos de datos confidenciales	Valor del filtrado
Fecha de nacimiento	`DATE_OF_BIRTH`
Número de identificación del permiso de conducir	Según el país o región: `AUSTRALIA_DRIVERS_LICENSE`, `AUSTRIA_DRIVERS_LICENSE`, `BELGIUM_DRIVERS_LICENSE`, `BULGARIA_DRIVERS_LICENSE`, `CANADA_DRIVERS_LICENSE`, `CROATIA_DRIVERS_LICENSE`, `CYPRUS_DRIVERS_LICENSE`, `CZECHIA_DRIVERS_LICENSE`, `DENMARK_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (para EE. UU.), `ESTONIA_DRIVERS_LICENSE`, `FINLAND_DRIVERS_LICENSE`, `FRANCE_DRIVERS_LICENSE`, `GERMANY_DRIVERS_LICENSE`, `GREECE_DRIVERS_LICENSE`, `HUNGARY_DRIVERS_LICENSE`, `INDIA_DRIV`

Tipos de datos confidenciales	Valor del filtrado
	ERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Número de registro electoral	UK_ELECTORAL_ROLL_NUMBER
Nombre completo	NAME
Coordenadas del sistema de posicionamiento global (GPS)	LATITUDE_LONGITUDE
Cookie HTTP	HTTP_COOKIE
Dirección postal	ADDRESS, BRAZIL_CEP_CODE
Número de identificación nacional	Según el país o región: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
Número de seguro nacional (NINO)	UK_NATIONAL_INSURANCE_NUMBER

Tipos de datos confidenciales	Valor del filtrado
Número de pasaporte	Según el país o región: `CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Número de residencia permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Número de teléfono	Según el país o región: `BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (para Canada y EE. UU.), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Número de Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número de la Seguridad Social (SSN)	Según el país o región: `SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Tipos de datos confidenciales	Valor del filtrado
Número de identificación o referencia del contribuyente	Según el país o región: `AUSTRALIA_TAX_FILE_NUMBER`, `BRAZIL_CNPJ_NUMBER`, `BRAZIL_CPF_NUMBER`, `FRANCE_TAX_IDENTIFICATION_NUMBER`, `GERMANY_TAX_IDENTIFICATION_NUMBER`, `INDIA_PERMANENT_ACCOUNT_NUMBER`, `SPAIN_NIE_NUMBER`, `SPAIN_NIF_NUMBER`, `SPAIN_TAX_IDENTIFICATION_NUMBER`, `UK_TAX_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Número de identificación de vehículo (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Investigación de los datos confidenciales con los hallazgos de Amazon Macie

Cuando se ejecutan trabajos de detección de datos confidenciales o Amazon Macie realiza una detección automática de datos confidenciales, Macie captura detalles sobre la ubicación de cada aparición de datos confidenciales que encuentra en los objetos de Amazon Simple Storage Service (Amazon S3). Esto incluye los datos confidenciales que Macie detecta utilizando identificadores de datos administrados y los datos que coinciden con los criterios de los identificadores de datos personalizados que usted configura para que utilice un trabajo o Macie.

Con los hallazgos de datos confidenciales, puede revisar estos detalles para un máximo de 15 apariciones de datos confidenciales que Macie encuentra en objetos de S3 individuales. Los detalles proporcionan información sobre la amplitud de las categorías y tipos de datos confidenciales que pueden contener determinados buckets y objetos de S3. Pueden ayudarle a localizar apariciones individuales de datos confidenciales en objetos y a determinar si debe realizar una investigación más profunda de buckets y objetos específicos.

Para obtener información adicional, puede configurar y utilizar opcionalmente Macie para recuperar muestras de datos confidenciales que Macie notifica en hallazgos individuales. Las muestras pueden

ayudarle a verificar la naturaleza de los datos confidenciales que encontró Macie. También pueden ser de ayuda para personalizar la investigación de un objeto y un bucket de S3 afectados. Si opta por recuperar muestras de datos confidenciales para un hallazgo, Macie utiliza los datos del hallazgo para localizar de 1 a 10 apariciones de cada tipo de datos confidenciales notificados por el hallazgo. A continuación, Macie extrae las apariciones de datos confidenciales del objeto afectado y muestra los datos para que usted los revise.

Si un objeto de S3 contiene muchas apariciones de datos confidenciales, un hallazgo también puede ayudarle a navegar hasta el resultado de detección de datos confidenciales correspondiente. A diferencia de un hallazgo de datos confidenciales, un resultado de detección de datos confidenciales proporciona datos de localización detallados de hasta 1000 apariciones de cada tipo de datos confidenciales que Macie encuentra en un objeto. Macie utiliza el mismo esquema para los datos de localización en los hallazgos de datos confidenciales y en los resultados de la detección de datos confidenciales. Para obtener más información sobre los resultados de la detección de datos confidenciales, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Los temas de esta sección explican cómo localizar y, opcionalmente, recuperar incidencias de datos confidenciales notificadas por hallazgos de datos confidenciales. También explican el esquema que utiliza Macie para informar de la ubicación de las apariciones individuales de datos confidenciales que encuentra.

Temas

- Localización de los datos confidenciales con los hallazgos de Amazon Macie
- Recuperación de muestras de datos confidenciales con los resultados de Amazon Macie
- Esquema JSON para ubicaciones de datos confidenciales

Localización de los datos confidenciales con los hallazgos de Amazon Macie

Cuando ejecuta trabajos de detección de datos confidenciales o Amazon Macie realiza una detección de datos confidenciales automática, Macie realiza una inspección profunda de la última versión de cada objeto de Amazon Simple Storage Service (Amazon S3) que analiza. Para cada ejecución de trabajo o ciclo de análisis, Macie utiliza un algoritmo de búsqueda en profundidad para rellenar los hallazgos resultantes con detalles sobre la ubicación de apariciones específicas de datos confidenciales que Macie encuentra en los objetos de S3. Estas apariciones proporcionan información sobre las categorías y los tipos de datos confidenciales que pueden contener un bucket

y un objeto de S3 afectados. Los detalles pueden ayudarle a localizar apariciones individuales de datos confidenciales en los objetos y a determinar si es necesario realizar una investigación más profunda de buckets y objetos específicos.

Con los hallazgos de datos confidenciales, puede determinar la ubicación de hasta 15 apariciones de datos confidenciales que Macie encontró en un objeto de S3 afectado. Esto incluye los datos confidenciales que Macie detectó mediante identificadores de datos administrados y los datos que cumplen los criterios de identificadores de datos personalizados que usted configuró para que utilizara un trabajo o Macie.

Un hallazgo de datos confidenciales puede proporcionar detalles como:

- El número de columna y fila de una celda o campo de un libro de Microsoft Excel, un archivo CSV o un archivo TSV.
- La ruta a un campo o matriz en un archivo JSON o líneas JSON.
- El número de línea de una línea de un archivo de texto no binario que no sea un archivo CSV, JSON, líneas JSON o TSV, por ejemplo, un archivo HTML, TXT o XML.
- El número de página de una página de un archivo en formato de documento portátil (PDF) de Adobe.
- El índice de registro y la ruta a un campo de un registro en un contenedor de objetos de Apache Avro o un archivo de Apache Parquet.

Puede acceder a estos detalles mediante la consola de Amazon Macie o la API de Amazon Macie. También puede acceder a estos detalles en los hallazgos que Macie publica en otros Servicios de AWS, tanto en Amazon EventBridge como en AWS Security Hub. Para obtener más información sobre las estructuras JSON que utiliza Macie para informar de estos detalles, consulte Esquema JSON para ubicaciones de datos confidenciales. Para obtener información sobre cómo acceder a los detalles de los hallazgos que Macie publica para otros Servicios de AWS, consulte Seguimiento y procesamiento de los hallazgos.

Si un objeto de S3 contiene muchas apariciones de datos confidenciales, también puede utilizar un hallazgo para navegar hasta su correspondiente resultado de detección de datos confidenciales. A diferencia de un hallazgo de datos confidenciales, un resultado de detección de datos confidenciales proporciona datos de localización detallados de hasta 1000 apariciones de cada tipo de dato confidencial que Macie haya encontrado en un objeto. Si un objeto de S3 es un archivo comprimido, como un archivo .tar o .zip, esto incluye apariciones de datos confidenciales en archivos individuales que Macie haya extraído del archivo (Macie no incluye esta información en los hallazgos de datos

confidenciales). Para obtener más información sobre los resultados de la detección de datos confidenciales, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales. Macie utiliza el mismo esquema para los datos de localización en los hallazgos de datos confidenciales y en los resultados de la detección de datos confidenciales.

Localización de apariciones de datos confidenciales

Para localizar apariciones de datos confidenciales, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Los siguientes pasos explican cómo localizar datos confidenciales mediante la consola.

Para localizar datos confidenciales mediante programación, utilice la operación GetFindings de la API de Amazon Macie. Si un hallazgo incluye detalles sobre la ubicación de una o más apariciones de un tipo específico de datos confidenciales, los objetos `occurrences` del hallazgo proporcionan estos detalles. Para obtener más información, consulte Esquema JSON para ubicaciones de datos confidenciales.

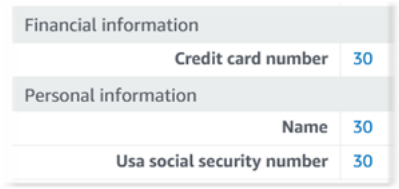
Para localizar apariciones de datos confidenciales

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Resultados.

   > **Tip**
   >
   > Puede utilizar la página Trabajos para mostrar todos los resultados de un trabajo concreto de detección de datos confidenciales. En el panel de navegación, seleccione Trabajos y, a continuación, seleccione el nombre del trabajo. En la parte superior del panel de detalles, seleccione Mostrar resultados y, a continuación, seleccione Mostrar hallazgos.

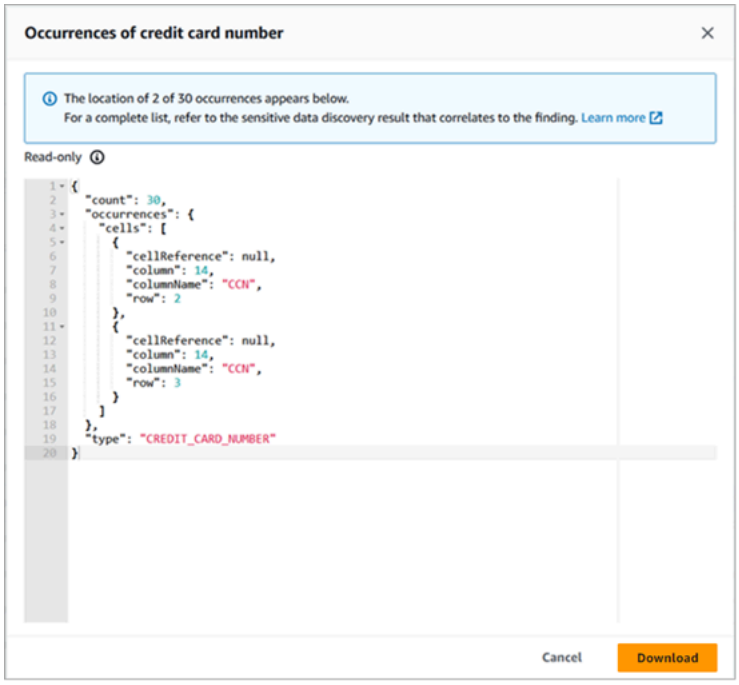
3. En la página Hallazgos, seleccione el hallazgo de los datos confidenciales que desea localizar. El panel de detalles muestra información sobre el resultado.
4. En el panel de detalles, desplácese hasta la sección Datos confidenciales. Esta sección proporciona información sobre las categorías y los tipos de datos confidenciales que Macie encontró en el objeto de S3 afectado. También indica el número de apariciones de cada tipo de datos confidenciales que encontró Macie.

Por ejemplo, en la siguiente imagen se muestran algunos detalles de un hallazgo que informa de 30 apariciones de números de tarjetas de crédito, 30 apariciones de nombres y 30 apariciones de números de la Seguridad Social estadounidense.



Si el hallazgo incluye detalles sobre la ubicación de una o más apariciones de un tipo específico de datos confidenciales, el número de apariciones es un enlace. Seleccione el enlace para mostrar los detalles. Macie abre una nueva ventana y muestra los detalles en formato JSON.

Por ejemplo, la siguiente imagen muestra la ubicación de dos apariciones de números de tarjetas de crédito en un objeto de S3 afectado.



Para guardar los detalles como un archivo JSON, seleccione Descargar y, a continuación, especifique un nombre y una ubicación para el archivo.

5. (Opcional) Para guardar todos los detalles del hallazgo como un archivo JSON, seleccione el identificador del hallazgo (ID del hallazgo) en la parte superior del panel de detalles. Macie abre una nueva ventana y muestra los detalles en formato JSON. Seleccione Descargar y, a continuación, especifique un nombre y una ubicación para el archivo.

Para acceder a los detalles sobre la ubicación de hasta 1000 apariciones de cada tipo de datos confidenciales en el objeto afectado, consulte el correspondiente resultado de detección de datos confidenciales para el hallazgo. Para ello, desplácese hasta el principio de la sección Detalles del panel. A continuación, seleccione el enlace en el campo Ubicación detallada del resultado. Macie abre la consola de Amazon S3 y muestra el archivo o la carpeta que contiene el resultado de la detección correspondiente.

Recuperación de muestras de datos confidenciales con los resultados de Amazon Macie

Para verificar la naturaleza de los datos confidenciales que Amazon Macie notifica en los resultados, puede configurar y usar Macie de manera opcional para recuperar y revelar muestras de datos confidenciales notificados por resultados individuales. Esto incluye los datos confidenciales que Macie detecta mediante identificadores de datos administrados y los datos que cumplen los criterios de identificadores de datos personalizados. Las muestras también pueden ser de ayuda a la hora de personalizar la investigación de un objeto y un bucket de Amazon Simple Storage Service (Amazon S3) afectados.

Si recupera y revela muestras de datos confidenciales de un resultado, Macie lleva a cabo las siguientes tareas generales:

1. Verifica que el resultado especifique la ubicación de las instancias individuales de datos confidenciales y la ubicación del resultado de la detección de datos confidenciales correspondiente.
2. Evalúa el resultado de la detección de datos confidenciales correspondiente y comprueba la validez de los metadatos del objeto de S3 afectado y de los datos de ubicación de las instancias individuales de datos confidenciales en el objeto afectado.
3. Al utilizar los datos del resultado de detección de datos confidenciales, localiza las primeras 1 a 10 ocurrencias de datos confidenciales reportadas por el resultado y extrae los primeros 1 a 128 caracteres de cada ocurrencia del objeto de S3 afectado. Si el resultado indica varios tipos de datos confidenciales, Macie lo hace para un máximo de 100 tipos.
4. Cifra los datos mediante una clave de AWS Key Management Service (AWS KMS) que especifique.
5. Almacena temporalmente los datos cifrados en una memoria caché y los muestra para que los revise. Los datos están cifrados en todo momento, tanto en tránsito como en reposo.

6. Poco después de la extracción y el cifrado, elimina permanentemente los datos de la memoria caché, a menos que se requiera una retención adicional temporal para resolver un problema operativo.

Si decide volver a recuperar y revelar muestras de datos confidenciales de un resultado, Macie repite las tareas de localización, extracción, cifrado, almacenamiento y, en última instancia, eliminación de las muestras.

Macie no utiliza el rol vinculado al servicio de Macie en su cuenta para realizar estas tareas. En su lugar, utiliza su identidad de AWS Identity and Access Management (IAM) o permite que Macie asuma un rol de IAM en su cuenta. Si a usted o a su rol se le permite acceder a los recursos y datos necesarios y llevar a cabo las acciones requeridas, puede recuperar y revelar muestras de datos confidenciales de un resultado. Se registran todas las acciones necesarias en AWS CloudTrail.

> **Important**
>
> Se recomienda que restrinja el acceso a esta funcionalidad mediante políticas de IAM personalizadas. Para tener un control de acceso adicional, le recomendamos que cree también un AWS KMS key dedicado para el cifrado de las muestras de datos confidenciales que se recuperen y restrinja el uso de la clave únicamente a las entidades principales a las que se les debe permitir recuperar y revelar las muestras de datos confidenciales.
> Para ver recomendaciones y ejemplos de políticas que puede usar para controlar el acceso a esta funcionalidad, consulte la entrada del blog sobre cómo usar Amazon Macie para obtener una vista previa de datos confidenciales en buckets de S3 en el blog de seguridad de AWS.

En los temas de esta sección se explica cómo configurar y usar Macie para recuperar y revelar muestras de datos confidenciales para resultados. Puede realizar estas tareas en todas las en las Regiones de AWS que Macie está disponible actualmente, excepto las de Asia-Pacífico (Osaka) e Israel (Tel Aviv).

Temas

- Opciones de configuración y requisitos para recuperar muestras de datos confidenciales con resultados
- Configuración de Amazon Macie para recuperar y revelar muestras de datos confidenciales con resultados
- Recuperación y revelación de muestras de datos confidenciales con resultados

Opciones de configuración y requisitos para recuperar muestras de datos confidenciales con resultados

Si lo desea, puede configurar y usar Amazon Macie de manera opcional para recuperar y revelar muestras de datos confidenciales que Macie notifica en resultados individuales. Si recupera y revela muestras de datos confidenciales para un resultado, Macie utiliza los datos del resultado de la detección de datos confidenciales correspondiente para localizar las instancias de datos confidenciales en el objeto de Amazon Simple Storage Service (Amazon S3) afectado. A continuación, Macie extrae muestras de esas ocurrencias del objeto afectado. Macie cifra los datos extraídos con una clave AWS Key Management Service (AWS KMS) que usted especifique, almacena temporalmente los datos cifrados en una memoria caché y devuelve los datos en sus resultados para el resultado. Poco después de la extracción y el cifrado, Macie elimina permanentemente los datos de la memoria caché, a menos que se requiera una retención adicional temporal para resolver un problema operativo.

Macie no utiliza el rol vinculado al servicio de Macie en su cuenta para localizar, recuperar, cifrar o revelar muestras de datos confidenciales de los objetos de S3 afectados. En su lugar, Macie utiliza los ajustes y los recursos que configura para su cuenta. Al configurar los ajustes en Macie, se especifica cómo acceder a los objetos de S3 afectados. También debe especificar qué AWS KMS key se usará para cifrar las muestras. Puede configurar estos ajustes en todas las Regiones de AWS en las que Macie está disponible actualmente, excepto Asia-Pacífico (Osaka) e Israel (Tel Aviv).

Para acceder a los objetos de S3 afectados y recuperar muestras de datos confidenciales de ellos, tiene dos opciones. Puede configurar Macie para que utilice credenciales de usuario de AWS Identity and Access Management (IAM) o asuma un rol de IAM:

- Utilizar las credenciales de usuario de IAM: con esta opción, cada usuario de su cuenta utilizará su identidad de IAM individual para localizar, recuperar, cifrar y revelar las muestras. Esto significa que un usuario puede recuperar y revelar muestras de datos confidenciales para un resultado si se le permite acceder a los recursos y datos necesarios y llevar a cabo las acciones necesarias.
- Asumir un rol de IAM: con esta opción, se crea un rol de IAM que delega el acceso a Macie. También debe asegurarse de que las políticas de confianza y permisos del rol cumplan todos los requisitos para que Macie lo asuma. A continuación, Macie asume ese rol cuando un usuario de su cuenta decide localizar, recuperar, cifrar y revelar muestras de datos confidenciales para un resultado.

Puede utilizar cualquier configuración con cualquier tipo de cuenta de Macie: la cuenta de administrador de Macie delegada para una organización, una cuenta de miembro de Macie de una organización o una cuenta de Macie independiente.

En los siguientes temas, se explican las opciones, los requisitos y las consideraciones que pueden ayudarle a determinar cómo configurar los ajustes y los recursos de su cuenta. Esto incluye las políticas de permisos y confianza que se van a asociar a un rol de IAM. Para ver recomendaciones y ejemplos adicionales de políticas que puede usar para recuperar y revelar muestras de datos confidenciales, consulte la entrada del blog sobre cómo usar Amazon Macie para obtener una vista previa de datos confidenciales en buckets de S3 en el blog de seguridad de AWS.

Temas

Determinación del método de acceso que se usará

Al determinar qué configuración es la mejor para su entorno de AWS, una consideración clave es si el entorno incluye varias cuentas de Amazon Macie que se administran de forma centralizada como una organización. Si es el administrador delegado de Macie en una organización, configurar Macie para que asuma un rol de IAM puede agilizar la recuperación de muestras de datos confidenciales de los objetos de S3 afectados para las cuentas de su organización. Con este enfoque, cree un rol de IAM en la cuenta de administrador. También puede crear un rol de IAM en cada cuenta de miembro aplicable. El rol de su cuenta de administrador delega el acceso a Macie. El rol en una cuenta de miembro delega el acceso entre cuentas al rol de su cuenta de administrador. Si se implementa, podrá utilizar el encadenamiento de roles para acceder a los objetos de S3 afectados en sus cuentas de miembros.

Tenga en cuenta también quién tiene acceso directo a los resultados individuales de forma predeterminada. Para recuperar y revelar muestras de datos confidenciales para un resultado, el usuario debe tener acceso al resultado antes:

- Trabajos de detección de datos confidenciales: solo la cuenta que crea un trabajo puede acceder a los resultados que genere el trabajo. Si tiene una cuenta de administrador de Macie, puede

configurar un trabajo para analizar los objetos de los buckets de S3 para cualquier cuenta de su organización. Por lo tanto, sus trabajos pueden generar resultados de objetos en los buckets que son propiedad de sus cuentas de miembros. Si tiene una cuenta de miembro o una cuenta de Macie independiente, puede configurar un trabajo para analizar los objetos únicamente en los buckets que sean propiedad de su cuenta.

- Detección de datos confidenciales automatizada: solo la cuenta de administrador de Macie puede acceder a los resultados que la detección automatizada genere para las cuentas de su organización. Las cuentas de los miembros no pueden acceder a estos resultados. Si tiene una cuenta de Macie independiente, solo podrá acceder a los resultados que genere la detección automatizada para su propia cuenta.

Si planea acceder a los objetos de S3 afectados mediante un rol de IAM, tenga en cuenta también lo siguiente:

- Para localizar instancias de datos confidenciales en un objeto, el resultado de la detección de datos confidenciales correspondiente a un resultado debe almacenarse en un objeto de S3 que Macie haya firmado con una AWS KMS key de código de autenticación de mensajes basado en hash (HMAC). Macie debe poder verificar la integridad y autenticidad del resultado de la detección de datos confidenciales. De lo contrario, Macie no asumirá el rol de IAM para recuperar muestras de datos confidenciales. Se trata de una barrera de protección adicional para restringir el acceso a los datos de los objetos de S3 de una cuenta.
- Para recuperar muestras de datos confidenciales de un objeto cifrado con una AWS KMS key administrada por el cliente, el rol de IAM debe poder descifrar los datos con la clave. Más específicamente, la política de claves debe permitir que el rol lleve a cabo la acción `kms:Decrypt`. Para otros tipos de cifrado del servidor, no se requieren permisos ni recursos adicionales para descifrar un objeto afectado. Para obtener más información, consulte Descifrado de los objetos de S3 afectados.
- Para recuperar muestras de datos confidenciales de un objeto para otra cuenta, actualmente debe ser el administrador delegado de Macie para la cuenta de la Región de AWS correspondiente. Además:
  - Actualmente, Macie debe estar habilitado para la cuenta de miembro en la región correspondiente.
  - La cuenta de miembro debe tener un rol de IAM que delegue el acceso entre cuentas a un rol de IAM en su cuenta de administrador de Macie. El nombre del rol debe ser el mismo en su cuenta de administrador de Macie y en la cuenta de miembro.

- La política de confianza del rol de IAM en la cuenta del miembro debe incluir una condición que especifique el ID externo correcto para su configuración. Este ID es una cadena alfanumérica única que Macie genera automáticamente después de configurar los ajustes de su cuenta de administrador de Macie. Para obtener más información sobre el uso de ID externos en las políticas de confianza, consulte Cómo utilizar un ID externo al otorgar acceso a los recursos de AWS a terceros en la Guía del usuario de AWS Identity and Access Management.
- Si el rol de IAM en la cuenta de miembro cumple todos los requisitos de Macie, la cuenta de miembro no necesita configurar ni habilitar los ajustes de Macie para poder recuperar muestras de datos confidenciales de los objetos de su cuenta. Macie utiliza únicamente la configuración y el rol de IAM de su cuenta de administrador de Macie y el rol de IAM de la cuenta de miembro.

> **Tip**
>
> Si su cuenta forma parte de una organización grande, considere la posibilidad de utilizar un conjunto de pilas y plantillas de AWS CloudFormation para aprovisionar y administrar los roles de IAM de las cuentas de los miembros de su organización. Para obtener información sobre la creación y el uso de conjuntos de pilas y plantillas, consulte la Guía del usuario de AWS CloudFormation.
>
> Para revisar y, si lo desea, descargar una plantilla de CloudFormation que pueda servir como punto de partida, puede utilizar la consola de Amazon Macie. En el panel de navegación de la consola, en Configuración, seleccione Revelar muestras. Elija Editar y, a continuación, elija Ver permisos de rol de miembro y plantilla de CloudFormation.

Los temas siguientes de esta sección proporcionan detalles y consideraciones adicionales para cada tipo de configuración. En el caso de los roles de IAM, esto incluye las políticas de permisos y confianza que se van a asociar a un rol. Si no tiene claro qué tipo de configuración es la mejor para su entorno, pida ayuda a su administrador de AWS.

Uso de las credenciales de usuario de IAM para acceder a los objetos de S3 afectados

Si configura Amazon Macie para recuperar muestras de datos confidenciales mediante credenciales de usuario de IAM, cada usuario de su cuenta de Macie utilizará su identidad de IAM para localizar, recuperar, cifrar y revelar muestras para resultados individuales. Esto significa que un usuario puede recuperar y revelar muestras de datos confidenciales para un resultado si su identidad de IAM tiene permiso para acceder a los recursos y datos necesarios y llevar a cabo las acciones necesarias. Se registran todas las acciones necesarias en AWS CloudTrail.

Para recuperar y revelar muestras de datos confidenciales para un resultado determinado, un usuario debe tener permiso para acceder a los siguientes datos y recursos: el resultado, el resultado de la detección de datos confidenciales correspondiente al resultado, el bucket de S3 afectado y el objeto de S3 afectado. También debe poder usar la AWS KMS key que se usó para cifrar el objeto afectado, si corresponde, y la AWS KMS key que configuró para que Macie usara para cifrar muestras de datos confidenciales. Si alguna política de IAM, política de recursos u otra configuración de permisos le deniega el acceso necesario, el usuario no podrá recuperar ni revelar muestras para el resultado.

Para establecer este tipo de configuración, lleve a cabo las siguientes tareas generales:

1. Compruebe que haya configurado un repositorio para los resultados de la detección de datos confidenciales.
2. Configure la AWS KMS key que se utilizará para el cifrado de muestras de datos confidenciales.
3. Compruebe sus permisos para configurar los ajustes en Macie.
4. Configure y habilite los ajustes de Macie.

Para obtener información acerca de cómo llevar a cabo estas tares, consulte Configuración de Amazon Macie para recuperar y revelar muestras de datos confidenciales con resultados.

Asunción de un rol de IAM para obtener acceso a los objetos de S3 afectados

Para configurar Amazon Macie a fin de que recupere muestras de datos confidenciales mediante la asunción de un rol de IAM, comience por crear un rol de IAM que delegue el acceso a Macie. Asegúrese de que las políticas de confianza y permisos del rol cumplan todos los requisitos para que Macie lo asuma. Cuando un usuario de su cuenta de Macie decide recuperar y revelar muestras de datos confidenciales para un resultado, Macie asume el rol de recuperar las muestras del objeto de S3 afectado. Macie solo asume ese rol cuando un usuario decide recuperar y revelar muestras para un resultado. Para asumir el rol, Macie usa la operación AssumeRole de la API de AWS Security Token Service (AWS STS). Se registran todas las acciones necesarias en AWS CloudTrail.

Para recuperar y revelar muestras de datos confidenciales para un resultado en particular, el usuario debe poder acceder al resultado, así como al resultado correspondiente de la detección de datos confidenciales y a la AWS KMS key que haya configurado para que Macie utilice para cifrar muestras de datos confidenciales. El rol de IAM debe permitir a Macie acceder al bucket de S3 y al objeto de S3 afectados. El rol también debe poder utilizar la AWS KMS key que se usó para cifrar el objeto afectado, si corresponde. Si alguna política de IAM, política de recursos u otra configuración de permisos le deniega el acceso necesario, el usuario no podrá recuperar ni revelar muestras para el resultado.

Para configurar este tipo de configuración, complete las siguientes tareas generales. Si tiene una cuenta de miembro en una organización, contacte con su administrador de Macie para determinar si debe configurar los ajustes y los recursos de su cuenta y de qué manera.

1. Defina lo siguiente:
   - El nombre del rol de IAM que desea que Macie asuma. Si su cuenta forma parte de una organización, este nombre debe ser el mismo para la cuenta de administrador delegado de Macie y para cada cuenta de miembro aplicable de la organización. De lo contrario, el administrador de Macie no podrá acceder a los objetos de S3 afectados desde la cuenta de miembro correspondiente.
   - El nombre de la política de permisos de IAM que se va a asociar al rol de IAM. Si su cuenta forma parte de una organización, le recomendamos que utilice el mismo nombre de política para cada cuenta de miembro aplicable de la organización. Esto puede agilizar el aprovisionamiento y la administración del rol en las cuentas de los miembros.
2. Compruebe que haya configurado un repositorio para los resultados de la detección de datos confidenciales.
3. Configure la AWS KMS key que se utilizará para el cifrado de muestras de datos confidenciales.
4. Compruebe sus permisos para crear roles de IAM y configurar los ajustes en Macie.
5. Si es el administrador delegado de Macie de una organización o si tiene una cuenta de Macie independiente:
   a. Cree y configure un rol de IAM para la cuenta. Asegúrese de que las políticas de confianza y permisos del rol cumplan todos los requisitos para que Macie lo asuma. Para obtener más información sobre estos requisitos, consulte el tema siguiente.
   b. Configure y habilite los ajustes de Macie. A continuación, Macie genera un ID externo para la configuración. Si es el administrador de Macie de una organización, anote este ID. La política de confianza del rol de IAM de cada una de sus cuentas de miembro correspondientes debe especificar este ID.
6. Si tiene una cuenta de miembro en una organización:
   a. Solicite al administrador de Macie el ID externo que especificará en la política de confianza para el rol de IAM de la cuenta. Compruebe también el nombre del rol de IAM y la política de permisos que se van a crear.
   b. Cree y configure un rol de IAM para la cuenta. Asegúrese de que las políticas de confianza y permisos del rol cumplan todos los requisitos para que el administrador de Macie lo asuma. Para obtener más información sobre estos requisitos, consulte el tema siguiente.

c. (Opcional) Si desea recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados para su propia cuenta, configure y habilite los ajustes en Macie. Si quiere que Macie asuma un rol de IAM para recuperar las muestras, comience por crear y configurar un rol de IAM adicional en su cuenta. Asegúrese de que las políticas de confianza y permisos de este rol adicional cumplan todos los requisitos para que Macie lo asuma. A continuación, configure los ajustes en Macie y especifique el nombre de este rol adicional. Para obtener más información sobre los requisitos de la política para el rol, consulte el tema siguiente.

Para obtener información acerca de cómo llevar a cabo estas tares, consulte Configuración de Amazon Macie para recuperar y revelar muestras de datos confidenciales con resultados.

Configuración de un rol de IAM para obtener acceso a los objetos de S3 afectados

Para acceder a los objetos de S3 afectados mediante un rol de IAM, comience por crear y configurar un rol que delegue el acceso a Amazon Macie. Asegúrese de que las políticas de confianza y permisos del rol cumplan todos los requisitos para que Macie lo asuma. La forma de hacerlo depende del tipo de cuenta de Macie que tenga.

En las siguientes secciones, se proporcionan detalles sobre las políticas de confianza y los permisos que se deben asociar al rol de IAM para cada tipo de cuenta de Macie. Elija la sección correspondiente al tipo de cuenta que tiene.

> **Note**
>
> Si tiene una cuenta de miembro en una organización, es posible que tenga que crear y configurar dos roles de IAM para la cuenta:
>
> - Para que el administrador de Macie pueda recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados para su cuenta, cree y configure un rol que pueda asumir la cuenta de su administrador. Para obtener estos detalles, elija la sección Cuenta de miembro de Macie.
> - Para recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados para la cuenta de su propiedad, cree y configure un rol que pueda asumir Macie. Para obtener estos detalles, elija la sección Cuenta independiente de Macie.
>
> Antes de crear y configurar cualquiera de los roles de IAM, trabaje con su administrador de Macie para determinar la configuración adecuada para su cuenta.

Para obtener información detallada sobre el uso de IAM para crear el rol, consulte Creación de un rol mediante políticas de confianza personalizadas en la Guía del usuario de AWS Identity and Access Management.

Cuenta de administrador de Macie

Si es el administrador delegado de Macie de una organización, empiece por utilizar el editor de políticas de IAM para crear la política de permisos para el rol de IAM. La política debe ser la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

Donde *IAMRoleName* es el nombre del rol de IAM que debe asumir Macie al recuperar muestras de datos confidenciales de los objetos de S3 afectados para las cuentas de su organización. Sustituya este valor por el nombre del rol que está creando para su cuenta y que planea crear para las cuentas de miembros aplicables de su organización. Este nombre debe ser el mismo para su cuenta de administrador de Macie y para cada cuenta de miembro aplicable.

> **Note**
>
> En la política de permisos anterior, el elemento `Resource` de la primera instrucción utiliza un carácter comodín (*). Esto permite que una entidad de IAM asociada recupere objetos de todos los buckets de S3 que son propiedad de su organización. Para permitir este acceso solo para buckets específicos, sustituya el carácter comodín por el nombre de recurso de Amazon (ARN) de cada bucket. Por ejemplo, para permitir el acceso únicamente a los objetos de un bucket denominado DOC-EXAMPLE-BUCKET, cambie el elemento por: `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> También puede restringir el acceso a objetos de buckets de S3 específicos de cuentas individuales. Para ello, especifique los ARN del bucket en el elemento `Resource` de la política de permisos para el rol de IAM en cada cuenta aplicable. Para obtener más información y ejemplos, consulte Elementos de política JSON de IAM: Resource en la Guía del usuario de AWS Identity and Access Management.

Tras crear la política de permisos para el rol de IAM, cree y configure el rol. Si lo hace mediante la consola de IAM, elija Política de confianza personalizada como Tipo de entidad de confianza para el rol. Para la política de confianza que define las entidades de confianza para el rol, especifique lo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Donde *accountId* es el ID de la cuenta de su Cuenta de AWS. Sustituya este valor por su ID de cuenta de 12 dígitos.

En la política de confianza anterior:

- El elemento `Principal` especifica la entidad principal de servicio que utiliza Macie al recuperar muestras de datos confidenciales de los objetos de S3 afectados, `reveal-samples.macie.amazonaws.com`.
- El elemento `Action` especifica la acción que la entidad principal de servicio puede llevar a cabo, la operación AssumeRole de la API de AWS Security Token Service (AWS STS).
- El elemento `Condition` define una condición que usa la clave de contexto de condición global aws:SourceAccount. Esta condición determina qué cuenta puede llevar a cabo la acción especificada. En este caso, permite a Macie asumir el rol solo para la cuenta especificada (*accountID*). La condición ayuda a evitar que Macie se utilice como un ayudante confuso durante las transacciones con AWS STS.

Tras definir la política de confianza para el rol de IAM, asocie la política de permisos al rol. Debe ser la política de permisos que creó antes de empezar a crear el rol. A continuación, complete los pasos restantes en IAM para terminar de crear y configurar el rol. Cuando termine, configure y habilite los ajustes en Macie.

Cuenta de miembro de Macie

Si tiene una cuenta de miembro de Macie y quiere permitir que su administrador de Macie recupere y revele muestras de datos confidenciales de los objetos de S3 afectados para su cuenta, empiece por pedir al administrador de Macie la siguiente información:

- El nombre del rol de IAM que se va a crear. El nombre de su cuenta debe ser el mismo que el de la cuenta de administrador de Macie de su organización.
- El nombre de la política de permisos de IAM que se va a asociar al rol.
- El ID externo que se va a especificar en la política de confianza para el rol. Este ID debe ser el ID externo que Macie generó para la configuración de su administrador de Macie.

Tras recibir esta información, utilice el editor de políticas de IAM para crear la política de permisos para el rol. La política debe ser la siguiente.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

La política de permisos anterior permite a una entidad de IAM asociada recuperar objetos de todos los buckets de S3 de su cuenta. Esto se debe a que el elemento `Resource` de la política utiliza un carácter comodín (*). Para permitir este acceso solo para buckets específicos, sustituya el carácter comodín por el nombre de recurso de Amazon (ARN) de cada bucket. Por ejemplo, para permitir el acceso únicamente a los objetos de un bucket denominado DOC-EXAMPLE-BUCKET2, cambie el elemento por:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

Para obtener más información y ejemplos, consulte Elementos de política JSON de IAM: Resource en la Guía del usuario de AWS Identity and Access Management.

Tras crear la política de permisos para el rol de IAM, cree el rol. Si crea el rol mediante la consola de IAM, elija Política de confianza personalizada como Tipo de entidad de confianza para el rol. Para la política de confianza que define las entidades de confianza para el rol, especifique lo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
```

```
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

En la política anterior, sustituya los valores de los marcadores de posición por los valores correctos para su entorno de AWS, donde:

- *`administratorAccountID`* es el ID de cuenta de 12 dígitos de su cuenta de administrador de Macie.
- *`IAMRoleName`* es el nombre del rol de IAM en su cuenta de administrador de Macie. Debe ser el nombre que recibió de su administrador de Macie.
- *`externalID`* es el ID externo que recibió de su administrador de Macie.

En general, la política de confianza permite al administrador de Macie asumir el rol de recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados para su cuenta. El elemento `Principal` especifica el ARN de un rol de IAM en la cuenta de administrador de Macie. Este es el rol que utiliza el administrador de Macie para recuperar y revelar muestras de datos confidenciales para las cuentas de su organización. El bloque `Condition` define dos condiciones que determinan aún más quién puede asumir el rol:

- La primera condición especifica un ID externo que es exclusivo de la configuración de su organización. Para obtener más información sobre ID externos, consulte Cómo utilizar un ID externo al otorgar acceso a los recursos de AWS a terceros en la Guía del usuario de AWS Identity and Access Management.
- La segunda condición usa la clave de contexto de condición global aws:PrincipalOrgID. El valor de la clave es una variable dinámica que representa el identificador único de una organización en AWS Organizations (`${aws:ResourceOrgID}`). La condición restringe el acceso solo a las cuentas que forman parte de la misma organización en AWS Organizations. Si se unió a su organización al aceptar una invitación en Macie, elimine esta condición de la política.

Tras definir la política de confianza para el rol de IAM, asocie la política de permisos al rol. Debe ser la política de permisos que creó antes de empezar a crear el rol. A continuación, complete los pasos

restantes en IAM para terminar de crear y configurar el rol. No configure ni introduzca ajustes para el rol en Macie.

Cuenta independiente de Macie

Si tiene una cuenta independiente de Macie o una cuenta de miembro de Macie y desea recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados para su propia cuenta, empiece por utilizar el editor de políticas de IAM para crear la política de permisos para el rol de IAM. La política debe ser la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

En la política de permisos anterior, el elemento `Resource` utiliza un carácter comodín (*). Esto permite que una entidad de IAM asociada recupere objetos de todos los buckets de S3 de su cuenta. Para permitir este acceso solo para buckets específicos, sustituya el carácter comodín por el nombre de recurso de Amazon (ARN) de cada bucket. Por ejemplo, para permitir el acceso únicamente a los objetos de un bucket denominado DOC-EXAMPLE-BUCKET3, cambie el elemento por:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

Para obtener más información y ejemplos, consulte Elementos de política JSON de IAM: Resource en la Guía del usuario de AWS Identity and Access Management.

Tras crear la política de permisos para el rol de IAM, cree el rol. Si crea el rol mediante la consola de IAM, elija Política de confianza personalizada como Tipo de entidad de confianza para el rol. Para la política de confianza que define las entidades de confianza para el rol, especifique lo siguiente.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Donde *accountId* es el ID de la cuenta de su Cuenta de AWS. Sustituya este valor por su ID de cuenta de 12 dígitos.

En la política de confianza anterior:

- El elemento `Principal` especifica la entidad principal de servicio que utiliza Macie al recuperar y revelar muestras de datos confidenciales de los objetos de S3 afectados, `reveal-samples.macie.amazonaws.com`.
- El elemento `Action` especifica la acción que la entidad principal de servicio puede llevar a cabo, la operación AssumeRole de la API de AWS Security Token Service (AWS STS).
- El elemento `Condition` define una condición que usa la clave de contexto de condición global aws:SourceAccount. Esta condición determina qué cuenta puede llevar a cabo la acción especificada. Permite a Macie asumir el rol solo para la cuenta especificada (*accountID*). La condición ayuda a evitar que Macie se utilice como un ayudante confuso durante las transacciones con AWS STS.

Tras definir la política de confianza para el rol de IAM, asocie la política de permisos al rol. Debe ser la política de permisos que creó antes de empezar a crear el rol. A continuación, complete los pasos restantes en IAM para terminar de crear y configurar el rol. Cuando termine, configure y habilite los ajustes en Macie.

Descifrado de los objetos de S3 afectados

Amazon S3 admite varias opciones de cifrado para los objetos S3. Para la mayoría de estas opciones, un rol o usuario de IAM no necesita recursos ni permisos adicionales para descifrar y recuperar muestras de datos confidenciales de un objeto afectado. Este es el caso de un objeto se cifra mediante el cifrado en el lado del servidor con una clave administrada por Amazon S3 o una AWS KMS key administrada por AWS.

Sin embargo, si un objeto de S3 se cifra con una AWS KMS key administrada por el cliente, se requieren permisos adicionales para descifrar y recuperar muestras de datos confidenciales del objeto. Más específicamente, la política de claves de la clave de KMS debe permitir que el rol o usuario de IAM lleve a cabo la acción `kms:Decrypt`. De lo contrario, se produce un error y Macie no recupera ninguna muestra del objeto. Para obtener información sobre cómo proporcionar este acceso a un usuario de IAM, consulte Autenticación y control de acceso de AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

La forma de proporcionar este acceso a un rol de IAM depende de si la cuenta propietaria de la AWS KMS key también lo es:

- Si la misma cuenta es propietaria de la clave de KMS y del rol, el usuario de la cuenta debe actualizar la política de claves.
- Si una cuenta es propietaria de la clave de KMS y otra cuenta es propietaria del rol, el usuario de la cuenta propietaria de la clave debe permitir el acceso entre cuentas a la clave.

En este tema, se describe cómo llevar a cabo estas tareas para un rol de IAM que creó a fin de recuperar muestras de datos confidenciales de objetos de S3. También proporciona ejemplos de ambos escenarios. Para obtener información sobre cómo permitir el acceso a la AWS KMS keys administrada por el cliente en otros escenarios, consulte Autenticación y control de acceso de AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Permitir el acceso de la misma cuenta a una clave administrada por el cliente

Si la misma cuenta es propietaria tanto de la AWS KMS key como del rol de IAM, el usuario de la cuenta debe agregar una instrucción a la política de claves. La instrucción adicional debe permitir que el rol de IAM utilice la clave para descifrar los datos. Para obtener información sobre cómo modificar una política de claves, consulte Modificación de una política de claves en la AWS Key Management ServiceGuía del desarrollador.

En la declaración:

- El elemento `Principal` debe especificar el nombre de recurso de Amazon (ARN) de un rol de IAM.
- La matriz `Action` debe especificar la acción `kms:Decrypt`. Esta es la única acción de AWS KMS que el rol de IAM debe poder llevar a cabo para descifrar un objeto que se cifró con la clave.

El siguiente es un ejemplo de la instrucción para añadir a la política para una clave KMS.

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

En el ejemplo anterior:

- El campo `AWS` del elemento `Principal` especifica el ARN del rol de IAM de la cuenta. Permite que el rol lleve a cabo la acción especificada en la instrucción de la política. *123456789012* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del rol y de la clave de KMS. *IAMRoleName* es un nombre de ejemplo. Sustituya este valor por el nombre del rol de IAM en la cuenta.
- La matriz `Action` especifica la acción que el rol de IAM puede llevar a cabo mediante la clave de KMS: descifrar el texto cifrado con la clave.

El lugar donde se añada esta declaración a una política de claves depende de la estructura y los elementos que la política contenga actualmente. Cuando añada la instrucción a la política, asegúrese de que la sintaxis sea válida. Las políticas de claves utilizan formato JSON. Esto significa que también hay que añadir una coma antes o después de la declaración, en función de dónde se añada la declaración a la política.

Permitir el acceso entre cuentas a una clave gestionada por el cliente

Si una cuenta posee la AWS KMS key (propietario de la clave) y otra cuenta posee el rol de IAM (propietario del rol), el propietario de la clave tiene que proporcionar al propietario del rol el

acceso entre cuentas a la clave. Una forma de hacerlo es con una concesión. Una concesión es un instrumento de política que permite a los principales AWS utilizar claves KMS en operaciones criptográficas si se cumplen las condiciones especificadas por la subvención. Para obtener más información sobre las Concesiones en AWS KMS, consulte Subvenciones en la AWS Key Management ServiceGuía para desarrolladores.

Con este método, el propietario de la clave se asegura primero de que la política de claves permita al propietario del rol crear una concesión para ella. A continuación, el propietario del rol crea una concesión para la clave. La concesión delega los permisos pertinentes en el rol de IAM de su cuenta. Permite que el rol descifre los objetos de S3 que están cifrados con la clave.

Paso 1: actualización de la política de claves

En la política de claves, el propietario de la clave debe asegurarse de que la política incluya una instrucción que permita al propietario del rol crear una concesión para el rol de IAM en su cuenta (la del propietario del rol). En esta instrucción, el elemento `Principal` debe especificar el ARN de la cuenta del propietario del rol. La matriz `Action` debe especificar la acción `kms:CreateGrant`. Un bloqueo `Condition` puede filtrar el acceso a la acción especificada. A continuación, se muestra un ejemplo de esta declaración en la política de una clave KMS.

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
        }
    }
}
```

En el ejemplo anterior:

- El campo `AWS` del elemento `Principal` especifica el ARN de la cuenta del propietario del rol. Permite que la cuenta lleve a cabo la acción especificada en la instrucción de la política. *`111122223333`* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del rol.
- La matriz `Action` especifica la acción que el propietario del rol puede llevar a cabo en la clave de KMS: crear una concesión para la clave.
- El bloque `Condition` utiliza los operadores de condición y las siguientes claves de condición para filtrar el acceso a la acción que el propietario del rol puede llevar a cabo en la clave de KMS:
  - kms:GranteePrincipal: esta condición permite al propietario del rol crear una concesión solo para la entidad principal del beneficiario especificado, que es el ARN del rol de IAM en su cuenta. En ese ARN, *`111122223333`* es un ejemplo de ID de cuenta. Sustituya este valor por el ID de la cuenta del propietario del rol. *`IAMRoleName`* es un nombre de ejemplo. Sustituya este valor por el nombre del rol de IAM en la cuenta del propietario del rol.
  - kms:GrantOperations: esta condición permite al propietario del rol crear una concesión únicamente para delegar el permiso para llevar a cabo la acción de AWS KMS `Decrypt` (descifrar el texto cifrado que se ha cifrado con la clave). Impide que el propietario del rol cree concesiones que deleguen permisos para llevar a cabo otras acciones en la clave de KMS. La acción `Decrypt` es la única acción de AWS KMS que el rol de IAM debe poder llevar a cabo para descifrar un objeto que se cifró con la clave.

Cuando el propietario de la clave agrega esta instrucción a la política de claves, depende de la estructura y los elementos que la directiva contenga actualmente. Cuando el propietario de la clave añada la declaración, debe asegurarse de que la sintaxis sea válida. Las políticas de claves utilizan formato JSON. Esto significa que el propietario de la clave también debe añadir una coma antes o después de la declaración, dependiendo de dónde añada la declaración a la política. Para obtener información sobre cómo modificar una política de claves, consulte Modificación de una política de claves en la AWS Key Management ServiceGuía del desarrollador.

Paso 2: creación de una concesión

Una vez que el propietario de la clave actualice la política de claves según sea necesario, el propietario del rol crea una concesión para la clave. La concesión delega los permisos pertinentes en el rol de IAM de su cuenta (la del propietario del rol). Antes de que el propietario del rol cree la concesión, debe comprobar que está autorizado a llevar a cabo la acción `kms:CreateGrant`. Esta acción le permite agregar una concesión a una AWS KMS key existente administrada por el cliente.

Para crear la concesión, el propietario del rol puede usar la operación CreateGrant de la API AWS Key Management Service. Cuando el propietario del rol cree la concesión, debe especificar los siguientes valores para los parámetros necesarios:

- `KeyId`: el ARN de la clave de KMS. Para el acceso entre cuentas a una clave KMS, este valor debe ser un ARN. No puede ser una clave de ID.
- `GranteePrincipal`: el ARN del rol de IAM de su cuenta. Este valor debe ser `arn:aws:iam::`*`111122223333`*`:role/`*`IAMRoleName`*, donde *`111122223333`* es el ID de cuenta del propietario del rol e *`IAMRoleName`* es el nombre del rol.
- `Operations`: la acción de descifrado de AWS KMS (`Decrypt`). Esta es la única acción de AWS KMS que el rol de IAM debe poder llevar a cabo para descifrar un objeto que se cifró con la clave de KMS.

Si el propietario del rol usa la AWS Command Line Interface (AWS CLI), puede ejecutar el comando create-grant para crear la concesión. El siguiente ejemplo muestra cómo. El ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

Donde:

- `key-id` especifica el ARN de la clave KMS a la que se va a aplicar la concesión.
- `grantee-principal` especifica el ARN del rol de IAM que puede llevar a cabo la acción especificada en la concesión. Este valor debe coincidir con el ARN especificado en la condición `kms:GranteePrincipal` de la política de claves.
- `operations` especifica la acción que la concesión permite llevar a cabo a la entidad principal especificada: descifrar el texto cifrado que se cifró con la clave.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
```

```
}
```

Donde `GrantToken` es una cadena única, no secreta, de longitud variable, codificada en base64 que representa la concesión que se creó y `GrantId` es el identificador único de la concesión.

Configuración de Amazon Macie para recuperar y revelar muestras de datos confidenciales con resultados

Si lo desea, puede configurar y usar Amazon Macie para recuperar y revelar muestras de datos confidenciales que Macie notifica en resultados de datos confidenciales individuales. Las muestras pueden ayudarle a verificar la naturaleza de los datos confidenciales que encontró Macie. También pueden ayudarle a personalizar la investigación de un objeto y un bucket de Amazon Simple Storage Service (Amazon S3) afectados. Puede recuperar y revelar muestras de datos confidenciales en todas las Regiones de AWS que Macie está disponible actualmente, excepto las de Asia-Pacífico (Osaka) e Israel (Tel Aviv).

Al recuperar y revelar muestras de datos confidenciales para un resultados, Macie utiliza los datos del correspondiente resultado de la detección de datos confidenciales para localizar las ocurrencias de datos confidenciales en el objeto S3 afectado. A continuación, Macie extrae muestras de esas ocurrencias del objeto afectado. Macie cifra los datos extraídos con una clave AWS Key Management Service (AWS KMS) que usted especifique, almacena temporalmente los datos cifrados en una memoria caché y devuelve los datos en sus resultados para el resultado. Poco después de la extracción y el cifrado, Macie elimina permanentemente los datos de la memoria caché, a menos que se requiera una retención adicional temporal para resolver un problema operativo.

Para recuperar y revelar muestras de datos confidenciales para los resultados, primero tiene que configurar y habilitar la configuración de su cuenta de Macie. También debe configurar los recursos y permisos de ayuda para su cuenta. Los temas de esta sección le guiarán por el proceso de configuración de Macie para que recupere y revele muestras de datos confidenciales, así como por el proceso de administración del estado de la configuración de su cuenta.

Temas

> **Tip**
>
> Para ver recomendaciones y ejemplos de políticas que puede usar para controlar el acceso a esta funcionalidad, consulte la entrada del blog sobre cómo usar Amazon Macie para obtener una vista previa de datos confidenciales en buckets de S3 en el blog de seguridad de AWS.

Antes de empezar

Antes de configurar Amazon Macie para que recupere y revele muestras de datos confidenciales de los resultados, complete las siguientes tareas para garantizar que disponga de los permisos y recursos que necesita.

Tareas

- Paso 1: configuración de un repositorio para los resultados de detección de datos confidenciales
- Paso 2: elección del método de acceso a los objetos de S3 afectados
- Paso 3: configuración de una AWS KMS key
- Paso 4: verificación de los permisos

Estas tareas son opcionales si ya ha configurado Macie para que recupere y revele muestras de datos confidenciales y solo desea cambiar los ajustes de configuración.

Paso 1: configuración de un repositorio para los resultados de detección de datos confidenciales

Al recuperar y revelar muestras de datos confidenciales para un resultados, Macie utiliza los datos del correspondiente resultado de la detección de datos confidenciales para localizar las ocurrencias de datos confidenciales en el objeto S3 afectado. Por lo tanto, es importante verificar que haya configurado un repositorio para los resultados de la detección de datos confidenciales. De lo contrario, Macie no podrá localizar las muestras de datos confidenciales que desee recuperar y revelar.

Para comprobar que haya configurado este repositorio para su cuenta, puede usar la consola de Amazon Macie: elija Resultados de la detección (en Configuración) en el panel de navegación. Para hacerlo mediante programación, utilice la operación GetClassificationExportConfiguration de la API de Amazon Macie. Para obtener más información sobre los resultados de la detección de datos confidenciales y sobre cómo configurar este repositorio, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Paso 2: elección del método de acceso a los objetos de S3 afectados

Para acceder a los objetos de S3 afectados y recuperar muestras de datos confidenciales de ellos, tiene dos opciones. Puede configurar Macie para que utilice sus credenciales de usuario de AWS Identity and Access Management (IAM). O bien, puede configurar Macie para que asuma un rol de IAM que delegue el acceso a Macie. Puede utilizar cualquier configuración con cualquier tipo de cuenta de Macie: la cuenta de administrador de Macie delegada para una organización, una cuenta de miembro de Macie de una organización o una cuenta de Macie independiente. Antes de configurar los ajustes de Macie, determine qué método de acceso desea utilizar. Para obtener información detallada sobre las opciones y los requisitos de cada método, consulte Opciones de configuración y requisitos para recuperar muestras de datos confidenciales con resultados.

Si planea usar un rol de IAM, cree y configure el rol antes de configurar los ajustes en Macie. Asegúrese también de que las políticas de confianza y permisos del rol cumplan con todos los requisitos para que Macie lo asuma. Si su cuenta forma parte de una organización que administra varias cuentas de Macie de forma centralizada, consúltelo antes con su administrador de Macie para determinar si desea configurar el rol de su cuenta y cómo hacerlo.

Paso 3: configuración de una AWS KMS key

Al recuperar y revelar muestras de datos confidenciales de un resultado, Macie cifra las muestras con una clave de AWS Key Management Service (AWS KMS) que tiene que especificar. Por lo tanto, debe determinar qué AWS KMS key desea utilizar para cifrar las muestras. La clave puede ser una clave de KMS existente de su propia cuenta o una clave de KMS existente que pertenezca a otra cuenta. Si desea utilizar una clave de otra cuenta, ingrese el nombre de recurso de Amazon (ARN) de la clave. Deberá especificar este ARN cuando configure los ajustes en Macie.

La clave de KMS debe ser una clave de cifrado simétrico administrada por el cliente. También debe ser una clave de una sola región que esté habilitada en la misma región Región de AWS que su cuenta de Macie. La clave de KMS puede estar en un almacén de claves externo. Sin embargo, es posible que la clave sea más lenta y menos fiable que una clave que se gestione íntegramente dentro de AWS KMS. Si la latencia o un problema de disponibilidad impiden a Macie cifrar las muestras de datos confidenciales que desea recuperar y revelar, se produce un error y Macie no devuelve ninguna muestra para el resultado.

Además, la política de claves para la clave debe permitir a las entidades principales correspondientes (roles de IAM, usuarios de IAM oCuentas de AWS) realizar las siguientes acciones:

- `kms:Decrypt`

- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> Para tener una capa de control de acceso adicional, le recomendamos que cree también una clave KMS dedicads para el cifrado de las muestras de datos confidenciales que se recuperen y restrinja el uso de la clave únicamente a las entidades principales a las que se les debe permitir recuperar y revelar las muestras de datos confidenciales. Si a un usuario no se le permite llevar a cabo las acciones anteriores con la clave, Macie rechaza su solicitud para recuperar y revelar muestras de datos confidenciales. Macie no devuelve ninguna muestra para el resultado.

Para obtener más información sobre la creación y configuración de claves de KMS, consulte Administración de claves en la Guía para desarrolladores de AWS Key Management Service. Para obtener información sobre las políticas de claves para administrar el acceso a claves de KMS, consulte Políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Paso 4: verificación de los permisos

Antes de configurar los ajustes de Macie, compruebe también que disponga de los permisos que necesita. Para verificar sus permisos, utilice AWS Identity and Access Management (IAM) para revisar las políticas de IAM asociadas a su identidad de IAM. A continuación, compare la información de esas políticas con la siguiente lista de acciones que debe estar autorizado a realizar.

Amazon Macie

En el caso de Macie, compruebe que está autorizado a realizar las siguientes acciones:

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

La primera acción le permite acceder a su cuenta de Macie. La segunda acción le permite cambiar los ajustes de configuración de la cuenta para recuperar y revelar las muestras de datos confidenciales. Esto incluye habilitar y deshabilitar la configuración de su cuenta.

Si lo desea, compruebe que también está autorizado a realizar la acción `macie2:GetRevealConfiguration`. Esta acción le permite recuperar los ajustes de configuración actuales y el estado actual de la configuración de su cuenta.

AWS KMS

Si planea utilizar la consola de Amazon Macie para ingresar los ajustes de configuración, compruebe también que cuenta con autorización para llevar a cabo las siguientes acciones de AWS Key Management Service (AWS KMS):

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

Estas acciones le permiten recuperar información sobre las AWS KMS keys de su cuenta. A continuación, puede elegir una de estas teclas al entrar en la configuración.

IAM

Si planea configurar Macie para que asuma un rol de IAM a fin de recuperar y revelar muestras de datos confidenciales, compruebe también que cuenta con autorización para llevar a cabo la siguiente acción de IAM: `iam:PassRole`. Esta acción le permite transferir el rol a Macie, lo que a su vez le permite a Macie asumir el rol. Cuando ingrese los ajustes de configuración de su cuenta, Macie también podrá comprobar que el rol exista en esta y que esté configurado correctamente.

Si no está autorizado a realizar las acciones necesarias, pida ayuda a su administrador de AWS.

Configuración y habilitación de los ajustes de Amazon Macie

Tras comprobar que disponga de los recursos y los permisos que necesita, puede configurar los ajustes en Amazon Macie y habilitar la configuración de su cuenta.

Si su cuenta forma parte de una organización que administra varias cuentas de Macie de forma centralizada, tenga en cuenta lo siguiente antes de configurar o cambiar los ajustes de su cuenta:

- Si tiene una cuenta de miembro, consúltelo con su administrador de Macie para determinar si desea configurar los ajustes de su cuenta y cómo hacerlo. El administrador de Macie puede brindarle ayuda para determinar los ajustes de configuración correctos para su cuenta.
- Si tiene una cuenta de administrador de Macie y cambia la configuración de acceso a los objetos de S3 afectados, los cambios podrían afectar a otras cuentas y recursos de su organización.

Esto depende de si Macie está configurado actualmente para asumir un rol de AWS Identity and Access Management (IAM) a fin de recuperar muestras de datos confidenciales. Si es así y vuelve a configurar Macie para que utilice las credenciales de usuario de IAM, Macie eliminará permanentemente la configuración existente del rol de IAM: el nombre del rol y el ID externo de la configuración. Si, posteriormente, su organización decide volver a utilizar los roles de IAM, tendrá que especificar un nuevo ID externo en la política de confianza para el rol en cada cuenta de miembro correspondiente.

Para obtener más información sobre las opciones de configuración para cada tipo de cuenta, consulte Opciones de configuración y requisitos para recuperar muestras de datos confidenciales con resultados.

Para configurar los ajustes de Macie y habilitar la configuración de su cuenta, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Para configurar y habilitar los ajustes mediante la consola de Amazon Macie, siga estos pasos.

Configuración y habilitación de los ajustes de Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Utilice el selector de Región de AWS de la esquina superior derecha de la página para seleccionar la región en la que desea configurar y habilitar Macie para recuperar y revelar muestras de datos confidenciales.
3. En el panel de navegación, en Configuración, seleccione Revelar muestras.
4. En la sección Settings (Configuración), elija Editar.
5. Para Status (Estado), elija Enabled (Habilitado).
6. En Acceso, especifique el método de acceso y la configuración que desee utilizar al recuperar muestras de datos confidenciales de los objetos de S3 afectados:

   - Para usar un rol de IAM que delegue el acceso a Macie, elija Asumir un rol de IAM. Si elige esta opción, Macie asume el rol de IAM que creó y configuró en su Cuenta de AWS para recuperar las muestras. En el recuadro Nombre de función, ingrese el nombre del rol.
   - Para usar las credenciales del usuario de IAM que solicita las muestras, elija Usar credenciales de usuario de IAM. Si elige esta opción, cada usuario de su cuenta utilizará su identidad de IAM individual para recuperar las muestras.

7. En Cifrado, especifique la clave de AWS KMS key que desea utilizar para cifrar las muestras de datos confidenciales que se recuperan:

   - Para usar una clave de su propia cuenta, elija Seleccionar una clave de la cuenta. Luego, en la lista AWS KMS key, seleccione la clave que desea usar. La lista muestra las claves KMS de cifrado simétrico para su cuenta.
   - Para usar una clave de KMS que pertenezca a otra cuenta, seleccione Ingrese el ARN de una clave de otra cuenta. A continuación, en el cuadro AWS KMS keyARN, introduzca el nombre de recurso de Amazon (ARN) de la clave de que se debe utilizar, como por ejemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.

8. Cuando termine con la configuración, elija Guardar.

Macie prueba la configuración para verificar que sea correcta. Si ha configurado Macie para que asuma un rol de IAM, Macie también comprueba que el rol exista en su cuenta y que las políticas de confianza y permisos estén configuradas correctamente. Si hay algún problema, Macie muestra un mensaje que describe el problema.

Para solucionar un problema relacionado con AWS KMS key, consulte los requisitos del tema anterior y especifique una clave de KMS que cumpla con los requisitos. Para solucionar un problema relacionado con el rol de IAM, comience por comprobar que haya ingresado el nombre correcto del rol. Si el nombre es correcto, asegúrese de que las políticas del rol cumplan con todos los requisitos para que Macie lo asuma. Para obtener estos detalles, consulte Configuración de un rol de IAM para obtener acceso a los objetos de S3 afectados. Puede guardar y habilitar la configuración cuando solucione los problemas.

> **Note**
>
> Si es el administrador de Macie de una organización y ha configurado Macie para que asuma un rol de IAM, Macie generará y mostrará un identificador externo después de guardar la configuración de su cuenta. Anote este ID. La política de confianza del rol de IAM de cada una de sus cuentas de miembro correspondientes debe especificar este ID. De lo contrario, no podrá recuperar muestras de datos confidenciales de los objetos de S3 de las cuentas.

API

Para configurar y habilitar los ajustes mediante programación, use la operación UpdateRevealConfiguration de la API de Amazon Macie. En la solicitud, especifique los valores apropiados para los parámetros admitidos:

- En cuanto a los parámetros `retrievalConfiguration`, especifique el método de acceso y la configuración que quiera utilizar al recuperar muestras de datos confidenciales de los objetos de S3 afectados:
  - Para asumir un rol de IAM que delegue el acceso a Macie, especifique `ASSUME_ROLE` en el parámetro `retrievalMode` y especifique el nombre del rol para el parámetro `roleName`. Si especifica esta configuración, Macie asume el rol de IAM que creó y configuró en su Cuenta de AWS para recuperar las muestras.
  - Para usar las credenciales del usuario de IAM que solicita las muestras, especifique `CALLER_CREDENTIALS` para el parámetro `retrievalMode`. Si especifica esta configuración, cada usuario de su cuenta utilizará su identidad de IAM individual para recuperar las muestras.

  > **Important**
  >
  > Si no especifica valores para estos parámetros, Macie establece el método de acceso (`retrievalMode`) en `CALLER_CREDENTIALS`. Si Macie está configurado actualmente para usar un rol de IAM para recuperar las muestras, Macie también eliminará permanentemente el nombre del rol actual y el ID externo de su configuración. Para conservar estos ajustes para una configuración existente, incluya los parámetros `retrievalConfiguration` en su solicitud y especifique la configuración actual para esos parámetros. Para recuperar la configuración actual, utilice la operación GetRevealConfiguration o, si usa AWS Command Line Interface (AWS CLI), ejecute el comando get-reveal-configuration.

- En el parámetro `kmsKeyId`, especifique la AWS KMS key que quiera usar para cifrar muestras de datos confidenciales que se recuperan:
  - Para usar una clave de KMS de su propia cuenta, especifique el nombre de recurso de Amazon (ARN), ID o alias de la clave. Si especifica un alias, incluya el prefijo de `alias/`, por ejemplo, `alias/ExampleAlias`.
  - Para usar una clave KMS que sea propiedad de otra cuenta, especifique el ARN de la clave, por ejemplo, `arn:aws:kms:us-`

`east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. O bien, especifique el ARN del alias de la clave, por ejemplo, `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`.

- Para el parámetro `status`, especifique `ENABLED` si desea habilitar la configuración de su cuenta de Macie.

En su solicitud, asegúrese también de especificar la Región de AWS donde desea activar y utilizar la configuración.

Para configurar y habilitar los ajustes mediante la AWS CLI, ejecute el comando update-reveal-configuration y especifique los valores adecuados para los parámetros admitidos. Por ejemplo, si está utilizando la AWS CLI en Microsoft Windows, ejecute el siguiente comando:

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

Donde:

- *us-east-1* es la región en la que se habilitará y utilizará la configuración. En este ejemplo, la region Este de EE. UU. (Norte de Virginia)
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias* es el ARN del alias que debe utilizar la clave de AWS KMS key. En este ejemplo, la clave pertenece a otra cuenta.
- El estado de la configuración es `ENABLED`.
- *ASSUME_ROLE* es el método de acceso que se debe utilizar. En este ejemplo, asuma el rol de IAM especificado.
- *MacieRevealRole* es el nombre del rol de IAM que Macie debe asumir al recuperar muestras de datos confidenciales.

En el ejemplo anterior, se utiliza el carácter de continuación de línea de marca de inserción (^) para mejorar la legibilidad.

Al enviar la solicitud, Macie comprueba la configuración. Si ha configurado Macie para que asuma un rol de IAM, Macie también comprueba que el rol exista en su cuenta y que las políticas de

confianza y permisos estén configuradas correctamente. Si se produce un problema, la solicitud fallará y Macie devolverá un mensaje que describe el problema. Para solucionar un problema relacionado con AWS KMS key, consulte los requisitos del tema anterior y especifique una clave de KMS que cumpla con los requisitos. Para solucionar un problema relacionado con el rol de IAM, comience por comprobar que haya especificado el nombre correcto del rol. Si el nombre es correcto, asegúrese de que las políticas del rol cumplan con todos los requisitos para que Macie lo asuma. Para obtener estos detalles, consulte Configuración de un rol de IAM para obtener acceso a los objetos de S3 afectados. Después de abordar el problema, envíe la solicitud de nuevo.

Si la solicitud es correcta, Macie habilita la configuración de su cuenta en la región especificada y recibirá un resultado similar al siguiente.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Donde `kmsKeyId` especifica la AWS KMS key que se utilizará para cifrar las muestras de datos confidenciales que se recuperen y revelen y `status` es el estado de la configuración de la cuenta de Macie. Los valores de `retrievalConfiguration` especifican el método de acceso y la configuración que se utilizarán al recuperar las muestras.

> **Note**
>
> Si es el administrador de Macie de una organización y ha configurado Macie para que asuma un rol de IAM, anote el ID externo (`externalId`) en la respuesta. La política de confianza del rol de IAM de cada una de sus cuentas de miembro correspondientes debe especificar este ID. De lo contrario, no podrá recuperar muestras de datos confidenciales de los objetos de S3 afectados de las cuentas.

Para comprobar posteriormente los ajustes o el estado de la configuración de su cuenta, utilice la operación getRevealConfiguration o, para la AWS CLI, ejecute el comando get-reveal-configuration.

Deshabilitación de la configuración de Amazon Macie

Puede deshabilitar los ajustes de configuración de su cuenta de Amazon Macie en cualquier momento. Si deshabilita la configuración, Macie conserva la configuración que especifica qué AWS KMS key debe usar para cifrar las muestras de datos confidenciales que se recuperen. Macie elimina permanentemente la configuración de acceso de Amazon S3 de la configuración.

> **Warning**
>
> Al deshabilitar los ajustes de configuración de su cuenta de Macie, también elimina permanentemente la configuración actual que especifica cómo acceder a los objetos de S3 afectados. Si Macie está configurado actualmente para acceder a los objetos afectados después de asumir un rol de AWS Identity and Access Management (IAM), esto incluye el nombre del rol y el ID externo que Macie generó para la configuración. Estas configuraciones no se pueden recuperar después de eliminarlas.

Para deshabilitar los ajustes de configuración de la cuenta de Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Para deshabilitar los ajustes de configuración de la cuenta mediante la consola de Amazon Macie, siga estos pasos.

Deshabilitación de la configuración de Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Utilice el selector de Región de AWS de la esquina superior derecha de la página para seleccionar la región en la que desea desactivar los ajustes de configuración de la cuenta de Macie.
3. En el panel de navegación, en Configuración, seleccione Revelar muestras.
4. En la sección Settings (Configuración), elija Editar.
5. En Estado, elija Desactivar.

6. Elija Guardar.

API

Para desactivar la detección automatizada mediante programación, use la operación UpdateRevealConfiguration de la API de Amazon Macie. En su solicitud, asegúrese también de especificar la Región de AWS donde desea deshabilitar la configuración. En el parámetro `status`, especifique `DISABLED`.

Para deshabilitar los ajustes de configuración mediante la AWS Command Line Interface (AWS CLI), ejecute el comando update-reveal-configuration. Utilice el parámetro `region` para especificar la región en la que desea deshabilitar la configuración. En el parámetro `status`, especifique `DISABLED`. Por ejemplo, si está utilizando la AWS CLI en Microsoft Windows, ejecute el siguiente comando:

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

Donde:

- *us-east-1* es la región en la que se deshabilitará la configuración. En este ejemplo, la region Este de EE. UU. (Norte de Virginia)
- `DISABLED` es el nuevo estado de la configuración.

Si la solicitud es correcta, Macie deshabilita la configuración de su cuenta en la región especificada y recibirá un resultado similar al siguiente.

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

Donde `status` es el nuevo estado de la configuración de su cuenta de Macie.

Si Macie se configuró para asumir un rol de IAM a fin de recuperar muestras de datos confidenciales, si lo desea, puede eliminar el rol y la política de permisos de este. Macie no elimina estos recursos

cuando deshabilita los ajustes de configuración de su cuenta. Además, Macie no utiliza estos recursos para llevar a cabo ninguna otra tarea en su cuenta. Para eliminar el rol y su política de permisos, puede utilizar la consola de IAM o la API de IAM. Para obtener más información, consulte Eliminación de roles en la Guía del usuario de AWS Identity and Access Management.

Recuperación y revelación de muestras de datos confidenciales con resultados

Con Amazon Macie puede recuperar y revelar muestras de datos confidenciales que Macie notifica en resultados de datos confidenciales individuales. Esto incluye los datos confidenciales que Macie detecta mediante identificadores de datos administrados y los datos que cumplen los criterios de identificadores de datos personalizados. Las muestras pueden ayudarle a verificar la naturaleza de los datos confidenciales que encontró Macie. También pueden ayudarle a personalizar la investigación de un objeto y un bucket de Amazon Simple Storage Service (Amazon S3) afectados. Puede recuperar y revelar muestras de datos confidenciales en todos los Regiones de AWS lugares donde Macie está disponible actualmente, excepto en las regiones de Asia Pacífico (Osaka) e Israel (Tel Aviv).

Si recupera y revela muestras de datos confidenciales para un hallazgo, Macie utilizará los datos del resultado del descubrimiento de datos confidenciales correspondiente para localizar las primeras 1 a 10 apariciones de datos confidenciales notificadas por el hallazgo. A continuación, Macie extrae los primeros 1 a 128 caracteres de cada ocurrencia del objeto de S3 afectado. Si el resultado indica varios tipos de datos confidenciales, Macie lo hace para un máximo de 100 tipos de datos confidenciales notificados por el resultado.

Cuando Macie extrae datos confidenciales de un objeto S3 afectado, los cifra con la clave AWS Key Management Service (AWS KMS) que usted especifique, almacena temporalmente los datos cifrados en una memoria caché y devuelve los datos incluidos en los resultados para su búsqueda. Poco después de la extracción y el cifrado, Macie elimina permanentemente los datos de la memoria caché, a menos que se requiera una retención adicional temporal para resolver un problema operativo.

Si decide recuperar y mostrar muestras de datos confidenciales para volver a encontrarlas, Macie repite el proceso de localización, extracción, cifrado, almacenamiento y, en última instancia, eliminación de las muestras.

Para ver una demostración de cómo puede recuperar y revelar muestras de datos confidenciales mediante la consola Amazon Macie, vea el siguiente vídeo: Recuperación y revelación de muestras de datos confidenciales con Amazon Macie.

Temas

Antes de empezar

Para recuperar y revelar muestras de datos confidenciales de los resultados, antes tiene que configurar y activar los ajustes de su cuenta de Amazon Macie. También debe trabajar con su AWS administrador para comprobar que dispone de los permisos y los recursos que necesita.

Al recuperar y revelar muestras de datos confidenciales de un resultado, Macie lleva a cabo una serie de tareas para localizar, recuperar, cifrar y revelar las muestras. Macie no utiliza el rol vinculado al servicio de Macie en su cuenta para realizar estas tareas. En su lugar, utiliza su identidad AWS Identity and Access Management (de IAM) o permite que Macie asuma una función de IAM en su cuenta.

Para recuperar y revelar muestras de datos confidenciales para realizar un hallazgo, debe tener acceso al hallazgo, al resultado correspondiente de la detección de datos confidenciales y al material que ha configurado a Macie para AWS KMS key que lo utilice para cifrar las muestras de datos confidenciales. Además, usted o el rol de IAM deben tener permiso para acceder al bucket de S3 y al objeto de S3 afectados. Usted o el rol también deben poder usar el AWS KMS key que se utilizó para cifrar el objeto afectado, si corresponde. Si alguna política de IAM, política de recursos u otra configuración de permisos le deniega el acceso necesario, se produce un error y Macie no devuelve ninguna muestra para el resultado.

También debe tener permiso para realizar las siguientes acciones de Macie:

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

Las tres primeras acciones le permiten acceder a su cuenta de Macie y recuperar los detalles de los resultados. La última acción le permite recuperar y revelar muestras de datos confidenciales de los resultados.

Para utilizar la consola de Amazon Macie a fin de recuperar y revelar muestras de datos confidenciales, también debe poder llevar a cabo la siguiente acción: `macie2:GetSensitiveDataOccurrencesAvailability`. Esta acción le permite determinar si hay muestras disponibles para cada resultado individual. No necesita permiso para realizar esta acción para recuperar y mostrar muestras mediante programación. Sin embargo, tener este permiso puede agilizar la recuperación de muestras.

Si es el administrador delegado de Macie en una organización y ha configurado Macie para que asuma un rol de IAM a fin de recuperar muestras de datos confidenciales, también debe poder llevar a cabo la siguiente acción: `macie2:GetMember`. Esta acción le permite recuperar información sobre la asociación entre su cuenta y la cuenta afectada. Permite a Macie comprobar que usted es actualmente el administrador de Macie de la cuenta afectada.

Si no se le permite realizar las acciones necesarias ni acceder a los datos y recursos necesarios, solicite ayuda a su AWS administrador.

Determinación de si hay muestras de datos confidenciales disponibles de un resultado

Para recuperar y revelar muestras de datos confidenciales para un resultado, el resultado debe cumplir ciertos criterios. Debe incluir datos de ubicación para ocurrencias específicas de datos confidenciales. Además, debe especificar la ubicación de un resultado de detección de datos confidenciales válido y correspondiente. El resultado del descubrimiento de datos confidenciales debe almacenarse en el mismo lugar que Región de AWS el hallazgo. Si configuró Amazon Macie para acceder a los objetos S3 afectados asumiendo una función AWS Identity and Access Management (IAM), el resultado del descubrimiento de datos confidenciales también debe almacenarse en un objeto S3 que Macie haya firmado con un código de autenticación de mensajes (HMAC) basado en Hash. AWS KMS key

El objeto S3 afectado también debe cumplir ciertos criterios. El tipo de MIME del objeto debe ser uno de los siguientes:

- application/avro, para un contenedor de objetos Apache Avro (.avro)
- application/gzip, para un archivo comprimido GNU Zip (.gz or .gzip)
- application/json, para un archivo JSON o líneas JSON (.json o .jsonl)
- application/parquet, para un archivo Apache Parquet (.parquet)
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, para un archivo de libro de Microsoft Excel (.xlsx)

- application/zip, para un archivo comprimido ZIP (.zip)
- text/csv, para un archivo CSV (.csv)
- text/plain, para un archivo de texto no binario que no sea CSV, JSON, JSON Lines o TSV
- text/tab-separated-values, para un archivo TSV (.tsv)

Además, el contenido del objeto de S3 debe ser el mismo que cuando se creó el resultado. Macie comprueba la etiqueta de entidad (ETag) del objeto para determinar si coincide con la ETag especificada por el resultado. Además, el tamaño de almacenamiento del objeto no puede superar la cuota de tamaño aplicable para recuperar y revelar muestras de datos confidenciales. Para obtener una lista de las cuotas aplicables, consulte Cuotas de Amazon Macie.

Si un resultado y el objeto S3 afectado cumplen los criterios anteriores, hay disponibles muestras de datos confidenciales para el resultado. Si lo desea, puede determinar si este es el caso de un resultado concreto antes de intentar recuperar y revelar muestras para el resultado.

Determinar si hay muestras de datos confidenciales disponibles para un resultado.

Puede utilizar la consola de Amazon Macie o la API de Amazon Macie para determinar si hay muestras de datos confidenciales disponibles para un resultado.

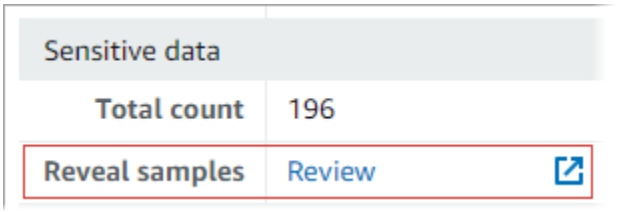
Console

Siga estos pasos en la consola de Amazon Macie para determinar si hay muestras de datos confidenciales disponibles para un resultado.

Determinar si hay muestras disponibles para un resultado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (resultados).
3. En la página Resultados, elija el resultado. El panel de detalles muestra información sobre el resultado.
4. En el panel de detalles, desplácese hasta la sección Datos confidenciales. A continuación, consulte el campo Revelar muestras.

   Si hay muestras de datos confidenciales disponibles para el resultado, aparece un enlace Revisar en el campo, como se muestra en la siguiente imagen.



Si las muestras de datos confidenciales no están disponibles para el resultado, el campo Revelar muestras muestra un texto que indica el motivo:

- La cuenta no está en la organización: no se le permite acceder al objeto de S3 afectado mediante Macie. La cuenta afectada no forma parte de la organización en estos momentos. O bien, la cuenta forma parte de la organización, pero Macie no está habilitado para la cuenta en la Región de AWS actual.
- Resultado de clasificación no válido: no hay un resultado de detección de datos confidenciales para el resultado. O bien, el resultado de la detección de datos confidenciales correspondiente no está disponible en la versión actual Región de AWS, tiene un formato incorrecto o está dañado, o utiliza un formato de almacenamiento no compatible. Macie no puede verificar la ubicación de los datos confidenciales que desea recuperar.
- Firma de resultado no válida: el resultado de la detección de datos confidenciales correspondiente se almacena en un objeto de S3 que Macie no firmó. Macie no puede verificar la integridad y autenticidad del resultado de la detección de datos confidenciales. Por lo tanto, Macie no puede verificar la ubicación de los datos confidenciales que desea recuperar.
- Rol de miembro demasiado permisivo: la política de confianza o permisos del rol de IAM en la cuenta de miembro afectada no cumple con los requisitos de Macie para restringir el acceso al rol. O bien, la política de confianza del rol no especifica el ID externo correcto para su organización. Macie no puede asumir el rol para recuperar los datos confidenciales.
- Falta GetMember el permiso: no está autorizado a recuperar información sobre la asociación entre su cuenta y la cuenta afectada. Macie no puede determinar si tiene permiso para acceder al objeto de S3 afectado como administrador delegado de Macie de la cuenta afectada.
- El objeto supera la cuota de tamaño: el tamaño de almacenamiento del objeto de S3 afectado supera la cuota de tamaño necesaria para recuperar y revelar muestras de datos confidenciales de ese tipo de archivo.

- Objeto no disponible: el objeto de S3 afectado no está disponible. Se cambió el nombre del objeto, se movió o se eliminó, o su contenido cambió después de que Macie creara el resultado. O bien, el objeto está cifrado con una AWS KMS key que está deshabilitada actualmente.
- Resultado no firmado: el resultado de la detección de datos confidenciales correspondiente se almacena en un objeto de S3 que no se ha firmado. Macie no puede verificar la integridad y autenticidad del resultado de la detección de datos confidenciales. Por lo tanto, Macie no puede verificar la ubicación de los datos confidenciales que desea recuperar.
- Rol demasiado permisivo: la cuenta está configurada para recuperar instancias de datos confidenciales mediante un rol de IAM cuya política de confianza o permisos no cumple con los requisitos de Macie para restringir el acceso a ese rol. Macie no puede asumir el rol para recuperar los datos confidenciales.
- Tipo de objeto no admitido: el objeto de S3 afectado utiliza un formato de archivo o almacenamiento que Macie no admite para recuperar y revelar muestras de datos confidenciales. El tipo MIME del objeto de S3 afectado no es uno de los valores de la lista anterior.

Si hay algún problema con el resultado de la detección de datos confidenciales, la información del campo Ubicación detallada de los resultados del resultado puede ser de ayuda para investigar el problema. Este campo especifica la ruta original al resultado en Amazon S3. Para investigar un problema relacionado con un rol de IAM, asegúrese de que las políticas del rol cumplan todos los requisitos para que Macie asuma ese rol. Para obtener estos detalles, consulte Configuración de un rol de IAM para obtener acceso a los objetos de S3 afectados.

API

Para determinar mediante programación si hay muestras de datos confidenciales disponibles para realizar una búsqueda, utilice el GetSensitiveDataOccurrencesAvailabilityfuncionamiento de la API Amazon Macie. Cuando envíe su solicitud, utilice el parámetro `findingId` para especificar el identificador único del resultado. Para obtener este identificador, puede utilizar la operación. ListFindings

Si utiliza AWS Command Line Interface (AWS CLI), ejecute el comando get-sensitive-data-occurrences-availability y utilice el `finding-id` parámetro para especificar el identificador único de la búsqueda. Para obtener este identificador, puede ejecutar el comando list-findings.

Si su solicitud es correcta y hay muestras disponibles para la búsqueda, verá un resultado similar al siguiente:

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

Si la solicitud es correcta y no hay muestras disponibles para el resultado, el valor del campo `code` campo es `UNAVAILABLE` y la matriz `reasons` especificará el motivo. Por ejemplo:

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

Si hay algún problema con el resultado de la detección de datos confidenciales, la información del campo `classificationDetails.detailedResultsLocation` del resultado puede ser de ayuda para investigar el problema. Este campo especifica la ruta original al resultado en Amazon S3. Para investigar un problema relacionado con un rol de IAM, asegúrese de que las políticas del rol cumplan todos los requisitos para que Macie asuma ese rol. Para obtener estos detalles, consulte Configuración de un rol de IAM para obtener acceso a los objetos de S3 afectados.

Recuperación y revelación de muestras de datos confidenciales de un resultado

Para recuperar y revelar muestras de datos confidenciales para un resultado, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

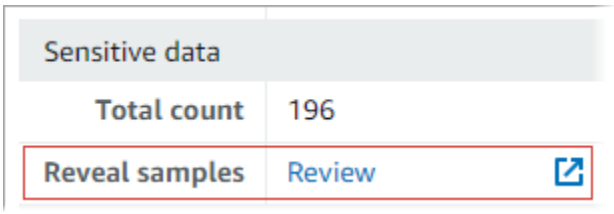
Console

Siga estos pasos para recuperar y revelar muestras de datos confidenciales para un resultado mediante la consola Amazon Macie.

Recuperación y revelación de muestras de datos confidenciales para un resultado

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (resultados).

3. En la página Resultados, elija el resultado. El panel de detalles muestra información sobre el resultado.
4. En el panel de detalles, desplácese hasta la sección Datos confidenciales. A continuación, en el campo Revelar muestras, seleccione Revisar:

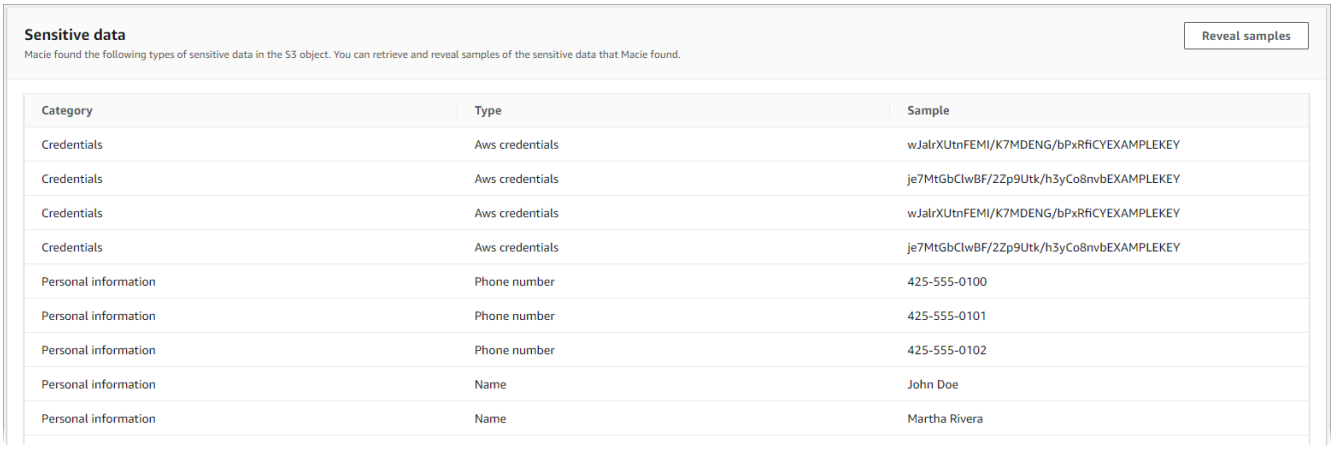


> **Note**
>
> Si el enlace Revisar no aparece en el campo Revelar muestras, las muestras de datos confidenciales no estarán disponibles para el resultado. Para obtener información acerca de por qué es así, consulte el tema anterior.

Tras seleccionar Revisar, Macie mostrará una página en la que se resumen los detalles clave del resultado. Los detalles incluyen las categorías, los tipos y el número de ocurrencias de datos confidenciales que Macie encontró en el objeto S3 afectado.

5. En la sección Datos confidenciales de la página, seleccione Revelar muestras. Macie recupera y revela muestras de las primeras instancias (10 como máximo) de datos confidenciales registradas por el resultado. Cada muestra contiene los primeros 1 a 128 caracteres de una ocurrencia de datos confidenciales. Puede tardar varios minutos en recuperar y revelar las muestras.

   Si el resultado indica varios tipos de datos confidenciales, Macie lo hace para un máximo de 100 tipos. Por ejemplo, en la siguiente imagen se muestran ejemplos que abarcan varias categorías y tipos de datos confidenciales:AWS credenciales, números de teléfono de EE. UU. y nombres de personas.



Las muestras se organizan primero por categoría de datos confidenciales y, después, por tipo de información confidencial.

API

Para recuperar y revelar muestras de datos confidenciales para encontrarlos mediante programación, utilice la GetSensitiveDataOccurrencesoperación de la API Amazon Macie. Cuando envíe su solicitud, utilice el parámetro `findingId` para especificar el identificador único del resultado. Para obtener este identificador, puede utilizar la operación. ListFindings

Para recuperar y revelar muestras de datos confidenciales mediante AWS Command Line Interface (AWS CLI), ejecute el get-sensitive-data-occurrencescomando y utilice el `finding-id` parámetro para especificar el identificador único del hallazgo. Por ejemplo:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

Donde *1f1c2d74db5d8caa76859ec52example* es el identificador único del resultado. Para obtener este identificador mediante el AWS CLI, puede ejecutar el comando list-findings.

Si su solicitud es correcta, Macie empezará a procesarla y verá un resultado similar al siguiente:

```
{
    "status": "PROCESSING"
}
```

Puede tardar varios minutos en crear su plantilla. Espere unos minutos y después envíe la solicitud de nuevo.

Si Macie puede localizar, recuperar y cifrar las muestras de datos confidenciales, Macie las devuelve en un mapa de `sensitiveDataOccurrences`. El mapa especifica de 1 a 100 tipos de datos confidenciales reportados por el resultado y, para cada tipo, de 1 a 10 muestras. Cada muestra contiene los primeros 1 a 128 caracteres de una ocurrencia de datos confidenciales notificados por el resultado.

En el mapa, cada clave es el ID del identificador de datos administrados que detectó los datos confidenciales o el nombre y el identificador único del identificador de datos personalizado que detectó los datos confidenciales. Los valores son muestras del identificador de datos administrados o del identificador de datos personalizado especificado. Por ejemplo, la siguiente respuesta proporciona tres ejemplos de nombres de personas y dos ejemplos de claves de acceso AWS secretas detectadas por los identificadores de datos gestionados (`NAME`y`AWS_CREDENTIALS`, respectivamente).

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

Si la solicitud es válida, pero no hay muestras de datos confidenciales disponibles para el resultado, recibirá un mensaje `UnprocessableEntityException` en el que se le indicará por qué las muestras no están disponibles. Por ejemplo:

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

En el ejemplo anterior, Macie intentó recuperar muestras del objeto de S3 afectado, pero el objeto ya no está disponible. El contenido del objeto cambió después de que Macie creara el resultado.

Si la solicitud es correcta, pero otro tipo de error ha impedido que Macie recupere y muestre muestras de datos confidenciales para el resultado, recibirá un resultado similar al siguiente:

```
{
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

El valor del campo `status` es `ERROR` y el campo `error` describe el error que se ha producido. La información del tema anterior puede ser de ayuda para solucionar el error.

Esquema JSON para ubicaciones de datos confidenciales

Amazon Macie utiliza estructuras JSON estandarizadas para almacenar información sobre los lugares en los que encuentra datos confidenciales de los objetos de Amazon Simple Storage Service (Amazon S3). Las estructuras se utilizan para hallar datos confidenciales y para los resultados de la detección de datos confidenciales. En el caso de los hallazgos de datos confidenciales, las estructuras forman parte del esquema JSON para los hallazgos. Si desea revisar el esquema JSON completo para ver los hallazgos, consulte Hallazgos en la Referencia de la API de Amazon Macie. Para obtener más información sobre los resultados de la detección de datos confidenciales, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Temas

- Descripción general del esquema JSON para ubicaciones de datos confidenciales

- Detalles y ejemplos del esquema JSON para ubicaciones de datos confidenciales

Descripción general del esquema JSON para ubicaciones de datos confidenciales

Para informar de la ubicación de los datos confidenciales que Amazon Macie ha encontrado en un objeto S3 afectado, el esquema JSON del hallazgo de datos confidenciales y los resultados de la detección de datos confidenciales incluye un objeto `customDataIdentifiers` y `sensitiveData`. El objeto `customDataIdentifiers` proporciona detalles sobre los datos que Macie ha detectado mediante identificadores de datos personalizados. El objeto `sensitiveData` proporciona detalles sobre los datos que Macie ha detectado mediante identificadores de datos gestionados.

Cada objeto `customDataIdentifiers` y `sensitiveData` contiene una o más matrices de `detections`:

- En un objeto `customDataIdentifiers`, la matriz de `detections` indica qué identificadores de datos personalizados han detectado los datos y producido el hallazgo. La matriz también indica el número de apariciones de los datos que ha detectado cada identificador de datos personalizado. También puede indicar la ubicación de los datos que ha detectado el identificador.
- En un objeto `sensitiveData`, la matriz de `detections` indica los tipos de datos confidenciales que Macie ha detectado mediante identificadores de datos gestionados. Para cada tipo de datos confidenciales, la matriz también indica el número de apariciones de los datos y puede especificar su ubicación.

Para el hallazgo de datos confidenciales, una matriz de `detections` puede incluir de 1 a 15 objetos `occurrences`. Cada objeto `occurrences` especifica la ubicación en la que Macie ha detectado las apariciones individuales de un tipo específico de datos confidenciales.

Por ejemplo, la siguiente matriz de `detections` indica la ubicación de tres apariciones de datos confidenciales (números de la Seguridad Social de EE. UU.) que Macie encontró en un archivo CSV.

```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
```

```
                {
                   "cellReference": null,
                   "column": 1,
                   "columnName": "SSN",
                   "row": 2
                },
                {
                   "cellReference": null,
                   "column": 1,
                   "columnName": "SSN",
                   "row": 3
                },
                {
                   "cellReference": null,
                   "column": 1,
                   "columnName": "SSN",
                   "row": 4
                }
             ]
          },
          "type": "USA_SOCIAL_SECURITY_NUMBER"
       }
```

La ubicación y el número de objetos `occurrences` de una matriz de `detections` varían en función de las categorías, los tipos y el número de apariciones de datos confidenciales que Macie detecte durante un ciclo de análisis automatizado de detección de datos confidenciales o durante la ejecución de un trabajo de detección de datos confidenciales. Para cada ciclo de análisis o ejecución del trabajo, Macie utiliza un algoritmo de búsqueda en profundidad para rellenar los hallazgos resultantes con datos de la ubicación que correspondan a las apariciones de la 1 a la 15 de datos confidenciales que Macie detecta en los objetos de S3. Estas ocurrencias indican las categorías y los tipos de datos confidenciales que pueden contener un bucket y un objeto de S3 afectados.

Un objeto `occurrences` puede contener cualquiera de las siguientes estructuras, según el tipo de archivo o el formato de almacenamiento del objeto de S3 afectado:

- Matriz de `cells`: esta matriz se aplica a los libros de trabajo, archivos CSV y archivos TSV de Microsoft Excel. El objeto de esta matriz especifica una celda o un campo en el que Macie detectó una aparición de datos confidenciales.
- Matriz de `lineRanges`: esta matriz se aplica a los archivos de mensajes de correo electrónico (EML) y a los archivos de texto no binarios distintos de los archivos CSV, JSON, JSON Lines y TSV, por ejemplo, los archivos HTML, TXT y XML. Un objeto de esta matriz especifica una línea o

un rango inclusivo de líneas en el que Macie ha detectado la presencia de datos confidenciales y la posición de los datos en la línea o líneas especificadas.

En algunos casos, el objeto de una matriz de `lineRanges` especifica la ubicación de una detección de datos confidenciales en un tipo de archivo o formato de almacenamiento compatible con otro tipo de matriz. Estos casos son: detección en una sección no estructurada de un archivo estructurado de otro modo, como un comentario en un archivo; detección en un archivo con formato incorrecto que Macie analiza como texto sin formato; y un archivo CSV o TSV que tiene uno o más nombres de columna en los que Macie detectó datos confidenciales.

- Matriz de `offsetRanges`: esto se reserva para un uso ulterior. Si esta matriz está presente, su valor es nulo.
- Matriz de `pages`: esta matriz se aplica a los archivos en formato de documento portátil (PDF) de Adobe. El objeto de esta matriz especifica una página en la que Macie detectó una aparición de datos confidenciales.
- Matriz de `records`: esta matriz se aplica a los contenedores de objetos Apache Avro, a los archivos Apache Parquet, a los archivos JSON y a los archivos JSON Lines. En el caso de los contenedores de objetos Avro y los archivos Parquet, el objeto de esta matriz especifica un índice de registros y la ruta al campo de un registro en el que Macie ha detectado la presencia de datos confidenciales. En el caso de los archivos JSON y JSON Lines, el objeto de esta matriz especifica la ruta al campo o a la matriz en los que Macie ha detectado la presencia de datos confidenciales. En el caso de los archivos JSON Lines, también especifica el índice de la línea que contiene los datos.

El contenido de estas matrices varía en función del tipo de archivo o formato de almacenamiento del objeto S3 afectado y de su contenido.

Detalles y ejemplos del esquema JSON para ubicaciones de datos confidenciales

Amazon Macie personaliza el contenido de las estructuras JSON que utiliza para indicar dónde detectó datos confidenciales en tipos específicos de archivos y contenido. En los siguientes temas se explican estas estructuras y se proporcionan ejemplos de ellas.

Temas

- Matriz de registros

Para obtener una lista completa de las estructuras de JSON que se pueden incluir en un hallazgo de datos confidenciales, consulte Hallazgos en la Referencia de la API de Amazon Macie.

Matriz de celdas

Se aplica a: libros de trabajo de Microsoft Excel, archivos CSV y archivos TSV

El objeto `cells` de una matriz de `Cell` especifica una celda o un campo en el que Macie detectó una aparición de datos confidenciales. En la siguiente tabla se describe el propósito de cada campo del objeto `Cell`.

Campo	Tipo	Descripción
`cellReference`	Cadena	La ubicación de la celda, como referencia completa de la celda, que contiene la ocurrencia. Este campo se aplica únicamente a los libros de Excel. Este valor es nulo para los archivos CSV y TSV.
`column`	Entero	El número de la columna que contiene la ocurrencia. En un libro de Excel, este valor se correlaciona con los caractere s alfabéticos del identificador de una columna, por ejemplo, 1 para la columna A, 2 para la columna B, etc.
`columnName`	Cadena	El nombre de la columna que contiene la ocurrencia, si está disponible.
`row`	Entero	El número de la fila que contiene la ocurrencia.

El siguiente ejemplo muestra la estructura de un objeto `Cell` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un archivo CSV.

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

En el ejemplo anterior, el hallazgo indica que Macie detectó datos confidenciales en el campo de la quinta fila de la tercera columna (denominada SSN) del archivo.

El siguiente ejemplo muestra la estructura de un objeto `Cell` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un libro de trabajo de Excel.

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

En el ejemplo anterior, el hallazgo indica que Macie detectó datos confidenciales en la hoja de trabajo denominada Sheet2 del libro de trabajo. En esa hoja de trabajo, Macie detectó datos confidenciales en la celda de la quinta fila de la tercera columna (columna C, denominada SSN).

Matriz LineRanges

Se aplica a: los archivos de mensajes de correo electrónico (EML) y a los archivos de texto no binarios distintos de los archivos CSV, JSON, JSON Lines y TSV, por ejemplo, los archivos HTML, TXT y XML

Un objeto de `lineRanges` de esta matriz `Range` especifica una línea o un rango inclusivo de líneas en el que Macie ha detectado la presencia de datos confidenciales y la posición de los datos en la línea o líneas especificadas.

Este objeto suele estar vacío en los tipos de archivos que son compatibles con otros tipos de matrices en objetos `occurrences`. Las excepciones son:

- Datos en secciones no estructuradas de un archivo estructurado de otro modo, como el comentario de un archivo.
- Datos de un archivo con formato incorrecto que Macie analiza como texto sin formato.
- Un archivo CSV o TSV que tiene uno o más nombres de columna en los que Macie detectó datos confidenciales.

En la siguiente tabla se describe el propósito de cada campo del objeto `Range` de una matriz de `lineRanges`.

Campo	Tipo	Descripción
`end`	Entero	El número de líneas desde el principio del archivo hasta el final de la ocurrencia.
`start`	Entero	El número de líneas desde el principio del archivo hasta el principio de la ocurrencia.
`startColumn`	Entero	El número de caracteres, con espacios y empezando por 1, desde el principio de la primera línea que contiene la ocurrencia (`start`) hasta el principio de la misma.

El siguiente ejemplo muestra la estructura de un objeto `Range` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en una única línea de un archivo TXT.

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
```

```
   }
]
```

En el ejemplo anterior, el resultado indica que Macie detectó una ocurrencia completa de datos confidenciales (una dirección postal) en la primera línea del archivo. El primer carácter de la aparición está a 119 caracteres (con espacios) del principio de esa línea.

El siguiente ejemplo muestra la estructura de un objeto `Range` que especifica la ubicación de una ocurrencia de datos confidenciales que abarca varias líneas de un archivo TXT.

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

En el ejemplo anterior, el hallazgo indica que Macie detectó una ocurrencia de datos confidenciales (una dirección de correo) que abarca de la línea 51 a la 54 del archivo. El primer carácter de la ocurrencia es el primer carácter de la línea 51 del archivo.

Matriz de páginas

Se aplica a: archivos en formato de documento portátil (PDF) de Adobe

El objeto `pages` de una matriz de `Page` especifica una página en la que Macie detectó una aparición de datos confidenciales. El objeto contiene un campo de `pageNumber`. El campo de `pageNumber` almacena un número entero que especifica el número de la página que contiene la ocurrencia.

El siguiente ejemplo muestra la estructura de un objeto `Page` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un archivo PDF.

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

En el ejemplo anterior, el hallazgo indica que la página 10 del archivo contiene la ocurrencia.

Matriz de registros

Se aplica a: contenedores de objetos Apache Avro, a los archivos Apache Parquet, a los archivos JSON y a los archivos JSON Lines

En el caso de un contenedor de objetos Avro o un archivo Parquet, el objeto `Record` de esta matriz de `records` especifica un índice de registros y la ruta al campo de un registro en el que Macie ha detectado la presencia de datos confidenciales. En el caso de los archivos JSON y JSON Lines,un objeto `Record` especifica la ruta al campo o a la matriz en los que Macie ha detectado la presencia de datos confidenciales. En el caso de los archivos JSON Lines, también especifica el índice de la línea que contiene la ocurrencia.

En la siguiente tabla se describe el propósito de cada campo del objeto `Record`.

Campo	Tipo	Descripción
`jsonPath`	Cadena	La ruta, como expresión de JSONPath, a la ocurrencia. En el caso de un contenedor de objetos Avro o un archivo Parquet, esta es la ruta al campo del registro (`recordIndex`) que contiene la ocurrencia. En el caso de un archivo JSON o JSON Lines, esta es la ruta al campo o matriz que contiene la ocurrencia. Si los datos son el valor de una matriz, la ruta también indica qué valor contiene la ocurrencia. Si Macie detecta datos confidenciales en el nombre de cualquier elemento de la ruta, omite el campo `jsonPath` de un objeto

Campo	Tipo	Descripción
		`Record`. Si el nombre de un elemento de la ruta supera los 240 caracteres, Macie lo trunca quitando los caractere s del principio del nombre. Si la ruta completa resultant e supera los 250 caractere s, Macie también la trunca, empezando por el primer elemento, hasta que contenga 250 caracteres o menos.
`recordIndex`	Entero	En el caso de un contenedor de objetos Avro o un archivo Parquet, el índice de registros , empezando por 0, es el registro que contiene la ocurrencia. En el caso de un archivo de líneas JSON, el índice de línea, empezando por 0, de la línea que contiene la ocurrencia. Este valor es siempre `0` para los archivos JSON.

El siguiente ejemplo muestra la estructura de un objeto `Record` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un archivo Parquet.

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

En el ejemplo anterior, el resultado indica que Macie detectó datos confidenciales en el registro del índice 7663 (número de registro 7664). En ese registro, Macie detectó datos confidenciales en el campo denominado `abcdefghijklmnopqrstuvwxyz`. La ruta JSON completa al campo del registro es `$.abcdefghijklmnopqrstuvwxyz`. El campo es un descendiente directo del objeto raíz (nivel exterior).

El siguiente ejemplo también muestra la estructura de un objeto `Record` para una ocurrencia de datos confidenciales que Macie detectó en un archivo Parquet. Sin embargo, en este ejemplo, Macie truncó el nombre del campo que contiene la ocurrencia porque supera el límite de caracteres.

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

En el ejemplo anterior, el campo es un descendiente directo del objeto raíz (nivel exterior).

En el siguiente ejemplo, también en el caso de una aparición de datos confidenciales que Macie detectó en un archivo Parquet, truncó la ruta completa del campo que la contiene. La ruta completa supera el límite de caracteres.

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

En el ejemplo anterior, el resultado indica que Macie detectó datos confidenciales en el registro del índice 2335 (número de registro 2336). En ese registro, Macie detectó datos confidenciales en el campo denominado `abcdefghijklmnopqrstuvwxyz`. La ruta JSON completa al campo del registro es:

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

El siguiente ejemplo muestra la estructura de un objeto `Record` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un archivo JSON. En este ejemplo, la ocurrencia es el valor específico de una matriz.

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

En el ejemplo anterior, el resultado indica que Macie detectó datos confidenciales en el segundo valor de una matriz denominada `key`. La matriz es un elemento secundario de un objeto denominado `access`.

El siguiente ejemplo muestra la estructura de un objeto `Record` que especifica la ubicación de una ocurrencia de datos confidenciales que Macie detectó en un archivo JSON Lines.

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

En el ejemplo anterior, el resultado indica que Macie detectó datos confidenciales en el tercer valor (línea) del archivo. En esa línea, la ocurrencia se encuentra en un campo denominado `key`, que es un elemento secundario de un objeto denominado `access`.

Supresión de resultados de Amazon Macie

Para agilizar su análisis de los resultados, puede crear y utilizar reglas de supresión. Una regla de supresión es un conjunto de criterios de filtrado basados en atributos que define los casos en los que desea que Amazon Macie archive los resultados automáticamente. Las reglas de supresión son útiles en situaciones en las que haya revisado una clase de resultados y no quiere que se le vuelva a notificar sobre ellos.

Por ejemplo, puede decidir permitir que los buckets de S3 contengan direcciones de correo, si los buckets no permiten el acceso público y cifran los objetos nuevos automáticamente con una AWS

KMS key particular. En ese caso, puede crear una regla de supresión que especifique los criterios de filtrado para los siguientes campos: Tipo de detección de datos confidenciales, Permiso de acceso público al bucket de S3 e ID de la clave KMS de cifrado del bucket de S3. La regla suprime los resultados futuros que coincidan con los criterios de filtrado.

Si suprime los resultados con una regla de supresión, Macie seguirá generando resultados para casos posteriores de datos confidenciales y posibles infracciones de las políticas que coincidan con los criterios de la regla. Sin embargo, Macie cambia automáticamente el estado de los resultados a archivado. Esto significa que los resultados no aparecen de forma predeterminada en la consola de Amazon Macie, pero permanecen en Macie hasta que caducan. Macie guarda los resultados durante 90 días.

Además, Macie no publica los resultados suprimidos en Amazon EventBridge como eventos o en AWS Security Hub. Sin embargo, Macie sigue creando y almacenando los resultados de la detección de datos confidenciales que se correlacionen con los resultados de datos confidenciales que usted suprima. Esto permite garantizar que tenga un historial inmutable de resultados de información confidencial para las auditorías o investigaciones de protección de datos que realice.

> **Note**
>
> Si su cuenta es parte de una organización que administra de forma centralizada varias cuentas de Macie, las reglas de supresión pueden funcionar de forma diferente para su cuenta. Esto depende de la categoría de resultados que desee suprimir y de si tiene una cuenta de administrador o de miembro de Macie:
>
> - Resultados de política: solo un administrador de Macie puede suprimir los resultados de política para las cuentas de la organización.
>
>   Si tiene una cuenta de administrador de Macie y crea una regla de supresión, Macie la aplicará a los resultados de política para todas las cuentas de su organización, a menos que configure la regla para excluir cuentas específicas. Si tiene una cuenta de miembro de Macie y desea suprimir los resultados de política para su cuenta, póngase en contacto con su administrador de Macie.
> - Resultados de datos confidenciales: un administrador de Macie y los miembros individuales pueden suprimir los resultados de datos confidenciales que generen sus trabajos de detección de datos confidenciales. Un administrador de Macie puede además ocultar los resultados que genere Macie al tiempo que realiza una detección automatizada de datos confidenciales para la organización.

Solo la cuenta que crea un trabajo de detección de datos confidenciales puede suprimir o acceder de otro modo a los resultados de datos confidenciales que genere el trabajo. Solo la cuenta de administrador de Macie de una organización puede suprimir o acceder de otro modo a los resultados que la detección automatizada de datos confidenciales genere para las cuentas de la organización.

Para obtener más información sobre las tareas que pueden realizar los administradores y los miembros, consulte Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

Para crear y gestionar reglas de supresión, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. En los siguientes temas se explica cómo hacerlo. En el caso de la API, los temas incluyen ejemplos de cómo realizar estas tareas mediante el AWS Command Line Interface(AWS CLI). También puede realizar estas tareas utilizando una versión actual de otra herramienta de línea de comandos AWS o un SDK AWS, o enviando solicitudes HTTPS directamente a Macie. Para obtener más información sobre las herramientas y los SDK de AWS, consulte Herramientas para crear en AWS.

Temas

Crear reglas de supresión

Antes de crear una regla de supresión, es importante tener en cuenta que no se pueden restaurar (desarchivar) los resultados que hayan suprimido mediante una regla de supresión. Sin embargo, puede revisar resultados suprimidos en la consola de Amazon Macie y acceder a los resultados suprimidos con la API de Amazon Macie.

Al crear una regla de supresión, se especifican los criterios de filtrado, un nombre y, si lo desea, una descripción de la regla. Puede crear una regla de supresión con la consola de Amazon Macie o la API de Amazon Macie.

Console

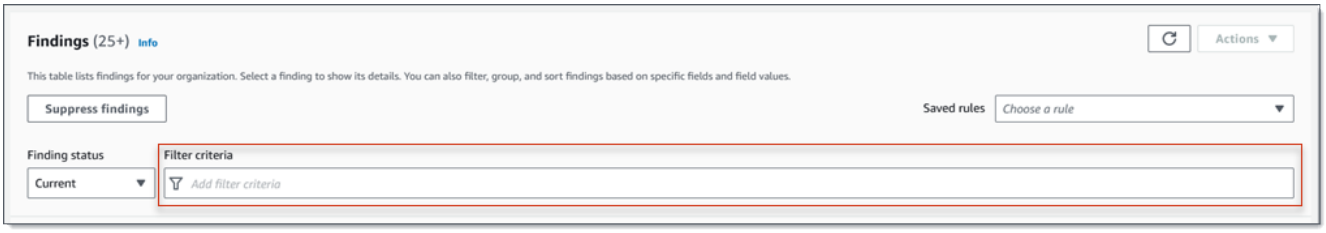
Siga estos pasos para crear una regla de supresión con la consola de Amazon Macie.

Para crear una regla de supresión

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Hallazgos).

> **Tip**
>
> Para usar una regla de supresión o filtrado existente como punto de partida, seleccione la regla de la lista de Reglas guardadas.
> También puede simplificar la creación de una regla primero centrándose y profundizando en los resultados por un grupo lógico predefinido. Si lo hace, Macie crea y aplica automáticamente las condiciones de filtrado adecuadas, lo que puede ser un punto de partida útil para crear una regla. Para ello, elija Por bucket, Por tipo o Por trabajo en el panel de navegación (en Resultados) y, a continuación, elija un elemento de la tabla. En el panel de detalles, elija el enlace para el campo en el que se va a dinamizar.

3. En el cuadro Criterios de filtrado, añada condiciones de filtrado que especifiquen los atributos de los resultados que desee que suprima la regla.



Para aprender cómo agregar condiciones de filtrado, consulte Crear y aplicar filtros a los resultados.

4. Cuando termine de agregar condiciones de filtrado a la regla, seleccione Suprimir resultados.
5. En Regla de supresión, introduzca un nombre y, opcionalmente, una descripción de la regla.
6. Seleccione Save.

API

Para crear una regla de supresión mediante programación, utilice la operación CreateFindingsFilter de la API de Amazon Macie y especifique los valores adecuados para los parámetros necesarios:

- Para el parámetro `action`, especifique el `ARCHIVE` para asegurarse de que Macie suprima los resultados que coincidan con los criterios de la regla.
- Para el parámetro `criterion`, especifique un mapa de condiciones que defina los criterios de filtrado de la regla.

  En el mapa, cada condición debe especificar un campo, un operador y uno o varios valores para el campo. El tipo y el número de valores dependen del campo y el operador que elija. Para obtener información sobre los campos, los operadores y los tipos de valores que puede usar en una condición, consulte Campos para filtrar los resultados, Uso de operadores en condiciones y Especificar valores para los campos.

Para crear una regla de supresión mediante AWS CLI, ejecute el comando create-findings-filter y especifique los valores adecuados para los parámetros necesarios. En los ejemplos siguientes se crea una regla de supresión que devuelve todos los resultados de datos confidenciales que se encuentran en el Región de AWS actual y muestra las apariciones de direcciones postales (y no de otros tipos de datos confidenciales) en los objetos de S3.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de continuación de línea de barra invertida (\) para mejorar la legibilidad.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
```

```
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

Donde:

- *my_suppression_rule* es el nombre personalizado de la regla.
- `criterion` es un mapa de las condiciones de filtro de la regla:
  - *ClassificationDetails.Result.SensitiveData.Detections.type* es el nombre en JSON del campo Tipo de detección de datos confidenciales.
  - *eqExactMatch* especifica el operador es igual a coincidencia exacta.
  - *ADDRESS* es un valor enumerado para el campo Tipo de detección de datos confidenciales.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Donde `arn` es el nombre de recurso de Amazon (ARN) de la regla de supresión que se creó y `id` es el identificador único de la regla.

Para ver ejemplos adicionales de criterios de filtrado, consulte Filtrar los resultados mediante programación con la API Amazon Macie.

Revisión de resultados suprimidos

De forma predeterminada, Macie no muestra los resultados suprimidos en la consola de Amazon Macie. Sin embargo, puedes revisar estos resultados en la consola cambiando la configuración del filtro.

Para revisar los resultados suprimidos en la consola

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Hallazgos). De forma predeterminada, en esta página se muestran los Resultados que Macie ha creado o actualizado para su cuenta en la

Región de AWS actual durante los últimos 90 días. De forma predeterminada, esto no incluye los resultados que se suprimieron mediante una regla de supresión.

3. Para el Estado del resultado, realice una de las siguientes acciones:

   - Para mostrar solo los resultados suprimidos, seleccione Archivado.
   - Para mostrar los resultados suprimidos y no suprimidos, seleccione Todos.
   - Para volver a ocultar los resultados suprimidos, seleccione Actual.

También puede acceder a los resultados suprimidos mediante la API de Amazon Macie. Para recuperar una lista de resultados suprimidos, utilice la operación ListFindings e incluya una condición de filtrado que especifique `true` para el campo `archived`. Para ver ejemplos de cómo hacerlo mediante la AWS CLI, consulte Filtrar los resultados mediante programación. Para recuperar después los detalles de uno o más resultados suprimidos, utilice la operación GetFindings y especifique el identificador único de cada resultado que desee recuperar.

Cambiar reglas de supresión

Puede cambiar la configuración de una regla de supresión en cualquier momento con la consola de Amazon Macie o la API de Amazon Macie. También puede asignar y administrar etiquetas para la regla.

Una etiqueta es una identificación que se define y se asigna a determinados tipos de recursos de AWS. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Para obtener más información, consulte Etiquetado de recursos de Amazon Macie.

Console

Para cambiar la configuración de una regla de supresión existente con la consola de Amazon Macie siga estos pasos.

Para crear una regla de supresión

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Hallazgos).

3. En la lista de Reglas guardadas, seleccione el icono de edición () situado junto a la regla de supresión que desee cambiar.
4. Realice uno de los siguientes procedimientos:
   - Para cambiar los criterios de la regla, utilice el cuadro Criterios de filtrado para introducir condiciones que especifiquen los atributos de los resultados que desea que la regla suprima. Para saber cómo hacerlo, consulte Crear y aplicar filtros a los resultados.
   - Para cambiar el nombre de la regla, introduzca un nombre nuevo en el cuadro Nombre bajo Regla de supresión.
   - Para cambiar la descripción de la regla, introduzca una nueva descripción en el cuadro Descripción bajo Regla de supresión.
   - Para asignar, revisar o editar las etiquetas de la regla, seleccione Administrar etiquetas bajo Regla de supresión. A continuación, revise y cambie las etiquetas según sea necesario. Una regla puede tener hasta 50 etiquetas.
5. Cuando termine de realizar los cambios, seleccione Save (Guardar).

API

Para cambiar una regla de supresión mediante programación, utilice la operación UpdateFindingsFilter de la API de Amazon Macie. Cuando envíe su solicitud, utilice los parámetros admitidos con el fin de especificar un nuevo valor para cada configuración que desee cambiar.

Para el parámetro `id`, especifique el identificador único de la regla que desee cambiar. Puede obtener este identificador mediante la operación ListFindingsFilter para recuperar una lista de las reglas de supresión y filtrado de su cuenta. Si utiliza AWS CLI, ejecute el comando list-findings-filters para recuperar esta lista.

Para cambiar una regla de supresión mediante AWS CLI, ejecute el comando update-findings-filter y utilice los parámetros compatibles para especificar un nuevo valor para cada configuración que desee cambiar. Por ejemplo, el comando siguiente cambia el nombre de una regla de supresión existente.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

Donde:

- *8a3c5608-aa2f-4940-b347-d1451example* es el identificador único de la regla.
- *mailing_addresses_only* es el nuevo nombre de la regla.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Donde `arn` es el nombre de recurso de Amazon (ARN) de la regla que se ha modificado y `id` es el identificador único de la regla.

Del mismo modo, en el siguiente ejemplo una regla de filtrado se convierte en una regla de supresión cambiando el valor del parámetro `action` de `NOOP` a`ARCHIVE`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

Donde:

- *8a1c3508-aa2f-4940-b347-d1451example* es el identificador único de la regla.
- *ARCHIVE* es la nueva acción que Macie realiza con los resultados que coincidan con los criterios de la regla: suprimir los resultados.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Donde `arn` es el nombre de recurso de Amazon (ARN) de la regla que se ha modificado y `id` es el identificador único de la regla.

Eliminar reglas de supresión

Puede eliminar una regla de supresión en cualquier momento con la consola de Amazon Macie o la API de Amazon Macie. Si elimina una regla de supresión, Macie dejará de suprimir los casos nuevos y posteriores de resultados que coincidan con los criterios de la regla y no supriman otras reglas. Sin embargo, tenga en cuenta que Macie podría seguir suprimiendo los resultados que esté procesando actualmente y que coincidan con los criterios de la regla.

Tras eliminar una regla de supresión, los casos nuevos y posteriores de resultados que coincidan con los criterios de la regla pasarán a tener el estado actual (no archivado). Esto significa que aparecerán de forma predeterminada en la consola Amazon Macie. Además, Macie publica estos resultados en Amazon EventBridge como eventos. Según la configuración de publicación de su cuenta, Macie también publica los resultados en AWS Security Hub.

Console

Siga estos pasos para eliminar una regla de supresión mediante la consola de Amazon Macie.

Para eliminar una regla de supresión

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Findings (Hallazgos).
3. En la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla de supresión que desee eliminar.
4. Bajo Regla de supresión, seleccione Eliminar.

API

Para eliminar una regla de supresión mediante programación, utilice la operación DeleteFindingsFilter de la API de Amazon Macie. Para el parámetro `id`, especifique el identificador único de la regla de supresión que desee eliminar. Puede obtener este identificador mediante la operación ListFindingsFilter para recuperar una lista de las reglas de supresión y filtrado de su cuenta. Si utiliza AWS CLI, ejecute el comando list-findings-filters para recuperar esta lista.

Para eliminar una regla de supresión mediante AWS CLI, ejecute el comando delete-findings-filter. Por ejemplo:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

Donde *8a3c5608-aa2f-4940-b347-d1451example* es el identificador único de la regla de supresión que se va a eliminar.

Si el comando se ejecuta correctamente, Macie devuelve una respuesta HTTP 200 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Puntuación de gravedad de los resultados de Amazon Macie

Cuando Amazon Macie genera una política o un resultado de datos confidenciales, asigna automáticamente una gravedad al resultado. La gravedad de un resultado refleja las características principales del resultado y puede ayudarle a evaluarlos y priorizarlos. La gravedad de un resultado no implica ni indica de otro modo la importancia o riesgo que un recurso afectado pueda tener para la organización.

En el caso de las conclusiones sobre políticas, la gravedad se basa en la naturaleza de un posible problema con la seguridad o la privacidad de un bucket de uso general de Amazon Simple Storage Service (Amazon S3). En el caso de los resultados de datos confidenciales, la gravedad se basa en la naturaleza y el número de casos de datos confidenciales que Macie encontró en un objeto de S3.

En Macie, la gravedad de un resultado se representa de dos maneras.

Nivel de gravedad

Se trata de una representación cualitativa de la gravedad. Los niveles de gravedad van desde Low, para los menos graves, hasta High, para los más graves.

Los niveles de gravedad aparecen directamente en la consola de Amazon Macie. También están disponibles en las representaciones JSON de los resultados en la consola de Macie, en la API de Amazon Macie y en los resultados de detección de datos confidenciales que se correlacionan con los resultados de datos confidenciales. Los niveles de gravedad también se incluyen en la búsqueda de eventos que Macie publica en Amazon EventBridge y en los hallazgos que Macie publica. AWS Security Hub

Puntuación de gravedad

Es una representación numérica de la gravedad. Las puntuaciones de gravedad van del 1 al 3 y se asignan directamente a los niveles de gravedad:

Puntuación de gravedad	Nivel de gravedad
1	Baja
2	Medio
3	Alta

Los niveles de gravedad aparecen directamente en la consola de Amazon Macie. No obstante, están disponibles en las representaciones JSON de los resultados en la consola de Macie, en la API de Amazon Macie y en los resultados de detección de datos confidenciales que se correlacionan con los resultados de datos confidenciales. Las puntuaciones de gravedad también se incluyen en la búsqueda de eventos que Macie publica en Amazon EventBridge. No se incluyen en los resultados en los que publica Macie. AWS Security Hub

Los temas de esta sección indican cómo Macie determina la gravedad de los resultados sobre políticas y datos confidenciales.

Temas

Puntuación de gravedad de los resultados sobre políticas

La gravedad de la constatación de una política se basa en la naturaleza de un posible problema con la seguridad o la privacidad de un paquete de uso general de S3. En la siguiente tabla se enumeran los niveles de gravedad que Macie asigna a cada tipo de resultado de política. Para obtener una descripción de los tipos de pasos, consulte Tipos de hallazgos.

Tipo de resultado	Nivel de gravedad
Policy:IAMUser/S3BlockPublicAccessDisabled	Alta
Policy:IAMUser/S3BucketEncryptionDisabled	Baja
Policy:IAMUser/S3BucketPublic	Alta

Tipo de resultado	Nivel de gravedad
Policy:IAMUser/S3BucketReplicatedExternally	Alta
Policy:IAMUser/S3BucketSharedExternally	Alta
Policy:IAMUser/S3BucketSharedWithCloudFront	Medio

La gravedad de un resultado de política no cambia en función del número de veces que se produzca el resultado.

Puntuación de gravedad de los resultados de datos confidenciales

La gravedad del resultado de datos confidenciales se basa en la naturaleza y el número de casos de datos confidenciales que Macie encontró en un objeto de S3. Los siguientes temas indican cómo Macie determina la gravedad de cada tipo de resultado de datos confidenciales:

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Para obtener información detallada sobre los tipos de datos confidenciales que Macie puede detectar e informar en los resultados de datos confidenciales, consulte Uso de identificadores de datos administrados y Creación de identificadores de datos personalizados.

SensitiveData:S3Object/Credentials

R: Un SensitiveDatahallazgo de S3Object/Credentials indica que un objeto de S3 contiene datos de credenciales confidenciales. Para este tipo de resultado, Macie determina la gravedad en función del tipo y el número de apariciones de los datos de credenciales que Macie encontró en el objeto.

En la siguiente tabla se indican los niveles de gravedad que Macie asigna a los resultados que notifican la aparición de datos de credenciales en un objeto de S3.

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más aparicion es
AWS clave de acceso secreta	Alta	Alta	Alta
Clave de API de Google Cloud	Alta	Alta	Alta
Encabezado de autorización básica de HTTP	Alta	Alta	Alta
Token web JSON (JWT)	Alta	Alta	Alta
Clave privada de OpenSSH	Alta	Alta	Alta
Clave privada de PGP	Alta	Alta	Alta
Clave privada del estándar de criptogra fía de clave pública (PKCS)	Alta	Alta	Alta
Clave privada PuTTY	Alta	Alta	Alta
Clave de API de Stripe	Alta	Alta	Alta

SensitiveData:S3Object/CustomIdentifier

Un objeto S3Object/ SensitiveData CustomIdentifier indica que un objeto S3 contiene texto que coincide con los criterios de detección de uno o más identificadores de datos personalizados. El objeto puede contener más de un tipo de datos confidenciales.

De forma predeterminada, Macie asigna el nivel de gravedad medio a este tipo de resultado. Si el objeto S3 contiene al menos una aparición de texto que coincide con los criterios de detección de al

menos un identificador de datos personalizado, Macie asigna automáticamente el nivel de gravedad medio al resultado. La gravedad del resultado no cambia en función del número de apariciones del texto que coincide con los criterios de un identificador de datos personalizado.

Sin embargo, la gravedad de este tipo de resultado puede variar si ha definido una configuración de gravedad personalizada para el identificador de datos personalizado que produjo el resultado. Si este es el caso, Macie determina la gravedad de la siguiente manera:

- Si el objeto S3 contiene texto que coincide con los criterios de detección de un solo identificador de datos personalizado, Macie determina la gravedad del resultado en función de la configuración de gravedad de ese identificador.
- Si el objeto S3 contiene texto que coincide con los criterios de detección de más de un identificador de datos personalizado, Macie determina la gravedad del resultado evaluando la configuración de gravedad de cada identificador de datos personalizado, determinando cuál de esas configuraciones produce la gravedad más alta y, a continuación, asignando esa gravedad más alta al resultado.

Para revisar la configuración de gravedad de un identificador de datos personalizado, elija Identificadores de datos personalizados en el panel de navegación de la consola de Amazon Macie. A continuación, elija el nombre del identificador de datos personalizado. La sección de gravedad muestra la configuración. Para obtener más información, consulte Definir la configuración de búsqueda del nivel de gravedad para los identificadores de los resultados.

SensitiveData:S3Object/Financial

R: Un resultado de S3Object/Financial indica que un objeto S3 contiene información financiera SensitiveDataconfidencial. Para este tipo de resultado, Macie determina la gravedad en función del tipo y el número de apariciones de la información financiera que Macie encontró en el objeto.

En la siguiente tabla se indican los niveles de gravedad que Macie asigna a los resultados que notifican la aparición de datos financieros en un objeto de S3.

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más aparicion es
Número de cuenta bancaria [1]	Alta	Alta	Alta

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más apariciones
Fecha de caducidad de la tarjeta	Baja	Medio	Alta
Datos de banda magnética de tarjetas de crédito	Alta	Alta	Alta
Número de tarjetas de crédito [2]	Alta	Alta	Alta
Código de verificación de tarjeta de crédito	Medio	Alta	Alta

1. Los niveles de gravedad son los mismos para cualquier tipo de número de cuenta bancaria: un número de cuenta bancaria básico (BBAN), un número de cuenta bancaria internacional (IBAN) o un número de cuenta bancaria canadiense o estadounidense.
2. Los niveles de gravedad son los mismos para los números de tarjetas de crédito que estén o no cerca de una palabra clave.

Si un resultado incluye varios tipos de información financiera en un objeto, Macie determina la gravedad del resultado calculando la gravedad de cada tipo de información financiera que Macie encontró, determinando qué tipo produce la gravedad más alta y asignando esa gravedad más alta al resultado. Por ejemplo, si Macie detecta 10 fechas de caducidad de tarjetas de crédito (nivel de gravedad medio) y 10 números de tarjetas de crédito (nivel de gravedad alto) en un objeto, Macie asigna un nivel de gravedad alto al resultado.

SensitiveData:S3Object/Personal

R: Un SensitiveDatahallazgo objeto/personal indica que un objeto S3 contiene información personal confidencial: información de salud personal (PHI), información de identificación personal (PII) o una

combinación de ambas. Para este tipo de resultado, Macie determina la gravedad en función del tipo y el número de apariciones de la información personal que Macie encontró en el objeto.

En la siguiente tabla se indican los niveles de gravedad que Macie asigna a los resultados que notifican la aparición de PHI en un objeto de S3.

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más apariciones
Número de registro de la Administración para el Control de Drogas (DEA)	Alta	Alta	Alta
Número de reclamación del seguro médico (HICN)	Alta	Alta	Alta
Número de seguro médico o identificación médica	Alta	Alta	Alta
Código del sistema de codificación de procedimientos comunes de atención médica (HCPCS)	Alta	Alta	Alta
Código nacional de medicamento (NDC)	Alta	Alta	Alta
Identificador nacional de proveedores (NPI)	Alta	Alta	Alta
Identificador único de dispositivo (UDI)	Baja	Medio	Alta

En la siguiente tabla se indican los niveles de gravedad que Macie asigna a los resultados que notifican la aparición de PII en un objeto de S3.

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más aparicion es
Fecha de nacimiento	Baja	Medio	Alta
Número de identific ación del permiso de conducir	Baja	Medio	Alta
Número de registro electoral	Alta	Alta	Alta
Nombre completo	Baja	Medio	Alta
Coordenadas del sistema de posiciona miento global (GPS)	Baja	Medio	Medio
Cookie HTTP	Baja	Medio	Alta
Dirección postal	Baja	Medio	Alta
Número de identific ación nacional	Alta	Alta	Alta
Número de seguro nacional (NINO)	Alta	Alta	Alta
Número de pasaporte	Medio	Alta	Alta
Número de residencia permanente	Alta	Alta	Alta
Número de teléfono	Baja	Medio	Alta

Tipos de datos confidenciales	1 aparición	2-99 apariciones	100 o más aparicion es
Número de Seguro Social (SIN)	Alta	Alta	Alta
Número de la Seguridad Social (SSN)	Alta	Alta	Alta
Número de identific ación o referencia del contribuyente	Alta	Alta	Alta
Número de identific ación de vehículo (VIN)	Baja	Baja	Medio

Si un resultado informa de varios tipos de PHI, PII o tanto de PHI como de PII en un objeto, Macie determina la gravedad del resultado calculando la gravedad de cada tipo, determinando qué tipo produce la gravedad más alta y asignando esa gravedad más alta al resultado.

Por ejemplo, si Macie detecta 10 nombres completos (nivel de gravedad medio) y 5 números de pasaporte (nivel de gravedad alto) en un objeto, Macie asigna un nivel de gravedad alto al resultado. Del mismo modo, si Macie detecta 10 nombres completos (nivel de gravedad medio) y 10 números de identificación del seguro médico (nivel de gravedad alto) en un objeto, Macie asigna un nivel de gravedad alto al resultado.

SensitiveData:S3Object/Multiple

R: Un SensitiveDatahallazgo de tipo S3Object/Multiple indica que un objeto S3 contiene datos que abarcan varias categorías de datos confidenciales (cualquier combinación de datos de credenciales, información financiera, información personal o texto) que coincide con los criterios de detección de uno o más identificadores de datos personalizados.

Para este tipo de resultado, Macie determina la gravedad calculando la gravedad de cada tipo de datos confidenciales que Macie encontró (como se ha indicado en los temas anteriores),

determinando qué tipo produce la gravedad más alta y asignando esa gravedad más alta al resultado.

Por ejemplo, si Macie detecta 10 nombres completos (nivel de gravedad medio) y 10 claves de acceso AWS secretas (nivel de gravedad alto) en un objeto, Macie asigna un nivel de gravedad alto al hallazgo.

Monitoreo y procesamiento de los resultados de Amazon Macie

Para facilitar la integración con otras aplicaciones, servicios y sistemas, como sistemas de monitorización o de administración de eventos, Amazon Macie publica automáticamente los resultados de datos confidenciales y políticas en Amazon EventBridge como eventos. Para obtener un análisis adicional y más amplio de la postura de seguridad de su organización, también puede publicar los resultados de datos confidenciales y políticas en AWS Security Hub.

Amazon EventBridge

Amazon EventBridge, anteriormente Eventos de Amazon CloudWatch, es un servicio de bus de eventos sin servidor que ofrece una transmisión de datos en tiempo real desde aplicaciones y servicios, y dirige esos datos a destinos como funciones AWS Lambda, temas de Amazon Simple Notification Service y transmisiones de Amazon Kinesis. Con EventBridge, puede automatizar el monitoreo y el procesamiento de ciertos tipos de eventos, incluidos los eventos que Macie publica para resultados. Para obtener más información acerca de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

Si integra las Notificaciones del usuario de AWS con Macie, también puede utilizar los eventos de EventBridge para generar automáticamente notificaciones sobre los eventos que Macie publica para los resultados. Con las notificaciones de usuario, puede configurar reglas y canales de entrega personalizados para recibir notificaciones sobre eventos de interés de EventBridge. Los canales de entrega incluyen el correo electrónico, las notificaciones por el chat AWS Chatbot y las notificaciones push de AWS Console Mobile Application. También puede revisar las notificaciones en una ubicación central en la AWS Management Console. Para obtener más información sobre las notificaciones de usuario, consulte la Guía del usuario de AWS User Notifications.

AWS Security Hub

AWS Security Hub es un servicio de seguridad que proporciona una visión integral de su estado de seguridad en todo su entorno AWS. Recopila datos de seguridad de Servicios de AWS y soluciones de seguridad AWS Partner Network compatibles, y le ayuda a comprobar su entorno frente a los estándares del sector de la seguridad y las prácticas recomendadas. A su vez, ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad. Security Hub le permite revisar los resultados de Macie como parte de un análisis más amplio de la postura de seguridad de su organización. También puede agregar hallazgos

de varias Regiones de AWS y monitorear y procesar los datos de los resultados agregados de una sola región. Para obtener más información sobre Security Hub, consulte la AWS Security HubGuía del usuario.

Cuando Macie crea un resultado, lo publica automáticamente en EventBridge como un evento nuevo. Según la configuración de publicación que elije para su cuenta, Macie también publica el resultado en Security Hub. Macie publica cada nuevo resultado inmediatamente después de procesar el resultado. Si Macie detecta una ocurrencia posterior de un resultado de política existente, publica una actualización del evento EventBridge existente para el resultado. Según la configuración de publicación que elije para su cuenta, Macie también publica la actualización en Security Hub. Macie publica estas actualizaciones de forma periódica, con la frecuencia de publicación que usted especifique en la configuración de publicación de su cuenta.

Temas

Configuración de los ajustes de publicación de los resultados de Amazon Macie

Para facilitar la integración con otras aplicaciones, servicios y sistemas, Amazon Macie publica automáticamente las conclusiones sobre políticas y datos confidenciales en Amazon EventBridge como eventos. Para obtener información sobre cómo puede utilizar EventBridge para supervisar y procesar los hallazgos, consulteIntegración de Amazon Macie con Amazon Eventbridge.

AWS Security Hub También puede configurar Macie para que publique automáticamente los resultados, utilizando las opciones de destino que especifique en la configuración de publicación de su cuenta. Con estas opciones, puede configurar Macie para que publique solo los hallazgos de políticas, solo los resultados de datos confidenciales o los hallazgos tanto de políticas como de datos confidenciales en Security Hub. También puede configurar a Macie para que deje de publicar resultados en Security Hub. Para obtener información sobre cómo puede utilizar Security Hub para monitorear y procesar resultados , consulte Integración de Amazon Macie con AWS Security Hub.

En cuanto a los resultados de políticas, el momento en que Macie publica un resultado en otro Servicio de AWS depende de si la conclusión es nueva y de la frecuencia de publicación que especifique para su cuenta. En el caso de los hallazgos de datos confidenciales, el momento es siempre inmediato: Macie publica un resultado de datos confidenciales inmediatamente después de terminar de procesarlo. A diferencia de los resultados de políticas, Macie trata todos los resultados de datos confidenciales como nuevos (únicos).

Observe que Macie no publica resultados de datos confidenciales o de políticas que se archiven automáticamente mediante una regla de supresión. En otras palabras, Macie no publica los resultados suprimidos en otros servicios Servicios de AWS.

Temas

Elección de los destinos de publicación de los resultados

Puede configurar Amazon Macie para que publique automáticamente las conclusiones sobre políticas y datos confidenciales, además de AWS Security Hub en Amazon. EventBridge De forma predeterminada, Macie publica solo los resultados de políticas nuevos y actualizados en Security Hub. Para cambiar o ampliar la configuración predeterminada, ajuste la configuración de destino de publicación de su cuenta.

Cuando ajusta la configuración de destino, elige las categorías de hallazgos que quiere que Macie publique en Security Hub: solo hallazgos de políticas, solo hallazgos de datos confidenciales o hallazgos tanto de políticas como de datos confidenciales. También puede optar por dejar de publicar cualquier categoría de resultados en Security Hub.

Si cambia la configuración de destino, el cambio solo se aplicará a la Región de AWSactual. Si es el administrador de Macie de una organización, la configuración solo se aplica a su cuenta. No se aplica a ninguna cuenta de miembro asociada. Para obtener más información, consulte Administración de varias cuentas .

Elegir los destinos de publicación de los resultados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Configuración.

3. En la sección Publicación de resultados, en Destinos, elija una de las siguientes opciones:

   - Publicar las conclusiones de las políticas en Security Hub: active esta casilla para empezar a publicar automáticamente las conclusiones de las políticas nuevas y actualizadas en Security Hub. Para dejar de publicar los resultados de políticas nuevas y actualizadas en Security Hub, desactive esta casilla de verificación.

     Si selecciona esta casilla de verificación y ya tiene las conclusiones de las políticas, Macie no las publicará automáticamente en Security Hub. En su lugar, Macie publica solo las conclusiones de las políticas que crea o actualiza después de guardar los cambios.
   - Publicar hallazgos de datos confidenciales en Security Hub: seleccione esta casilla para empezar a publicar automáticamente nuevos hallazgos de datos confidenciales en Security Hub. Para dejar de publicar nuevos hallazgos de datos confidenciales en Security Hub, desactive esta casilla de verificación.

     Si selecciona esta casilla y ya tiene datos confidenciales encontrados, Macie no los publicará automáticamente en Security Hub. En su lugar, Macie publica solo los datos confidenciales que obtiene después de guardar los cambios.
4. Seleccione Guardar.

Si ha decidido publicar cualquier categoría de hallazgos en Security Hub, asegúrese de habilitar también Security Hub en la región actual y configurarlo para que acepte los hallazgos de Macie. De lo contrario, no podrá acceder a los resultados en Security Hub. Para obtener información sobre cómo aceptar las conclusiones de Security Hub, consulte Administrar integraciones de productos en la AWS Security Hub Guía del usuario.

Establecimiento de la frecuencia de publicación de los resultados

En Amazon Macie, cada resultado tiene un identificador único. Macie usa este identificador para determinar cuándo publicar un resultado en otro Servicio de AWS:

- Nuevos resultados: cuando Macie crea una nueva política o un resultado de datos confidenciales, asigna un identificador único al resultado como parte del procesamiento del resultado. Inmediatamente después de que Macie termine de procesar el hallazgo, lo publica como un nuevo EventBridge evento de Amazon. Según la configuración de publicación de su cuenta, Macie también publica el resultado como un nuevo resultado en AWS Security Hub.

- Resultados actualizados: cuando Macie detecta una ocurrencia posterior de un resultado de política existente, actualiza resultado existente añadiendo detalles sobre la ocurrencia posterior e incrementando el recuento de incidencias. Macie también publica estas actualizaciones en el EventBridge evento existente y, en función de la configuración de publicación de su cuenta, en el resultado del Security Hub existente. Macie lo hace solo en relación con los resultados de políticas. Los resultados de datos confidenciales, a diferencia de los resultados de políticas, se tratan todos como nuevos (únicos).

  De forma predeterminada, Macie publica los resultados actualizados cada 15 minutos como parte de un ciclo de publicación recurrente. Esto significa que los resultados de las políticas que se actualicen después del ciclo de publicación más reciente se conservarán, se volverán a actualizar según sea necesario y se incluirán en el siguiente ciclo de publicación (aproximadamente 15 minutos después). Puede cambiar este cronograma eligiendo una frecuencia de publicación diferente. Por ejemplo, si configura Macie para que publique los resultados actualizados cada hora y la publicación se publique a las 12:00, cualquier actualización que se produzca después de las 12:00 se publicará a las 13:00.

Tenga en cuenta que ninguno de estos casos se aplica a los resultados que se archivan automáticamente según una regla de supresión. Macie no publica los hallazgos suprimidos en otras personas. Servicios de AWS

Establecimiento de la frecuencia de publicación de los resultados

Puede cambiar el calendario que Amazon Macie utiliza para publicar las actualizaciones de las conclusiones de las políticas existentes en otros. Servicios de AWSDe forma predeterminada, Macie publica los resultados cada 15 minutos. Si cambia este horario, el cambio se aplicará únicamente a la Región de AWSactual. Si es el administrador de Macie de una organización, el cambio también se aplicará a todas las cuentas miembro asociadas en la región. Para obtener más información, consulte Administración de varias cuentas .

Cambiar la frecuencia de publicación de los resultados actualizados

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En el panel de navegación, seleccione Configuración.
3. En la sección Publicación de resultados, en Actualizar frecuencia de los resultados de políticas, elija la frecuencia con la que desea que Macie publique los resultados de políticas actualizados para otros Servicios de AWS.

4. Elija Guardar.

Integración de Amazon Macie con Amazon Eventbridge

Amazon EventBridge, anteriormente Eventos de Amazon CloudWatch, es un servicio de bus de eventos sin servidor. EventBridge ofrece una transmisión de datos en tiempo real desde aplicaciones y servicios, y dirige esos datos a destinos como funciones AWS Lambda, temas de Amazon Simple Notification Service (Amazon SNS) y transmisiones de Amazon Kinesis. Para obtener más información acerca de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

Con EventBridge, puede automatizar la supervisión y el procesamiento de determinados tipos de eventos. Esto incluye eventos que Amazon Macie publica automáticamente para nuevos resultados de políticas y resultados información confidencial. También incluye los eventos que Macie publica automáticamente para que se repitan posteriormente los resultados de las políticas existentes. Para obtener más información sobre cómo y cuándo Macie publica estos eventos, consulte Configuración de los ajustes de publicación de los resultados .

Al utilizar EventBridge y los eventos que publica Macie para los resultados, puede monitorear y procesar los hallazgos casi en tiempo real. A continuación, podrá actuar en función de los resultados mediante el uso de otras aplicaciones y servicios. Por ejemplo, puede usar EventBridge para enviar tipos específicos de nuevos resultados a una función de AWS Lambda. A continuación, la función de Lambda podría procesar y enviar los datos a su sistema de gestión de incidentes y eventos de seguridad (SIEM). Si integra las Notificaciones del usuario de AWS con Macie, también puede usar los eventos para recibir notificaciones automáticas de los resultados a través de los canales de entrega que especifique.

Además de la supervisión y el procesamiento automatizados, el uso de EventBridge permite conservar los datos de sus resultados a más largo plazo. Macie guarda los resultados durante 90 días. Con EventBridge, puede enviar los datos de los resultados a su plataforma de almacenamiento preferida y almacenar los datos durante el tiempo que desee.

> **Note**
>
> Para la retención a largo plazo, configure Macie para almacenar los resultados de la detección de información confidencial en un bucket de S3. Un resultado de detección de datos confidenciales es un registro de los detalles sobre el análisis que Macie realizó en un objeto de S3 para determinar si el objeto contiene datos sensibles. Para obtener más

información, consulte Almacenamiento y retención de los resultados de descubrimiento de datos confidenciales.

Temas

Trabajo con Amazon EventBridge

Con Amazon EventBridge, puede crear reglas para especificar qué eventos desea supervisar y qué objetivos desea que realicen acciones automatizadas para esos eventos. Un objetivo es un destino al que EventBridge envía eventos.

Para automatizar las tareas de supervisión y procesamiento de los resultados, puede crear una regla de EventBridge que detecte automáticamente los eventos de resultado de Amazon Macie y los envíe a otra aplicación o servicio para su procesamiento o cualquier otra acción. Puede personalizar la regla para que envíe solo los eventos que cumplan determinados criterios. Para ello, especifique los criterios que se deriven de Esquema de eventos de EventBridge para resultados.

Por ejemplo, puede crear una regla que envíe tipos específicos de nuevos resultados a una función de AWS Lambda. La función de Lambda puede entonces realizar tareas como: procesar y enviar los datos a su sistema SIEM; aplicar automáticamente un determinado tipo de cifrado del lado del servidor a un objeto S3; o restringir el acceso a un objeto S3 cambiando la lista de control de acceso (ACL) del objeto. O puede crear una regla que envíe automáticamente nuevos resultadosde alta gravedad a un tema de Amazon SNS, que luego notifica el resultado a su equipo de respuesta a incidentes.

Además de invocar funciones de Lambda y notificar temas de Amazon SNS, EventBridge admite otros tipos de destinos y acciones, como la transmisión de eventos a Amazon Kinesis, la activación de máquinas de estado AWS Step Functions, y la invocación del comando de ejecución de AWS Systems Manager. Para obtener más información sobre los destinos admitidos, consulte Destinos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Creación de reglas de Amazon EventBridge para resultados

En los siguientes procedimientos se explica cómo utilizar la consola de Amazon EventBridge y AWS Command Line Interface(AWS CLI) para crear una regla de EventBridge para los resultados de

Amazon Macie. La regla detecta eventos de EventBridge que utilizan el esquema y el patrón de eventos para los resultados de Macie y, a continuación, envía esos eventos a una función de AWS Lambda para su procesamiento.

AWS Lambda es un servicio informático que permite ejecutar código sin aprovisionar ni administrar servidores. El código se empaqueta y se carga en AWS Lambda como una función de Lambda. AWS Lambda ejecuta a continuación la función cuando esta se invoca. Una función se puede invocar manualmente, automáticamente en respuesta a eventos o en respuesta a solicitudes de aplicaciones o servicios. Para obtener más información acerca de crear e invocar funciones de Lambda, consulte la AWS LambdaGuía para desarrolladores.

Console

En este procedimiento se explica cómo utilizar la consola de Amazon EventBridge para crear una regla que envíe automáticamente todos los eventos de resultados de Macie a una función de Lambda para su procesamiento. La regla usa la configuración predeterminada para las reglas que se ejecutan cuando se reciben eventos específicos. Para obtener más información sobre la configuración de reglas o para aprender a crear una regla que utilice una configuración personalizada, consulte Creación de reglas que reaccionan a los eventos en la Guía del usuario de Amazon EventBridge.

> **Tip**
>
> También puede crear una regla que utilice un patrón de eventos personalizado para detectar y actuar únicamente sobre un subconjunto de eventos de resultados de MAcie.. Este subconjunto se puede basar en campos específicos que Macie incluya en un evento de resultado. Para obtener más información sobre los campos disponibles, consulte Esquema de eventos de EventBridge para resultados. Para obtener información sobre cómo crear este tipo de regla, consulte Filtrado de contenido en patrones de eventos en la Guía del usuario de Amazon EventBridge.

Antes de crear la regla, cree la función de Lambda que quiere que la regla utilice como destino. Cuando cree la regla, tendrá que especificar esta función como destino.

Crear una regla para un evento utilizando la consola de

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. En el panel de navegación, en Events (Eventos), elija Rules (Reglas).

3. En la sección Rules (Reglas), elija Create rule (Crear regla).
4. En la página Definir detalle de la regla, haga lo siguiente:
   - En Name (Nombre), ingrese el nombre de la regla.
   - (Opcional) En Descripción, ingrese una breve descripción de la regla de autorización.
   - En el caso del Bus de eventos, asegúrese de que esté seleccionada la opción predeterminada y que esté activada la opción Habilitar la regla en el bus de eventos seleccionado.
   - En Rule type (Tipo de regla), elija Rule with an event pattern (Regla con un patrón de evento).
5. Cuando haya terminado, elija Next (Siguiente).
6. En la página Crear patrón de evento, realice una de las siguientes acciones:
   - En Origen del evento, elija AWSEventos o eventos de socios de EventBridge.
   - (Opcional) En el caso de un evento de muestra, revise un ejemplo de evento de resultados para que Macie sepa qué puede contener un evento. Para ello, seleccione AWSeventos. A continuación, en Ejemplos de eventos, seleccione Resultados de Macie.
   - En la sección Patrón de eventos, elija Formulario de patrón de eventos. Ingrese la siguiente configuración:
     - En Event source (Origen del evento), elija Servicios de AWS.
     - Para Servicio de AWS, introduzca Macie.
     - En Tipo de evento, elija Resultado de Macie.
7. Cuando haya terminado, elija Next (Siguiente).
8. En la página Seleccionar destinos, haga lo siguiente:
   - Para Target types (Tipos de destino), elija Servicio de AWS.
   - En Seleccione un destino, introduzca Función de Lambda. Luego, en Función, elija la función de Lambda a la que quiera enviar los eventos de resultados.
   - En Configurar version/alias, ingrese la configuración de versión y alias de la función de Lambda de destino.
   - (Opcional) En Configuración adicional, introduzca una configuración personalizada para especificar qué datos de eventos desea enviar a la función de Lambda. También puede especificar cómo gestionar los eventos que no se envíen correctamente a la función.
9. Cuando haya terminado, elija Next (Siguiente).

10. En la página Configurar etiquetas, si lo desea, introduzca una o más etiquetas para asignarlas a la regla. A continuación, elija Next.
11. En la página Revisar y crear, revise cada configuración y compruebe que es correcta.

    Para cambiar una configuración, elija Editar en la sección que contiene la configuración y, a continuación, escriba la configuración adecuada. También puede usar las pestañas de navegación para ir a la página que contiene una configuración.
12. Cuando termine de verificar la configuración, elija Crear regla.

AWS CLI

En este procedimiento se explica cómo utilizar AWS CLI para crear una regla de EventBridge que envíe todos los eventos de resultados de Macie a una función de Lambda para su procesamiento. La regla usa la configuración predeterminada para las reglas que se ejecutan cuando se reciben eventos específicos. En el procedimiento, los comandos se formatean para Microsoft Windows. Para Unix, Linux y macOS, reemplace el carácter de continuación de línea de intercalación (^) por una barra invertida (\).

Antes de crear la regla, cree la función de Lambda que quiere que la regla utilice como destino. Al crear la función, anote el nombre de recurso de Amazon (ARN) de la función. Deberá ingresar este ARN cuando especifique el destino de la regla.

Para crear una regla de eventos mediante el AWS CLI

1. Cree una regla que detecte eventos para todos los resultados que Macie publique en EventBridge. Para ello, utilice el comando put-rule de EventBridge. Por ejemplo:

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

   Donde *MacieFindings* es el nombre que desea para la regla.

   Si el comando se ejecuta correctamente, EventBridge responde con el ARN de la regla. Anote este ARN. Tendrá que ingresarlo en el paso 3.

> **Tip**
>
> También puede crear una regla que utilice un patrón de eventos personalizado para detectar y actuar únicamente sobre un subconjunto de eventos de resultados de MAcie.. Este subconjunto se puede basar en campos específicos que Macie incluya en un evento de resultado. Para obtener más información sobre los campos disponibles, consulte Esquema de eventos de EventBridge para resultados. Para obtener información sobre cómo crear este tipo de regla, consulte Filtrado de contenido en patrones de eventos en la Guía del usuario de Amazon EventBridge.

2. Especifique la función de Lambda que se va a utilizar como destino de la regla. Para ello, utilice el comando put-targets de EventBridge. Por ejemplo:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-findings-function
```

Donde *MacieFindings* es el nombre que especificó para la regla en el paso 1, y el valor del parámetro `Arn` es el ARN de la función que quiere que la regla utilice como destino.

3. Agregue permisos que permitan a la regla invocar la función de Lambda de destino. Para ello, utilice el comando add-permission de Lambda. Por ejemplo:

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

Donde:

- *my-findings-function* es el nombre de la función de Lambda que quiere que la regla utilice como destino.
- *Sid* es un identificador único que se define para describir la instrucción en la política de la función de Lambda.
- `source-arn` es el ARN de la regla de EventBridge.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente:

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

El valor de `Statement` es una versión de cadena JSON de la instrucción que se agregó a la política de la función Lambda.

Integración de Amazon Macie con AWS Security Hub

AWS Security Hub es un servicio que proporciona una visión completa de su estado de seguridad en el medio AWS y lo ayuda a comprobar su entorno con las prácticas recomendadas y los estándares del sector de seguridad. Esto lo consigue, en parte, mediante el consumo, la agregación, la organización y la priorización de los resultados de soluciones de seguridad múltiples Servicios de AWS y compatiblesAWS Partner Network. Security Hub lo ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad. Con Security Hub, también puede agregar resultados de varias Regiones de AWS y monitorizar y procesar los datos de los resultados agregados de una sola región. Para obtener más información sobre Security Hub, consulte la AWS Security HubGuía del usuario.

Amazon Macie se integra con Security Hub, lo que significa que puede publicar automáticamente los hallazgos de Macie en Security Hub. Security Hub puede incluir esos resultados en su análisis de la posición de seguridad. Además, puede usar Security Hub para monitorear y procesar las conclusiones sobre políticas y datos confidenciales como parte de un conjunto agregado más amplio de datos de hallazgos para su AWS entorno. En otras palabras, puede analizar los hallazgos de Macie y, al mismo tiempo, realizar análisis más amplios de la postura de seguridad de su organización y corregir los hallazgos según sea necesario. Security Hub reduce la complejidad de

abordar grandes volúmenes de resultados de múltiples proveedores. Además, utiliza un formato estándar para todos los resultado, incluidos los de Macie. El uso de este formato, el AWSFormato Security Finding (ASFF), elimina la necesidad de realizar esfuerzos de conversión de datos que consumen mucho tiempo.

Temas

Cómo publica Amazon Macie sus resultados en AWS Security Hub

En AWS Security Hub, los problemas de seguridad se rastrean como resultados. Algunos resultados provienen de problemas detectados porServicios de AWS, como Amazon Macie, o por soluciones de seguridad AWS Partner Network compatibles. Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de un resultado en particular. Para obtener información sobre cómo hacerlo, consulte Visualización de listas de resultados y detalles en la AWS Security Hub Guía del usuario. También puede realizar un seguimiento del estado de una investigación de un resultado. Consulte Adopción de medidas sobre los resultados en la Guía del usuario de AWS Security Hub.

Todos los resultados en Security Hub usan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado. Para obtener más información, consulte AWS Security Finding Format (ASFF) en la Guía del usuario de AWS Security Hub.

Tipos de resultados que Macie publica

En función de la configuración de publicación que elija para su cuenta de Macie, Macie puede publicar todos los resultados que cree en Security Hub, tanto los resultados de datos confidenciales como los de políticas. Para obtener más información acerca de estas configuraciones y de cómo cambiarlas, consulte Configuración de los ajustes de publicación de los resultados . De forma predeterminada, Macie publica solo los resultados de políticas nuevos y actualizados en Security Hub. Macie no publica los resultados de datos confidenciales en Security Hub.

Resultados de datos confidenciales

Si configura a Macie para que publique resultados de datos confidenciales en Security Hub, Macie publica automáticamente cada resultado de datos confidenciales que cree para su cuenta y lo hace inmediatamente después de terminar de procesar el resultado. Macie lo hace con todos los resultados de datos confidenciales que encuentre y que no se archiven automáticamente mediante una regla de supresión.

Si es el administrador de Macie de una organización, la publicación se limita a los resultados de los trabajos de detección de datos confidenciales que haya realizado y a las actividades de detección automatizada de datos confidenciales que Macie realizó para su organización. Solo la cuenta que crea un trabajo puede publicar los datos confidenciales que genere el trabajo. Solo la cuenta de administrador de Macie puede publicar los datos confidenciales que la detección automatizada de datos confidenciales genere para su organización.

Cuando Macie publica los resultados de datos confidenciales en Security Hub, utiliza el formato de resultados de seguridad de AWS (ASFF), que es el formato estándar para todos los resultados en Security Hub. En el ASFF, el campo `Types` indica el tipo de resultado. Este campo usa una taxonomía ligeramente diferente de la taxonomía del tipo de resultado de Macie.

En la siguiente tabla se muestra el tipo de resultado ASFF para cada tipo de resultado de datos confidenciales que Macie puede crear.

Tipo de resultado de Macie.	Tipo de resultado de ASFF
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple

Tipo de resultado de Macie.	Tipo de resultado de ASFF
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

Hallazgos de políticas

Si configura Macie para que publique resultados de políticas en Security Hub, Macie publica automáticamente cada resultado de política que cree para su cuenta y lo hace inmediatamente después de terminar de procesar el resultado. Si Macie detecta la aparición posterior de un resultado de política existente, publica automáticamente una actualización del resultado existente en Security Hub, utilizando la frecuencia de publicación que especifique para su cuenta. Macie lo hace con todos los resultados de políticas que encuentre y que no se archiven automáticamente mediante una regla de supresión.

Si es el administrador de Macie de una organización, la publicación se limita a las conclusiones sobre las políticas de los segmentos de S3 que son propiedad directa de su cuenta. Macie no publica los resultados de las políticas que crea o actualiza para las cuentas de los miembros de su organización. Esto ayuda a garantizar que no haya datos de resultados duplicados en Security Hub.

Como ocurre con los resultados de datos confidenciales, Macie utiliza el formato de resultados de seguridad de AWS (ASFF) cuando publica los resultados de políticas nuevos y actualizados en Security Hub. En el ASFF, el campo `Types` usa una taxonomía ligeramente diferente de la taxonomía del tipo de resultado de Macie.

En la siguiente tabla se muestra el tipo de resultado ASFF para cada tipo de resultado de política que Macie puede crear. Si Macie creó o actualizó un resultado de política en Security Hub el 28 de enero de 2021 o después, el resultado tiene uno de los siguientes valores para el campo `Types` ASFF de Security Hub.

Tipo de resultado de Macie.	Tipo de resultado de ASFF
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled

Tipo de resultado de Macie.	Tipo de resultado de ASFF
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Si Macie creó o actualizó un resultado de política en Security Hub el 28 de enero de 2021 o después, el resultado tiene uno de los siguientes valores para el campo `Types` ASFF de Security Hub.

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

Los valores de la lista anterior se asignan directamente a los valores del campo Tipo de resultado (`type`) de Macie.

> **Note**
>
> Al revisar y procesar los resultados de las políticas en Security Hub, tenga en cuenta las siguientes excepciones:
>
> - En algunos Regiones de AWS, Macie comenzó a utilizar los tipos de resultado del ASFF para los hallazgos nuevos y actualizados a partir del 25 de enero de 2021.
> - Si actuó en función de un resultado de política en Security Hub antes de que Macie empezara a utilizar los tipos de resultado de ASFF en su Región de AWS, el valor del campo `Types` ASFF del resultado será uno de los tipos de resultado de Macie de la lista anterior. No será uno de los tipos de resultado de ASFF de la tabla anterior. Esto es válido en el caso de los resultados sobre políticas que se hayan tomado en cuenta al utilizar la consola AWS Security Hub o el BatchUpdateFindings funcionamiento de la API AWS Security Hub.

Latencia para la publicación de resultados

Cuando Macie crea un nuevo resultado de política o de datos confidenciales, lo publica en Security Hub inmediatamente después de terminar de procesarlo.

Cuando Macie detecta una aparición posterior de una constatación de un resultado de política existente, publica una actualización del hallazgo existente en Security Hub. El momento de la actualización depende de la frecuencia de publicación que elija para su cuenta de Macie. De forma predeterminada, Macie publica las actualizaciones cada 15 minutos. Para obtener más información, incluido el modo de cambiar la configuración de su cuenta, consulte Configuración de los ajustes de publicación de los resultados .

Reintentar cuando Security Hub no está disponible

Si Security Hub no está disponible, Macie crea una cola de resultados que Security Hub no ha recibido. Cuando se restablece el sistema, Macie vuelve a intentar la publicación hasta que Security Hub reciba los resultados.

Actualización de los resultados existentes en Security Hub

Después de que Macie publique un hallazgo de política en Security Hub, Macie lo actualiza para reflejar cualquier incidencia adicional del resultado o de su actividad. Macie lo hace solo en relación

con los resultados de políticas. Los resultados de datos confidenciales, a diferencia de los resultados de políticas, se tratan todos como nuevos (únicos).

Cuando Macie publica una actualización de un resultado de política, actualiza el valor del campo Actualizado en (`UpdatedAt`) del resultado. Puede usar este valor para determinar cuándo Macie detectó por última vez una posible infracción de la política o problema que dio lugar al resultado.

Macie también podría actualizar el valor del campo Tipos (`Types`) de un resultado si el valor existente del campo no es un tipo de resultado ASFF. Esto depende de si ha actuado en función del resultado publicado en Security Hub. Si no ha actuado en función del resultado, Macie cambia el valor del campo por el tipo de resultado ASFF adecuado. Si ha actuado en función del resultado, utilizando la consola AWS Security Hub o el funcionamiento BatchUpdateFindings de la API AWS Security Hub, Macie no cambia el valor del campo.

Ejemplos de resultados de Amazon Macie en AWS Security Hub

Cuando Amazon Macie publica los resultados en AWS Security Hub, utiliza el AWS Security Finding Format (ASFF). Este es el formato estándar para todos los resultados en Security Hub. Los siguientes ejemplos utilizan datos de muestra para demostrar la estructura y la naturaleza de los datos de los resultados que Macie publica en Security Hub en este formato:

- Ejemplo de un resultado de datos confidenciales
- Ejemplo de un resultado de política

Ejemplo de un resultado de datos confidenciales en Security Hub

Este es un ejemplo de un resultado de datos confidenciales que Macie publicó en Security Hub utilizando el ASFF.

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
```

```
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
```

```
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
```

```
                                            "Row": 1,
                                            "ColumnName": "Other"
                                        }
                                    ]
                                }
                            }
                        ],
                        "TotalCount": 1
                    }
                ],
                "CustomDataIdentifiers": {
                    "Detections": [
                    ],
                    "TotalCount": 0
                }
            }
        },
        "Details": {
            "AwsS3Object": {
                "LastModified": "2022-04-22T18:16:46.000Z",
                "ETag": "ebe1ca03ee8d006d457444445example",
                "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                "ServerSideEncryption": "aws:kms",
                "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
    }
],
"WorkflowState": "NEW",
"Workflow": {
    "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
    "Severity": {
        "Label": "HIGH"
    },
    "Types": [
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ]
},
"Sample": false,
"ProcessedAt": "2022-05-11T10:23:49.667Z"
```

```
}
```

Ejemplo de un resultado de política en Security Hub

Este es un ejemplo de un nuevo resultado de política que Macie publicó en Security Hub utilizando el ASFF.

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
```

```
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
                "RestrictPublicBuckets": false
               }
            }
         }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
```

```
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
}
```

Habilitación y configuración de la integración AWS Security Hub

Para integrar Amazon Macie conAWS Security Hub, habilite Security Hub para su. Cuenta de AWS Para obtener información sobre cómo hacerlo, consulte Habilitar Security Hub en la Guía del AWS Security Hub usuario.

Cuando habilita Macie y Security Hub, la integración se activa automáticamente. De forma predeterminada, Macie comienza a publicar automáticamente las conclusiones de las políticas nuevas y actualizadas en Security Hub. No necesita tomar medidas adicionales para configurar la integración. Si tiene conclusiones de políticas existentes cuando la integración está habilitada, Macie no las publica en Security Hub. En su lugar, Macie publica solo los resultados de las políticas que crea o actualiza una vez habilitada la integración.

Si lo desea, puede personalizar su configuración eligiendo la frecuencia con la que Macie publica las actualizaciones de los resultados de políticas en Security Hub. También puede optar por publicar los hallazgos de datos confidenciales en Security Hub. Para saber cómo hacerlo, consulte Configuración de los ajustes de publicación de los resultados .

Detener la publicación de resultados en AWS Security Hub

Para dejar de publicar los resultadosAWS Security Hub, puede cambiar la configuración de publicación de su cuenta de Amazon Macie. Para saber cómo hacerlo, consulte Elección de los destinos de publicación de los resultados . También puede hacerlo mediante la consola de Security Hub o la API de Security Hub. Para saber cómo hacerlo, consulte Desactivar y habilitar el flujo de resultados desde una integración (consola) o Desactivar el flujo de resultados desde una integración (Security Hub API, AWS) en la Guía del usuario de AWS Security Hub.

Integración de Amazon Macie con las notificaciones del usuario de AWS

Notificaciones del usuario de AWS es un servicio que actúa como ubicación central para AWS sus notificaciones en el AWS Management Console. Esto incluye notificaciones como alarmas de

Amazon CloudWatch, casos AWS Support y comunicaciones de otros Servicios de AWS. Con las notificaciones de usuario, puede configurar reglas y canales de entrega personalizados para recibir notificaciones sobre determinados tipos de eventos de Amazon EventBridge. Los canales de entrega incluyen el correo electrónico, las notificaciones por el chat AWS Chatbot y las notificaciones push de AWS Console Mobile Application. También puede revisar las notificaciones en la consola de notificaciones del usuario de AWS. Para obtener más información sobre las notificaciones de usuario, consulte la Guía del usuario de AWS User Notifications.

Macie se integra con las Notificaciones del usuario de AWS, lo que significa que puede configurar las Notificaciones de usuario para que le notifiquen los eventos que Macie publica en EventBridge para los resultados de políticas y datos confidenciales. Si un evento de resultado coincide con los criterios que especificó, las Notificaciones de usuario genera una notificación. La notificación incluye los detalles clave del resultado asociado, como el tipo y la gravedad del resultado, y el nombre del recurso afectado. Las Notificaciones de usuario también pueden enviar la notificación a uno o más canales de entrega que especifique. Puede personalizar los canales de entrega que desee para adaptarlos a sus flujos de trabajo de seguridad y cumplimiento.

Por ejemplo, puede configurar las Notificaciones de usuario para que generen notificaciones para tipos específicos de nuevos resultados de alta gravedad. También puedes especificar AWS Chatbot como canal de entrega para esas notificaciones. A continuación, las Notificaciones de usuario detecta los eventos de EventBridge para los resultados, genera notificaciones que incluyen datos de los resultados y envía las notificaciones a AWS Chatbot. AWS Chatbot podría entonces dirigir las notificaciones a un canal de Slack o a una sala de chat de Amazon Chime para notificar a tu equipo de respuesta a incidentes.

Temas

- Trabajar con notificaciones del usuario de AWS
- Habilitación y configuración de las notificaciones del usuario de AWS para los resultados de Amazon Macie
- Asignación de campos de notificaciones del usuario de AWS a campos de resultado de Amazon Macie
- Cambiar la configuración de notificaciones del usuario de AWS para los resultados de Amazon Macie
- Desactivar las notificaciones del usuario de AWS para los resultados de Amazon Macie

Trabajar con notificaciones del usuario de AWS

Con las notificaciones del usuario de AWS, puede crear reglas para especificar los tipos de eventos de Amazon EventBridge que desea supervisar y de los que desea recibir notificaciones. Una regla define los criterios que debe cumplir un evento de EventBridge para generar una notificación. También puede elegir uno o más canales de entrega para una regla. Los canales de entrega especifican dónde desea recibir las notificaciones de los eventos que coinciden con los criterios de una regla.

Si las Notificaciones de usuario detecta un evento de EventBridge que coincide con los criterios de una regla, realiza las siguientes tareas generales:

1. Extraer un subconjunto de datos del evento.
2. Generar una notificación que contiene los datos extraídos.
3. Enviar la notificación a los canales de entrega que especifique para ese tipo de evento.

El diseño y la estructura de la notificación están optimizados para cada canal de entrega al que se envía.

Para controlar la frecuencia o el número de notificaciones que recibe, puede configurar los ajustes de agregación de una regla. Si habilita esta configuración, las notificaciones de usuario combinan los datos de varios eventos en una sola notificación. Puede optar por enviar notificaciones de eventos agregadas de forma rápida y frecuente, que quizás prefiera en el caso de eventos de resultado de alta gravedad. O envíelas con menos frecuencia para recibir menos notificaciones, que tal vez le interese en el caso de eventos de resultado de baja gravedad. Si combina los datos de los eventos, puede profundizar para revisar los detalles de cada evento agregado mediante la consola de notificaciones del usuario de AWS. Desde allí, también puede navegar hasta cada resultado asociado en la consola de Amazon Macie.

Habilitación y configuración de las notificaciones del usuario de AWS para los resultados de Amazon Macie

Para permitir que las Notificaciones del usuario de AWS genere notificaciones sobre los resultados de Amazon Macie, cree una configuración de notificaciones para Macie en las Notificaciones del usuario de AWS. Una configuración de notificaciones especifica los criterios de una regla. También especifica los canales de entrega y otros ajustes para supervisar y enviar notificaciones sobre los eventos de Amazon EventBridge que coincidan con los criterios de la regla. Para obtener información

detallada sobre la creación de una configuración de notificaciones, consulte Introducción a las notificaciones de usuarios de AWS en la Guía del usuario de AWS User Notifications.

Para crear una configuración de notificaciones para los resultados de Macie, elija las siguientes opciones para la regla de eventos:

- Para el nombre de Servicio de AWS, elija Macie.
- En Tipo de evento, elija Resultado de Macie.
- Para las Regiones, seleccione cada Región de AWS en las que utilice Macie y desee que se le notifiquen los resultados.

Con esta configuración, las Notificaciones de usuarios de AWS supervisa los eventos de EventBridge para su Cuenta de AWS y genera notificaciones para todos los eventos de resultado de Macie en las regiones que haya seleccionado. Los eventos cumplen los siguientes criterios:

- `source` es igual a `aws.macie`
- `detail-type` es igual a `Macie Finding`

El patrón JSON subyacente de la regla de eventos es:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

Para refinar la regla y generar notificaciones solo para un subconjunto de resultados, puede personalizar el patrón JSON de la regla. Para ello, especifique criterios adicionales que se deriven del esquema de eventos de EventBridge para los resultados de Macie.

Si crea una regla que utilice un patrón JSON personalizado, puede crear varias configuraciones de notificación para los resultados de Macie. A continuación, puede personalizar los canales de entrega y otros ajustes para cada configuración a fin de adaptarlos a sus flujos de trabajo de seguridad y conformidad en función de los tipos de resultados específicos.

Por ejemplo, puede crear una regla que le notifique si Macie genera o actualiza un resultado Policy:IAMUser/S3BucketPublic. En este caso, el patrón de la regla podría ser:

```
{
```

```
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

También puede crear otra regla que te notifique si Macie genera un resultado de datos confidenciales para un bucket de S3 al que se puede acceder públicamente. En este caso, el patrón de la regla podría ser:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Si crea varias configuraciones de notificación para los resultados de Macie, es una buena idea asegurarse de que la regla de cada configuración sea única. De lo contrario, es posible que reciba notificaciones duplicadas para cada resultado individual.

Para obtener más información sobre la personalización de los patrones de eventos para las reglas, consulte Uso de patrones de eventos JSON personalizados en la Guía del usuario de AWS User Notifications.

Asignación de campos de notificaciones del usuario de AWS a campos de resultado de Amazon Macie

Cuando las Notificaciones del usuario de AWS genera una notificación para un resultado de Amazon Macie, rellena la notificación con datos de un subconjunto de campos del evento de Amazon EventBridge correspondiente. Estos campos proporcionan detalles clave del resultado asociado, como el tipo y la gravedad del resultado y el nombre del recurso afectado.

Si revisa una notificación en la consola de notificaciones del usuario de AWS, la notificación incluye todos los datos de este subconjunto de campos. También proporciona un enlace al resultado

asociado en la consola de Amazon Macie. Si revisa una notificación en otros canales de entrega, es posible que solo contenga datos de algunos de los campos. Esto se debe a que las Notificaciones de usuarios de AWS adapta el diseño y la estructura de sus notificaciones para que funcionen con cada tipo de canal de entrega compatible.

En la siguiente tabla se enumeran los campos que se pueden incluir en una notificación para obtener un resultado. En la tabla, la columna del Campo de notificación describe (en cursiva) o indica el nombre de un campo de una notificación. La columna de Campo de evento de resultado utiliza la notación de puntos para indicar el nombre del campo JSON correspondiente en un evento de EventBridge para un resultado. La columna Descripción describe los datos que se almacenan en el campo.

Campo de notificación	Campo de resultado del evento	Descripción
Título del mensaje	`detail.type`	El tipo de resultado. Por ejemplo: `Policy:IAMUser/S3BucketPublic` o `Sensitive Data:S3Object/Financial`.
Resumen	`detail.title`	La descripción del resultado Por ejemplo: `The S3 object contains financial information.`
Descripción	`detail.description`	La descripción completa del resultado Por ejemplo: `The S3 object contains financial information such as bank account numbers or credit card numbers.`

Campo de notificación	Campo de resultado del evento	Descripción
Gravedad	`detail.severity.description`	La representación cualitativa de la gravedad del resultado: `Low`, `Medium` o `High`.
ID del resultado	`detail.id`	Un identificador único para el resultado.
Created (Creado)	`detail.createdAt`	La fecha y la hora en que Macie creó el resultado.
Actualizado	`detail.updatedAt`	La fecha y la hora en que Macie actualizó el resultado por última vez. En el caso de los resultados de datos confidenciales, este valor es el mismo que el del campo Creado (`detail.createdAt`). Todos los resultados de datos confidenciales se consideran nuevos (únicos).
Bucket de S3 afectado	`detail.resourcesAffected.s3Bucket.arn`	El nombre de recurso de Amazon (ARN) del bucket de S3.

Campo de notificación	Campo de resultado del evento	Descripción
Objeto de S3 afectado	`detail.resourcesAffected.s3Object.path`	El nombre (clave) del objeto S3 afectado, incluido el nombre del bucket que almacena el objeto y, si corresponde, el prefijo del objeto. Este campo no se incluye en las notificaciones de resultados de políticas.

Campo de notificación	Campo de resultado del evento	Descripción

Detección de datos confidenciales	`detail.classificationDetails.result.sensitiveData.detections...`
	
	O
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		Se trata de una concatenación de varios campos en un evento para un resultado de datos confidenciales. Este campo no se incluye en las notificaciones de resultados de políticas.
		
		Si un identificador de datos gestionados detectó los datos confidenciales, este campo especifica la categoría, el tipo y el número (`count`) de apariciones de los datos confidenciales detectados. Por ejemplo: `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences .`
		
		Si un identificador de datos personalizado detectó los datos confidenciales, este campo especifica el nombre del identificador de datos personalizado y el número (`count`) de apariciones de los datos confidenciales detectados. Por ejemplo: `Employee ID 20 occurrences .`

Campo de notificación	Campo de resultado del evento	Descripción
		Si un resultado informa de varios tipos de datos confidenciales, la notificación incluye datos de hasta cuatro tipos. Los datos se rellenan primero con los identificadores de datos personalizados aplicables y, a continuación, con los identificadores de datos gestionados aplicables.

Cambiar la configuración de notificaciones del usuario de AWS para los resultados de Amazon Macie

Puede cambiar la configuración de notificaciones del usuario de AWS para los resultados de Amazon Macie en cualquier momento. Para ello, edite la configuración de notificaciones en Notificaciones de usuario. Para obtener información sobre cómo hacerlo, consulte Administrar las configuraciones de notificaciones en la Guía del usuario de AWS User Notifications.

Si tiene varias configuraciones de notificación para los resultados de Macie, cambiar los ajustes de una configuración no afectará a los ajustes de las demás configuraciones. Puede editar todas las configuraciones o solo algunas de ellas.

Desactivar las notificaciones del usuario de AWS para los resultados de Amazon Macie

Para dejar de generar y recibir notificaciones del usuario de AWS para Amazon Macie, elimine la configuración de notificaciones en notificaciones de usuario. Para obtener información sobre cómo hacerlo, consulte Administrar las configuraciones de notificaciones en la Guía del usuario de AWS User Notifications.

Si tiene varias configuraciones de notificación para los hallazgos de Macie, la eliminación de una configuración no afecta a las demás configuraciones. Puede eliminar todas las configuraciones o solo algunas.

Esquema de eventos de Amazon EventBridge para los resultados de Amazon Macie

Para facilitar la integración con otras aplicaciones, servicios y sistemas, como sistemas de monitorización o de administración de eventos, Amazon Macie publica automáticamente los resultados en Amazon EventBridge como eventos. EventBridge, anteriormente Eventos de Amazon CloudWatch, es un servicio de bus de eventos sin servidor que ofrece una transmisión de datos en tiempo real desde aplicaciones y otros Servicios de AWS a destinos como funciones AWS Lambda, temas de Amazon Simple Notification Service y transmisiones de Amazon Kinesis. Para obtener más información acerca de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

> **Note**
>
> Si actualmente usa CloudWatch Events, tenga en cuenta que EventBridge y CloudWatch Events son el mismo servicio subyacente y la misma API. Sin embargo, EventBridge incluye características adicionales que le permiten recibir eventos de aplicaciones de software como servicio (SaaS) y de sus propias aplicaciones. Como el servicio y la API subyacentes son los mismos, el esquema de eventos de los resultados de Macie también es el mismo.

Macie publica automáticamente los eventos de todos los resultados nuevos e instancias posteriores de los resultados de políticas existentes, excepto los resultados que se archivan automáticamente mediante una regla de supresión. Los eventos son objetos JSON que se adaptan al esquema de EventBridge para los eventos de AWS. Cada evento contiene una representación JSON de un resultado específico. Como los datos están estructurados como eventos de EventBridge, puede supervisar, procesar y actuar en función de los resultados más fácilmente mediante el uso de otras aplicaciones, servicios y herramientas. Para obtener más información sobre cómo y cuándo publica Macie eventos de resultados, consulte Configuración de los ajustes de publicación de los resultados .

Temas

Esquema de eventos

El siguiente ejemplo muestra el esquema de un evento de Amazon EventBridge para un resultado de Amazon Macie. Para obtener descripciones detalladas de los campos de JSON que puede incluir un evento de resultado, consulte Resultados en la referencia de la API de Amazon Macie. La estructura y los campos de un evento de búsqueda se corresponden estrechamente con el objeto Resultado de la API de Amazon Macie.

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "Cuenta de AWS ID (string)",
    "time": "event timestamp (string)",
    "region": "Región de AWS (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

Ejemplo de evento para el resultado de una política

En el siguiente ejemplo, se utilizan datos de muestra para demostrar la estructura y la naturaleza de los objetos y campos de un evento de Amazon EventBridge para un resultado de política.

En este ejemplo, el evento informa de una ocurrencia posterior de una política existente: se deshabilitó la configuración de bloqueo del acceso público para un bucket de S3. Los siguientes campos y valores pueden ayudarle a determinar si este es el caso:

- El campo `type` está establecido en `Policy:IAMUser/S3BlockPublicAccessDisabled`.
- Los valores para los campos `createdAt` y `updatedAt` son distintos. Este es un indicador de que el evento informa de la ocurrencia posterior de una constatación de política existente. Los valores de estos campos serían los mismos si el evento informara de un nuevo resultado.

- El campo `count` está establecido en 2, lo que indica que es la segunda ocurrencia del resultado.
- El campo `category` está establecido en `POLICY`.
- El valor del campo `classificationDetails` es `null`, lo que ayuda a diferenciar este evento para un resultado de políticas de un evento para un resultado de datos confidenciales. En el caso de un resultado de datos confidenciales, este valor sería un conjunto de objetos y campos que proporcionan información sobre cómo y qué datos confidenciales se encontraron.

Observe que el valor del campo `sample` es `true`. Este valor hace hincapié en que se trata de un evento de ejemplo para su uso en la documentación.


```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "name": "DOC-EXAMPLE-BUCKET1",
```

```
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
```

```
                                "blockPublicPolicy": true
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "FALSE"
            },
            "s3Object": null
        },
        "category": "POLICY",
        "classificationDetails": null,
        "policyDetails": {
            "action": {
                "actionType": "AWS_API_CALL",
                "apiCallDetails": {
                    "api": "PutBucketPublicAccessBlock",
                    "apiServiceName": "s3.amazonaws.com",
                    "firstSeen": "2021-04-29T15:46:02.401Z",
                    "lastSeen": "2021-04-30T23:12:15.401Z"
                }
            },
            "actor": {
                "userIdentity": {
                    "type": "AssumedRole",
                    "assumedRole": {
                        "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
                            }
```

```
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
                },
                "domainDetails": null
            }
        },
        "sample": true,
        "archived": false
    }
}
```


Ejemplo de evento para un resultado de datos confidenciales

En el siguiente ejemplo, se utilizan datos de muestra para demostrar la estructura y la naturaleza de los objetos y campos de un evento de Amazon EventBridge para un resultado de datos confidenciales.

En este ejemplo, el evento informa de un nuevo resultado de datos confidenciales: Amazon Macie encontró más de una categoría de datos confidenciales en un objeto de S3. Los siguientes campos y valores pueden ayudarle a determinar si este es el caso:

- El campo `type` está establecido en `SensitiveData:S3Object/Multiple`.
- Los campos `updatedAt` y `createdAt` tienen los mismos valores. A diferencia de los resultados de políticas, este siempre es el caso de los resultados de datos confidenciales. Todos los resultados de datos confidenciales se consideran nuevos.
- El campo `count` está establecido en `1`, lo que indica que se trata de un resultado nuevo. A diferencia de los resultados de políticas, este siempre es el caso de los resultados de datos confidenciales. Todos los resultados de datos confidenciales se consideran únicos (nuevos).
- El campo `category` está establecido en `CLASSIFICATION`.
- El valor del campo `policyDetails` es `null`, lo que ayuda a diferenciar este evento para un resultado de datos confidenciales de un evento para un resultado de políticas. En el caso de un resultado de políticas, este valor sería un conjunto de objetos y campos que proporcionan información sobre una posible infracción de la política o un problema relacionado con la seguridad o la privacidad de un bucket de S3.

Observe que el valor del campo `sample` es `true`. Este valor hace hincapié en que se trata de un evento de ejemplo para su uso en la documentación.

```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
```

```
        "description": "The S3 object contains more than one category of sensitive
 data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
```

```
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
```

```
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
```

```
                                {
                                    "row": 4,
                                    "column": 1,
                                    "columnName": "SSN",
                                    "cellReference": null
                                }
                            ]
                        }
                    },
                    {
                        "type": "NAME",
                        "count": 35,
                        "occurrences": {
                            "lineRanges": null,
                            "offsetRanges": null,
                            "pages": null,
                            "records": null,
                            "cells": [
                                {
                                    "row": 2,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                },
                                {
                                    "row": 3,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                }
                            ]
                        }
                    }
                ]
            },
            {
                "category": "FINANCIAL_INFORMATION",
                "totalCount": 30,
                "detections": [
                    {
                        "type": "CREDIT_CARD_NUMBER",
                        "count": 30,
                        "occurrences": {
                            "lineRanges": null,
```

```
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        }
                                    ]
                                }
                            }
                        ]
                    }
                ],
                "customDataIdentifiers": {
                    "totalCount": 0,
                    "detections": []
                }
            },
            "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
            "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
        },
        "policyDetails": null,
        "sample": true,
        "archived": false
    }
}
```

Previsión y supervisión de los costos de Amazon Macie

Para ayudarle a prever y supervisar sus costos derivados del uso de Amazon Macie, Macie calcula y proporciona los costos estimados de uso de su cuenta. Con estos datos, puede determinar si desea ajustar el uso del servicio o las cuotas de su cuenta. Si actualmente participa en una prueba gratuita de 30 días de Macie, puede utilizar estos datos para estimar sus costos de uso de Macie una vez que finalice la prueba gratuita. También puede comprobar el estado de la versión de prueba.

Puede revisar sus costos estimados de uso en la consola de Amazon Macie y acceder a ellos mediante programación con la API de Amazon Macie. Si es el administrador de Macie de una organización, puede revisar y acceder tanto a los datos agregados de su organización como a los desgloses de los datos de las cuentas de su organización.

Además de los costos de uso estimados que proporciona Macie, puede revisar y monitorear sus costos reales utilizando AWS Billing and Cost Management. AWS Billing and Cost Management proporciona funciones diseñadas para ayudarle a realizar un seguimiento Servicios de AWS, analizar los costes y gestionar los presupuestos de su cuenta u organización. También proporciona características que pueden ayudarlo a pronosticar los costos de uso en función de los datos históricos. Para obtener más información, consulte la AWS Billing Guía del usuario.

Temas

Entender cómo se calculan los costos estimados de uso para Amazon Macie

Los precios de Amazon Macie se basan en las siguientes dimensiones.

Supervisión de controles preventivos

> Estos costes se derivan del mantenimiento de un inventario de los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) y de la evaluación y supervisión de los depósitos para garantizar la seguridad y el control de acceso. Para obtener más información, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.

Se le cobrará en función del número total de depósitos de uso general de S3 que Macie monitorea para su cuenta. Los cargos se prorratean por día.

Supervisión de objetos para la detección automatizada de datos confidenciales

Estos costos se derivan de la supervisión y la evaluación de su inventario de buckets de S3 para identificar los objetos de S3 que son aptos para análisis mediante detección automática de datos confidenciales. Para obtener más información, consulte Cómo funciona la detección automatizada de datos confidenciales.

Se te cobrará en función del número total de objetos de S3 en los depósitos de uso general que Macie monitorea para tu cuenta. Los cargos se prorratean por día.

Análisis de objetos mediante trabajos de detección de datos confidenciales y detección automatizada de datos confidenciales

Estos costos se derivan del análisis de los objetos de S3 y de la elaboración de informes de los datos confidenciales que Macie encuentre en los objetos. Esto incluye los análisis y la elaboración de informes según los trabajos de detección de datos confidenciales y la detección automatizada de datos confidenciales.

Se le cobrará en función de la cantidad de datos sin comprimir que Macie analice en los objetos de S3. No se le cobrará por los objetos que Macie no pueda analizar por motivos como uso de una clase de almacenamiento de Amazon S3 no compatible, el uso de un archivo o formato de almacenamiento no compatibles o la configuración de permisos. Para obtener más información, consulte Detección de datos confidenciales. Además, estos costos no varían en función de la cantidad de resultados de datos confidenciales producidos por sus trabajos o por la detección automatizada de datos confidenciales.

Para gestionar los costos de la detección automatizada de datos confidenciales, puede excluir buckets de S3 individuales de los análisis. Por ejemplo, puede excluir los buckets que se sepa que cumplen los requisitos de seguridad y conformidad de su organización. Para excluir buckets, puede actualizar los ajustes de configuración de su cuenta. También puedes excluir los depósitos de case-by-case forma individual al revisar los detalles de cada uno de los depósitos de tu inventario.

Los costos de los trabajos de detección de datos confidenciales están restringidos por la cuota de detección de datos confidenciales mensual de su cuenta. (La cuota predeterminada es de 5 TB de datos). Si un trabajo está en ejecución y el análisis de los objetos aptos alcanza esta cuota, Macie lo detiene automáticamente hasta que comience el siguiente mes natural (y se restablezca la cuota mensual de su cuenta) o usted aumente la cuota de su cuenta.

Si es el administrador de Macie de una organización, los costos de los trabajos de detección de datos confidenciales están restringidos por la cuota mensual de detección de datos confidenciales de cada cuenta para la que analice datos. La cuota de una cuenta de miembro define la cantidad máxima de datos de la cuenta que sus trabajos y los de la cuenta de miembro pueden analizar durante un mes natural. Si se está ejecutando un trabajo y el análisis de los objetos aptos alcanza esta cuota para una cuenta de miembro, Macie deja de analizar los objetos que son propiedad de la cuenta. Cuando Macie termina de analizar los objetos de todas las demás cuentas que no han alcanzado la cuota, Macie detiene automáticamente el trabajo. Si se trata de un trabajo único, Macie reanudará automáticamente el trabajo cuando comience el siguiente mes natural o se aumente la cuota para todas las cuentas afectadas, lo que ocurra primero. Si se trata de un trabajo periódico, Macie lo reanudará automáticamente cuando esté previsto que comience la siguiente ejecución o cuando comience el siguiente mes natural, lo que ocurra primero. Si una ejecución programada comienza antes de que comience el siguiente mes natural o si se aumenta la cuota para una cuenta afectada, Macie no analiza los objetos que son propiedad de la cuenta.

> **Tip**
>
> Para obtener consejos útiles sobre cómo administrar o reducir los costos de detección de datos confidenciales, consulte la entrada del blog How to use Amazon Macie to reduce the cost of discovering sensitive data en el blog de seguridad de AWS .

Para obtener información detallada y ejemplos de los costos de uso, consulte los precios de Amazon Macie.

Cuando utilice Macie para revisar sus costos estimados de uso, es importante entender cómo se calculan los costos estimados. Considere lo siguiente:

- Las estimaciones se indican en dólares estadounidenses y son únicamente para la Región de AWS actual. Si utiliza Macie en varias regiones, los datos no están agregados para todas las regiones en las que utilice Macie.
- En la consola, las estimaciones incluyen el mes natural en curso hasta la fecha. Si consulta los datos mediante programación con la API de Amazon Macie, puede seleccionar un intervalo de tiempo inclusivo para las estimaciones. Puede ser un intervalo de tiempo continuo de los 30 días anteriores o el mes natural en curso hasta la fecha.
- Las estimaciones no reflejan todos los descuentos que podrían ser aplicables a su cuenta. La excepción son los descuentos que se derivan de los niveles de precios por volumen regionales, tal

y como se describe en los precios de Amazon Macie. Si su cuenta cumple los requisitos para este tipo de descuento, las estimaciones reflejan ese descuento.

- Si es el administrador de Macie de una organización, las estimaciones no reflejan los descuentos por volumen de uso en conjunto de su organización. Para obtener información sobre estos descuentos, consulte los descuentos por volumen en la Guía del usuario de AWS Billing .
- Para la supervisión de controles preventivos, la estimación se basa en el costo diario promedio para el intervalo de tiempo aplicable. El costo se prorratea por día.
- En el caso de la detección automatizada de datos confidenciales, la estimación general se basa en el costo medio diario de la supervisión de objetos (prorrateado por día) y en la cantidad de datos sin comprimir que Macie haya analizado hasta el momento durante el intervalo de tiempo aplicable. Si es el administrador de Macie de una organización y analiza los datos de una cuenta de miembro, los costos estimados de esas actividades se incluyen en las estimaciones de cada cuenta aplicable.
- En el caso de los trabajos de detección de datos confidenciales, la estimación se basa en la cantidad de datos sin comprimir que sus trabajos hayan analizado hasta el momento durante el intervalo de tiempo aplicable. Si es el administrador de Macie de una organización y ejecuta trabajos que analizan los datos de una cuenta de miembro, el costo estimado de esos trabajos se incluye en la estimación de la cuenta de miembro correspondiente.
- Si su cuenta es una cuenta de miembro de una organización y su administrador de Macie realiza la detección automática de datos confidenciales o realiza tareas de detección de datos confidenciales para analizar sus datos, los costos estimados de esas actividades se incluyen en las estimaciones de su cuenta.
- Las estimaciones no incluyen los costos en los que incurra al utilizar otros Servicios de AWS con determinadas características de Macie. Por ejemplo, el uso de AWS KMS keys administrado por el cliente para describir objetos de S3 que desee inspeccionar en busca de datos confidenciales.

Tenga en cuenta además que Macie ofrece un nivel mensual gratuito para el análisis de objetos de S3 mediante trabajos de detección de datos confidenciales y la detección automatizada de datos confidenciales. Cada mes, el análisis de hasta 1 GB de datos para detectar e informar de datos confidenciales en objetos de S3 es gratuito. Si se analiza más de 1 GB de datos durante un mes determinado, su cuenta empezará a acumular cargos por la detección de datos confidenciales después del primer GB de datos. Si se analiza menos de 1 GB de datos durante un mes determinado, la asignación restante no se transfiere al mes siguiente. Si su cuenta es parte de una organización con facturación unificada, el nivel gratuito se aplica al conjunto de datos analizados

para su organización. En otras palabras, analizar hasta 1 GB de datos al mes de todas las cuentas de la organización es gratuito.

Revisión de los costos estimados de uso de Amazon Macie

Para revisar los costos estimados de uso actuales de Amazon Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Tanto la consola como la API proporcionan costos estimados de las dimensiones de los precios de Macie. Si actualmente participa en una prueba gratuita de 30 días, puede utilizar estos datos para estimar sus costos de uso de Macie una vez que finalice la prueba gratuita. Para obtener información sobre dimensiones y consideraciones de los precios de Macie, consulte Entender cómo se calculan los costos estimados de uso. Para obtener información detallada y ejemplos de los costos de uso, consulte los precios de Amazon Macie.

En Macie, los costos estimados de uso se indican en dólares estadounidenses y se aplican únicamente a la Región de AWS actual. Si utiliza la consola para revisar los datos, las estimaciones de costos corresponden al mes natural en curso hasta la fecha (inclusive). Si consulta los datos mediante programación con la API de Amazon Macie, puede especificar un intervalo de tiempo inclusivo para las estimaciones, ya sea un intervalo de tiempo continuo de los 30 días previos o el mes natural en curso hasta la fecha.

Temas

Revisión de los costos estimados de uso en la consola de Amazon Macie

En la consola de Amazon Macie, las estimaciones de costos se organizan de la siguiente manera:

- Supervisión del control preventivo: este es el coste estimado de mantener un inventario de los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) y de evaluar y supervisar los depósitos para garantizar la seguridad y el control de acceso.
- Trabajos de detección de datos confidenciales: se trata del costo estimado de los trabajos de detección de datos confidenciales que ha realizado.
- Detección automatizada de datos confidenciales: estos son los costos estimados de realizar la detección automatizada de datos confidenciales. Esto incluye la supervisión y la evaluación del inventario de buckets de S3 para identificar los objetos que puedan analizarse. También

incluye el análisis de los objetos aptos y la presentación de informes sobre datos confidenciales, estadísticas, resultados y otros tipos de resultados.

Siga estos pasos para revisar sus costos estimados de uso mediante la consola de Amazon Macie.

Para revisar los costos estimados de uso de la consola

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee revisar los costes estimados.
3. En el panel de navegación, elija Uso.

Si tiene una cuenta de Macie independiente o si su cuenta es una cuenta de miembro de una organización, la página de uso muestra un desglose de los costos estimados de uso de su cuenta.

Si es el administrador de Macie de una organización, la página de uso muestra las cuentas de su organización. En la tabla:

- Cuota de servicio (puestos de trabajo): es la cuota mensual actual para ejecutar tareas de descubrimiento de datos confidenciales a fin de analizar los objetos de S3 en los depósitos que son propiedad de una cuenta.
- Prueba gratuita: estos campos indican si una cuenta participa actualmente en la prueba gratuita para el control preventivo, la supervisión o el descubrimiento automatizado de datos confidenciales. Un campo de la Prueba gratuita está vacío si la correspondiente prueba gratuita ha finalizado para una cuenta.
- Total: es el costo total estimado de una cuenta.

La sección de Costos estimados muestra el costo total estimado para su organización y un desglose de esos costos. Para revisar el desglose de los costos estimados para una cuenta específica de su organización, seleccione la cuenta en la tabla. A continuación, en la sección de Costos estimados se muestra este desglose. Para mostrar estos datos para otra cuenta, seleccione la cuenta en la tabla. Para borrar la selección de su cuenta, elija X junto al ID de la cuenta.

Consulte los costos estimados de uso con la API de Amazon Macie

Para consultar los costos estimados de uso mediante programación, puede usar las siguientes operaciones de la API Amazon Macie:

- GetUsageTotals – Esta operación devuelve los costos de uso totales estimados de su cuenta, agrupados por métrica de uso. Si es el administrador de Macie de una organización, esta operación devuelve estimaciones de costos agregadas para todas las cuentas de su organización. Para obtener más información sobre esta operación, consulte los Totales de uso en la referencia de la API de Amazon Macie.
- GetUsageStatistics – Esta operación devuelve las estadísticas de uso y los datos relacionados de su cuenta, agrupados por cuenta y, a continuación, por métrica de uso. Los datos incluyen los costos estimados de uso totales y las cuotas de la cuenta actual. Según corresponda, también indican cuándo comenzó su prueba gratuita de 30 días de Macie y de detección automática de datos confidenciales. Si es el administrador de Macie de una organización, esta operación muestra un desglose de los datos de todas las cuentas de su organización. Puede personalizar la consulta ordenando y filtrando los resultados de la consulta. Para obtener más información sobre esta operación, consulte las Estadísticas de uso en la referencia de la API de Amazon Macie.

Al utilizar cualquiera de las dos operaciones, si lo desea, puede especificar un intervalo de tiempo inclusivo para los datos. Este intervalo de tiempo puede ser un intervalo de tiempo continuo de los 30 días anteriores (`PAST_30_DAYS`) o del mes natural en curso hasta la fecha (`MONTH_TO_DATE`). Si no especifica un intervalo de tiempo, Macie devuelve los datos de los 30 días naturales anteriores.

En los siguientes ejemplos se muestra cómo consultar los costos estimados de uso y las estadísticas mediante AWS Command Line Interface (AWS CLI). También puedes consultar los datos mediante una versión actual de otra herramienta de línea de AWS comandos o un AWS SDK, o enviando las solicitudes HTTPS directamente a Macie. Para obtener información sobre AWS las herramientas y los SDK, consulte Herramientas sobre las que basarse. AWS

Ejemplos

- Ejemplo 1: Consulta de los costos estimados de uso totales
- Ejemplo 2: Consulta de estadísticas de uso

Ejemplo 1: Consulta de los costos estimados de uso totales

Para consultar los costes de uso totales estimados mediante el AWS CLI, ejecute el get-usage-totalscomando y, si lo desea, especifique un intervalo de tiempo para los datos. Por ejemplo:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Donde *MONTH_TO_DATE* especifica el mes natural en curso hasta la fecha como intervalo de tiempo para los datos.

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

Donde `estimatedCost` es el costo estimado de uso total para la métrica de uso asociada (`type`):

- `SENSITIVE_DATA_DISCOVERY`, para analizar objetos de S3 con trabajos de detección de datos confidenciales.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, para analizar objetos de S3 con detección automatizada de datos confidenciales.
- `DATA_INVENTORY_EVALUATION`, para monitorear y evaluar los depósitos de uso general de S3 con fines de seguridad y control de acceso.

- `AUTOMATED_OBJECT_MONITORING`, para evaluar y supervisar su inventario de buckets de S3 a fin de identificar los objetos de S3 que son aptos para análisis mediante detección automatizada de datos confidenciales.

Ejemplo 2: Consulta de estadísticas de uso

Para consultar las estadísticas de uso mediante el AWS CLI, ejecute el get-usage-statisticscomando. Si lo desea, puede ordenar, filtrar y especificar un intervalo de tiempo para los resultados de la consulta. El siguiente ejemplo recupera las estadísticas de uso de una cuenta de administrador de Macie durante los 30 días anteriores. Los resultados se ordenan en orden ascendente por Cuenta de AWS ID.

Para Linux, macOS o Unix, utilice el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad:

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Para Microsoft Windows, utilice el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad:

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

Donde:

- *accountId* especifica el campo que se utilizará para ordenar los resultados.
- *ASC* es el orden de clasificación que se aplica a los resultados, en función del valor del campo especificado (*accountId*).
- *PAST_30_DAYS*especifica los 30 días anteriores como intervalo de tiempo para los datos.

Si el comando se ejecuta correctamente, Macie devuelve una matriz `records`. La matriz contiene un objeto para cada cuenta que se incluye en los resultados de la consulta. Por ejemplo:

```
{
    "records": [
```

```
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2022-11-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
```

```
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```

Donde `estimatedCost` es el costo estimado de uso total para la métrica de uso asociada (`type`) para una cuenta:

- `DATA_INVENTORY_EVALUATION`, para monitorear y evaluar los depósitos de uso general de S3 con fines de seguridad y control de acceso.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, para analizar objetos de S3 con detección automatizada de datos confidenciales.
- `SENSITIVE_DATA_DISCOVERY`, para analizar objetos de S3 con trabajos de detección de datos confidenciales.
- `AUTOMATED_OBJECT_MONITORING`, para evaluar y supervisar el inventario de buckets de S3 de la cuenta a fin de identificar los objetos de S3 que pueden analizarse mediante la detección automática de datos confidenciales.

Participar en la prueba gratuita de Amazon Macie

Al activar Amazon Macie por primera vez, Cuenta de AWS se inscribe automáticamente en la versión de prueba gratuita de 30 días de Macie. Esto incluye las cuentas de los miembros individuales de una organización. AWS Organizations

Durante la prueba gratuita, el uso de Macie no conlleva ningún cargo específico Región de AWS para:

- Realice una supervisión de control preventivo: esto incluye la generación y el mantenimiento de un inventario de los depósitos de uso general de Amazon Simple Storage Service (Amazon S3) en la región. También incluye evaluar y supervisar los buckets para ofrecer seguridad y control de acceso. Para obtener más información, consulte Cómo supervisa Macie la seguridad de los datos de Amazon S3.
- Realizar una detección automatizada de datos confidenciales: esto incluye la supervisión y la evaluación del inventario de buckets de S3 en la región para identificar los objetos de S3 que son aptos para análisis. También incluye el análisis de los objetos aptos y la presentación de informes sobre datos confidenciales, estadísticas, resultados y otros tipos de resultados. Para obtener más información, consulte Cómo funciona la detección automatizada de datos confidenciales.

  La detección automatizada de datos confidenciales solo está disponible para las cuentas de administrador de Macie y las cuentas independientes de Macie. Si tiene una cuenta de administrador de Macie, puede utilizar esta característica para analizar los objetos de los buckets de S3 que sean propiedad de sus cuentas de miembro.

Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie en Referencia general de AWS.

La prueba gratuita dura 30 días consecutivos. No puede pausarla una vez que haya comenzado. Una vez finalizada la prueba gratuita, se empiezan a acumular cargos por realizar la supervisión de controles preventivos. También comienzan a acumularse los cargos por realizar la detección automatizada de datos confidenciales. Si es el administrador Macie de una organización, los cargos se acumulan según corresponda para cada cuenta de su organización. Puede utilizar Macie para revisar los desgloses de los costos estimados de uso de las cuentas individuales de su organización.

> **Note**
>
> La prueba gratuita no incluye el análisis de objetos de S3 mediante trabajos de detección de datos confidenciales. Durante la prueba gratuita, incurrirá en gastos si crea y ejecuta trabajos de detección de datos confidenciales que analicen más de 1 GB de datos sin comprimir. (Macie ofrece un nivel gratuito mensual de detección de datos confidenciales. Cada mes, analizar hasta 1 GB de datos sin comprimir en objetos de S3 es gratuito. Después del primer GB de datos, se van acumulando costos). También puede incurrir en gastos por otras funciones Servicios de AWS que utilice con determinadas funciones de Macie, por ejemplo, si utiliza objetos S3 gestionados por el cliente para desencriptar objetos de S3 que AWS KMS keys desee inspeccionar en busca de datos confidenciales.

Comprobar su estado y los costos estimados durante la prueba gratuita

Durante la prueba gratuita, puede comprobar el estado de la prueba y revisar los costos estimados de uso de su cuenta. Las estimaciones de costos se basan en el uso que haya hecho de Macie hasta el momento durante la prueba gratuita. Pueden ayudarlo a conocer cuáles podrían ser algunos de sus costos de uso una vez finalizada la prueba. Para obtener más información sobre cómo calcula Macie estos valores, consulte Entender cómo se calculan los costos estimados de uso.

Sigue estos pasos para comprobar el estado de su versión de prueba y revisar sus costos estimados de uso en la consola de Amazon Macie. También puede acceder a estos datos mediante programación mediante el GetUsageStatisticsfuncionamiento de la API Amazon Macie.

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee comprobar el estado de la prueba gratuita y sus costes de uso estimados.
3. En el panel de navegación, elija Uso.

La página de Uso indica el número de días restantes de su prueba gratuita. También muestra un desglose de los costos estimados de uso en dólares estadounidenses:

- Supervisión del control preventivo: se trata del coste total previsto de mantener un inventario de los depósitos de uso general de S3 y de evaluar y supervisar los depósitos para garantizar la seguridad y el control de acceso una vez finalizada la prueba gratuita.

- Trabajos de detección de datos confidenciales: se trata del costo total estimado de cualquier trabajo de detección de datos confidenciales que haya realizado. Los trabajos de detección de datos confidenciales no están incluidos en la prueba gratuita.
- Detección automatizada de datos confidenciales: se trata de los costos totales previstos de realizar la detección automatizada de datos confidenciales una vez finalizada la prueba gratuita, desglosados por dimensión del precio: supervisión de objetos y análisis de objetos.

Si es el administrador de Macie de una organización, la página de uso proporciona detalles sobre las cuentas de Macie de su organización. En la tabla:

- Cuota de servicio (puestos de trabajo): es la cuota mensual actual para ejecutar tareas de descubrimiento de datos confidenciales a fin de analizar los objetos de S3 en los depósitos que son propiedad de una cuenta.
- Prueba gratuita: estos campos indican si una cuenta participa actualmente en la prueba gratuita para el control preventivo, la supervisión o el descubrimiento automatizado de datos confidenciales. Un campo de la Prueba gratuita está vacío si la correspondiente prueba gratuita ha finalizado para una cuenta.
- Total: es el costo total estimado de una cuenta.

En la sección Costos estimados se muestran los costos estimados para su organización en general. Para revisar el desglose de los costos estimados para una cuenta específica de su organización, seleccione la cuenta en la tabla. A continuación, en la sección de Costos estimados se muestra este desglose. Para mostrar estos datos para otra cuenta, seleccione la cuenta en la tabla. Para borrar la selección de la cuenta, elija X junto al ID de la cuenta.

> **Note**
>
> Si una cuenta almacena más de 150 TB de datos en Amazon S3, los costos estimados y reales de la detección automatizada de datos confidenciales para la cuenta podrían ser superiores a las proyecciones de costos que Macie proporciona durante la prueba gratuita de 30 días. Esto se debe a que el análisis de objetos mediante la detección automática de datos confidenciales se detiene cuando se hayan analizado 150 GB de datos sin comprimir para una cuenta que se haya inscrito en la prueba gratuita. El análisis de objetos se reanuda para la cuenta una vez finalizada la prueba gratuita.
>
> Si necesita ayuda para la previsión de costos para una cuenta que almacene más de 150 TB de datos en Amazon S3, póngase en contacto con AWS Support. Para gestionar los

costos de la detección automatizada de datos confidenciales una vez finalizada la prueba gratuita, puede excluir buckets de S3 individuales de los análisis posteriores. Para excluir buckets, puede actualizar los ajustes de configuración de su cuenta. También puedes excluir los grupos de case-by-case forma individual al revisar los detalles de cada uno de los grupos de tu inventario.

Administración de varias cuentas de Amazon Macie

Si su entorno AWS tiene varias cuentas, puede asociar las cuentas de Amazon Macie a su entorno y administrarlas de forma centralizada como una organización en Macie. Con esta configuración, un administrador designado de Macie puede evaluar y supervisar el estado general de seguridad del patrimonio de datos de Amazon Simple Storage Service (Amazon S3) de su organización y detectar datos confidenciales en los buckets S3 de su organización. El administrador también puede realizar diversas tareas de gestión y administración de cuentas a gran escala, como supervisar los costos de uso estimados y evaluar las cuotas de las cuentas.

En Macie, una organización consta de una cuenta de administrador designada de Macie y una o más cuentas de miembros asociadas. Puede asociar las cuentas de dos maneras: integrando Macie con AWS Organizations o enviando y aceptando invitaciones de membresía en Macie. Recomendamos que integre Macie con AWS Organizations.

AWS Organizations es un servicio de administración de cuentas global que permite a los administradores AWS consolidar y administrar múltiples Cuentas de AWS de forma centralizada. Proporciona características de facturación unificada y administración de cuentas que están diseñadas para satisfacer las necesidades de presupuestos, seguridad y conformidad. Se ofrece sin coste adicional y se integra con varios Servicios de AWS, incluidos Macie, AWS Security Hub y Amazon GuardDuty. Para obtener más información, consulte la AWS Organizations Guía del usuario.

Si prefiere administrar de forma centralizada varias cuentas de Macie sin necesidad de usar AWS Organizations, puede utilizar en su lugar invitaciones de membresía. Si envía una invitación y otra cuenta la acepta, su cuenta pasa a ser la cuenta de administrador de Macie de la otra cuenta. Si recibe y acepta una invitación, su cuenta pasa a ser una cuenta de miembro de Macie y la cuenta de administrador de Macie puede acceder a determinados ajustes, datos y recursos de su cuenta de Macie y gestionarlos.

Temas

Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie

Si gestiona de forma centralizada varias cuentas de Amazon Macie como organización, el administrador de Macie tendrá acceso a los datos de inventario de Amazon Simple Storage Service (Amazon S3), a los resultados de las políticas y a determinadas configuraciones y recursos de Macie de las cuentas de miembros asociadas. El administrador también puede realizar la detección automatizada de datos confidenciales y ejecutar trabajos de detección de datos confidenciales para detectar dichos datos en los buckets de S3 propiedad de las cuentas de miembros. La compatibilidad para determinados trabajos varía en función de si una cuenta de administrador de Macie está asociada a una cuenta de miembro mediante AWS Organizations o por invitación.

En la tabla siguiente, se detalla la relación entre la cuenta de administrador y las cuentas miembro de Macie. Indica los permisos predeterminados para cada tipo de cuenta. Para restringir aún más el acceso a las características y operaciones de Macie, puede utilizar AWS Identity and Access Managementpolíticas de IAM personalizadas.

En la tabla:

- Auto indica que la cuenta no puede realizar la tarea para ninguna de las cuentas asociadas.
- Cualquiera indica que la cuenta puede realizar la tarea para una cuenta individual asociada.
- Todas indica que la cuenta puede realizar la tarea y que este se aplica a todas las cuentas asociadas.

Un guion (—) indica que la cuenta no puede realizar la acción.

Task	A través de AWS Organizations		Por invitación	
	Administrador	Miembro	Administrador	Miembro
Enable Macie	Any	–	Self	Self
Review the organizat ion's account inventory [1]	All	–	All	–

Add a member account	Any	–	Any	–
Review statistics and metadata for S3 buckets	All	Self	All	Self
Review policy findings	All	Self	All	Self
Suppress (archive) policy findings [2]	All	–	All	–
Publish policy findings [3]	Self	Self	Self	Self
Configure a repository for sensitive data discovery results	Self	Self	Self	Self
Create and use allow lists	Self	Self	Self	Self
Create and use custom data identifiers	Self	Self	Self	Self
Configure and perform automated sensitive data discovery	All	–	All	–

Review automated sensitive data discovery statistics, data, and results	All	–	All	–
Create and run sensitive data discovery jobs [4]	Any	Self	Any	Self
Review the details of sensitive data discovery jobs [5]	Self	Self	Self	Self
Review sensitive data findings [6]	Self	Self	Self	Self
Suppress (archive) sensitive data findings [6]	Self	Self	Self	Self
Publish sensitive data findings [6]	Self	Self	Self	Self
Configure Macie to retrieve sensitive data samples for findings	Self	Self	Self	Self
Retrieve sensitive data samples for findings [7]	Self	Self	Self	Self

Configure publication destinations for findings	Self	Self	Self	Self
Set the publication frequency for findings	All	Self	All	Self
Create sample findings	Self	Self	Self	Self
Review account quotas and estimated usage costs	All	Self	All	Self
Suspend Macie [8]	Any	–	Any	Self
Disable Macie [9]	Self	Self	Self	Self
Remove (disassociate) a member account	Any	–	Any	–
Disassociate from an administrator account	–	–	–	Self
Delete an association with another account [10]	Any	–	Any	Self

1. El administrador de una organización en AWS Organizations puede revisar todas las cuentas de la organización, incluidas las cuentas que no tienen habilitado Macie. El administrador de

una organización basada en invitaciones solo puede revisar las cuentas que se añadan a su inventario.

2. Solo un administrador puede suprimir los resultados de la política. Si un administrador crea una regla de supresión, Macie la aplica a los resultados de la política para todas las cuentas de la organización, a menos que la regla esté configurada para excluir cuentas específicas. Si un miembro crea una regla de supresión, Macie no la aplica a los resultados de política de la cuenta del miembro.

3. Solo la cuenta propietaria de un recurso afectado puede publicar los resultados de la política del recurso en AWS Security Hub. Tanto las cuentas de administrador como las de miembros publican automáticamente los resultados de las políticas de un recurso afectado en Amazon EventBridge.

4. Un miembro puede configurar un trabajo para analizar objetos únicamente en los buckets de S3 que sean propiedad de su cuenta. Un administrador puede configurar un trabajo para analizar objetos de los buckets que sean propiedad de su cuenta o de la cuenta de un miembro. Para obtener información sobre cómo se aplican las cuotas y cómo se calculan los costos de los trabajos con varias cuentas, consulte Entender cómo se calculan los costos estimados de uso.

5. Solo la cuenta que crea un trabajo puede acceder a los detalles del trabajo. Esto incluye los detalles relacionados con el trabajo en el inventario de buckets de S3.

6. Solo la cuenta que crea un trabajo puede acceder, suprimir o publicar los resultados de datos confidenciales que genere el trabajo. Solo un administrador puede acceder a los resultados de datos confidenciales, suprimirlos o publicarlos que se obtengan mediante la detección automatizada de datos confidenciales.

7. Si un resultado de datos confidenciales se aplica a un objeto de S3 que es propiedad de una cuenta de miembro, el administrador podría recuperar muestras de datos confidenciales notificados por el resultado. Esto depende del origen del resultado y de los ajustes de configuración y los recursos de la cuenta de administrador y de la cuenta de miembro. Para obtener más información, consulte Opciones de configuración y requisitos para recuperar muestras de datos confidenciales con resultados.

8. Para que un administrador suspenda Macie en su propia cuenta, primero debe desvincular su cuenta de todas las cuentas de los miembros.

9.

Para que un administrador deshabilite Macie en su propia cuenta, primero debe desvincular su cuenta de todas las cuentas de los miembros y eliminar las asociaciones entre su cuenta y todas esas cuentas. El administrador de una organización en AWS Organizations puede hacerlo mediante la cuenta de administración de la organización para designar una cuenta diferente como cuenta de administrador.

Para que un miembro de una organización de AWS Organizations deshabilite Macie, el administrador debe desvincular antes la cuenta del miembro de su cuenta de administrador. En una organización basada en invitaciones, el miembro puede desvincular la cuenta de su cuenta de administrador y, a continuación, deshabilitar Macie.

10. El administrador de una organización en AWS Organizations puede eliminar una asociación con la cuenta de un miembro después de desvincular la cuenta de su cuenta de administrador. La cuenta sigue apareciendo en el inventario de cuentas del administrador, pero su estado indica que no es una cuenta de miembro. El administrador de una organización basada en invitaciones puede eliminar una asociación con otra cuenta después de desvincular la cuenta de otra cuenta . A continuación, la otra cuenta deja de aparecer en su inventario de cuentas.

Gestionar las cuentas de Amazon Macie con AWS Organizations

Si usa AWS Organizations para gestionar varias Cuentas de AWS de forma centralizada, puede integrar Amazon Macie con AWS Organizations, y luego gestionar Macie para las cuentas de su organización de forma centralizada. Con esta configuración, un administrador designado de Macie puede habilitar y gestionar Macie para hasta 10 000 cuentas. El administrador también puede acceder a los datos de inventario de Amazon Simple Storage Service (Amazon S3) y detectar datos confidenciales en los buckets de S3 que sean propiedad de las cuentas. Para obtener más información sobre las tareas que pueden realizar los administradores, consulte Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

Para integrar Macie con AWS Organizations, hay que empezar por designar una cuenta como la cuenta de administrador delegado de Macie para la organización. A continuación, el administrador de Macie habilita Macie para otras cuentas de la organización, las añade como cuentas de miembros de Macie y configura los ajustes y los recursos de Macie para las cuentas.

> **Tip**
>
> Si ya asoció una cuenta de administrador de Macie a las cuentas de los miembros mediante invitaciones, puede designar esa cuenta como la cuenta de administrador de Macie delegada para su organización en AWS Organizations. Si lo hace, todas las cuentas de miembro asociadas actualmente seguirán siendo miembros y podrá aprovechar al máximo las ventajas de gestionar las cuentas mediante el uso de AWS Organizations. Para obtener más información, consulte Pasar de una organización basada en invitaciones.

En los temas de esta sección se explica cómo integrar Macie con AWS Organizations y cómo administrar y gestionar Macie para las cuentas de una organización.

Temas

Consideraciones y recomendaciones para usar Amazon Macie con AWS Organizations

Antes de integrar Amazon Macie AWS Organizations y configurar su organización en Macie, tenga en cuenta los siguientes requisitos y recomendaciones. Asegúrese también de que entiende la relación entre las cuentas de administrador y de miembro de Macie.

Temas

Designación de una cuenta de administrador de Macie

Al determinar qué cuenta debe ser la cuenta de administrador de Macie delegada para su organización, tenga en cuenta lo siguiente:

- Una organización solo puede tener una cuenta de administrador de Macie delegada.
- Una cuenta no puede ser cuenta de administrador de Macie y cuenta de miembro al mismo tiempo.
- Solo la cuenta AWS Organizations de administración de una organización puede designar la cuenta de administrador delegado de Macie para la organización, y solo la cuenta de administración puede cambiar o eliminar posteriormente esa designación.
- La cuenta AWS Organizations de administración de una organización también puede ser la cuenta de administrador delegada de Macie para la organización. Sin embargo, no recomendamos esta configuración basándonos en las mejores prácticas AWS de seguridad y en el principio del privilegio mínimo. Es probable que los usuarios que tienen acceso a la cuenta de administración para fines de facturación no sean los mismos que los usuarios que necesitan acceder a Macie por motivos de seguridad de la información.

  Si prefiere esta configuración, debe habilitar Macie para la cuenta de administración de la organización en al menos una Región de AWS antes de designar la cuenta como cuenta de administrador delegado de Macie. De lo contrario, la cuenta no podrá acceder a la configuración y los recursos de Macie para las cuentas de miembros y administrarlos.
- A diferencia de AWS Organizations esto, Macie es un servicio regional. Esto significa que la designación de una cuenta de administrador de Macie es una designación Regional. También significa que las asociaciones entre las cuentas de administrador y miembro de Macie son Regionales. Por ejemplo, si la cuenta de administración designa una cuenta de administrador de Macie en la región del Este de EE. UU. (Norte de Virginia), el administrador de Macie solo podrá gestionar Macie para las cuentas de los miembros de esa Región.

  Para gestionar de forma centralizada varias cuentas de Macie Regiones de AWS, la cuenta de administración debe iniciar sesión en cada región en la que la organización utilice o vaya a utilizar Macie y, a continuación, designar la cuenta de administrador de Macie en cada una de esas regiones. De esa forma, la cuenta de administrador de Macie puede configurar la organización en cada una de esas regiones. Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie en Referencia general de AWS.
- Las cuentas se pueden asociar solo a una cuenta de administrador de Macie a la vez. Si su organización utiliza Macie en varias Regiones, la cuenta de administrador de Macie designada

debe ser la misma en todas esas Regiones. Sin embargo, la cuenta de administración de su organización debe designar la cuenta de administrador por separado en cada región.

- Una cuenta puede ser la cuenta de administrador delegada de Macie para una sola organización a la vez. Si gestiona varias organizaciones AWS Organizations, debe designar una cuenta de administrador de Macie diferente para cada organización. Esto se debe a un AWS Organizations requisito: una cuenta solo puede ser miembro de una organización a la vez.
- Si Cuenta de AWS se suspende, aísla o cierra la cuenta del administrador de Macie, todas las cuentas de miembros de Macie asociadas se eliminan automáticamente como cuentas de miembros de Macie, pero Macie no se inhabilita para ellas.

Cambiar o eliminar la designación de una cuenta de administrador de Macie

Solo la cuenta AWS Organizations de administración de una organización puede cambiar o eliminar la designación de una cuenta de administrador delegado de Macie para la organización.

Si la cuenta de administración elimina la designación, todas las cuentas de miembros asociadas se eliminan como cuentas de miembros de Macie, pero Macie no se inhabilita para las cuentas. Para que una cuenta también pueda pausar o dejar de usar Macie, el usuario de la cuenta debe suspender (pausar) o deshabilitar (detener) a Macie para la cuenta.

Agregar y eliminar cuentas de miembros de Macie

A la hora de agregar, eliminar y administrar cuentas de miembros de su organización, tenga en cuenta lo siguiente:

- Una cuenta de administrador de Macie puede estar asociada a un máximo de 10 000 cuentas de miembros de Macie activas (habilitadas) en cada Región de AWS. Si su organización supera esta cuota, el administrador de Macie no podrá añadir cuentas de miembros hasta que elimine el número necesario de cuentas de miembros existentes en la Región.

  Cuando una organización cumple con esta cuota, se lo notificamos al administrador de Macie mediante la creación AWS Health de CloudWatch eventos de Amazon para su cuenta. También envíamos un correo electrónico a la dirección de correo vinculada con su cuenta

  Si es el administrador de Macie de una organización, puede determinar cuántas cuentas de miembros activas están asociadas actualmente a su cuenta mediante la página Cuentas de la consola de Amazon Macie o mediante el funcionamiento de DescribeOrganizationConfigurationla

API de Amazon Macie. Para obtener más información, consulte Revisión de las cuentas de Amazon Macie para una organización.

- Las cuentas se pueden asociar solo a una cuenta de administrador de Macie a la vez. Esto significa que una cuenta no puede aceptar una invitación de Macie desde otra cuenta si ya está asociada a la cuenta de administrador de Macie de una organización en AWS Organizations.

  Del mismo modo, si una cuenta ya ha aceptado una invitación, el administrador de Macie de una organización no AWS Organizations podrá añadir la cuenta como cuenta de miembro de Macie. La cuenta primero debe desasociarse de su cuenta de administrador actual, basada en una invitación.
- Para añadir la cuenta AWS Organizations de gestión como cuenta de miembro de Macie, un usuario de la cuenta de gestión debe habilitar primero Macie para la cuenta. El administrador de Macie no puede habilitar Macie para la cuenta de administración.
- Una cuenta de miembro no se puede desvincular de su cuenta de administrador de Macie. Solo el administrador de Macie puede eliminar una cuenta como cuenta de miembro de Macie.
- Si el administrador de Macie elimina una cuenta de miembro de Macie, Macie seguirá habilitada para la cuenta. Para que una cuenta también pueda pausar o dejar de usar Macie, el usuario de la cuenta debe suspender (pausar) o deshabilitar (detener) Macie para la cuenta.

Pasar de una organización basada en invitaciones

Si ya asoció una cuenta de administrador de Macie a las cuentas de los miembros mediante invitaciones de membresía de Macie, le recomendamos que designe esa cuenta como la cuenta de administrador de Macie delegada para su organización en AWS Organizations. Esto simplifica la transición desde una organización basada en invitaciones.

Si lo hace, todas las cuentas de miembros actualmente asociadas seguirán siendo miembros. Si una cuenta de miembro forma parte de su organización AWS Organizations, la asociación de la cuenta cambiará automáticamente de Por invitación a Via AWS Organizations in Macie. Si la cuenta de un miembro no forma parte de tu organización en AWS Organizations, la asociación de la cuenta seguirá siendo Por invitación. En ambos casos, las cuentas seguirán asociadas a la cuenta de administrador delegado de Macie como cuentas de miembros.

Recomendamos este enfoque porque una cuenta no se puede asociar a más de una cuenta de administrador de Macie al mismo tiempo. Si designa una cuenta diferente como cuenta de administrador de Macie para su organización AWS Organizations, el administrador designado no podrá administrar las cuentas que ya estén asociadas a otra cuenta de administrador de Macie por invitación. Cada cuenta de miembro debe desvincularse primero de su cuenta de

administrador actual, basada en una invitación. El administrador de Macie de su organización en AWS Organizations podrá entonces añadir la cuenta como cuenta de miembro de Macie y empezar a administrarla.

Tras integrar Macie AWS Organizations y configurar su organización en Macie, si lo desea, puede designar otra cuenta de administrador de Macie para la organización. También puede seguir utilizando las invitaciones para asociar y administrar cuentas de miembros que no formen parte de su organización en AWS Organizations.

Integración y configuración de una organización en Amazon Macie

Cuando usa Amazon Macie con AWS Organizations, la cuenta de administración AWS Organizations de la organización puede designar una cuenta de la organización como la cuenta de administrador delegada de Macie. Esto habilita a Macie como servicio de confianza en AWS Organizations. También habilita a Macie en la cuenta Región de AWS de administrador actual designada y permite que la cuenta de administrador designada habilite y administre Macie para otras cuentas de la organización en esa región. Para obtener información sobre cómo se conceden estos permisos, consulte Uso AWS Organizations con otros Servicios de AWS en la Guía del usuario AWS Organizations.

A continuación, el administrador delegado de Macie configura la organización en Macie, principalmente añadiendo las cuentas de la organización como cuentas de miembros de Macie en la región. A continuación, el administrador puede acceder a determinados ajustes, datos y recursos de Macie para esas cuentas de esa región.

En este tema se explica cómo designar a un administrador delegado de Macie para una organización y cómo añadir las cuentas de la organización como cuentas de miembros de Macie. Antes de realizar estas tareas, asegúrese de entender la relación entre las cuentas de administrador y de miembro. También es una buena idea revisar las consideraciones y recomendaciones para usar Macie con AWS Organizations.

Tareas

- Paso 1: Verificar sus permisos
- Paso 2: designar la cuenta de administrador delegada de Macie para la organización
- Paso 3: habilitar automáticamente nuevas cuentas de miembro de la organización como cuentas miembro de Macie
- Paso 4: habilitar y añadir cuentas de la organización existentes como cuentas de miembros de Macie

Para integrar y configurar la organización en varias regiones, la cuenta de administración AWS Organizations y el administrador delegado de Macie repiten estos pasos en cada región adicional.

Paso 1: Verificar sus permisos

Antes de designar la cuenta de administrador de Macie delegada para su organización, compruebe que usted (como usuario de la cuenta de administración AWS Organizations) está autorizado a realizar la siguiente acción de Macie: `macie2:EnableOrganizationAdminAccount`. Esta acción le permite designar la cuenta de administrador de Macie delegada para su organización mediante Macie.

Compruebe también que está autorizado a realizar las siguientes acciones: AWS Organizations

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Estas acciones le permiten: recuperar información sobre su organización; integrar Macie con AWS Organizations; recuperar la información con la que Servicios de AWS se ha integrado con AWS Organizations; y designar una cuenta de administrador de Macie delegada para su organización.

Para conceder estos permisos, incluya la siguiente declaración en la política (de IAM) AWS Identity and Access Management de su cuenta:

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

Si desea designar su cuenta de administración AWS Organizations como la cuenta de administrador delegada de Macie para la organización, su cuenta también necesita permiso para realizar la

siguiente acción de IAM: `CreateServiceLinkedRole`. Esta acción le permite habilitar Macie para la cuenta de administración. Sin embargo, basándonos en las mejores prácticas de seguridad AWS y en el principio del privilegio mínimo, no le recomendamos que lo haga.

Si decide conceder este permiso, añada la siguiente instrucción a la política de IAM para la cuenta de administración AWS Organizations:

```
{
   "Sid": "Grant permissions to enable Macie",
   "Effect": "Allow",
   "Action": [
      "iam:CreateServiceLinkedRole"
   ],
   "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
   "Condition": {
      "StringLike": {
         "iam:AWSServiceName": "macie.amazonaws.com"
      }
   }
}
```

En la instrucción, sustituya *111122223333* por el identificador de cuenta de la cuenta de gestión.

Si desea administrar Macie en una Región de AWS opcional (región que está deshabilitada de forma predeterminada), actualice también el valor de la entidad principal de servicio de Macie en el elemento `Resource` y la condición `iam:AWSServiceName`. El valor debe especificar el código de región de la región. Por ejemplo, para administrar Macie en la región de Medio Oriente (Baréin), que tiene el código de región me-south-1, haga lo siguiente:

- En el elemento `Resource`, sustituya

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  with

  `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`

Donde *111122223333* especifica el ID de la cuenta de administración y *me-south-1* especifica el código de la región.

- En la condición `iam:AWSServiceName`, sustituya `macie.amazonaws.com` por `macie.me-south-1.amazonaws.com`, donde *me-south-1* especifica el código de la región.

Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie cuotas en la Referencia general de AWS. Para obtener más información, consulte Especificación de las Regiones de AWS que puede usar su cuenta en la Guía de referencia de AWS Account Management.

Paso 2: designar la cuenta de administrador delegada de Macie para la organización

Tras verificar sus permisos, usted (como usuario de la cuenta de administración AWS Organizations) puede designar la cuenta de administrador delegado de Macie para su organización.

Designar la cuenta de administrador delegada de Macie para una organización

Para designar la cuenta de administrador delegado de Macie para su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Solo un usuario de la cuenta de administración AWS Organizations puede realizar esta tarea.

Console

Siga estos pasos para designar la cuenta de administrador delegada de Macie mediante la consola de Amazon Macie.

Designar la cuenta de administrador delegada de Macie

1. Inicie sesión en la AWS Management Console mediante la cuenta de administración de AWS Organizations.
2. Con el selector Región de AWS de la esquina superior derecha de la página, seleccione la Región en la que desea designar la cuenta de administrador delegada de Macie para su organización.
3. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
4. Lleve a cabo una de las siguientes acciones, en función de si Macie está habilitada para su cuenta de administración en la región actual:

   - Si Macie no está activado, seleccione Comenzar en la página de bienvenida.

- Si Macie está activado, seleccione Configuración en el panel de navegación.

5. En Administrador delegado, introduzca el ID de cuenta de 12 dígitos para el Cuenta de AWS que desea designar como cuenta de administrador de Macie.
6. Seleccione Delegar.

Repita los pasos anteriores en cada región adicional en la que desee integrar la organización con Macie. Debe designar la misma cuenta de administrador de Macie en cada una de esas regiones.

API

Para designar la cuenta de administrador de Macie delegada mediante programación, utilice la operación EnableOrganizationAdminAccount de la API de Amazon Macie. Para designar la cuenta en varias regiones, envíe la designación para cada región en la que desee integrar la organización con Macie. Debe designar la misma cuenta de administrador de Macie en cada una de esas regiones.

Cuando envíe la designación, use el parámetro de `adminAccountId`, especifique el ID de cuenta de 12 dígitos de la Cuenta de AWS para designar como la nueva cuenta de administrador de Macie para la organización. Asegúrese también de especificar la región a la que se aplica la designación.

Para designar la cuenta de administrador de Macie mediante AWS Command Line Interface(AWS CLI), ejecute el comando enable-organization-admin-account. Para el parámetro de `admin-account-id`, especifique el ID de cuenta de 12 dígitos para la Cuenta de AWS que desea designar. Utilice el parámetro de `region` para especificar la región a la que se aplica la designación. Por ejemplo:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333
```

Cuando *us-east-1* es la región a la que se aplica la designación (Este de EE. UU. (Norte de Virginia)) y *111122223333* es el ID de la cuenta que se va a designar.

Tras designar la cuenta de administrador de Macie para su organización, el administrador de Macie puede empezar a configurar la organización en Macie.

Paso 3: habilitar automáticamente nuevas cuentas de miembro de la organización como cuentas miembro de Macie

De forma predeterminada, Macie no se habilita automáticamente para las cuentas nuevas cuando las añade a su organización en AWS Organizations. Además, las cuentas no se añaden automáticamente como cuentas de miembro de Macie. Las cuentas aparecen en el inventario de cuentas del administrador de Macie. Sin embargo, Macie no está necesariamente habilitado para las cuentas y el administrador de Macie no necesariamente puede acceder a la configuración, los datos y los recursos de Macie relacionados con las cuentas.

Si es el administrador delegado de Macie para la organización, puede cambiar este ajuste de configuración para su organización. Si activas la configuración de Activación automática, Macie se habilitará automáticamente para nuevas cuentas al añadirlas a tu organización en AWS Organizations, y las cuentas se asociarán automáticamente a tu cuenta de administrador de Macie como cuentas de miembros. La habilitación de esta configuración no afecta a las cuentas existentes en la organización. Para habilitar y administrar Macie para las cuentas existentes, debe añadir manualmente las cuentas como cuentas de miembro de Macie. El siguiente paso explica cómo se realiza.

> **Note**
>
> Si activa la configuración de Activación automática, ten en cuenta las siguientes excepciones:
>
> - Si ya hay una cuenta nueva asociada a otra cuenta de administrador de Macie, Macie no añadirá automáticamente la cuenta como cuenta de miembro de su organización.
>
> La cuenta debe desasociarse de su cuenta de administrador actual de Macie para poder formar parte de su organización en Macie. A continuación, puede añadir la cuenta manualmente. Para identificar las cuentas en las que este sea el caso, puede revisar el inventario de cuentas de su organización.
> - Si su organización alcanza la cuota de 10 000 cuentas de miembros de Macie en unaRegión de AWS, Macie desactiva automáticamente esta configuración en la región.
>
> Si esto ocurre, se lo notificaremos mediante la creación de eventos AWS Health de Amazon CloudWatch para su cuenta de administrador de Macie. También enviamos correos electrónicos a la dirección asociada a esa cuenta. Si el número total de cuentas se reduce posteriormente a menos de 10 000 cuentas, Macie volverá a activar automáticamente la configuración.

Para habilitar y añadir automáticamente nuevas cuentas de la organización como cuentas de miembros de Macie

Para activar y añadir nuevas cuentas automáticamente como cuentas de miembro de Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Sólo el administrador de Macie delegado de la organización puede realizar esta tarea.

Console

Para realizar esta tarea mediante la consola, debe poder realizar la siguiente acción AWS Organizations: `organizations:ListAccounts`. Esta acción permite recuperar y mostrar información sobre las cuentas de la organización. Si dispone de estos permisos, siga estos pasos para activar y añadir automáticamente nuevas cuentas de la organización como cuentas de miembros de Macie.

Activar y añadir nuevas cuentas de organización automáticamente

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea habilitar y añadir automáticamente nuevas cuentas como cuentas de miembros de Macie.
3. En el panel de navegación, en Configuración, seleccione Cuentas.
4. En la página Cuentas, junto a Añadir cuentas, active la configuración de Activación automática.

Repita los pasos anteriores en cada región adicional en la que desee configurar la organización de Macie.

Para cambiar posteriormente esta configuración y dejar de habilitar y añadir nuevas cuentas automáticamente, repita los pasos anteriores y desactive la configuración de Activación automática.

API

Para activar y añadir automáticamente nuevas cuentas de miembros de Macie mediante programación, utilice la operación UpdateOrganizationConfiguration de la API de Amazon Macie. Cuando envíe su solicitud, defina el valor del parámetro `autoEnable` en `true`. (El valor predeterminado es `false`). Asegúrese también de especificar la región a la que se aplica la

solicitud. Para habilitar y añadir nuevas cuentas automáticamente en otras regiones, envíe la solicitud para cada región adicional.

Si utiliza la AWS CLI para enviar la solicitud, ejecute el comando update-organization-configuration y especifique el parámetro `auto-enable` para habilitar y añadir nuevas cuentas automáticamente. Por ejemplo:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

Mientras *us-east-1* es la región en la que se habilitan y agregan nuevas cuentas de forma automática, la región Este de EE. UU. (Norte de Virginia).

Para cambiar posteriormente esta configuración y dejar de habilitar y añadir nuevas cuentas automáticamente, ejecute el mismo comando de nuevo y utilice el parámetro `no-auto-enable`, en lugar del parámetro `auto-enable`, en cada región aplicable.

Paso 4: habilitar y añadir cuentas de la organización existentes como cuentas de miembros de Macie

Cuando integra Macie concAWS Organizations, Macie no se habilita automáticamente para todas las cuentas existentes en tu organización. Además, las cuentas no se asocian automáticamente a la cuenta de administrador delegada de Macie como cuentas de miembros de Macie.

Por lo tanto, el último paso para integrar y configurar su organización en Macie es añadir las cuentas de la organización existentes como cuentas de miembros de Macie. Al añadir una cuenta existente como cuenta de miembro de Macie, Macie se habilita automáticamente para la cuenta y usted (como administrador delegado de Macie) obtiene acceso a determinados ajustes, datos y recursos de Macie para la cuenta.

Tenga en cuenta que no puede añadir una cuenta que esté asociada actualmente a otra cuenta de administrador de Macie. Para añadir la cuenta, trabaje con el propietario de la cuenta para desasociarla primero de su cuenta de administrador actual. Además, no puedes añadir una cuenta existente si Macie está actualmente suspendida en la cuenta. El propietario de la cuenta primero debe volver a habilitar Macie para la cuenta. Por último, si desea añadir la cuenta de administración AWS Organizations como una cuenta de miembro, el usuario de esa cuenta primero debe habilitar Macie para la cuenta.

Habilitar y añadir cuentas de organización existentes como cuentas de miembros de Macie

Para activar y añadir cuentas de organización existentes como cuentas de miembros de Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Sólo el administrador de Macie delegado de la organización puede realizar esta tarea.

Console

Para realizar esta tarea mediante la consola, debe poder realizar la siguiente acción AWS Organizations: `organizations:ListAccounts`. Esta acción permite recuperar y mostrar información sobre las cuentas de la organización. Si dispone de estos permisos, siga estos pasos para activar y añadir las cuentas existentes como cuentas de miembro de Macie.

Para activar y añadir las cuentas de la organización existentes

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea habilitar y añadir cuentas de organización existentes como cuentas de miembros de Macie.
3. En el panel de navegación, en Configuración, seleccione Cuentas.

   Se abre la página de Cuentas y muestra una tabla con las cuentas asociadas a su cuenta de Macie. Si una cuenta forma parte de su organización en AWS Organizations, su Tipo es Vía AWS Organizations. Si una cuenta no es una cuenta de miembro de Macie, su Estado es No miembro.
4. En la tabla Cuentas, seleccione la casilla de verificación para cada cuenta que desee agregar como cuenta de miembro de Macie.

   > **Tip**
   >
   > Para identificar más fácilmente las cuentas que desea añadir, puede filtrar la tabla. Para ello, coloque el cursor en el cuadro de filtro situado encima de la tabla y, a continuación, seleccione Estado. A continuación, seleccione Estado = No es miembro.
5. En el menú Acciones, elija Añadir miembro.
6. Confirme que desea añadir como miembros el número de cuentas seleccionadas.

Tras confirmar la adición de las cuentas seleccionadas, el estado de las cuentas cambia a Creación/Activación y, a continuación, Activada.

Repita los pasos anteriores en cada región adicional en la que desee configurar la organización de Macie.

API

Para habilitar y añadir mediante programación una o más cuentas existentes como cuentas de miembros de Macie, utilice la operación CreateMember de la API de Amazon Macie. Cuando envíe su solicitud, utilice los parámetros admitidos para especificar el ID de cuenta de 12 dígitos y la dirección de correo electrónico de cada Cuenta de AWS para activarlas y añadirlas. Especifica también la región a la que se aplica la solicitud. Para habilitar y añadir cuentas existentes en regiones adicionales, envíe la solicitud para cada región adicional.

Para recuperar el ID de cuenta y la dirección de correo electrónico de una Cuenta de AWS para habilitar y añadir, puede utilizar opcionalmente la operación ListMembers de la API de Amazon Macie. Esta operación proporciona detalles sobre las cuentas asociadas a su cuenta de Macie, incluidas las cuentas que no son cuentas de miembros de Macie. Si el valor de la propiedad `relationshipStatus` de una cuenta no es`Enabled`, la cuenta no es una cuenta de miembro de Macie.

Para habilitar y añadir una o más cuentas existentes mediante el AWS CLI, ejecute el comando create-member. Utilice el parámetro `region` para especificar la región en la que desea habilitar y añadir las cuentas. Utilice los parámetros `account` para especificar el ID de cuenta y la dirección de correo electrónico de cada Cuenta de AWS para añadirlos. Por ejemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Donde *us-east-1* es la región en la que se debe habilitar y añadir la cuenta como cuenta de miembro de Macie (Este de EE. UU. (Norte de Virginia)), y `account` los parámetros especifican el identificador de cuenta (*123456789012*) y la dirección de correo electrónico (*janedoe@example.com*) de la cuenta.

Si la solicitud se aprueba, el estado (`relationshipStatus`) de la cuenta especificada cambia a `Enabled` en el inventario de su cuenta.

Revisión de las cuentas de Amazon Macie para una organización

Una vez integrada y configurada una organización AWS Organizations en Amazon Macie, el administrador delegado de Macie de la organización puede acceder a un inventario de las cuentas

de la organización en Macie. Como administrador de Macie de una organización, puede utilizar este inventario para revisar las estadísticas y los detalles de las cuentas de Macie de su organización en Región de AWS. También puede utilizar este inventario para gestionar las cuentas de los miembros de Macie en una Región.

Revisión de las cuentas de Macie para una organización

Para revisar las cuentas de su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para revisar las cuentas de Macie de su organización mediante la consola de Amazon Macie.

Para revisar las cuentas de su organización

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea revisar las cuentas de su organización.
3. En el panel de navegación, en Settings, seleccione Accounts.

Se abre la página Cuentas y muestra estadísticas añadidas y una tabla de las cuentas que están asociadas a su cuenta de Macie en el Región de AWS actual.

En la parte superior de la página de Cuentas, encontrará las siguientes estadísticas agregadas.

Vía AWS Organizations

Informes activos indica el número total de cuentas que están asociadas a su cuenta mediante AWS Organizations y que actualmente son cuentas de miembros de Macie en su organización. Macie está habilitado para estas cuentas y tú eres el administrador de las cuentas en Macie.

Todos indica el número total de cuentas que están asociadas a su cuenta mediante AWS Organizations, incluidas las cuentas que actualmente no son cuentas de miembros de Macie.

Por invitación

Informes activos indica el número total de cuentas que están asociadas a su cuenta mediante Macie y que actualmente son cuentas de miembros de Macie. (Estas cuentas no están

asociadas directamente a su cuenta mediante AWS Organizations). Macie está habilitado para las cuentas y usted es el administrador de las cuentas de Macie porque ellos han aceptado una invitación suya a ser miembro de Macie.

Todos indica el número total de cuentas asociadas a su cuenta por invitación de Macie, incluidas las cuentas que no han respondido a una invitación suya.

Activo/Todos

Activo indica el número total de cuentas que actualmente son cuentas de miembros de Macie para su cuenta, ya sea mediante AWS Organizations o por invitación de Macie. Macie está habilitado para estas cuentas y tú eres el administrador de las cuentas en Macie.

Todos indica el número total de cuentas que están asociadas a su cuenta, ya sea por AWS Organizations o por invitación de Macie. Esto incluye las cuentas que forman parte de su organización en AWS Organizations y que actualmente no son cuentas de miembros de Macie, así como las cuentas que no hayan respondido a una invitación suya para ser miembros de Macie.

En la tabla, encontrará detalles sobre cada cuenta de la Región actual. La tabla incluye todas las cuentas que están asociadas a tu cuenta de Macie, ya sea por AWS Organizations o por invitación de Macie.

ID de cuenta

El ID de cuenta y la dirección de correo electrónico para Cuenta de AWS.

Nombre

El nombre de la cuenta para Cuenta de AWS. Este valor suele ser N/A para las cuentas que están asociadas a su cuenta por invitación de Macie.

Tipo

Cómo se asocia la cuenta a tu cuenta, mediante AWS Organizations o una invitación de Macie.

Estado

El estado de la relación entre su cuenta y la cuenta. Para una cuenta de una organización AWS Organizations (el tipo es mediante AWS Organizations), los valores posibles son:

- Cuenta suspendida: La Cuenta de AWS está suspendida.

- Creada/activación: Macie está procesando una solicitud para habilitar y añadir la cuenta como cuenta de miembro de Macie.
- Activada: la cuenta es una cuenta de miembro de Macie. Macie está habilitado para esta cuenta y tú eres el administrador de la cuenta en Macie.
- No es miembro: la cuenta forma parte de su organización en AWS Organizations pero no es una cuenta de miembro de Macie.
- En pausa (suspendida): la cuenta es una cuenta de miembro de Macie, pero Macie está actualmente suspendida.
- Región deshabilitada: la cuenta forma parte de su organización en AWS Organizations pero la región actual está deshabilitada para Cuenta de AWS.
- Eliminada (disociada): la cuenta anteriormente era una cuenta de miembro de Macie, pero posteriormente se eliminó como cuenta de miembro. Has desvinculado la cuenta de tu cuenta de administrador de Macie. Macie sigue habilitada para la cuenta.

Última acción

Cuando usted o la cuenta asociada realizaron por última vez una acción que afectó a la relación entre sus cuentas.

Para ordenar la tabla por un campo específico, haga clic en el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a hacer clic en el encabezado de la columna. Para filtrar la tabla, coloque el cursor en el cuadro de filtro y, a continuación, añada una condición de filtro para un campo. Para refinar aún más los resultados, añada condiciones de filtro para campos adicionales.

API

Para revisar las cuentas de su organización mediante programación, utilice la operación ListMembers de la API Amazon Macie y asegúrese de especificar la región a la que se aplica su solicitud. Para revisar las cuentas en otras Regiones, envíe su solicitud en cada Región adicional.

Cuando envíe su solicitud, utilice el parámetro `onlyAssociated` para especificar qué cuentas incluir en la respuesta. Por defecto, Macie solo devuelve los detalles de las cuentas que son cuentas de miembros de Macie en la región especificada, ya sea mediante AWS Organizations o una invitación de Macie. Para recuperar estos detalles de todas las cuentas asociadas a su cuenta de Macie, incluidas las cuentas que no son cuentas de miembros, incluya el parámetro `onlyAssociated` en su solicitud y establezca el valor del parámetro en `false`.

Para revisar las cuentas de su organización mediante AWS Command Line Interface(AWS CLI), ejecute el comando list-members. Para el parámetro `only-associated`, especifique si desea incluir todas las cuentas asociadas o solo las cuentas de los miembros de Macie. Para incluir solo las cuentas de los miembros, omita este parámetro o establezca el valor del parámetro en `true`. Para incluir todas las cuentas, defina este valor en `false`. Por ejemplo:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Si *us-east-1* es la región a la que se aplica la solicitud, la región Este de EE. UU. (Norte de Virginia).

Si la solicitud se realiza correctamente, Macie devuelve una `members` matriz. La matriz contiene un objeto `member` para cada cuenta que cumple los criterios especificados en la solicitud. En ese objeto, el campo `relationshipStatus` indica el estado actual de la relación entre su cuenta y la otra cuenta de la región especificada. Para una cuenta de una AWS Organizations organización, los valores posibles son:

- `AccountSuspended`: La Cuenta de AWS está suspendida.
- `Created`: Macie está procesando una solicitud para habilitar y añadir la cuenta como cuenta de miembro de Macie.
- `Enabled`: La cuenta es una cuenta de miembro de Macie. Macie está habilitado para esta cuenta y tú eres el administrador de la cuenta en Macie.
- `Paused`: La cuenta es una cuenta de miembro de Macie, pero actualmente Macie tiene la cuenta suspendida (en pausa).
- `RegionDisabled`: La cuenta forma parte de su organización, AWS Organizations pero la región actual está deshabilitada para la. Cuenta de AWS
- `Removed`: la cuenta anteriormente era una cuenta de miembro de Macie, pero posteriormente se eliminó como cuenta de miembro. Has desvinculado la cuenta de tu cuenta de administrador de Macie. Macie sigue habilitada para la cuenta.

Para obtener información sobre otros campos del objeto `member`, consulte Miembros en la Referencia de API de Amazon Macie.

Administrar las cuentas de los miembros de Amazon Macie para una organización

Una vez integrada y configurada una organización AWS Organizations en Amazon Macie, el administrador de Macie delegado de la organización puede acceder a determinados ajustes, datos y recursos de Macie para las cuentas de los miembros.

Como administrador de Macie de una organización, puede realizar determinadas tareas de administración y administración de cuentas de forma centralizada en Macie. Por ejemplo:

- Agregar y eliminar cuentas de miembros de Macie
- Administre el estado de Macie para cuentas individuales, por ejemplo, habilite o suspenda Macie para una cuenta
- Supervise las cuotas de Macie y los costos de uso estimados de las cuentas individuales y de la organización en general

También puede consultar los datos de inventario de Amazon Simple Storage Service (Amazon S3) y los resultados de las políticas de las cuentas de los miembros de Macie. Además, puede encontrar datos confidenciales en los buckets de S3 que son propiedad de las cuentas. Para obtener una lista detallada de las tareas que puede realizar, consulteComprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

De forma predeterminada, Macie le ofrece visibilidad de los datos y recursos relevantes de todas las cuentas de miembros de Macie de su organización. También puede profundizar para revisar los datos y los recursos de las cuentas individuales. Por ejemplo, si utiliza el panel Resumen para evaluar la postura de seguridad de Amazon S3 de su organización, puede filtrar los datos por cuenta. Del mismo modo, si monitoriza los costos de uso estimados, puede acceder a los desgloses de los costos estimados de las cuentas de los miembros individuales.

Además de las tareas que son comunes a las cuentas de administrador y de miembros, puede realizar diversas tareas administrativas para su organización.

Tareas

- Agregar cuentas de miembros de Amazon Macie a una organización
- Suspensión de Amazon Macie para las cuentas de los miembros de una organización
- Eliminar cuentas de miembro de Amazon Macie de una organización

Como administrador de Macie de una organización, puede realizar estas tareas mediante la consola de Amazon Macie o la API de Amazon Macie. Si prefiere usar la consola, tenga en cuenta que debe poder realizar la siguiente acción AWS Organizations: `organizations:ListAccounts`. Esta acción le permite recuperar y mostrar información sobre cuentas que forman parte de su organización en AWS Organizations.

Agregar cuentas de miembros de Amazon Macie a una organización

En algunos casos, es posible que tenga que agregar manualmente una cuenta como cuenta de miembro de Macie. Este es el caso de las cuentas que previamente eliminó (desasoció) como cuentas de miembro. Este también es el caso si no configuraste Macie para que habilitara y agregara automáticamente nuevas cuentas como cuentas de miembro cuando se agreguen cuentas a tu organización en AWS Organizations.

Al añadir una cuenta como cuenta de miembro de Macie, Macie se habilita para la cuenta en la actual Región de AWS, si aún no lo está en esa región, y la cuenta se asocia a su cuenta de administrador de Macie como cuenta de miembro en la región. La cuenta de miembro no recibe ninguna invitación ni ninguna otra notificación en la que se indique que usted ha establecido esta relación entre sus cuentas.

Tenga en cuenta que no puede añadir una cuenta que ya esté asociada a otra cuenta de administrador de Macie. La cuenta primero debe desasociarse de su cuenta de administrador actual. Además, no puede añadir la cuenta de administración AWS Organizations como cuenta de miembro a menos que la cuenta de administración ya haya habilitado Macie para la cuenta. Para obtener más información sobre los requisitos adicionales, consulte Consideraciones y recomendaciones para usar Amazon Macie con AWS Organizations.

Añadir una cuenta de miembro de Macie a una organización

Para añadir una o más cuentas de miembros de Macie a su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para añadir una o más cuentas de miembro de Macie mediante la consola de Amazon Macie.

Añadir una cuenta de miembro de Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. Con el selector Región de AWS de la esquina superior derecha de la página, seleccione la región de en la que desea añadir una cuenta de miembro.
3. En el panel de navegación, en Configuración, seleccione Cuentas. Se abre la página Cuentas y muestra una tabla con las cuentas asociadas a su cuenta.
4. (Opcional) Para identificar más fácilmente las cuentas que forman parte de su organización en AWS Organizations y no son cuentas de miembros de Macie, utilice el cuadro de filtro situado encima de la tabla para añadir las siguientes condiciones de filtrado:

   - Tipo: Organization
   - Estado: No es miembro

   Para mostrar también las cuentas que ha eliminado anteriormente y que tal vez desee añadir como cuentas de miembros, añada también la condición de filtro Estado = Eliminado.
5. En la tabla Cuentas, seleccione la cuenta o cuentas que desea añadir como miembro al marcar la casilla.
6. En el menú Acciones, elija Añadir miembro.
7. Confirme que desea añadir la cantidad seleccionada de cuentas como cuentas de miembros.

Tras confirmar las selecciones, el estado de las cuentas seleccionadas cambia a Creado/Activado y, a continuación, Activado en el inventario de cuentas.

Repita los pasos anteriores en cada región adicional en la que desee añadir una cuenta de miembro.

API

Para añadir una o más cuentas de miembros de Macie mediante programación, utilice la operación CreateMember de la API de Amazon Macie.

Cuando envíe su solicitud, utilice los parámetros admitidos para especificar el ID de cuenta de 12 dígitos y la dirección de correo electrónico de cada Cuenta de AWS que desee añadir. Especifica también la región a la que se aplica la solicitud. Para añadir una cuenta en regiones adicionales, envíe su solicitud en cada región adicional.

Para recuperar el ID de cuenta y la dirección de correo electrónico de la cuenta que desee añadir, puede correlacionar el resultado de la operación ListAccounts de la API AWS Organizations y la operación ListMembers de la API de Amazon Macie. Para la operación ListMembers de la API de Macie, incluya el parámetro `onlyAssociated` en su solicitud y defina el valor del parámetro

en `false`. Si la operación se realiza correctamente, Macie devuelve una matriz `members` que proporciona detalles sobre todas las cuentas asociadas a su cuenta de administrador de Macie en la región especificada, incluidas las cuentas que actualmente no son cuentas de miembros. En la matriz, anote lo siguiente:

- Si el valor de la propiedad `relationshipStatus` de una cuenta no es `Enabled`, la cuenta está asociada a la suya, pero no es una cuenta de miembro de Macie.
- Si una cuenta no está incluida en la matriz, pero sí en el resultado de la operación ListAccountsde la APIAWS Organizations , la cuenta forma parte de su organización en AWS Organizations pero no está asociada a ella y, por lo tanto, no es una cuenta de miembro de Macie.

Para añadir una cuenta de miembro mediante el AWS CLI, ejecute el comando create-member. Utilice el parámetro `region` para especificar la región en la que se va a añadir la cuenta. Utilice los parámetros `account` para especificar el ID de cuenta y la dirección de correo electrónico de cada cuenta que desee añadir. Por ejemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Donde *us-east-1* es la región en la que se va a añadir la cuenta como cuenta de miembro (Este de EE. UU. (Norte de Virginia)), y los parámetros `account` especifican el identificador de la cuenta (*123456789012*) y la dirección de correo electrónico (*janedoe@example.com*) de la cuenta.

Si la solicitud se aprueba, el estado (`relationshipStatus`) de la cuenta especificada cambia a `Enabled` en el inventario de su cuenta.

Suspensión de Amazon Macie para las cuentas de los miembros de una organización

Como administrador de Macie de una organización en AWS Organizations, puedes suspender a Macie por una cuenta de miembro de tu organización. Si lo hace, también podrá volver a habilitar Macie para la cuenta más adelante.

Cuando se suspende Macie de una cuenta de miembro:

- Macie pierde el acceso y deja de proporcionar metadatos sobre los datos Amazon S3 de la cuenta en el actual Región de AWS.

- Macie deja de realizar todas las actividades para la cuenta en la región. Esto incluye la supervisión de los buckets de S3 para garantizar la seguridad y el control de acceso, la detección automática de datos confidenciales y la ejecución de las tareas de detección de datos confidenciales que se estén realizando actualmente.
- Macie cancela todos los trabajos de detección de datos confidenciales creados por la cuenta en la región. Un trabajo no se puede reanudar ni reiniciar después de cancelarse.

  Si ha creado trabajos para analizar los datos que son propiedad de la cuenta de miembro, Macie no los cancela. En su lugar, los trabajos omiten los recursos que son propiedad de la cuenta.

Mientras una cuenta esté suspendida, Macie conserva el identificador de sesión de Macie, la configuración y los recursos de la cuenta en la región correspondiente. Por ejemplo, los resultados de la cuenta permanecen intactos y no se ven afectados durante un máximo de 90 días. Su organización no incurre en cargos de Macie por la cuenta en la región correspondiente mientras Macie esté suspendida por la cuenta en esa región.

Suspender Macie para una cuenta de miembro de una organización

Para suspender a Macie de una cuenta de miembro de una organización, puede usar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para suspender Macie de una cuenta de miembro mediante la consola Amazon Macie.

Para suspender Macie de una cuenta de miembro

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS de la esquina superior derecha de la página, seleccione la región en la que desea suspender Macie de la cuenta de miembro.
3. En el panel de navegación, en Configuración, seleccione Cuentas.
4. En la tabla Cuentas, seleccione la casilla de verificación de la cuenta que desea suspender.
5. En el menú Acciones, seleccione Suspender Macie.
6. Confirme que desea suspender Macie de la cuenta.

Tras confirmar la suspensión, el estado de la cuenta cambiará a En pausa (suspendido) en el inventario de la cuenta.

Repita los pasos anteriores en cada región adicional en la que desee suspender a Macie de la cuenta.

API

Para suspender a Macie de una cuenta de miembro mediante programación, utilice la operación UpdateMemberSession de la API de Amazon Macie.

Cuando envíes tu solicitud, usa el parámetro `id` para especificar el ID de cuenta de 12 dígitos de la cuenta por la Cuenta de AWS que deseas suspender Macie. Para el parámetro `status`, especifique `PAUSED` como el nuevo estado de la cuenta de Macie. Especifica también la región a la que se aplica la solicitud. Para suspender la cuenta en otras regiones, envíe su solicitud en cada región adicional.

Para recuperar el identificador de la cuenta que se va a suspender, puede utilizar la operación ListMembers de la API de Amazon Macie. Si lo hace, considere filtrar los resultados incluyendo el parámetro `onlyAssociated` en su solicitud. Si establece el valor de este parámetro en `true`, Macie devolverá una matriz `members` que proporciona detalles únicamente sobre las cuentas que actualmente son cuentas de miembros.

Para suspender Macie de una cuenta de miembro mediante el AWS CLI, ejecute el comando update-member-session. Utilice el parámetro `region` para especificar la región en la que se va a suspender Macie y utilice el parámetro `id` para especificar el identificador de la cuenta por la que Cuenta de AWS se va a suspender Macie. En el parámetro `status`, especifique `PAUSED`. Por ejemplo:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Mientras que *`us-east-1`* es la región en la que se suspende Macie (Este de EE. UU. (Norte de Virginia)), *`123456789012`* es el identificador de la cuenta para la que se va a suspender Macie y `PAUSED` es el nuevo estado de Macie para la cuenta.

Si tu solicitud se aprueba, Macie devuelve una respuesta vacía y el estado de la cuenta especificada cambia al `Paused` de su inventario de cuentas.

Eliminar cuentas de miembro de Amazon Macie de una organización

Si quiere dejar de acceder a la configuración, los datos y los recursos de Macie para una cuenta de miembro, puede eliminar la cuenta como cuenta de miembro de Macie. Puede hacerlo desvinculado la cuenta de tu cuenta de administrador de Macie. Tenga en cuenta que solo usted puede hacer esto con una cuenta de miembro. La cuenta de un miembro AWS Organizations no se puede desasociar de su cuenta de administrador de Macie.

Al eliminar una cuenta de miembro de Macie, Macie permanece habilitada para la cuenta actual Región de AWS. Sin embargo, la cuenta se disocia de su cuenta de administrador de Macie y pasa a ser una cuenta de Macie independiente. Esto significa que perderá el acceso a todos los ajustes, datos y recursos de Macie de la cuenta, incluidos los metadatos y las conclusiones de las políticas de los datos de Amazon S3 de la cuenta. Esto también significa que ya no puedes usar a Macie para descubrir datos confidenciales en los buckets de S3 que son propiedad de la cuenta. Si ya ha creado tareas de detección confidenciales para hacerlo, estas omitirán los buckets que son propiedad de la cuenta.

Tras eliminar una cuenta de miembro de Macie, la cuenta seguirá apareciendo en el inventario de cuentas. Macie no notifica al propietario de la cuenta que la ha eliminado.

Eliminar una cuenta de miembro de su organización

Para eliminar una cuenta de miembro de Macie de su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Sigue estos pasos para eliminar una cuenta de miembro de Macie mediante la consola de Amazon Macie.

Eliminar una cuenta de miembro de Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea eliminar la cuenta de miembro.
3. En el panel de navegación, en Configuración, seleccione Cuentas.
4. En la tabla Cuentas, seleccione la casilla de la cuenta que desea eliminar como cuenta de miembro.

5. En el menú Acciones, seleccione Desvincular la cuenta.
6. Confirme que desea eliminar la cuenta seleccionada como cuenta de miembro.

Tras confirmar su selección, el estado de la cuenta cambiará a Eliminada (desvinculada) en el inventario de su cuenta.

Repita los pasos anteriores en cada región adicional de en la que desee eliminar la cuenta de miembro.

API

Para eliminar una cuenta de miembro de Macie mediante programación, utilice la operación DisassociateMember de la API de Amazon Macie.

Cuando envíe su solicitud, utilice el parámetro `id` para especificar el identificador de 12 dígitos Cuenta de AWS que debe eliminar la cuenta de miembro. Especifica también la región a la que se aplica la solicitud. Para eliminar la cuenta en otras regiones, envíe la solicitud en cada región adicional.

Para recuperar el identificador de la cuenta de miembro que va a eliminar, puede utilizar la operación ListMembers de la API de Amazon Macie. Si lo hace, considere filtrar los resultados incluyendo el parámetro `onlyAssociated` en su solicitud. Si establece el valor de este parámetro en `true`, Macie devolverá una matriz `members` que proporciona detalles únicamente sobre las cuentas que actualmente son cuentas de miembros de Macie.

Para eliminar una cuenta de miembro de Macie mediante el AWS CLI, ejecute el comando disassociate-member. Utilice el parámetro `region` para especificar la región en la que se va a eliminar la cuenta. Utilice el parámetro `id` para especificar el ID de cuenta de la cuenta de miembro que se va a eliminar. Por ejemplo:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Donde *us-east-1* es la región en la que se va a eliminar la cuenta (Este de EE. UU. (Norte de Virginia)) y *123456789012* es el identificador de la cuenta que se va a eliminar.

Si tu solicitud se aprueba, Macie devuelve una respuesta vacía y el estado de la cuenta especificada cambia al `Removed` de su inventario de cuentas.

Designar una cuenta diferente de administrador de Amazon Macie para una organización

Una vez integrada y configurada una AWS Organizations organización en Amazon Macie, la cuenta de AWS Organizations administración puede designar una cuenta diferente como la cuenta de administrador delegado de Macie para la organización.

Como usuario de la cuenta de AWS Organizations administración de una organización, compruebe que cumple los siguientes requisitos de permisos antes de designar otra cuenta de administrador de Macie para su organización:

- Debe tener los mismos permisos que se necesitaron para designar inicialmente una cuenta de administrador de Macie para su organización. También debe poder realizar la siguiente AWS Organizations acción:`organizations:DeregisterDelegatedAdministrator`. Esta acción adicional le permite eliminar la designación actual.
- Si su cuenta es actualmente una cuenta de miembro de Macie, el administrador actual de Macie debe eliminarla como cuenta de miembro de Macie. De lo contrario, no podrá acceder a las operaciones de Macie para designar una cuenta diferente de administrador. Tras designar una nueva cuenta de administrador, el nuevo administrador de Macie podrá volver a añadir su cuenta como cuenta de miembro de Macie.

Si su organización utiliza Macie en varias ocasiones Regiones de AWS, asegúrese también de cambiar la cuenta de administrador delegado de Macie en cada región en la que su organización utilice Macie; la cuenta de administrador de Macie delegada debe ser la misma en todas esas regiones. Si administra varias organizaciones en AWS Organizations, tenga en cuenta también que una cuenta solo puede ser la cuenta de administrador delegado de Macie para una organización a la vez. Para obtener más información sobre los requisitos adicionales, consulte Consideraciones y recomendaciones para usar Amazon Macie con AWS Organizations.

Para designar una cuenta de administrador de Macie para su organización

Para designar una cuenta de administrador de Macie diferente para su organización, puede utilizar la consola de Amazon Macie o una combinación de Amazon Macie y las API. AWS Organizations Solo un usuario de la cuenta de AWS Organizations administración puede cambiar la designación de su organización.

Console

Para cambiar la designación mediante la consola de Amazon Macie, siga los pasos siguientes.

Designe una cuenta de administrador diferente

1. Inicie sesión AWS Management Console con su cuenta AWS Organizations de administración.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee cambiar la designación.
3. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
4. Lleve a cabo una de las siguientes acciones, en función de si Macie está habilitada para su cuenta de administración en la región actual:
   - Si Macie no está activado, seleccione Comenzar en la página de bienvenida.
   - Si Macie está activado, seleccione Configuración en el panel de navegación.
5. En Administrador delegado, seleccione Eliminar. Para cambiar la designación, primero debe eliminar la designación actual.
6. Confirme que desea eliminar la designación actual.
7. En Administrador delegado, introduzca el identificador de cuenta de 12 dígitos que desee designar como la Cuenta de AWS nueva cuenta de administrador de Macie para la organización.
8. Elija Delegar.

Repita los pasos anteriores en cada región adicional en la que haya integrado Macie con AWS Organizations.

API

Para cambiar la designación mediante programación, debe utilizar dos operaciones de la API de Amazon Macie y una operación de la API. AWS Organizations Esto se debe a que debe eliminar la designación actual tanto en Macie como AWS Organizations antes de enviar la nueva designación.

Para eliminar la designación actual:

1. Utilice el DisableOrganizationAdminAccountfuncionamiento de la API de Macie. Para el `adminAccountId` parámetro obligatorio, especifique el ID de cuenta de 12 dígitos de la

Cuenta de AWS cuenta actualmente designada como cuenta de administrador de Macie para la organización.

2. Utilice el DeregisterDelegatedAdministratorfuncionamiento de la AWS Organizations API. Para el parámetro de `AccountId`, especifique el ID de cuenta de 12 dígitos para la cuenta que está actualmente designada como cuenta de administrador de Macie para la organización. Este valor debe coincidir con el ID de cuenta que especificó en la solicitud de Macie anterior. Para el parámetro de `ServicePrincipal`, especifique la entidad principal de servicio de Macie (`macie.amazonaws.com`).

Tras eliminar la designación actual, envíe la nueva designación mediante la EnableOrganizationAdminAccountoperación de la API de Macie. Para el `adminAccountId` parámetro obligatorio, especifique el ID de cuenta de 12 dígitos que desee Cuenta de AWS designar como la nueva cuenta de administrador de Macie para la organización.

Para cambiar la designación mediante el AWS CLI, ejecute el disable-organization-admin-accountcomando de la API de Macie y el deregister-delegated-administratorcomando de la API. AWS Organizations Estos comandos eliminan la designación actual en Macie y AWS Organizations, respectivamente. Para los `account-id` parámetros `admin-account-id` y, especifique el ID de cuenta de 12 dígitos que desea Cuenta de AWS eliminar como cuenta de administrador actual de Macie. Utilice el parámetro `region` para especificar la región que desea eliminar. Por ejemplo:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

Donde:

- *`us-east-1`* es la región a la que se aplica la eliminación, la región Este de EE. UU. (Norte de Virginia).
- *`111122223333`* es el ID de la cuenta que se va a eliminar como cuenta de administrador de Macie.
- `macie.amazonaws.com` es la entidad principal de servicio de Macie.

Tras eliminar la designación actual, ejecute el enable-organization-admin-accountcomando de la API de Macie para enviar la nueva designación. En el `admin-account-id` parámetro,

especifique el identificador de cuenta de 12 dígitos que desee Cuenta de AWS designar como la nueva cuenta de administrador de Macie para la organización. Utilice el parámetro de `region` para especificar la región a la que se aplica la designación. Por ejemplo:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

Cuando *us-east-1* es la región a la que se aplica la designación (Este de EE. UU. (Norte de Virginia)) y *444455556666* es el ID de la cuenta que se va a designar como nueva cuenta de administrador de Macie.

Desactivar la integración de Amazon Macie con AWS Organizations

Una vez que una organización AWS Organizations se ha integrado con Amazon Macie, la cuenta de administración AWS Organizations puede deshabilitar posteriormente la integración. Como usuario de la cuenta de administración AWS Organizations, puede hacerlo desactivando el acceso a servicios de confianza para Macie en AWS Organizations.

Al deshabilitar el acceso a un servicio de confianza para Macie, ocurre lo siguiente:

- Macie pierde su condición de servicio de confianza en AWS Organizations.
- La cuenta de administrador Macie de la organización pierde el acceso a todos los ajustes, datos y recursos Macie de todas las cuentas de miembros Macie en todos los Regiones de AWS.
- Todas las cuentas de los miembros de Macie se convierten en cuentas de Macie independientes. Si Macie tenía habilitada una cuenta de miembro en una o más Regiones, Macie seguirá teniendo habilitada la cuenta en esas Regiones. Sin embargo, la cuenta ya no está asociada a una cuenta de administrador de Macie en ninguna Región.

Para obtener información adicional sobre los resultados de la desactivación del acceso a un servicio de confianza, consulte Utilizar AWS Organizations con otros Servicios de AWS en la Guía del usuario de AWS Organizations.

Para deshabilitar el acceso de confianza para Macie

Para deshabilitar el acceso a servicios de confianza, puede utilizar la consola AWS Organizations o la API AWS Organizations. Solo un usuario de la cuenta de administración AWS Organizations puede deshabilitar el acceso de Macie a los servicios de confianza. Para obtener más información

sobre los permisos que necesita, consulte los Permisos necesarios para deshabilitar el acceso de confianza en la Guía del usuario de AWS Organizations.

Antes de deshabilitar el acceso a los servicios de confianza, si lo desea, póngase en contacto con el administrador delegado de Macie de su organización para suspender o deshabilitar Macie para las cuentas de los miembros y limpiar los recursos de Macie para esas cuentas.

Console

Para deshabilitar el acceso a servicios de confianza mediante la consola AWS Organizations, siga estos pasos.

Para deshabilitar el acceso de confianza

1. Inicie sesión en la AWS Management Console mediante la cuenta de administración de AWS Organizations.
2. Abra la consola de AWS Organizations en https://console.aws.amazon.com/organizations/.
3. En el panel de navegación, elija Servicios.
4. En Servicios integrados, elija Amazon Macie.
5. Elija Deshabilitar el acceso de confianza.
6. Confirme que desea deshabilitar el acceso de confianza.

API

Para deshabilitar el acceso a los servicios de confianza mediante programación, utilice la operación DisableAWSServiceAccess de la API AWS Organizations. Para el parámetro de `ServicePrincipal`, especifique la entidad principal de servicio de Macie (`macie.amazonaws.com`).

Para deshabilitar el acceso a un servicio confiable mediante AWS Command Line Interface(AWS CLI), ejecute el comando disable-aws-service-access de la API. AWS Organizations Para el parámetro de `service-principal`, especifique la entidad principal de servicio de Macie (`macie.amazonaws.com`). Por ejemplo:

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

Administración de cuentas de Amazon Macie por invitación

Puedes administrar de forma centralizada varias cuentas de Amazon Macie de dos maneras: integrando Macie con AWS Organizations o mediante invitaciones de membresía. Si utilizas invitaciones de membresía, un administrador designado de Macie puede administrar Macie para un máximo de 1000 cuentas. El administrador también puede acceder a los datos de inventario de Amazon Simple Storage Service (Amazon S3) y detectar datos confidenciales en los buckets de S3 que sean propiedad de las cuentas. Para obtener más información sobre las tareas que pueden realizar los administradores, consulta Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

En una organización basada en invitaciones, en la que las cuentas de Macie se asocian entre sí enviando y aceptando invitaciones de membresía. Si envía una invitación y es aceptada por otra cuenta, se convierte en el administrador de Macie para la otra cuenta y la otra cuenta se convierte en una cuenta de miembro en su organización. Si recibe y acepta una invitación, su cuenta pasa a ser una cuenta de miembro y la cuenta de administrador de Macie puede acceder a determinados ajustes, datos y recursos de su cuenta.

> **Tip**
>
> Si crea una organización basada en invitaciones en Macie, posteriormente puede hacer la transición usando AWS Organizations en su lugar. También puede utilizar ambos métodos al mismo tiempo para gestionar varias cuentas de Macie. Por ejemplo, si su entorno AWS incluye cuentas de prueba, puede excluirlas de su organización em AWS Organizations y administrarlas por separado mediante invitación.

En los temas de esta sección se explica cómo crear una organización basada en invitaciones y participar en ella, y cómo realizar diversas tareas administrativas para la organización.

Temas

- Consideraciones y recomendaciones para las organizaciones basadas en invitaciones en Amazon Macie
- Administrar su membresía en una organización basada en invitaciones en Amazon Macie
- Revisión de las cuentas de Amazon Macie para una organización basada en invitaciones
- Designación de una cuenta de administrador de Amazon Macie para una organización por invitación

- Administrar su membresía en una organización basada en invitaciones en Amazon Macie

Consideraciones y recomendaciones para las organizaciones basadas en invitaciones en Amazon Macie

Antes de crear o comenzar a administrar una organización basada en invitaciones en Amazon Macie, tenga en cuenta los siguientes requisitos y recomendaciones. Asegúrese también de que entiende la relación entre las cuentas de administrador y de miembro de Macie.

Temas

- Elegir una cuenta de administrador de Macie
- Envío de invitaciones y administración de las cuentas de miembros de Macie
- Responder y administrar invitaciones de membresía
- Transición al uso de AWS Organizations

Elegir una cuenta de administrador de Macie

Al determinar qué cuenta debe ser la cuenta de administrador de Macie para la organización, tenga en cuenta lo siguiente:

- Una organización solo puede tener una cuenta de administrador de Macie.
- Una cuenta no puede ser cuenta de administrador de Macie y cuenta de miembro al mismo tiempo.
- Macie es un servicio regional. Esto significa que la asociación entre una cuenta de administrador de Macie y una cuenta de miembro es regional: la asociación solo existe en la Región de AWS desde la que se envía una invitación y en la que se acepta. Por ejemplo, si el administrador de Macie envía invitaciones a la región Este de EE. UU. (Norte de Virginia) y esas invitaciones son aceptadas, el administrador de Macie solo podrá administrar las cuentas de los miembros en esa región.

  Para administrar de forma centralizada las cuentas de Macie en varias Regiones de AWS, el administrador de Macie puede iniciar sesión en cada región en la que la organización utilice o vaya a utilizar Macie y, enviar invitaciones a las cuentas apropiadas en cada una de esas regiones. Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie en Referencia general de AWS.
- Una cuenta de miembro solo se puede asociar a una cuenta de administrador de Macie a la vez. Si su organización utiliza Macie en varias regiones, significa que la cuenta de administrador de

Macie debe ser la misma en todas esas regiones. Sin embargo, las cuentas de administrador y de miembro deben enviar y aceptar las invitaciones por separado en cada región.

- Si la Cuenta de AWS del administrador Macie se suspende, aísla o cierra, todas las cuentas de miembro asociadas se eliminan automáticamente como cuentas de miembro, pero Macie no se desactiva para esas cuentas.

Envío de invitaciones y administración de las cuentas de miembros de Macie

Como administrador de Macie de una organización basada en invitaciones, tenga en cuenta lo siguiente al enviar invitaciones y administrar las cuentas de la organización:

- Si envía una invitación, es posible que se transfieran datos relacionados entre Regiones de AWS. Esto se debe a que Macie verifica la dirección de correo electrónico de la cuenta receptora mediante un servicio de verificación de correo electrónico que opera únicamente en la región Este de EE. UU. (Norte de Virginia).
- Puede enviar una invitación a cualquier Cuenta de AWS activa, incluidas las cuentas que no tengan habilitado Macie. Para aceptar o rechazar una invitación, debe activar Macie en la región desde la que se envió la invitación.
- Una cuenta de administrador de Macie puede estar asociada a un máximo de 10 000 cuentas en cada Región de AWS. Esto incluye las cuentas que aún no hayan respondido a las invitaciones. Si su cuenta llega al límite, no podrá añadir ni invitar a más cuentas hasta que elimine el número necesario de cuentas asociadas, reciba el número necesario de invitaciones rechazadas o una combinación de ambas cosas.

  Para determinar cuántas cuentas están asociadas actualmente a su cuenta, puede utilizar la página Cuentas de la consola de Amazon Macie o la operación ListMembers de la API de Amazon Macie. Para obtener más información, consulte Revisión de las cuentas de Amazon Macie para una organización basada en invitaciones.
- Las cuentas se pueden asociar solo a una cuenta de administrador de Macie a la vez. Esto significa que una cuenta no puede aceptar una invitación si ya está asociada a otra cuenta de administrador de Macie. La cuenta primero debe desasociarse de su cuenta de administrador de Macie actual.
- En una organización basada en invitaciones, la cuenta de un miembro puede desvincularse de su cuenta de administrador de Macie en cualquier momento. Si esto ocurre, Macie seguirá habilitada para la cuenta y la cuenta pasará a ser una cuenta de Macie independiente. Macie no le notifica si la cuenta de un miembro se desvincula de su cuenta de administrador. Sin embargo,

la cuenta seguirá apareciendo en su inventario de cuentas y tendrá el estado de Miembro que ha renunciado.

- Si eliminas la cuenta de un miembro de tu organización, Macie seguirá habilitando la cuenta y la cuenta pasará a ser una cuenta de Macie independiente.

Responder y administrar invitaciones de membresía

Como destinatario de una invitación o miembro de una organización basada en invitaciones, tenga en cuenta lo siguiente al responder y administrar las invitaciones que reciba:

- Antes de aceptar una invitación, asegúrese de entender la relación entre las cuentas de administrador y de miembro de Macie.
- Las cuentas solo se pueden asociar a una cuenta de administrador de Macie a la vez. Si acepta una invitación y, posteriormente, quiere unirse a otra organización (mediante invitación o a través de AWS Organizations), primero debe desvincular su cuenta de su actual cuenta de administrador de Macie. A continuación, podrá unirse a la otra organización.
- Para aceptar o rechazar una invitación, debes habilitar a Macie en Región de AWS desde donde se envió la invitación. La cuenta que envió la invitación no puede habilitar Macie en esa región para usted. Rechazar una invitación es opcional. Si rechaza una invitación puede, si lo desea, inhabilitar a Macie en la región correspondiente después de rechazarla.
- Si es administrador de Macie, no puede aceptar una invitación para convertirse en una cuenta de miembro: una cuenta no puede ser de administrador de Macie y de miembro al mismo tiempo. Para convertirse en una cuenta de miembro, primero debe desvincular su cuenta de todas sus cuentas de miembro eliminando todas las cuentas de miembro de su organización actual.
- Macie es un servicio regional. Si acepta una invitación, la asociación entre su cuenta y la cuenta de administrador de Macie es regional; la asociación solo existe en el lugar desde el que se envió y en el Región de AWS que se aceptó la invitación.
- Si utiliza Macie en varias regiones, la cuenta de administrador de Macie de su cuenta debe ser la misma en todas esas regiones. Sin embargo, el administrador de Macie debe enviarle las invitaciones por separado en cada región y usted debe aceptarlas por separado en cada región.
- Puede desvincular su cuenta de una cuenta de administrador de Macie en cualquier momento. Si esto ocurre, Macie seguirá habilitada para la cuenta y la cuenta pasará a ser una cuenta de Macie independiente.
- Si esto ocurre, Macie seguirá habilitada para la cuenta y la cuenta pasará a ser una cuenta de Macie independiente.

Transición al uso de AWS Organizations

Después de crear una organización basada en invitaciones en Macie, puede pasar a utilizar AWS Organizations en su lugar. Para simplificar la transición, le recomendamos que designe la cuenta de administrador existente, basada en invitaciones, como cuenta de administrador de Macie de la organización en la que se encuentra. AWS Organizations

Si lo hace, todas las cuentas de miembros actualmente asociadas seguirán siendo miembros. Si la cuenta de un miembro forma parte de la organizaciónAWS Organizations, la asociación de la cuenta cambia automáticamente de Por invitación a Via AWS Organizations en Macie. Si la cuenta de un miembro no forma parte de la organizaciónAWS Organizations, la asociación de la cuenta seguirá siendo Por invitación. En ambos casos, las cuentas seguirán asociadas a la cuenta de administrador de Macie como cuentas de miembros.

Recomendamos este enfoque porque una cuenta de miembro solo se puede asociar a una cuenta de administrador de Macie a la vez. Si designa una cuenta diferente como cuenta de administrador de Macie para una organización en la que AWS Organizations se encuentre, el administrador designado no podrá gestionar las cuentas que ya estén asociadas a otra cuenta de administrador de Macie por invitación. Cada cuenta de miembro debe desvincularse primero de su cuenta de administrador actual, basada en una invitación. Solo entonces el administrador de Macie de la AWS Organizations organización podrá añadir la cuenta de miembro a su organización y empezar a gestionar Macie para la cuenta.

Tras integrar Macie con AWS Organizations y configurar su organización en Macie, si lo desea, puede designar una cuenta de administrador de Macie diferente para la organización. También puede seguir utilizando las invitaciones para asociar y administrar cuentas de miembros que no formen parte de su organización en AWS Organizations.

Administrar su membresía en una organización basada en invitaciones en Amazon Macie

Para crear una organización basada en invitaciones en Amazon Macie, comience por determinar qué cuenta desea que sea la cuenta de administrador de Macie para la organización. Luego, use esa cuenta para agregar cuentas de miembros: envíe invitaciones de membresía a otras Cuentas de AWS, invitando a las cuentas a unirse a la organización como cuentas de miembros de Macie en la actual Región de AWS. Para crear la organización en varias regiones, envíe invitaciones de membresía desde cada región en la que las otras cuentas usen Macie actualmente o vayan a utilizarlo.

Cuando una cuenta acepta una invitación, pasa a ser una cuenta de miembro de Macie asociada a la cuenta de administrador de Macie en la región correspondiente. La cuenta de administrador de Macie puede acceder a determinados ajustes, datos y recursos de Macie para la cuenta de miembro en esa región.

Como administrador de Macie para una organización basada en invitaciones, puede revisar los datos de inventario de Amazon Simple Storage Service (Amazon S3) y los resultados de políticas de cuentas de miembros. El administrador también puede realizar la detección automatizada de datos confidenciales y ejecutar trabajos de detección de datos confidenciales para detectar dichos datos en los buckets de S3 propiedad de las cuentas de miembros. Para obtener una lista detallada de las tareas que puede realizar, consulte Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

De forma predeterminada, Macie le brinda visibilidad de los datos y recursos relevantes para su organización en general. También puede desglosar la información para revisar los datos y recursos de las cuentas individuales de su organización. Por ejemplo, si utiliza el panel Resumen para evaluar la postura de seguridad de Amazon S3 de su organización, puede filtrar los datos por cuenta. Del mismo modo, si monitoriza los costos de uso estimados, puede acceder a los desgloses de los costos estimados de las cuentas de los miembros individuales.

Además de las tareas que son comunes a las cuentas de administrador y de miembros, puede realizar de forma centralizada diversas tareas administrativas para su organización. Antes de realizar estas tareas, es recomendable revisar las consideraciones y recomendaciones para gestionar las organizaciones basadas en invitaciones en Macie.

Tareas

- Añadir cuentas de miembros de Amazon Macie de una organización basada en invitaciones
- Para suspender Amazon Macie para una cuenta de miembro en una organización basada en invitaciones
- Eliminar cuentas de miembros de Amazon Macie de una organización basada en invitaciones
- Eliminar asociaciones con otras cuentas

Añadir cuentas de miembros de Amazon Macie de una organización basada en invitaciones

Como administrador de Macie de una organización basada en invitaciones, puede añadir cuentas de miembros a su organización siguiendo dos pasos principales:

1. Añadir las cuentas a su inventario de cuentas en Macie. Esto asocia las cuentas a su cuenta.
2. Envíar las invitaciones de membresía a las cuentas

Una vez que la cuenta acepta una invitación, pasa a ser una cuenta miembro de la organización.

Paso 1: Agregue las cuentas

Para añadir una o más cuentas al inventario de cuentas, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Con la consola Amazon Macie, puede añadir una cuenta a la vez o añadir varias cuentas al mismo tiempo cargando un archivo de valores separados por comas (CSV). Siga estos pasos para agregar una o más cuentas con la consola.

Para añadir una cuenta

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea añadir una cuenta.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. Elija Add accounts.
5. En la sección Introducir los detalles de la cuenta, seleccione la pestaña Añadir cuenta. A continuación, proceda del modo siguiente:
   - En el campo ID de cuenta, introduzca el ID de cuenta de 12 dígitos de la Cuenta de AWS que desea añadir.
   - En el caso de la dirección de correo electrónico, introduzca la dirección de correo electrónico de la Cuenta de AWS que desea añadir.
6. Elija Agregar características y, luego, seleccione Siguiente.

Macie añade las cuentas a su inventario de cuentas. El tipo de cuenta es Por invitación y su estado es Creada. Repita los pasos previos en cada región adicional en la que desee agregar la cuenta.

Para añadir varias cuentas

1. Con un editor de texto, cree un archivo CSV de la siguiente manera:

   a. Añada el siguiente encabezado como primera línea del archivo: `Account ID,Email`

   b. Para cada cuenta, cree una línea nueva que contenga el ID de cuenta de 12 dígitos que desea Cuenta de AWS añadir y la dirección de correo electrónico de la cuenta. Separe las entradas con una coma, por ejemplo: `111111111111,janedoe@example.com`

      La dirección de correo electrónico debe coincidir con la dirección de correo electrónico asociada a Cuenta de AWS.

   c. Compruebe que el contenido del archivo tenga el formato que se muestra en el siguiente ejemplo, que contiene el encabezado y la información necesarios para tres cuentas:

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

   d. Guarde el archivo en su ordenador.

2. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
3. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea añadir la cuenta.
4. En el panel de navegación, en Settings, seleccione Accounts.
5. Elija Add accounts.
6. En la sección Introducir los detalles de la cuenta, seleccione la pestaña Cargar lista (CSV).
7. Elija Examinar y, a continuación, seleccione el archivo CSV que ha creado en el paso 1.
8. Elija Agregar características y, luego, seleccione Siguiente.

Macie añade las cuentas a su inventario de cuentas. Su tipo es Por invitación y su estado es Creado. Repita los pasos 3 a 8 en cada región adicional en la que desee agregar las cuentas.

API

Para habilitar y añadir mediante programación una o más cuentas, utilice la operación CreateMember de la API de Amazon Macie. Cuando envíe su solicitud, utilice los parámetros admitidos para especificar el ID de cuenta de 12 dígitos y la dirección de correo electrónico de cada Cuenta de AWS para añadirlas. Especifica también la región a la que se aplica la solicitud.

Para añadir cuentas existentes en regiones adicionales, envíe la solicitud para cada región adicional.

Para añadir cuentas mediante AWS Command Line Interface(AWS CLI), ejecute el comando create-member. Utilice el parámetro `region` para especificar la región en la que desea añadir las cuentas. Utilice los parámetros `account` para especificar el ID de cuenta y la dirección de correo electrónico de cada Cuenta de AWS para añadirlos. Por ejemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

Donde *us-east-1* es la región en la que se va a añadir la cuenta (Este de EE. UU. (Norte de Virginia)) y los parámetros `account` especifican el identificador de la cuenta (*1111*) y la dirección de correo electrónico (*janedoe@example.com*) que se va a añadir.

Si su solicitud es correcta, Macie añadirá cada cuenta a su inventario de cuentas cuyo estado sea de `Created` y recibirá un resultado similar al siguiente:

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

Dónde `arn` es el nombre de recurso de Amazon (ARN) del recurso que se creó para la asociación entre su cuenta y la cuenta que ha agregado. En este ejemplo, `123456789012` es el ID de cuenta de la cuenta que creó la asociación y `111111111111` es el ID de la cuenta que se agregó.

Paso 2: Envíe las invitaciones de membresía a las cuentas

Tras añadir una cuenta al inventario de cuentas, puede invitar a esa cuenta a unirse a su organización como cuenta de miembro de Macie. Para ello, envíe una invitación de membresía a la cuenta. Cuando envía una invitación, en la consola de Amazon Macie aparecen una insignia de Cuentas y una notificación para la cuenta del destinatario, si Macie está habilitada para la cuenta. Macie también crea un evento de AWS Health para la cuenta.

En función de si utiliza la consola o la API de Amazon Macie para enviar la invitación, Macie también la envía a la dirección de correo electrónico que especificó para la cuenta del destinatario al agregar la cuenta. El mensaje de correo electrónico indica que quiere convertirse en el administrador de Macie para su cuenta e incluye su ID de cuenta de su Cuenta de AWS y el Cuenta de AWS del

destinatario. El mensaje también explica cómo acceder a la invitación. Si lo desea, puede añadir texto personalizado al mensaje.

Para responder a una invitación de membresía, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para responder a una invitación de membresía mediante la consola Amazon Macie.

Para enviar una invitación de membresía

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región a la que desea envíar la invitación.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. En la tabla Cuentas, active la casilla de verificación de cada cuenta a la que desee enviar la invitación.

   > **Tip**
   >
   > Para identificar más fácilmente las cuentas que ha añadido y a las que aún no ha enviado invitaciones, puede filtrar la tabla. Para ello, coloque el cursor en el cuadro de filtro situado encima de la tabla y, a continuación, seleccione Estado. A continuación, elija Estado = Creado.

5. En el menú Acciones, elija Invitar.
6. (Opcional) En el cuadro Mensaje, ingrese el texto personalizado que desee incluir en el mensaje de correo electrónico que contiene la invitación. El texto puede contener hasta 80 caracteres alfanuméricos.
7. Elija Invite.

Para enviar la invitación en otras Regiones de AWS, repita los pasos anteriores en cada región adicional.

Tras enviar la invitación, el estado de la cuenta del destinatario cambia a Verificación del correo electrónico en curso en su inventario de cuentas. Si Macie puede verificar la dirección de correo

electrónico de una cuenta, el estado de la cuenta cambiará posteriormente a Invitada. Si Macie no puede verificar la dirección, el estado de la cuenta cambia a Fallo en la verificación del correo electrónico. Si esto ocurre, contacte con el propietario de la cuenta para obtener la dirección de correo electrónico correcta. A continuación, elimine la asociación entre sus cuentas, vuelva a añadir la cuenta y vuelva a enviar la invitación.

Cuando un destinatario acepta una invitación, el estado de la cuenta del destinatario cambia a Habilitada en su inventario de cuentas. Si un destinatario rechaza una invitación, la cuenta del destinatario se desvincula de su cuenta y se elimina de su inventario de cuentas.

API

Para enviar una invitación mediante programación, utilice la operación CreateInvitations de la API de Amazon Macie. Cuando envíe su solicitud, utilice los parámetros admitidos para especificar el ID de cuenta de 12 dígitos y la dirección de correo electrónico de cada Cuenta de AWS para envíar la invitación. El ID de cuenta debe coincidir con el ID de cuenta de una cuenta de su inventario de cuentas. En caso contrario, se produce un error. Especifique también la región desde la que deseas enviar la invitación. Para enviar la invitación desde otras regiones, envíe la solicitud en cada región adicional.

En su solicitud, también puede especificar si desea enviar la invitación como un mensaje de correo electrónico y si desea incluir un texto personalizado en ese mensaje. Si decide enviar un mensaje de correo electrónico, Macie enviará la invitación a la dirección de correo electrónico que especificó para una cuenta cuando la agregó al inventario de su cuenta. Para enviar la invitación como un mensaje de correo electrónico, omita el parámetro `disableEmailNotification` o establezca el valor del parámetro en `false`. (El valor predeterminado es `false`). Para añadir texto personalizado al mensaje, utilice el parámetro `message` para especificar el texto que desee añadir. El texto puede contener hasta 80 caracteres alfanuméricos.

Para enviar invitaciones mediante el AWS CLI, ejecute el comando create-invitation. Utilice el parámetro `region` para especificar la región desde la que se va a enviar la invitación. Utilice el parámetro `account-ids` para especificar el ID de la cuenta para cada Cuenta de AWS para envíar la invitación. Por ejemplo:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

Donde *us-east-1* es la región desde la que se va a enviar la invitación (la región Este de EE. UU. [Norte de Virginia]) y el parámetro `account-ids` especifica los ID de las tres cuentas a

las que se va a enviar la invitación. Para enviar una invitación también como mensaje de correo electrónico, incluya también el parámetro `no-disable-email-notification` y, si lo desea, incluya el parámetro `message` para especificar el texto personalizado que desee añadir al mensaje.

Tras enviar la invitación, el estado de cada cuenta del destinatario cambia a`EmailVerificationInProgress`. Si Macie puede verificar la dirección de correo electrónico de una cuenta, el estado de la cuenta cambiará posteriormente a `Invited`. Si Macie no puede verificar la dirección, el estado de la cuenta cambia a. `EmailVerificationFailed` Si esto ocurre, contacte con el propietario de la cuenta para obtener la dirección correcta. A continuación, elimine la asociación entre sus cuentas, vuelva a añadir la cuenta y vuelva a enviar la invitación.

Cuando un destinatario acepta una invitación, el estado de la cuenta del destinatario cambia a `Enabled` en su inventario de cuentas. Si un destinatario rechaza una invitación, la cuenta del destinatario se desvincula de su cuenta y se elimina de su inventario de cuentas.

Para suspender Amazon Macie para una cuenta de miembro en una organización basada en invitaciones

Como administrador de Macie de una organización, puede suspender a Macie en una Región de AWS específica para cuentas de miembros individuales de su organización. Sin embargo, tenga en cuenta que no puede volver a habilitar Macie para una cuenta de miembro después de suspenderla. Posteriormente, solo el usuario de la cuenta puede volver a habilitar Macie para esa cuenta.

Cuando se suspende Macie de una cuenta de miembro:

- Macie pierde el acceso y deja de proporcionar metadatos sobre los datos de Amazon S3 de la cuenta en la región.
- Macie deja de realizar todas las actividades para la cuenta en la región. Esto incluye la supervisión de los buckets de S3 para garantizar la seguridad y el control de acceso, la detección automática de datos confidenciales y la ejecución de las tareas de detección de datos confidenciales que se estén realizando actualmente.
- Macie cancela todos los trabajos de detección de datos confidenciales creados por la cuenta en la región. Un trabajo no se puede reanudar ni reiniciar después de cancelarse.

  Si ha creado trabajos para analizar datos que son propiedad de la cuenta de miembro, Macie no los cancela. En su lugar, los trabajos omiten los recursos que son propiedad de la cuenta.

Mientras una cuenta esté suspendida, Macie conserva el identificador de sesión de Macie, la configuración y los recursos de la cuenta en la región correspondiente. Por ejemplo, los resultados de la cuenta permanecen intactos y no se ven afectados durante un máximo de 90 días. No se cobrará a la cuenta por usar Macie en la región correspondiente mientras Macie esté suspendido en esa región.

Para suspender Macie de una cuenta de miembro en una organización basada en invitaciones

Para suspender Macie para una cuenta de miembro en una organización basada en invitaciones, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para suspender Macie de una cuenta de miembro mediante la consola Amazon Macie.

Para suspender Macie de una cuenta de miembro

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea suspender Macie.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. En la tabla Cuentas, seleccione la casilla de verificación de la cuenta que desea suspender.
5. En el menú Acciones, seleccione Suspender Macie.
6. Confirme que desea suspender Macie para la cuenta seleccionada.

Tras confirmar la suspensión, el estado de la cuenta cambiará a En pausa (suspendido) en el inventario de la cuenta.

Repita los pasos anteriores en cada región adicional en la que desee suspender a Macie de la cuenta.

API

Para suspender a Macie de una cuenta de miembro mediante programación, utilice la operación UpdateMemberSession de la API de Amazon Macie. Cuando envíe su solicitud, utilice el parámetro `id` para especificar el ID de cuenta de 12 dígitos del Cuenta de AWS con el que desea suspender Macie. Para el parámetro `status`, especifique `PAUSED` como el nuevo estado de la

cuenta de Macie. Especifica también la región a la que se aplica la solicitud. Para suspender Macie en otras regiones, repita los pasos anteriores en cada región adicional.

Para recuperar el ID de la cuenta que se va a eliminar, puede utilizar la operación ListMembers de la API de Amazon Macie. Si lo hace, considere filtrar los resultados incluyendo el parámetro `onlyAssociated` en su solicitud. Si establece el valor de este parámetro en `true`, Macie devolverá una matriz `members` que proporciona detalles únicamente sobre las cuentas que actualmente sean cuentas miembros de su cuenta de administrador.

Para suspender Macie de una cuenta de miembro mediante AWS CLI, ejecute el comando update-member-session. Utilice el parámetro `region` para especificar la región en la que se va a suspender Macie y use el parámetro `id` para especificar el ID de cuenta de la cuenta en la que se va a suspender Macie. En el parámetro `status`, especifique `PAUSED`. Por ejemplo:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Mientras que *`us-east-1`* es la región en la que se suspende Macie (Este de EE. UU. (Norte de Virginia)), *`123456789012`* es el identificador de la cuenta para la que se va a suspender Macie y `PAUSED` es el nuevo estado de Macie para la cuenta.

Si tu solicitud se aprueba, Macie devuelve una respuesta vacía y el estado de la cuenta especificada cambia al `Paused` de su inventario de cuentas.

Eliminar cuentas de miembros de Amazon Macie de una organización basada en invitaciones

Como administrador de Macie, puede eliminar una cuenta de miembro de su organización. Puede hacerlo desvinculado la cuenta de tu cuenta de administrador de Macie.

Si elimina una cuenta de miembro, Macie seguirá teniendo habilitada la cuenta y la cuenta seguirá apareciendo en su inventario de cuentas. Sin embargo, la cuenta se convierte en una cuenta de Macie independiente. Macie no notifica al propietario de la cuenta cuando la elimina. Por lo tanto, considere ponerse en contacto con el propietario de la cuenta para asegurarse de que comience a administrar la configuración y los recursos de su cuenta.

Cuando elimina una cuenta de miembro, pierde el acceso a todos los ajustes, recursos y datos de Macie para esa cuenta. Esto incluye los resultados de políticas y los metadatos de los buckets de S3

que sean propiedad de la cuenta. Además, ya no puede usar Macie para detectar datos sensibles en los depósitos de S3 que sean propiedad de la cuenta. Si ya ha creado tareas de detección de datos sensibles para ello, estas tareas omiten los buckets que son propiedad de la cuenta.

Después de eliminar una cuenta de miembro, puede volver a añadirla a su organización enviando una nueva invitación a la cuenta. También puede eliminarla por completo del inventario de su cuenta eliminando la asociación entre sus cuentas.

Para eliminar una cuenta de miembro de una organización basada en invitaciones

Para eliminar una cuenta de miembro de su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para responder a una invitación de membresía mediante la consola Amazon Macie.

Eliminar cuenta de miembro

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea eliminar la cuenta de miembro.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. En la tabla Cuentas, active la casilla de verificación de la cuenta que desea eliminar.
5. En el menú Acciones, seleccione Desvincular la cuenta.
6. Confirme que desea eliminar la cuenta seleccionada como cuenta de miembro.

Tras confirmar su selección, el estado de la cuenta cambiará a Eliminada (desvinculada) en el inventario de su cuenta.

Repita los pasos anteriores en cada región adicional de en la que desee eliminar la cuenta de miembro.

API

Para eliminar una cuenta de miembro mediante programación, utilice la operación DisassociateMember de la API Amazon Macie. Cuando envíe su solicitud, utilice el parámetro `id` para especificar el identificador Cuenta de AWS de 12 dígitos que debe eliminar la cuenta de

miembro. Especifica también la región a la que se aplica la solicitud. Para eliminar la cuenta en otras regiones, envíe la solicitud en cada región adicional.

Para recuperar el ID de la cuenta que se va a eliminar, puede utilizar la operación ListMembers de la API de Amazon Macie. Si lo hace, considere filtrar los resultados incluyendo el parámetro `onlyAssociated` en su solicitud. Si establece el valor de este parámetro en `true`, Macie devolverá una matriz `members` que proporciona detalles únicamente sobre las cuentas que actualmente sean cuentas miembros de su cuenta.

Para eliminar una cuenta de miembro mediante el AWS CLI, ejecute el comando disassociate-member. Utilice el parámetro `region` para especificar la región en la que se va a eliminar la cuenta. Utilice el parámetro `id` para especificar el identificador de la cuenta que se va a eliminar. Por ejemplo:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Donde *us-east-1* es la región en la que se va a eliminar la cuenta (Este de EE. UU. (Norte de Virginia)) y *123456789012* es el identificador de la cuenta que se va a eliminar.

Si tu solicitud se aprueba, Macie devuelve una respuesta vacía y el estado de la cuenta especificada cambia al `Removed` de su inventario de cuentas.

Eliminar asociaciones con otras cuentas

Después de añadir una cuenta al inventario de cuentas, puede eliminar la asociación entre su cuenta y la otra cuenta. Puede hacerlo para cualquier cuenta de su inventario, excepto:

- Una cuenta de que forme parte de la organización en AWS Organizations. Este tipo de asociación se controla mediante AWS Organizations y no Macie.
- Una cuenta de miembro que aceptó una invitación de membresía de Macie para unirse a su organización. Si este es el caso, debe eliminar la cuenta de miembro antes de poder eliminar la asociación.

Cuando elimina una asociación, Macie elimina la cuenta del inventario de su cuenta. Si posteriormente desea restablecer la asociación, tendrá que volver a añadir la cuenta como si se tratara de una cuenta completamente nueva.

Eliminación de una asociación con otra cuenta

Para eliminar una asociación entre su cuenta y otra cuenta, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Para usar la consola Amazon Macie para eliminar una asociación con otra cuenta, siga estos pasos.

Eliminación de una asociación

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el uso del selector Región de AWS de la esquina superior derecha de la página, seleccione la región en la que desea eliminar la asociación.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. En la tabla Cuentas, active la casilla de verificación de la cuenta cuya asociación desee eliminar.
5. En el menú Acciones, elija Eliminar la cuenta.
6. Confirme que desea eliminar la asociación seleccionada.

Repita los pasos anteriores en cada región adicional en la que desee eliminar la asociación.

API

Para eliminar una regla de filtrado mediante programación, utilice la operación DeleteFindingsFilter de la API de Amazon Macie. Cuando envíe su solicitud, utilice el parámetro `id` para especificar el ID de cuenta de 12 dígitos del Cuenta de AWS con el que desea eliminar la asociación. Especifica también la región a la que se aplica la solicitud. Para eliminar la asociación en regiones adicionales, envíe su solicitud en cada región adicional.

Para recuperar el ID de la cuenta, puede utilizar la operación ListMembers de la API de Amazon Macie. Si lo hace, incluya el parámetro `onlyAssociated` en su solicitud y establezca el valor del parámetro en `false`. Si la operación se realiza correctamente, Macie devuelve una matriz `members` que proporciona detalles sobre todas las cuentas asociadas a su cuenta, incluidas las cuentas que actualmente no son cuentas de miembros.

Para eliminar una asociación con otra cuenta mediante el AWS CLI, ejecute el comando delete-member. Utilice el parámetro `region` para especificar la región en la que se va a eliminar la asociación y el parámetro `id` para especificar el ID de cuenta de la cuenta. Por ejemplo:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

Donde *us-east-1* es la región en la que se va a eliminar la asociación con la otra cuenta (la región Este de EE. UU. [Norte de Virginia]) y *123456789012* es el identificador de la cuenta.

Si su solicitud es correcta, Macie devolverá una respuesta vacía y se eliminará la asociación entre su cuenta y la otra cuenta. La cuenta previamente asociada se elimina del inventario de su cuenta.

Revisión de las cuentas de Amazon Macie para una organización basada en invitaciones

Para ayudarle a administrar las cuentas de su organización, Amazon Macie proporciona un inventario de las cuentas que están asociadas a su cuenta de Macie en cada Región de AWS donde utilice Macie. Al utilizar este inventario, puede comprobar el estado de las cuentas individuales y revisar las estadísticas y los detalles de las cuentas de su organización. También puede administrar el estado de la relación entre su cuenta y las cuentas individuales.

Para revisar las cuentas de una organización basada en invitaciones

Para revisar las cuentas de su organización, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para revisar las cuentas de su organización mediante la consola de Amazon Macie.

Para revisar las cuentas de su organización

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea revisar las cuentas de su organización.
3. En el panel de navegación, en Settings, seleccione Accounts.

Se abre la página Cuentas y muestra estadísticas añadidas y una tabla de las cuentas que están asociadas a su cuenta de Macie en el Región de AWS actual.

En la parte superior de la página de Cuentas, encontrará las siguientes estadísticas agregadas.

Vía AWS Organizations

Si usted es el administrador de Macie para una organización en AWS Organizations, Activo indica el número total de cuentas asociadas a su cuenta a través de AWS Organizations y que actualmente son cuentas de miembro de Macie en su organización. Macie está habilitado para estas cuentas y tú eres el administrador de las cuentas en Macie.

Todos indica el número total de cuentas que están asociadas a su cuenta mediante AWS Organizations, incluidas las cuentas que actualmente no son cuentas de miembros de Macie.

Por invitación

Activo indica el número total de cuentas que actualmente son cuentas de miembros de Macie en su organización basada en invitaciones. Macie está habilitado para las cuentas y usted es el administrador de las cuentas de Macie porque ellos han aceptado una invitación suya a ser miembro de Macie.

Todos indica el número total de cuentas asociadas a su cuenta por invitación de Macie, incluidas las cuentas que no han respondido a una invitación suya.

Activo/Todos

Activo indica el número total de cuentas que actualmente son miembros de Macie para su cuenta, ya sea a través de AWS Organizations o por invitación. Macie está habilitado para estas cuentas y tú eres el administrador de las cuentas en Macie.

Todos indica el número total de cuentas que están asociadas a su cuenta, ya sea por AWS Organizations o por invitación de Macie. Esto incluye las cuentas que no han aceptado una invitación tuya a ser miembros de Macie. Esto también incluye las cuentas asociadas a su cuenta a través de AWS Organizations y que no son actualmente cuentas de miembro de Macie.

En la tabla, encontrará detalles sobre cada cuenta de la Región actual. La tabla incluye todas las cuentas asociadas a su cuenta de Macie, ya sea por invitación de Macie o a través de AWS Organizations.

ID de cuenta

El ID de cuenta y la dirección de correo electrónico para Cuenta de AWS.

Nombre

El nombre de la cuenta para Cuenta de AWS. Este valor suele ser N/A para las cuentas que están asociadas a su cuenta por invitación de Macie.

Tipo

Cómo se asocia la cuenta con su cuenta, por invitación o a través de AWS Organizations.

Estado

El estado de la relación entre su cuenta y la cuenta. Para una cuenta de una organización basada en invitaciones (el Tipo es Por invitación), los valores posibles son:

- Cuenta suspendida: la Cuenta de AWS está suspendida.
- Creada (invitación): añadió la cuenta pero no envió una invitación de membresía.
- Fallo en la verificación del correo electrónico: intentó enviar una invitación de membresía a la cuenta, pero la dirección de correo electrónico especificada no es válida para la cuenta.
- Verificación del correo electrónico en curso: envió una invitación de membresía a la cuenta y Macie está procesando la solicitud.
- Activada: la cuenta es una cuenta de miembro. Macie está habilitado para esta cuenta y usted es el administrador de la cuenta en Macie.
- Invitado: ha enviado una invitación de membresía a la cuenta y la cuenta no ha respondido a su invitación.
- Miembro que ha renunciado: la cuenta era anteriormente una cuenta de miembro. Sin embargo, la cuenta abandonó su organización al desvincularse de su cuenta.
- En pausa (suspendida): la cuenta es una cuenta de miembro de Macie, pero Macie está actualmente suspendido para esta cuenta.
- Región deshabilitada: la región actual está deshabilitada para el Cuenta de AWS.
- Eliminada (disociada): la cuenta era anteriormente una cuenta de miembro. Sin embargo, la ha eliminado como cuenta de miembro al desasociarla de su cuenta.

Última acción

Cuando usted o la cuenta asociada realizaron por última vez una acción que afectó a la relación entre sus cuentas.

Para ordenar la tabla por un campo específico, haga clic en el encabezado de la columna del campo. Para cambiar el orden de clasificación, vuelva a hacer clic en el encabezado de la

columna. Para filtrar la tabla, coloque el cursor en el cuadro de filtro y, a continuación, añada una condición de filtro para un campo. Para refinar aún más los resultados, añada condiciones de filtro para campos adicionales.

API

Para revisar las cuentas de su organización mediante programación, utilice la operación ListMembers de la API Amazon Macie y asegúrese de especificar la región a la que se aplica su solicitud. Para revisar las cuentas en otras Regiones, envíe su solicitud en cada Región adicional.

Cuando envíe su solicitud, utilice el parámetro `onlyAssociated` para especificar qué cuentas incluir en la respuesta. Por defecto, Macie solo devuelve los detalles de las cuentas que son cuentas de miembros de Macie en la región especificada, ya sea mediante AWS Organizations o una invitación de Macie. Para extraer los detalles de todas las cuentas asociadas, incluidas las cuentas que no son cuentas de miembros, incluya el `onlyAssociated` parámetro en su solicitud y establezca el valor del parámetro en `false`.

Para revisar las cuentas de su organización mediante AWS Command Line Interface(AWS CLI), ejecute el comando list-members. Para el parámetro `only-associated`, especifique si desea incluir todas las cuentas asociadas o solo las cuentas de los miembros. Para incluir solo las cuentas de los miembros, omita este parámetro o establezca el valor del parámetro en `true`. Para incluir todas las cuentas, defina este valor en `false`. Por ejemplo:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Si *us-east-1* es la región a la que se aplica la solicitud, la región Este de EE. UU. (Norte de Virginia).

Si la solicitud se realiza correctamente, Macie devuelve una `members` matriz. La matriz contiene un objeto `member` para cada cuenta que cumple los criterios especificados en la solicitud. En ese objeto, el campo `relationshipStatus` indica el estado actual de la relación entre su cuenta y la otra cuenta de la región especificada. Para una cuenta de una organización basada en invitaciones, los valores posibles son:

- `AccountSuspended`: la Cuenta de AWS está suspendida.
- `Created`: añadió la cuenta pero no envió una invitación de membresía.
- `EmailVerificationFailed`: intentó enviar una invitación de membresía a la cuenta, pero la dirección de correo electrónico especificada no es válida para la cuenta.

- `EmailVerificationInProgress`: ha enviado una invitación de membresía a la cuenta y Macie está procesando la solicitud.
- `Enabled`: la cuenta es una cuenta de miembro. Macie está habilitado para esta cuenta y usted es el administrador de la cuenta en Macie.
- `Invited`: ha enviado una invitación de membresía a la cuenta y la cuenta no ha respondido a su invitación.
- `Paused`: la cuenta es una cuenta de miembro, pero Macie está suspendido (pausado) para la cuenta.
- `RegionDisabled`: la región actual está deshabilitada para el Cuenta de AWS.
- `Removed`: la cuenta era anteriormente una cuenta de miembro. Sin embargo, la ha eliminado como cuenta de miembro al desasociarla de su cuenta.
- `Resigned`: la cuenta era anteriormente una cuenta de miembro. Sin embargo, la cuenta abandonó su organización al desvincularse de su cuenta.

Para obtener información sobre otros campos del objeto `member`, consulte Miembros en la Referencia de API de Amazon Macie.

Designación de una cuenta de administrador de Amazon Macie para una organización por invitación

Después de crear y establecer una organización basada en invitaciones, puede cambiar la cuenta de administrador de Amazon Macie de la organización. Para ello, los administradores y miembros de la organización deben seguir estos pasos:

1. El administrador actual de Macie exporta opcionalmente el inventario actual de las cuentas de los miembros activos de la organización. Esto simplifica la transición al ayudarlo a identificar las cuentas de los miembros que deberían seguir formando parte de la organización.
2. El administrador actual de Macie elimina todas las cuentas de los miembros de la organización actual. Esto disocia las cuentas de la cuenta de administrador actual, pero Macie sigue habilitando las cuentas.
3. El nuevo administrador de Macie añade las cuentas de los miembros anteriores a la nueva organización. Esto asocia las cuentas a la nueva cuenta de administrador.
4. Cada cuenta de miembro acepta la invitación para unirse a la nueva organización. Cuando una cuenta acepta la invitación, se convierte en una cuenta de miembro activo de la nueva

organización. El nuevo administrador de Macie podrá entonces acceder a la configuración, los datos y los recursos de Macie de la cuenta.

Si su organización utiliza Macie en varias Regiones de AWS, lleve a cabo los pasos anteriores en cada una de esas regiones.

Para exportar el inventario actual de las cuentas de los miembros activos, el administrador actual de Macie puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Con la consola, el administrador actual puede exportar estos datos a un archivo de valores separados por comas (CSV). A continuación, el nuevo administrador puede usar la consola para cargar el archivo CSV y añadir todas las cuentas (en bloque) a la nueva organización.

Para exportar los datos de las cuentas de los miembros mediante la consola

1. Inicie sesión en AWS Management Console con la cuenta de administrador actual de Macie.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea exportar los datos.
3. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
4. En el panel de navegación, en Settings, seleccione Accounts.
5. (Opcional) Para filtrar la tabla de Cuentas y mostrar solo las que actualmente son cuentas de miembros de Macie activas en la organización, utilice el cuadro de filtro situado encima de la tabla para añadir las siguientes condiciones de filtrado:
   - Tipo = Invitación
   - Estado = Activado
6. En la tabla Cuentas, active la casilla de verificación de cada cuenta de miembro activa para incluirla en los datos exportados.
7. Seleccione Exportar CSV.
8. Para especificar la ubicación y el nombre de archivo de la salida.

Con la API de Amazon Macie, el administrador actual de Macie puede extraer los datos en formato JSON. El nuevo administrador de Macie puede usar esos datos para generar la lista de ID de cuenta y direcciones de correo electrónico de las cuentas para añadir e invitar a la nueva organización. Para extraer los datos en formato JSON, utilice la operación ListMembers de la API Amazon Macie. Si la operación se realiza correctamente, Macie devuelve una matriz `members` que proporciona detalles

sobre todas las cuentas asociadas a la cuenta del administrador. Si una cuenta es una cuenta de miembro de Macie activa en la organización actual basada en invitaciones, el valor de la propiedad `relationshipStatus` de la cuenta es `Enabled` y la propiedad `invitedAt` especifica una fecha y una hora.

Administrar su membresía en una organización basada en invitaciones en Amazon Macie

Si le invitan a unirse a una organización en Amazon Macie, puede aceptar o rechazar la invitación si lo desea. En Macie, una organización es un conjunto de cuentas que se administran de forma centralizada como un grupo de cuentas relacionadas. Una organización consta de una cuenta de administrador designada de Macie y una o más cuentas de miembros asociadas.

Después de aceptar la invitación, su cuenta se convierte en una cuenta miembro de la organización. Al aceptar, la cuenta que envió la invitación pasa a ser la cuenta de administrador de Macie para su cuenta: usted asocia su cuenta a la otra cuenta y establece una relación de administrador-miembro entre las cuentas. El administrador de Macie podrá entonces acceder a determinadas configuraciones de Macie, los datos y los recursos de la cuenta en la Región de AWS compatible. Para obtener más información, consulte Comprensión de la relación entre la cuenta de administrador y las cuentas miembro de Amazon Macie.

Si rechaza una invitación, el estado y la configuración actuales de su cuenta de Macie no cambiarán.

Temas

- Para responder a una invitación para ser miembro de organizaciones
- Desvincularse de una cuenta de administrador de Amazon Macie

Para responder a una invitación para ser miembro de organizaciones

Cuando recibe una invitación para unirse a una organización, Amazon Macie se lo notifica de varias maneras. De forma predeterminada, Macie le envía la invitación como un mensaje de correo electrónico. Macie también crea un evento de AWS Health para su Cuenta de AWS. Si ya utiliza Macie en la Región de AWS desde la que se envió la invitación, Macie también mostrará una insignia de Cuentas y una notificación en la consola de Macie.

Después de recibir una invitación, puede aceptarla o rechazarla si lo desea. Antes de responder, tenga en cuenta lo siguiente:

- Una cuenta no puede pertenecer a más de una organización a la vez. Si recibe varias invitaciones, solo puede aceptar una. O bien, si ya es miembro de una organización, debe desvincular su cuenta de su cuenta de administrador actual de Macie antes de poder unirse a otra organización.
- Si utiliza Macie en varias regiones, su cuenta debe tener la misma cuenta de administrador de Macie en todas esas regiones. El administrador de Macie tiene que enviarle las invitaciones por separado desde cada región y usted tiene que aceptarlas por separado en cada región.
- Para aceptar o rechazar una invitación, debe activar Macie en la región desde la que se envió la invitación. Rechazar una invitación es opcional. Si permite que Macie rechace una invitación, puede inhabilitar a Macie en la región después de rechazar la invitación. Esto ayuda a garantizar que no incurra en cargos innecesarios por usar Macie en la región.

Para consideraciones adicionales, consulte Responder y administrar invitaciones de membresía.

Para responder a una invitación a ser miembro de una organización

Para responder a una invitación de membresía, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para responder a una invitación de membresía mediante la consola Amazon Macie.

Para responder a una invitación para ser miembro

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que recibió la invitación.
3. Si no ha activado Macie en la región, seleccione Comenzar y, a continuación, seleccione Habilitar Macie. Tiene que habilitar Macie para poder aceptar o rechazar una invitación.
4. En el panel de navegación, en Settings, seleccione Accounts.
5. En Cuenta de administrador, realice una de las siguientes acciones:

   - Para aceptar la invitación, active Aceptar () junto a la invitación. A continuación, seleccione Aceptar la invitación o Actualizar, en función de si ha aceptado previamente otra invitación.

- Para rechazar la invitación, seleccione Rechazar invitación junto a la invitación y, a continuación, confirme que desea rechazarla.

Si ha recibido la invitación y quieres responder a esta en otras regiones, repita los pasos anteriores en cada región adicional.

API

Para responder a una invitación mediante programación, utilice la operación AcceptInvitation o DeclineInvitations de la API Amazon Macie, en función de si desea aceptar o rechazar la invitación. Cuando envíe su solicitud, asegúrese de especificar la región desde la que se envió la invitación. Para revisar las cuentas en otras Regiones, envíe su solicitud para cada Región adicional.

En una solicitud de `AcceptInvitation`, use el parámetro `administratorAccountId` para especificar el ID de cuenta de 12 dígitos de la Cuenta de AWS que envió la invitación. Utilice el parámetro `invitationId` para especificar el ID único que debe aceptar la invitación.

En una solicitud de `DeclineInvitations`, use el parámetro `accountIds` para especificar el ID de cuenta de 12 dígitos de la Cuenta de AWS que envió la invitación para rechazarla.

Para recuperar los ID, puede utilizar la operación ListInvitations de la API de Amazon Macie. Si la operación se realiza correctamente, Macie devuelve una matriz `invitations` que proporciona detalles sobre las invitaciones que ha recibido, incluido el ID de cuenta de la cuenta que envió cada invitación y el ID único de cada invitación. Si el valor de la propiedad `relationshipStatus` de una invitación es `Invited`, todavía no ha respondido a la invitación.

Para responder a una invitación mediante AWS Command Line Interface(AWS CLI), ejecute el comando accept-invitation o decline-invitations, en función de si desea aceptar o rechazar la invitación. Utilice el parámetro `region` para especificar la región desde la que se envió la invitación. Por ejemplo:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Donde *us-east-1* es la región desde la que se envió la invitación (la región Este de EE. UU. [Norte de Virginia]), *123456789012* es el identificador de cuenta de la cuenta que envió la invitación y *d8bdad0e203fd1242e0a4721bexample* es el identificador único para aceptar la invitación.

Si la solicitud de aceptación de una invitación se realiza correctamente, Macie devuelve una respuesta vacía. Si la solicitud para rechazar una invitación se realiza correctamente, Macie devuelve una matriz `unprocessedAccounts` vacía.

Cuando rechace una invitación, esta seguirá siendo un recurso para su cuenta de Macie. Como alternativa, puede eliminar la invitación mediante la operación DeleteInvitations o, en el caso de AWS CLI, el comando delete-invitations.

Desvincularse de una cuenta de administrador de Amazon Macie

Si acepta una invitación para unirse a una organización en Amazon Macie, puede renunciar posteriormente a la organización desvinculando su cuenta de su cuenta de administrador de Macie actual. Tenga en cuenta que no puede hacerlo si su cuenta es una cuenta miembro de una organización AWS Organizations. Para dejar de pertenecer a una organización de AWS Organizations, póngase en contacto con su administrador de Macie para eliminar su cuenta como cuenta de miembro de Macie.

Si desvincula su cuenta de su cuenta de administrador de Macie, el administrador de Macie pierde el acceso a todos los ajustes, datos y recursos de su cuenta de Macie. Esto incluye los metadatos y los resultados de políticas de datos de Amazon S3 que sean de su propiedad. Esto también significa que el administrador ya no puede analizar sus datos de Amazon S3 mediante la detección automática de datos confidenciales o la ejecución de tareas de detección de datos confidenciales.

Al desvincular su cuenta, Macie seguirá habilitado para su cuenta en la región correspondiente. Sin embargo, su cuenta pasa a ser una cuenta Macie independiente en la región. El estado de su cuenta cambia a Miembro que ha renunciado en el inventario de cuentas del administrador.

Para desvincularse de una cuenta de administrador de Macie

Para desvincular su cuenta de su cuenta de administrador de Macie actual, puede utilizar la consola de Amazon Macie o la API de Amazon Macie.

Console

Siga estos pasos para desvincular su cuenta de su cuenta de administrador de Macie mediante la consola de Amazon Macie.

Para desvincularse de su cuenta de administrador

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.

2. Con el selector Región de AWS de la esquina superior derecha de la página, seleccione la región de en la que desea desvincular su cuenta de su cuenta de administrador.
3. En el panel de navegación, en Settings, seleccione Accounts.
4. En Cuenta de administrador, desactive Aceptar () junto a la invitación y, a continuación, seleccione Actualizar.

La cuenta sigue apareciendo en la página de cuentas. Si decide volver a unirse a la organización, puede utilizar esta página para aceptar la invitación original. También puede rechazar y eliminar la invitación que, a su vez elimina la asociación entre su cuenta y la otra cuenta. Para ello, seleccione Rechazar la invitación.

Si desea desvincular su cuenta de la cuenta de administrador de Macie en otras regiones, repita los pasos anteriores en cada región adicional.

API

Para desvincular su cuenta de su cuenta de administrador de Macie mediante programación, utilice la operación DisassociateFromAdministratorAccount de la API de Amazon Macie. Cuando envíe su solicitud, asegúrese de especificar la región a la que se aplica la solicitud. Para desvincular las cuentas en otras Regiones, envíe su solicitud en cada Región adicional.

Para desvincular su cuenta de su cuenta de administrador de Macie mediante el AWS CLI, ejecute el comando disassociate-from-administrator-account. Utilice el parámetro `region` para especificar la región en la que desea desvincularse de la cuenta.

Si la solicitud se realiza correctamente, Macie devuelve una respuesta vacía.

Tras desvincularse de la cuenta, la invitación original seguirá siendo un recurso para su cuenta de Macie, a menos que la elimine. Si decide volver a unirse a la organización, puede utilizar este recurso para volver a aceptar la invitación original. Como alternativa, puede eliminar la invitación mediante la operación DeleteInvitations o, en el caso de AWS CLI, el comando delete-invitations. Si elimina la invitación, también elimina la asociación entre su cuenta y la otra cuenta.

Seguridad en Amazon Macie

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta Servicios de AWS en Nube de AWS. Además, AWS proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener información sobre los programas de conformidad que se aplican a Amazon Macie, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el Servicios de AWS que utilice. 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 Macie. En los siguientes temas, se le mostrará cómo configurar Macie para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayudarán a supervisar y a proteger los recursos de Macie.

Temas

Protección de los datos en Amazon Macie

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Macie. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta la totalidad de 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 Modelo de responsabilidad compartida y GDPR de AWS en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se conceden a cada usuario los permisos necesarios para cumplir con 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 de AWS. reSe recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de 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. Incluye las situaciones en las que se trabaja con Macie u otros Servicios de AWS a través de la consola, la API, la AWS CLI, o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos

encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Amazon Macie almacena de forma segura sus datos en reposo mediante soluciones de cifrado de AWS. Macie cifra los datos, como los resultados, mediante una Clave administrada de AWS de AWS Key Management Service (AWS KMS).

Si desactiva Macie, eliminará permanentemente todos los recursos que almacena o mantiene para usted, como las tareas de detección de datos confidenciales, los identificadores de datos personalizados y los resultados.

Cifrado en tránsito

Macie cifra todos los datos en tránsito entre Servicios de AWS.

Amazon Macie analiza los datos de Amazon S3 y exporta los resultados de la detección de datos confidenciales a un bucket de S3. Una vez que Macie obtiene la información que necesita de los objetos de S3, estos se descartan.

Macie accede a Amazon S3 mediante un punto de conexión de VPC con tecnología de AWS PrivateLink. Por lo tanto, el tráfico entre Macie y Amazon S3 permanece en la red de Amazon y no pasa por la internet pública. Para obtener más información, consulte AWS PrivateLink.

Administración de identidades y accesos para Amazon Macie

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar los recursos de Macie. IAM es un servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- Roles vinculados a servicios para Amazon Macie
- Políticas administradas por AWS para Amazon Macie
- Solución de problemas de identidad y acceso de Amazon Macie

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en Macie.

Usuario de servicio: si utiliza el servicio de para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Macie para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Macie, consulte Solución de problemas de identidad y acceso de Amazon Macie.

Administrador de servicio: si está a cargo de los recursos de Macie en su empresa, probablemente tenga acceso completo a Macie. Su trabajo consiste en determinar a qué características y recursos de Macie 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 , consulte Cómo trabaja Amazon Macie con AWS Identity and Access Management.

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 Macie. Para consultar ejemplos de políticas basadas en la identidad de Macie que se pueden utilizar en IAM, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del 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 accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja 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, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a los servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de

identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de 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 de tu cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, 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 IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). 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.
- Acceso entre servicios: algunos servicios de AWS utilizan características de 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 a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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 obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

- Rol vinculado a servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en su Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de 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

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

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 añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la consola, AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política en función de identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad 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 asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener 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. Las entidades 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 se puede utilizar políticas de IAM administradas por AWS 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 política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. 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 en función de 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 especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada rootlong. Para más información sobre organizaciones y las SCP, consulte Funcionamiento de las SCP en la Guía del Usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política 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 obtener información sobre cómo AWS decide si permite o no una

solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo trabaja Amazon Macie con AWS Identity and Access Management

Antes de utilizar AWS Identity and Access Management (IAM) para administrar el acceso a Amazon Macie, conozca qué características de IAM se pueden utilizar con Macie.

Características de IAM que puede utilizar con Amazon Macie

Características de IAM	Soporte de Macie
Políticas basadas en identidad	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
Listas de control de acceso (ACL)	No
Control de acceso basado en atributos (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 perspectiva general sobre cómo funcionan Macie y otros Servicios de AWS con la mayoría de las características de IAM, consulte Servicios de AWSque funcionan con IAM en la Guía del usuario de IAM.

Políticas de Amazon Macie basadas en identidades

Compatibilidad con las políticas basadas en identidad	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 identidad 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 obtener más información sobre los elementos que puede utilizar en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Macie admite políticas basadas en identidad. Para ver ejemplos, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Políticas basadas en recursos de Amazon Macie

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. Las entidades 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 la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política en función de 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.

Macie no admite políticas basadas en recursos. Es decir, no se puede adjuntar una política directamente a un recurso de Macie.

Acciones de políticas para Amazon Macie

Admite acciones de política	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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.

Las acciones de políticas de Macie utilizan el siguiente prefijo antes de la acción:

```
macie2
```

Por ejemplo, para conceder a alguien permiso para acceder a la información sobre todos los identificadores de datos administrados que proporciona Macie, que es una acción que corresponde al funcionamiento de `ListManagedDataIdentifiers` de la API de Amazon Macie, incluye la acción de `macie2:ListManagedDataIdentifiers` en su política:

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo:

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

También puede utilizar caracteres comodín (*) para especificar varias acciones. Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

```
"Action": "macie2:List*"
```

Sin embargo, recomendamos que las políticas se creen según el principio de privilegios mínimos. En otras palabras, debe crear políticas que incluyan solo los permisos necesarios para realizar una tarea específica.

Para ver una lista de las acciones de Macie, consulte Acciones definidas por Amazon Macie en la Referencia de autorizaciones de servicio. Para ver ejemplos de políticas que especifican acciones de Macie, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Recursos de políticas para Amazon Macie

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Macie define los siguientes tipos de recursos:

- Lista de permitidos
- Identificador de datos personalizado
- Regla de filtrado o supresión, también denominada filtro de resultados
- Cuenta de miembro
- Trabajo de detección de datos confidenciales, también denominado trabajo de clasificación

Puede especificar estos tipos de recursos en políticas utilizando los ARN.

Por ejemplo, para crear una política para el trabajo de detección de datos confidenciales que tenga el ID de trabajo 3ce05dbb7ec5505def334104bexample, puede usar el siguiente ARN:

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

O bien, para especificar todos los trabajos de detección de datos confidenciales de una cuenta determinada, utilice un comodín (*):

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

Donde *123456789012* es el identificador de la cuenta para la Cuenta de AWS que creó los trabajos. Sin embargo, recomendamos que las políticas se creen según el principio de privilegios mínimos. En otras palabras, debe crear políticas que incluyan solo los permisos necesarios para realizar una tarea específica en un recurso específico.

Algunas acciones de Macie pueden aplicarse a varios recursos. Por ejemplo, la acción `macie2:BatchGetCustomDataIdentifiers` puede recuperar los detalles de varios identificadores de datos personalizados. En estos casos, la entidad principal debe tener permisos para acceder a todos los recursos a los que se aplica la acción. Para especificar varios recursos en una única instrucción, separe los ARN con comas:

```
"Resource": [
```

```
  "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
  "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
  "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

Para ver una lista de los tipos de recursos de Amazon VPC y sus ARN, consulte Tipos de recursos definidos por Amazon Macie en la Referencia de autorizaciones de servicio. Para saber qué acciones puede especificar con cada tipo de recurso, consulte Acciones definidas por Amazon Macie en la Referencia de autorización de servicios. Para ver ejemplos de políticas que especifican recursos, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Claves de condición de políticas para Amazon Macie

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `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 con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

Para ver una lista de las claves de condición de Macie, consulte Claves de condición para Amazon Macie en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon Macie. Para ver ejemplos de políticas que utilizan claves de condición, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Listas de control de acceso (ACL) de Amazon Macie

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.

Amazon Simple Storage Service (Amazon S3) es un ejemplo de un Servicio de AWS que admite las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Macie no admite las ACL. Es decir, no se puede adjuntar una ACL a un recurso de Macie.

Control de acceso basado en atributos (ABAC) con Amazon Macie

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 entidades de IAM (usuarios o roles) y a muchos recursos de AWS. 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.

Puede adjuntar etiquetas a los recursos de Macie: listas de permitidos, identificadores de datos personalizados, reglas de filtrado y supresión, cuentas de miembros y tareas de la detección de datos confidenciales. También puede controlar el acceso a estos tipos de recursos proporcionando información sobre las etiquetas en el elemento `Condition` de una política. Para obtener información acerca del etiquetado de recursos de Macie, consulte Etiquetado de recursos de Amazon Macie. Para obtener un ejemplo de política basada en identidad que controla el acceso a un recurso basado en etiquetas, consulte Ejemplos de políticas basadas en identidad para Amazon Macie.

Uso de credenciales temporales con Amazon Macie

Admite el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utilice credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Macie admite el uso de credenciales temporales.

Sesiones de acceso directo para Amazon Macie

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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.

Macie envía solicitudes de FAS a Servicios de AWS posteriores cuando lleva a cabo las tareas siguientes:

- Creación o actualización de la configuración de Macie para una lista de elementos permitidos almacenada en un bucket de S3.
- Comprobación del estado de una lista de elementos permitidos almacenada en un bucket de S3.
- Recuperación de muestras de datos confidenciales de un objeto de S3 afectado mediante las credenciales de usuario de IAM.
- Cifrado de las muestras de datos confidenciales que se recuperan con las credenciales de usuario de IAM o un rol de IAM.
- Habilitación de Macie para que se integre con AWS Organizations.
- Designación de la cuenta de administrador delegada de Macie para una organización en AWS Organizations.

En lo que respecta a otras tareas, Macie permite al rol vinculado a un servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Roles vinculados a servicios para Amazon Macie.

Roles de servicio para Amazon Macie

Compatible con ROLES de servicio	No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Macie no asume ni utiliza roles de servicio. Macie utiliza un rol vinculado a un servicio para llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Roles vinculados a servicios para Amazon Macie.

Roles vinculados a servicios para Amazon Macie

Admite roles vinculados a servicios	Sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en su Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Macie permite al rol vinculado al servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte Roles vinculados a servicios para Amazon Macie.

Ejemplos de políticas basadas en identidad para Amazon Macie

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar recursos de Macie. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador puede crear políticas de IAM. Luego, el administrador puede agregar las políticas de IAM a 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 Macie, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Amazon Macie en la Referencia de autorizaciones de servicio.

Al crear una política, asegúrese de resolver advertencias de seguridad, errores, advertencias generales y sugerencias de AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) antes de guardar la política. IAM Access Analyzer ejecuta verificaciones de política para validarla contra la Gramática de la política de IAM y las prácticas recomendadas. Estas verificaciones generan hallazgos y proporcionan recomendaciones procesables para ayudarlo a crear políticas funcionales y que se ajustan a las prácticas recomendadas de seguridad. Para obtener más información sobre la validación de políticas utilizando IAM Access Analyzer, consulte Validación de políticas de IAM Access Analyzer en la Guía del usuario de IAM. Para ver una lista de advertencias, errores y sugerencias que devuelve IAM Access Analyzer, consulte Referencia de verificación de políticas de IAM Access Analyzer en la Guía del usuario de IAM.

Temas

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Macie de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con

el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se 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 de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.
- Use 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. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida 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 de usuario de IAM.

Uso de la consola de Amazon Macie

Para acceder a la consola de Amazon Macie, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos en su Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos

necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan usar la consola de Amazon Macie, cree políticas de IAM que les proporcionen acceso a la consola. Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Si crea una política que permite a los usuarios o roles utilizar la consola de Amazon Macie, asegúrese de que la política permita la acción `macie2:GetMacieSession`. De lo contrario, esos usuarios o roles no podrán acceder a ningún recurso o dato de Macie en la consola.

Asegúrese también de que la política permita tomar las medidas `macie2:List` adecuadas en relación con los recursos a los que esos usuarios o roles necesitan acceder en la consola. De lo contrario, no podrán acceder a esos recursos ni mostrar detalles sobre ellos en la consola. Por ejemplo, para revisar los detalles de un trabajo de detección de datos confidenciales mediante la consola, el usuario debe poder realizar la acción `macie2:DescribeClassificationJob` correspondiente al trabajo y la acción `macie2:ListClassificationJobs`. Si a un usuario no se le permite realizar la acción `macie2:ListClassificationJobs`, no podrá mostrar una lista de trabajos en la página Trabajos de la consola y, por lo tanto, no podrá elegir el trabajo para mostrar sus detalles. Para que los detalles incluyan información sobre el identificador de datos personalizado que utiliza el trabajo, el usuario también debe poder realizar la acción `macie2:BatchGetCustomDataIdentifiers` correspondiente al identificador de datos personalizado.

Ejemplo: Permitir que los usuarios vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Ejemplo: permitir a los usuarios crear trabajos de detección de datos confidenciales

En este ejemplo se muestra cómo podría crear una política que permita a un usuario crear trabajos de detección de datos confidenciales.

En el ejemplo, la primera sentencia concede permisos `macie2:CreateClassificationJob` al usuario. Estos permisos permiten al usuario crear trabajos. La declaración también concede permisos `macie2:DescribeClassificationJob`. Estos permisos permiten al usuario acceder a los detalles de los trabajos existentes. Si bien estos permisos no son necesarios para crear trabajos, el acceso a estos detalles puede ayudar al usuario a crear trabajos con ajustes de configuración únicos.

La segunda afirmación del ejemplo permite al usuario crear, configurar y revisar trabajos mediante la consola Amazon Macie. Los permisos `macie2:ListClassificationJobs` permiten al usuario

mostrar los trabajos existentes en la página Trabajos de la consola. Todos los demás permisos de la declaración permiten al usuario configurar y crear un trabajo mediante las páginas Crear trabajo de la consola.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo: permitir a los usuarios administrar un trabajo de detección de datos confidenciales

En este ejemplo se muestra cómo podría crear una política que permita a un usuario tener acceso a los detalles de un trabajo de detección de información confidencial en particular, el trabajo cuyo identificador es `3ce05dbb7ec5505def334104bexample`. El ejemplo también permite al usuario cambiar el estado del trabajo según sea necesario.

En el ejemplo, la primera instrucción concede permisos `macie2:DescribeClassificationJob` y `macie2:UpdateClassificationJob` al usuario. Estos permisos permiten al usuario recuperar los

detalles del trabajo y cambiar su estado, respectivamente. La segunda instrucción otorga permisos `macie2:ListClassificationJobs` al usuario, lo que le permite acceder al trabajo mediante la página Trabajos de la consola de Amazon Macie.

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

También puede permitir que el usuario acceda a los datos de registro (eventos de registro) que Macie publica en Registros de Amazon CloudWatch para el trabajo. Para ello, puede añadir instrucciones que concedan permisos para realizar acciones de registros CloudWatch (`logs`) en el grupo de registro y transmitir la tarea. Por ejemplo:

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
    },
    {
```

```
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

Para obtener más información sobre administración de accesos a registros de CloudWatch, consulte Información general sobre la administración de los permisos de acceso a los registros de CloudWatch en la Guía del usuario de Registros de Amazon CloudWatch.

Ejemplo: permitir a los usuarios revisar los resultados

En este ejemplo se muestra cómo crear una política que permita el acceso de un ususario a los datos de resultados.

En este ejemplo, los permisos `macie2:GetFindings` y `macie2:GetFindingStatistics` permiten al usuario recuperar los datos mediante la API de Amazon Macie o la consola de Amazon Macie. Los permisos `macie2:ListFindings` permiten al usuario recuperar y revisar los datos mediante el panel Resumen y las páginas Resultados de la consola de Amazon Macie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

También puede permitir que el usuario cree y administre reglas de filtrado y reglas de supresión para los resultados. Para ello, puede incluir una instrucción que conceda los siguientes permisos: `macie2:CreateFindingsFilter`, `macie2:GetFindingsFilter`, `macie2:UpdateFindingsFilter`, y `macie2:DeleteFindingsFilter`. Para permitir que el usuario administre las reglas mediante la consola de Amazon Macie, incluya también los permisos `macie2:ListFindingsFilters` en la política. Por ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
        {
            "Sid": "ListRulesOnConsole",
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

Ejemplo: permitir a los usuarios revisar los identificadores de datos personalizados en función de las etiquetas

En la política basada en la identidad, puede utilizar condiciones para controlar el acceso a los recursos de Amazon Macie basados en etiquetas. En este ejemplo se muestra cómo podría crear una política que permita a un usuario revisar identificadores de datos personalizados mediante la consola de Amazon Macie o la API de Amazon Macie. Sin embargo, los permisos solo se conceden si la etiqueta `Owner` tiene el valor del nombre de usuario.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

En este ejemplo, si un usuario que tiene el nombre de usuario `richard-roe` intenta revisar los detalles de un identificador de datos personalizado, el identificador de datos personalizado debe estar etiquetado `Owner=richard-roe` o `owner=richard-roe`. De lo contrario, se deniega el acceso al usuario. La clave de la etiqueta de condición `Owner` coincide con `Owner` y `owner` porque los nombres de clave de condición no distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

Roles vinculados a servicios para Amazon Macie

Amazon Macie utiliza un rol vinculado a un servicio AWS Identity and Access Management (IAM) denominado. `AWSServiceRoleForAmazonMacie` Este rol vinculado a servicio es un rol de IAM que está vinculado directamente a Macie. Está predefinido por Macie e incluye todos los permisos que Macie necesita para llamar a otros recursos Servicios de AWS y supervisarlos en su nombre. AWS Macie utiliza esta función vinculada al servicio en todos los Regiones de AWS donde Macie está disponible.

Un rol vinculado a un servicio simplifica la configuración de Macie porque ya no tendrá que agregar manualmente los permisos necesarios. Macie define los permisos de este rol vinculado a un servicio y, a menos que esté definido de otra manera, solo Macie puede asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Debe configurar permisos para permitir a una entidad de IAM (como usuario 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. Solo puede eliminar un rol vinculado a servicios únicamente después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de , ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Seleccione una opción Sí con una conexión para revisar la documentación acerca del rol vinculado a un servicio en cuestión.

Temas

- Permisos de roles vinculados a un servicio para Amazon Macie
- Creación del rol vinculado a un servicio para Amazon Macie
- Edición del rol vinculado a un servicio para Amazon Macie
- Eliminación de un rol vinculado a un servicio para Amazon Macie
- Compatible con Regiones de AWS el rol vinculado al servicio Amazon Macie

Permisos de roles vinculados a un servicio para Amazon Macie

Amazon Macie usa el rol vinculado a servicios denominado `AWSServiceRoleForAmazonMacie`. Este rol vinculado a un servicio confía en el servicio `macie.amazonaws.com` para asumir el rol.

La política de permisos del rol, denominada `AmazonMacieServiceRolePolicy`, permite a Macie realizar tareas como las siguientes en los recursos especificados:

- Utilizar las acciones de Amazon S3 para recuperar información sobre buckets y objetos de S3.
- Utilizar las acciones de Amazon S3 para recuperar objetos de S3.
- Usa AWS Organizations acciones para recuperar información sobre las cuentas asociadas.
- Utilice las acciones de Amazon CloudWatch Logs para registrar eventos para trabajos de descubrimiento de datos confidenciales.

El rol se configura con la siguiente política de permisos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Para obtener más información sobre actualizaciones a la política `AmazonMacieServiceRolePolicy`, consulte Actualizaciones de Amazon Macie en las políticas administradas por AWS. Para recibir alertas automáticas sobre los cambios en esta política, suscríbase a la fuente RSS de la página del historial de documentos de Macie.

Debe configurar permisos para permitir a una entidad de IAM (como usuario 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.

Creación del rol vinculado a un servicio para Amazon Macie

No necesita crear manualmente el rol vinculado a un servicio `AWSServiceRoleForAmazonMacie` para Amazon Macie. Cuando habilitas Macie para ti Cuenta de AWS, Macie crea automáticamente el rol vinculado al servicio para ti.

Si elimina el rol vinculado a un servicio de Macie y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando se vuelve a habilitar Macie, esta se encarga de volver a crear el rol vinculado a un servicio para usted.

Edición del rol vinculado a un servicio para Amazon Macie

Amazon Macie no le permite editar el rol vinculado a un servicio `AWSServiceRoleForAmazonMacie`. Una vez creado un rol vinculado a servicios, no puede cambiar el nombre del rol porque varias entidades pueden hacer referencia a este. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Amazon Macie

Si ya no utiliza Amazon Macie, le recomendamos que elimine manualmente el rol vinculado a servicios `AWSServiceRoleForAmazonMacie`. Cuando inhabilita Macie, esta no elimina el rol por usted.

Antes de eliminar el rol, debes deshabilitar a Macie en cada Región de AWS lugar donde lo hayas activado. También debe limpiar manualmente los recursos del rol. Para eliminar el rol, puede usar la consola de IAM AWS CLI, la o la AWS API. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

> **Note**
>
> Si Macie está utilizando el rol `AWSServiceRoleForAmazonMacie` cuando intente eliminar los recursos, es posible que se produzcan errores en la operación de eliminación. En ese caso, espere unos minutos e intente de nuevo la operación.

Si elimina el rol vinculado a un servicio `AWSServiceRoleForAmazonMacie` y necesita crearlo de nuevo, puede hacerlo habilitando Macie para su cuenta. Cuando se vuelve a habilitar Macie, esta se encarga de volver a crear el rol vinculado a un servicio para usted.

Compatible con Regiones de AWS el rol vinculado al servicio Amazon Macie

Amazon Macie admite el uso de la función `AWSServiceRoleForAmazonMacie` vinculada al servicio en todos los Regiones de AWS lugares en los que Macie esté disponible. Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión y cuotas de Amazon Macie en la Referencia general de AWS.

Políticas administradas por AWS para Amazon Macie

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

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. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas por AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Amazon Macie ofrece varias políticas administradas AWS: la política `AmazonMacieFullAccess`, la política `AmazonMacieReadOnlyAccess` y la `AmazonMacieServiceRolePolicy` política.

Temas

- Política administrada por AWS: AmazonMacieFullAccess
- Política administrada por AWS: AmazonMacieReadOnlyAccess
- Política administrada por AWS: AmazonMacieServiceRolePolicy
- Actualizaciones de Amazon Macie en las políticas administradas por AWS

Política administrada por AWS: AmazonMacieFullAccess

También puede adjuntar la política `AmazonMacieFullAccess` a sus entidades de IAM.

Esta política concede todos los permisos administrativos que permiten a una identidad de IAM (entidad principal) crear el rol vinculado al servicio de Amazon Macie y realizar todas las acciones de

lectura y escritura para Amazon Macie. Los permisos incluyen funciones de mutación como crear, actualizar y eliminar. Si esta política está vinculada a una entidad principal, esta entidad podrá crear, recuperar y acceder de cualquier otro modo a todos los recursos, datos y ajustes de Macie de su cuenta.

Esta política debe estar vinculada a la entidad principal antes de que esta pueda habilitar a Macie para su cuenta; la entidad principal debe poder crear el rol vinculado al servicio de Macie para habilitar a Macie para su cuenta.

Detalles sobre los permisos

Esta política incluye los siguientes permisos:

- `macie2`: permite a las entidades principales realizar todas las acciones de lectura y escritura para Amazon Macie.
- `iam`: permite que las entidades principales creen un rol vinculado al servicio. El elemento `Resource` especifica el rol vinculado al servicio para Macie. El elemento `Condition` utiliza la clave de condición `iam:AWSServiceNamey` el operador de condición `StringLike` para restringir los permisos al rol vinculado al servicio de Macie.
- `pricing`: permite a las entidades principales recuperar sus datos de precios. Cuenta de AWS de AWS Billing and Cost Management. Macie utiliza estos datos para calcular y mostrar los costos estimados cuando las entidades principales crean y configuran tareas de detección de datos confidenciales.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
```

```
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
   ]
}
```

Política administrada por AWS: AmazonMacieReadOnlyAccess

También puede adjuntar la política `AmazonMacieReadOnlyAccess` a sus entidades de IAM.

Esta política concede permisos de solo lectura que permiten a una identidad de IAM (entidad principal) realizar todas las acciones de lectura para Amazon Macie. Los permisos incluyen funciones de mutación como crear, actualizar y eliminar. Si esta política está vinculada a una entidad principal, esta podrá crear, recuperar y acceder de cualquier otro modo a todos los recursos, datos y ajustes de Macie de su cuenta.

Detalles sobre los permisos

Esta política incluye los siguientes permisos:

`macie2`: permite a las entidades principales realizar todas las acciones de lectura para Amazon Macie.

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

```
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

Política administrada por AWS: AmazonMacieServiceRolePolicy

No puede adjuntar la política `AmazonMacieServiceRolePolicy` a sus entidades de IAM. Esta política está adjunta a un rol vinculado al servicio que permite a Macie realizar acciones en su nombre. Para obtener más información, consulte Roles vinculados a servicios para Amazon Macie.

Actualizaciones de Amazon Macie en las políticas administradas por AWS

Consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon Macie debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Macie.

Cambio	Descripción	Fecha
AmazonMacieReadOnlyAccess agregó una nueva política.	Macie agregó una nueva política, la política `AmazonMacieReadOnlyAccess` . Esta política otorga permisos de solo lectura que permiten a las entidades principales recuperar todos los recursos, datos y configuraciones de Macie para sus cuentas.	15 de junio de 2023

Cambio	Descripción	Fecha
AmazonMacieFullAccess: actualización de una política existente	En la política `AmazonMacieFullAccess`, Macie actualizó el nombre de recurso de Amazon (ARN) del rol vinculado al servicio de Macie (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	30 de junio de 2022
AmazonMacieServiceRolePolicy: actualización de una política existente	Macie eliminó las acciones y los recursos de Amazon Macie Classic de la política `AmazonMacieServiceRolePolicy`. Amazon Macie Classic se ha descatalogado y ya no está disponible. Más específicamente, Macie eliminó todas las acciones AWS CloudTrail. Macie también eliminó todas las acciones de Amazon S3 para los siguientes recursos: `arn:aws:s3:::awsmacie-*`, `arn:aws:s3:::awsmacietrail-*`, `yarn:aws:s3:::*-awsmacietrail-*`.	20 de mayo de 2022

Cambio	Descripción	Fecha
AmazonMacieFullAccess: actualización de una política existente	Macie agregó una acción AWS Billing and Cost Management (`pricing`) a la política `AmazonMacieFullAccess` . Esta acción permite a las entidades principales recuperar sus datos de precios para su cuenta. Macie utiliza estos datos para calcular y mostrar los costos estimados cuando las entidades principales crean y configuran tareas de detección de datos confidenciales. Macie eliminó las acciones de Amazon Macie Classic (`macie`) de la política `AmazonMacieFullAccess` .	7 de marzo de 2022
AmazonMacieServiceRolePolicy: actualización de una política existente	Macie agregó acciones de registros de Amazon CloudWatch a la política `AmazonMacieServiceRolePolicy` . Estas acciones permiten a Macie publicar eventos de registros en los registros de CloudWatch para tareas de detección de datos confidenciales.	13 de abril de 2021

Cambio	Descripción	Fecha
Macie comenzó a realizar seguimiento de los cambios	Macie comenzó a realizar el seguimiento de los cambios en sus políticas administradas de AWS	13 de abril de 2021

Solución de problemas de identidad y acceso de Amazon Macie

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Amazon Macie yAWS Identity and Access Management (IAM).

Temas

- No tengo autorización para realizar una acción en Amazon Macie
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Amazon Macie

No tengo autorización para realizar una acción en Amazon Macie

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `macie2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `macie2:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador de AWS. 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 de Amazon Macie

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 admite estas características, consulte Cómo trabaja Amazon Macie con AWS Identity and Access Management.
- 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.

Registro y monitoreo en Amazon Macie

Amazon Macie está integrado con AWS CloudTrail, que es un servicio que proporciona un registro de las acciones realizadas en Macie por un usuario, un rol u otro Servicio de AWS. Entre estas se incluyen las acciones realizadas desde la consola de Amazon Macie y las llamadas mediante programación a las operaciones de la API de Amazon Macie. Mediante el uso de la información recopilada por CloudTrail, se puede determinar qué solicitudes se realizaron en Macie. Para cada solicitud, puede identificar cuándo se realizó, la dirección IP desde la que se realizó, quién la realizó e información adicional. Para obtener más información, consulte Registro de llamadas a la API de Amazon Macie mediante AWS CloudTrail.

Validación de la conformidad de Amazon Macie

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon Macie

La infraestructura global de AWS está conformada por Regiones de AWS y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en Amazon Macie

Como se trata de un servicio administrado, Amazon Macie se encuentra protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Macie a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales 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 de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Amazon Macie y puntos de conexión de VPC de tipo interfaz (AWS PrivateLink)

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus recursos de AWS, puede establecer una conexión entre su VPC y Amazon Macie. Amazon VPC es un servicio de Servicio de AWS que puede utilizar para lanzar recursos de AWS en una red virtual que usted defina. Con una VPC, puede controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red.

Para conectar su VPC a , debe definir un punto de conexión de VPC para . Los puntos de conexión de la interfaz cuentan con AWS PrivateLink, una tecnología que permite acceder de forma privada a las API de Amazon Macie sin necesidad de contar con una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las API de Amazon Macie. El tráfico entre la VPC y Macie no sale de la red de Amazon.

Cada punto de enlace de la interfaz está representado por una o más interfaces de redes elásticas en las subredes. Para obtener más información, consulte Acceso a un servicio de Servicio de AWS a través de un punto de conexión de VPC de tipo interfaz en la Guía de usuario de Amazon VPC.

Temas

- Consideraciones sobre los puntos de conexión de VPC de Amazon Macie.
- Creación de un punto de conexión de VPC de tipo interfaz para Amazon Macie

Consideraciones sobre los puntos de conexión de VPC de Amazon Macie.

Amazon Macie admite puntos de conexión de VPC en todas las en las Regiones de AWS que está disponible actualmente, excepto las regiones Asia-Pacífico (Osaka) e Israel (Tel Aviv). Para obtener una lista de todas las regiones en las que Macie se encuentra actualmente disponible, consulte Puntos de conexión de Amazon Macie y cuotas en la Referencia general de AWS. Ademas, Macie admite realizar llamadas a todas las acciones de la API desde su VPC.

Si crea un punto de conexión de VPC de interfaz para Macie, considere la posibilidad de hacer lo mismo con otros Servicios de AWS que brinden soporte para VPC y se integren con Macie, como Amazon EventBridge y AWS Security Hub. Luego, Macie y esos servicios pueden usar puntos de conexión de VPC para la integración. Por ejemplo, si crea un punto de conexión de VPC para Macie y un punto de enlace de VPC para Security Hub, Macie puede usar su punto de conexión de VPC cuando publique los resultados en Security Hub y Security Hub puede usar su punto de conexión de VPC cuando reciba los resultados. Para obtener información sobre los servicios que admiten puntos de conexión de VPC, consulte qué Servicios de AWS se integra con AWS PrivateLink en la Guía del usuario de Amazon VPC.

Para obtener información adicional, consulte Acceso a un Servicio de AWS utilizando un punto de conexión de VPC de interfaz en la Guía del usuario de Amazon VPC.

Las políticas de punto de conexión de VPC no son compatibles con Macie. De forma predeterminada, el acceso completo a Macie se permite a través del punto de conexión. Para obtener más información, consulte Administración de identidades y accesos para puntos de conexión de VPC y servicios de puntos de conexión de VPC en la Guía de usuario de Amazon VPC.

Creación de un punto de conexión de VPC de tipo interfaz para Amazon Macie

Puede crear un punto de conexión de la VPC para el servicio de Amazon Macie mediante la consola de Amazon VPC o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Para crear un punto de conexión de VPC para Macie, utilice el siguiente nombre de servicio:

- com.amazonaws.*region*.macie 2

Donde la *región* es el código de región para la Región de AWS correspondiente.

Si habilita DNS privado para el punto de enlace, puede realizar solicitudes a la API para usando su nombre de DNS predeterminado para la región, por ejemplo del `macie2.us-east-1.amazonaws.com` Este de EE. UU. (Norte de Virginia).

Para obtener más información, consulte Acceso a un servicio de Servicio de AWS a través de un punto de conexión de VPC de tipo interfaz en la Guía de usuario de Amazon VPC.

Registro de llamadas a la API de Amazon Macie mediante AWS CloudTrail

Amazon Macie está integrado con AWS CloudTrail, que es un servicio que proporciona un registro de las acciones realizadas en Macie por un usuario, un rol u otro Servicio de AWS. CloudTrail captura las llamadas a la API de Macie como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Amazon Macie y las llamadas programáticas a las operaciones de la API de Amazon Macie.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos para Macie. Si no configura un registro de seguimiento, puede revisar los eventos más recientes en el campo Historial de eventos de la consola de AWS CloudTrail. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Macie, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la AWS CloudTrailGuía del usuario de .

Temas

Información sobre Amazon Macie en AWS CloudTrail

AWS CloudTrail se habilita para su Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Amazon Macie, dicha actividad se registra en un evento de CloudTrail junto con los demás eventos de AWS en Historial de eventos. Puede revisar, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de Macie, cree un registro de seguimiento. Un seguimiento habilita a CloudTrail a enviar archivos de registro a un bucket de Amazon Simple Storage Service (Amazon S3). De forma predeterminada, cuando se crea un registro de seguimiento con la consola de AWS CloudTrail, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de S3

especificado. También es posible configurar otros Servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas en la Guía del usuario deAWS CloudTrail:

- Creación de un registro de seguimiento para su Cuenta de AWS
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Amazon Macie se registran en CloudTrail y están documentadas en la referencia de la API de Amazon Macie. Por ejemplo, las llamadas a las acciones `CreateClassificationJob`, `DescribeBuckets` y `ListFindings` generan entradas en archivos de registro de CloudTrail.

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 credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de 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 Elemento userIdentity de CloudTrail en la Guía del usuario de AWS CloudTrail.

Descripción de las entradas de archivos de registro de Amazon Macie

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Un evento representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de AWS CloudTrail contienen una o más entradas de registro de los eventos. Los archivos de registro de

CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Los siguientes ejemplos muestran entradas de registro de CloudTrail que ilustran los eventos de acciones de Amazon Macie. Para obtener más información sobre los detalles que puede contener una entrada de registro, consulte Referencia de eventos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.

Ejemplo: enumeración de resultados

El siguiente ejemplo muestra una entrada de registro de CloudTrail que ilustra un evento de la acción ListFindings de Macie. En este ejemplo, un usuario de AWS Identity and Access Management (IAM) (`Mary_Major`) utilizó la consola de Amazon Macie para recuperar un subconjunto de información sobre los resultados de las políticas actuales de su cuenta.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
```

```
        "findingCriteria": {
            "criterion": {
                "archived": {
                    "eq": [
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Ejemplo: recuperación y revelación de muestras de datos confidenciales de un resultado

En este ejemplo, se muestran las entradas de registro de CloudTrail que ilustran los eventos de recuperación y revelación de muestras de datos confidenciales que Macie notificó en un resultado. En este ejemplo, un usuario de IAM (`JohnDoe`) utilizó la consola de Amazon Macie para recuperar y revelar muestras de datos confidenciales. La cuenta de Macie del usuario está configurada para asumir un rol de IAM (`MacieReveal`) a fin de recuperar y revelar muestras de datos confidenciales.

El siguiente evento de registro muestra detalles sobre la solicitud del usuario para recuperar y revelar muestras de datos confidenciales mediante la acción GetSensitiveDataOccurrences de Macie.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


El siguiente evento de registro muestra detalles sobre cómo Macie asume el rol de IAM especificado (`MacieReveal`) mediante la acción de AWS Security Token Service (AWS STS) AssumeRole.


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Etiquetado de recursos de Amazon Macie

Una etiqueta es una etiqueta opcional con la que se puede definir y asociar opcionalmente a recursos de AWS, incluidos determinados tipos de recursos de Amazon Macie . Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede asignar etiquetas a los siguientes tipos de recursos de Macie: listas de permitidos, identificadores de datos personalizados, reglas de filtrado y reglas de supresión de resultados y tareas de detección de datos confidenciales. Si es el administrador Macie de una organización, también puede asignar etiquetas a las cuentas de los miembros de su organización.

Temas

Aspectos básicos del etiquetado

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta está formada por una clave de etiqueta y un valor de etiqueta opcional, ambos definidos por el usuario. Una clave de etiqueta es una etiqueta general que actúa como una categoría para valores de etiqueta más específicos. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Por ejemplo, si crea identificadores de datos personalizados y tareas de detección de datos confidenciales para analizar los datos en diferentes puntos de un flujo de trabajo (un conjunto para los datos por etapas y otro para los datos de producción), puede asignar una clave de `Stack` etiqueta a esos recursos. El valor de etiqueta de esta clave de etiqueta puede ser `Staging` para identificadores de datos personalizados y trabajos diseñados para analizar datos por etapas, y `Production` para los demás.

Al definir y asignar etiquetas a recursos, tenga en cuenta lo siguiente:

- Cada recurso puede tener un máximo de 50 etiquetas.
- Para cada recurso, cada clave de etiqueta debe ser única y sólo puede tener un valor.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Como práctica recomendada, le aconsejamos que decida una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos sus recursos.
- Una clave de etiqueta puede tener un máximo de 128 caracteres UTF-8. Un valor de etiqueta puede tener una longitud máxima de 256 caracteres UTF-8. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
- El prefijo `aws:` se reserva para uso de AWS. No puede utilizarla en ninguna clave de etiqueta ni en ningún valor que defina. Además, las claves o valores de etiqueta que utilizan este prefijo no se pueden modificar ni quitar. Las etiquetas que usan este prefijo no cuentan para la cuota de 50 etiquetas por recurso.
- Las etiquetas que asigne estarán disponibles solo para suCuenta de AWS y sólo en el lugar Región de AWS en el que las asigne.
- Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Para obtener más restricciones, consejos y prácticas recomendadas, consulte la Guía del usuario para el etiquetado de recursos de AWS.

> **Important**
>
> No almacene datos confidenciales ni de otro tipo en etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluyendo AWS Billing and Cost Management. No se diseñaron para utilizarse con datos confidenciales.

Para añadir y gestionar etiquetas para los recursos de Macie, puede utilizar la consola de Amazon Macie, la API de Amazon Macie, el editor de etiquetas de la consola AWS Resource Groups, o la API de etiquetado AWS Resource Groups. Con Macie, puede añadir etiquetas a los recursos al crear el recurso. También puede añadir y gestionar etiquetas para los recursos individuales existentes. Con Resource Groups, puede añadir y administrar etiquetas de forma masiva para varios recursos existentes que abarcan varios Servicios de AWS, incluido Macie. Para obtener más información, consulte la Guía del usuario para el etiquetado de recursos de AWS.

Uso de etiquetas en las políticas de IAM

Una vez que comience a etiquetar recursos, puede definir permisos de recursos basados en etiquetas en las políticas de IAM AWS Identity and Access Management. Al utilizar las etiquetas de esta manera, puede implementar un control detallado de los usuarios y roles de su Cuenta de AWS que tienen permiso para crear y etiquetar recursos, y los usuarios y grupos que tienen permiso para añadir, editar y quitar etiquetas de forma más general. Para controlar el acceso en función de etiquetas, puede utilizar claves de condición relacionadas con etiquetas en el Elemento de condición de las políticas de IAM.

Por ejemplo, puede crear una política que permita a un usuario tener acceso completo a todos los recursos de Amazon Macie si la etiqueta `Owner` del recurso especifica su nombre de usuario:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Si define los permisos de nivel de recurso basados en etiquetas, estos entrarán en vigor inmediatamente. Esto significa que sus recursos están más seguros en cuanto se crean y que puede empezar a aplicar el uso de etiquetas de nuevos recursos rápidamente. También puede usar permisos de nivel de recurso para controlar las claves y valores de etiqueta que se pueden asociar a recursos nuevos y existentes. Para obtener más información, consulte Control del acceso a los recursos de AWS mediante etiquetas en la Guía del usuario de IAM.

Adición de etiquetas a los recursos de Amazon Macie

Para añadir etiquetas a un recurso individual de Amazon Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Para añadir etiquetas a varios recursos de Macie al mismo tiempo,

utilice el Editor de etiquetas de la consola de AWS Resource Groups o las operaciones de etiquetado de la API de etiquetado de AWS Resource Groups.

> **Important**
>
> Añadir etiquetas a un recurso puede afectar al acceso al recurso. Antes de añadir una etiqueta a un recurso, revise las políticas (de IAM) AWS Identity and Access Management que puedan usar etiquetas para controlar el acceso a los recursos.

Console

Al crear una lista de permitidos, un identificador de datos personalizado o un trabajo de detección de datos confidenciales, la consola de Amazon Macie ofrece opciones para añadir etiquetas al recurso. Siga las instrucciones de la consola para añadir etiquetas a estos tipos de recursos cuando los cree. Para añadir etiquetas a una regla de filtrado o supresión o a la cuenta de un miembro de una organización, debe crear el recurso antes de poder añadirle etiquetas.

Para agregar una o más etiquetas a un recurso existente mediante la consola de Amazon Macie, siga estos pasos.

Para añadir una etiqueta a un recurso

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En función del tipo de recurso al que desea añadir una etiqueta, seleccione una de las siguientes opciones:
   - Para ver una lista de permitidos, seleccione Permitir listas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la lista. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para un identificador de datos personalizado, seleccione Identificadores de datos personalizados en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación del identificador de datos personalizado. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para una regla de filtrado o supresión, seleccione Resultados en el panel de navegación.

A continuación, en la lista Reglas guardadas, seleccione el icono de edición ( ) situado junto a la regla. A continuación, seleccione Administrar etiquetas.

- Para una cuenta de miembro de su organización, seleccione Cuentas en el panel de navegación.

  A continuación, en la tabla, seleccione la casilla de verificación de la cuenta. A continuación, seleccione Administrar etiquetas en el menú Acciones.

- Para un trabajo de detección de datos confidenciales, seleccione Trabajos en el panel de navegación.

  A continuación, en la tabla, seleccione la casilla de verificación del trabajo. A continuación, seleccione Administrar etiquetas en el menú Acciones.

La ventana Administrar etiquetas muestra todas las etiquetas que están actualmente asignadas al recurso.

3. En la ventana Administrar etiquetas, seleccione Editar etiquetas.
4. Elija Añadir etiqueta.
5. En el cuadro Clave, introduzca la clave de etiqueta de la etiqueta que desee añadir al recurso. A continuación, en el cuadro Valor, si lo desea, introduzca un valor de etiqueta para la clave.

   Una clave de etiqueta incluye hasta 128 caracteres. Un valor de etiqueta puede incluir hasta 256 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
6. (Opcional) Para agregar otra fuente, seleccione Añadir fuente y, a continuación, repita los pasos anteriores. Puede asignar hasta 50 etiquetas a un recurso.
7. Cuando haya terminado de agregar etiquetas, seleccione Guardar.

API

Para crear un recurso y añadirle una o más etiquetas mediante programación, utilice la operación `Create` adecuada para el tipo de recurso que desee crear:

- Permitir lista: utilice la operación createAllowList o, si utiliza AWS Command Line Interface (AWS CLI), ejecute el comando create-allow-list.
- Identificador de datos personalizado: utilice la operación createCustomDataIdentifier o, si está utilizando el AWS CLI, ejecute el comando create-custom-data-identifier.
- Regla de filtrado o supresión: utilice la operación CreateFindingsFilter o, si utiliza la AWS CLI, ejecute el comando create-findings-filter.
- Cuenta de miembro: utilice la operación CreateMember o, si está utilizando la AWS CLI , ejecute el comando create-member.
- Trabajo de detección de datos confidenciales: utilice la operación CreateClassificationJob o, si está utilizando la AWS CLI, ejecute el comando create-classification-job.

En la solicitud, utilice el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que desee añadir al recurso. El parámetro `tags` especifica un mapa de cadena a cadena de las claves de etiqueta y sus valores de etiqueta asociados.

Para añadir una o más etiquetas a un recurso existente, utilice la operación TagResource de la API de Amazon Macie o, si utiliza la AWS CLI, ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso al que desea añadir una etiqueta. Utilice el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que desee añadir al recurso. Como ocurre con las operaciones y los comandos `Create`, el parámetro `tags` especifica un mapa cadena a cadena de las claves de las etiquetas y sus valores de etiqueta asociados.

Por ejemplo, el siguiente comando AWS CLI añade una clave de etiqueta `Stack` con un valor de etiqueta `Production` al trabajo especificado. Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

Donde:

- `resource-arn` especifica el ARN del trabajo al que se va a añadir una etiqueta.

- *Stack* es la clave de etiqueta de la etiqueta que se va a añadir al trabajo.
- *Production* El valor de la clave de etiqueta especificada (*Stack*).

En el siguiente ejemplo, el comando añade varias etiquetas al trabajo:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

Para cada etiqueta de un mapa `tags`, se requieren los argumentos `key` y `value`. Sin embargo, el valor del argumento `value` puede ser una cadena vacía. Si no desea asociar un valor de etiqueta a una clave de etiqueta, no especifique un valor para el argumento `value`. Por ejemplo, el siguiente comando AWS CLI añade una clave de etiqueta `Owner` sin ningún valor de etiqueta asociado:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

Si la operación de etiquetado se realiza correctamente, Macie devuelve una respuesta HTTP 204 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Revisión de etiquetas para recursos de Amazon Macie

Puede revisar las etiquetas (tanto las claves como los valores de las etiquetas) de un recurso de Amazon Macie mediante la consola de Amazon Macie o la API de Amazon Macie. Si prefiere hacerlo para varios recursos de Macie al mismo tiempo, puedes usar el Editor de etiquetas de la consola de AWS Resource Groups o las operaciones de etiquetado de la API de etiquetado AWS Resource Groups.

Console

Siga estos pasos para revistar las etiquetas de un recurso mediante la consola de Amazon Macie.

Revisar las etiquetas de un recurso

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Dependiendo del tipo de recurso cuyas etiquetas desea revisar, realice una de las siguientes acciones:

   - Para ver una lista de permitidos, seleccione Permitir listas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la lista. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para un identificador de datos personalizado, seleccione Identificadores de datos personalizados en el panel de navegación.

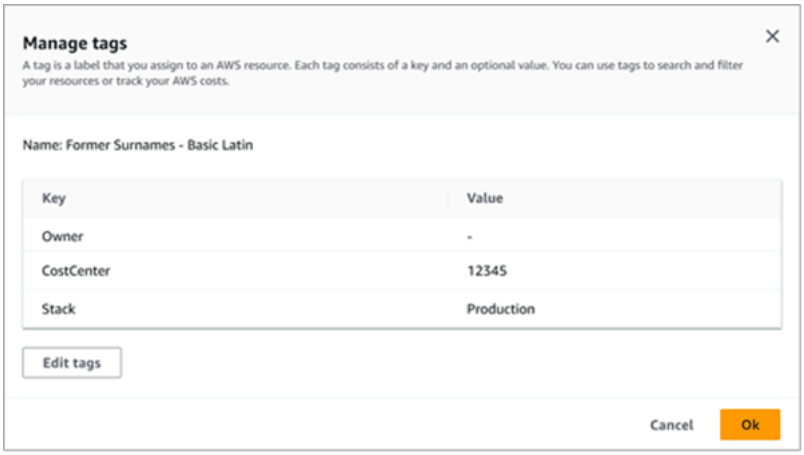
     A continuación, en la tabla, seleccione la casilla de verificación del identificador de datos personalizado. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para una regla de filtrado o supresión, seleccione Resultados en el panel de navegación.

     A continuación, en la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla. A continuación, seleccione Administrar etiquetas.
   - Para una cuenta de miembro de su organización, seleccione Cuentas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la cuenta. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para un trabajo de detección de datos confidenciales, seleccione Trabajos en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación del trabajo. A continuación, seleccione Administrar etiquetas en el menú Acciones.

   La ventana Administrar etiquetas muestra todas las etiquetas que están actualmente asignadas al recurso. Por ejemplo, la siguiente imagen muestra las etiquetas asignadas a un identificador de datos personalizado.



En este ejemplo, se asignan tres etiquetas al identificador de datos personalizado: la clave de etiqueta Owner sin ningún valor de etiqueta asociado; la clave de etiqueta CostCenter con 12345 como valor de etiqueta asociado; y la clave de etiqueta Stack con Production como valor de etiqueta asociado.

3. Cuando termine de revisar las etiquetas, pulse Cancelar para cerrar la ventana.

API

Para recuperar y revisar las etiquetas de un recurso existente mediante programación, puede utilizar la operación `Get` o `Describe` adecuada para el tipo de recurso cuyas etiquetas desee revisar. Por ejemplo, si utilizas la operación getCustomDataIdentifier o ejecutas el comando get-custom-data-identifier desde el AWS Command Line Interface (AWS CLI), la respuesta incluye un objeto `tags`. El objeto muestra todas las etiquetas (tanto las claves como los valores de las etiquetas) que están asignadas actualmente al recurso.

Puede utilizar la operación ListTagsForResourcede la API de Amazon Macie. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso. Si utiliza el AWS CLI, ejecute el comando list-tags-for-resource y utilice el parámetro `resource-arn` para especificar el ARN del recurso. Por ejemplo:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

En el ejemplo anterior, *`arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample`* es el ARN de un trabajo de detección de datos confidenciales existente.

Si la operación se realiza correctamente, Macie devuelve un objeto `tags` que muestra todas las etiquetas (tanto las claves como los valores de las etiquetas) que están asignadas actualmente al recurso. Por ejemplo:

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

Donde `StackCostCenter`, y `Owner` son las claves de etiqueta que se asignan al recurso. `Production` es el valor de etiqueta asociado a la clave de etiqueta `Stack`. `12345` es el valor de etiqueta asociado a la clave de etiqueta `CostCenter`. La clave de etiqueta `Owner` no tiene un valor de etiqueta asociado.

Para mostrar una lista de todos los recursos de que tienen etiquetas y todas las etiquetas asociadas a cada uno de esos recursos, use la operación GetResources de la API de etiquetado de AWS Resource Groups. En su solicitud, defina el valor del parámetro `ResourceTypeFilters` en `macie2`. Para ello, utilice el AWS CLI, ejecute el comando get-resources y defina el valor del parámetro `resource-type-filters` en. `macie2` Por ejemplo:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Si la operación se realiza correctamente, Resource Groups devuelve una matriz `ResourceTagMappingList` que contiene los ARN de todos los recursos de Macie que tienen etiquetas y las claves y valores de las etiquetas que están asignados a cada uno de esos recursos.

Edición de etiquetas para recursos de Amazon Macie

Para editar las etiquetas (claves o valores de etiqueta) de un recurso de Amazon Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Para hacerlo con varios recursos de Macie al mismo tiempo, utilice el Editor de etiquetas de la consola de AWS Resource Groups o las operaciones de etiquetado de la API de etiquetado AWS Resource Groups.

> **Important**
>
> La edición de las etiquetas de un recurso puede afectar al acceso al recurso. Antes de editar la clave o el valor de una etiqueta para un recurso, revise las políticas (de IAM) AWS Identity and Access Management que puedan utilizar la etiqueta para controlar el acceso a los recursos.

Console

Siga estos pasos para editar las etiquetas de un recurso mediante la consola de Amazon Macie.

Editar las etiquetas de un recurso

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Dependiendo del tipo de recurso cuyas etiquetas desea editar, realice una de las siguientes acciones:
   - Para ver una lista de permitidos, seleccione Permitir listas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la lista. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para un identificador de datos personalizado, seleccione Identificadores de datos personalizados en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación del identificador de datos personalizado. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para una regla de filtrado o supresión, seleccione Resultados en el panel de navegación.

     A continuación, en la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla. A continuación, seleccione Administrar etiquetas.
   - Para una cuenta de miembro de su organización, seleccione Cuentas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la cuenta. A continuación, seleccione Administrar etiquetas en el menú Acciones.

- Para un trabajo de detección de datos confidenciales, seleccione Trabajos en el panel de navegación.

  A continuación, en la tabla, seleccione la casilla de verificación del trabajo. A continuación, seleccione Administrar etiquetas en el menú Acciones.

La ventana Administrar etiquetas muestra todas las etiquetas que están actualmente asignadas al recurso.

3. En la ventana Administrar etiquetas, seleccione Editar etiquetas.
4. Realice uno de los siguientes procedimientos:

   - Para añadir un valor de etiqueta a una clave de etiqueta, introduzca el valor en el cuadro Valor situado junto a la clave de etiqueta.
   - Para cambiar una clave de etiqueta existente, seleccione Eliminar junto a la etiqueta. A continuación, seleccione Añadir etiqueta. En el cuadro Clave que aparece, introduzca la nueva clave de etiqueta. Si lo desea, introduzca en el cuadro Valor el valor de la etiqueta asociado.
   - Para cambiar el valor de una etiqueta existente, seleccione X en el cuadro Valor que contiene el valor. A continuación, escriba el valor de la etiqueta en el cuadro Valor.
   - Para eliminar un valor de etiqueta existente, seleccione X en el cuadro Valor que contiene el valor.
   - Para eliminar una etiqueta existente (la clave de etiqueta y el valor de la etiqueta), seleccione Eliminar junto a la etiqueta.

   Un recurso puede tener hasta 50 etiquetas. Una clave de etiqueta incluye hasta 128 caracteres. Un valor de etiqueta puede incluir hasta 256 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
5. Cuando haya terminado de editar la regla, seleccione Guardar.

API

Al editar una etiqueta de un recurso mediante programación, sobrescribe la etiqueta existente con valores nuevos. Por lo tanto, la mejor forma de editar una etiqueta depende de si desea editar una clave de etiqueta, un valor de etiqueta o ambos. Para editar una clave de etiqueta, elimine la etiqueta actual y añada una nueva.

Para editar o eliminar sólo el valor de etiqueta asociado a una clave de etiqueta, sobrescriba el valor existente mediante la operación TagResource de la API de Amazon Macie o, si usa el AWS Command Line Interface (AWS CLI) ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso cuyo valor de etiqueta desea editar o eliminar.

Para editar el valor de etiqueta de una clave de etiqueta, utilice el parámetro `tags` para especificar la clave de etiqueta cuyo valor de etiqueta desee cambiar y especifique el nuevo valor de etiqueta de la clave. Por ejemplo, el siguiente comando cambia el valor de etiqueta de `Production` a `Staging` para la clave de etiqueta `Stack` asociada al trabajo de detección de datos confidenciales especificado. Este ejemplo está formateado para Microsoft Windows y utiliza el carácter de continuación de línea de intercalación (^) para mejorar la legibilidad.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

Donde:

- `resource-arn` especifica el ARN del trabajo.
- *`Stack`* es la clave de etiqueta asociada al valor de etiqueta que desea cambiar.
- *`Staging`* es el nuevo valor de etiqueta que se utilizará para la clave de etiqueta especificada (*`Stack`*).

Para eliminar un valor de etiqueta de una clave de etiqueta, no especifique un valor para el argumento `value` en el parámetro `tags`. Por ejemplo:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

Si la operación se realiza correctamente, Macie devuelve una respuesta HTTP 204 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Eliminar etiquetas de los recursos de Amazon Macie

Para eliminar etiquetas de un recurso de Amazon Macie, puede utilizar la consola de Amazon Macie o la API de Amazon Macie. Para hacerlo con varios recursos de Macie al mismo tiempo, utilice el Editor de etiquetas de la consola de AWS Resource Groups o las operaciones de etiquetado de la API de etiquetado AWS Resource Groups.

> **Important**
>
> La eliminación de etiquetas de un recurso puede afectar al acceso al recurso. Antes de eliminar una etiqueta, revise cualquier política (de IAM) AWS Identity and Access Management que pueda utilizar la etiqueta para controlar el acceso a los recursos.

Console

Siga estos pasos para eliminar una o más etiquetas de un recurso mediante la consola de Amazon Macie.

Eliminar una etiqueta de un recurso

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. En función del tipo de etiqueta que desea eliminar del recurso, realice una de las siguientes acciones:

   - Para ver una lista de permitidos, seleccione Permitir listas en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación de la lista. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para un identificador de datos personalizado, seleccione Identificadores de datos personalizados en el panel de navegación.

     A continuación, en la tabla, seleccione la casilla de verificación del identificador de datos personalizado. A continuación, seleccione Administrar etiquetas en el menú Acciones.
   - Para una regla de filtrado o supresión, seleccione Resultados en el panel de navegación.

     A continuación, en la lista Reglas guardadas, seleccione el icono de edición () situado junto a la regla. A continuación, seleccione Administrar etiquetas.

- Para una cuenta de miembro de su organización, seleccione Cuentas en el panel de navegación.

  A continuación, en la tabla, seleccione la casilla de verificación de la cuenta. A continuación, seleccione Administrar etiquetas en el menú Acciones.
- Para un trabajo de detección de datos confidenciales, seleccione Trabajos en el panel de navegación.

  A continuación, en la tabla, seleccione la casilla de verificación del trabajo. A continuación, seleccione Administrar etiquetas en el menú Acciones.

La ventana Administrar etiquetas muestra todas las etiquetas que están actualmente asignadas al recurso.

3. En la ventana Administrar etiquetas, seleccione Editar etiquetas.
4. Realice uno de los siguientes procedimientos:
   - Para eliminar únicamente el valor de etiqueta de una etiqueta, seleccione X en el cuadro Valor que contiene el valor que desee eliminar.
   - Para eliminar la clave de etiqueta y el valor de la etiqueta (como un par) de una etiqueta, seleccione Eliminar junto a la etiqueta que desee eliminar.
5. (Opcional) Para eliminar más etiquetas del recurso, repita el paso anterior para cada etiqueta adicional que desee eliminar.
6. Cuando termine de eliminar las etiquetas, seleccione Guardar.

API

Para eliminar una o más etiquetas de un recurso mediante programación, utilice la operación UntagResource de la API Amazon Macie. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso del que desea eliminar una etiqueta. Utilice el parámetro `tagKeys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Para eliminar sólo un valor de etiqueta específico (no una clave de etiqueta) de un recurso, edite la etiqueta en lugar de eliminarla.

Si usa AWS Command Line Interface (AWS CLI), ejecute el comando untag-resource y use el parámetro `resource-arn` para especificar el ARN del recurso del que quieres eliminar una etiqueta. Utilice el parámetro `tag-keys` para especificar la clave de etiqueta de la etiqueta que

se va a eliminar. Por ejemplo, el siguiente comando elimina la etiqueta `Stack` (tanto la clave como el valor de la etiqueta) del trabajo de detección de datos confidenciales especificado:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

Donde `resource-arn` especifica el ARN del trabajo del que se va a eliminar una etiqueta y *`Stack`* es la clave de etiqueta de la etiqueta que se va a eliminar.

Para eliminar varias etiquetas de un recurso, añada cada clave adicional como argumento para el parámetro `tag-keys`. Por ejemplo:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

Donde `resource-arn` especifica el ARN del trabajo del que se van a eliminar las etiquetas, y *`Stack`* y *`Owner`* son las claves de las etiquetas que se van a eliminar.

Si la operación se realiza correctamente, Macie devuelve una respuesta HTTP 204 vacía. De lo contrario, Macie devuelve una respuesta HTTP 4 xx o 500 que indica el motivo del error de la operación.

Crear recursos de Amazon Macie con AWS CloudFormation

Amazon Macie está integrado con AWS CloudFormation, un servicio que lo ayuda a modelar y configurar los 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 (tales como identificadores de datos personalizados) y AWS CloudFormation aprovisiona y configura estos recursos por usted.

Cuando utiliza AWS CloudFormation, puede volver a utilizar la plantilla para configurar sus recursos de Macie 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 de AWS y Regiones de AWS.

Temas

Amazon Macie y plantillas AWS CloudFormation

Para aprovisionar y configurar los recursos de Amazon Macie y los 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 AWS CloudFormation Designer, una herramienta gráfica para crear y modificar plantillas AWS CloudFormation. Con Designer, puede hacer un diagrama de los recursos de su plantilla con una interfaz de arrastrar y soltar y, a continuación, editar sus detalles mediante el editor de JSON y YAML integrado. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

Puede crear plantillas de AWS CloudFormation para los siguientes tipos de recursos de Macie:

- Listas de permitidos
- Identificadores de datos personalizados
- Regla de filtrado o supresión, también denominada filtro de resultados

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para estos recursos, consulte la referencia del tipo de recurso de Amazon Macie 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

Suspensión o deshabilitación de Amazon Macie

Puede suspender o deshabilitar Amazon Macie en una Región de AWS específica con la consola de Amazon Macie o la API de Amazon Macie. Macie deja de realizar todas las actividades para su cuenta en esa región. No se le cobrará por usar Macie en la región mientras esté suspendido o deshabilitado.

Si suspende o inhabilita Macie, podrá volver a activarlo más adelante.

Temas

Suspensión de Amazon Macie

Si suspende Amazon Macie, Macie conservará el identificador de sesión, la configuración y los recursos de su cuenta, en la Región de AWS correspondiente. Por ejemplo, sus resultados actuales permanecen intactos y se retienen durante un máximo de 90 días. Sin embargo, cuando suspende Macie, deja de realizar todas las actividades de su cuenta en la región correspondiente. Esto incluye la supervisión de sus datos de Amazon Simple Storage Service (Amazon S3), la detección automática de datos confidenciales y la ejecución de cualquier trabajo de detección de datos confidenciales que se esté realizando en ese momento. Macie también cancela todos sus trabajos de detección de datos confidenciales en la región.

Después de suspender Macie, puede activarlo de nuevo. Luego recuperará el acceso a todos los ajustes y recursos de la región correspondiente, y Macie reanuda todas las actividades de su cuenta en esa región. Esto incluye actualizar el inventario de buckets de S3 de su cuenta y monitorear los buckets de seguridad y control de acceso. Esto no incluye la reanudación o el reinicio de sus trabajos de detección de datos confidenciales. Los trabajos de detección de datos confidenciales no se pueden reanudar ni reiniciar una vez cancelados.

En este tema se explica cómo suspender Macie con la consola Amazon Macie. Si prefiere hacerlo mediante programación, puede utilizar la operación UpdateMacieSession de la API de Amazon Macie.

> **Note**
>
> Si usted es el administrador de Macie de una organización, debe eliminar todas las cuentas de miembros asociadas a su cuenta antes de suspender Macie para su cuenta. Para obtener más información, consulte Administración de varias cuentas .

Para suspender Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región en la que desea suspender Macie.
3. En el panel de navegación, seleccione Settings (Configuración).
4. Seleccione Suspender Macie.
5. Cuando se le solicite confirmación, ingrese **Suspend** y luego, elija Suspender

Para suspender Macie en otras regiones, repita los pasos anteriores en cada región adicional.

Deshabilitación de Amazon Macie

Cuando se deshabilita Amazon Macie, Macie deja de realizar todas las actividades para su cuenta en la correspondiente Región de AWS. Esto incluye la supervisión de sus datos de Amazon Simple Storage Service (Amazon S3), la detección automática de datos confidenciales y la ejecución de cualquier trabajo de detección de datos confidenciales que se esté realizando en ese momento. Macie también elimina todas las configuraciones y los recursos existentes que almacene o mantenga para su cuenta en la región correspondiente, incluidos sus resultados y trabajos de detección de datos confidenciales. Los datos que haya almacenado o publicado en otros Servicios de AWS permanecerán intactos y no se verán afectados; por ejemplo, los resultados de la detección de datos confidenciales en Amazon S3 y los eventos de resultados en Amazon EventBridge.

> **Warning**
>
> Si desactiva Macie, también eliminará permanentemente todos los resultados existentes, los trabajos de detección de datos confidenciales, los identificadores de datos personalizados y otros recursos que Macie almacene o mantenga para su cuenta en la región

correspondiente. Estos recursos no se pueden recuperar una vez eliminados. Para conservar los recursos y solo pausar su uso de Macie, suspenda Macie en lugar de deshabilitarlo.

En este tema se explica cómo deshabilitar Macie con la consola de Amazon Macie. Si prefiere hacerlo mediante programación, puede utilizar la operación DisableMacie de la API de Amazon Macie.

> **Note**
>
> Si su cuenta es parte de una organización que administra de forma centralizada varias cuentas Macie, debe hacer lo siguiente antes de deshabilitar Macie:
>
> - Si su cuenta es una cuenta de miembro de Macie, póngase en contacto con su administrador de Macie para eliminarla como cuenta de miembro.
> - Si su cuenta es una cuenta de administrador de Macie, elimine todas las cuentas de miembros que estén asociadas a su cuenta y elimine las asociaciones entre su cuenta y esas cuentas.
>
> La forma de realizar las tareas anteriores dependerá de si su cuenta de Macie está asociada a otras cuentas mediante AWS Organizations o mediante invitación. Para obtener más información, consulte Administración de varias cuentas .

Para deshabilitar Macie

1. Abra la consola de Amazon Macie en https://console.aws.amazon.com/macie/.
2. Con el selector Región de AWS en la esquina superior derecha de la página, seleccione la región de en la que desea deshabilitar Macie.
3. En el panel de navegación, seleccione Settings (Configuración).
4. Seleccione Habilitar Macie.
5. Cuando se le solicite confirmación, ingrese **`Disable`** y luego, elija Deshabilitar

Para deshabilitar a Macie en otras regiones, repita los pasos anteriores en cada región adicional.

Cuotas de Amazon Macie

Su Cuenta de AWS tiene algunas cuotas predeterminadas, anteriormente conocidas como límites, para cada Servicio de AWS. Estas cuotas establecen el número máximo de recursos u operaciones de servicio que puede haber en su cuenta. En este tema, se enumeran las cuotas que se aplican a los recursos y las operaciones de Amazon Macie para su cuenta. A menos que se indique lo contrario, cada cuota se aplica a su cuenta en cada Región de AWS.

Algunas cuotas pueden aumentarse, mientras que otras no. Para solicitar el aumento de una cuota, use la consola de Service Quotas. Para saber cómo solicitar el aumento de una cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si no hay una cuota disponible en la consola de Service Quotas, utilice el formulario de aumento del límite de servicio en AWS Support Center Console para solicitar un aumento de la cuota.

Cuentas

- Cuentas de los miembros por invitación: 1000
- Cuentas de miembros hasta AWS Organizations: 10 000

Resultados

- Reglas de filtrado y reglas de supresión por cuenta: 1000
- Hallazgos por ejecución de un trabajo de detección de datos confidenciales: 100 000 más el 5 % de los hallazgos restantes una vez alcanzado el umbral de 100 000

  Esta cuota se aplica únicamente a la consola de Amazon Macie y a la API de Amazon Macie. No hay un límite para el número de eventos de hallazgos que Macie publica en Amazon EventBridge ni para el número de resultados de detección de datos confidenciales que crea Macie para cada ejecución de un trabajo.
- Ubicaciones de detección por hallazgo de datos confidenciales: 15
- Solicitudes para recuperar y revelar muestras de datos confidenciales de un objeto de Amazon S3: 100 por día

  Esta cuota se restablece cada 24 horas a las 00:00:01 UTC+0.
- Tamaño de un objeto de Amazon S3 para recuperar y revelar muestras de datos confidenciales de:
  - Archivo contenedor de objetos Apache Avro (.avro): 70 MB

- Archivo de Apache Parquet (.parquet): 100 MB
- Archivo CSV (.csv): 255 MB
- Archivo comprimido GNU Zip (.gz o .gzip): 90 MB
- Archivo JSON o JSON Lines (.json o .jsonl): 25 MB
- Archivo de libro de trabajo de Microsoft Excel (.xlsx): 20 MB
- Archivo de texto no binario (text/plain): 100 MB
- Archivo TSV (.tsv): 75 MB
- Archivo de ZIP comprimido (.zip): 355 MB

Si un resultado se aplica a un archivo de almacenamiento que genera varios archivos .gz para obtener los resultados de la detección de datos confidenciales correspondientes, no se podrán recuperar ni revelar muestras de datos confidenciales del archivo de almacenamiento.

Detección de datos confidenciales

- Análisis mensual por cuenta mediante trabajos de detección de datos confidenciales: 5 TB

  Esta cuota solo se aplica a trabajos de detección de datos confidenciales. Para aumentar la cuota hasta 1000 TB (1 PB), utilice la consola Service Quotas. Para solicitar un aumento de más de 1 PB, utilice el formulario de aumento del límite de servicio que se encuentra en AWS Support Center Console.
- Identificadores de datos personalizados por cuenta: 10 000
- Listas de permisos por cuenta: 10, de 1 a 5 listas de permisos que especifiquen texto predefinido y de 1 a 5 listas de permisos que especifiquen expresiones regulares

  Se aplican cuotas adicionales a una lista de permisos que especifique texto predefinido. La lista no puede contener más de 100 000 entradas y su tamaño de almacenamiento no puede superar los 35 MB.
- Bucket de S3 que se deben excluir de la detección automática de datos confidenciales: 1000

  Si su cuenta es la cuenta de administrador de Macie de una organización, esta cuota se aplica a su organización en general.
- Bucket de S3 por trabajo de detección de datos confidenciales: 1000

  Esta cuota no se aplica a los trabajos que utilizan los criterios de los bucket de tiempo de ejecución para determinar qué bucket analizar. Se aplica a un trabajo solo si lo configura para analizar los

bucket específicos que seleccione. Si su cuenta es la cuenta de administrador de Macie de una organización, puede seleccionar hasta 1000 bucket que abarquen hasta 1000 cuentas de su organización.

- Identificadores de datos personalizados por trabajo de detección de datos confidenciales: 30
- Listas de permisos por trabajo de detección de datos confidenciales: 10, de 1 a 5 listas de permisos que especifiquen texto predefinido y de 1 a 5 listas de permisos que especifiquen expresiones regulares
- Operación CreateClassificationJob: 0,1 solicitudes por segundo
- Tiempo de análisis de un archivo individual: 10 horas
- Tamaño de un archivo individual a analizar:
  - Archivo en formato de documento portátil de Adobe (.pdf): 1024 MB
  - Archivo contenedor de objetos Apache Avro (.avro): 8 GB
  - Archivo de Apache Parquet (.parquet): 8 GB
  - Archivo de mensajes de correo electrónico (.eml): 20 GB
  - Archivo comprimido GNU Zip (.gz o .gzip): 8 GB
  - Archivo de libro de trabajo de Microsoft Excel (.xls o .xlsx): 512 MB
  - Archivo de documento de Microsoft Word (.doc o.docx): 512 MB
  - Archivo de texto no binario: 20 GB
  - Archivo TAR (.tar): 20 GB
  - Archivo de ZIP comprimido (.zip): 8 GB

  Si un archivo supera la cuota correspondiente, Macie no analiza ningún dato del archivo.
- Extracción y análisis de los datos de un archivo comprimido o archivado:
  - Tamaño de almacenamiento (comprimido): 8 GB para un archivo comprimido GNU Zip (.gz o .gzip) o ZIP (.zip); 20 GB para un archivo TAR (.tar)
  - Profundidad del archivo anidado: 10 niveles
  - Archivos extraídos: 1 000 000
  - Bytes extraídos: 10 GB de datos sin comprimir en total. 3 GB de datos sin comprimir por cada archivo extraído que utilice un tipo de archivo o formato de almacenamiento compatible.

  Si los metadatos de un archivo comprimido o archivado indican que el archivo contiene más de 10 niveles anidados o que supera la cuota correspondiente de tamaño de almacenamiento o de bytes extraídos, Macie no extrae ni analiza ningún dato del archivo. Si Macie comienza a extraer

y analizar los datos de un archivo comprimido o archivado y, posteriormente, determina que el archivo contiene más de 1 000 000 de archivos o supera la cuota de bytes extraídos, deja de analizar los datos del archivo y crea hallazgos de datos confidenciales y resultados de detección solo para los datos que se procesaron.

- Análisis de elementos anidados en datos estructurados: 256 niveles por archivo

  Esta cuota solo se aplica a los archivos JSON (.json) y JSON Lines (.jsonl). Si la profundidad anidada de cualquier tipo de archivo supera esta cuota, Macie no analiza ningún dato del archivo.
- Ubicaciones de detección por resultado de detección de datos confidenciales: 1000 por tipo de detección de datos confidenciales
- Detección de nombres completos: 1000 por archivo, incluidos los archivados

  Cuando Macie detecta las primeras 1000 apariciones de nombres completos en un archivo, Macie deja de aumentar el recuento y de proporcionar los datos de la ubicación de los nombres completos.
- Detección de direcciones de correo electrónico: 1000 por archivo, incluidos los archivados

  Cuando Macie detecta las primeras 1000 apariciones de direcciones de correo electrónico en un archivo, Macie deja de aumentar el recuento y de proporcionar los datos de la ubicación de las direcciones.

Historial de documentación para la guía de usuario de Amazon Macie

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de Amazon Macie. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Última actualización de la documentación: 20 de febrero de 2024

Cambio	Descripción	Fecha
Nueva funcionalidad	AWS Security Hub ahora proporciona controles de seguridad que comprueban el estado de Macie y la detección automática de datos confidenciales para las cuentas. Si estos controles están habilitados, Security Hub ejecuta periódicamente comprobaciones de seguridad para determinar si Macie está habilitada para un Cuenta de AWS (control Macie.1) y si la detección automática de datos confidenciales está habilitada para una cuenta de Macie (control Macie.2).	20 de febrero de 2024
Nueva funcionalidad	Macie ahora puede analizar los objetos de Amazon S3 cifrados mediante el cifrado de doble capa del lado del servidor con AWS KMS keys (DSSE-KMS). Estos objetos ahora pueden analizarse	17 de enero de 2024

	cuando Macie realiza un descubrimiento automatizado de datos confidenciales o usted ejecuta tareas de descubrimiento de datos confidenciales. Además, los buckets y objetos de S3 que utilizan el cifrado DSSE-KMS ahora se incluyen en las estadísticas y los metadatos que Macie proporciona sobre sus datos de Amazon S3.	
Nueva característica	Ahora puede configurar a Macie para que asuma una función AWS Identity and Access Management (IAM) cuando decida recuperar y revelar muestras de datos confidenciales de los que Macie informa en sus hallazgos. Las muestras pueden ser de ayuda para verificar la naturaleza de los datos confidenciales que encuentre Macie y para adaptar la investigación de un bucket y un objeto de Amazon S3 afectados.	16 de noviembre de 2023

Nueva funcionalidad	Macie ahora proporciona identificadores de datos gestionados diseñados para detectar números de cuentas bancarias internacionales (IBAN) en otros 47 países y regiones. Ahora puede utilizar Macie para detectar la aparición de números IBAN en más de 50 países y regiones.	1 de noviembre de 2023
Nueva funcionalidad	Macie ahora ofrece identificadores de datos gestionados diseñados para detectar los siguientes tipos de datos confidenciales: claves de API de Google Cloud, claves de API de Stripe y números de Aadhaar, números de cuenta permanentes (PAN) y números de identificación del carné de conducir de la India.	25 de septiembre de 2023

Nuevas cuotas	Para ayudarlo a verificar la naturaleza de los datos confidenciales informados por los resultados, hemos aumentado las cuotas de tamaño para recuperar y revelar muestras de datos confidenciales de objetos de Amazon S3. Ahora puede extraer y revelar muestras de objetos S3 cuyo tamaño de almacenamiento supere los 10 MB. Para obtener una lista de las nuevas cuotas, consulte Cuotas de Amazon Macie.	7 de septiembre de 2023
Disponibilidad en las regiones	Macie ya está disponible en la región de Israel (Tel Aviv). Para obtener una lista de Regiones de AWS en las que Macie se encuentra actualmente disponible, consulte puntos de conexión y cupos de Amazon Macie en Referencia general de AWS.	28 de agosto de 2023

Funcionalidad actualizada	Implementamos un nuevo conjunto dinámico de identificadores de datos administrados predeterminados para la detección automatizada de datos confidenciales. El conjunto predeterminado incluye los identificadores de datos administrados que recomendamos para la detección automatizada de datos confidenciales. Está diseñado para detectar categorías y tipos de datos confidenciales comunes y, al mismo tiempo, optimizar los resultados de detección de datos confidenciales automatizados.	2 de agosto de 2023

Funcionalidad actualizada	Para ayudarle a localizar las apariciones de datos confidenciales que Macie menciona en las búsquedas de datos confidenciales y en los resultados de detección de datos confidenciales, cambiamos el límite de caracteres de 20 a 240 para los nombres de los elementos de la ruta JSON en los objetos `Record`. Este cambio afecta a la búsqueda de nuevos datos confidenciales y a los resultados de detección de los contenedores de objetos de Apache Avro, los archivos Apache Parquet, los archivos JSON y los archivos JSON Lines.	24 de julio de 2023
Funcionalidad actualizada	Si es el administrador delegado de Macie en una organización AWS Organizations, ahora puede gestionar Macie para un máximo de 10 000 cuentas de su organización.	30 de junio de 2023

Nueva característica	Ahora puede crear y configurar trabajos de detección de datos confidenciales para utilizar automáticamente el conjunto de identificadores de datos administrados que recomendamos para los trabajos. Este conjunto recomendado de identificadores de datos administrados está diseñado para detectar categorías y tipos comunes de datos confidenciales y optimizar los resultados de su trabajo.	28 de junio de 2023
Política nueva	Hemos añadido una nueva AWS política gestionada, la `AmazonMacieReadOnlyAccess` política. Esta política concede permisos de solo lectura que permiten a una identidad de IAM (entidad principal) extraer todos los recursos, datos y ajustes de Macie de su cuenta.	15 de junio de 2023

Nueva característica	Para ayudarlo a evaluar y monitorear la cobertura automatizada de detección de datos confidenciales de sus datos de Amazon S3, la consola de Macie ahora incluye una página de cobertura de recursos. La página proporciona una vista unificada de las estadísticas de cobertura y los datos de todos sus buckets de S3, incluida una acumulación de problemas de análisis (si los hubiera) que ocurriero n recientemente para cada bucket. Si se produjeran problemas, la página también proporciona una guía para solucionarlos.	15 de mayo de 2023

Nueva característica	Macie se integra con AWS User Notifications, que es una nueva ubicación Servicio de AWS que actúa como ubicación central para tus AWS notificaciones en la. AWS Management ConsoleCon Notificaciones de usuario, puedes configurar reglas y canales de entrega personalizados para generar y enviar notificaciones sobre EventBridge los eventos de Amazon que publica Macie para encontrar políticas y datos confidenciales.	5 de mayo de 2023

Contenido actualizado	Se han actualizado las descripciones de estadísticas y metadatos que Macie proporciona sobre la configuración de cifrado predeterminada para buckets de S3. También se ha actualizado la descripción del Policy:IAMUser/S3BucketEncryptionDisabledresultado de política. Amazon S3 aplica ahora el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) como el nivel básico de cifrado para cada objeto añadido a un bucket nuevo o existente. Para obtener información sobre este cambio en Amazon S3, consulte Configuración del comportamiento predeterminado de cifrado del lado del servidor para buckets de S3 en la Guía del usuario del servicio de almacenamiento simple de Amazon.	27 de febrero de 2023

Nueva funcionalidad	Macie ahora puede generar un tipo adicional de resultado de política para un bucket de S3: `Policy:IAMUser/S3BucketSharedWithCloudFront` . Este tipo de hallazgo indica que se ha modificado la política de un bucket para permitir que el bucket se comparta con una identidad de acceso a CloudFront origen (OAI) de Amazon, un control de acceso a CloudFront origen (OAC) o ambos. Además, los buckets que se comparten con las CloudFront OAI o los OAC ahora se consideran compartidos externamente en las estadísticas y los metadatos que Macie proporciona sobre sus datos de Amazon S3.	24 de febrero de 2023

Nueva funcionalidad	Macie ahora es compatible con la clase de almacenamiento Amazon S3 Glacier Instant Retrieval para el detección de datos confidenciales. Los objetos S3 que utilizan esta clase de almacenamiento ahora son aptos para el análisis cuando Macie realiza la detección automatizada de datos confidenciales o cuando ejecuta trabajos de detección de este tipo de datos. También se consideran objetos clasificables en las estadísticas y los metadatos que Macie proporciona sobre sus datos de Amazon S3.	21 de diciembre de 2022

Nueva característica	Ahora puede configurar Macie para que detecte automáticamente los datos confidenciales de su cuenta u organización. Con la detección automatizada de datos confidenciales, Macie evalúa continuamente sus datos de Amazon S3 y utiliza técnicas de muestreo para identific ar, seleccionar y analizar objetos representativos en sus buckets de S3, inspeccio nando los objetos en busca de datos confidenciales. Podrá evaluar los resultados de los análisis en estadísticas, resultados y otra información que Macie proporcione sobre sus datos de Amazon S3.	28 de noviembre de 2022

Nueva característica	Ahora puede crear y usar listas de permisos para especificar textos y patrones de texto que desea que Macie ignore cuando inspeccione los objetos de Amazon S3 en busca de datos confidenciales. Mediante el uso de listas de permisos, puede definir excepciones de datos confidenciales para sus escenarios o entornos particulares, por ejemplo, los nombres de los representantes públicos de su organización, números de teléfono específicos o datos de muestra que su organización utiliza para las pruebas.	30 de agosto de 2022
Nueva característica	Para verificar la naturaleza de los datos confidenciales que Macie encuentra en los objetos de S3, ahora puede configurar y usar Macie para extraer muestras de datos confidenciales informados por los resultados.	26 de julio de 2022

Funcionalidad actualizada	En la AmazonMacieFullAccess política, actualizamos el Nombre de recurso de Amazon (ARN) del rol vinculado a servicios de Macie (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	30 de junio de 2022
Funcionalidad actualizada	Actualizamos la AmazonMacieServiceRolePolicypolítica , que es la que se adjunta al papel vinculado al servicio Macie (`AWSServiceRoleForAmazonMacie`). La política ya no especifica las acciones y los recursos de Amazon Macie Classic. Amazon Macie Classic se ha descatalogado y ya no está disponible.	20 de mayo de 2022
Nueva funcionalidad	Macie ahora incluye este `OriginType` campo en los hallazgos de datos confidenciales en los que AWS Security Hubpublica. El campo `OriginType` especifica cómo Macie encontró los datos confidenciales que dieron lugar a un resultado.	11 de mayo de 2022

Contenido actualizado	Se aclaró cómo funcionan las configuraciones de palabras clave y distancia máxima de coincidencia para los identificadores de datos personalizados.	22 de abril de 2022
Nueva funcionalidad	Macie ahora proporciona identificadores de datos gestionados que están diseñados para detectar encabezados de autorización básica HTTP, cookies HTTP y tokens web JSON.	21 de abril de 2022
Nuevo contenido	Se añadieron descripciones y definiciones de conceptos y términos clave para Macie.	16 de marzo de 2022
Nueva funcionalidad	Para calcular y mostrar los costos estimados al crear y configurar trabajos de descubrimiento de datos confidenciales, Macie ahora recupera los datos de precios para usted. Cuenta de AWS AWS Billing and Cost ManagementPara respaldar esta funcionalidad, hemos añadido una acción de Administración de costos y facturación a la AmazonMacieFullAccesspolítica.	7 de marzo de 2022

Nueva funcionalidad	Macie ahora incluye este `Sample` campo en las conclusiones que publica. AWS Security Hub El campo `Sample` especifica si un resultado es un resultado de muestra.	24 de febrero de 2022
Nuevo contenido	Se añadió información sobre el uso de Amazon Virtual Private Cloud para establecer una conexión privada entre su VPC y Macie.	19 de enero de 2022
Nueva funcionalidad	Ahora puede usar la consola de Amazon Macie para asignar y administrar etiquetas para identificadores de datos personalizados, reglas de filtrado y supresión de resultados, trabajos de detección de datos confidenciales y, si es el administrador de Macie de una organización, las cuentas de los miembros de su organización. Una etiqueta es un identificador que puede definir y asociar opcionalmente a ciertos tipos de AWS recursos.	12 de enero de 2022
Nuevo contenido	Se añadió información sobre el uso de AWS Identity and Access Management para administrar el acceso a Macie.	20 de diciembre de 2021

Nueva característica	Al crear un identificador de datos personalizado, ahora puede definir la configuración de gravedad para los resultados de datos confidenciales que produce. Con esta configuración, puede especificar la gravedad que desea asignar a un resultado en característica del número de apariciones de texto que coincidan con los criterios de detección del identificador de datos personalizado.	4 de noviembre de 2021
Nueva funcionalidad	Para obtener información sobre los distintos tipos de resultados que proporciona Macie, puede generar ejemplos de resultados. Los resultados de la muestra utilizan datos de ejemplo y valores de marcador de posición para demostrar los tipos de información que Macie podría incluir en cada tipo de resultado.	28 de octubre de 2021
Nueva funcionalidad	Macie ahora incluye este `OwnerAccountId` campo en las conclusiones en las que publica. AWS Security HubEste campo especifica el ID de Cuenta de AWS cuenta del propietario del bucket de S3 afectado.	27 de octubre de 2021

Nuevo contenido	Se añadió información sobre la administración centralizada de varias cuentas de Macie. Puede hacerlo de dos maneras: integrando Macie con Macie AWS Organizations o enviando invitaciones de membresía desde Macie.	13 de octubre de 2021
Nueva funcionalidad	El inventario del bucket de S3 ahora indica si la configuración de permisos de un bucket impide que Macie recupere información sobre el bucket o los objetos del bucket y evalúe y supervise la seguridad y la privacidad de los datos del bucket. Además, actualizamos las referencias AWS KMS keys y las claves administradas por el cliente para reflejar la terminología actual.	5 de octubre de 2021

Nueva funcionalidad	Macie almacena sus resultados de política y datos confidenciales durante 90 días en lugar de 30. Si Macie creó o actualizó un resultado el 31 de agosto de 2021 o después de esa fecha, podrá acceder al resultado durante un máximo de 90 días mediante la consola o la API de Macie. De hecho Regiones de AWS, Macie comenzó a retener las conclusiones durante 90 días a partir del 27 de septiembre de 2021.	1 de octubre de 2021
Nueva característica	Al crear un trabajo de detección de datos confidenciales, ahora puede especificar qué identificadores de datos gestionados desea que utilice el trabajo cuando analice los objetos de S3. Con esta característica, puede personalizar el análisis de un trabajo para que se centre en determinados tipos de datos confidenciales.	17 de septiembre de 2021
Nueva funcionalidad	Los resultados de datos confidenciales ahora proporcionan información adicional para ayudarle a localizar datos confidenciales en archivos JSON y JSON Lines.	6 de julio de 2021

Funcionalidad actualizada	Macie ahora usa el tipo `AwsS3Bucket` de recurso en los hallazgos en los que publica. AWS Security Hub(Macie anteriormente estableció este valor en.) `AWS::S3::Bucket` `AwsS3Bucket` es el valor del tipo de recurso que se utiliza para los buckets S3 en el formato de búsqueda AWS de seguridad (ASFF).	28 de junio de 2021
Nueva característica	Al crear un trabajo de detección de datos confidenciales, ahora puede definir los criterios de tiempo de ejecución que determinan qué buckets de S3 analiza el trabajo. Con esta característica, el alcance del análisis de un trabajo puede adaptarse dinámicamente a los cambios en el inventario de bucket.	15 de mayo de 2021

Nueva funcionalidad	El inventario de bucket de S3 y el panel de resumen ahora proporcionan metadatos de cifrado y estadísticas que indican si las políticas de bucket requieren el cifrado de los nuevos objetos en el servidor. Además, ahora puede realizar actualiza ciones bajo demanda de los metadatos de los objetos para los buckets individuales de su inventario de bucket.	30 de abril de 2021
Nueva característica	Ahora puede usar Amazon CloudWatch Logs para monitorear y analizar los eventos que se producen cuando ejecuta trabajos de descubrimiento de datos confidenciales. Para admitir esta función, hemos añadido las acciones de CloudWatc h Logs a la política AWS gestionada para la función vinculada al servicio de Macie.	14 de abril de 2021
Disponibilidad en las regiones	Macie ya está disponible en la región de AWS Asia Pacífico (Osaka).	5 de abril de 2021
Nueva característica	Ahora puede configurar Macie para que publique los resultados de datos confidenc iales para AWS Security Hub.	22 de marzo de 2021

Nuevo contenido	Se ha añadido información sobre el seguimiento y la previsión de los costos de Macie y sobre la participación en la prueba gratuita.	26 de febrero de 2021
Contenido actualizado	Hemos sustituido el término cuenta maestra por el término cuenta de administrador. Una cuenta de administrador se utiliza para gestionar varias cuentas de forma centralizada.	12 de febrero de 2021
Nueva funcionalidad	Ahora puede refinar el alcance de las tareas de detección de datos confidenciales mediante el uso de prefijos de objetos de S3 en los criterios personalizados de inclusión y exclusión.	2 de febrero de 2021
Contenido actualizado	Macie ahora sigue la taxonomía de tipos de hallazgo del AWS Security Finding Format (ASFF) al publicar las conclusiones de las políticas. AWS Security Hub	28 de enero de 2021
Nuevo contenido	Se añadió información sobre la supervisión de los datos de Amazon S3 y la evaluación de la seguridad y la privacidad de esos datos.	8 de enero de 2021

Disponibilidad en las regiones	Macie ya está disponible en la región de AWS África (Ciudad del Cabo), la región de AWS Europa (Milán) y la región de AWS Oriente Medio (Bahréin).	21 de diciembre de 2020
Nueva funcionalidad	Si su cuenta es una cuenta de administrador de Macie, ahora puede crear y ejecutar trabajos de detección de datos confidenciales que analicen datos para hasta 1000 buckets que abarcan hasta 1000 cuentas en su organización.	25 de noviembre de 2020
Nueva funcionalidad	Su inventario de bucket de S3 ahora indica si ha configurado tareas puntuales o periódicas de detección de datos confidenciales para analizar los datos de un bucket. Si fuese el caso, también proporcionará detalles sobre el trabajo que se ejecutó más recientemente.	23 de noviembre de 2020
Nuevo contenido	Se añadió información sobre el filtrado de los resultados.	12 de noviembre de 2020

Nueva funcionalidad	Los resultados de datos confidenciales ahora proporcionan información adicional para ayudarlo a localizar datos confidenciales en los contenedores de objetos de Apache Avro, los archivos de Apache Parquet y los libros de trabajo de Microsoft Excel.	9 de noviembre de 2020
Nueva característica	Ahora puede usar los resultados de datos confidenciales para localizar apariciones individuales de datos confidenciales en objetos de S3.	22 de octubre de 2020
Nueva característica	Ahora puede pausar y reanudar las tareas de detección de datos confidenciales.	16 de octubre de 2020
Nuevo contenido	Se añadieron detalles sobre el sistema de puntuación de gravedad de los resultados sobre políticas y datos confidenciales.	6 de octubre de 2020
Nuevas características	Ahora puede ver las estadísticas que indican la cantidad de datos que Macie puede analizar en buckets de S3 individuales cuando ejecuta un trabajo de detección de datos confidenciales. Además, ahora puede ver el costo estimado de un trabajo al crearlo.	3 de septiembre de 2020

Nuevo contenido	Se añadió información sobre la configuración, la ejecución y la administración de los trabajos de detección de datos confidenciales.	31 de agosto de 2020
Nueva funcionalidad	Los identificadores de datos gestionados ahora pueden detectar ciertos tipos de información de identificación personal de Brasil.	31 de julio de 2020
Contenido actualizado	Se añadió información sobre la sintaxis admitida para las expresiones regulares en los identificadores de datos personalizados.	30 de julio de 2020
Contenido actualizado	Se añadieron requisitos de palabras clave para los identificadores de datos administrados y se aumentó la cuota para el número de resultados que cada trabajo de detección de datos confidenciales puede generar.	17 de julio de 2020

Nuevo contenido	Se agregó información sobre el uso de Amazon EventBridge y AWS Security Hub para monitorear y procesar los hallazgos. Esto incluye el esquema de EventBridge eventos para las conclusiones y ejemplos de eventos para las conclusiones sobre políticas y datos confidenciales.	22 de junio de 2020
Nuevo contenido	Se añadió información sobre el análisis y la supresión de los resultados.	17 de junio de 2020
Nuevo contenido	Se añadieron instrucciones para configurar Macie de manera que almacene los resultados de detección detallados en un bucket de S3.	2 de junio de 2020
Nuevo contenido	Se añadió información sobre los tipos de datos confidenciales que Macie puede detectar y los requisitos de cifrado para detectar datos confidenciales en los objetos de Amazon S3.	28 de mayo de 2020
Disponibilidad general	Esta es la versión pública inicial de la Guía del usuario de Amazon Macie.	13 de mayo de 2020

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.