aws

Manual do usuário

Amazon Macie

Amazon Macie: Manual do usuário

Table of Contents

O que é o Amazon Macie?

O Amazon Macie é um serviço de segurança de dados que descobre dados sigilosos usando machine learning e correspondência de padrões, fornece visibilidade dos riscos de segurança de dados e permite proteção automatizada contra esses riscos.

Para ajudar você a gerenciar a postura de segurança do conjunto de dados do Amazon Simple Storage Service (Amazon S3) da organização, o Macie fornece um inventário de seus buckets do S3 e os avalia e monitora automaticamente para segurança e controle de acesso. Se o Macie detectar um possível problema com a segurança ou a privacidade dos dados, como um bucket que se torna acessível ao público, ele gerará uma descoberta para você revisar e corrigir conforme necessário.

O Macie também automatiza a descoberta e a emissão de relatórios de dados sigilosos para compreender melhor os dados armazenados pela organização no Amazon S3. Para detectar dados sigilosos, é possível usar critérios e técnicas incorporados que o Macie fornece, critérios personalizados que você define ou uma combinação dos dois. Se o Macie detectar dados sigilosos em um objeto do S3, ele gerará uma descoberta para notificar você sobre os dados sensíveis que o Macie encontrar.

Além das descobertas, o Macie fornece estatísticas e outros dados que oferecem uma visão sobre o procedimento de segurança dos dados do Amazon S3 e sobre onde os dados confidenciais podem residir na propriedade dos dados. As estatísticas e os dados podem orientar suas decisões para realizar investigações mais profundas de buckets e objetos específicos do S3. Você pode revisar e analisar descobertas, estatísticas e outros dados usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode aproveitar a integração do Macie com o Amazon EventBridge e AWS Security Hub para monitorar, processar e corrigir descobertas usando outros serviços, aplicativos e sistemas.

Tópicos

Recursos do Amazon Macie

Aqui estão algumas das principais maneiras pelas quais o Amazon Macie pode ajudá-lo a descobrir, monitorar e proteger seus dados confidenciais no Amazon S3.

Automatize a descoberta de dados sigilosos

Com o Macie, é possível automatizar a descoberta e a emissão de relatórios de dados sigilosos de duas maneiras: configurar o Macie para realizar descoberta automática de dados sigilosos e criar e executar trabalhos de descoberta de dados sigilosos. Se o detectar dados confidenciais em um objeto do S3, ele também criará uma descoberta de dados confidenciais para você. A descoberta fornece um relatório detalhado dos dados confidenciais que o Macie encontrou.

A descoberta automatizada de dados confidenciais fornece ampla visibilidade sobre onde os dados confidenciais podem residir em seu patrimônio de dados do Amazon S3. Com essa opção, o Macie avalia continuamente seu inventário de buckets do S3 e usa técnicas de amostragem para identificar e selecionar objetos representativos do S3 em seus buckets. Em seguida, o Macie recupera e analisa os objetos selecionados, inspecionando-os em busca de dados confidenciais.

Trabalhos confidenciais de descoberta de dados fornecem uma análise mais profunda e direcionada. Com essa opção, você define a amplitude e a profundidade da análise — os buckets do S3 a serem analisados, a profundidade da amostragem e os critérios personalizados que derivam das propriedades dos objetos do S3. Você também pode configurar um trabalho para ser executado somente uma vez para análise e avaliação sob demanda, ou de forma recorrente para análise, avaliação e monitoramento periódicos.

Ambas as opções podem ajudar você a criar e manter uma visão abrangente dos dados armazenados pela organização no Amazon S3 e dos riscos de segurança ou conformidade desses dados.

Descubra uma variedade de tipos de dados confidenciais

Para descobrir dados confidenciais com o Macie, é possível usar técnicas e critérios incorporados, como machine learning e comparação de padrões, para analisar objetos nos buckets do S3. Esses critérios e técnicas, denominados identificadores de dados gerenciados, podem detectar uma lista extensa e crescente de tipos de dados sigilosos para muitos países e regiões, inclusive vários tipos de informações de identificação pessoal (PII), informações financeiras e dados de credenciais.

Você também pode usar identificadores de dados personalizados. Um identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais — uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados. Com esse tipo de identificador, é possível detectar dados confidenciais que refletem determinados cenários, propriedade intelectual ou dados proprietários. Você pode complementar os identificadores de dados gerenciados fornecidos pelo Macie.

Para ajustar as análises, você também pode usar listas de permissões. As listas de permissões definem textos e padrões de texto específicos que você deseja que o Macie ignore nos objetos do S3. Normalmente, essas são exceções de dados confidenciais para seus cenários ou ambientes específicos; por exemplo, os nomes dos representantes públicos da sua organização, números de telefone públicos da sua organização ou dados de amostra que sua organização usa para testes.

Avalie e monitore dados para segurança e controle de acesso

Quando você ativa o Macie, o Macie gera automaticamente e começa a manter um inventário completo de seus buckets do S3. O Macie também começa a avaliar e monitorar os buckets em relação à segurança e ao controle de acesso. Se o Macie detectar um possível problema com a segurança ou a privacidade de um bucket, ele criará uma descoberta de política para você.

Além de descobertas específicas, um painel fornece uma visão geral das estatísticas agregadas dos seus dados do Amazon S3. Isso inclui estatísticas das principais métricas, como quantos dos seus buckets estão acessíveis ao público ou são compartilhados com outras Contas da AWS. Você pode detalhar cada estatística para analisar os dados de suporte.

O Macie também fornece informações e estatísticas detalhadas para buckets do S3 individuais em seu inventário. Os dados incluem detalhamentos das configurações de acesso público e criptografia de um bucket e o tamanho e o número de objetos que o Macie pode analisar para detectar dados confidenciais no bucket. Você pode navegar pelo inventário ou classificar e filtrar o inventário por determinados campos. Quando você escolhe um bucket, um painel exibe os detalhes do bucket.

Revise e analise as descobertas

No Macie, uma descoberta é um relatório detalhado de dados sigilosos que Macie detecta em um objeto do S3 ou de um possível problema com a segurança ou a privacidade de um bucket do S3. Cada descoberta fornece uma classificação de gravidade, informações sobre o recurso afetado e detalhes adicionais, como quando e como Macie encontrou o problema.

Para revisar, analisar e gerenciar descobertas, você pode usar as páginas de descobertas no console do Amazon Macie. Essas páginas listam suas descobertas e fornecem os detalhes de descobertas individuais. Elas também oferecem várias opções para agrupar, filtrar, classificar e suprimir descobertas. Também é possível usar a API do Amazon Macie para consultar, recuperar e suprimir descobertas. Se você usa a API, pode passar os dados para outro aplicativo, serviço ou sistema para uma análise mais profunda, armazenamento de longo prazo ou geração de relatórios.

Monitore e processe as descobertas com outros serviços e sistemas

Para oferecer suporte à integração com outros serviços e sistemas, o Macie publica descobertas no Amazon EventBridge como eventos de descoberta. O EventBridge é um serviço de barramento de eventos com tecnologia sem servidor que pode encaminhar dados de descobertas para destinos como funções AWS Lambda e tópicos do Amazon Simple Notification Service (Amazon SNS). Com o EventBridge, você pode monitorar e processar descobertas quase em tempo real como parte de seus fluxos de trabalho de segurança e conformidade existentes.

Você pode configurar o Macie para também publicar descobertas em arquivos para oAWS Security Hub. O Security Hub é um serviço que fornece uma visão abrangente da sua postura de segurança em todo o seu ambiente AWS e ajuda a verificar seu ambiente em relação aos padrões e práticas recomendadas do setor de segurança. Com o Security Hub, é possível monitorar e processar com mais facilidade suas descobertas como parte de uma análise mais ampla da postura de segurança da organização na AWS. Você também pode agregar descobertas de várias Regiões da AWS e monitorar e processar dados de descobertas agregadas de uma única região.

Gerencie centralmente várias contas Macie

Se o seu ambiente AWS tiver várias contas, você poderá gerenciar centralmente o Macie para contas no seu ambiente. Você pode fazer isso de duas maneiras: integrando o Macie com AWS Organizations ou enviando e aceitando convites de adesão no Macie.

Em uma configuração de várias contas, um administrador designado do Macie pode executar determinadas tarefas e acessar determinadas configurações, dados e recursos do Macie para contas que são membros da mesma organização. As tarefas incluem revisar as informações sobre os buckets do S3 que pertencem às contas dos membros, analisar as descobertas das políticas desses buckets e inspecionar os buckets em busca de dados confidenciais. Se as contas estiverem associadas por meio de AWS Organizations, o administrador do Macie também poderá habilitar o Macie para contas de membros na organização.

Desenvolva e gerencie recursos de forma programática

Além do console do Amazon Macie, você pode interagir com o Macie usando a API do Amazon Macie. A API do Amazon Macie oferece acesso abrangente e programático às configurações, dados e recursos da sua conta Macie.

Para interagir com o Macie programaticamente, você pode enviar solicitações HTTPS diretamente para o Macie ou usar uma versão atual de uma ferramenta de linha de comando da AWS ou de um SDK da AWS. A AWS fornece ferramentas e SDKs que consistem em bibliotecas e códigos de exemplo para várias linguagens e plataformas, como PowerShell, Java, Go, Python, C++ e .NET.

Acessando o Amazon Macie

O Amazon Macie está disponível na maioria das Regiões da AWS. Para obter uma lista de regiões onde o Macie está disponível atualmente, consulte Endpoints e cotas do Amazon Macie no Referência geral da AWS. Para obter informações sobre como gerenciar as Regiões da AWS em sua Conta da AWS, consulte Especificação de qual Regiões da AWS sua conta pode usar no Guia de referência do AWS Account Management.

Em cada região, você pode trabalhar com o Macie de qualquer uma das seguintes maneiras.

AWS Management Console

O AWS Management Console é uma interface baseada em navegador que você pode usar para criar e gerenciar recursos da AWS. Como parte desse console, o console Amazon Macie fornece acesso à sua conta, dados e recursos do Macie. Você pode realizar qualquer tarefa do Macie usando o console do Macie: revisar estatísticas e outras informações sobre seus buckets do S3, criar e executar trabalhos confidenciais de descoberta de dados, revisar e analisar descobertas e muito mais.

ferramentas de linha de comando da AWS

Com ferramentas de linha de comando da AWS, você pode emitir comandos na linha de comando do seu sistema para executar tarefas do Macie e tarefas da AWS. Usar a linha de comando pode ser mais rápido e mais conveniente do que usar o console. As ferramentas da linha de comando também são úteis se você quiser criar scripts que realizem tarefas da .

A AWS fornece dois conjuntos de ferramentas de linha de comando: a AWS Command Line Interface (AWS CLI) e o AWS Tools for PowerShell. Para obter informações sobre a instalação

e o uso da AWS CLI, consulte o Guia do usuário da AWS Command Line Interface. Para obter informações sobre a instalação e o uso do Tools for PowerShell, consulte o Guia do usuário do AWS Tools for PowerShell.

AWS SDKs

O AWS fornece SDKs que consistem em bibliotecas e códigos de amostra para diversas linguagens de programação e plataformas — por exemplo, Java, Go, Python, C++ e .NET. Os SDKs fornecem acesso conveniente e programático ao Macie e outros Serviços da AWS. Eles também lidam com tarefas como assinar solicitações criptograficamente, gerenciar erros e repetir solicitações automaticamente. Para obter informações sobre como instalar e usar os SDKs da AWS, consulte Ferramentas para criar na AWS.

API REST do Amazon Macie

A API REST do Amazon Macie oferece acesso abrangente e programático à sua conta, dados e recursos do Macie. Com esta API, você pode enviar solicitações HTTPS diretamente para o Macie. No entanto, ao contrário das ferramentas de linha de comando e SDK da AWS, o uso dessa API exige que o aplicativo trate detalhes de baixo nível, como gerar um hash para assinar uma solicitação. Para obter informações sobre essa API, consulte a Referência da API do Amazon Macie.

Definição de preços do Amazon Macie

Assim como em outros produtos da AWS, não há contratos nem compromissos mínimos para usar o Amazon Macie.

Os preços do Macie são baseados em várias dimensões: avaliação e monitoramento de buckets do S3 para segurança e controle de acesso, monitoramento de objetos do S3 para descoberta automatizada de dados confidenciais e análise de objetos do S3 para descobrir e relatar dados confidenciais nos objetos. Para obter mais informações, consulte Definição de preços do Amazon Macie.

Para ajudar você a entender e prever o custo do uso do Macie, o Macie fornece custos estimados de uso da sua conta. Você pode revisar essas estimativas no console do Amazon Macie e acessá-las com a API do Amazon Macie. Dependendo de como você usa o serviço, você pode incorrer em custos adicionais ao usar outros Serviços da AWS em combinação com determinados atributos do Macie, como recuperar dados do bucket do Amazon S3 e usar o gerenciamento do cliente para descriptografar objetos AWS KMS keys para análise.

Ao ativar o Macie pela primeira vez, sua Conta da AWS será automaticamente inscrita na avaliação gratuita de 30 dias do Macie. Isso inclui contas individuais habilitadas como parte de uma organização no AWS Organizations. Durante o teste gratuito, não há cobrança pelo uso do Macie na Região da AWS aplicável para avaliar e monitorar seus buckets do S3 para segurança e controle de acesso. Dependendo das configurações da sua conta, o teste gratuito também pode incluir a descoberta automática de dados confidenciais para seus dados do Amazon S3. O teste gratuito não inclui executar trabalhos confidenciais de descoberta de dados confidenciais para detectar e relatar dados confidenciais nos objetos do S3.

Para ajudá-lo a entender e prever o custo do uso do Macie após o término do teste gratuito, o Macie fornece custos de uso estimados com base no uso do Macie durante o teste. Seus dados de uso também indicam o tempo que resta até o término do teste gratuito. Você pode revisar esses dados no console do Amazon Macie e acessá-los com a API do Amazon Macie.

Serviços relacionados

Para proteger ainda mais seus dados, workloads e aplicativos na AWS, considere usar o seguinte Serviços da AWS em combinação com o Amazon Macie.

AWS Security Hub

O AWS Security Hub oferece uma visão abrangente do estado de segurança de recursos da AWS e ajuda a verificar seu ambiente AWS em relação aos padrões e práticas recomendadas do setor de segurança. Ele faz isso em parte consumindo, agregando, organizando e priorizando suas descobertas de segurança de vários produtos de Serviços da AWS (incluindo Macie) e produtos AWS Partner Network (APN) compatíveis. O Security Hub ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade em seu ambiente AWS.

Para saber mais sobre o Security Hub, consulte o Guia do usuário da AWS Security Hub. Para saber como usar o Macie e o Security Hub juntos, consulteIntegração do Amazon Macie com o AWS Security Hub.

Amazon GuardDuty

O Amazon GuardDuty é um serviço de monitoramento de segurança que analisa e processa determinados tipos de logs AWS, como logs de eventos de dados do AWS CloudTrail para o Amazon S3 e logs de eventos de gerenciamento do CloudTrail. Ele usa feeds de inteligência contra ameaças, como listas de endereços IP e domínios mal-intencionados, e machine learning

para identificar atividades inesperadas, mal-intencionadas e possivelmente não autorizadas no seu ambiente da AWS.

Para saber mais sobre o GuardDuty, consulte o Manual do usuário do Amazon GuardDuty.

Para saber mais sobre serviços de segurança adicionais da AWS, consulte Segurança, identidade e conformidade na AWS.

Conceitos básicos do Amazon Macie

Este tutorial fornece uma introdução ao Amazon Macie. Você aprenderá como habilitar o Macie para o seu Conta da AWS. Você também aprenderá a avaliar a postura de segurança do seu Amazon Simple Storage Service (Amazon S3) e definir as principais configurações do Macie para descobrir e relatar dados confidenciais em seus buckets no S3.

Tarefas

- Antes de começar
- Etapa 1: habilitar o Amazon Macie
- Etapa 2: Configurar um repositório de resultados de descoberta de dados confidenciais
- Etapa 3: explorar exemplos de descobertas
- Etapa 4: criar um trabalho para descobrir dados confidenciais
- Etapa 5: Revise suas descobertas

Antes de começar

Quando você se cadastra na Amazon Web Services, sua conta (AWS) é cadastrada automaticamente em todos os produtos da Serviços da AWS, incluindo o Amazon Macie. Porém, para usar o Macie, é necessário configurar permissões que permitam o acesso às operações de API e ao console do Amazon Macie. Você ou seu administrador AWS pode fazer isso usando AWS Identity and Access Management (IAM) para anexar a política AWS gerenciada chamada `AmazonMacieFullAccess` à sua identidade do IAM. Para saber mais, consulte AWS políticas gerenciadas para o Amazon Macie.

Etapa 1: habilitar o Amazon Macie

Depois de configurar as permissões necessárias, você pode habilitar o Amazon Macie para seu Conta da AWS. Siga estas etapas para habilitar o Macie para sua conta.

Para habilitar o Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor Região da AWS no canto superior direito da página, selecione a região na qual você deseja habilitar e usar o Macie.

3. Na página do Amazon Macie, selecione Comece a usar.
4. (Opcional) Quando você ativa o Macie, o Macie cria automaticamente uma função vinculada ao serviço que concede ao Macie as permissões necessárias para chamar outras pessoas Serviços da AWS e monitorar AWS recursos em seu nome. Para revisar a política de permissões para essa função, selecione Visualizar permissões da função no console. Para saber mais sobre essa função, consulte Funções vinculadas ao serviço do Amazon Macie.
5. Escolha Enable Macie (Habilitar Macie).

Em minutos, o Macie gera automaticamente e começa a manter um inventário completo de seus buckets no S3 na região atual. O Macie também começa a avaliar e monitorar os buckets em relação à segurança e ao controle de acesso. Para saber mais, consulte Como o Macie monitora a segurança de dados do Amazon S3.

Dependendo das configurações da sua conta, o Macie também começa a realizar a descoberta automática de dados confidenciais para seus buckets no S3. Macie começa a identificar, selecionar e revisar continuamente objetos representativos do S3 em seus buckets, inspecionando os objetos em busca de dados confidenciais. À medida que as análises progridem, o Macie fornece estatísticas e outros resultados que você pode revisar, normalmente dentro de 48 horas após ativar o Macie para sua conta. Você pode personalizar as análises definindo configurações automatizadas de descoberta de dados confidenciais para sua conta. Para saber mais, consulte Como funciona a descoberta automatizada de dados confidenciais.

Para revisar estatísticas agregadas, selecione Resumo no painel de navegação no console. Para revisar detalhes sobre buckets no S3 individuais em seu inventário, selecione buckets no S3 no painel de navegação. Para exibir os detalhes de um bucket, selecione o bucket. O painel de detalhes exibe estatísticas e outras informações que fornecem informações sobre a segurança, a privacidade e a confidencialidade dos dados do bucket. Para saber mais sobre esses detalhes, consulte Analisar seu inventário de buckets do S3.

Etapa 2: Configurar um repositório de resultados de descoberta de dados confidenciais

Com o Amazon Macie, você pode descobrir dados confidenciais em seus buckets no S3 de duas maneiras: configurando o Macie para realizar a descoberta automática de dados confidenciais e executando trabalhos de descoberta de dados confidenciais. Um trabalho de descoberta de dados

confidenciais é um trabalho que você cria para revisar objetos em buckets no S3 para determinar se os objetos contêm dados confidenciais.

O Macie cria um registro para cada objeto do S3 que ele analisa quando você executa trabalhos de descoberta de dados confidenciais ou realiza a descoberta automatizada de dados confidenciais. Esses registros, chamados de resultados confidenciais da descoberta de dados, registram detalhes sobre a análise de objetos individuais. O Macie também cria resultados confidenciais de descoberta de dados para objetos que ele não pode revisar devido a erros ou problemas. Os resultados confidenciais da descoberta de dados fornecem registros de análise que podem ser úteis para auditorias ou investigações de privacidade e proteção de dados.

O Macie armazena seus resultados confidenciais de descoberta de dados por apenas 90 dias. Para acessar os resultados e permitir seu armazenamento e retenção a longo prazo, configure o Macie para armazenar os resultados em um bucket do S3. Você deve fazer isso dentro de 30 dias após ativar o Macie. Depois de fazer isso, o bucket pode servir como um repositório definitivo e de longo prazo para todos os seus resultados confidenciais de descoberta de dados.

Para saber como configurar esse repositório, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Etapa 3: explorar exemplos de descobertas

No Amazon Macie, uma descoberta é um relatório detalhado de uma possível violação de política que o Macie detecta em um bucket no S3 ou em dados confidenciais que o Macie detecta em um objeto do S3. Macie fornece duas categorias de descobertas: descobertas de políticas e descobertas de dados confidenciais. O Macie cria uma descoberta de política quando as políticas ou configurações de um bucket são alteradas de forma a reduzir a segurança ou a privacidade do bucket e dos objetos do bucket. O Macie cria uma descoberta de dados confidenciais ao detectar dados sigilosos em um objeto do S3. Dentro de cada categoria, há vários tipos de descobertas.

Para explorar e aprender sobre as diferentes categorias e tipos de descobertas que o Macie fornece, opcionalmente, crie e revise amostras de descobertas. As descobertas de amostra usam dados de exemplo e valores de espaço reservado para demonstrar os tipos de informações que o Macie pode incluir em cada tipo de descoberta.

Siga estas etapas para criar e revisar amostras de descobertas.

Para criar e revisar amostras de descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. No painel de navegação, selecione Settings (configurações).
3. Em Sample findings, escolha Generate sample findings. O Macie gera uma amostra de descoberta para cada tipo de descoberta que o Macie suporta.
4. No painel de navegação, selecione Descobertas. A página Descobertas exibe as descobertas de sua conta na Região da AWS atual. Isso inclui as descobertas de amostra que você criou na etapa anterior.
5. Na página Descobertas, localize descobertas cujo tipo começa com [AMOSTRA].
6. Para revisar os detalhes de uma descoberta de amostra específica, selecione a descoberta. O painel detalhes exibirá os detalhes da descoberta.

Para saber mais sobre cada tipo de descoberta, consulte Tipos de descobertas. Para saber mais sobre como criar e revisar exemplos de descobertas, consulte Como trabalhar com amostras de descobertas.

Etapa 4: criar um trabalho para descobrir dados confidenciais

Para descobrir e relatar dados confidenciais em buckets no S3, você pode executar trabalhos de descoberta de dados confidenciais. Um trabalho de descoberta de dados confidenciais é um trabalho que você cria para revisar objetos em buckets no S3 para determinar se os objetos contêm dados confidenciais. Ao contrário da descoberta automatizada de dados confidenciais, você define a amplitude e a profundidade da análise. Você também especifica com que frequência executar um trabalho — uma vez ou periodicamente de forma programada.

Siga estas etapas para criar um trabalho que seja executado uma vez, imediatamente após sua criação, e use as configurações padrão. Para saber como criar um trabalho que é executado periodicamente ou usa configurações personalizadas, consulte Criar um trabalho de descoberta de dados confidenciais.

Para criar um trabalho de descoberta de dados confidenciais

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Escolha Create job (Criar trabalho).
4. Para a etapa Escolher buckets do S3, selecione Selecionar buckets específicos. Em seguida, na tabela, marque a caixa de seleção para cada bucket no S3 que você deseja que o trabalho revise.

A tabela fornece um inventário completo dos seus buckets no S3 atualmente. Região da AWS Para encontrar buckets específicos com mais facilidade, insira critérios de filtro na caixa de filtros acima da tabela. Você também pode classificar a tabela escolhendo um título de coluna na tabela.

5. Ao terminar de selecionar os buckets, selecione Avançar.
6. Para a etapa Revisar buckets no S3, revise e verifique suas seleções de bucket e, em seguida, selecione Avançar.
7. Para a etapa Refinar o escopo, selecione Trabalho único e, em seguida, selecione Avançar.
8. Para a etapa Selecionar identificadores de dados gerenciados, selecione Recomendado. Opcionalmente, revise a tabela de identificadores de dados gerenciados que recomendamos para trabalhos e selecione Avançar.

   Um identificador de dados gerenciados é um conjunto de critérios e técnicas integrados projetados para detectar um tipo específico de dados confidenciais – por exemplo, números de cartão de crédito, AWS chaves de acesso secretas ou números de passaporte de um determinado país ou região. Para saber mais, consulte Usar identificadores de dados gerenciados.
9. Para a etapa Selecionar identificadores de dados personalizados, selecione Avançar.

   Um identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais — uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados. Para saber mais, consulte Criar identificadores de dados personalizados.
10. Para a etapa Selecionar listas de permissões, selecione Avançar.

    No Macie, uma lista de permissões especifica um texto ou um padrão de texto que você deseja que o Macie ignore ao inspecionar objetos do S3 em busca de dados confidenciais. Normalmente, essas são exceções de dados confidenciais para cenários ou ambientes específicos. Para saber mais, consulte Como definir exceções de dados sigilosos com listas de permissões.
11. Para a etapa Inserir configurações gerais, insira um nome e, opcionalmente, uma descrição do trabalho. Em seguida, escolha Next (Próximo).
12. Para a etapa Revisar e criar, revise as definições de configuração do trabalho e verifique se estão corretas.

Também é possível revisar o custo total estimado (em USD) da execução do trabalho. A estimativa pode ajudá-lo a determinar se as configurações da tarefa devem ser ajustadas antes de salvá-la. Para saber mais, consulte Prever o custo de um trabalho de descoberta de dados confidenciais.

13. Ao terminar de revisar e verificar as configurações do trabalho, selecione Enviar.

Macie imediatamente começa a executar o trabalho. Para saber como monitorar o trabalho, consulte Verificação do status de trabalhos confidenciais de descoberta de dados.

Etapa 5: Revise suas descobertas

O Amazon Macie monitora automaticamente os buckets no S3 quanto à segurança e ao controle de acesso e cria descobertas de políticas para relatar possíveis problemas com a segurança ou a privacidade dos buckets. Se você criar e executar um trabalho de descoberta de dados confidenciais ou configurar o Macie para realizar a descoberta automatizada de dados confidenciais, o Macie também cria descobertas de dados confidenciais para relatar dados confidenciais detectados em objetos do S3. Para saber mais sobre as descobertas, consulte Analisando descobertas.

Siga estas etapas para revisar suas descobertas.

Para visualizar descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas. A página Descobertas exibe as descobertas de sua conta na Região da AWS atual.
3. (Opcional) Para filtrar as descobertas por critérios específicos, insira os critérios na caixa de filtro acima da tabela.
4. Para visualizar os detalhes de uma descoberta, escolha descoberta. O painel de detalhes exibe os detalhes da descoberta.

Para saber mais, inclusive como agrupar e filtrar descobertas, consulte Analisar descobertas.

Conceitos e terminologia do Amazon Macie

No Amazon Macie, nos baseamos em conceitos e AWSterminologias comuns e usamos esses termos adicionais.

conta

Uma Conta da AWS padrão que contém os seus recursos AWS e as identidades que podem acessar esses recursos.

Para usar o Macie, você faz login em AWS com suas credenciais Conta da AWS, seleciona a Região da AWS em que deseja usar o Macie e, em seguida, habilita o Macie para a sua Conta da AWS naquela região. Para obter mais informações, consulte Conceitos básicos do Amazon Macie.

Existem três tipos de contas no Macie:

- Conta de administrador – Esse tipo de conta gerencia as contas Macie de uma organização. Uma organização é um conjunto de contas Macie que são associadas entre si e gerenciadas centralmente como um grupo de contas relacionadas em uma Região da AWS específica.
- Conta de membro – Esse tipo de conta é associado e gerenciado pela conta de administrador do Macie de uma organização.
- Conta autônoma – Esse tipo de conta não é uma conta de administrador nem uma conta de membro. Ela não faz parte de uma organização.

Você pode adicionar contas do Macie a uma organização de duas maneiras: integrando o Macie com AWS Organizations ou enviando e aceitando convites de associação do Macie. Para obter mais informações, consulte Gerenciar várias contas da .

conta de administrador

No Macie, uma conta que gerencia as contas Macie de uma organização. Uma organização é um conjunto de contas Macie que são associadas entre si e gerenciadas centralmente como um grupo de contas relacionadas em uma Região da AWS específica.

Os usuários de uma conta de administrador do Macie têm acesso aos dados de inventário do Amazon Simple Storage Service (Amazon S3), às descobertas de políticas e a determinadas

configurações e recursos do Macie para todas as contas em sua organização. Eles também podem fazer a descoberta automatizada de dados sigilosos e executar trabalhos de descoberta de dados sigilosos para detectar dados sigilosos nos buckets do S3 de propriedade das contas. Dependendo de como uma conta é designada como conta de administrador, eles também podem realizar tarefas adicionais para outras contas em sua organização.

Para obter mais informações, consulte Gerenciar várias contas da .

lista de permissões

No Macie, uma lista de permissões define um texto específico ou um padrão de texto que o Macie deverá ignorar ao inspecionar objetos S3 em busca de dados sigilosos.

Você pode criar dois tipos de listas de permissões no Macie: um arquivo de texto sem formatação que liste palavras específicas e outros tipos de sequências de caracteres a serem ignoradas ou uma expressão regular (regex) que defina um padrão de texto a ser ignorado. Se um objeto contiver um texto que corresponda a uma entrada ou padrão em uma lista de permissões, o Macie não reportará o texto em descobertas de dados sigilosos, estatísticas e outros tipos de resultados, mesmo que o texto corresponda aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizado.

Para obter mais informações, consulte Como definir exceções de dados sigilosos com listas de permissões.

descoberta automatizada de dados sigilosos

Uma série de atividades de análise automatizada que o Macie executa continuamente para identificar e selecionar objetos representativos dos buckets do S3 e inspecionar os objetos selecionados em busca de dados sigilosos.

À medida que as análises progridem, o Macie produz registros dos dados sigilosos que encontra (descobertas de dados sigilosos) e da análise que realiza (resultados de descoberta de dados sigilosos). O Macie também atualiza estatísticas e outras informações que fornece sobre os dados do Amazon S3.

Para obter mais informações, consulte Realizando a descoberta automatizada de dados confidenciais.

Formato de descoberta de segurança da AWS (ASFF)

Um formato JSON padronizado para o conteúdo das descobertas publicadas ou geradas pelo AWS Security Hub. O ASFF inclui detalhes sobre a origem de um problema de segurança, os recursos afetados e o status atual de uma descoberta.

Para obter mais informações sobre ASFF, consulte AWS Formato de descoberta de segurança (Security Finding Format ASFF) no Manual do usuário do AWS Security Hub. Para obter informações sobre a publicação das descobertas do Macie no Security Hub, consulte Integração do Amazon Macie com o AWS Security Hub.

bytes ou tamanho classificáveis

Nas estatísticas do bucket do S3 que o Macie fornece, o tamanho total do armazenamento de todos os objetos classificáveis em um bucket do S3.

Se o controle de versionamento estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto classificável no bucket. Se um objeto for um arquivo compactado, esse valor não refletirá o tamanho real do conteúdo do arquivo depois que o arquivo for descompactado.

Para obter mais informações, consulte Analisar seu inventário de buckets do S3 e Avaliando sua postura de segurança no Amazon S3.

objeto classificável

Um objeto S3 que o Macie pode analisar para detectar dados sigilosos.

Ao calcular as estatísticas do bucket do S3, o Macie determina que um objeto é classificável com base na classe de armazenamento e na extensão do nome do arquivo do objeto. Nesses dados, um objeto é classificável se usar uma classe de armazenamento do Amazon S3 compatível e tiver uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível.

Para obter mais informações, consulte Analisar seu inventário de buckets do S3 e Avaliando sua postura de segurança no Amazon S3.

Para a descoberta de dados sigilosos, o Macie determina que um objeto é classificável com base na classe de armazenamento, na extensão do nome do arquivo e no conteúdo do objeto. Nesses dados, um objeto é classificável se: usar uma classe de armazenamento do Amazon S3 compatível e tiver uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível.

Para obter mais informações, consulte Descobrir dados confidenciais e Custos de previsão e monitoramento.

identificador de dados personalizado

Um conjunto de critérios que você define para detectar dados sigilosos.

Os critérios consistem em uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados. As sequências de caracteres podem ser:

- Palavras-chave, que são palavras ou frases que devem estar na proximidade do texto que correspondente ao regex, ou
- Palavras a ignorar, que são palavras ou frases a serem excluídas dos resultados.

Além dos critérios de detecção, você pode definir configurações de severidade personalizadas para as descobertas de dados sigilosos que um identificador de dados personalizado produz.

Para obter mais informações, consulte Criar identificadores de dados personalizados.

regra de filtros

Um conjunto de critérios de filtro baseados em atributos que você cria e salva para analisar descobertas no console do Amazon Macie. As regras de filtro podem ajudá-lo a realizar uma análise consistente de descobertas com características específicas, como todas as descobertas de alta severidade que relatam um tipo específico de dados sigilosos.

Para obter mais informações, consulte Como criar e gerenciar regras de filtro para descobertas.

descoberta

Um relatório detalhado de dados sigilosos que Macie encontrou em um objeto do S3 ou de um possível problema com a segurança ou a privacidade de um bucket do S3. Cada descoberta fornece detalhes como uma classificação de gravidade, informações sobre o recurso afetado e quando o Macie encontrou os dados ou o problema.

O Macie gera duas categorias de descobertas: descobertas de dados sigilosos, para dados sigilosos que o Macie detecta em objetos do S3, e descobertas de políticas, para possíveis problemas que o

Macie detecta com as configurações de segurança e controle de acesso dos buckets do S3. Dentro de cada categoria, há vários tipos de descobertas.

Para obter mais informações, consulte Tipos de descobertas do Amazon Macie.

descoberta de evento

Um evento do Amazon EventBridge que contém os detalhes de uma descoberta de dados sigilosos ou descoberta de política.

O Macie publica automaticamente descobertas de dados sigilosos e descobertas de políticas no Amazon EventBridge como eventos. Um evento é um objeto JSON que está em conformidade com o esquema do EventBridge para eventos da AWS. Você pode usar esses eventos para monitorar, processar e agir de acordo com as descobertas usando outros aplicativos, serviços e sistemas.

Para obter mais informações, consulte Integração do Amazon Macie com o Amazon Eventbridge e Esquema de eventos do Amazon EventBridge para descobertas do Amazon Macie.

trabalho

Consulte o trabalho de descoberta de dados sigilosos.

identificadores de dados gerenciados

Um conjunto de técnicas e critérios incorporados projetados para detectar um tipo específico de dados sigilosos. Exemplos de dados sigilosos incluem números de cartão de crédito, chaves de acesso secretas AWS ou números de passaporte para um determinado país ou região. Esses identificadores podem detectar uma lista extensa e crescente de tipos de dados sigilosos para muitos países e regiões.

Para obter mais informações, consulte Usar identificadores de dados gerenciados.

conta-membro

Uma conta Macie gerenciada pela conta de administrador designada da Macie para uma organização. Uma organização é um conjunto de contas Macie que são associadas entre si e gerenciadas centralmente como um grupo de contas relacionadas em uma Região da AWS específica.

Uma conta pode se tornar uma conta-membro de duas maneiras: integrando o Macie à organização da conta AWS Organizations ou aceitando um convite de membro do Macie.

Se você tiver uma conta de membro, seu administrador do Macie tem acesso aos dados de inventário Amazon S3, às descobertas de políticas e a determinadas configurações e recursos do Macie para a sua conta. O seu administrador também pode realizar a descoberta automatizada de dados sigilosos e executar trabalhos de descoberta de dados sigilosos para detectar dados sigilosos em seus buckets do S3. Eles também podem realizar tarefas adicionais em sua conta, dependendo de como a sua conta se tornou uma conta-membro.

Para obter mais informações, consulte Gerenciar várias contas da .

organização

Um conjunto de contas Macie que são associadas entre si e gerenciadas centralmente como um grupo de contas relacionadas em uma Região da AWS específica.

Cada organização consiste em uma conta de administrador designada do Macie e uma ou mais contas-membro associadas. A conta de administrador pode acessar determinadas configurações, dados e recursos do Macie para contas-membro. Você pode criar uma organização de duas maneiras: integrando o Macie com AWS Organizations ou enviando e aceitando convites de associação no Macie.

Para obter mais informações, consulte Gerenciar várias contas da .

descobertas de políticas

Um relatório detalhado de uma violação de política em potencial ou problema com as configurações de segurança e controle de acesso de um bucket do S3. Os detalhes incluem uma classificação de gravidade, informações sobre o recurso afetado e quando o Macie encontrou o problema.

O Macie cria uma descoberta de política quando as políticas ou configurações de um bucket são alteradas de forma a reduzir a segurança ou a privacidade do bucket e dos objetos do bucket. O Macie gera essas descobertas como parte de suas atividades contínuas de monitoramento dos dados do seu Amazon S3. O Macie pode gerar vários tipos de descobertas de políticas.

Para obter mais informações, consulte Tipos de descobertas do Amazon Macie e Como monitorar a segurança e a privacidade dos dados.

exemplo de descoberta

Uma descoberta que usa dados de exemplo e valores de marcador para demonstrar os tipos de informações que uma descoberta pode conter.

Para obter mais informações, consulte Como trabalhar com amostras de descobertas.

descoberta de dados sigilosos

Um relatório detalhado dos dados sigilosos que o Macie encontrou em um objeto do S3. Os detalhes incluem uma classificação de gravidade, informações sobre o recurso afetado, o tipo e o número de ocorrências dos dados sigilosos encontrados pelo Macie e quando o Macie encontrou os dados sigilosos.

O Macie gera descobertas de dados sigilosos se detectar dados sigilosos em objetos do S3 que ele analisa quando você executa trabalhos de descoberta de dados sigilosos ou realiza uma descoberta automatizada de dados sigilosos. O Macie pode gerar vários tipos de descobertas de dados sigilosos.

Para obter mais informações, consulte Tipos de descobertas do Amazon Macie e Descobrir dados confidenciais.

trabalho de descoberta de dados sigilosos

Também conhecida como trabalho, uma série de tarefas automatizadas de processamento e análise que o Macie executa para detectar e relatar dados sigilosos em objetos do S3. Ao criar um trabalho, especifique com que frequência deseja que o trabalho seja executado e defina o escopo e a natureza da análise do trabalho.

Quando um trabalho é executado, o Macie produz registros dos dados sigilosos encontrados (descobertas de dados sigilosos) e da análise que ele executa (resultados da descoberta de dados sigilosos). O Macie também publica dados de logs no Amazon CloudWatch Logs.

Para obter mais informações, consulte Executando trabalhos de descoberta de dados confidenciais.

resultado de descoberta de dados sigilosos

Um log que registra detalhes sobre a análise que o Macie realizou em um objeto do S3 para determinar se o objeto contém dados sigilosos. O Macie gera e grava esses registros em arquivos

JSON Lines (.jsonl), que ele criptografa e armazena em um bucket do S3 especifica por você. Os registros seguem um esquema padronizado.

Quando você executa um trabalho de descoberta de dados sigilosos ou o Macie realiza uma descoberta automatizada de dados sigilosos, o Macie cria um resultado de descoberta de dados sigilosos para cada objeto que é incluído no escopo da análise. Isso inclui:

- Objetos nos quais Macie encontra dados sigilosos e, portanto, também produzem descobertas de dados sigilosos.
- Objetos nos quais Macie não encontra dados sigilosos e, portanto, também não produzem descobertas de dados sigilosos.
- Objetos que o Macie não consegue analisar devido a erros ou problemas, como configurações de permissões ou uso de um arquivo ou formato de armazenamento não suportado.

Para obter mais informações, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

conta autônoma

Uma conta Macie que não é uma conta de administrador nem uma conta-membro em uma organização. A conta não faz parte de uma organização.

descoberta suprimida

Uma descoberta que foi arquivada automaticamente por uma regra de supressão. Ou seja, o Macie alterou automaticamente o status da descoberta para arquivada porque a descoberta correspondia aos critérios de uma regra de supressão quando Macie gerou a descoberta.

Para obter mais informações, consulte Suprimir descobertas.

regra de supressão

Um conjunto de critérios de filtro baseados em atributos que você cria e salva para arquivar (suprimir) descobertas automaticamente. As regras de supressão são úteis em situações em que você revisou uma classe de descobertas e não quer ser notificado sobre elas novamente.

Se você suprimir descobertas com uma regra de supressão, Macie continuará gerando descobertas que correspondam aos critérios da regra. No entanto, o Macie altera automaticamente o status

das descobertas para arquivadas. Isso significa que as descobertas não aparecem por padrão no console do Amazon Macie e o Macie não as publica em outros Serviços da AWS.

Para obter mais informações, consulte Suprimir descobertas.

bytes ou tamanho inclassificáveis

Nas estatísticas do bucket do S3 que o Macie fornece, o tamanho total do armazenamento de todos os objetos inclassificáveis em um bucket do S3.

Se o controle de versionamento estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto classificável no bucket. Se um objeto for um arquivo compactado, esse valor não refletirá o tamanho real do conteúdo do arquivo depois que o arquivo for descompactado.

Para obter mais informações, consulte Analisar seu inventário de buckets do S3 e Avaliando sua postura de segurança no Amazon S3.

objetos inclassificáveis

Um objeto do S3 que o Macie não consegue analisar para detectar dados sigilosos.

Ao calcular as estatísticas do bucket do S3, o Macie determina que um objeto é inclassificável com base na classe de armazenamento e na extensão do nome do arquivo do objeto. Um objeto é inclassificável se não usar uma classe de armazenamento do Amazon S3 ou não tiver uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível.

Para obter mais informações, consulte Analisar seu inventário de buckets do S3 e Avaliando sua postura de segurança no Amazon S3.

Para a descoberta de dados sigilosos, o Macie determina que um objeto inclassificável com base na classe de armazenamento, na extensão do nome do arquivo e no conteúdo do objeto. Um objeto é inclassificável se: não usar uma classe de armazenamento compatível com o Amazon S3, se não tiver uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível, ou se o Macie não conseguiu extrair e analisar os dados do objeto. Por exemplo, o objeto é um arquivo malformado.

Para obter mais informações, consulte Descobrir dados confidenciais e Custos de previsão e monitoramento.

Como monitorar a segurança e a privacidade dos dados com o Amazon Macie

Quando você habilita o Amazon Macie para seu Conta da AWS, o Macie gera automaticamente e começa a manter um inventário completo dos seus buckets do Amazon Simple Storage Service (Amazon S3) no Região da AWS atual. O Macie também começa a avaliar e monitorar os buckets em relação à segurança e ao controle de acesso. Se o Macie detectar um evento que reduza a segurança ou a privacidade de um bucket do S3, ele também criará as descobertas de políticas para você analisar e corrigir conforme necessário.

Para também avaliar e monitorar buckets do S3 quanto à presença de dados confidenciais, você pode criar e executar trabalhos de detecção de dados confidenciais. Trabalhos de detecção de dados confidenciais podem realizar análises incrementais de objetos do bucket diariamente, semanalmente ou mensalmente. Dependendo das configurações da sua conta, você também pode definir o Macie para começar a realizar a detecção automática de dados confidenciais para seus buckets. A detecção automatizada de dados confidenciais usa técnicas de amostragem para identificar, selecionar e analisar continuamento objetos representativos em seus buckets. Se o Macie detectar dados confidenciais em um objeto do S3, ele criará uma descoberta de dados confidenciais para notificar você dos dados confidenciais encontrados por ele. Para obter mais informações, consulte Descobrir dados confidenciais.

Além das descobertas, o Macie fornece visibilidade constante sobre a segurança e a privacidade dos seus dados do Amazon S3. Para avaliar a postura de segurança de seus dados e determinar onde agir, você pode usar o painel de Resumo no console. O painel fornece um instantâneo das estatísticas agregadas para seus dados do Amazon S3. As estatísticas incluem dados das principais métricas de segurança, como o número de buckets que são acessíveis ao público ou compartilhados com outras Contas da AWS. O painel também exibe grupos de dados de descobertas agregadas da sua conta; por exemplo, os nomes dos buckets 1-5 que geraram mais descobertas nos sete dias anteriores. Você pode detalhar cada estatística para analisar os dados de suporte. Se preferir consultar as estatísticas de forma programática, você pode usar a operação GetBucketStatistics da API do Amazon Macie.

Para uma análise e avaliação mais profundas, o Macie também fornece informações e estatísticas detalhadas para buckets do S3 individuais em seu inventário. Isso inclui detalhamentos das configurações de acesso público e criptografia de um bucket e o tamanho e o número de objetos que o Macie pode analisar para detectar dados confidenciais no bucket. O inventário também indica se você configurou algum trabalho de detecção de dados confidenciais para analisar objetos em um

bucket e, em caso afirmativo, quando um desses trabalhos foi executado mais recentemente. Você pode navegar, classificar e filtrar o inventário usando o console do Amazon Macie ou a operação DescribeBuckets da API do Amazon Macie.

Se você for o administrador do Macie de uma organização, você pode acessar dados estatísticos e outros dados sobre buckets do S3 que pertencem às contas dos seus membros. Você também pode acessar as descobertas de políticas que o Macie cria para os buckets e inspecionar os buckets em busca de dados confidenciais. Como administrador do Macie, você pode usar o Macie para avaliar e monitorar a postura geral de segurança do patrimônio de dados do Amazon S3 da sua organização. Para obter mais informações, consulte Gerenciar várias contas da .

Tópicos

Como o Amazon Macie monitora a segurança de dados do Amazon S3

Quando você ativa o Amazon Macie para seu Conta da AWS, o Macie cria uma função vinculada ao serviço AWS Identity and Access Management (IAM) para a sua conta atual Região da AWS. A política de permissões para esse perfil permite que o Macie ligue para outras pessoas Serviços da AWS e monitore recursos AWS em seu nome. Ao usar essa função, o Macie gera e mantém um inventário completo dos seus buckets do Amazon Simple Storage Service (Amazon S3) na região, e o Macie monitora e avalia os buckets para segurança e controle de acesso.

Se você for o administrador do Macie de uma organização, o inventário incluirá buckets que são de propriedade de contas-membro em sua organização. Com esses dados, você pode usar o Macie para monitorar e avaliar a postura de segurança da sua organização em todo o seu ambiente Amazon S3. Para obter mais informações, consulte Gerenciar várias contas da .

Tópicos

Componentes principais

O Amazon Macie usa uma combinação de atributos e técnicas para fornecer e manter dados sobre os buckets do S3 e para monitorar e avaliar os buckets para segurança e controle de acesso.

Coleta de metadados e cálculo de estatísticas

Para gerar e manter metadados e estatísticas para seu inventário de buckets, o Macie recupera metadados de bucket e do objeto diretamente do Amazon S3. Para cada bucket, os metadados incluem:

- Informações gerais sobre o bucket, como nome do bucket, nome do recurso da Amazon (ARN), data de criação, configurações de criptografia, tags e a ID da conta do Conta da AWS proprietário do bucket.
- Configurações de permissões no nível da conta que se aplicam ao bucket, como as configurações de bloqueio de acesso público para a conta.
- Configurações de permissões em nível de bucket para o bucket, como as configurações de bloqueio de acesso público para o bucket e configurações derivadas de uma política de bucket ou lista de controle de acesso (ACL).
- Configurações de acesso e replicação compartilhados para o bucket, incluindo se os dados do bucket são replicados ou compartilhados com Contas da AWS que não fazem parte da sua organização.
- Contagens e configurações de objetos no bucket, como o número de objetos no bucket e os detalhamentos das contagens de objetos por tipo de criptografia, tipo de arquivo e classe de armazenamento.

O Macie fornece essas informações diretamente para você. O Macie também usa as informações para calcular estatísticas e fornecer avaliações sobre a segurança e a privacidade de seu inventário geral do seu bucket e de buckets individuais em seu inventário. Por exemplo, você pode encontrar o tamanho total do armazenamento e o número de buckets em seu inventário, o tamanho total do armazenamento e o número de objetos nesses buckets e o tamanho total do armazenamento e o número de objetos que o Macie pode analisar para detectar dados sigilosos nos buckets.

Por padrão, os metadados e as estatísticas incluem dados de qualquer parte do objeto que exista devido a carregamentos incompletos de várias partes. Se você atualizar manualmente os metadados do objeto para um bucket específico, o Macie recalcula as estatísticas do bucket e do inventário geral do bucket e exclui os dados das partes do objeto dos valores recalculados.

Na próxima vez que o Macie recuperar metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização, o Macie atualizará seus dados de inventário e incluirá novamente os dados das partes do objeto. Para obter informações sobre quando o Macie recupera metadados do bucket e do objeto, consulte Atualizações de dados.

É importante observar que o Macie não consegue analisar partes do objeto para detectar dados sigilosos. O Amazon S3 deve primeiro concluir a montagem das peças em um ou mais objetos para que o Macie analise. Para obter informações sobre uploads de várias partes e partes de objetos, incluindo como excluir peças automaticamente com regras de ciclo de vida, consulte Carregar e copiar objetos usando o upload de várias partes no Guia do usuário do Amazon Simple Storage Service. Para identificar buckets que contêm partes de objetos, você pode consultar métricas incompletas de upload de várias partes na Lente de Armazenamento do Amazon S3. Para obter mais informações, consulte Avaliação de sua atividade de armazenamento e uso com o Amazon S3 Storage Lens no Guia do usuário do Amazon S3.

Monitorando a segurança e a privacidade do bucket

Para ajudar a garantir a precisão dos dados em nível de bucket em seu inventário, o Macie monitora e analisa determinados AWS CloudTraileventos que podem ocorrer com os dados do Amazon S3. Se ocorrer um evento relevante, o Macie atualiza os dados de inventário apropriados.

Por exemplo, se você habilitar as configurações de bloqueio de acesso público para um bucket, o Macie atualizará todos os dados sobre as configurações de acesso público do bucket. Da mesma forma, se você adicionar ou atualizar a política de um bucket, o Macie analisará a política e atualizará os dados relevantes em seu inventário.

O Macie monitora e analisa os dados dos seguintes eventos do CloudTrail:

- Eventos em nível de conta — DeletePublicAccessBlock e PutPublicAccessBlock
- Eventos em nível de bucket — CreateBucket, DeleteAccountPublicAccessBlock, DeleteBucket, DeleteBucketEncryption, DeleteBucketPolicy, DeleteBucketPublicAccessBlock, DeleteBucketReplication, DeleteBucketTagging put, AccountPublicAccessBlock, PutBucketACL, PutBucket Encryption, PutBucketPolicy, PutBucket PublicAccessBlock, PutBucket Replication, PutBucketTagging e PutBucketVersioning

Você não pode ativar o monitoramento de eventos adicionais do CloudTrail nem desativar o monitoramento de nenhum dos eventos anteriores. Para obter informações detalhadas sobre as

operações correspondentes dos eventos anteriores, consulte a Referência da API do Amazon Simple Storage Service.

> **Tip**
>
> Para monitorar eventos no nível do objeto, recomendamos que você use o atributo de proteção do Amazon S3 do Amazon GuardDuty. Esse atributo monitora eventos de dados do Amazon S3 em nível de objeto e os analisa em busca de atividades maliciosas e suspeitas. Para obter mais informações, consulte Proteção do Amazon S3 no Amazon GuardDuty no Guia do usuário do Amazon GuardDuty.

Avaliando a segurança e o controle de acesso do bucket

Para avaliar a segurança e o controle de acesso em nível de bucket, Macie usa raciocínio automatizado baseado em lógica para analisar políticas baseadas em recursos que se aplicam a um bucket. O Macie também analisa as configurações de permissões em nível de conta e de bucket que se aplicam a um bucket. Essa análise considera políticas de bucket, ACLs em nível de bucket e configurações de bloqueio de acesso público para a conta e o bucket.

Para políticas baseadas em recursos, Macie usa Zelkova. Zelkova é um mecanismo de raciocínio automatizado que converte políticas do IAM AWS Identity and Access Management em instruções lógicas e executa um conjunto de solucionadores lógicos especializados e de uso geral (teorias do módulo da satisfatibilidade) em relação ao problema da decisão. O Macie aplica o Zelkova repetidamente a uma política com consultas cada vez mais específicas para caracterizar classes de comportamentos permitidos pela política. Para saber mais sobre a natureza dos solucionadores que Zelkova usa, consulte Teorias do Módulo de Satisfabilidade.

> **Important**
>
> Para realizar as tarefas anteriores em um bucket, o Macie deve ter permissão para acessar o bucket. Se as configurações de permissões de um bucket impedirem que o Macie recupere metadados do bucket ou dos objetos do bucket, o Macie só poderá fornecer um subconjunto de informações sobre o bucket, como o seu nome e data de criação. Macie não pode realizar nenhuma tarefa adicional para o bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Atualizações de dados

Quando você habilita o Amazon Macie para seu Conta da AWS, o Macie recupera metadados para seus buckets e objetos do S3 diretamente do Amazon S3. Depois disso, o Macie recupera automaticamente os metadados do bucket e do objeto diretamente do Amazon S3 diariamente, como parte de um ciclo diário de atualização.

O Macie também recuperará metadados do bucket diretamente do Amazon S3 quando uma das seguintes situações ocorre:

- Você atualiza seus dados de inventário escolhendo atualizar () no console do Amazon Macie. Você pode atualizar os dados a cada cinco minutos.
- Você envia uma solicitação DescribeBuckets para a API do Amazon Macie de forma programática e não enviou uma DescribeBuckets solicitação nos últimos cinco minutos.
- Macie detecta um evento AWS CloudTrail relevante.

O Macie também pode recuperar os metadados mais recentes do objeto para um bucket específico se você optar por atualizar esses dados manualmente. Isso pode ser útil se você criou recentemente um bucket ou fez alterações significativas nos objetos de um bucket nas últimas 24 horas. Para atualizar manualmente os metadados do objeto para um bucket, selecione refresh () na seção Estatísticas do objeto do painel de detalhes do bucket na página de buckets do S3 do console. Esse atributo está disponível para buckets que contêm 30.000 objetos ou menos.

Sempre que o Macie recupera metadados do bucket ou do objeto, o Macie atualiza automaticamente todos os dados relevantes em seu inventário. Se o Macie detectar diferenças que afetem a segurança ou a privacidade de um bucket, o Macie imediatamente começará a avaliar e analisar as alterações. Quando a análise estiver concluída, o Macie atualiza os dados relevantes em seu inventário. Se uma diferença reduzir a segurança ou a privacidade de um bucket, ele também criará as descobertas de políticas apropriadas para você revisar e corrigir conforme necessário.

Para determinar quando o Macie recuperou mais recentemente os metadados de bucket ou objeto da sua conta, você pode consultar o campo Última atualização no console. Esse campo aparece no painel de resumo e na página de buckets do S3, e no painel de detalhes do bucket na página de buckets do S3. (Se você usa a API do Amazon Macie para consultar dados de inventário, o campo `lastUpdated` fornece essas informações.) Se você for o administrador do Macie de uma

organização, o campo Última atualização indicará a data e a hora mais antigas quando o Macie recuperou os dados de uma conta em sua organização.

Em raras ocasiões, sob certas condições, a latência e outros problemas podem impedir que o Macie recupere metadados do bucket e do objeto. Eles também podem atrasar as notificações que o Macie recebe sobre alterações em seu inventário de buckets ou sobre as configurações e políticas de permissões para buckets individuais. Por exemplo, problemas de entrega com eventos do CloudTrail podem causar atrasos. Se isso acontecer, o Macie analisará dados novos e atualizados na próxima vez que realizar a atualização diária, que ocorre em até 24 horas.

Considerações adicionais

Ao usar o Amazon Macie para monitorar e avaliar a postura de segurança dos seus dados do Amazon S3, lembre-se do seguinte:

- Os dados de inventário se aplicam somente aos buckets do S3 no Região da AWS atual. Para acessar os dados de regiões adicionais, habilite e use o Macie em cada região adicional.
- Se você for o administrador do Macie de uma organização, poderá acessar os dados de inventário de uma conta membro somente se o Macie estiver habilitado para essa conta na região atual.
- Se as configurações de permissões de um bucket impedirem o Macie de recuperar informações sobre o bucket ou os objetos do bucket, o Macie não poderá avaliar e monitorar a segurança e a privacidade dos dados do bucket nem fornecer informações detalhadas sobre o bucket.

  Para ajudá-lo a identificar um bucket em que esse seja o caso, Macie faz o seguinte:

  - Em seu inventário de buckets, o Macie exibe um ícone de aviso (⚠) para o bucket. Para os detalhes do bucket, o Macie exibe somente um subconjunto de campos e dados: o ID da conta do proprietário do Conta da AWS bucket; o nome do bucket, nome do recurso da Amazon (ARN), a data de criação e a região; e a data e a hora em que o Macie recuperou mais recentemente os metadados do bucket e do objeto do bucket como parte do ciclo de atualização diária. Se você usar a API do Amazon Macie para consultar dados de inventário, o Macie fornecerá um código de erro e uma mensagem para o bucket, e o valor da maioria das propriedades do bucket será nulo.
  - No painel Resumo, o bucket tem um valor de Desconhecido para estatísticas de acesso público, criptografia e compartilhamento. (Se você usar a API do Amazon Macie para consultar as estatísticas, o bucket terá um valor de `unknown` para essas estatísticas.) Além disso, o Macie exclui o bucket ao calcular dados para estatísticas de armazenamento e objetos.

Para investigar o problema, revise as configurações de políticas e permissões do bucket no Amazon S3. Por exemplo, o bucket pode ter uma política restritiva de bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

- Os dados sobre acesso e permissões são limitados às configurações no nível da conta e do bucket. Ela não reflete as configurações em nível de objeto que determinam o acesso a objetos específicos em um bucket. Por exemplo, se o acesso público estiver habilitado para um objeto específico em um bucket, o Macie não informa que o bucket ou os objetos do bucket estão acessíveis publicamente.

  Para monitorar eventos no nível do objeto, recomendamos que você use o atributo de proteção do Amazon S3 do Amazon GuardDuty. Esse atributo monitora eventos de dados do Amazon S3 em nível de objeto e os analisa em busca de atividades maliciosas e suspeitas. Para obter mais informações, consulte Proteção do Amazon S3 no Amazon GuardDuty no Guia do usuário do Amazon GuardDuty.
- Se você atualizar manualmente os metadados do objeto para um bucket específico, o Macie reportará temporariamente Desconhecido para obter estatísticas de criptografia que se aplicam aos objetos. Na próxima vez que o Macie realizar a atualização diária dos dados (dentro de 24 horas), o Macie reavalia os metadados de criptografia dos objetos e relata novamente os dados quantitativos para as estatísticas.
- Se você atualizar manualmente os metadados do objeto para um bucket específico, o Macie excluirá temporariamente os dados de qualquer parte do objeto que o bucket contenha como resultado de uploads incompletos de várias partes. Na próxima vez que o Macie realizar a atualização diária dos dados (em 24 horas), o Macie recalcula as contagens e os valores do tamanho de armazenamento dos objetos do bucket e inclui os dados das peças nesses cálculos.
- Em casos raros, o Macie pode não conseguir determinar se um bucket é acessível ao público ou compartilhado, ou se requer criptografia do lado do servidor de novos objetos. Por exemplo, um problema temporário pode impedir que o Macie recupere e analise os dados necessários. Ou talvez Macie não consiga determinar completamente se uma ou mais declarações de política concedem acesso a uma entidade externa. Nesses casos, Macie relata Desconhecido para as estatísticas e campos relevantes no inventário. Para investigar o problema, revise as configurações de políticas e permissões do bucket no Amazon S3.

Observe também que o Macie gera descobertas de políticas somente se a segurança ou a privacidade de um bucket forem reduzidas depois que você habilitar o Macie para sua conta. Por exemplo, se você desabilitar as configurações de bloqueio de acesso público para um bucket depois

de habilitar o Macie, o Macie gerará uma descoberta policy:iamuser/s3blockPublicAccessDisabled para o bucket. Por exemplo, se você desabilitar as configurações de bloqueio de acesso público para um bucket depois de habilitar o Macie, o Macie gerará uma descoberta policy:iamuser/s3blockPublicAccessDisabled para o bucket.

Além disso, quando o Macie avalia a segurança e a privacidade de um bucket, ele não examina os logs de acesso nem analisa usuários, funções e outras configurações relevantes das contas. Em vez disso, o Macie analisa e relata os dados das principais configurações que indicam possíveis riscos de segurança. Por exemplo, se uma descoberta de política indicar que um bucket está acessível publicamente, isso não significa necessariamente que uma entidade externa acessou o bucket. Da mesma forma, se uma descoberta de política indicar que um bucket é compartilhado com um Conta da AWS externo à sua organização, o Macie não tenta determinar se esse acesso é intencional e seguro. Em vez disso, essas descobertas indicam que uma entidade externa pode potencialmente acessar os dados do bucket, o que pode ser um risco de segurança não intencional.

Avaliando sua postura de segurança no Amazon S3 com o Amazon Macie

Para avaliar a postura de segurança geral de seus dados no Amazon Simple Storage Service (Amazon S3) e determinar onde agir, você pode usar o painel de Resumo no console do Amazon Macie.

O painel Resumo fornece uma imagem das estatísticas agregadas seus dados do Amazon S3 no Região da AWS atual. As estatísticas do painel incluem dados das principais métricas de segurança, como o número de buckets que são acessíveis ao público ou compartilhados com outras Contas da AWS. O painel também exibe grupos de dados agregados de descobertas da sua conta, como, por exemplo, os tipos de descobertas que tiveram o maior número de ocorrências durante os sete dias anteriores. Se você for o administrador do Macie de uma organização, o painel fornece estatísticas e dados agregados para todas as contas da sua organização. Opcionalmente, você pode filtrar os dados por conta.

Para realizar uma análise mais profunda, você pode detalhar e revisar os dados de suporte de itens individuais no painel. Você também pode revisar e analisar seu inventário de bucket do S3 usando o console do Amazon Macie ou consultar e analisar dados de inventário de forma programática usando a operação da API DescribeBucketsdo Amazon Macie.

Tópicos

Exibindo o painel Resumo

No console do Amazon Macie, o painel Resumo fornece um snapshot das estatísticas agregadas e dos dados de descobertas dos dados do Amazon S3 (Amazon S3) na Região da AWS atual. Se você preferir consultar as estatísticas programaticamente, você pode usar a GetBucketStatisticsoperação da API do Amazon Macie.

Para exibir o painel de resumo

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Resumo. O Macie exibe o painel Resumo.
3. Para determinar quando o Macie recuperou mais recentemente os metadados de bucket ou objeto da sua conta no Amazon S3, você pode consultar o campo Última atualização na parte superior do painel. Para ter mais informações, consulte Atualizações de dados.
4. Para detalhar e revisar os dados de suporte de um item no painel, selecione o item.

Se você for o administrador do Macie de uma organização, o painel fornece estatísticas e dados agregados para a sua conta e as contas-membro da sua organização. Para filtrar o painel e exibir dados apenas para uma conta em particular, insira o ID da conta na caixa Conta acima do painel.

Entendendo os componentes do painel Resumo

No painel Resumo, as estatísticas e os dados são organizados em várias seções. Na parte superior do painel, você encontrará estatísticas agregadas que indicam quantos dados você armazena no Amazon S3 e quanto desses dados o Amazon Macie pode analisar para detectar dados confidenciais. Você também pode consultar o campo Última atualização para determinar quando o Macie recuperou mais recentemente os metadados de bucket ou objeto do Amazon S3 para a sua conta. Seções adicionais fornecem estatísticas e dados de descobertas recentes que podem ajudá-lo a avaliar a segurança, a privacidade e a sensibilidade de seus dados do Amazon S3 na Região da AWS atual.

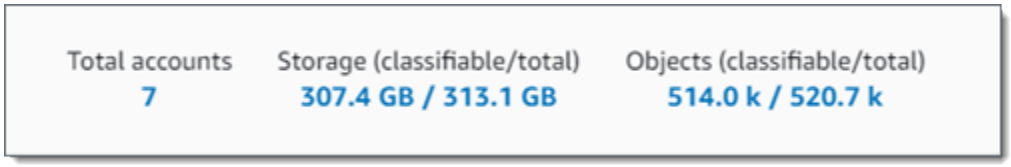
As estatísticas e os dados são organizados nas seguintes seções:

Armazenamento e descoberta de dados confidenciais | Problemas com a descoberta automatizada e de cobertura | Segurança de dados | Principais buckets do S3) | Principais tipos de descobertas | Descobertas de políticas

Ao revisar cada seção, selecione, opcionalmente, um item para detalhar e revisar os dados de suporte.

Armazenamento e descoberta de dados confidenciais

Na parte superior do painel, você encontrará estatísticas agregadas que indicam quantos dados você armazena no Amazon S3 e quanto desses dados o Amazon Macie pode analisar para detectar dados confidenciais. Por exemplo: .



Nesta seção:

- Total de contas – este campo é exibido se você for o administrador do Macie de uma organização ou se tiver uma conta independente no Macie. Ele indica o número total de Contas da AWS que possuem buckets em seu inventário de buckets do S3. Se você for um administrador do Macie, esse é o número total de contas do Macie que você gerencia para sua organização. Se você tiver uma conta independente do Macie, esse valor será 1.

  Total de buckets do S3 – este campo aparece se sua conta do Macie for membro de uma organização. Ele indica o número total de buckets em seu inventário, incluindo os buckets que não contêm nenhum objeto.
- Armazenamento – estas métricas fornecem informações sobre o tamanho de armazenamento dos objetos em seu inventário de buckets:
  - Classificável – o tamanho total de armazenamento de todos os objetos que o Macie pode analisar nos buckets.
  - Total — O tamanho total de armazenamento de todos os objetos nos buckets, incluindo objetos que o Macie não consegue analisar.

  Se algum dos objetos for um arquivo compactado, esses valores não refletirão o tamanho real desses arquivos depois de serem descompactados. Se o controle de versão estiver habilitado para qualquer um dos buckets, esses valores serão baseados no tamanho de armazenamento da versão mais recente de cada objeto nesses buckets.

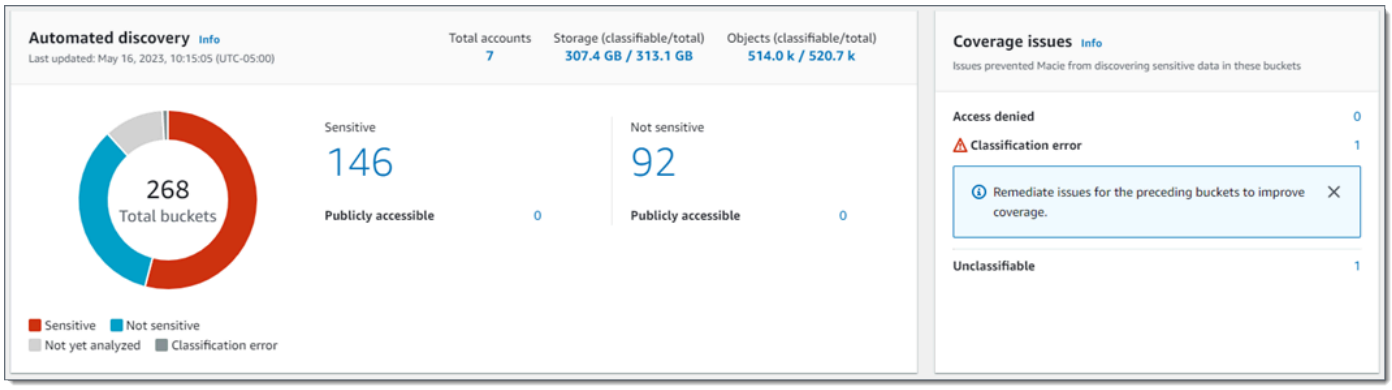
- Objetos – estas métricas fornecem informações sobre o número de objetos em seu inventário de bucket:
  - Classificável – o número total de objetos que o Macie pode analisar nos buckets.
  - Total – O tamanho total de armazenamento de todos os objetos nos buckets, incluindo objetos que o Macie não consegue analisar.

Nas estatísticas anteriores, os dados e objetos são classificáveis se usarem uma classe de armazenamento do Amazon S3 compatível e tiverem uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Você pode detectar dados confidenciais nos objetos usando Macie. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

Observe que as estatísticas Armazenamento e Objetos não incluem dados sobre objetos em buckets que o Macie não tem permissão para acessar. Por exemplo, objetos em buckets que têm políticas restritivas de bucket. Para identificar buckets onde esse é o caso, você pode revisar seu inventário de buckets usando a tabela de S3 buckets. Se o ícone de aviso (⚠) for exibido ao lado do nome de um bucket, o Macie não poderá acessar o bucket.

Problemas com as descobertas automatizadas e cobertura

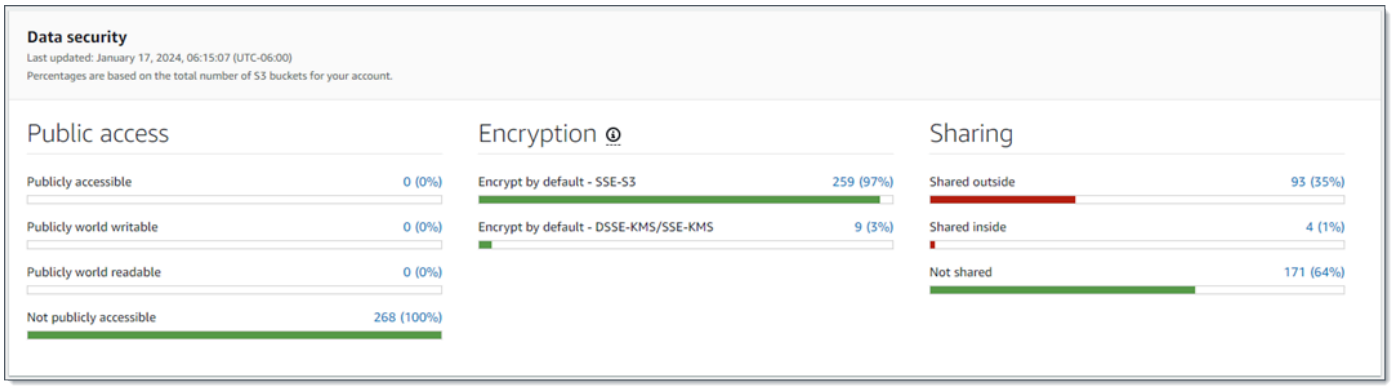
Se a descoberta automatizada de dados confidenciais estiver ativada em sua conta, essas seções serão exibidas no painel. As estatísticas dessas seções capturam o status e os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora para seus dados do Amazon S3. Por exemplo: .



Para obter detalhes sobre essas estatísticas, consulte Revisando estatísticas agregadas de confidencialidade de dados no painel de resumo.

Segurança de dados

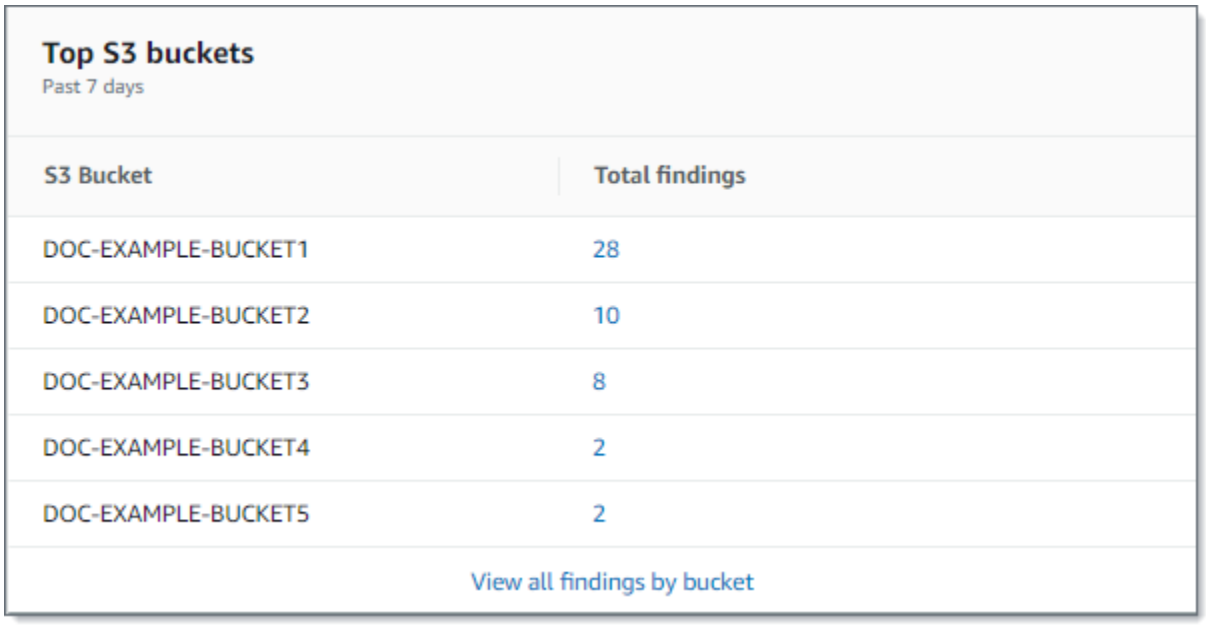
Esta seção fornece estatísticas que indicam possíveis riscos de segurança e privacidade para seus dados do Amazon S3. Por exemplo: .



Para obter detalhes sobre essas estatísticas, consulte Entendendo as estatísticas de segurança de dados no painel Resumo.

Principais buckets do S3

Esta seção lista os buckets do S3 que geraram mais descobertas de qualquer tipo durante os sete dias anteriores, para até cinco buckets. Também indica o número de descobertas que o Macie criou para cada bucket. Por exemplo: .



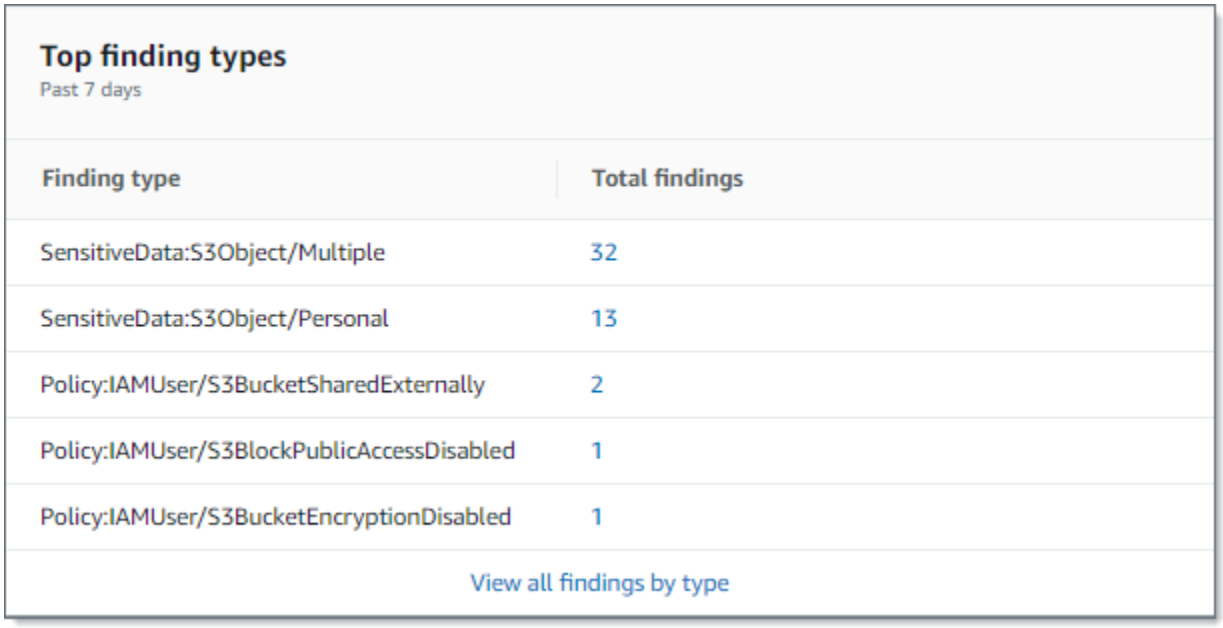
Para exibir e, opcionalmente, detalhar todas as descobertas de um bucket nos sete dias anteriores, selecione o valor no campo Total de descobertas. Para exibir todas as descobertas

atuais de todos os seus buckets, agrupadas por bucket, selecione Exibir todas as descobertas por bucket.

Essa seção estará vazia se o Macie não tiver criado nenhuma descoberta nos sete dias anteriores. Ou se todas as descobertas criadas durante os sete dias anteriores foram suprimidas por uma regra de supressão.

Principais tipos de descobertas

Essa seção lista os tipos de descobertas que tiveram o maior número de ocorrências nos sete dias anteriores, para até cinco tipos de descobertas. Ela também indica o número de descobertas que o Macie criou para cada tipo. Por exemplo: .



Para exibir e, opcionalmente, detalhar todas as descobertas de um determinado tipo nos sete dias anteriores, selecione o valor no campo Total de descobertas. Para exibir todas as descobertas atuais, agrupadas por tipo de descoberta, selecione Exibir todas as descobertas por tipo.

Essa seção estará vazia se o Macie não tiver criado nenhuma descoberta nos sete dias anteriores. Ou se todas as descobertas criadas durante os sete dias anteriores foram suprimidas por uma regra de supressão.

Descobertas de política

Essa seção lista as descobertas de políticas que o Macie criou ou atualizou mais recentemente, para até dez descobertas. Por exemplo: .

Para visualizar os detalhes de uma descoberta, selecione descoberta.

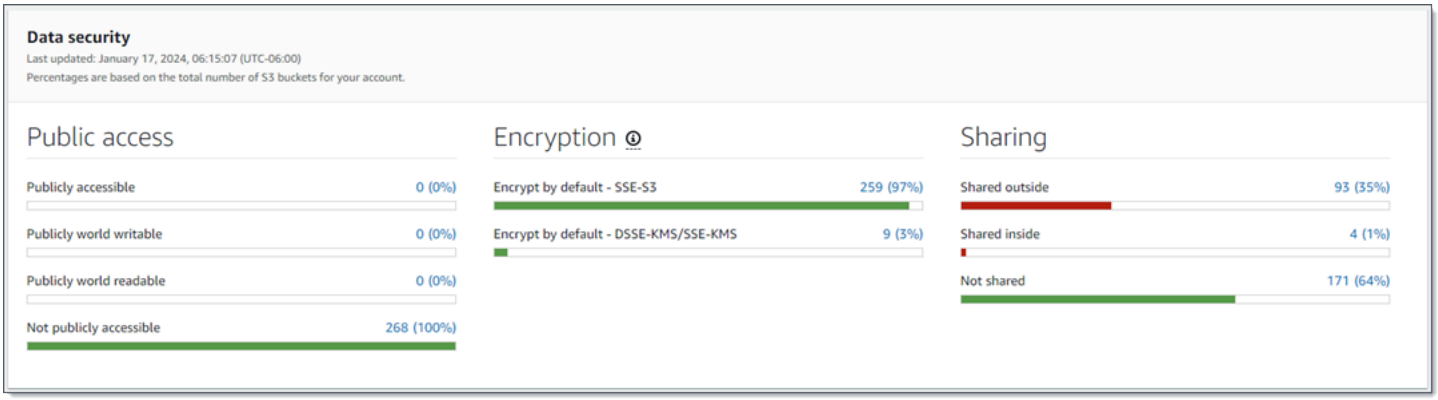
Essa seção estará vazia se o Macie não tiver criado ou atualizado nenhuma descoberta de política durante os sete dias anteriores. Ou se todas as descobertas de política que foram criadas ou atualizadas durante os sete dias anteriores foram suprimidas por uma regra de supressão.

Entendendo as estatísticas de segurança de dados no painel Resumo

A seção Segurança de dados do painel Resumo fornece estatísticas que podem ajudá-lo a identificar e investigar possíveis riscos de segurança e privacidade para seus dados do Amazon S3 na Região da AWS atual. Por exemplo, você pode usar esses dados para identificar buckets do S3 que são acessíveis publicamente ou compartilhados com outras Contas da AWS.

Se sua conta no Macie for membro de uma organização, storage and sensitive data discovery statistics (estatísticas e armazenamento de descobertas de dados confidenciais), na parte superior dessa seção, indicam quantos dados você armazena no Amazon S3 e quantos desses dados o Macie pode analisar para detectar dados confidenciais.

Para qualquer tipo de conta do Macie, estatísticas adicionais são organizadas em três áreas, conforme mostrado na seguinte imagem.



As estatísticas individuais em cada área são as seguintes.

Acesso público

Essas estatísticas indicam quantos buckets do S3 estão ou não acessíveis ao público:

- Acessível publicamente – o número e a porcentagem de buckets que permitem que o público em geral tenha acesso de leitura ou gravação ao bucket.
- Publicamente editável mundialmente – o número e a porcentagem de buckets que permitem que o público em geral tenha acesso de gravação no bucket.
- Publicamente legível mundialmente – o número e a porcentagem de buckets que permitem que o público em geral tenha acesso de leitura ao bucket.
- Não acessível publicamente – o número e a porcentagem de buckets que não permitem que o público em geral tenha acesso de leitura ou gravação ao bucket.

Para calcular cada porcentagem, o Macie divide o número de buckets aplicáveis pelo número total de buckets em seu inventário de buckets.

Para determinar os valores nessa seção, o Macie analisa uma combinação de configurações em nível de conta e de bucket para cada bucket: as configurações de bloqueio de acesso público para a conta; as configurações de bloqueio de acesso público para o bucket; a política de bucket para o bucket e a lista de controle de acesso (ACL) para o bucket. Para obter informações sobre essas configurações, consulte Gerenciamento de identidade e acesso no Amazon S3 e Bloqueio do acesso público ao seu armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Em certos casos, a seção Acesso público também exibe valores para Desconhecido. Se esses valores aparecerem, o Macie não conseguiu avaliar as configurações de acesso público para o número e a porcentagem especificados de buckets. Por exemplo, um problema temporário ou as configurações de permissões dos buckets impediram que o Macie recuperasse os dados necessários. Ou, talvez, o Macie não conseguiu determinar completamente se uma ou mais instruções de política concedem acesso aos buckets a uma entidade externa.

Criptografia

Essas estatísticas indicam quantos buckets do S3 estão configurados para aplicar certos tipos de criptografia do lado do servidor aos objetos que são adicionados aos buckets:

- Criptografar por padrão — SSE-S3 – o número e a porcentagem de buckets cujas configurações de criptografia padrão estão definidas para criptografar novos objetos com

uma chave gerenciada do Amazon S3. Para esses buckets, novos objetos são criptografados automaticamente usando a criptografia SSE-S3.

- Criptografar por padrão — DSSE-KMS/SSE-KMS — O número e a porcentagem de compartimentos cujas configurações de criptografia padrão estão definidas para criptografar novos objetos com uma chave gerenciada pelo cliente ou uma chave gerenciada pelo cliente. AWS KMS key Chave gerenciada pela AWS Para esses buckets, novos objetos são criptografados automaticamente usando criptografia DSSE-KMS ou SSE-KMS.

Para calcular cada porcentagem, o Macie divide o número de buckets aplicáveis pelo número total de buckets em seu inventário de buckets.

Para determinar os valores nessa seção, o Macie analisa as configurações de criptografia padrão para cada bucket. A partir de 5 de janeiro de 2023, o Amazon S3 aplica automaticamente a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para objetos adicionados aos buckets. Opcionalmente, você pode definir as configurações de criptografia padrão de um bucket para, em vez disso, usar a criptografia do lado do servidor com uma AWS KMS chave (SSE-KMS) ou a criptografia do lado do servidor de camada dupla com uma chave (DSSE-KMS). AWS KMS Para obter informações sobre as configurações e opções de criptografia padrão, consulte Como definir o comportamento padrão de criptografia do lado do servidor para buckets S3 no Guia do usuário do Amazon Simple Storage Service.

Em certos casos, a seção Criptografia também exibe valores para Desconhecido. Se esses valores forem exibidos, o Macie não conseguiu avaliar as configurações de criptografia padrão para o número e a porcentagem especificados de buckets. Por exemplo, um problema temporário ou as configurações de permissões dos buckets impediram que o Macie recuperasse os dados necessários.

Compartilhamento

Essas estatísticas indicam quantos buckets do S3 são ou não compartilhados com outras identidades de acesso de CloudFront origem (OAIs) ou controles de acesso de CloudFront origem (OACs) da Contas da AWS Amazon:

- Compartilhado externamente — o número e a porcentagem de buckets que são compartilhados com um ou mais dos itens a seguir ou com qualquer combinação dos seguintes: um CloudFront OAI, um CloudFront OAC ou uma conta que não está na mesma organização.
- Compartilhado internamente — O número e a porcentagem de buckets que são compartilhados com uma ou mais contas na mesma organização. Esses buckets não são compartilhados com CloudFront OAIs ou OACs.

- Não compartilhado — o número e a porcentagem de buckets que não são compartilhados com outras contas, CloudFront OAIs ou CloudFront OACs.

Para calcular cada porcentagem, o Macie divide o número de buckets aplicáveis pelo número total de buckets em seu inventário de buckets.

Para determinar se os buckets são compartilhados com outras Contas da AWS, o Macie analisa a política e a ACL de cada bucket. Além disso, uma organização é definida como um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio do AWS Organizations ou por convite do Macie. Para obter informações sobre as opções de compartilhamento de buckets do Amazon S3, consulte Identity and Access Management no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Em certos casos, o Macie pode relatar incorretamente que um bucket está compartilhado com uma Conta da AWS que não está na mesma organização. Isso pode ocorrer se o Macie não conseguir avaliar totalmente a relação entre o elemento `Principal` em uma política do bucket e determinadas chaves de contexto de condição global AWS ou chaves de condição do Amazon S3 no elemento `Condition` da política. As chaves de condição aplicáveis são: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPaths`, `aws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, `aws:userid`, `s3:DataAccessPointAccount` e `s3:DataAccessPointArn`.
> Para determinar se esse é o caso para determinados buckets, selecione a estatística Compartilhado externamente no painel. Na tabela exibida, anote o nome de cada bucket. Em seguida, use o Amazon S3 para revisar a política de cada bucket e determinar se as configurações de acesso compartilhado são intencionais e seguras.

Para determinar se os buckets são compartilhados com CloudFront OAIs ou OACs, o Macie analisa a política de bucket para cada bucket. Um CloudFront OAI ou OAC permite que os usuários acessem os objetos de um bucket por meio de uma ou mais distribuições especificadas CloudFront . Para obter informações sobre CloudFront OAIs e OACs, consulte Restringir o acesso a uma origem do Amazon S3 no Amazon Developer Guide. CloudFront

Em certos casos, a seção Compartilhamento também exibe valores para Desconhecido. Se esses valores aparecerem, Macie não conseguiu determinar se o número e a porcentagem

especificados de buckets são compartilhados com outras contas, CloudFront OAIs ou OACs. CloudFront Por exemplo, um problema temporário ou as configurações de permissões dos buckets impediram que o Macie recuperasse os dados necessários. Ou, talvez, o Macie não conseguiu avaliar totalmente as políticas ou ACLs dos buckets.

Analisando sua postura de segurança do Amazon S3 com o Amazon Macie

Para ajudá-lo a realizar uma análise aprofundada e avaliar a postura de segurança dos seus dados do Amazon Simple Storage Service (Amazon S3), o Amazon Macie mantém um inventário completo dos seus buckets do S3 em cada Região da AWS em que você usa o Macie. Para saber como a Macie mantém esse inventário para você, consulte Como o Macie monitora a segurança de dados do Amazon S3. Se você for o administrador do Macie de uma organização, o inventário inclui dados dos buckets do S3 que suas contas membros possuem.

Ao usar esse inventário, você pode revisar sua propriedade de dados do Amazon S3 e examinar detalhes e estatísticas das principais configurações e métricas de segurança que se aplicam a buckets individuais do S3. Por exemplo, você pode acessar detalhamentos das configurações de acesso público e criptografia de cada bucket e o tamanho e o número de objetos que o Macie pode analisar para detectar dados confidenciais em cada bucket. Você também pode determinar se configurou algum trabalho confidencial de descoberta de dados para analisar objetos em um bucket e, em caso afirmativo, quando um desses trabalhos foi executado mais recentemente. Se a descoberta automatizada de dados confidenciais estiver ativada em sua conta, você também poderá usar o inventário para analisar os resultados das atividades automatizadas de descoberta de dados confidenciais que a Macie realizou até agora para sua conta ou organização. Para obter mais informações, consulte Descobrir dados confidenciais.

Você pode navegar e filtrar dados de inventário usando a página de buckets do S3 no console do Amazon Macie. Você também pode acessar seus dados de inventário de forma programática usando a operação DescribeBuckets da API Amazon Macie.

Tópicos

- Analisar seu inventário de buckets do S3 com o Amazon Macie
- Como filtrar o seu inventário de buckets do S3 com o Amazon Macie

Analisar seu inventário de buckets do S3 com o Amazon Macie

No console do Amazon Macie, a página Buckets do S3 fornece uma visão detalhada sobre a segurança e a privacidade dos dados atuais do Amazon Simple Storage Service (Amazon S3). Região da AWS Com essa página, você pode revisar e analisar um inventário completo de seus buckets do S3 na região atual e analisar informações e estatísticas detalhadas de buckets individuais. Se você for o administrador do Macie de uma organização, seu inventário inclui detalhes e estatísticas dos buckets do S3 que pertencem às contas dos membros da sua organização.

A página Buckets do S3 também indica quando o Macie recuperou mais recentemente os metadados do bucket ou do objeto do Amazon S3 para sua conta. Você pode encontrar essas informações no campo Última atualização na parte superior da página. Se você for o administrador do Macie para uma organização, esse campo indica a data e a hora mais antigas em que o Macie recuperou os dados de uma conta na sua organização. Para ter mais informações, consulte Atualizações de dados.

Observe que a maioria dos dados de inventário está limitada aos buckets que o Macie pode acessar para sua conta. Se as configurações de permissões de um bucket impedirem o Macie de recuperar informações sobre o bucket ou os objetos do bucket, o Macie só poderá fornecer um subconjunto de informações sobre o bucket. Se esse for o caso de um determinado bucket, o Macie exibirá um ícone de aviso (⚠) e uma mensagem para o bucket em seu inventário de bucket. Para obter os detalhes do bucket, o Macie exibe somente um subconjunto de campos e de dados: o ID da conta do Conta da AWS proprietário do bucket; o nome do bucket, o nome de recurso da Amazon (ARN), a data de criação e a região; e, quando o Macie recuperou mais recentemente os metadados do bucket e do objeto como parte do ciclo de atualização diária. Para investigar o problema, revise as configurações de políticas e permissões do bucket no Amazon S3. Por exemplo, o bucket pode ter uma política restritiva de bucket. Para ter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Se você preferir acessar e consultar seus dados de inventário de forma programática, você pode usar a DescribeBucketsoperação da API do Amazon Macie.

Tópicos

Analisar seu inventário de buckets do S3

A página S3 buckets no console do Amazon Macie fornece informações sobre seus buckets do S3 no Região da AWS atual. Nessa página, uma tabela exibe informações resumidas para cada bucket em seu inventário. Para personalizar sua visualização, você pode classificar e filtrar a tabela. Se você escolher um bucket na tabela, o painel de detalhes exibirá informações adicionais sobre o bucket. Isso inclui detalhes e estatísticas de configurações e métricas que fornecem informações sobre a segurança e a privacidade dos dados do bucket. Você pode, opcionalmente, exportar dados da tabela para um arquivo de valores separados por vírgula (CSV).

Se a descoberta automatizada de dados confidenciais estiver habilitada em sua conta, você também terá a opção de analisar seu inventário usando um mapa de calor interativo. O mapa fornece uma representação visual da confidencialidade dos dados em toda a sua propriedade de dados do Amazon S3. Ele captura os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou para sua conta ou organização. Para saber mais sobre esse mapa, consulte Como visualizar a confidencialidade dos dados com o mapa de buckets do S3.

Para analisar seu inventário de buckets do S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Buckets S3. A página de buckets do S3 exibe seu inventário de buckets.

   Se a página exibir um mapa interativo do seu inventário do bucket, selecione tabela () na parte superior da página. Em seguida, o Macie exibe o número de buckets em seu inventário e uma tabela dos buckets.
3. Na parte superior da página, escolha opcionalmente atualizar () para recuperar os metadados mais recentes do bucket a partir do Amazon S3.

   Se o ícone de informações () aparecer ao lado de qualquer nome de bucket, recomendamos que você faça isso. Esse ícone indica que um bucket foi criado nas últimas 24 horas, possivelmente após a última vez que Macie recuperou os metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização.

4. Na página Buckets S3, use a tabela para analisar um subconjunto de informações sobre cada bucket em seu inventário:

   - Confidencialidade — A pontuação de confidencialidade atual do bucket. Essa coluna aparece somente se a descoberta automatizada de dados confidenciais estiver habilitada em sua conta. Para obter informações sobre o intervalo de pontuações de confidencialidade que o Macie define, consulte Pontuação de confidencialidade para buckets do S3.
   - Bucket – O nome do bucket.
   - Conta – O ID da Conta da AWS à qual o bucket pertence.
   - Objetos classificáveis – O número total de objetos que o Macie pode analisar para detectar dados confidenciais no bucket.
   - Tamanho classificável – O tamanho total de armazenamento de todos os objetos que o Macie pode analisar para detectar dados confidenciais no bucket.

     Observe que esse valor não reflete o tamanho real de nenhum objeto compactado depois de descompactado. Além disso, se o controle de versão estiver habilitado para o bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto no bucket.
   - Monitorado por trabalho — se algum trabalho de descoberta de dados confidenciais estiver configurada para analisar periodicamente objetos no bucket diariamente, semanalmente ou mensalmente.

     Se o valor desse campo for Sim, o bucket será incluído explicitamente em um trabalho periódico ou corresponderá aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.
   - Última execução do trabalho — se algum trabalho de descoberta de dados confidenciais único ou periódico estiver configurado para analisar objetos no bucket, o valor desse campo indicará a data e a hora mais recentes em que um desses trabalhos começou a ser executado. Caso contrário, esse campo fica vazio.

   Nos dados anteriores, os objetos serão classificáveis se usarem uma classe de armazenamento compatível do Amazon S3 e tiverem uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Você pode detectar dados confidenciais nos objetos usando Macie. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

5. Para analisar o inventário usando a tabela, siga um destes procedimentos:

   - Para classificar a tabela por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna.
   - Para filtrar a tabela e exibir somente os buckets que têm um valor específico para um campo, coloque o cursor na caixa de filtro e adicione uma condição de filtro para o campo. Para refinar ainda mais os resultados, adicione condições de filtro para campos adicionais. Para ter mais informações, consulte Como filtrar o seu inventário de buckets do S3.

6. Para analisar detalhes e estatísticas de um bucket específico, selecione o nome do bucket na tabela e consulte o painel de detalhes.

   > **Tip**
   >
   > Você pode dinamizar e detalhar muitos dos campos no painel de detalhes do bucket. Para mostrar buckets que têm o mesmo valor para um campo, selecione
   >
   > no campo. Para mostrar buckets que têm o mesmo valor para um campo, escolha
   >
   > no campo.

7. Para exportar dados da tabela para um arquivo CSV, marque a caixa de seleção para cada linha que você deseja exportar ou marque a caixa de seleção no título da coluna de seleção para selecionar todas as linhas. Em seguida, selecione Exportar para CSV na parte superior da página. Você pode exportar até 50.000 linhas da tabela.

Analisar os detalhes dos buckets do S3

No console do Amazon Macie, você pode usar o painel de detalhes na página de buckets do S3 para analisar estatísticas e outras informações sobre buckets individuais do S3 em seu inventário de buckets. Isso inclui detalhes e estatísticas de configurações e métricas que fornecem informações sobre a segurança e a privacidade dos dados de um bucket.

Por exemplo, você pode analisar detalhamentos das configurações de acesso público de um bucket do S3 e determinar se um bucket está configurado para replicar objetos ou é compartilhado com outros. Contas da AWS Você também pode determinar se algum trabalho de descoberta de dados confidenciais está configurado para inspecionar o bucket em busca de dados confidenciais.

Se houver, você poderá acessar detalhes sobre o trabalho executado mais recentemente e, opcionalmente, exibir todas as descobertas que o trabalho produziu.

Se a descoberta automatizada de dados confidenciais estiver habilitada em sua conta, você também poderá usar o painel de detalhes para analisar estatísticas de descoberta de dados confidenciais e outras informações sobre buckets individuais do S3. O painel captura os resultados das atividades automatizadas de descoberta de dados confidenciais que Macie realizou até agora em um bucket. Para saber mais sobre esses detalhes, consulteAnalisando detalhes de confidencialidade de dados para buckets do S3 individuais.

Para analisar os detalhes de um bucket S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Buckets S3. A página Buckets do S3 exibirá seu inventário de buckets.
3. Na parte superior da página, selecione opcionalmente atualizar
   ()
   para recuperar os metadados mais recentes de bucket do Amazon S3.
4. Na tabela ou no mapa de buckets do S3, selecione o bucket cujos detalhes você deseja analisar. O painel de detalhes exibe estatísticas, configurações e outras informações sobre o bucket.

No painel de detalhes, as estatísticas e as informações do bucket são organizadas nas seguintes seções principais:

Visão geral | Estatísticas de objetos | Criptografia do lado do servidor | Descoberta de dados confidenciais | Acesso público | Replicação | Tags

Ao analisar as informações em cada seção, você pode, como opção, dinamizar e fazer uma busca detalhada em determinados campos. Para mostrar buckets que têm o mesmo valor para um campo, selecione

no campo. Para mostrar buckets que têm outros valores para um campo, escolha

no campo.

Visão geral

Esta seção fornece informações gerais sobre o bucket, como o nome do bucket, quando o bucket foi criado e o ID da conta do Conta da AWS proprietário do bucket. Vale ressaltar que o campo Última atualização indica quando o Macie recuperou mais recentemente os metadados do Amazon S3 para o bucket ou os objetos do bucket.

O campo Acesso compartilhado indica se o bucket está compartilhado com outroConta da AWS, com uma identidade de acesso de CloudFront origem da Amazon (OAI) ou com um controle de acesso de CloudFront origem (OAC):

- Externo — O bucket é compartilhado com um ou mais dos itens a seguir ou com qualquer combinação dos seguintes: um CloudFront OAI, um CloudFront OAC ou uma conta externa (que não faz parte da) sua organização.
- Interno — o bucket é compartilhado com uma ou mais contas internas à (parte da) sua organização. Não é compartilhado com um CloudFront OAI ou OAC.
- Não compartilhado — O bucket não é compartilhado com outra conta, um CloudFront OAI ou um CloudFront OAC.
- Desconhecido — o Macie não conseguiu avaliar as configurações de acesso compartilhado do bucket.

Para determinar se um bucket é compartilhado com outroConta da AWS, o Macie analisa a política do bucket e a lista de controle de acesso (ACL) do bucket. A análise é limitada às configurações em nível de bucket. Ela não reflete nenhuma configuração em nível de objeto para compartilhar objetos específicos no bucket. Além disso, uma organização é definida como um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio de AWS Organizations ou por convite do Macie. Para saber mais sobre as opções do Amazon S3 para compartilhamento de buckets, consulte Gerenciamento de identidade e acesso no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Em certos casos, o Macie pode indicar incorretamente que um bucket está compartilhado com um Conta da AWS que é externo à sua organização (que não faz parte dela). Isso pode ocorrer se o Macie não conseguir avaliar totalmente a relação entre o `Principal` elemento na política do bucket e determinadas chaves de contexto de condição AWS global ou chaves de condição do Amazon S3 no elemento `Condition` da política. As

chaves de condição aplicáveis são: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPaths`, `aws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, `aws:userid`, `s3:DataAccessPointAccount` e `s3:DataAccessPointArn`. Recomendamos que você analise a política do bucket para determinar se esse acesso é intencional e seguro.

Para determinar se um bucket é compartilhado com um CloudFront OAI ou OAC, o Macie analisa a política de bucket para o bucket. Um CloudFront OAI ou OAC permite que os usuários acessem os objetos de um bucket por meio de uma ou mais distribuições especificadas CloudFront . Para saber mais sobre CloudFront OAIs e OACs, consulte Restringir o acesso a uma origem do Amazon S3 no Amazon Developer Guide. CloudFront

A seção Visão geral do painel também inclui o campo Última execução de descoberta automatizada. Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta, esse campo indica quando o Macie analisou objetos no bucket mais recentemente enquanto realizava a descoberta automatizada em sua conta. Se a descoberta automatizada de dados confidenciais estiver desabilitada em sua conta, um traço (—) aparecerá nesse campo.

Estatísticas de objetos

Esta seção fornece informações sobre os objetos no bucket, começando com o número total de objetos no bucket (contagem total), o tamanho total de armazenamento de todos esses objetos (tamanho total do armazenamento) e o tamanho total do armazenamento de todos os objetos que são arquivos compactados (.gz, .gzip ou .zip) (tamanho total compactado). Estatísticas adicionais nesta seção podem ajudá-lo a avaliar a quantidade de dados que o Macie pode analisar para detectar dados confidenciais no bucket.

Se você criou o bucket recentemente ou fez alterações significativas nos objetos do bucket nas últimas 24 horas, opcionalmente, escolha atualizar () para recuperar os metadados mais recentes dos objetos do bucket. O Macie exibe o ícone de informações () para ajudá-lo a determinar se esse pode ser o caso. A opção de atualização está disponível se um bucket contiver 30.000 objetos ou menos.

Ao analisar as estatísticas desta seção, lembre-se do seguinte:

- Se o controle de versão estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto no bucket.
- Se o bucket contiver objetos compactados, os valores de tamanho não refletirão o tamanho real desses objetos depois que eles forem descompactados.
- Se você atualizar os metadados do objeto para um bucket, o Macie reportará temporariamente Desconhecido para as estatísticas de criptografia que se aplicam aos objetos. O Macie reavaliará e atualizará os dados dessas estatísticas quando realizar a próxima atualização diária dos metadados do bucket e do objeto, que ocorre em 24 horas.
- Por padrão, as contagens de objetos e os valores de tamanho incluem dados de todas as partes do objeto que o bucket contém como resultado de carregamentos incompletos de várias partes. Se você atualizar os metadados do objeto para um bucket, o Macie excluirá os dados das partes do objeto dos valores recalculados. Quando o Macie realiza a próxima atualização diária dos metadados do bucket e do objeto (em 24 horas), o Macie recalcula e atualiza os valores dessas estatísticas e inclui novamente os dados das partes do objeto nos valores.

  Observe que o Macie não consegue analisar partes do objeto para detectar dados confidenciais. O Amazon S3 deve primeiro concluir a montagem das peças em um ou mais objetos para que o Macie analise. Para obter informações sobre uploads de várias partes e partes de objetos, incluindo como excluir peças automaticamente com regras de ciclo de vida, consulte Carregar e copiar objetos usando o upload de várias partes no Guia do usuário do Amazon Simple Storage Service. Para identificar buckets que contêm partes de objetos, você pode consultar métricas incompletas de upload de várias partes na Lente de Armazenamento do Amazon S3. Para obter mais informações, consulte Avaliando sua atividade e uso de armazenamento no Guia do usuário Amazon Simple Storage Service .

As estatísticas do objeto são organizadas da seguinte forma.

Objetos classificáveis

Esta seção indica o número total de objetos que o Macie pode analisar para detectar dados confidenciais e o tamanho total de armazenamento desses objetos. Esses objetos usam uma classe de armazenamento compatível do Amazon S3 e têm uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Você pode detectar dados confidenciais nos objetos usando o Macie. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

Objetos inclassificáveis

Esta seção indica o número total de objetos que o Macie não consegue analisar para detectar dados confidenciais e o tamanho total de armazenamento desses objetos. Esses objetos não usam uma classe de armazenamento do Amazon S3 ou não têm uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível.

Objetos não classificáveis: classe de armazenamento

Esta seção fornece um detalhamento do número e do tamanho de armazenamento dos objetos que o Macie não pode analisar porque os objetos não usam uma classe de armazenamento compatível do Amazon S3.

Objetos inclassificáveis: tipo de arquivo

Esta seção fornece um detalhamento do número e do tamanho de armazenamento dos objetos que o Macie não pode analisar porque os objetos não têm uma extensão de nome de arquivo para um formato de arquivo ou de armazenamento compatível.

Objetos por tipo de criptografia

Esta seção fornece um detalhamento do número de objetos que usam cada tipo de criptografia compatível com o Amazon S3:

- Fornecido pelo cliente — O número de objetos que são criptografados com uma chave fornecida pelo cliente. Esses objetos usam criptografia SSE-C.
- AWS KMSgerenciado — O número de objetos que são criptografados com uma AWS KMS key chave gerenciada pelo cliente Chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. Esses objetos usam criptografia DSSE-KMS ou SSE-KMS.
- Amazon S3 gerenciado — O número de objetos que são criptografados com uma chave gerenciada do Amazon S3. Esses objetos usam criptografia SSE-S3.
- Sem criptografia — O número de objetos que não estão criptografados ou usam criptografia do lado do cliente. (Se um objeto for criptografado usando criptografia do lado do cliente, o Macie não poderá acessar e reportar dados de criptografia do objeto.)
- Desconhecido — O número de objetos para os quais o Macie não tem metadados de criptografia atuais. Isso geralmente ocorre se você optou recentemente por atualizar manualmente os metadados dos objetos do bucket. O Macie atualizará as estatísticas de criptografia quando realizar a próxima atualização diária dos metadados do bucket e do objeto, que ocorre em 24 horas.

Para obter informações sobre cada tipo de criptografia compatível, consulte Proteção de dados com criptografia no Guia do usuário do Amazon Simple Storage Service.

Criptografia do lado do servidor

Esta seção fornece informações sobre as configurações de criptografia do lado do servidor para o bucket.

O campo de política de Criptografia exigida pelo bucket indica se a política do bucket exige criptografia de objetos no lado do servidor quando os objetos são adicionados ao bucket:

- Não — o bucket não tem uma política de bucket ou a política do bucket não exige criptografia do lado do servidor de novos objetos. Se existir uma política de bucket, ela não exigirá que as PutObjectsolicitações incluam um cabeçalho de criptografia válido no lado do servidor.
- Sim — a política do bucket exige criptografia de novos objetos no lado do servidor. PutObjectas solicitações para o bucket devem incluir um cabeçalho de criptografia válido do lado do servidor. Caso contrário, o Amazon S3 negará a solicitação.
- Desconhecido — Macie não conseguiu avaliar a política do bucket para determinar se ela exige criptografia no lado do servidor de novos objetos.

Para essa avaliação, os cabeçalhos de criptografia válidos do lado do servidor são: `x-amz-server-side-encryption` com um valor de `AES256` ou `aws:kms` e `x-amz-server-side-encryption-customer-algorithm` com um valor de. `AES256` Para obter informações sobre o uso de políticas de bucket para exigir criptografia no lado do servidor de novos objetos, consulte Proteção de dados com criptografia no lado do servidor no Guia do usuário do Amazon Simple Storage Service.

O campo Criptografia padrão indica qual algoritmo de criptografia do lado do servidor o bucket está configurado para aplicar por padrão aos objetos que são adicionados ao bucket:

- AES256 — As configurações de criptografia padrão do bucket são definidas para criptografar novos objetos com uma chave gerenciada do Amazon S3. Os novos objetos são criptografados automaticamente usando criptografia SSE-S3.
- aws:kms — As configurações de criptografia padrão do bucket são definidas para criptografar novos objetos com uma AWS KMS key, uma Chave gerenciada pela AWS ou uma chave gerenciada pelo cliente. Novos objetos são criptografados automaticamente usando a criptografia SSE-KMS. O AWS KMS keycampo mostra o Amazon Resource Name (ARN) ou o identificador exclusivo (ID da chave) da chave usada.

- aws:kms:dsse — As configurações de criptografia padrão do bucket são definidas para criptografar novos objetos com uma chaveAWS KMS key, uma ou uma chave gerenciada pelo cliente. Chave gerenciada pela AWS Novos objetos são criptografados automaticamente usando a criptografia DSSE-KMS. O AWS KMS keycampo mostra o ARN ou ID da chave usada.
- Nenhuma — As configurações de criptografia padrão do bucket não especificam o comportamento de criptografia do lado do servidor para novos objetos.

A partir de 5 de janeiro de 2023, o Amazon S3 aplica automaticamente a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como o nível básico de criptografia para objetos que são adicionados aos buckets. Opcionalmente, você pode definir as configurações de criptografia padrão de um bucket para, em vez disso, usar a criptografia do lado do servidor com uma AWS KMS chave (SSE-KMS) ou a criptografia do lado do servidor de camada dupla com uma chave (DSSE-KMS). AWS KMS Para obter informações sobre configurações e opções de criptografia padrão, consulte Definindo o comportamento padrão de criptografia do lado do servidor para buckets S3 no Guia do usuário do Amazon Simple Storage Service.

Descoberta de dados confidenciais

Esta seção indica se algum trabalho confidencial de descoberta de dados está configurado para analisar periodicamente objetos no bucket diariamente, semanalmente ou mensalmente. Se o valor do campo Monitorado ativamente por cargo for Sim, o período será incluído explicitamente em um trabalho periódico ou o período correspondeu aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.

Se algum tipo de trabalho de descoberta de dados confidenciais (seja um trabalho periódico ou um trabalho único) estiver configurado para inspecionar o bucket, o campo Trabalho mais recente fornecerá o identificador exclusivo do trabalho que começou a ser executado mais recentemente. O campo Última execução do trabalho indica quando esse trabalho começou a ser executado.

> **Tip**
>
> Para exibir todas as descobertas de dados confidenciais que o trabalho produziu, escolha o link no campo Trabalho mais recente. No painel de detalhes do trabalho exibido, escolha Mostrar resultados na parte superior do painel e, em seguida, escolha Mostrar descobertas.

Acesso público

Esta seção indica se o bucket é acessível publicamente. Ele também fornece um detalhamento das várias configurações em nível de conta e bucket que determinam se esse é o caso. O campo Permissão efetiva indica o resultado cumulativo dessas configurações:

- Não público – O bucket não é acessível publicamente.
- Público – O bucket é acessível publicamente.
- Desconhecido — Macie não conseguiu avaliar todas as configurações de acesso público do bucket.

Observe que esses dados estão limitados às configurações no nível da conta e do bucket. Ela não reflete as configurações em nível de objeto que permitem o acesso público a objetos específicos em um bucket.

Para saber mais sobre as configurações do Amazon S3 para gerenciar o acesso público aos buckets e aos dados do bucket, consulte Gerenciamento de identidade e acesso no Amazon S3 e Bloqueio do acesso público ao seu armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Replicação

Nesta seção, o campo Replicado indica se o bucket está configurado para replicar objetos em outros buckets. Se o valor desse campo for Sim, uma ou mais regras de replicação serão configuradas e habilitadas para o bucket. Em seguida, essa seção também lista o ID da conta de cada um Conta da AWS que possui um bucket de destino.

O campo Replicado externamente indica se o bucket está configurado para replicar objetos em buckets para Contas da AWS que são externos à sua organização (que não fazem parte dela). Uma organização é um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio de AWS Organizations ou por convite do Macie. Se o valor desse campo for Sim, uma regra de replicação será configurada e habilitada para o bucket, e a regra será configurada para replicar objetos em um bucket de propriedade de um Conta da AWS externo.

> **Note**
>
> Sob certas condições, o Macie pode indicar incorretamente que um bucket está configurado para replicar objetos em um bucket que pertence a um Conta da AWS externo. Isso pode

ocorrer se o bucket de destino tiver sido criado em um local diferente Região da AWS durante as 24 horas anteriores, depois que o Macie recuperou os metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização.
Para investigar o problema usando o Macie, escolha atualizar
()
para recuperar os metadados mais recentes do bucket do Amazon S3. Em seguida, analise a lista de IDs de conta nesta seção. Para uma investigação mais aprofundada, use o Amazon S3 para analisar as regras de replicação do bucket.

Para saber mais sobre as opções e configurações do Amazon S3 para replicar objetos de bucket, consulte Replicação de objetos no Guia do usuário do Amazon Simple Storage Service.

Tags

Se as tags estiverem associadas ao bucket, essa seção aparecerá no painel e listará essas tags. As tags são rótulos que você pode definir e atribuir a determinados tipos de recursos AWS, incluindo os buckets do S3. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional.

Para saber mais sobre marcação de buckets, consulte Usando tags de bucket S3 de alocação de custos no Guia do usuário do Amazon Simple Storage Service.

Como filtrar o seu inventário de buckets do S3 com o Amazon Macie

Para identificar e focar nos buckets que têm características específicas, você pode filtrar seu inventário de buckets do S3 no console do Amazon Macie e nas consultas que você envia programaticamente usando a API do Amazon Macie. Ao criar um filtro, você usa atributos específicos dos buckets para definir critérios para incluir ou excluir buckets de uma exibição ou dos resultados da consulta. Um Atributo de bucket é um campo que armazena metadados específicos para um bucket.

No Macie, um filtro consiste em uma ou mais condições. Cada condição, também chamada de critério, consiste em três partes:

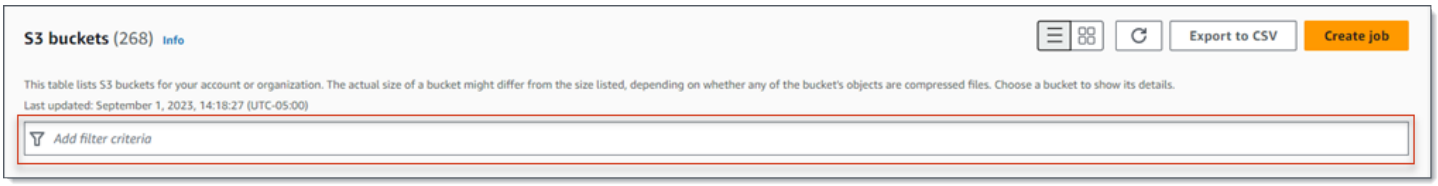
- Um campo baseado em atributos, como Nome do bucket, chave de tag ou definido no trabalho.
- Um operador, como igual ou não igual.
- Um ou mais valores. O tipo e o número de valores dependem do campo e do operador que você escolher.

A forma como você define e aplica as condições do filtro depende do uso do console do Amazon Macie ou da API do Amazon Macie.

Tópicos

Como filtrar o seu inventário no console do Amazon Macie

Se você usa o console do Amazon Macie para filtrar o seu inventário do bucket do S3, o Macie oferece opções para ajudá-lo a escolher campos, operadores e valores para condições individuais. Você acessa essas opções usando as configurações de filtro na página bucket do S3, conforme mostrado na imagem a seguir.

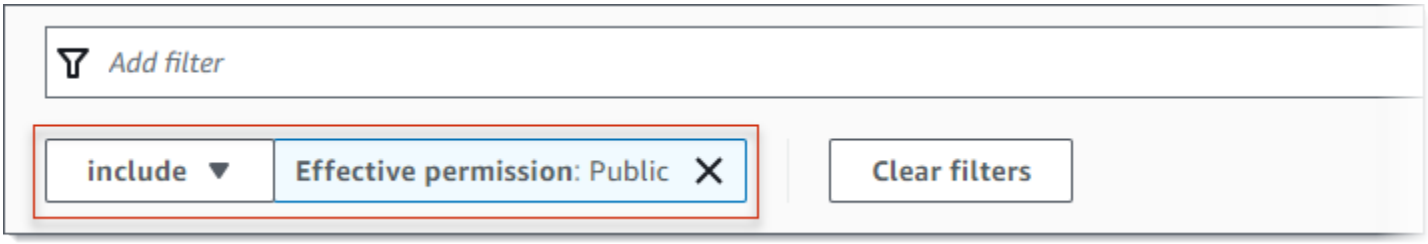


Quando você coloca o seu cursor na caixa Critérios de filtro, o Macie exibe uma lista de campos que você pode usar em condições do filtro. Os campos são organizados por categoria lógica. Por exemplo, a categoria Campos comuns inclui campos que armazenam informações gerais sobre um bucket do S3. As categorias de acesso público incluem campos que armazenam dados sobre os vários tipos de configurações de acesso público que podem ser aplicados a um bucket. Os campos são classificados em ordem alfabética dentro de cada categoria.

Para adicionar uma condição, comece escolhendo um campo na lista. Para encontrar um campo, navegue pela lista completa ou insira parte do nome do campo para restringir a lista de campos.

Dependendo do campo que você escolher, O Macie exibirá diferentes opções. As opções refletem o tipo e a natureza do campo escolhido. Por exemplo, se você escolher o campo Acesso compartilhado, o Macie exibirá uma lista de valores para escolher. Se você escolher o campo Nome do bucket, o Macie exibirá uma caixa de texto na qual você poderá inserir o nome de um bucket do S3. Seja qual for o campo escolhido, o Macie o guiará pelas etapas para adicionar uma condição que inclua as configurações necessárias para o campo.

Depois de adicionar uma condição, o Macie aplica os critérios para a condição e exibe a condição em um token de filtro abaixo da caixa de filtros, conforme mostrado na imagem a seguir.



Neste exemplo, a condição está configurada para incluir todos os buckets que são acessíveis ao público e excluir todos os outros buckets. Ele retorna buckets em que o valor do campo Permissão efetiva é igual a Público.

Conforme você adiciona mais condições, o Macie aplica seus critérios e os exibe abaixo da caixa de filtros. Se você adicionar várias condições, o Macie usa a lógica AND para unir as condições e avaliar os critérios de filtro. Isso significa que um bucket do S3 corresponde aos critérios de filtro somente se corresponder a todas as condições do filtro. Você pode consultar a área abaixo da caixa de filtros a qualquer momento para determinar quais critérios aplicou.

Para filtrar um inventário usando o console

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Buckets S3. A página Buckets do S3 exibirá seu inventário de buckets.
3. Na parte superior da página, selecione opcionalmente atualizar
   ()
   para recuperar os metadados mais recentes do bucket do Amazon S3.
4. Coloque o cursor na caixa de filtros e selecione o campo a ser usado para a condição.
5. Escolha ou insira o tipo de valor apropriado para o campo, tendo em mente as dicas a seguir.

   Datas, horas e intervalos de tempo

   Para datas e horas, use as caixas De e Para para definir um intervalo de tempo inclusivo:

   - Para definir um intervalo de tempo fixo, use as caixas De e Para para especificar a primeira data e hora e a última data e hora no intervalo, respectivamente.
   - Para definir um intervalo de tempo relativo que começa em uma determinada data e hora e termina na hora atual, insira a data e a hora de início nas caixas De e exclua qualquer texto nas caixas Para.

- Para definir um intervalo de tempo relativo que termina em uma determinada data e hora, insira a data e a hora de término nas caixas Para e exclua qualquer texto nas caixas De.

Observe que os valores de tempo usam a notação de 24 horas. Se você usar o seletor de datas para escolher datas, poderá refinar os valores inserindo texto diretamente nas caixas De e Para.

Números e intervalos numéricos

Para valores numéricos, use as caixas De e Para para inserir números inteiros que definam um intervalo numérico inclusivo:

- Para definir um intervalo numérico fixo, use as caixas De e Para para especificar os números mais baixos e mais altos no intervalo, respectivamente.
- Para definir um intervalo numérico fixo limitado a um valor específico, insira o valor nas caixas De e Para. Por exemplo, para incluir somente os buckets do S3 que contêm exatamente 15 objetos, insira **`15`** nas caixas De e Para.
- Para definir um intervalo numérico relativo que comece em um determinado número, insira o número na caixa De e não insira nenhum texto na caixa Para.
- Para definir um intervalo numérico relativo que termina em um determinado número, insira o número na caixa Para e não insira nenhum texto na caixa De.

Valores de texto (string)

Para esse tipo de valor, insira um valor completo e válido para o campo. Os valores diferenciam maiúsculas de minúsculas.

Observe que você não pode usar um valor parcial ou caracteres curinga nesse tipo de valor. A única exceção é o campo Nome do bucket. Para esse campo, você pode especificar um prefixo em vez de um nome completo do bucket. Por exemplo, para encontrar todos os buckets do S3 cujos nomes começam com my-s3, insira **`my-S3`** como valor do filtro para o campo Nome do bucket. Se você inserir qualquer outro valor, como **`My-s3`** ou **`my*`**, o Macie não retornará os buckets.

6. Ao terminar de adicionar um valor para o campo, selecione Aplicar. O Macie aplica os critérios de filtro e exibe a condição a um token de filtro abaixo da caixa de filtros.
7. Repita as etapas 4 a 6 para cada condição que deseja adicionar.
8. Para remover uma condição, selecione X no token de filtro da condição.
9. Para remover uma condição, remova a condição escolhendo X no token de filtro da condição. Em seguida, repita a etapa 4 a 6 para adicionar uma condição com as configurações corretas.

Como filtrar seu inventário de forma programática com a API do Amazon Macie

Para filtrar seu inventário de buckets do S3 de forma programática, especifique os critérios de filtro nas consultas que você envia usando a operação DescribeBuckets da API do Amazon. Essa operação retorna uma matriz de objetos. Cada objeto contém dados estatísticos e outras informações sobre um bucket que correspondem aos critérios de filtro.

Para especificar critérios de filtro em uma consulta, inclua um mapa das condições do filtro em sua solicitação. Para cada condição, você deve especificar um campo, um operador e um ou mais valores para o campo. O tipo e o número de valores dependem do campo e do operador que você escolher. Para obter informações sobre os campos, operadores e tipos de valores que você pode usar em uma condição, consulte Fontes de dados do Amazon S3 na Referência de API do Amazon Macie.

Os exemplos a seguir mostram como especificar critérios de filtro nas consultas enviadas usando o AWS Command Line Interface(AWS CLI). Você também pode fazer isso usando uma versão atual de outra AWS ferramenta de linha de comando ou de um AWS SDK, ou enviando solicitações HTTPS diretamente para o Macie. Para obter mais informações sobre AWS ferramentas e SDKs, consulte Ferramentas para aproveitar AWS.

Exemplos

- Exemplo 1: como encontrar buckets pelo nome do bucket
- Exemplo 2: como encontrar buckets que sejam acessíveis ao público
- Exemplo 3: como encontrar buckets que contêm objetos não criptografados
- Exemplo 4: como encontrar buckets que não são monitorados por um trabalho
- Exemplo 5: como encontrar buckets que replicam dados para contas externas
- Exemplo 6: como encontrar buckets base em vários critérios

Os exemplos usam o comando describe-buckets. Se um exemplo for executado com sucesso, o Macie retornará uma matriz `buckets`. A matriz contém um objeto para cada bucket que está no Região da AWS atual e corresponde aos critérios de filtro. Para ver um exemplo desse resultado, expanda a seguinte seção.

Exemplo de uma matriz **`buckets`**

Neste exemplo, a matriz `buckets` fornece detalhes sobre dois buckets que correspondem aos critérios de filtro especificados em uma 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
        }
    ]
}
```

Se nenhum bucket corresponder aos critérios de filtro, o Macie retornará uma matriz `buckets` vazia.

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

Exemplo 1: como encontrar buckets pelo nome do bucket

Este exemplo usa o comando describe-buckets para consultar metadados de todos os buckets cujos nomes começam com my-s3 e estão no atual. Região da AWS

Para Linux, macOS ou Unix:

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

Para o Microsoft Windows:

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

Onde:

- *bucketName* especifica o nome JSON do campo Nome do Bucket.
- *prefix* especifica o operador prefixo.
- *my-s3* é o valor do campo Nome do bucket.

Exemplo 2: como encontrar buckets que sejam acessíveis ao público

Este exemplo usa o comando describe-buckets para consultar metadados de buckets que estão no Região da AWS atual e, com base em uma combinação de configurações de permissões, estão acessíveis ao público.

Para Linux, macOS ou Unix:

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

Para o Microsoft Windows:

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

Onde:

- *publicAccess.effectivePermission* especifica o nome JSON do campo Permissão efetiva..
- *eq* especifica o operador igual.
- *PUBLIC* é um valor enumerado para o campo Permissão efetiva.

Exemplo 3: como encontrar buckets que contêm objetos não criptografados

Este exemplo usa o comando describe-buckets para consultar metadados de buckets que estão no Região da AWS atual e contêm objetos não criptografados.

Para Linux, macOS ou Unix:

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

Para o Microsoft Windows:

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

Onde:

- *objectCountByEncryptionType.unencrypted* especifica o nome JSON do campo Sem criptografia.
- *gte* especifica o operador maior ou igual a .
- *1* é o valor mais baixo em um intervalo numérico relativo e inclusivo para o campo Sem criptografia.

Exemplo 4: como encontrar buckets que não são monitorados por um trabalho

Este exemplo usa o comando describe-buckets para consultar metadados de buckets que estão no momento Região da AWS atual e não estão associados a nenhum trabalho periódico de descoberta de dados confidenciais.

Para Linux, macOS ou Unix:

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

Para o Microsoft Windows:

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

Onde:

- *jobDetails.isMonitoredByJob* especifica o nome JSON do campo Monitorado ativamente por trabalho.
- *eq* especifica o operador igual.
- *FALSE* é um valor enumerado para o campo Monitorado ativamente por trabalho.

Exemplo 5: como encontrar buckets que replicam dados para contas externas

Este exemplo usa o comando describe-buckets para consultar metadados de buckets que estão no Região da AWS atual e que estão configurados para replicar objetos para um Conta da AWS que não faz parte da sua organização.

Para Linux, macOS ou Unix:

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

Para o Microsoft Windows:

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

Onde:

- *replicationDetails.replicatedExternally* especifica o nome JSON do campo Replicado externamente.
- *eq* especifica o operador igual.
- *true* especifica um valor booleano para o campo Replicado externamente.

Exemplo 6: como encontrar buckets base em vários critérios

Este exemplo usa o comando describe-buckets para consultar metadados de buckets que estão no Região da AWS atual e que correspondem aos seguintes critérios: são acessíveis publicamente com base em uma combinação de configurações de permissão; contêm objetos não criptografados; e não estão associados a nenhum trabalho periódico de descoberta de dados confidenciais.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade:

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

Para o Microsoft Windows, usando o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade:

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

Onde:

- *publicAccess.effectivePermission* especifica o nome JSON do campo Permissão efetiva, e:
  - *eq* especifica o operador igual.
  - *PUBLIC* é um valor enumerado para o campo Permissão efetiva.
- *objectCountByEncryptionType.unencrypted* especifica o nome JSON do campo Sem criptografia, e:
  - *gte* especifica o operador maior ou igual a .

  - *1* é o valor mais baixo em um intervalo numérico relativo e inclusivo para o campo Sem criptografia.
- *jobDetails.isMonitoredByJob* especifica o nome JSON do campo Monitorado ativamente por trabalho, e:
  - *eq* especifica o operador igual.
  - *FALSE* é um valor enumerado para o campo Monitorado ativamente por trabalho.

Permitindo que o Amazon Macie acesse buckets e objetos do S3

Quando você habilita o Amazon Macie para sua Conta da AWS, o Macie cria um perfil vinculado a serviços que concede ao Macie as permissões necessárias para chamar o Amazon Simple Storage Service (Amazon S3) e outros Serviços da AWS em seu nome. Um perfil vinculado a serviços simplifica o processo de configuração de um AWS service (Serviço da AWS), pois você não precisa adicionar manualmente as permissões para o serviço concluir as ações em seu nome. Para saber mais sobre esse tipo de perfil, consulte Usando perfis vinculados a serviços no Guia do usuário AWS Identity and Access Management.

A política de permissões para o perfil vinculado a serviços do Macie (`AWSServiceRoleForAmazonMacie`) permite que o Macie execute ações que incluem recuperar informações sobre buckets e objetos do S3 e recuperar objetos de buckets. Se você for o administrador do Macie de uma organização, a política também permite que o Macie execute essas ações em seu nome para contas-membro em sua organização.

O Macie usa essas permissões para executar tarefas como:

- Gerar e manter um inventário de seus buckets do S3
- Fornecer dados estatísticos e outros dados sobre os buckets e objetos nos buckets
- Monitorar e avaliar os buckets quanto à segurança e o controle de acesso
- Analisar objetos nos buckets para detectar dados confidenciais

Na maioria dos casos, o Macie tem as permissões necessárias para realizar essas tarefas. No entanto, se um bucket do S3 tiver uma política restritiva de bucket, a política poderá impedir que o Macie execute algumas ou todas essas tarefas.

Uma política de bucket é uma política do (IAM) AWS Identity and Access Management baseada em recursos que especifica quais ações uma entidade principal (usuário, conta, serviço ou outra

entidade) pode realizar em um bucket do S3, bem como as condições em que uma entidade principal pode realizar essas ações. As ações e condições podem ser aplicadas a operações em nível de bucket, como a recuperação de informações sobre um bucket, e a operações em nível de objeto, como a recuperação de objetos de um bucket.

Geralmente, as políticas de bucket concedem ou restringem o acesso usando instruções e condições explícitas `Allow` ou `Deny`. Por exemplo, uma política de buckets pode conter uma instrução `Allow` ou `Deny` que nega acesso a um bucket, a menos que endereços IP de origem específicos. endpoints do Amazon Virtual Private Cloud (Amazon VPC) ou VPCs sejam usados para acessar o bucket. Para obter informações sobre como usar políticas de buckets para conceder ou restringir o acesso aos buckets, consulte as Políticas de buckets e políticas de usuário e Como o Amazon S3 autoriza uma solicitação no Guia do Usuário do Serviço Amazon Simple Storage.

Se uma política de bucket usa uma instrução `Allow` explícita, a política não impede que o Macie recupere informações sobre o bucket e os objetos do bucket, nem que ele recupere objetos do bucket. Isso ocorre porque as instruções `Allow` na política de permissões para o perfil vinculado a serviços do Macie concedem essas permissões.

No entanto, se uma política de bucket usa uma instrução `Deny` explícita com uma ou mais condições, talvez o Macie não tenha permissão para recuperar informações sobre o bucket ou os objetos do bucket, nem de recuperar os objetos do bucket. Por exemplo, se uma política de bucket negar explicitamente o acesso de todas as fontes, salvo de um endereço IP específico, o Macie não poderá analisar os objetos do bucket quando você executar um trabalho de descoberta de dados confidenciais. Isso ocorre porque as políticas de bucket restritivas têm precedência sobre as instruções `Allow` na política de permissões para o perfil vinculado a serviços do Macie.

Para permitir que o Macie acesse um bucket do S3 que tenha uma política restritiva de bucket, você pode adicionar uma condição para o perfil vinculado a serviços do Macie (`AWSServiceRoleForAmazonMacie`) à política do bucket. A condição pode impedir que o perfil vinculado a serviços do Macie corresponda à restrição `Deny` na política. Ela pode fazer isso usando a chave de contexto de condição global `aws:PrincipalArn` e o nome do recurso da Amazon (ARN) do perfil vinculado a serviços do Macie.

O procedimento a seguir orientará você durante esse processo e fornecerá um exemplo.

Para adicionar o perfil vinculado a serviços do Macie a uma política de bucket

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. No painel de navegação, escolha Buckets.
3. Selecione o bucket do S3 que você deseja que o Macie acesse.
4. Na guia Permissions (Permissões), escolha Bucket policy (Política de bucket), Edit (Editar).
5. No editor Políticas do Bucket, identifique cada instrução `Deny` que restringe o acesso e impede que o Macie acesse o bucket ou os objetos do bucket.
6. Em cada instrução `Deny`, adicione uma condição que use a chave de contexto de condição global `aws:PrincipalArn` e especifique o ARN do perfil vinculado a serviços do Macie para sua Conta da AWS.

   O valor da chave de condição deve ser `arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, em que *`123456789012`* é o ID da conta da sua Conta da AWS.

Onde você adiciona isso a uma política de bucket depende da estrutura, dos elementos e das condições que a política contém atualmente. Para saber mais sobre estruturas e elementos compatíveis, consulte Políticas e permissões no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Veja a seguir um exemplo de uma política de bucket que usa uma instrução `Deny` explícita para restringir o acesso a um bucket do S3 chamado DOC-EXAMPLE-BUCKET. Com a política atual, o bucket só pode ser acessado a partir do endpoint da VPC cujo ID é `vpce-1a2b3c4d`. O acesso de todos os outros endpoints da VPC é negado, incluindo o acesso do AWS Management Console e do Macie.

```
{
   "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 alterar essa política e permitir que o Macie acesse o bucket do S3 e os objetos do bucket, podemos adicionar uma condição que usa o operador de condição `StringNotLike` e a chave de contexto de condição global `aws:PrincipalArn`. Essa condição adicional impede que o perfil vinculado a serviços do Macie corresponda à restrição `Deny`.

```
{
   "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"
            }
         }
      }
   ]
}
```

No exemplo anterior, o operador da condição `StringNotLike` usa a chave de contexto de condição `aws:PrincipalArn` para especificar o ARN do perfil vinculado a serviços do Macie, onde:

- `123456789012` é o ID da conta para a Conta da AWS que tem permissão para usar o Macie para recuperar informações sobre o bucket e os objetos do bucket e recuperar objetos do bucket.
- `macie.amazonaws.com` é o identificador da entidade principal de serviço do Macie.
- `AWSServiceRoleForAmazonMacie` é o nome do perfil vinculado a serviços do Macie.

Usamos o operador `StringNotLike` porque a política já usa um operador `StringNotEquals`. Uma política só pode usar o operador `StringNotEquals` uma vez.

Para obter outros exemplos de políticas e informações detalhadas sobre o gerenciamento aos recursos do Amazon S3, consulte Gerenciamento de identidade e acesso no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Descobrindo dados confidenciais com o Amazon Macie

Com o Amazon Macie, é possível automatizar a descoberta, o registro e o relato de dados confidenciais em seu estado de dados do Amazon Simple Storage Service (Amazon S3) Você pode fazer isso de duas maneiras: configurando o Macie para realizar a descoberta automatizada de dados confidenciais para sua conta ou organização e criando e executando trabalhos de descoberta de dados confidenciais para sua conta ou organização.

Descoberta automatizada de dados confidenciais

A descoberta automatizada de dados confidenciais fornece ampla visibilidade sobre onde os dados confidenciais podem residir em seu patrimônio de dados do Amazon S3. Com essa opção, o Macie avalia diariamente seu inventário de buckets do S3 e usa técnicas de amostragem para identificar e selecionar objetos representativos do S3 em seus buckets. Em seguida, o Macie recupera e analisa os objetos selecionados, inspecionando-os em busca de dados confidenciais. Para obter mais informações, consulte Realizando a descoberta automatizada de dados confidenciais.

Trabalho de descoberta de dados confidenciais

Trabalhos confidenciais de descoberta de dados fornecem uma análise mais profunda e direcionada. Com essa opção, você define a amplitude e a profundidade da análise — buckets do S3 específicos que você seleciona ou buckets que correspondem a critérios específicos. Você também pode refinar o escopo da análise escolhendo opções, como os critérios personalizados que derivam das propriedades dos objetos do S3. Além disso, você também pode configurar um trabalho para ser executado somente uma vez para análise e avaliação sob demanda, ou de forma recorrente para análise, avaliação e monitoramento periódicos. Para obter mais informações, consulte Executando trabalhos de descoberta de dados confidenciais.

Com qualquer uma das opções, a descoberta automatizada de dados confidenciais ou os trabalhos de descoberta de dados confidenciais, é possível analisar objetos do S3 usando identificadores de dados gerenciados que o Macie fornece, identificadores de dados personalizados que você define ou uma combinação dos dois. Você também pode refinar a análise usando listas de permissões.

Identificadores de dados gerenciados

Os identificador de dados gerenciados são critérios e técnicas integrados que são projetados para detectar tipos específicos de dados confidenciais, como, por exemplo, números de

cartão de crédito, chaves de acesso secretas AWS ou números de passaporte para um determinado país ou região. Eles podem detectar uma lista grande e em crescimento de tipos de dados confidenciais para muitos países e regiões, incluindo vários tipos de dados de credenciais, informações financeiras e informações de identificação pessoal (PII). Para obter mais informações, consulte Usar identificadores de dados gerenciados.

Identificadores de dados personalizados

Os identificadores de dados personalizado definem critérios personalizados para detectar dados confidenciais. Cada identificador de dados personalizados especifica uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados. É possível usá-los para detectar dados confidenciais que refletem determinados cenários, propriedade intelectual ou dados proprietários, como, por exemplo, IDs de funcionários, números de contas de clientes ou classificações de dados internos. Para obter mais informações, consulte Criar identificadores de dados personalizados.

Listas de permissões

No Macie, as listas de permissões especificam texto e padrões de texto a serem ignorados nos objetos do S3, geralmente exceções de dados confidenciais para seus cenários ou ambientes específicos, como, por exemplo, nomes públicos ou números de telefone da sua organização ou dados de amostra que sua organização usa para testes. Se o Macie encontrar um textos que corresponda a uma entrada ou um padrão em uma lista de permissões, o Macie não reportará essa ocorrência de texto, mesmo que os dados correspondam aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizados. Para obter mais informações, consulte Como definir exceções de dados sigilosos com listas de permissões.

Quando o Amazon Macie analisa um objeto do S3, o Macie recupera a versão mais recente do objeto do Amazon S3 e, em seguida, realiza uma inspeção profunda do conteúdo do objeto. O Macie pode analisar um objeto se o seguinte for verdadeiro:

- O objeto usa um arquivo ou formato de armazenamento compatível e é armazenado diretamente no Amazon S3 usando uma classe de armazenamento compatível. Para obter mais informações, consulte Classes e formatos de armazenamento suportados.
- Se o objeto for criptografado, ele é criptografado com uma chave que o Macie pode acessar e tem permissão para usar. Para obter mais informações, consulte Analisando objetos criptografados do S3.

- Se o objeto estiver armazenado em um bucket que tenha uma política de bucket restritiva, a política permitirá que o Macie acesse objetos no bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Para ajudá-lo a atender e manter a conformidade com seus requisitos de segurança e privacidade de dados, o Macie produz registros dos dados confidenciais que encontra e da análise que realiza — descobertas de dados confidenciais e resultados de descobertas de dados confidenciais. Uma descoberta de dados confidenciais é um relatório detalhado de dados confidenciais que o Macie encontrou em um objeto do S3. Um resultado de descoberta de dados confidenciais é um registro de detalhes sobre a análise de um objeto. Cada tipo de registro segue um esquema padronizado, que pode ajudá-lo a consultá-los, monitorá-los e processá-los usando outros aplicativos, serviços e sistemas, conforme necessário.

> **Tip**
>
> Embora o Macie seja otimizado para o Amazon S3, você pode usá-lo para descobrir dados confidenciais em recursos que você atualmente armazena em outro lugar. Você pode fazer isso movendo os dados para o Amazon S3 temporariamente ou permanentemente. Por exemplo, exporte os snapshots do Serviço do banco de dados relacional Amazon ou do Amazon Aurora para o Amazon S3 no formato Apache Parquet. Ou exporte uma tabela do Amazon DynamoDB para o Amazon S3. Em seguida, você pode criar um trabalho confidencial de descoberta de dados para analisar os dados no Amazon S3.

Tópicos

Usar identificadores de dados gerenciados no Amazon Macie

O Amazon Macie usa uma combinação de critérios e técnicas, incluindo machine learning e correspondência de padrões, para detectar dados confidenciais em objetos do Amazon Simple Storage Service (Amazon S3). Esses critérios e técnicas, coletivamente denominados identificadores de dados gerenciados, podem detectar uma lista grande e crescente de tipos de dados confidenciais para muitos países e regiões, incluindo vários tipos de dados de credenciais, informações financeiras, informações pessoais de saúde (PHI) e informações de identificação pessoal (PII). Cada identificador de dados gerenciado é projetado para detectar um tipo específico de dados sigilosos - por exemplo, AWS chaves de acesso secretas, números de cartão de crédito ou números de passaporte de um determinado país ou região.

O Macie pode detectar as seguintes categorias de dados sigilosos usando identificadores de dados gerenciados:

- Credenciais, para dados de credenciais, como chaves privadas e AWS chaves de acesso secretas.
- Informações financeiras, para dados financeiros, como números de cartão de crédito e números de conta bancária.
- Informações pessoais, para PHI, como seguro saúde e números de identificação médica, e PII, como números de identificação de carteira de motorista e números de passaporte.

Dentro de cada categoria, o Macie pode detectar vários tipos de dados confidenciais. Os tópicos dessa seção listam e descrevem cada tipo e todos os requisitos relevantes para detectá-lo. Para cada tipo, eles também indicam o identificador exclusivo (ID) do identificador de dados gerenciados projetado para detectar os dados. Ao criar um trabalho de descoberta de dados confidenciais ou definir configurações automatizadas de descoberta de dados confidenciais, você pode usar essas IDs para especificar quais identificadores de dados gerenciados você deseja que o Macie use ao analisar objetos do S3.

Para obter uma lista de identificadores de dados gerenciados que recomendamos para trabalhos, consulte Identificadores de dados gerenciados recomendados para trabalhos de descoberta de dados sigilosos. Para obter uma lista de identificadores de dados gerenciados que recomendamos e que são usados por padrão para a descoberta automatizada de dados confidenciais, consulte Configurações padrão para descoberta automatizada de dados confidenciais.

Tópicos

Requisitos de palavras-chave para identificadores de dados gerenciados do Amazon Macie

Para detectar determinados tipos de dados confidenciais usando identificadores de dados gerenciados, o Amazon Macie exige que uma palavra-chave esteja próxima aos dados. Se esse for o caso de determinado tipo de dado, um tópico posterior nesta seção indicará requisitos específicos da palavra-chave para esses dados.

Se uma palavra-chave precisar estar próxima de um tipo específico de dados, a palavra-chave normalmente precisará estar dentro de 30 caracteres (inclusive) dos dados. Os requisitos adicionais de proximidade variam com base no tipo de arquivo ou no formato de armazenamento de um objeto do Amazon Simple Storage Service (Amazon S3).

Dados estruturados e colunares

> Para dados colunares, uma palavra-chave precisa fazer parte do mesmo valor ou estar no nome da coluna ou campo que armazena um valor. Isso vale para pastas de trabalho do Microsoft Excel, arquivos CSV e arquivos TSV.
>
> Por exemplo, se o valor de um campo contiver SSN e um número de nove dígitos que usa a sintaxe de um número do Seguro Social dos EUA (SSN), o Macie poderá detectar o SSN no campo. Da mesma forma, se o nome de uma coluna contiver SSN, o Macie poderá detectar cada SSN na coluna. O Macie trata os valores nessa coluna como se estivessem próximos da palavra-chave SSN.

Dados estruturados e baseados em registros

> Para dados baseados em registros, uma palavra-chave precisa fazer parte do mesmo valor ou estar no nome de um elemento do caminho para o campo ou matriz que armazena um valor. Isso vale para contêineres de objetos Apache Avro, arquivos Apache Parquet, arquivos JSON e arquivos JSON Lines.
>
> Por exemplo, se o valor de um campo contém credenciais e uma sequência de caracteres que usa a sintaxe de uma chave de acesso secreta AWS, o Macie pode detectar a chave no campo. Da mesma forma, se o caminho para um campo for `$.credentials.aws.key`, o Macie poderá

detectar uma chave de acesso secreta AWS no campo. O Macie trata o valor no campo como estando próximo às credenciais da palavra-chave.

Dados não estruturados

Não há requisitos adicionais de proximidade para arquivos Adobe Portable Document Format, documentos do Microsoft Word, mensagens de e-mail e arquivos de texto não binários, exceto arquivos CSV, JSON, JSON Lines e TSV. Uma palavra-chave normalmente precisa estar dentro de 30 caracteres (inclusive) dos dados. Isso inclui quaisquer dados estruturados, como tabelas, nesses tipos de arquivos.

As palavras-chave não diferenciam maiúsculas de minúsculas. Além disso, se uma palavra-chave contiver um espaço, o Macie faz automaticamente a correspondência com as variações de palavras-chave que não contêm o espaço ou contêm um sublinhado (_) ou um hífen (-) em vez do espaço. Em certos casos, o Macie também estende ou abrevia uma palavra-chave para abordar variações comuns da palavra-chave.

Para uma demonstração de como as palavras-chave fornecem contexto e ajudam o Macie a detectar tipos específicos de dados confidenciais, assista ao vídeo a seguir: Como o Amazon Macie usa palavras-chave para descobrir dados confidenciais.

Referência rápida: identificadores de dados gerenciados pelo Amazon Macie

No Amazon Macie, um identificador de dados gerenciados é um conjunto de critérios e técnicas incorporados projetados para detectar um tipo específico de dados confidenciais, por exemplo, números de cartão de crédito, chaves de acesso AWS secretas ou números de passaportes de um determinado país ou região. Esses identificadores podem detectar uma lista grande e crescente de tipos de dados confidenciais para muitos países e regiões, incluindo vários tipos de dados de credenciais, informações financeiras, informações pessoais de saúde (PHI) e informações de identificação pessoal (PII).

A tabela a seguir lista todos os identificadores de dados gerenciados que o Macie fornece atualmente, organizados por tipo de dados confidenciais. Para cada tipo, ela fornece as seguintes informações:

- Categoria de dados confidenciais — especifica a categoria geral de dados confidenciais que inclui o tipo: Credenciais, para dados de credenciais, como chaves privadas; Informações financeiras,

para dados financeiros, como números de cartão de crédito e números de contas bancárias; Informações pessoais: PHI para informações pessoais de saúde, como seguro saúde e números de identificação médica; e Informações pessoais: PII para informações de identificação pessoal, como números de identificação de carteira de motorista e números de passaporte.

- ID do identificador de dados gerenciado — Especifica o identificador exclusivo (ID) de um ou mais identificadores de dados gerenciados projetados para detectar os dados. Ao criar um trabalho de descoberta de dados confidenciais ou definir configurações automatizadas de descoberta de dados confidenciais, você pode usar essas IDs para especificar quais identificadores de dados gerenciados você deseja que o Macie use ao analisar dados. Para obter uma lista de identificadores de dados gerenciados que recomendamos para trabalhos, consulte Identificadores de dados gerenciados recomendados para trabalhos de descoberta de dados sigilosos.
  Para obter uma lista de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais, consulte Configurações padrão para descoberta automatizada de dados confidenciais.
- Palavra-chave obrigatória — Especifica se a detecção exige que uma palavra-chave esteja próxima aos dados. Para obter informações sobre como o Macie usa palavras-chave ao analisar dados, consulte Requisitos de palavras-chave.
- Países e regiões — especifica para quais países ou regiões os identificadores de dados gerenciados aplicáveis foram projetados. Se os identificadores de dados gerenciados não forem projetados para determinados países ou regiões, esse valor será Qualquer.

Para revisar detalhes adicionais sobre os identificadores de dados gerenciados para um tipo específico de dados confidenciais, selecione o tipo.

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Chave de acesso secreta da AWS	Credenciais	AWS_CREDENTIALS	Sim	Any

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de conta bancária	Informações financeiras	BANK_ACCOUNT_NUMBER (para o Canadá e os EUA)	Sim	Canadá, EUA
Número básico da conta bancária (BBAN)	Informações financeiras	Dependendo do país ou região: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Sim	França, Alemanha, Itália, Espanha, Reino Unido
Datas de nascimento	Informações pessoais: PII	DATE_OF_BIRTH	Sim	Any
Data de validade do cartão de crédito	Informações financeiras	CREDIT_CARD_EXPIRATION	Sim	Any
Dados da tarja magnética do cartão de crédito	Informações financeiras	CREDIT_CARD_MAGNETIC_STRIPE	Sim	Any

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Números de cartão de crédito	Informações financeiras	CREDIT_CARD_NUMBER (para números de cartão de crédito próximos a uma palavra-chave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (para números de cartão de crédito que não estejam próximos de uma palavra-chave)	Varia	Any
Código de verificação do cartão de crédito	Informações financeiras	CREDIT_CARD_SECURITY_CODE	Sim	Any

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de identificação da carteira de habilitação	Informações pessoais: PII	Dependendo do país ou região: 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	Sim	Austrália, Áustria, Bélgica, Bulgária, Canadá, Croácia, Chipre, República Checa, Dinamarca, Estónia, Finlândia, França, Alemanha, Grécia, Hungria, Índia, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Romênia, Eslováquia, Eslovênia

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, Espanha, Suécia, Reino Unido, EUA
Número de registro da Agência Antidrogas (DEA)	Informações pessoais: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sim	EUA
Número de registro eleitoral	Informações pessoais: PII	UK_ELECTORAL_ROLL_NUMBER	Sim	Reino Unido
Nome completo	Informações pessoais: PII	NAME	Não	Qualquer, se o nome usar um conjunto de caracteres latinos

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Coordenadas do sistema de posicionamento global (GPS)	Informações pessoais: PII	LATITUDE_LONGITUDE	Sim	Qualquer, se as coordenadas estiverem próximas de uma palavra-chave em inglês
Chave da API do Google Cloud	Credenciais	GCP_API_KEY	Sim	Any
Número de solicitação de seguro saúde (HICN)	Informações pessoais: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sim	EUA
Número de identificação médica ou do seguro de saúde	Informações pessoais: PHI	Dependendo do país ou região: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sim	Canadá, UE, Finlândia, França, Reino Unido, EUA

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Código do Healthcare Common Procedure Coding System (HCPCS)	Informações pessoais: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sim	EUA
Cabeçalho de autorização básica HTTP	Credenciais	HTTP_BASIC_AUTH_HEADER	Não	Any
Cookie HTTP	Informações pessoais: PII	HTTP_COOKIE	Não	Any

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número internacional de conta bancária (IBAN)	Informações financeiras	Dependendo do país ou região: 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,	Não	Albânia, Andorra, Bósnia-Herzegovina, Brasil, Bulgária, Costa Rica, Croácia, Chipre, República Checa, Dinamarca, República Dominicana, Egito, Estónia, Ilhas Faroé, Finlândia, França, Geórgia, Alemanha, Grécia, Groelândia, Hungria, Islândia, Irlanda, Itália, Jordânia, Kosovo,

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		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,		Liechtenstein, Lituânia, Malta, Mauritânia, Maurícias, Mónaco, Montenegro, Países Baixos, Macedônia do Norte, Polónia, Portugal, São Marino, Senegal, Sérvia, Eslováquia, Eslovênia, Espanha, Suécia, Suíça, Timor-Leste, Tunísia, Turquia, Reino Unido, Ucrânia, Emirados Árabes

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(para as Ilhas Virgens Britânicas)		Unidos, Ilhas Virgens (Britânicas)
JSON Web Token (JWT)	Credenciais	JSON_WEB_TOKEN	Não	Any
Endereço postal	Informações pessoais: PII	ADDRESS, BRAZIL_CEP_CODE (para o Código de Endereçamento Postal do Brasil)	Varia	Austrália, Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA
National Drug Code (NDC)	Informações pessoais: PHI	USA_NATIONAL_DRUG_CODE	Sim	EUA

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de identificação nacional	Informações pessoais: PII	Dependendo do país ou região: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Sim	Brasil, França, Alemanha, Índia, Itália, Espanha
Número do Seguro Nacional (NINO)	Informações pessoais: PII	UK_NATIONAL_INSURANCE_NUMBER	Sim	Reino Unido
National Provider Identifier (NPI)	Informações pessoais: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sim	EUA
Chave privada OpenSSH	Credenciais	OPENSSH_PRIVATE_KEY	Não	Any
Número de passaporte	Informações pessoais: PII	Dependendo do país ou região: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sim	Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de residência permanente	Informações pessoais: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Sim	Canadá
Chave privada PGP	Credenciais	PGP_PRIVATE_KEY	Não	Any
Número de telefone	Informações pessoais: PII	Dependendo do país ou região: 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	Varia	Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA
Chave privada do padrão de criptografia de chave pública (PKCS)	Credenciais	PKCS	Não	Any
Chave privada PuTTY	Credenciais	PUTTY_PRIVATE_KEY	Não	Any

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número do Seguro Social (SIN)	Informações pessoais: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sim	Canadá
Número da Previdência Social (SSN)	Informações pessoais: PII	Dependendo do país ou região: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sim	Espanha, EUA
the section called “Chave da API Stripe”	Credenciais	STRIPE_CREDENTIALS	Não	Any
Identificação do contribuinte ou número de referência	Informações pessoais: PII	Dependendo do país ou região: 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	Sim	Austrália, Brasil, França, Alemanha, Índia, Itália, Espanha, Reino Unido, EUA

Tipo de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Identificador exclusivo de dispositivo (UDI)	Informações pessoais: PHI	MEDICAL_DEVICE_UDI	Sim	EUA
Número de identificação de veículo (VIN)	Informações pessoais: PII	VEHICLE_IDENTIFICATION_NUMBER	Sim	Qualquer um, se o VIN estiver próximo a uma palavra-chave em um dos seguintes idiomas: inglês, francês, alemão, lituano, polonês, português, romeno ou espanhol

Referência detalhada: identificadores de dados gerenciados pelo Amazon Macie

No Amazon Macie, identificadores de dados gerenciados são técnicas e critérios incorporados projetados para detectar tipos específicos de dados sigilosos. Eles podem detectar uma lista grande e crescente de tipos de dados confidenciais para muitos países e regiões, incluindo vários tipos de

dados de credenciais, informações financeiras e informações pessoais. Cada identificador de dados gerenciados é projetado para detectar um tipo específico de dados confidenciais — por exemplo, AWS chaves de acesso secretas, números de cartão de crédito ou números de passaporte de um determinado país ou região.

O Macie pode detectar as seguintes categorias de dados sigilosos usando identificadores de dados gerenciados: Em cada categoria, o Macie pode detectar vários tipos de dados sigilosos. Os tópicos nesta seção listam e descrevem cada tipo e quaisquer requisitos relevantes para detectar os dados. Para obter detalhes sobre os identificadores de dados gerenciados para tipos específicos de dados confidenciais, você pode navegar pelos tópicos por categoria:

- Credenciais — Para dados de credenciais, como chaves privadas e chaves de acesso AWS secretas.
- Informações financeiras, para dados financeiros, como números de cartão de crédito e números de conta bancária.
- Informações pessoais: PHI — Para informações pessoais de saúde (PHI), como seguro saúde e números de identificação médica.
- Informações pessoais: PII — Para informações de identificação pessoal (PII), como números de identificação da carteira de motorista e números de passaporte.

Ou você pode escolher um tipo específico de dados confidenciais na tabela a seguir. A tabela lista todos os identificadores de dados gerenciados que o Macie fornece atualmente, organizados por tipo de dados confidenciais. A tabela também resume os requisitos relevantes para a detecção de cada tipo.

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Chave de acesso secreta da AWS	Credenciais	AWS_CREDENTIALS	Sim	Any

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de conta bancária	Informações financeiras	BANK_ACCOUNT_NUMBER (para o Canadá e os EUA)	Sim	Canadá, EUA
Número básico da conta bancária (BBAN)	Informações financeiras	Dependendo do país ou região: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Sim	França, Alemanha, Itália, Espanha, Reino Unido
Datas de nascimento	Informações pessoais: PII	DATE_OF_BIRTH	Sim	Any
Data de validade do cartão de crédito	Informações financeiras	CREDIT_CARD_EXPIRATION	Sim	Any
Dados da tarja magnética do cartão de crédito	Informações financeiras	CREDIT_CARD_MAGNETIC_STRIPE	Sim	Any

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Números de cartão de crédito	Informações financeiras	CREDIT_CARD_NUMBER (para números de cartão de crédito próximos a uma palavra-chave), CREDIT_CARD_NUMBER_(NO_KEYWORD) (para números de cartão de crédito que não estejam próximos de uma palavra-chave)	Varia	Any
Código de verificação do cartão de crédito	Informações financeiras	CREDIT_CARD_SECURITY_CODE	Sim	Any

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de identificação da carteira de habilitação	Informações pessoais: PII	Dependendo do país ou região: 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	Sim	Austrália, Áustria, Bélgica, Bulgária, Canadá, Croácia, Chipre, República Checa, Dinamarca, Estónia, Finlândia, França, Alemanha, Grécia, Hungria, Índia, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Romênia, Eslováquia, Eslovênia

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		, Espanha, Suécia, Reino Unido, EUA
Número de registro da Agência Antidrogas (DEA)	Informações pessoais: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Sim	EUA
Número de registro eleitoral	Informações pessoais: PII	UK_ELECTORAL_ROLL_NUMBER	Sim	Reino Unido
Nome completo	Informações pessoais: PII	NAME	Não	Qualquer, se o nome usar um conjunto de caracteres latinos

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Coordenadas do sistema de posicionamento global (GPS)	Informações pessoais: PII	LATITUDE_LONGITUDE	Sim	Qualquer, se as coordenadas estiverem próximas de uma palavra-chave em inglês
Chave da API do Google Cloud	Credenciais	GCP_API_KEY	Sim	Any
Número de solicitação de seguro saúde (HICN)	Informações pessoais: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Sim	EUA
Número de identificação médica ou do seguro de saúde	Informações pessoais: PHI	Dependendo do país ou região: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Sim	Canadá, UE, Finlândia, França, Reino Unido, EUA

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Código do Healthcare Common Procedure Coding System (HCPCS)	Informações pessoais: PHI	USA_HEALTHCARE_PROCEDURE_CODE	Sim	EUA
Cabeçalho de autorização básica HTTP	Credenciais	HTTP_BASIC_AUTH_HEADER	Não	Any
Cookie HTTP	Informações pessoais: PII	HTTP_COOKIE	Não	Any

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número internacional de conta bancária (IBAN)	Informações financeiras	Dependendo do país ou região: 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,	Não	Albânia, Andorra, Bósnia-Herzegovina, Brasil, Bulgária, Costa Rica, Croácia, Chipre, República Checa, Dinamarca, República Dominicana, Egito, Estónia, Ilhas Faroé, Finlândia, França, Geórgia, Alemanha, Grécia, Groelândia, Hungria, Islândia, Irlanda, Itália, Jordânia, Kosovo,

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		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,		Liechtenstein, Lituânia, Malta, Mauritânia, Maurícias, Mónaco, Montenegro, Países Baixos, Macedônia do Norte, Polónia, Portugal, São Marino, Senegal, Sérvia, Eslováquia, Eslovênia, Espanha, Suécia, Suíça, Timor-Leste, Tunísia, Turquia, Reino Unido, Ucrânia, Emirados Árabes

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(para as Ilhas Virgens Britânicas)		Unidos, Ilhas Virgens (Britânicas)
JSON Web Token (JWT)	Credenciais	JSON_WEB_TOKEN	Não	Any
Endereço postal	Informações pessoais: PII	ADDRESS, BRAZIL_CEP_CODE (para o Código de Endereçamento Postal do Brasil)	Varia	Austrália, Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA
National Drug Code (NDC)	Informações pessoais: PHI	USA_NATIONAL_DRUG_CODE	Sim	EUA

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de identificação nacional	Informações pessoais: PII	Dependendo do país ou região: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Sim	Brasil, França, Alemanha, Índia, Itália, Espanha
Número do Seguro Nacional (NINO)	Informações pessoais: PII	UK_NATIONAL_INSURANCE_NUMBER	Sim	Reino Unido
National Provider Identifier (NPI)	Informações pessoais: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Sim	EUA
Chave privada OpenSSH	Credenciais	OPENSSH_PRIVATE_KEY	Não	Any
Número de passaporte	Informações pessoais: PII	Dependendo do país ou região: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Sim	Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número de residência permanente	Informações pessoais: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Sim	Canadá
Chave privada PGP	Credenciais	PGP_PRIVATE_KEY	Não	Any
Número de telefone	Informações pessoais: PII	Dependendo do país ou região: 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	Varia	Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA
Chave privada do padrão de criptografia de chave pública (PKCS)	Credenciais	PKCS	Não	Any
Chave privada PuTTY	Credenciais	PUTTY_PRIVATE_KEY	Não	Any

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Número do Seguro Social (SIN)	Informações pessoais: PII	CANADA_SOCIAL_INSURANCE_NUMBER	Sim	Canadá
Número da Previdência Social (SSN)	Informações pessoais: PII	Dependendo do país ou região: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Sim	Espanha, EUA
the section called “Chave da API Stripe”	Credenciais	STRIPE_CREDENTIALS	Não	Any
Identificação do contribuinte ou número de referência	Informações pessoais: PII	Dependendo do país ou região: 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	Sim	Austrália, Brasil, França, Alemanha, Índia, Itália, Espanha, Reino Unido, EUA

Tipos de dados confidenciais	Categoria de dados confidenciais	ID do identificador de dados gerenciados	Palavra-chave obrigatória	Países e regiões
Identificador exclusivo de dispositivo (UDI)	Informações pessoais: PHI	MEDICAL_DEVICE_UDI	Sim	EUA
Número de identificação de veículo (VIN)	Informações pessoais: PII	VEHICLE_IDENTIFICATION_NUMBER	Sim	Qualquer um, se o VIN estiver próximo a uma palavra-chave em um dos seguintes idiomas: inglês, francês, alemão, lituano, polonês, português, romeno ou espanhol

Identificadores de dados gerenciados para dados de credenciais

O Amazon Macie pode detectar vários tipos de dados de credenciais confidenciais usando identificadores de dados gerenciados. Os tópicos desta página especificam cada tipo e fornecem informações sobre o identificador de dados gerenciados projetado para detectar os dados. Cada tópico fornece as seguintes informações:

- ID do identificador de dados gerenciado — especifica o identificador exclusivo (ID) do identificador de dados gerenciados projetado para detectar os dados. Ao criar um trabalho de descoberta de dados confidenciais ou definir as configurações de descobertas automatizadas de dados confidenciais, você pode usar esse ID para especificar se você pode quer que o Macie use o identificados de dados gerenciados quando ele analisa os dados.
- Países e regiões compatíveis — indica para quais países ou regiões os identificadores de dados gerenciados pertinentes foram projetados. Se o identificador de dados gerenciados não for projetado para determinados países ou regiões, esse valor será Qualquer.
- Palavra-chave obrigatória — especifica se a detecção exige que uma palavra-chave esteja próxima aos dados. Se uma palavra-chave for necessária, o tópico também fornecerá exemplos de palavras-chave obrigatórias. Para obter informações sobre como o Macie usa palavras-chave ao analisar dados, consulte Requisitos de palavras-chave.
- Comentários — Fornece todos os detalhes relevantes que possam afetar sua selecione de identificador de dados gerenciados ou sua investigação sobre ocorrências relatadas de dados confidenciais. Os detalhes incluem informações como padrões suportados, requisitos de sintaxe e exceções.

Os tópicos são listados em ordem alfabética por tipo de dados confidenciais.

Tipos de dados confidenciais

- Chave de acesso secreta da AWS
- Chave da API do Google Cloud
- Cabeçalho de autorização básica HTTP
- JSON Web Token (JWT)
- Chave privada OpenSSH
- Chave privada PGP
- Chave privada do padrão de criptografia de chave pública (PKCS)
- Chave privada PuTTY
- Chave da API Stripe

Chave de acesso secreta da AWS

ID do identificador de dados gerenciados: AWS_CREDENTIALS

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

Comentários: o Macie não relata ocorrências das seguintes sequências de caracteres, que são comumente usadas como exemplos fictícios: `je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` e `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Chave da API do Google Cloud

ID do identificador de dados gerenciados: GCP_API_KEY

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Comentários: o Macie pode detectar somente o componente string (`keyString`) de uma chave de API do Google Cloud. O suporte não inclui a detecção do componente ID ou nome de exibição de uma chave de API do Google Cloud.

Cabeçalho de autorização básica HTTP

ID do identificador de dados gerenciados: HTTP_BASIC_AUTH_HEADER

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: a detecção requer um cabeçalho completo, incluindo o nome do campo e a diretiva do esquema de autenticação, conforme especificado pela RFC 7617. Por exemplo: `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` e `Proxy-Authorization: Basic dGVzdDoxMjPCow==`.

JSON Web Token (JWT)

ID do identificador de dados gerenciados: JSON_WEB_TOKEN

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: o Macie pode detectar JSON Web Tokens (JWTs) que estejam em conformidade com os requisitos especificados pela RFC 7519 para estruturas de assinatura web JSON (JWS). Os tokens podem ser assinados ou não assinados.

Chave privada OpenSSH

ID do identificador de dados gerenciados: OPENSSH_PRIVATE_KEY

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: nenhum

Chave privada PGP

ID do identificador de dados gerenciados: PGP_PRIVATE_KEY

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: nenhum

Chave privada do padrão de criptografia de chave pública (PKCS)

ID do identificador de dados gerenciados: PKCS

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: nenhum

Chave privada PuTTY

ID do identificador de dados gerenciados: PUTTY_PRIVATE_KEY

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Não

Comentários: O Macie pode detectar chaves privadas PuTTY que usam os seguintes cabeçalhos e sequência de cabeçalhos padrão`PuTTY-User-Key-File`:`Encryption`,,`Comment`,`Public-`

`Lines`, `Private-Lines` e. `Private-MAC` Os valores do cabeçalho podem conter caracteres alfanuméricos, hífens (`-`) e caracteres de nova linha (\nou). `\r` `Public-Linese` `Private-Lines` os valores também podem conter barras (`/`), sinais de adição (+) e sinais de igualdade (=). `Private-MAC`os valores também podem conter sinais de adição (+). O suporte não inclui a detecção de chaves privadas com valores de cabeçalho que contenham outros caracteres, como espaços ou sublinhados (_). O suporte também não inclui a detecção de chaves privadas que incluem cabeçalhos personalizados.

Chave da API Stripe

ID do identificador de dados gerenciados: STRIPE_CREDENTIALS

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: não.

Comentários: o Macie não relata ocorrências das seguintes sequências de caracteres, que são comumente usadas em exemplos de código do Stripe: `sk_test_4eC39HqLyjWDarjtT1zdp7dc` e `pk_test_TYooMQauvdEDq54NiTphI7jx`.

Identificadores de dados gerenciados para informações financeiras

O Amazon Macie pode detectar vários tipos de informações financeiras confidenciais usando identificadores de dados gerenciados. Os tópicos desta página listam cada tipo e fornecem informações sobre os identificadores de dados gerenciados projetados para detectar os dados. Cada tópico fornece as seguintes informações:

- ID do identificador de dados gerenciado — Especifica o identificador exclusivo (ID) de um ou mais identificadores de dados gerenciados projetados para detectar os dados. Ao criar um trabalho de descoberta de dados confidenciais ou definir configurações automatizadas de descoberta de dados confidenciais, você pode usar essas IDs para especificar quais identificadores de dados gerenciados você deseja que o Macie use ao analisar dados.
- Países e regiões compatíveis — indica para quais países ou regiões os identificadores de dados gerenciados aplicáveis foram projetados. Se os identificadores de dados gerenciados não forem projetados para determinados países ou regiões, esse valor será Qualquer.
- Palavra-chave obrigatória — Especifica se a detecção exige que uma palavra-chave esteja próxima aos dados. Se uma palavra-chave for necessária, o tópico também fornecerá exemplos de palavras-chave obrigatórias. Para obter informações sobre como o Macie usa palavras-chave ao analisar dados, consulte Requisitos de palavras-chave.

- Comentários — Fornece todos os detalhes relevantes que possam afetar sua selecione de identificador de dados gerenciados ou sua investigação sobre ocorrências relatadas de dados confidenciais. Os detalhes incluem informações como padrões suportados, requisitos de sintaxe e exceções.

Os tópicos são listados em ordem alfabética por tipo de dados confidenciais.

Tipos de dados confidenciais

- Número de conta bancária
- Número básico da conta bancária (BBAN)
- Data de validade do cartão de crédito
- Dados da tarja magnética do cartão de crédito
- Números de cartão de crédito
- Código de verificação do cartão de crédito
- Número internacional de conta bancária (IBAN)

Número de conta bancária

O Macie pode detectar números de contas bancárias canadenses e norte-americanas que consistem em sequências de 9 a 17 dígitos e não contêm espaços.

ID do identificador de dados gerenciados: BANK_ACCOUNT_NUMBER

Países e regiões compatíveis: Canadá, EUA

Palavra-chave obrigatória: sim. As palavras-chave incluem: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Comentários: esse identificador de dados gerenciados foi projetado explicitamente para detectar números de contas bancárias no Canadá e nos EUA. Esses países não usam os formatos de número básico de contas bancárias (BBAN) ou de número internacional de contas bancárias (IBAN) definidos pelo padrão internacional ISO para numeração de contas bancárias, conforme especificado pela ISO 13616. Para detectar números de contas bancárias em outros países e regiões, use os identificadores de dados gerenciados projetados para esses formatos. Para ter mais informações, consulte Número básico da conta bancária (BBAN) e Número internacional de conta bancária (IBAN).

Número básico da conta bancária (BBAN)

O Macie pode detectar números básicos de contas bancárias (BBANs) que estão em conformidade com a estrutura BBAN definida pelo padrão internacional ISO para numeração de contas bancárias, conforme especificado pela ISO 13616. Isso inclui BBANs que não contêm espaços nem usam separadores de espaço ou hífen, como, por exemplo, `NWBK60161331926819`, `NWBK 6016 1331 9268 19` e `NWBK-6016-1331-9268-19`.

ID do identificador de dados gerenciados: dependendo do país ou região, FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

Países e regiões compatíveis França, Alemanha, Itália, Espanha, Reino Unido

Palavra-chave obrigatória: sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

País ou região	Palavras-chave
França	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
Alemanha	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
Itália	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

País ou região	Palavras-chave
Espanha	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account 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

Comentários: esses identificadores de dados gerenciados também podem detectar números internacionais de contas bancárias (IBANs) que estejam em conformidade com o padrão ISO 13616. Para ter mais informações, consulte Número internacional de conta bancária (IBAN). O identificador de dados gerenciados para o Reino Unido (UK_BANK_ACCOUNT_NUMBER) também pode detectar números de contas bancárias domésticas no Reino Unido, como, por exemplo, `60-16-13 31926819`.

Data de validade do cartão de crédito

ID do identificador de dados gerenciados: CREDIT_CARD_EXPIRATION

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: exp d, exp m, exp y, expiration, expiry

Comentários: o suporte inclui a maioria dos formatos de data, como todos os dígitos e combinações de dígitos e nomes de meses. Os componentes de data podem ser separados por barras (/), hífens (-) ou palavras-chave pertinentes. Por exemplo, o Macie pode detectar datas do tipo `02/26`, `02/2026`, `Feb 2026`, `26-Feb` e `expY=2026, expM=02`.

Dados da tarja magnética do cartão de crédito

ID do identificador de dados gerenciados: CREDIT_CARD_MAGNETIC_STRIPE

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: card data, iso7813, mag, magstripe, stripe, swipe

Comentários: o suporte inclui as faixas 1 e 2.

Números de cartão de crédito

ID do identificador de dados gerenciados: CREDIT_CARD_NUMBER para números de cartão de crédito próximos a uma palavra-chave, CREDIT_CARD_NUMBER_(NO_KEYWORD) para números de cartão de crédito que não estão próximos a uma palavra-chave

Países e regiões compatíveis: qualquer

Palavra-chave necessária: varia. As palavras-chave são exigidas pelo identificador de dados CREDIT_CARD_NUMBER gerenciados. As palavras-chave incluem: 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. As palavras-chave não são exigidas pelo identificador de dados CREDIT_CARD_NUMBER_(NO_KEYWORD) gerenciados.

Comentários: A detecção exige que os dados sejam uma sequência de 13 a 19 dígitos que siga a fórmula de cheque de Luhn e use um prefixo de número de cartão padrão para qualquer um dos seguintes tipos de cartão de crédito: American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard e Visa. UnionPay

O Macie não relata ocorrências das seguintes sequências, que as operadoras de cartão de crédito reservaram para testes públicos: 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, 63049017740292441, 63049506000000000, 6331101999990016, 6759649826438453, 679999010000000019 e 76009244561.

Código de verificação do cartão de crédito

ID do identificador de dados gerenciados: CREDIT_CARD_SECURITY_CODE

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: 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

Comentários: nenhum

Número internacional de conta bancária (IBAN)

O Macie pode detectar números de contas bancárias internacionais (IBANs) compostos de até 34 caracteres alfanuméricos, incluindo elementos como o código do país. Mais especificamente, o Macie pode detectar IBANs que estejam em conformidade com o padrão internacional ISO para numeração de contas bancárias, conforme especificado pela ISO 13616. Isso inclui IBANs que não contêm espaços nem usam separadores de espaço ou hífen, como, por exemplo, `GB29NWBK60161331926819`, `GB29 NWBK 6016 1331 9268 19` e `GB29-NWBK-6016-1331-9268-19`. A detecção inclui verificações de validação com base no esquema Modulus 97.

ID do identificador de dados gerenciados: dependendo do país ou região, 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 (para as Ilhas Virgens Britânicas)

Países e regiões compatíveis: Albânia, Andorra, Bósnia-Herzegovina, Brasil, Bulgária, Costa Rica, Croácia, Chipre, República Checa, Dinamarca, República Dominicana, Egito, Estónia, Ilhas Faroé, Finlândia, França, Geórgia, Alemanha, Grécia, Groelândia, Hungria, Islândia, Irlanda, Itália, Jordânia, Kosovo, Liechtenstein, Lituânia, Malta, Mauritânia, Maurícias, Mónaco, Montenegro, Países Baixos, Macedônia do Norte, Polónia, Portugal, São Marino, Senegal, Sérvia, Eslováquia, Eslovênia, Espanha, Suécia, Suíça, Timor-Leste, Tunísia, Turquia, Reino Unido, Ucrânia, Emirados Árabes Unidos, Ilhas Virgens (Britânicas)

Palavra-chave obrigatória: não

Comentários: Os identificadores de dados gerenciados da França, Alemanha, Itália, Espanha e Reino Unido também podem detectar números básicos de contas bancárias (BBANs) que estejam em conformidade com a estrutura BBAN definida pelo padrão ISO 13616, se a sequência de caracteres estiver próxima a uma palavra-chave. Para ter mais informações, consulte Número básico da conta bancária (BBAN).

Identificadores de dados gerenciados para informações pessoais de saúde (PHI)

O Amazon Macie pode detectar vários tipos de informações pessoais de saúde (PHI) confidenciais usando identificadores de dados gerenciados. Os tópicos desta página especificam cada tipo e fornecem informações sobre o identificador de dados gerenciados projetado para detectar os dados. Cada tópico fornece as seguintes informações:

- ID do identificador de dados gerenciado — especifica o identificador exclusivo (ID) do identificador de dados gerenciados projetado para detectar os dados. Ao criar um trabalho de descoberta

de dados confidenciais ou definir as configurações de descobertas automatizadas de dados confidenciais, você pode usar esse ID para especificar se você pode quer que o Macie use o identificados de dados gerenciados quando ele analisa os dados.

- Países e regiões compatíveis — indica para quais países ou regiões os identificadores de dados gerenciados pertinentes foram projetados. Se o identificador de dados gerenciados não for projetado para determinados países ou regiões, esse valor será Qualquer.
- Palavra-chave obrigatória — especifica se a detecção exige que uma palavra-chave esteja próxima aos dados. Se uma palavra-chave for necessária, o tópico também fornecerá exemplos de palavras-chave obrigatórias. Para obter informações sobre como o Macie usa palavras-chave ao analisar dados, consulte Requisitos de palavras-chave.
- Comentários — fornece todos os detalhes relevantes que possam afetar sua escolha de identificador de dados gerenciados ou sua investigação sobre ocorrências relatadas de dados confidenciais. Os detalhes incluem informações como padrões suportados, requisitos de sintaxe e exceções.

Os tópicos são listados em ordem alfabética por tipo de dados confidenciais.

Tipos de dados confidenciais

- Número de registro da Agência Antidrogas (DEA)
- Número de solicitação de seguro saúde (HICN)
- Número de identificação médica ou do seguro de saúde
- Código do Healthcare Common Procedure Coding System (HCPCS)
- National Drug Code (NDC)
- National Provider Identifier (NPI)
- Identificador exclusivo de dispositivo (UDI)

Número de registro da Agência Antidrogas (DEA)

ID do identificador de dados gerenciados: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: dea number, dea registration

Comentários: nenhum

Número de solicitação de seguro saúde (HICN)

ID do identificador de dados gerenciados: USA_HEALTH_INSURANCE_CLAIM_NUMBER

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

Comentários: nenhum

Número de identificação médica ou do seguro de saúde

O suporte inclui números do Cartão Europeu de Plano Saúde para a UE e a Finlândia, números de planos saúde para a França, identificadores de beneficiários do Medicare para os EUA, números do NHS para o Reino Unido e números pessoais de saúde para o Canadá.

ID do identificador de dados gerenciados: dependendo do país ou região, 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 e regiões que recebem suporte: Canadá, UE, Finlândia, França, Reino Unido, EUA

Palavra-chave obrigatória: Sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

Country or region (País ou região)	Keywords
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

Country or region (País ou região)	Keywords
	number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d'assurance maladie, numéro de carte d'assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausva kuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicher ungsnummer
Finlândia	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
França	carte d'assuré social, carte vitale, insurance card
Reino Unido	national health service, NHS
EUA	mbi, medicare beneficiary

Comentários: nenhum

Código do Healthcare Common Procedure Coding System (HCPCS)

ID do identificador de dados gerenciados: USA_HEALTHCARE_PROCEDURE_CODE

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: current procedural terminology, hcpcs, healthcare common procedure coding system

Comentários: nenhum

National Drug Code (NDC)

ID do identificador de dados gerenciados: USA_NATIONAL_DRUG_CODE

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: national drug code, ndc

Comentários: nenhum

National Provider Identifier (NPI)

ID do identificador de dados gerenciados: USA_NATIONAL_PROVIDER_IDENTIFIER

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: hipaa, n.p.i, national provider, npi

Comentários: nenhum

Identificador exclusivo de dispositivo (UDI)

ID do identificador de dados gerenciados: MEDICAL_DEVICE_UDI

Países e regiões compatíveis: EUA

Palavra-chave obrigatória: Sim. As palavras-chave incluem: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Comentários: o Macie pode detectar identificadores exclusivos de dispositivos (UDIs) que estão em conformidade com os formatos aprovados pela Food and Drug Administration dos EUA. Isso inclui formatos padrão definidos por GS1, HIBCC e ICCBBA. O suporte do ICCBA é para o padrão ISBT.

Identificadores de dados gerenciados para informações de identificação pessoal (PII)

O Amazon Macie pode detectar vários tipos de informações de identificação pessoal (PII) confidenciais usando identificadores de dados gerenciados. Os tópicos desta página listam cada tipo

e fornecem informações sobre os identificadores de dados gerenciados projetados para detectar os dados. Cada tópico fornece as seguintes informações:

- ID do identificador de dados gerenciado — Especifica o identificador exclusivo (ID) de um ou mais identificadores de dados gerenciados projetados para detectar os dados. Ao criar um trabalho de descoberta de dados confidenciais ou definir configurações automatizadas de descoberta de dados confidenciais, você pode usar essas IDs para especificar quais identificadores de dados gerenciados você deseja que o Macie use ao analisar dados.
- Países e regiões compatíveis — indica para quais países ou regiões os identificadores de dados gerenciados aplicáveis foram projetados. Se os identificadores de dados gerenciados não forem projetados para determinados países ou regiões, esse valor será Qualquer.
- Palavra-chave obrigatória — Especifica se a detecção exige que uma palavra-chave esteja próxima aos dados. Se uma palavra-chave for necessária, o tópico também fornecerá exemplos de palavras-chave obrigatórias. Para obter informações sobre como o Macie usa palavras-chave ao analisar dados, consulte Requisitos de palavras-chave.
- Comentários — Fornece todos os detalhes relevantes que possam afetar sua selecione de identificador de dados gerenciados ou sua investigação sobre ocorrências relatadas de dados confidenciais. Os detalhes incluem informações como padrões suportados, requisitos de sintaxe e exceções.

Os tópicos são listados em ordem alfabética por tipo de dados confidenciais.

Tipos de dados confidenciais

- Datas de nascimento
- Número de identificação da carteira de habilitação
- Número de registro eleitoral
- Nome completo
- Coordenadas do sistema de posicionamento global (GPS)
- Cookie HTTP
- Endereço postal
- Número de identificação nacional
- Número do Seguro Nacional (NINO)
- Número de passaporte
- Número de residência permanente

- Número de telefone
- Número do Seguro Social (SIN)
- Número da Previdência Social (SSN)
- Identificação do contribuinte ou número de referência
- Número de identificação de veículo (VIN)

Datas de nascimento

ID de dados gerenciados: DATE_OF_BIRTH

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Sim. As palavras-chave incluem: bday, b-day, birth date, birthday, date of birth, dob

Comentários: o suporte inclui a maioria dos formatos de data, como todos os dígitos e combinações de dígitos e nomes de meses. Os componentes de data podem ser separados por espaços, barras (/) ou hífens (-).

Número de identificação da carteira de habilitação

ID do identificador de dados gerenciados: dependendo do país ou região, 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

Países e regiões compatíveis: Austrália, Áustria, Bélgica, Bulgária, Canadá, Croácia, Chipre, República Checa, Dinamarca, Estónia, Finlândia, França, Alemanha, Grécia, Hungria, Índia, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal , Romênia, Eslováquia, Eslovênia, Espanha, Suécia, Reino Unido, EUA

Palavra-chave obrigatória: Sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

País ou região	Palavras-chave
Austrália	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
Áustria	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
Bulgária	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
Croácia	vozačka dozvola

País ou região	Palavras-chave
Chipre	άδεια οδήγησης
República Tcheca	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
Estônia	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finlândia	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
França	permis de conduire
Alemanha	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
Grécia	δεια οδήγησης, adeia odigisis
Hungria	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
Índia	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 ou região	Palavras-chave
Itália	patente di guida, patente di guida numero, patente guida, patente guida numero
Letônia	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
Lituânia	vairuotojo pažymėjimas
Luxemburgo	fahrerlaubnis, führerschäin
Malta	liċenzja tas-sewqan
Holanda	permis de conduire, rijbewijs, rijbewijsnummer
Polônia	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
Romênia	numărul permisului de conducere, permis de conducere
Eslováquia	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Eslovênia	vozniško dovoljenje

País ou região	Palavras-chave
Espanha	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
Suécia	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
EUA	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

Comentários: Nenhum

Número de registro eleitoral

ID de dados gerenciados: UK_ELECTORAL_ROLL_NUMBER

Países e regiões compatíveis: Reino Unido

Palavra-chave obrigatória: Sim. As palavras-chave incluem: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Comentários: Nenhum

Nome completo

ID de dados gerenciados: NAME

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Não

Comentários: Macie consegue detectar apenas nomes completos. O suporte é limitado aos conjuntos de caracteres latinos.

Coordenadas do sistema de posicionamento global (GPS)

ID de dados gerenciados: LATITUDE_LONGITUDE

Países e regiões compatíveis: qualquer, se as coordenadas estiverem próximas de uma palavra-chave em inglês.

Palavra-chave obrigatória: Sim. As palavras-chave incluem: coordinate, coordinates, lat long, latitude longitude, position

Comentários: o Macie poderá detectar coordenadas de GPS se as coordenadas de latitude e longitude estiverem armazenadas como um par e estiverem no formato de graus decimais (DD), por exemplo `41.948614,-87.655311`. O suporte não inclui detecção de coordenadas no formato de minutos ou graus decimais (DDM), por exemplo `41°56.9168'N 87°39.3187'W`; ou formato de graus, minutos ou segundos (DMS), por exemplo `41°56'55.0104"N 87°39'19.1196"W`.

Cookie HTTP

ID de dados gerenciados: HTTP_COOKIE

Países e regiões compatíveis: qualquer um

Palavra-chave obrigatória: Não

Comentários: A detecção requer um `Cookie` completo ou cabeçalho `Set-Cookie`. O cabeçalho pode incluir um ou mais pares de nome-valor, por exemplo: `Set-Cookie: id=TWlrZQ` e `Cookie: session=3948; lang=en`.

Endereço postal

ID de identificador de dados gerenciados: ADDRESS (para Austrália, Canadá, França, Alemanha, Itália, Espanha, Reino Unido e EUA), BRAZIL_CEP_CODE (para o Código de Endereçamento Postal do Brasil)

Países e regiões compatíveis: Austrália, Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA

Palavra-chave necessária: Varia. As palavras-chave não são exigidas pelo identificador de dados ADDRESS gerenciados. As palavras-chave são exigidas pelo identificador de dados BRAZIL_CEP_CODE gerenciados. As palavras-chave incluem: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

Comentários: Embora uma palavra-chave não seja exigida pelo identificador de dados ADDRESS gerenciados, a detecção exige que um endereço inclua o nome de uma cidade ou local e um CEP ou CEP correspondente em um país ou região compatível. O identificador de dados BRAZIL_CEP_CODE gerenciados pode detectar somente a parte do Código de Endereçamento Postal (CEP) de um endereço.

Número de identificação nacional

A compatibilidade inclui números Aadhaar para a Índia, números do Codice Fiscale para a Itália, identificadores do Documento Nacional de Identidad (DNI) para a Espanha, códigos do Instituto Nacional Francês de Estatística e Estudos Econômicos (INSEE), números da carteira de identidade nacional alemã e números do Registro Geral (RG) para o Brasil.

ID do identificador de dados gerenciados: dependendo do país ou região, BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Países e regiões compatíveis: Brasil, França, Alemanha, Índia, Itália, Espanha

Palavra-chave obrigatória: Sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

País ou região	Palavras-chave
Brasil	registro geral, rg
França	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#
Alemanha	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
Índia	aadhaar, aadhar, adhaar, uidai
Itália	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Espanha	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#

Comentários: Nenhum

Número do Seguro Nacional (NINO)

ID de dados gerenciados: UK_NATIONAL_INSURANCE_NUMBER

Países e regiões compatíveis: Reino Unido

Palavra-chave obrigatória: Sim. As palavras-chave incluem: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

Comentários: Nenhum

Número de passaporte

ID do identificador de dados gerenciados: dependendo do país ou região, CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

Países e regiões compatíveis: Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA

Palavra-chave obrigatória: Sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

País ou região	Palavras-chave
Canadá	passeport, passeport#, passport, passport#, passportno, passportno#
França	numéro de passeport, passeport, passeport #, passeport n °, passeport non
Alemanha	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
Itália	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
Espanha	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport

País ou região	Palavras-chave
Reino Unido	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
EUA	passport, travel document

Comentários: Nenhum

Número de residência permanente

ID de dados gerenciados: CANADA_NATIONAL_IDENTIFICATION_NUMBER

Países e regiões compatíveis: Canadá

Palavra-chave obrigatória: Sim. As palavras-chave incluem: 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

Comentários: Nenhum

Número de telefone

ID do identificador de dados gerenciados: dependendo do país ou região, 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 e regiões compatíveis: Brasil, Canadá, França, Alemanha, Itália, Espanha, Reino Unido, EUA

Palavra-chave necessária: Varia. Se uma palavra-chave estiver próxima dos dados, o número não precisará incluir o código do país. As palavras-chave incluem: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Para o Brasil, as palavras-chave também incluem: cel, celular, fone, móvel, número residencial, numero residencial, telefone. Se uma palavra-chave estiver próxima dos dados, o número não precisará incluir o código do país.

Comentários: Para os EUA, o suporte inclui números de chamada gratuita.

Número do Seguro Social (SIN)

ID de dados gerenciados: CANADA_SOCIAL_INSURANCE_NUMBER

Países e regiões compatíveis: Canadá

Palavra-chave obrigatória: Sim. As palavras-chave incluem: canadian id, numéro d'assurance sociale, sin, social insurance number

Comentários: Nenhum

Número da Previdência Social (SSN)

ID do identificador de dados gerenciados: dependendo do país ou região, SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Países e regiões compatíveis: Espanha, EUA

Palavra-chave obrigatória: Sim. Para a Espanha, as palavras-chave incluem: número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Para os EUA, as palavras-chave incluem: social security, ss#, ssn.

Comentários: Nenhum

Identificação do contribuinte ou número de referência

O suporte inclui: números CIF, NIE e NIF para a Espanha; números CNPJ e CPF para o Brasil; números do Codice Fiscale para a Itália; ITINs para os EUA; PANs para a Índia; números Steueridentifikationsnummer para a Alemanha; TFNs para a Austrália; TINs para a França; e números TRN e UTR para o Reino Unido.

ID do identificador de dados gerenciados: dependendo do país ou região, 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 e regiões compatíveis: Austrália, Brasil, França, Alemanha, Índia, Itália, Espanha, Reino Unido, EUA

Palavra-chave obrigatória: Sim. A tabela a seguir lista as palavras-chave que o Macie reconhece para países e regiões específicos.

País ou região	Palavras-chave
Austrália	tax file number, tfn
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
França	numéro d'identification fiscal, tax id, tax identific ation number, tax number, tin, tin#
Alemanha	identifikationsnummer, steuer id, steueride ntifikationsnummer, steuernummer, tax id, tax identification number, tax number
Índia	e-pan, pan card, pan number, permanent account number
Itália	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Espanha	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

País ou região	Palavras-chave
	reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
EUA	i.t.i.n., número de identificação de contribuinte individual, itin

Comentários: Nenhum

Número de identificação de veículo (VIN)

ID de dados gerenciados: VEHICLE_IDENTIFICATION_NUMBER

Países e regiões compatíveis: qualquer um, se o VIN estiver próximo a uma palavra-chave em um dos seguintes idiomas: inglês, francês, alemão, lituano, polonês, português, romeno ou espanhol.

Palavra-chave obrigatória: Sim. As palavras-chave incluem: 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

Comentários: o Macie pode detectar VINs que consistem em uma sequência de 17 caracteres e aderem aos padrões ISO 3779 e 3780. Esses padrões foram projetados para uso em todo o mundo.

Criar identificadores de dados personalizados no Amazon Macie

Um identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais em objetos do Amazon Simple Storage Service (Amazon S3). Os critérios consistem em uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados.

Com identificadores de dados personalizados, você pode definir critérios de detecção que refletem determinados cenários, propriedade intelectual ou dados proprietários particulares de sua organização — por exemplo, IDs de funcionários, números de conta de cliente ou classificações de dados internas. Se você configurar trabalhos de descoberta de dados confidenciais ou descoberta automática de dados confidenciais para usar esses identificadores, poderá analisar objetos do S3 de uma forma que complemente os identificadores de dados gerenciados fornecidos pelo Amazon Macie.

Além dos critérios de detecção, você pode definir configurações de gravidade personalizadas para descobertas de dados confidenciais que um identificador de dados personalizado produz. Por padrão, o Macie atribui a gravidadeMédia a todas as descobertas que um identificador de dados personalizado produz — a gravidade não muda com base no número de ocorrências de texto que correspondem aos critérios de detecção de um identificador de dados personalizado. Ao definir configurações de gravidade personalizadas, você pode especificar qual gravidade atribuir com base no número de ocorrências de texto que correspondem aos critérios.

Tópicos

Definindo critérios de detecção para identificadores de dados personalizados

Ao criar um identificador de dados personalizado, você especifica uma expressão regular (regex) que define um padrão de texto para corresponder aos objetos S3. O Macie suporta um subconjunto da sintaxe do padrão regex fornecida pela biblioteca Perl Compatible Regular Expressions (PCRE). Para obter mais informações, consulte Suporte Regex mais adiante nesta seção.

Você também pode especificar sequências de caracteres, como palavras e frases, e uma regra de proximidade para refinar os resultados.

Palavras chave

Estas são sequências de caracteres específicas que devem estar próximas do texto que corresponde ao padrão regex. Os requisitos de proximidade variam de acordo com o formato de armazenamento ou o tipo de arquivo de um objeto S3:

- Para dados estruturados em colunas, o Macie inclui um resultado se o texto corresponder ao padrão regex e uma palavra-chave estiver no nome do campo ou coluna que armazena o texto, ou se o texto for precedido por e dentro da distância máxima de correspondência de uma palavra-chave no mesmo campo ou valor de célula. Isso vale para pastas de trabalho do Microsoft Excel, arquivos CSV e arquivos TSV.

- Para dados estruturados baseados em registros, o Macie inclui um resultado se o texto corresponder ao padrão regex e estiver dentro da distância máxima de correspondência de uma palavra-chave. A palavra-chave pode estar no nome de um elemento no caminho para o campo ou matriz que armazena o texto, ou pode preceder e fazer parte do mesmo valor no campo ou matriz que armazena o texto. Isso vale para contêineres de objetos Apache Avro, arquivos Apache Parquet, arquivos JSON e arquivos JSON Lines.
- Para dados estruturados baseados em registros, o Macie inclui um resultado se o texto corresponder ao padrão regex e estiver dentro da distância máxima de correspondência de uma palavra-chave. Isso vale para arquivos Adobe Portable Document Format, documentos do Microsoft Word, mensagens de e-mail e arquivos de texto não binários que não sejam arquivos CSV, JSON, JSON Lines e TSV. Isso inclui quaisquer dados estruturados, como tabelas, nesses tipos de arquivos.

Você pode especificar até 50 palavras-chave. Cada palavra-chave pode conter de 3 a 90 caracteres UTF-8. Palavras-chave não diferenciam maiúsculas de minúsculas.

Distância máxima de partida

Essa é uma regra de proximidade baseada em caracteres para palavras-chave. O Macie usa essa configuração para determinar se uma palavra-chave precede o texto que corresponde ao padrão regex. A configuração define o número máximo de caracteres que podem existir entre o fim de uma palavra-chave completa e o fim do texto que corresponde ao padrão regex. Se o texto corresponder ao padrão regex, ocorrer após pelo menos uma palavra-chave completa e ocorrer dentro da distância especificada da palavra-chave, Macie o incluirá nos resultados. Caso contrário, Macie o exclui dos resultados.

Você pode especificar uma distância de 1 a 300 caracteres. A distância padrão é de 50 caracteres. Para obter melhores resultados, essa distância deve ser maior que o número mínimo de caracteres de texto que o regex foi projetado para detectar. Se apenas parte do texto estiver dentro da distância máxima de correspondência de uma palavra-chave, Macie não a incluirá nos resultados.

Ignorar palavras

Estas são sequências de caracteres específicas a serem excluídas dos resultados. Se o texto corresponder ao padrão regex, mas contiver uma palavra a ser ignorada, o Macie não o incluirá nos resultados.

Você pode especificar até 10 palavras ignoradas. Cada palavra a ser ignorada pode conter de 4 a 90 caracteres UFT-8. Palavras ignoradas diferenciam maiúsculas de minúsculas.

Por exemplo, muitas empresas têm uma sintaxe específica para IDs de funcionários. Uma dessas sintaxes pode ser: uma letra maiúscula que indica se o funcionário é funcionário em tempo integral (F) ou meio período (P), seguida por um hífen (-), seguido por uma sequência de oito dígitos que identifica o funcionário. Os exemplos são: F-12345678, para um funcionário em tempo integral, e P-87654321, para um funcionário em tempo parcial.

Se você criar um identificador de dados personalizado para detectar IDs de funcionários que usam essa sintaxe, você pode usar o seguinte regex: `[A-Z]-\d{8}`. Para refinar a análise e evitar falsos positivos, você também pode configurar o identificador de dados personalizado para usar as palavras-chave ID do funcionário e do funcionário e uma distância máxima de correspondência de 20 caracteres. Com esses critérios, os resultados incluem texto que corresponda ao regex somente se o texto ocorrer após a palavra-chave funcionário ou ID do funcionário e todo o texto ocorrer dentro de 20 caracteres de uma dessas palavras-chave.

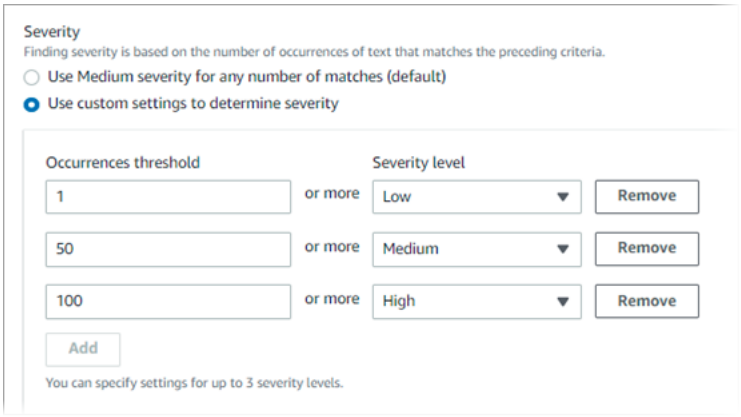
Para ver uma demonstração de como as palavras-chave podem ajudar você a encontrar dados confidenciais e evitar falsos positivos, assista ao vídeo a seguir: How Amazon Macie uses keywords to discover sensitive data.

Definindo configurações de gravidade de busca para identificadores de dados personalizados

Ao criar um identificador de dados personalizado, você também pode definir configurações de gravidade personalizadas para descobertas de dados confidenciais que o identificador produz. Por padrão, o Macie atribui a gravidade Média a todas as descobertas que um identificador de dados personalizado produz. Se um objeto do S3 contiver pelo menos uma ocorrência de texto que corresponda aos critérios de detecção de um identificador de dados personalizado, o Macie atribuirá automaticamente gravidade Média à descoberta resultante.

Com as configurações de gravidadepe rsonalizadas, você pode especificar qual gravidade atribuir com base no número de ocorrências de texto que correspondem aos critérios de detecção do identificador de dados personalizado. Para fazer isso, você define limites de ocorrências para até três níveis de gravidade: Baixo (menos grave), Médio e Alto (mais grave). Um limite de ocorrências é o número mínimo de correspondências que devem existir em um objeto do S3 para produzir uma descoberta com a gravidade especificada. Se você especificar mais de um limite, os limites deverão estar em ordem crescente por gravidade, passando de Baixo para Alto.

Por exemplo, a imagem a seguir mostra as configurações de gravidade de um identificador de dados personalizado que especifica três limites de ocorrências, um para cada nível de gravidade suportado pelo Macie.



A tabela a seguir indica a gravidade das descobertas que o identificador de dados personalizado produz.

Limite de ocorrências	Nível de gravidade	Result
1	Baixo	Se um objeto do S3 contiver de 1 a 49 ocorrências de texto que correspondam aos critérios de detecção, a gravidade da descoberta resultante será Baixa.
50	Médio	Se um objeto do S3 contiver de 50 a 99 ocorrências de texto que correspondam aos critérios de detecção, a gravidade da descoberta resultante será Média.
100	Alta	Se um objeto do S3 contiver 100 ou mais ocorrências de texto que correspondam aos critérios de detecção,

Limite de ocorrências	Nível de gravidade	Result
		a gravidade da descoberta resultante será Alta.

Você também pode usar as configurações de gravidade para especificar se deseja criar uma descoberta. Se um objeto do S3 contiver menos ocorrências do que o limite mais baixo de ocorrências, o Macie não criará uma descoberta.

Criando identificadores de dados personalizados

Siga estas etapas para criar um identificador de dados personalizado usando o console do Amazon Macie. Para criar um identificador de dados personalizado de forma programática, use a operação CreateCustomDataIdentifier da API do Amazon Macie.

Para criar um identificador de dados personalizado

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, escolha Identificadores de dados personalizados.
3. Escolha Create (Criar).
4. Para Nome insira um nome para o identificador de dados personalizado. Um nome pode conter até 128 caracteres.

   Evite incluir qualquer dado confidencial no nome. Outros usuários da sua conta poderão ver o nome, dependendo das ações que têm permissão para realizar no Macie.
5. (Opcional) Em Description,insira uma breve descrição do identificador de dados personalizado. A descrição pode conter até 512 caracteres.

   Evite incluir qualquer dado confidencial no nome. Outros usuários da sua conta poderão ver a descrição, dependendo das ações que têm permissão para realizar no Macie.
6. Para a Regular expression, insira a expressão regular (regex) que define o padrão de texto a ser correspondido. Um nome regex pode conter até 512 caracteres. Para saber mais sobre a sintaxe e as restrições suportadas, consulte Suporte Regex mais adiante nesta seção.
7. (Opcional) Em Palavras-chave, insira até 50 sequências de caracteres (separadas por vírgulas) para definir um texto específico que deve estar próximo ao texto que corresponda ao padrão regex. Cada palavra-chave pode conter de 3 a 90 caracteres UTF-8. Palavras-chave não diferenciam maiúsculas de minúsculas.

O Macie inclui uma ocorrência nos resultados somente se o texto corresponder ao padrão regex e estiver dentro da distância máxima de correspondência de uma dessas palavras-chave, conforme explicado no tópico anterior.

8. (Opcional) Em Ignorar palavras, insira até 10 sequências de caracteres (separadas por vírgulas) que definam um texto específico a ser excluído dos resultados. Cada palavra a ser ignorada pode conter de 4 a 90 caracteres UFT-8. Palavras ignoradas diferenciam maiúsculas de minúsculas.

   O Macie exclui uma ocorrência dos resultados se o texto corresponder ao padrão regex, mas contiver uma dessas palavras ignoradas.

9. (Opcional) Para Maximum match distance de correspondência, insira o número máximo de caracteres que podem existir entre o final de uma palavra-chave e o final do texto que corresponde ao padrão regex. A distância pode ser de 1 a 300 caracteres. A distância padrão é de 50 caracteres.

   O Macie inclui uma ocorrência nos resultados somente se o texto corresponder ao padrão regex e estiver dentro da distância máxima de correspondência de uma dessas palavras-chave, conforme explicado no tópico anterior.

10. Em Gravidade, escolha como você deseja que o Macie atribua gravidade às descobertas de dados confidenciais que o identificador de dados personalizado produz:

    - Para atribuir automaticamente a gravidade Média a todas as descobertas, escolha Usar gravidade Média para qualquer número de correspondências (padrão). Com essa opção, o Macie atribui automaticamente a gravidadeMédia a uma descoberta se o objeto S3 afetado contiver uma ou mais ocorrências de texto que correspondam aos critérios de detecção.
    - Para atribuir gravidade com base nos limites de ocorrências que você especificar, escolha Usar configurações personalizadas para determinar a gravidade. Em seguida, use as opções Limite de ocorrências e Nível de gravidade para especificar o número mínimo de correspondências que devem existir em um objeto do S3 para produzir uma descoberta com uma gravidadeselecionada.

      Por exemplo, para atribuir a gravidade Alta a uma descoberta que relata 100 ou mais ocorrências de texto que correspondam aos critérios de detecção, insira **`100`** na caixa Limite de ocorrências e escolha Alta na lista Nível de gravidade.

      Você pode especificar até três limites de ocorrências, um para cada nível de gravidade suportado pelo Macie: Baixo (para menos grave), Médio ou Alto (para mais grave). Se você

especificar mais de um, os limites deverão estar em ordem crescente por gravidade, de Baixo a Alto. Se um objeto do S3 contiver menos ocorrências do que o limite mais baixo de ocorrências, o Macie não criará uma descoberta.

11. (Opcional) Em Tags, escolha Adicionar tag e, em seguida, insira até 50 tags para atribuir ao trabalho.

    Uma tag é um rótulo que você define e atribui a determinados tipos de atributos AWS. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional. As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.

12. (Opcional) Em Avaliar, insira até 1.000 caracteres na caixa Dados da amostra e escolha Testar para testar os critérios de detecção. Macie avalia os dados da amostra e relata o número de ocorrências de texto que correspondem aos critérios. Você pode repetir essa etapa quantas vezes quiser para refinar e otimizar os critérios.

    > **Note**
    >
    > Recomendamos enfaticamente que você teste e refine os critérios de detecção antes de salvar o identificador de dados personalizado. Como identificadores de dados personalizados são usados por trabalhos confidenciais de descoberta de dados, não é possível editar um identificador de dados personalizado depois de salvá-lo. Isso ajuda a garantir que você tenha um histórico imutável de descobertas de dados sigilosos e resultados de descoberta para auditorias de privacidade de dados e proteção de dados ou investigações que você realiza.

13. Quando terminar, escolha Submit (Enviar).

O Macie testa as configurações e verifica se ele pode compilar o regex. Se houver um problema com qualquer uma das configurações ou com o regex, ocorre um erro e indica a natureza do problema. Depois de resolver qualquer problema, você pode salvar o identificador de dados personalizado.

Suporte regex em identificadores de dados personalizados

O Macie suporta um subconjunto da sintaxe do padrão regex fornecida pela biblioteca Perl Compatible Regular Expressions (PCRE). Das estruturas fornecidas pela biblioteca PCRE, o Macie não suporta os seguintes elementos de padrão:

- Referências anteriores
- Capturar grupos
- Padrões condicionais
- Código incorporado
- Sinalizadores de padrões globais, como `/i`, `/m` e `/x`
- Padrões recursivos
- Afirmações positivas e negativas de largura zero de retrospectiva e prospectiva, como e `?=`, `?!`, `?<=` e `?<!`.

Para criar padrões de regex eficazes para identificadores de dados personalizados, observe também as dicas e recomendações a seguir:

- Âncoras — Use âncoras (^ ou $) somente se você espera que o padrão apareça no início ou no final de um arquivo, não no início ou no final de uma linha.
- Repetições limitadas — Por motivos de desempenho, o Macie reduz o tamanho dos grupos de repetição limitados. Por exemplo, `\d{100,1000}` não compilará no Macie. Para aproximar essa funcionalidade, você pode usar uma repetição aberta, como `\d{100,}`.
- Insensibilidade a maiúsculas e minúsculas — Para tornar partes de um padrão insensíveis a maiúsculas e minúsculas, você pode usar a `(?i)` estrutura em vez do `/i` sinalizador.
- Desempenho — Não há necessidade de otimizar prefixos ou alternâncias manualmente. Por exemplo, mudar `/hello|hi|hey/` para `/h(?:ello|i|ey)/` não melhorará o desempenho.
- Curingas — Por motivos de desempenho, Macie limita o número de curingas repetidas. Por exemplo, `a*b*a*` não compilará no Macie.

Para se proteger contra expressões malformadas ou de longa duração, o Macie testa automaticamente os padrões de regex em uma coleção de texto de amostra.

Como definir exceções de dados sigilosos com as listas de permissões do Amazon Macie

Com listas de permissões no Amazon Macie, você pode definir um texto específico e padrões de texto que você quer que o Macie ignore ao inspecionar objetos do Amazon Simple Storage Service (Amazon S3) em busca de dados sigilosos. Normalmente, essas são exceções de dados sigilosos

para seus cenários ou ambientes específicos. Se os dados corresponderem a um padrão de texto em uma lista de permissões, o Macie não os reportará, mesmo se os dados corresponderem aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizado. Ao usar listas de permissões, você pode refinar a sua análise dos dados do Amazon S3 e reduzir o ruído.

Você pode criar e usar dois tipos de listas de permissões no Macie:

- Texto predefinido – Para esse tipo de lista, você especifica determinadas sequências de caracteres a serem ignoradas, por exemplo, os nomes dos representantes públicos da sua organização, números de telefone específicos ou dados de amostra específicos que a sua organização usa para testes. Se você usar esse tipo de lista, o Macie ignorará um texto que corresponder exatamente a uma entrada da lista.

  Esse tipo de lista é útil se você deseja especificar palavras, frases e outros tipos específicos de sequências de caracteres que não são sigilosos, não têm probabilidade de serem alterados e não seguem necessariamente um padrão comum.
- Expressão regular – Para esse tipo de lista, você especifica uma expressão regular (regex) que define um padrão de texto a ser ignorado, por exemplo, números de telefone públicos da sua organização, endereços de e-mail do domínio da sua organização ou dados de amostra padronizados que a sua organização usa para testes. Se você usar esse tipo de lista, o Macie ignorará texto que corresponda exatamente ao padrão definido pela lista.

  Esse tipo de lista é útil quando você deseja especificar um texto que não é sigiloso, mas que varia ou pode ser alterado enquanto também segue um padrão comum.

Depois de criar uma lista de permissões, você pode criar e configurar trabalhos de descoberta de dados sigilosos para usá-la ou adicioná-la às suas configurações automatizadas de descoberta de dados sigilosos. Em seguida, Macie usa a lista ao analisar os dados. Se o Macie encontrar um texto que corresponda a uma entrada ou padrão em uma lista de permissões, o Macie não relatará essa ocorrência de texto em descobertas de dados sigilosos, estatísticas e outros tipos de resultados.

Você pode criar e usar listas de permissões em todas as Regiões da AWS em que o Macie está atualmente disponível, exceto na região Asia Pacific (Osaka).

Tópicos

- Permitir opções e requisitos de listas no Amazon Macie
- Criação e gerenciamento de listas de permissão no Amazon Macie

Permitir opções e requisitos de listas no Amazon Macie

No Amazon Macie, você pode usar listas de permissões para especificar um texto ou padrões de texto que você deseja que o Macie ignore ao inspecionar objetos do Amazon Storage Service (Amazon S3) em busca de dados confidenciais. O Macie fornece opções para dois tipos de listas de permissões, texto predefinido e expressões regulares.

Uma lista de texto predefinido é útil quando você deseja que o Macie ignore palavras, frases e outros tipos específicos de sequências de caracteres que você não considera confidenciais. Os exemplos são os nomes dos representantes públicos da sua organização, números de telefone específicos ou dados de amostra específicos que sua organização usa para testes. Se o Macie encontrar um texto que corresponda aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizado e o texto também corresponder a uma entrada em uma lista de permissões, o Macie não reportará essa ocorrência de texto em descobertas de dados confidenciais, estatísticas e outros tipos de resultados.

Uma expressão regular (regex) é útil quando você deseja que o Macie ignore um texto que varia ou pode ser alterado e, ao mesmo tempo, também segue um padrão comum. O regex especifica um padrão de texto a ser ignorado. Os exemplos são números de telefone públicos da sua organização, endereços de e-mail do domínio da sua organização ou dados de amostra padronizados que sua organização usa para testes. Se o Macie encontrar um texto que corresponda aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizado e o texto também corresponder a um padrão de regex em uma lista de permissões, o Macie não reportará essa ocorrência de texto em descobertas de dados confidenciais, estatísticas e outros tipos de resultados.

Você pode criar e usar os dois tipos de listas de permissões em todos os Regiões da AWS onde o Macie está disponível atualmente, exceto na região Ásia-Pacífico (Osaka). Ao criar e gerenciar listas de permissões, lembre-se das seguintes opções e requisitos. Observe também que não há suporte para permitir entradas de lista e padrões de regex para endereços de correspondência.

Tópicos

- Suporte e recomendações de sintaxe
- Exemplos

Opções e requisitos para listas de texto predefinido

Para esse tipo de lista de permissões, você fornece um arquivo de texto simples delimitado por linhas que lista sequências de caracteres específicas a serem ignoradas. As entradas da lista são normalmente palavras, frases e outros tipos de sequências de caracteres que você não considera confidenciais, que provavelmente não serão alteradas e não necessariamente aderem a um padrão específico. Se você usar esse tipo de lista, o Amazon Macie não relatará ocorrências de texto que correspondam exatamente a uma entrada na lista. Macie trata cada entrada da lista como um valor literal de string.

Para usar esse tipo de lista de permissões, comece criando a lista em um editor de texto e salvando-a como um arquivo de texto simples. Em seguida, faça o upload da lista em um bucket do S3 e garanta que as configurações de armazenamento e criptografia do bucket e do objeto permitam que o Macie recupere e descriptografe a lista. Em seguida, crie e defina as configurações da lista no Macie.

Depois de definir as configurações no Macie, recomendamos que você teste a lista de permissões com um conjunto pequeno e representativo de dados da sua conta ou organização. Para testar uma lista, você pode criar um trabalho único e configurar o trabalho para usar a lista, além dos identificadores de dados gerenciados e identificadores de dados personalizados que você normalmente usa para analisar dados. Em seguida, você pode analisar os resultados do trabalho — descobertas de dados confidenciais, resultados de detecções de dados confidenciais ou ambos. Se os resultados do trabalho forem diferentes do esperado, você poderá alterar e testar a lista até que os resultados sejam os esperados.

Depois de concluir a configuração e o teste de uma lista de permissões, você pode criar e configurar trabalhos adicionais para usá-la ou adicioná-la às configurações automatizadas de descoberta de dados confidenciais da sua conta. Quando esses trabalhos começam a ser executados ou o próximo ciclo automatizado de análise de descoberta começa, o Macie recupera a versão mais recente da lista do Amazon S3 e a armazena na memória temporária. Em seguida, o Macie usa essa cópia temporária da lista ao inspecionar objetos do S3 em busca de dados confidenciais. Quando um trabalho termina de ser executado ou o ciclo de análise é concluído, o Macie exclui permanentemente sua cópia da lista da memória. A lista não persiste no Macie. Somente as configurações da lista persistem no Macie.

> **Important**
>
> Como as listas de texto predefinido não persistem no Macie, é importante verificar o status de suas listas de permissão periodicamente. Se o Macie não conseguir recuperar ou analisar uma lista para a qual você configurou um trabalho ou uma descoberta automatizada, o Macie não usará a lista. Isso pode produzir resultados inesperados, como descobertas de dados confidenciais para texto que você especificou na lista.

Tópicos

Requisitos de sintaxe

Ao criar esse tipo de lista de permissões, observe os seguintes requisitos para o arquivo da lista:

- A lista deve ser armazenada como um arquivo de texto simples (`text/plain`), como um arquivo.txt, .text ou .plain.
- A lista deve usar quebras de linha para separar entradas individuais. Por exemplo: .

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

  Macie trata cada linha como uma entrada única e distinta na lista. O arquivo também pode conter linhas em branco para melhorar a legibilidade. O Macie ignora as linhas em branco ao analisar o arquivo.
- Cada palavra-chave pode conter de 1 a 90 caracteres UTF-8.
- Cada entrada deve ser uma correspondência completa e exata para que o texto seja ignorado. O Macie não suporta o uso de caracteres curinga ou valores parciais para entradas. Macie trata cada

entrada como um valor literal de string. As correspondências não fazem distinção entre maiúsculas e minúsculas.

- O arquivo pode conter de 1 a 100.000 entradas.
- O tamanho total de armazenamento do arquivo não pode exceder 35 MB.

Requisitos de armazenamento

Ao adicionar e gerenciar listas de permissões no Amazon S3, observe os seguintes requisitos e recomendações de armazenamento:

- Suporte regional — Uma lista de permissões deve ser armazenada em um bucket do S3 que esteja no mesmo Região da AWS que a sua conta do Macie. Macie não pode acessar uma lista de permissões se ela estiver armazenada em uma região diferente.
- Propriedade do bucket — Uma lista de permissões deve ser armazenada em um bucket do S3 que seja de sua Conta da AWS propriedade. Se você quiser que outras contas usem a mesma lista de permissões, considere criar uma regra de replicação do Amazon S3 para replicar a lista em buckets pertencentes a essas contas. Para obter informações sobre como replicar objetos do S3, consulte Replicar objetos, no Guia do usuário do Amazon Simple Storage Service.

  Além disso, sua identidade AWS Identity and Access Management (IAM) deve ter acesso de leitura ao bucket e ao objeto do S3 que armazenam a lista. Caso contrário, você não poderá criar ou atualizar as configurações da lista ou verificar o status da lista usando o Macie.
- Políticas de bucket — Se você armazenar uma lista de permissões em um bucket do S3 que tenha uma política de bucket restritiva, certifique-se de que a política permita que o Macie recupere a lista. Para fazer isso, você pode adicionar uma condição para a função vinculada ao serviço do Macie à política do bucket. Para ter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

  Além disso, certifique-se de que a política permita que sua identidade do IAM tenha acesso de leitura ao bucket. Caso contrário, você não poderá criar ou atualizar as configurações da lista ou verificar o status da lista usando o Macie.
- Caminhos de objetos — Se você armazenar mais de uma lista de permissões no Amazon S3, o caminho do objeto para cada lista deve ser exclusivo. Em outras palavras, cada lista de permissões deve ser armazenada separadamente como seu próprio objeto do S3.
- Classes de armazenamento — Uma lista de permissões deve ser armazenada diretamente no Amazon S3 usando uma das seguintes classes de armazenamento: Redundância reduzida

(RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone — IA, S3 Standard ou S3 Standard-IA.

- Controle de versão — Quando você adiciona uma lista de permissões a um bucket do S3, recomendamos que você também habilite o controle de versão para o bucket. Em seguida, você pode usar valores de data e hora para correlacionar versões da lista com os resultados de trabalhos de descoberta de dados confidenciais e ciclos automatizados de descoberta de dados confidenciais que usam a lista. Isso pode ajudar nas auditorias ou investigações de privacidade e proteção de dados que você realiza.
- Bloqueio de objeto — Para evitar que uma lista de permissões seja excluída ou substituída por um determinado período ou indefinidamente, você pode habilitar o Bloqueio de objeto para o bucket do S3 que armazena a lista. Habilitar essa configuração não impede que o Macie acesse a lista. Para obter informações sobre essa configuração, consulte Usar o bloqueio de objeto do S3 no Guia do usuário do Amazon Simple Storage Service.

Requisitos de criptografia/descriptografia

Se você criptografar uma lista de permissões no Amazon S3, a política de permissões para a função vinculada ao serviço Macie normalmente concede ao Macie as permissões necessárias para descriptografar a lista. No entanto, isso depende do tipo de criptografia usada:

- Se uma lista for criptografada usando criptografia do lado do servidor com uma chave gerenciada do Amazon S3 (SSE-S3), o Macie poderá descriptografar a lista. A função vinculada ao serviço da sua conta Macie concede à Macie as permissões de que ela precisa.
- Se uma lista for criptografada usando criptografia do lado do servidor com um AWS gerenciado AWS KMS key (DSSE-KMS ou SSE-KMS), o Macie poderá descriptografar a lista. A função vinculada ao serviço da sua conta Macie concede à Macie as permissões de que ela precisa.
- Se uma lista for criptografada usando criptografia do lado do servidor com um cliente gerenciado AWS KMS key (DSSE-KMS ou SSE-KMS), o Macie só poderá descriptografar a lista se você permitir que o Macie use a chave. Para aprender a fazer isso, consulte Permitir que o Macie use uma AWS KMS key gerenciada pelo cliente.

> **Note**
>
> Você pode criptografar uma lista com um cliente gerenciado AWS KMS key em um armazenamento de chaves externo. No entanto, a chave pode, então, ser mais lenta e menos confiável do que uma chave totalmente gerenciada no AWS KMS. Se a latência ou um problema de disponibilidade impedir o Macie de decifrar a lista, o Macie não

usará a lista ao analisar objetos do S3. Isso pode produzir resultados inesperados, como descobertas de dados confidenciais para texto que você especificou na lista. Para reduzir esse risco, considere armazenar a lista em um bucket do S3 configurado para usar a chave como chave do bucket do S3.
Para obter informações sobre o uso de chaves KMS em repositórios de chaves externos, consulte Repositórios de chaves externos no Guia do desenvolvedor do AWS Key Management Service. Para obter informações sobre como usar chaves de bucket do S3, consulteReduzindo o custo do SSE-KMS com chaves de bucket do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

- Se uma lista for criptografada usando a criptografia do lado do servidor com uma chave fornecida pelo cliente (SSE-C) ou a criptografia do lado do cliente, o Macie não poderá descriptografar a lista. Em vez disso, considere usar a criptografia SSE-S3, DSSE-KMS ou SSE-KMS.

Se uma lista for criptografada com uma chave KMS AWS gerenciada ou uma chave KMS gerenciada pelo cliente, sua identidade AWS Identity and Access Management (IAM) também deverá ter permissão para usar a chave. Caso contrário, você não poderá criar ou atualizar as configurações da lista ou verificar o status da lista usando o Macie. Para saber como verificar ou alterar as permissões de uma chave KMS, consulte Políticas de chaves AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Para obter informações detalhadas sobre as opções de criptografia para dados do Amazon S3, consulte Proteção de dados com criptografia no Guia do usuário do Amazon Simple Storage Service.

Considerações e recomendações de design

Em geral, Macie trata cada entrada em uma lista de permissões como um valor literal de string. Ou seja, Macie ignora cada ocorrência de texto que corresponda exatamente a uma entrada completa em uma lista de permissões. As correspondências não fazem distinção entre maiúsculas e minúsculas.

No entanto, o Macie usa as entradas como parte de uma estrutura maior de extração e análise de dados. A estrutura inclui funções de aprendizado de máquina e correspondência de padrões que fatoram dimensões como variações gramaticais e sintáticas e, em muitos casos, proximidade de palavras-chave. A estrutura também considera o tipo de arquivo ou formato de armazenamento de um objeto S3. Portanto, lembre-se das seguintes considerações e recomendações ao adicionar e gerenciar as entradas em uma lista de permissões.

Prepare-se para diferentes tipos de arquivos e formatos de armazenamento

Para dados não estruturados, como texto em um arquivo Adobe Portable Document Format (.pdf), o Macie ignora o texto que corresponde exatamente a uma entrada completa em uma lista de permissões, incluindo texto que abrange várias linhas ou páginas.

Para dados estruturados, como dados colunares em um arquivo CSV ou dados baseados em registros em um arquivo JSON, o Macie ignora o texto que corresponda exatamente a uma entrada completa em uma lista de permissões se todo o texto estiver armazenado em um único campo, célula ou matriz. Esse requisito não se aplica a dados estruturados armazenados em um arquivo não estruturado, como uma tabela em um arquivo.pdf.

Por exemplo, considere o seguinte conteúdo em um arquivo CSV:

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

Se `Akua Mansa` e `John Doe` forem entradas em uma lista de permissões, o Macie ignorará esses nomes no arquivo CSV. O texto completo de cada entrada da lista é armazenado em um único `Name` campo.

Por outro lado, considere um arquivo CSV que contenha as seguintes colunas e campos:

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

Se `Akua Mansa` e `John Doe` forem entradas em uma lista de permissões, o Macie não ignorará esses nomes no arquivo CSV. Nenhum dos campos no arquivo CSV contém o texto completo de uma entrada na lista de permissões.

Inclua variações comuns

Adicione entradas para variações comuns de dados numéricos, nomes próprios, termos e sequências de caracteres alfanuméricos. Por exemplo, se você adicionar nomes ou frases que contenham somente um espaço entre as palavras, adicione também variações que incluam dois espaços entre as palavras. Da mesma forma, adicione palavras e frases que contenham ou não caracteres especiais e considere incluir variações sintáticas e semânticas comuns.

Para o número de telefone 425-555-0100 dos EUA, por exemplo, você pode adicionar essas entradas a uma lista de permissões:

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

Para a data de 1º de fevereiro de 2022 em um contexto multinacional, você pode adicionar entradas que incluam variações sintáticas comuns para inglês e francês, incluindo variações que incluem e não incluem caracteres especiais:

```
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 nomes de pessoas, inclua entradas para várias formas de nome que você não considera confidenciais. Por exemplo, inclua: o nome seguido pelo sobrenome; o sobrenome seguido pelo nome, o nome e o sobrenome separados por um espaço; o nome e o sobrenome separados por dois espaços; e apelidos.

Para o nome Martha Rivera, por exemplo, você pode adicionar:

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

Se você quiser ignorar variações de um nome específico que contém muitas partes, crie uma lista de permissões que use uma expressão regular em vez disso. Por exemplo, para o nome Dra. Martha Lyda Rivera, PhD, você pode usar a seguinte expressão regular: `^(Dr. )?Martha \s(Lyda|L\.)?\s?Rivera,?( PhD)?$`

Opções e requisitos para expressões regulares em listas de permissões

Para esse tipo de lista de permissões, você especifica uma expressão regular (regex) que define um padrão de texto a ser ignorado — por exemplo, números de telefone públicos da sua organização, endereços de e-mail do domínio da sua organização ou dados de amostra padronizados que sua organização usa para testes. O regex define um padrão comum para um tipo específico de dados que você não considera confidenciais. Se você usar esse tipo de lista de permissões, o Amazon Macie não relatará ocorrências de texto que correspondam completamente ao padrão especificado. Ao contrário de uma lista de permissões que especifica texto predefinido a ser ignorado, você cria e armazena a regex e todas as outras configurações de lista no Macie.

Ao criar ou atualizar esse tipo de lista de permissões, você pode testar o regex da lista com dados de amostra antes de salvar a lista. Recomendamos fazer isso com vários conjuntos de dados de amostra. Se você criar um regex muito geral, o Macie poderá ignorar ocorrências de texto que você considera confidenciais. Se um regex for muito específico, o Macie pode não ignorar ocorrências de texto que você não considera confidenciais. Para se proteger contra expressões malformadas ou de longa duração, o Macie também compila e testa automaticamente o regex em uma coleção de texto de amostra e notifica você sobre problemas a serem resolvidos.

Para testes adicionais, recomendamos que você também teste o regex da lista com um conjunto pequeno e representativo de dados da sua conta ou organização. Para fazer isso, você pode criar um trabalho único e configurar o trabalho para usar a lista, além dos identificadores de dados gerenciados e identificadores de dados personalizados que você normalmente usa para analisar dados. Em seguida, você pode analisar os resultados do trabalho — descobertas de dados confidenciais, resultados de detecções de dados confidenciais ou ambos. Se os resultados do trabalho forem diferentes do esperado, você poderá alterar e testar o regex até que os resultados sejam os esperados.

Depois de configurar e testar uma lista de permissões, você pode criar e configurar trabalhos adicionais para usá-la ou adicioná-la às configurações automatizadas de descoberta de dados confidenciais da sua conta. Quando esses trabalhos são executados ou o Macie realiza uma descoberta automatizada para sua conta, o Macie usa a versão mais recente do regex da lista para analisar os dados.

Tópicos

- Suporte e recomendações de sintaxe
- Exemplos

Suporte e recomendações de sintaxe

Uma lista de permissões pode especificar uma expressão regular (regex) que contém até 512 caracteres. O Macie suporta um subconjunto da sintaxe do padrão regex fornecida pela biblioteca Perl Compatible Regular Expressions (PCRE). Das estruturas fornecidas pela biblioteca PCRE, o Macie não suporta os seguintes elementos de padrão:

- Referências anteriores
- Capturar grupos
- Padrões condicionais
- Código incorporado
- Sinalizadores de padrões globais, como `/i`, `/m` e `/x`
- Padrões recursivos
- Afirmações positivas e negativas de largura zero de retrospectiva e prospectiva, como e `?=`, `?!`, `?<=` e `?<!`.

Para criar padrões de regex eficazes para listas de permissões, observe também as dicas e recomendações a seguir:

- Âncoras — Use âncoras (^ou$) somente se você espera que o padrão apareça no início ou no final de um arquivo, não no início ou no final de uma linha.
- Repetições limitadas — Por motivos de desempenho, o Macie reduz o tamanho dos grupos de repetição limitados. Por exemplo, `\d{100,1000}` não compilará no Macie. Para aproximar essa funcionalidade, você pode usar uma repetição aberta, como `\d{100,}`.
- Insensibilidade a maiúsculas e minúsculas — Para tornar partes de um padrão insensíveis a maiúsculas e minúsculas, você pode usar a `(?i)` estrutura em vez do `/i` sinalizador.
- Desempenho — Não há necessidade de otimizar prefixos ou alternâncias manualmente. Por exemplo, mudar `/hello|hi|hey/` para `/h(?:ello|i|ey)/` não melhorará o desempenho.
- Curingas — Por motivos de desempenho, Macie limita o número de curingas repetidas. Por exemplo, `a*b*a*` não compilará no Macie.
- Alternação — Para especificar mais de um padrão em uma única lista de permissões, você pode usar o operador de alternância (`|`) para concatenar os padrões. Se você fizer isso, Macie usa a lógica OR para combinar os padrões e formar um novo padrão. Por exemplo, se você especificar`(apple|orange)`, Macie reconhecerá maçã e laranja como coincidentes e ignorará as

ocorrências de ambas as palavras. Se você concatenar padrões, certifique-se de limitar o tamanho total da expressão concatenada a 512 caracteres ou menos.

Por fim, ao desenvolver o regex, projete-o para acomodar diferentes tipos de arquivo e formatos de armazenamento. O Macie usa o regex como parte de uma estrutura maior de extração e análise de dados. A estrutura considera o tipo de arquivo ou formato de armazenamento de um objeto do S3. Para dados estruturados, como dados colunares em um arquivo CSV ou dados baseados em registros em um arquivo JSON, o Macie ignora textos que correspondam completamente ao padrão somente se todo o texto estiver armazenado em um único campo, célula ou matriz. Esse requisito não se aplica a dados estruturados armazenados em um arquivo não estruturado, como uma tabela em um arquivo Adobe Portable Document Format (.pdf). Para dados não estruturados, como texto em um arquivo.pdf, o Macie ignora textos que correspondam completamente ao padrão, incluindo textos que se estendem por várias linhas ou páginas.

Exemplos

Os exemplos a seguir demonstram padrões de regex válidos para alguns cenários comuns.

Endereços de e-mail

Se você usar um identificador de dados personalizado para detectar endereços de e-mail, poderá ignorar endereços de e-mail que não considere confidenciais, como endereços de e-mail da sua organização.

Para ignorar endereços de e-mail de um determinado domínio de segundo e primeiro nível, você pode usar esse padrão:

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

Onde *exemplo* é o nome do domínio de segundo nível e *com* é o domínio de primeiro nível. Nesse caso, Macie combina e ignora endereços como johndoe@example.com e john.doe@example.com.

Para ignorar endereços de e-mail de um domínio específico em qualquer domínio genérico de primeiro nível (gTLD), como .com ou .gov, você pode usar esse padrão:

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

Onde *exemplo* é o nome do domínio. Nesse caso, Macie combina e ignora endereços como johndoe@example.com, john.doe@example.gov e johndoe@example.edu.

Para ignorar endereços de e-mail de um domínio específico em qualquer domínio de primeiro nível com código de país (ccTLD), como .ca para o Canadá ou .au para a Austrália, você pode usar esse padrão:

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

Onde *exemplo* é o nome do domínio e *ca* e *au* são ccTLDs específicos a serem ignorados. Nesse caso, Macie combina e ignora endereços como johndoe@example.ca e john.doe@example.au.

Para ignorar endereços de e-mail que são de um determinado domínio e gTLD e incluir domínios de terceiro e quarto níveis, você pode usar esse padrão:

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

Onde *exemplo* é o nome do domínio e *com* é o gTLD. Nesse caso, Macie combina e ignora endereços como johndoe@www.example.com e john.doe@www.team.example.com.

Números de telefone

O Macie fornece identificadores de dados gerenciados que podem detectar números de telefone de vários países e regiões. Para ignorar determinados números de telefone, como números gratuitos ou números de telefone públicos da sua organização, você pode usar padrões como os seguintes.

Para ignorar números de telefone gratuitos dos EUA que usam o código de área 800 e estão formatados como (800) ###-####:

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

Para ignorar números de telefone gratuitos dos EUA que usam o código de área 888 e estão formatados como (888) ###-####:

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

Para ignorar números de telefone franceses de 10 dígitos que incluem o código do país 33 e estão formatados como +33 ## ## ## ## ##:

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

Para ignorar os números de telefone dos EUA e do Canadá que usam códigos de área e de câmbio específicos, não inclua um código de país e estão formatados como (###) ###-####:

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

Onde *123* é o código de área e *555* é o código de troca.

Para ignorar os números de telefone dos EUA e do Canadá que usam códigos de área e de câmbio específicos, inclua um código de país e estejam formatados como +1 (###) ###-####:

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

Onde *123* é o código de área e *555* é o código de troca.

Criação e gerenciamento de listas de permissão no Amazon Macie

No Amazon Macie, uma lista de permissões define um texto específico ou um padrão de texto que você deseja que o Macie deverá ignorar ao inspecionar objetos do Amazon Simple Storage Service (Amazon S3) em busca de dados em busca de dados confidenciais. Se o texto corresponder a uma entrada ou padrão em uma lista de permissões, o Macie não relatará o texto em descobertas de dados confidenciais, estatísticas ou outros tipos de resultados, mesmo que o texto corresponda aos critérios de um identificador de dados gerenciados ou de um identificador de dados personalizado.

Você pode criar e gerenciar os seguintes tipos de listas de permissão no Macie.

Texto predefinido

Use esse tipo de lista para especificar palavras, frases e outros tipos de sequências de caracteres que não são sensíveis, não têm probabilidade de mudar e não necessariamente aderem a um padrão comum. Os exemplos são os nomes dos representantes públicos da sua organização, números de telefone específicos e dados de amostra específicos que sua organização usa para testes. Se você usar esse tipo de lista, o Macie ignorará um texto que corresponder exatamente a uma entrada da lista.

Para esse tipo de lista, você cria um arquivo de texto simples delimitado por linha que lista o texto específico a ser ignorado. Em seguida, você armazena o arquivo em um bucket S3 e define as configurações para que o Macie acesse a lista no bucket. Em seguida, você pode criar e configurar trabalhos de descoberta de dados confidenciais para usar a lista ou adicioná-la às configurações automatizadas de descoberta de dados confidenciais da sua conta. Quando cada trabalho começa a ser executado ou o próximo ciclo automatizado de análise de descoberta começa, Macie recupera a versão mais recente da lista no Amazon S3. Em seguida, o Macie usa essa versão da lista ao inspecionar objetos do S3 em busca de dados confidenciais. Se o Macie

encontrar um texto que corresponda exatamente a uma entrada da lista, o Macie não reportará essa ocorrência de texto como dados confidenciais.

Expressão regular

Use este tipo de lista para especificar uma expressão regular (regex) que defina um padrão de texto a ser ignorado. Os exemplos são números de telefone públicos da sua organização, endereços de e-mail do domínio da sua organização e dados de amostra padronizados que sua organização usa para testes. Se você usar esse tipo de lista, o Macie ignorará o texto que corresponda completamente ao padrão regex definido pela lista.

Para esse tipo de lista, você cria um regex que define um padrão comum para um texto que não é confidencial mas que varia ou pode ser alterado. Ao contrário de uma lista de texto predefinido, você cria e armazena o regex e todas as outras configurações de lista no Macie. Em seguida, você pode criar e configurar trabalhos de descoberta de dados confidenciais para usar a lista ou adicioná-la às configurações automatizadas de descoberta de dados confidenciais da sua conta. Quando esses trabalhos são executados ou quando o Macie realiza uma descoberta automática para sua conta, o Macie usa a versão mais recente do regex da lista para analisar os dados. Se o Macie encontrar um texto que corresponda exatamente ao padrão definido pela lista, o Macie não reportará essa ocorrência de texto como dados confidenciais.

Para obter requisitos detalhados, recomendações e exemplos de cada tipo de lista, consulte Permitir opções e requisitos de listas. Você pode criar até 10 listas de permissão para sua conta em cada Região da AWS compatível, até cinco listas de permissão que especificam texto predefinido e até cinco listas de permissão que especificam expressões regulares. Você pode criar e usar listas de permissões em todas as Regiões da AWS em que o Macie está atualmente disponível, exceto na região Asia Pacific (Osaka).

Para criar e gerenciar listas de permissões, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Os tópicos a seguir explicam como. Para a API, os tópicos incluem exemplos de como realizar essas tarefas usando o AWS Command Line Interface (AWS CLI). Você também pode realizar essas tarefas usando uma versão atual de outra ferramenta de linha de comando da AWS ou de um AWS SDK, ou enviando solicitações HTTPS diretamente para o Macie. Para obter informações sobre ferramentas e SDKs AWS, consulte Ferramentas para construir na AWS.

Tópicos

- Criação de listas de permissões
- Verificar o status das listas de permissão

- Alterando as listas de permissões
- Excluindo listas de permissões

Criação de listas de permissões

A forma como você cria uma lista de permissões no Amazon Macie depende do tipo de lista que você deseja criar. Uma lista de permissões pode ser um arquivo que lista texto predefinido a ser ignorado ou pode ser uma expressão regular (regex) que define um padrão de texto a ser ignorado. Escolha a seção do tipo de lista que você deseja criar.

Texto predefinido

Antes de criar esse tipo de lista de permissões no Macie, execute as seguintes etapas:

1. Usando um editor de texto, crie um arquivo de texto simples delimitado por linha que lista texto específico a ser ignorado — por exemplo, um arquivo.txt, .text ou.plain. Para obter mais informações, consulte Requisitos de sintaxe para listas de texto predefinido.
2. Faça upload do arquivo em um bucket do S3 e anote o nome do bucket e do objeto. Você precisará inserir esses nomes ao definir as configurações no Macie.
3. Certifique-se de que as configurações do bucket e do objeto do S3 permitam que você e o Macie recuperem a lista do bucket. Para obter mais informações, consulte Requisitos de armazenamento para listas de texto predefinido.
4. Se você criptografou o objeto do S3, certifique-se de que ele esteja criptografado com uma chave que você e o Macie tenham permissão para usar. Para obter mais informações, consulte Requisitos de criptografia/descriptografia para listas de texto predefinido.

Depois de executar essas etapas, você estará pronto para definir as configurações da lista no Macie. Você pode definir as configurações usando o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para definir as configurações de uma lista de permissões usando o console do Amazon Macie.

Para definir as configurações da lista de permissões no Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. No painel de navegação, em Configurações, selecione Listas de permissões.
3. Na página Listas de permissões, escolha Criar.
4. Em Selecionar um tipo de lista, escolha Texto predefinido.
5. Em Configurações da lista, use as seguintes opções para inserir configurações adicionais para a lista de permissões:

   - Em Nome, insira um nome para a regra. Um nome pode conter até 128 caracteres.
   - Para Descrição, insira opcionalmente uma breve descrição da lista. A descrição pode conter até 512 caracteres.
   - Em Nome do bucket do S3, insira o nome completo do bucket que armazena a lista.

     No Amazon S3, você pode encontrar esse valor no campo Nome das propriedades do bucket. Esse valor diferencia maiúsculas de minúsculas. Além disso, não use caracteres curinga ou valores parciais ao inserir o nome.
   - Em Nome do objeto do S3, insira o nome completo do objeto do S3 que armazena a lista.

     No Amazon S3, você pode encontrar esse valor no campo Chave das propriedades do objeto. Se o nome incluir um caminho, certifique-se de incluir o caminho completo ao inserir o nome, por exemplo **`allowlists/macie/mylist.txt`**. Esse valor diferencia maiúsculas de minúsculas. Além disso, não use caracteres curinga ou valores parciais ao inserir o nome.
6. (Opcional) Em Tags, escolha Adicionar tag e insira até 50 tags para atribuir à lista de permissões.

   Tag é um rótulo que você define e atribui a determinados tipos de recursos da AWS. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional. As tags podem ajudar a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.
7. Ao concluir, selecione Create.

Macie testa as configurações da lista. O Macie também verifica se pode recuperar a lista do Amazon S3 e analisar o conteúdo da lista. Se ocorrer um erro, o Macie exibirá uma mensagem que descreve o erro. Para obter informações detalhadas que podem ajudar você a resolver o erro, consulte Opções e requisitos para listas de texto predefinido. Depois de corrigir qualquer erro, você pode salvar as configurações da lista.

API

Para definir as configurações da lista de permissões programaticamente, use a operação CreateAllowList da API do Amazon Macie e especifique os valores apropriados para os parâmetros necessários.

Para o parâmetro `criteria`, use um objeto `s3WordsList` para especificar o nome do bucket do S3 (`bucketName`) e o nome do objeto do S3 (`objectKey`) que armazena a lista. Para determinar o nome do bucket, consulte o campo `Name` no Amazon S3. Para determinar o nome do objeto, consulte o campo `Key` no Amazon S3. Observe que esses valores diferenciam maiúsculas de minúsculas. Além disso, não use caracteres curinga ou valores parciais ao especificar esses nomes.

Para definir as configurações usando o AWS CLI, execute o comando create-allow-list e especifique os valores apropriados para os parâmetros necessários. Os exemplos a seguir mostram como definir as configurações de uma lista de permissões armazenada em um bucket do S3 chamado *DOC-EXAMPLE-BUCKET*. O nome do objeto S3 que armazena a lista é *allowlists/macie/mylist.txt*.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade.

```
$ 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 exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
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."
```

Quando você envia sua solicitação, o Macie testa as configurações da lista. O Macie também verifica se pode recuperar a lista do Amazon S3 e analisar o conteúdo da lista. Se ocorrer um erro, sua solicitação falhará e o Macie retornará uma mensagem descrevendo o erro. Para obter

informações detalhadas que podem ajudar você a resolver o erro, consulte Opções e requisitos para listas de texto predefinido.

Se o Macie puder recuperar e analisar a lista, sua solicitação será bem-sucedida e você receberá um resultado semelhante ao seguinte.

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

Onde `arn` está o nome do recurso da Amazon (ARN) da lista de permissões que foi criada e `id` é o identificador exclusivo da lista.

Depois de salvar as configurações da lista, você pode criar e configurar trabalhos de descoberta de dados confidenciais para usar a lista ou adicionar a lista às suas configurações automatizadas de descoberta de dados confidenciais. Cada vez que esses trabalhos começam a ser executados ou um ciclo automatizado de análise de descoberta é iniciado, o Macie recupera a versão mais recente da lista no Amazon S3. Em seguida, Macie usa essa versão da lista ao analisar os dados.

Expressão regular

Ao criar uma lista de permissões que especifica uma expressão regular (regex), você define a regex e todas as outras configurações da lista diretamente no Macie. O Macie suporta um subconjunto da sintaxe do padrão regex fornecida pela biblioteca Perl Compatible Regular Expressions (PCRE). Para obter mais informações, consulte Suporte e recomendações de sintaxe.

Você pode criar esse tipo de lista usando o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para criar uma lista de permissões usando o console do Amazon Macie.

Para criar uma lista de permissões

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Listas de permissões.
3. Na página Listas de permissões, escolha Criar.

4. Em Selecionar um tipo de lista, escolha Expressão regular.
5. Em Configurações da lista, use as seguintes opções para inserir configurações adicionais para a lista de permissões:

   - Em Nome, insira um nome para a regra. Um nome pode conter até 128 caracteres.
   - Para Descrição, insira opcionalmente uma breve descrição da lista. A descrição pode conter até 512 caracteres.
   - A expressão regular, insira a regex que define o padrão de texto a ser ignorado. A regex pode conter até 512 caracteres.
6. (Opcional) Em Avaliar, insira até 1.000 caracteres na caixa Dados de exemplo e escolha Testar para testar o regex. Macie avalia os dados da amostra e relata o número de ocorrências de texto que correspondem ao regex. Você pode repetir essa etapa quantas vezes quiser para refinar e otimizar o regex.

   > **Note**
   >
   > Recomendamos que você teste e refine o regex com vários conjuntos de dados de amostra. Se você criar um regex muito geral, o Macie poderá ignorar ocorrências de texto que você considera confidenciais. Se um regex for muito específico, o Macie pode não ignorar ocorrências de texto que você não considera confidenciais.
7. (Opcional) Em Tags, escolha Adicionar tag e insira até 50 tags para atribuir à lista de permissões.

   Tag é um rótulo que você define e atribui a determinados tipos de recursos da AWS. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional. As tags podem ajudar a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.
8. Ao concluir, selecione Create.

Macie testa as configurações da lista. O Macie também testa o regex para verificar se ele pode compilar a expressão. Se ocorrer um erro, o Macie exibirá uma mensagem que descreve o erro. Para obter informações detalhadas que podem ajudar você a resolver o erro, consulte Opções e requisitos para expressões regulares em listas de permissões. Depois de corrigir qualquer erro, você pode salvar a lista de permissões.

API

Antes de criar esse tipo de lista de permissões no Macie, recomendamos que você teste e refine a expressão regular com vários conjuntos de dados de amostra. Se você criar um regex muito geral, o Macie poderá ignorar ocorrências de texto que você considera confidenciais. Se um regex for muito específico, o Macie pode não ignorar ocorrências de texto que você não considera confidenciais.

Para testar uma expressão com o Macie, você pode usar a operação testCustomDataIdentifier da API do Amazon Macie ou, para o AWS CLI, executar o comando test-custom-data-identifier. O Macie usa o mesmo código subjacente para compilar expressões para listas de permissões e identificadores de dados personalizados. Se você testar uma expressão dessa forma, certifique-se de especificar valores somente para os parâmetros `regex` e `sampleText`. Caso contrário, você receberá resultados imprecisos.

Quando você estiver pronto para criar esse tipo de lista de permissões, use a operação CreateAllowList da API do Amazon Macie e especifique os valores apropriados para os parâmetros necessários. Para o parâmetro `criteria`, use o campo `regex` para especificar a expressão regular que define o padrão de texto a ser ignorado. A expressão pode conter até 512 caracteres.

Para criar esse tipo de lista usando o AWS CLI, execute o comando create-allow-list e especifique os valores apropriados para os parâmetros necessários. Os exemplos a seguir criam uma lista de permissões chamada *`my_allow_list`*. O regex foi criado para ignorar todos os endereços de e-mail que um identificador de dados personalizado poderia detectar no domínio `example.com`.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade.

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

Este exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
```

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

Quando você envia sua solicitação, o Macie testa as configurações da lista. O Macie também testa o regex para verificar se ele pode compilar a expressão. Se ocorrer um erro, a solicitação falhará e o Macie retornará uma mensagem descrevendo o erro. Para obter informações detalhadas que podem ajudar você a resolver o erro, consulte Opções e requisitos para expressões regulares em listas de permissões.

Se o Macie puder compilar a expressão, a solicitação será bem-sucedida e você receberá um resultado semelhante a este:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Onde `arn` está o nome do recurso da Amazon (ARN) da lista de permissões que foi criada e `id` é o identificador exclusivo da lista.

Depois de salvar a lista, você pode criar e configurar trabalhos de descoberta de dados confidenciais para usá-la ou adicioná-la às suas configurações automatizadas de descoberta de dados confidenciais. Quando esses trabalhos são executados ou quando o Macie realiza uma descoberta automática para sua conta, o Macie usa a versão mais recente do regex da lista para analisar os dados.

Verificar o status das listas de permissão

É importante verificar o status de suas listas de permissão periodicamente. Caso contrário, erros podem fazer com que o Amazon Macie produza resultados de análise inesperados, como descobertas de dados confidenciais para textos que você especificou em uma lista de permissões.

Se você configurar uma tarefa de descoberta de dados confidenciais para usar uma lista de permissões e o Macie não conseguir acessar ou usar a lista quando a tarefa começar a ser executada, a tarefa continuará sendo executada. No entanto, Macie não usa a lista ao analisar objetos do S3. Da mesma forma, se um ciclo de análise for iniciado para a descoberta automatizada de dados confidenciais e o Macie não puder acessar ou usar uma lista de permissões especificada, a análise continuará, mas o Macie não usará a lista.

É improvável que ocorram erros em uma lista de permissões que especifica uma expressão regular (regex). Isso ocorre em parte porque o Macie testa automaticamente o regex quando você cria ou atualiza as configurações da lista. Além disso, você armazena o regex e todas as outras configurações da lista no Macie.

No entanto, podem ocorrer erros em uma lista de permissões que especifica texto predefinido, em parte porque você armazena a lista no Amazon S3, não no Macie. As causas comuns de erros são:

- O bucket ou objeto do S3 é excluído.
- O bucket ou objeto do S3 é renomeado e as configurações da lista no Macie não especificam o novo nome.
- As configurações de permissões do bucket do S3 são alteradas e o Macie perde o acesso ao bucket e ao objeto.
- As configurações de criptografia do bucket do S3 foram alteradas e o Macie não consegue descriptografar o objeto que armazena a lista.
- A política da chave de criptografia é alterada e Macie perde o acesso à chave. Macie não consegue decifrar o objeto do S3 que armazena a lista.

> **Important**
>
> Como esses erros afetam os resultados de suas análises, recomendamos que você verifique o status de suas listas de permissões periodicamente. Recomendamos que você também faça isso se alterar as permissões ou as configurações de criptografia de um bucket do S3 que armazena uma lista de permissões ou alterar a política de uma chave AWS Key Management Service (AWS KMS) usada para criptografar uma lista.

Você pode verificar o status de suas listas de permissão usando o console do Amazon Macie ou a API do Amazon Macie. Para obter informações detalhadas que podem ajudá-lo a solucionar erros que ocorrem, consulte Opções e requisitos para listas de texto predefinido.

Console

Siga estas etapas para verificar o status de suas listas de permissão usando o console do Amazon Macie.

Para verificar o status de suas listas de permissão

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Listas de permissões.
3. Na página Permitir listas, escolha atualizar ().

   O Macie testa as configurações de todas as suas listas de permissão e atualiza o campo Status para indicar o status atual de cada lista.

   Se uma lista especificar uma expressão regular, seu status normalmente será OK. Isso significa que o Macie pode compilar a expressão. Se uma lista especificar um texto predefinido, seu status poderá ser qualquer um dos seguintes valores.

   OK

   O Macie pode recuperar e analisar o conteúdo da lista.

   Acesso negado

   Macie não tem permissão para acessar o objeto do S3 que armazena a lista. O Amazon S3 negou a solicitação de recuperação do objeto. Uma lista também pode ter esse status se o objeto for criptografado com um AWS KMS key gerenciado pelo cliente que o Macie não tem permissão de usar.

   Para resolver esse erro, revise a política do bucket e outras configurações de permissões do bucket e do objeto. Certifique-se de que o Macie tenha permissão para acessar e recuperar o objeto. Se o objeto for criptografado com uma chave do AWS KMS gerenciada pelo cliente, revise também a política de chaves e certifique-se de que Macie tenha permissão para usar a chave.

   Erro

   Ocorreu um erro transitório ou interno quando o Macie tentou recuperar ou analisar o conteúdo da lista. Uma lista de permissões também poderá ter esse status se estiver criptografada com uma chave de criptografia que o Amazon S3 e o Macie não possam acessar ou usar.

   Para resolver esse erro, aguarde alguns minutos e escolha refresh ()

novamente. Se o status continuar sendo Erro, verifique as configurações de criptografia do objeto S3. Certifique-se de que o objeto seja criptografado com uma chave que o Amazon S3 e o Macie possam acessar e usar.

O objeto está vazio

O Macie pode recuperar a lista do Amazon S3 mas a lista não tem nenhum conteúdo.

Para resolver esse erro, baixe o objeto do Amazon S3 e certifique-se de que ele contenha as entradas corretas. Se as entradas estiverem corretas, revise as configurações da lista no Macie. Verifique se os nomes especificados do bucket e do objeto estão corretos.

Objeto não encontrado

A lista não existe no Amazon S3.

Para solucionar esse erro, revise as configurações da lista no Macie. Verifique se os nomes especificados do bucket e do objeto estão corretos.

Cota excedida

Macie pode acessar a lista no Amazon S3. No entanto, o número de entradas na lista ou o tamanho do armazenamento da lista excede a cota de uma lista de permissões.

Para resolver esse erro, divida a lista em vários arquivos. Certifique-se de que cada arquivo contenha menos de 100.000 entradas. Certifique-se também de que o tamanho de cada arquivo seja menor que 35 MB. Em seguida, faça o upload de cada arquivo no Amazon S3. Ao terminar, defina as configurações da lista de permissões no Macie para cada arquivo. Você pode ter até cinco listas de texto predefinidos em cada Região da AWS suportada.

Limitados

O Amazon S3 limitou a solicitação para recuperar a lista.

Para resolver esse erro, aguarde alguns minutos e escolha refresh
()
novamente.

Acesso do usuário negado

O Amazon S3 negou a solicitação de recuperação do objeto. Se o objeto especificado existir, você não tem permissão para acessá-lo ou ele está criptografado com uma chave do AWS KMS que você não tem permissão de usar.

Para resolver esse erro, trabalhe com seu administrador AWS para garantir que as configurações da lista especifiquem os nomes corretos do bucket e do objeto e que você tenha acesso de leitura ao bucket e ao objeto. Se o objeto for criptografado, certifique-se também de que ele seja criptografado com uma chave que o Macie tenha permissão de usar.

4. Para revisar as configurações e o status de uma lista específica, escolha o nome da lista.

API

Para verificar o status de uma lista de permissões programaticamente, use a operação GetAllowList da API Amazon Macie ou, para o AWS CLI, execute o comando get-allow-list.

Para o parâmetro `id`, especifique o identificador exclusivo da lista de permissões cujo status você deseja verificar. Para obter esse identificador, você pode usar a operação ListAllowLists. A operação ListAllowLists recupera informações sobre todas as listas de permissão da sua conta. Se você estiver usando o AWS CLI, você pode executar o comando list-allow-lists para recuperar essas informações.

Quando você envia uma solicitação GetAllowList, o Macie testa todas as configurações da lista de permissões. Se as configurações especificarem uma expressão regular (regex), o Macie verifica se ele pode compilar a expressão. Se as configurações especificarem uma lista de texto predefinido, o Macie verifica se ele pode recuperar e analisar a lista.

Em seguida, Macie retorna um objeto `GetAllowListResponse` que fornece os detalhes da lista de permissões. No objeto `GetAllowListResponse`, o objeto `status` indica o status atual da lista: um código de status (`code`) e, dependendo do código de status, uma breve descrição do status da lista (`description`).

Se a lista de permissões especificar um regex, o código de status normalmente é `OK` e não há uma descrição associada. Isso significa que Macie compilou a expressão com sucesso.

Se a lista de permissões especificar um texto predefinido, o código de status varia de acordo com os resultados do teste:

- Se Macie recuperou e analisou a lista com sucesso, o código de status é `OK` e não há uma descrição associada.
- Se um erro impediu que o Macie recuperasse ou analisasse a lista, o código de status e a descrição indicarão a natureza do erro que ocorreu.

Para obter uma lista de possíveis códigos de status e uma descrição de cada um, consulte AllowListStatus na referência da API do Amazon Macie.

Alterando as listas de permissões

Depois de criar uma lista de permissões, você pode alterar a maioria das configurações da lista no Amazon Macie. Por exemplo, você pode alterar o nome e a descrição da lista e adicionar e editar as tags da lista. A única configuração que você não pode alterar é o tipo de lista. Por exemplo, se uma lista de permissões existente especificar uma expressão regular, você não poderá alterar seu tipo para texto predefinido.

Se uma lista de permissões especificar um texto predefinido, você também poderá alterar as entradas na lista. Para fazer isso, atualize o arquivo que contém as entradas e, em seguida, faça o upload da nova versão do arquivo para o Amazon S3. Na próxima vez que Macie se preparar para usar a lista, Macie recuperará a versão mais recente do arquivo do Amazon S3. Ao fazer o upload do novo arquivo, certifique-se de armazená-lo no mesmo bucket e objeto do S3. Ou, se você alterar o nome do bucket ou objeto, certifique-se de atualizar as configurações da lista no Macie.

Você pode alterar as configurações de uma lista de permissões usando o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para alterar as configurações de uma lista de permissões usando o console do Amazon Macie.

Para alterar uma lista de permissões

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Listas de permissões.
3. Na página Listas de permissões, escolha o nome da lista de permissões que você deseja alterar. A página da lista de permissões é aberta e exibe as configurações atuais da lista.

4. Para atribuir ou editar tags para a lista de permissões, escolha Gerenciar tags na seção Tags. Em seguida, altere as etiquetas conforme necessário. Ao concluir, escolha Save.
5. Para alterar outras configurações da lista de permissões, escolha Editar na seção Configurações da lista. Em seguida, altere as configurações desejadas:

   - Nome — Insira um novo nome para a lista. Um nome pode conter até 128 caracteres.
   - Descrição — Insira uma nova descrição da lista. A descrição pode conter até 512 caracteres.
   - Se a lista de permissões especificar um texto predefinido:
     - Nome do bucket do S3 — Insira o nome completo do bucket que atualmente armazena a lista.

       No Amazon S3, você pode encontrar esse valor no campo Nome das propriedades do bucket. Esse valor diferencia maiúsculas de minúsculas. Além disso, não use caracteres curinga ou valores parciais ao inserir o nome.
     - Nome do objeto do S3 — Insira o nome completo do objeto S3 que atualmente armazena a lista.

       No Amazon S3, você pode encontrar esse valor no campo Chave das propriedades do objeto. Se o nome incluir um caminho, certifique-se de incluir o caminho completo ao inserir o nome, por exemplo **`allowlists/macie/mylist.txt`**. Esse valor diferencia maiúsculas de minúsculas. Além disso, não use caracteres curinga ou valores parciais ao inserir o nome.
   - Se a lista de permissões especificar uma expressão regular (regex), insira uma nova regex na caixa Expressão regular. A regex pode conter até 512 caracteres.

     Depois de inserir o novo regex, teste-o opcionalmente. Para fazer isso, insira até 1.000 caracteres na caixa Dados da amostra e escolha Teste. Macie avalia os dados da amostra e relata o número de ocorrências de texto que correspondem ao regex. Você pode repetir essa etapa quantas vezes quiser para refinar e otimizar o regex antes de salvar suas alterações.

   Ao terminar de alterar as configurações, escolha Salvar.

Macie testa as configurações da lista. Para obter uma lista de texto predefinido, o Macie também verifica se ele pode recuperar a lista do Amazon S3 e analisar o conteúdo da lista. Para um

regex, o Macie também verifica se ele pode compilar a expressão. Se ocorrer um erro, o Macie exibirá uma mensagem que descreve o erro. Para obter informações detalhadas que podem ajudar você a resolver o erro, consulte Permitir opções e requisitos de listas. Depois de resolver qualquer erro, você poderá salvar as alterações.

API

Para alterar uma lista de permissões programaticamente, use a operação UpdateAllowList da API Amazon Macie ou, para o AWS CLI, execute o comando update-allow-list. Em sua solicitação, use os parâmetros compatíveis para especificar um novo valor para cada configuração que você deseja alterar. Observe que os parâmetros `criteria`, `id` e `name` são obrigatórios. Se você não quiser alterar o valor de um parâmetro obrigatório, especifique o valor atual do parâmetro.

Por exemplo, o comando a seguir altera o nome e a descrição de uma lista de permissões existente. O exemplo está formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
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"
```

Onde:

- *km2d4y22hp6rv05example* é o identificador exclusivo da lista.
- *my_allow_list-email* é o novo nome da lista.
- *[a-z]@example.com* é o critério da lista, uma expressão regular.
- *Ignora todos os endereços de e-mail do domínio example.com* é a nova descrição da lista.

Quando você envia sua solicitação, o Macie testa as configurações da lista. Se a lista especificar um texto predefinido, isso inclui verificar se o Macie pode recuperar a lista do Amazon S3 e analisar o conteúdo da lista. Se a lista especificar um regex, isso inclui verificar se o Macie pode compilar a expressão.

Se ocorrer um erro ao testar as configurações, sua solicitação falhará e o Macie retornará uma mensagem descrevendo o erro. Para obter informações detalhadas que podem ajudar você a

resolver o erro, consulte Permitir opções e requisitos de listas. Se a solicitação falhar por outro motivo, o Macie retornará uma resposta HTTP 4xx ou 500 que indica por que a operação falhou.

Se a sua solicitação for realizada com êxito, o Macie atualizará as configurações da lista e você receberá um resultado semelhante ao seguinte.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Onde `arn` está o nome do recurso da Amazon (ARN) da lista de permissões que foi atualizada e `id` é o identificador exclusivo da lista.

Excluindo listas de permissões

Ao excluir uma lista de permissões no Amazon Macie, você exclui permanentemente todas as configurações da lista. Essas configurações não podem ser recuperadas depois de excluídas. Se as configurações especificarem uma lista de texto predefinido que você armazena no Amazon S3, o Macie não excluirá o objeto do S3 que armazena a lista. Somente as configurações no Macie são excluídas.

Se você configurar trabalhos confidenciais de descoberta de dados para usar uma lista de permissões e, posteriormente, excluir a lista, os trabalhos serão executados conforme programado. No entanto, os resultados do seu trabalho, tanto descobertas de dados confidenciais quanto resultados de descoberta de dados confidenciais, podem relatar texto que você especificou anteriormente em uma lista de permissões. Da mesma forma, se você configurar a descoberta automática de dados confidenciais para usar uma lista e, posteriormente, excluir a lista, os ciclos diários de análises continuarão. No entanto, descobertas de dados confidenciais, estatísticas ou outros tipos de resultados podem relatar texto que você especificou anteriormente em uma lista de permissões.

Antes de excluir uma lista de permissões, recomendamos que você revise seu inventário de trabalhos para identificar trabalhos que usam a lista e estão programados para serem executados no futuro. No inventário, o painel de detalhes indica se um trabalho está configurado para usar qualquer lista de permissões e, em caso afirmativo, quais. Além disso, verifique suas configurações automatizadas de descoberta de dados confidenciais. Você pode determinar que é melhor alterar uma lista em vez de excluí-la.

Como proteção adicional, Macie verifica as configurações de todos os seus trabalhos quando você tenta excluir uma lista de permissões. Se você configurou trabalhos para usar a lista e qualquer um desses trabalhos tiver um status diferente de Concluído ou Cancelado, o Macie não excluirá a lista, a menos que você forneça uma confirmação adicional.

Você pode excluir uma lista de permissões usando o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para excluir uma lista de permissões usando o console do Amazon Macie.

Para excluir uma lista de permissões

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Listas de permissões.
3. Na página Listas de permissões, marque a caixa de seleção da lista de permissões que você deseja excluir.
4. No menu Ações, escolha Excluir.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Delete.

API

Para excluir uma lista de permissões programaticamente, use a operação DeleteAllowList da API do Amazon Macie. Para o parâmetro `id`, especifique o identificador exclusivo da lista de permissões a ser excluída. Você pode obter esse identificador usando a operação ListAllowLists. A operação ListAllowLists recupera informações sobre todas as listas de permissão da sua conta. Se você estiver usando o AWS CLI, você pode executar o comando list-allow-lists para recuperar essas informações.

Para o parâmetro `ignoreJobChecks`, especifique se deseja forçar a exclusão da lista, mesmo que trabalhos confidenciais de descoberta de dados estejam configurados para usar a lista:

- Se você especificar `false`, o Macie verifica as configurações de todos os seus trabalhos que têm um status diferente de `COMPLETE` ou `CANCELLED`. Se nenhum desses trabalhos estiver configurado para usar a lista, o Macie excluirá a lista permanentemente. Se algum desses trabalhos estiver configurado para usar a lista, o Macie rejeitará sua solicitação e retornará um

erro HTTP 400 (`ValidationException`). A mensagem de erro indica o número de trabalhos aplicáveis para até 200 trabalhos.

- Se você especificar `true`, o Macie excluirá a lista permanentemente sem verificar as configurações de nenhum dos seus trabalhos.

Para excluir uma lista de permissões usando o AWS CLI, execute o comando delete-allow-list. Por exemplo:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

Onde *nkr81bmtu2542yyexample* é o identificador exclusivo da lista de permissões a ser excluída.

Se a sua solicitação for realizada com êxito, o Macie retornará uma resposta HTTP 200 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500 que indica por que a operação falhou.

Se a lista de permissões especificar um texto predefinido, você pode, opcionalmente, excluir o objeto do S3 que armazena a lista. No entanto, manter esse objeto pode ajudar a garantir que você tenha um histórico imutável de descobertas de dados confidenciais e resultados de descoberta para auditorias ou investigações de privacidade e proteção de dados.

Utilizando a descoberta automatizada de dados confidenciais com o Amazon Macie

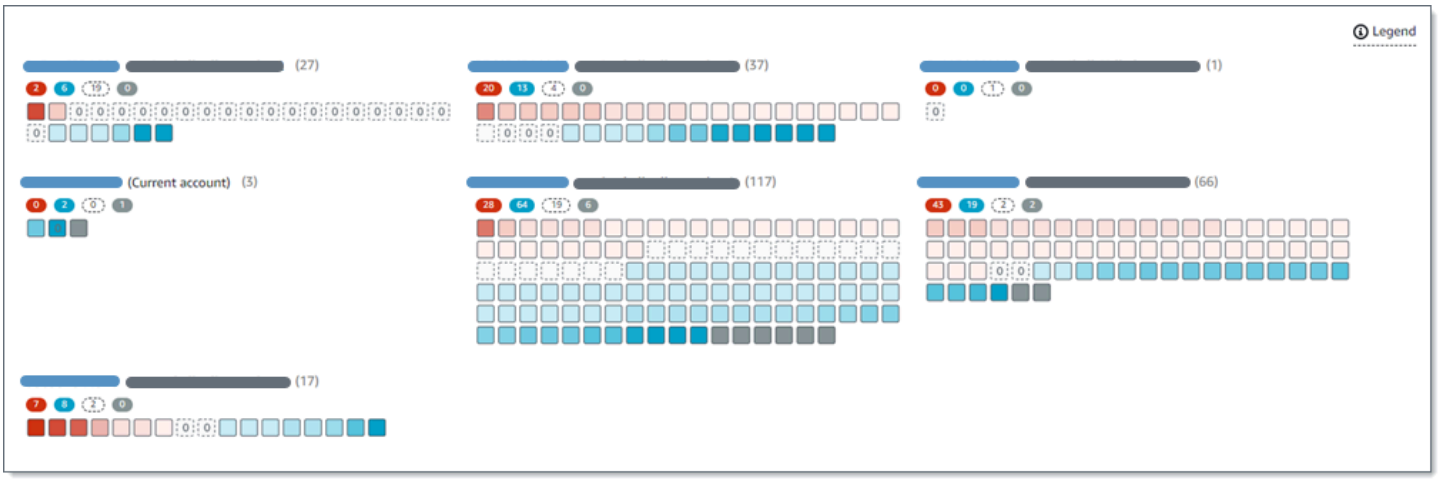
Para obter ampla visibilidade sobre onde os dados confidenciais podem residir em seu patrimônio de dados do Amazon Simple Storage Service (Amazon S3), configure o Amazon Macie para realizar a descoberta automática de dados confidenciais para a sua conta ou organização. Com a descoberta automatizada de dados confidenciais, o Macie avalia continuamente seu inventário de buckets do S3 e usa técnicas de amostragem para identificar e selecionar objetos representativos do S3 em seus buckets. Em seguida, o Macie recupera e analisa os objetos selecionados, inspecionando-os em busca de dados confidenciais.

Por padrão, o Macie analisa objetos do S3 usando o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. Você

pode personalizar as análises configurando o Macie para usar identificadores de dados gerenciados específicos, identificadores de dados personalizados e listas de permissões ao realizar a descoberta automática de dados confidenciais para a sua conta ou organização. Além disso, o Macie seleciona e analisa automaticamente objetos de todos os seus buckets do S3. Se você for o administrador do Macie em uma organização, isso inclui objetos nos buckets do S3 que as contas de seus membros possuem. Você pode ajustar o escopo das análises excluindo buckets específicos, por exemplo, buckets S3 que normalmente armazenam dados de log AWS.

À medida que a análise avança a cada dia, o Macie produz registros dos dados confidenciais que descobre e da análise que realiza: descobertas de dados confidenciais que relatam dados confidenciais que o Macie descobre em objetos individuais do S3 e resultados confidenciais da descoberta de dados que registram detalhes em log sobre a análise de objetos individuais do S3. O Macie também atualiza estatísticas e outras informações que fornece sobre os dados do Amazon S3.

Por exemplo, um mapa de calor interativo no console fornece uma representação visual da sensibilidade dos dados em todo o seu estado de dados:



Esses atributos foram projetados para ajudar você a avaliar a sensibilidade dos dados em todo o seu conjunto de dados do Amazon S3 e detalhá-los para investigar e avaliar contas, buckets e objetos individuais. Eles também podem ajudar você a determinar onde realizar análises mais profundas e imediatas ao executar tarefas de descoberta de dados confidenciais. Combinado com as informações que o Macie fornece sobre a segurança e a privacidade dos seus dados do Amazon S3, você também pode usar esses atributos para identificar casos em que uma remediação imediata possa ser necessária — por exemplo, um bucket acessível ao público no qual o Macie encontrou dados confidenciais.

Para configurar e usar a descoberta automatizada de dados confidenciais, sua conta deve ser uma conta autônoma do Macie ou a conta de administrador do Macie de uma organização.

Tópicos

Como funciona a descoberta automatizada de dados confidenciais

Quando você ativa o Amazon Macie para seu Conta da AWS, o Macie cria um perfil vinculado a serviçosAWS Identity and Access Management (IAM) para a sua conta atual Região da AWS. A política de permissões para esse perfil permite que o Macie ligue para outras pessoas Serviços da AWS e monitore recursos AWS em seu nome. Ao usar esse perfil, o Macie gera e mantém um inventário completo dos seus buckets do Amazon Simple Storage Service (Amazon S3) na região. O inventário inclui informações sobre cada um dos seus buckets do S3 e os objetos nos buckets. Se você for o administrador do Macie em uma organização, o inventário inclui informações sobre os buckets do S3 que as contas-membro possuem. Para obter mais informações, consulte Gerenciar várias contas da .

Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta do Macie, o Macie avaliará os dados de inventário diariamente para identificar objetos do S3 que são elegíveis para descoberta automatizada. Como parte da avaliação, o Macie também seleciona uma amostra de objetos representativos para analisar. Em seguida, o Macie recupera e analisa a versão mais recente de cada objeto selecionado do Amazon S3, inspecionando cada objeto em busca de dados confidenciais.

À medida em que a análise progride a cada dia, o Macie também atualiza estatísticas e outras informações que fornece sobre os dados do Amazon S3. O Macie também produz registros dos dados confidenciais que encontra e das análises que realiza. Os dados resultantes fornecem informações sobre onde o Macie encontrou dados confidenciais em seu patrimônio de dados do Amazon S3, abrangendo todos os buckets do S3 que o Macie monitora e analisa para sua conta. Os dados podem ajudá-lo a avaliar a segurança e a privacidade de seus dados confidenciais, determinar onde realizar uma investigação mais profunda e identificar casos em que a remediação é necessária.

Para uma breve demonstração de como funciona a descoberta automatizada de dados confidenciais, assista ao vídeo a seguir: Visão geral da descoberta automatizada de dados do Amazon Macie.

Para configurar e usar a descoberta automatizada de dados confidenciais, sua conta deve ser uma conta autônoma do Macie ou a conta de administrador do Macie de uma organização.

Tópicos

Componentes principais

O Amazon Macie usa uma combinação de recursos e técnicas para realizar a descoberta automatizada de dados confidenciais para seus dados do Amazon S3. Eles funcionam em conjunto com recursos e técnicas que o Macie usa para ajudar você a monitorar seus dados do Amazon S3 quanto à segurança e o controle de acesso.

Selecionando os objetos do S3 para análise

Diariamente, o Macie avalia seus dados no Inventário Amazon S3 para identificar objetos do S3 que são elegíveis para análise por meio da descoberta automatizada de dados confidenciais. Se você for o administrador do Macie em uma organização, isso inclui dados do inventário dos buckets do S3 que as contas-membro possuem.

Como parte da avaliação, o Macie usa técnicas de amostragem para selecionar objetos representativos para análise. As técnicas definem grupos de objetos que têm metadados semelhantes e, provavelmente, têm conteúdo semelhante. Os grupos são baseados em dimensões como nome, prefixo, classe de armazenamento, extensão do nome do arquivo e data da última modificação do bucket. Em seguida, o Macie seleciona um conjunto representativo de amostras de cada grupo, recupera a versão mais recente de cada objeto selecionado do Amazon S3 e analisa cada objeto selecionado para determinar se o objeto contém dados confidenciais. Quando a análise é concluída, o Macie descarta sua cópia do objeto.

A estratégia de amostragem prioriza análises distribuídas. Em geral, ele usa uma abordagem abrangente para seu patrimônio de dados do Amazon S3. Todos os dias, um conjunto representativo de objetos do S3 é selecionado a partir do maior número possível de buckets com base no tamanho total de armazenamento de todos os objetos classificáveis em seu patrimônio

de dados do Amazon S3. Por exemplo, se o Macie já analisou e encontrou dados confidenciais em objetos em um bucket do S3 e ainda não analisou objetos em outro bucket, o último bucket é uma prioridade maior para análise. Com essa abordagem, você obtém uma visão ampla da confidencialidade dos seus dados do Amazon S3 mais rapidamente. Dependendo do tamanho do seu patrimônio de dados, os resultados da análise podem começar a aparecer dentro de 48 horas após a ativação da descoberta automatizada de dados confidenciais em sua conta.

A estratégia de amostragem também prioriza a análise de diferentes tipos de objetos do S3 e objetos que foram criados ou alterados recentemente. Não é garantido que uma amostra de objeto único seja conclusiva. Portanto, a análise de um conjunto diversificado de objetos pode gerar uma visão melhor dos tipos e da quantidade de dados confidenciais que um bucket do S3 pode conter. Além disso, priorizar objetos novos ou alterados recentemente ajuda a análise a se adaptar às mudanças em seu inventário de buckets. Por exemplo, se os objetos forem criados ou alterados após uma análise anterior, esses objetos terão prioridade maior para análises subsequentes. Por outro lado, se um objeto foi analisado anteriormente e não mudou desde essa análise, o Macie não analisará o objeto novamente. Essa abordagem ajuda você a estabelecer linhas de base de confiabilidade para determinados buckets do S3. Então, à medida que as análises incrementais contínuas progridem em sua conta, suas avaliações de confiabilidade de determinados buckets podem se tornar cada vez mais profundas e detalhadas a uma velocidade previsível.

Definindo o escopo das análises

Por padrão, o Macie inclui todos os buckets do S3 que ele monitora e analisa para sua conta ao avaliar seus dados de inventário e selecionar objetos do S3 para análise. Se você for o administrador do Macie em uma organização, isso inclui buckets que as contas de seus membros possuem.

Você pode excluir buckets do S3 específicos das análises. Por exemplo, você pode preferir excluir buckets que normalmente armazenam dados de log da AWS, como registros de AWS CloudTrail eventos. Para excluir um bucket, você pode alterar as configurações automatizadas de descoberta de dados confidenciais da sua conta ou do bucket. Se você fizer isso, o Macie começará a excluir o bucket quando o próximo ciclo diário de avaliação e análise começar. Você pode excluir até mil buckets das análises.

Se você excluir um bucket, você poderá incluí-lo novamente. Para fazer isso, altere novamente as configurações de descoberta automatizada de dados confidenciais da sua conta ou do bucket. O Macie, então, começará a incluir o bucket quando o próximo ciclo diário de avaliação e análise começar.

Determinando quais tipos de dados confidenciais devem ser detectados e reportados

Por padrão, o Macie inspeciona objetos do S3 usando o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. Para obter uma lista desses identificadores de dados gerenciados, consulte Configurações padrão para descoberta automatizada de dados confidenciais.

Você pode personalizar as análises para se concentrarem em tipos específicos de dados confidenciais. Para fazer isso, altere as configurações de descoberta automatizada de dados confidenciais de sua conta de qualquer uma das seguintes maneiras:

- Adicione ou remova identificadores específicos de dados gerenciados – um identificador de dados gerenciados é um conjunto de critérios e técnica integrados que são projetados para detectar um tipo específico de dados confidenciais, como, por exemplo, números de cartão de crédito, chaves de acesso secretas AWS ou números de passaporte para um determinado país ou região. Para obter mais informações, consulte Usar identificadores de dados gerenciados.
- Adicione ou remova, posteriormente, identificadores de dados personalizados – um identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais. Com identificadores de dados personalizados, você pode detectar dados confidenciais que refletem determinados cenários, propriedade intelectual ou dados proprietários, como IDs de funcionários, números da conta de clientes ou classificações de dados internos, da sua organização. Para obter mais informações, consulte Criar identificadores de dados personalizados.
- Adicione ou remova, posteriormente, listas de permissões – no Macie, uma lista de permissões especifica um texto ou um padrão de texto que você deseja que o Macie ignore nos objetos do S3. Normalmente, são exceções de dados confidenciais para seu cenário ou ambiente específicos, como nomes públicos ou números de telefone da sua organização, ou dados de amostra que sua organização usa para testes. Para obter mais informações, consulte Como definir exceções de dados sigilosos com listas de permissões.

Se você alterar as configurações, o Macie aplicará suas alterações quando o próximo ciclo diário de análise começar.

Você também pode ajustar as configurações no nível do bucket que determinam se tipos específicos de dados confidenciais são incluídos nas avaliações da sensibilidade de um bucket. Para saber como, consulte Gerenciando a descoberta automatizada de dados confidenciais para buckets do S3 individuais.

Calculando pontuações de confidencialidade

Por padrão, o Macie calcula automaticamente uma pontuação de confidencialidade para cada bucket do S3 que ele monitora e analisa para sua conta. Se você for o administrador do Macie em uma organização, isso inclui buckets que as contas de seus membros possuem.

No Macie, uma pontuação de confidencialidade é uma medida quantitativa da interseção de duas dimensões principais: a quantidade de dados confidenciais que o Macie encontrou em um bucket e a quantidade de dados que o Macie analisou em um bucket. Uma pontuação de confidencialidade de um bucket do S3 determina qual rótulo de sensibilidade Macie atribui ao bucket. Um rótulo de confidencialidade é uma representação qualitativa da pontuação de confidencialidade de um bucket, como, por exemplo, Confidencial, Não confidencial e Não analisado ainda. Para obter detalhes sobre a faixa de pontuações de confidencialidade e rótulos que Macie define, consulte Pontuação de confidencialidade para buckets do S3.

> **Important**
>
> A pontuação e o rótulo de confidencialidade de um bucket do S3 não implicam nem indicam a criticidade ou a importância que o bucket ou os objetos do bucket podem ter para sua organização. Em vez disso, eles têm como objetivo fornecer pontos de referência que podem ajudá-lo a identificar e monitorar possíveis riscos de segurança.

Quando você habilita inicialmente a descoberta automatizada de dados confidenciais para sua conta, o Macie atribui automaticamente uma pontuação de confidencialidade de 50 e o rótulo de Não analisado ainda a cada bucket do S3. A exceção são os buckets vazios. Um bucket vazio é um bucket que não contém nenhum objeto ou no qual todos os objetos contêm zero (0) bytes de dados. Se esse for o caso de um bucket, o Macie atribui uma pontuação de 1 ao bucket e atribui o rótulo de Não confidencial ao bucket.

À medida que a descoberta automatizada progride em sua conta, o Macie atualiza as pontuações e rótulos de confidencialidade para refletir os resultados das análises. Por exemplo:

- Se o Macie não encontrar dados confidenciais em um objeto, o Macie diminui a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se o Macie encontrar dados confidenciais em um objeto, o Macie aumenta a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.

- Se o Macie encontrar dados confidenciais em um objeto que é alterado posteriormente, o Macie remove as detecções de dados confidenciais do objeto da pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se o Macie encontrar dados confidenciais em um objeto que é excluído posteriormente, o Macie remove as detecções de dados confidenciais do objeto da pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.

Você pode ajustar as configurações de pontuação de sensibilidade para determinados buckets do S3 incluindo ou excluindo tipos específicos de dados confidenciais da pontuação de um bucket. Você também pode substituir a pontuação calculada de um bucket atribuindo manualmente a pontuação máxima (100) ao bucket. Se você atribuir a pontuação máxima, o bucket será rotulado como Confidencial. Para obter mais informações, consulte Gerenciando a descoberta automatizada para buckets do S3 individuais.

Gerando metadados, estatísticas e resultados

Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta, o Macie gera e mantém automaticamente dados adicionais de inventário, estatísticas e outras informações sobre os buckets do S3 que ele monitora e analisa para sua conta. Se você for o administrador do Macie em uma organização, isso inclui buckets que as contas de seus membros possuem.

As informações adicionais capturam os resultados das atividades automatizadas de descoberta de dados confidenciais que a Macie realizou até agora em sua conta. Também complementa outras informações que o Macie fornece sobre seus dados do Amazon S3, como as configurações de acesso público e acesso compartilhado para determinados buckets. As informações adicionais incluem:

- As estatísticas agregadas de confidencialidade de dados, como o número total de buckets nos quais o Macie encontrou dados confidenciais e quantos desses buckets estão acessíveis ao público.
- Uma representação visual e interativa da confidencialidade dos dados no seu patrimônio de dados do Amazon S3.
- Detalhes no nível do bucket que indicam o status atual das análises, como uma lista dos objetos que o Macie analisou em um bucket, os tipos de dados confidenciais que o Macie encontrou em um bucket e o número de ocorrências de cada tipo de dado confidencial que o Macie encontrou.

Para obter mais informações, consulte Analisando estatísticas e resultados automatizados de descoberta de dados confidenciais.

As informações adicionais também incluem estatísticas e detalhes que podem ajudá-lo a avaliar e monitorar a cobertura dos seus dados do Amazon S3. Você pode verificar o status geral das análises de seu patrimônio de dados e para determinados buckets do S3 em seu inventário de buckets. Você também pode identificar problemas que impediram o Macie de analisar objetos em buckets específicos. Se você corrigir os problemas, poderá aumentar a cobertura dos dados do Amazon S3 durante os ciclos de análise subsequentes. Para obter mais informações, consulte Como avaliar a cobertura da descoberta automatizada de dados confidenciais.

O Macie recalcula e atualiza automaticamente essa informação enquanto realiza a descoberta automatizada de dados confidenciais em sua conta. Por exemplo, se o Macie encontrar dados confidenciais em um objeto que é posteriormente alterado ou excluído, o Macie atualiza os metadados do bucket pertinente: remove o objeto da lista de objetos analisados; remove as ocorrências de dados confidenciais que o Macie encontrou no objeto; recalcula a pontuação de sensibilidade, se a pontuação for calculada automaticamente, e atualiza o rótulo de confidencialidade, conforme necessário, para refletir a nova pontuação.

Além de metadados e estatísticas, o Macie produz registros dos dados confidenciais que ele descobre e da análise que realiza: descobertas de dados confidenciais que relatam dados confidenciais que o Macie descobre em objetos individuais do S3 e resultados confidenciais da descoberta de dados que registram detalhes em log sobre a análise de objetos individuais do S3.

Considerações

Ao usar o Amazon Macie para realizar a descoberta automatizada de dados confidenciais para seus dados do Amazon S3, lembre-se do seguinte:

- Suas configurações de descoberta automatizada se aplicam somente à Região da AWS atual. Consequentemente, as análises e os dados resultantes se aplicam somente aos buckets e objetos do S3 na Região atual. Para realizar a descoberta automatizada e acessar os dados resultantes em Regiões adicionais, habilite e configure a descoberta automatizada em cada Região adicional.
- Se você for o administrador do Macie de uma organização:
  - Você pode realizar a descoberta automatizada de uma conta-membro somente se o Macie estiver habilitado para a conta na Região atual. As contas-membro não podem realizar a descoberta automatizada de suas próprias contas.

  - As contas-membro não podem acessar as configurações de descoberta automatizada que se aplicam aos buckets do S3. Somente o administrador do Macie pode acessar essas configurações.
  - As contas-membro não podem acessar estatísticas de descobertas de dados confidenciais e outros resultados que o Macie fornece diretamente para seus buckets do S3. Por exemplo, uma conta-membro não pode usar o console do Amazon Macie para rever as pontuações de confidencialidade de seus buckets do S3. Somente o administrador do Macie pode acessar essas configurações.
- Se as configurações de permissões de um bucket do S3 impedirem o Macie de recuperar informações ou acessar o bucket ou os objetos do bucket, o Macie não poderá realizar a descoberta automatizada do bucket. O Macie só pode fornecer um subconjunto de informações sobre o bucket, como o ID da conta da Conta da AWS que possui o bucket, o nome do bucket e quando o Macie recuperou mais recentemente os metadados do bucket e do objeto para o bucket como parte do ciclo diário de atualizações. Em seu inventário de buckets, a pontuação de confidencialidade desses buckets é 50 e seu rótulo de confidencialidade é Não analisado ainda.

  Para identificar rapidamente os buckets do S3 para os quais esse é o caso, consulte seus dados de cobertura de descoberta automatizada. Para obter mais informações, consulte Como avaliar a cobertura da descoberta automatizada de dados confidenciais. Para investigar o problema de um determinado bucket, revise as configurações de políticas e permissões do bucket no Amazon S3. Por exemplo, o bucket pode ter uma política restritiva de bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.
- Para ser elegível para seleção e análise, um objeto do S3 deve ser classificável. Um objeto é classificável se usar uma classe de armazenamento do Amazon S3 compatível e tiver uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Para obter mais informações, consulte Classes e formatos de armazenamento suportados.
- Se um objeto do S3 for criptografado, o Macie só poderá analisá-lo se o objeto for criptografado com uma chave que o Macie possa acessar e tem permissão para usar. Para obter mais informações, consulte Analisando objetos criptografados do S3. Para identificar casos em que as configurações de criptografia impediram o Macie de analisar um ou mais objetos em um bucket, consulte seus dados de cobertura de descoberta automatizada. Para obter mais informações, consulte Como avaliar a cobertura da descoberta automatizada de dados confidenciais.

Configurando a descoberta automatizada de dados confidenciais para sua conta

Com a descoberta automatizada de dados confidenciais, o Amazon Macie seleciona, continuamente, objetos de amostra de seus buckets do Amazon Simple Storage Service (Amazon S3) e analisa os objetos para determinar se eles contêm dados confidenciais. Se você for o administrador do Macie em uma organização, isso inclui objetos nos buckets do S3 que as contas de seus membros possuem. Conforme as análises progridem, o Macie também atualiza estatísticas e outras informações que fornece sobre os dados do Amazon S3. O Macie também produz registros dos dados confidenciais que encontra e das análises que realiza.

Para configurar e usar a descoberta automatizada de dados confidenciais, sua conta deve ser uma conta autônoma do Macie ou a conta de administrador do Macie de uma organização. Se você tiver uma conta-membro e desejar realizar uma descoberta automatizada para seus buckets do S3, entre em contato com o administrador do Macie da sua organização. Para obter mais informações, consulte Gerenciar várias contas da .

Tópicos

Quando você habilita, configura ou desabilita a descoberta automatizada de dados confidenciais em sua conta, suas alterações se aplicam somente à Região da AWS atual. Para fazer as mesmas alterações em outras regiões, repita as etapas pertinentes em cada região.

Antes de começar

Antes de configurar a descoberta automatizada de dados confidenciais para sua conta, verifique se você tem as permissões necessárias. Verifique também se você configurou um repositório para os resultados da descoberta de dados confidenciais.

Para verificar suas permissões, use AWS Identity and Access Management (IAM) para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações nessas políticas com a seguinte lista de ações que você deve ter permissão para realizar:

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`

A primeira ação permite que você acesse sua conta do Amazon Macie. A segunda ação permite que você altere as configurações de descoberta automatizada de dados confidenciais da sua conta. Isso inclui habilitar e desabilitar a configuração. Opcionalmente, verifique se você também tem permissão para realizar a ação `macie2:GetAutomatedDiscoveryConfiguration`. Essa ação permite que você recupere as configurações atuais e o status atual da configuração.

Além de verificar suas permissões, verifique se você configurou um repositório para armazenar os resultados da descoberta de dados confidenciais. Um resultado de descoberta de dados confidenciais é um registro de detalhes sobre a análise de um objeto do S3 que o Macie realizou. O Macie cria um registro para cada objeto do S3 que ele analisa quando você executa trabalhos de descoberta de dados confidenciais ou realiza a descoberta automatizada de dados confidenciais. Isso inclui objetos nos quais o Macie não encontra dados confidenciais e, portanto, não produz descobertas de dados confidenciais, e objetos que o Macie não pode analisar devido a erros ou problemas, como configurações de permissões. Se o Macie descobrir dados confidenciais em um objeto, o resultado da descoberta de dados confidenciais incluirá dados da descoberta correspondente. Ele também contém informações adicionais. Esses resultados fornecem registros de análise que podem ser úteis para auditorias ou investigações de privacidade e proteção de dados.

O Macie armazena seus resultados confidenciais de descoberta de dados por apenas 90 dias. Para acessar os resultados e permitir seu armazenamento e retenção a longo prazo, configure o Macie para armazenar os resultados em um bucket do S3. O bucket pode servir como um repositório definitivo e de longo prazo para todos os seus resultados confidenciais de descoberta de dados.

Para verificar se você configurou esse repositório para a sua conta, selecione Resultados da descoberta no painel de navegação no console do Amazon Macie. Se você preferir fazer isso de forma programática, use a operação GetClassificationExportConfiguration da API do Amazon Macie. Para saber como configurar esse repositório, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Se você configurou o repositório, o Macie cria uma pasta chamada automated-sensitive-data-discovery no repositório quando a descoberta automatizada de dados confidenciais é habilitada inicialmente para sua conta. Essa pasta armazena os resultados da descoberta de dados confidenciais que o Macie cria ao realizar a descoberta automatizada para a sua conta.

Habilitando a descoberta automatizada de dados confidenciais para a sua conta

Quando você habilita a descoberta automatizada de dados confidenciais para a sua conta, o Amazon Macie começa a avaliar seus dados no Inventário Amazon S3 e a realizar outras atividades de descoberta automatizada para a sua conta no Região da AWS atual. Dependendo do tamanho do seu estado de dados do Amazon S3, as estatísticas da descoberta de dados confidenciais e outros resultados podem começar a aparecer dentro de 48 horas após a habilitação da descoberta automatizada em sua conta.

Siga estas etapas para habilitar a descoberta automatizada de dados confidenciais para a sua conta usando o console do Amazon Macie. Para habilitar a descoberta automatizada de forma programática, use a operação UpdateAutomatedDiscoveryConfiguration da API do Amazon Macie.

Habilitando a descoberta automatizada de dados confidenciais para a sua conta

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja habilitar a descoberta automatizada de dados confidenciais.
3. No painel de navegação, em Configurações, selecione Descoberta automatizada.
4. Na seção Status, selecione Habilitar.
5. Quando a confirmação for solicitada, escolha Enable (Habilitar).

Depois de ativar a descoberta automatizada de dados confidenciais, revise e defina suas configurações para refinar as análises que o Macie executará posteriormente.

Configurando a descoberta automatizada de dados confidenciais para sua conta

Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta, você poderá ajustar as configurações de descoberta automatizada da sua conta para refinar as análises que o Amazon Macie realiza. Essas configurações especificam quais buckets do S3 você deseja incluir nas análises. Elas também especificam quais tipos e ocorrências de dados confidenciais você deseja que o Macie detecte e reporte: identificadores de dados gerenciados, identificadores de dados personalizados e listas de permissões para serem usadas ao analisar objetos do S3.

Por padrão, o Macie realiza uma descoberta automatizada de dados confidenciais para todos os buckets do S3 monitorados e analisados para sua conta. Se você for o administrador do Macie em uma organização, isso inclui buckets do S3 que as contas de seus membros possuem. Você pode excluir buckets específicos das análises. Por exemplo, você pode excluir buckets que normalmente

armazenam dados de log da AWS, como registros de AWS CloudTrail eventos. Se você excluir um bucket, você poderá incluí-lo novamente posteriormente.

Além disso, o Macie analisa objetos do S3 usando somente o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. O Macie não usa identificadores de dados personalizados nem permite listas que você definiu. Para personalizar as análises, você pode configurar o Macie para usar listas de permissões específicas, identificadores de dados personalizados e identificadores de dados gerenciados.

As seções a seguir fornecem informações adicionais sobre cada tipo de configuração e explicam como alterar uma configuração usando o console do Amazon Macie. Escolha uma seção para saber mais. Para revisar ou alterar as configurações de forma programática, você pode usar as seguintes operações da API do Amazon Macie: UpdateClassificationScope, para especificar quais buckets do S3 excluir das análises, e UpdateSensitivityInspectionTemplate, para especificar quais listas de permissões, identificadores de dados personalizados e identificadores de dados gerenciados usar.

Se você alterar uma configuração, o Macie aplicará sua alteração quando o próximo ciclo de avaliação e análise começar para a descoberta automatizada de dados confidenciais, normalmente em 24 horas.

Exclua ou inclua buckets do S3 nas análises

Por padrão, o Macie realiza uma descoberta automatizada de dados confidenciais para todos os buckets do S3 monitorados e analisados para sua conta. Se você for o administrador do Macie em uma organização, isso inclui buckets do S3 que as contas de seus membros possuem. Para refinar o escopo, você pode excluir até mil buckets das análises.

Se você excluir um bucket do S3, o Macie para de analisar objetos no bucket quando realiza a descoberta automatizada de dados confidenciais da sua conta. As estatísticas de descoberta de dados confidenciais existentes e os detalhes do bucket persistirão — por exemplo, a pontuação de confidencialidade atual do bucket permanecerá inalterada. Depois de excluir um bucket, você poderá incluí-lo novamente.

Para excluir ou incluir buckets do S3 específicos

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja excluir ou incluir buckets do S3 específicos das análises da descoberta automatizada.

3. No painel de navegação, em Configurações, selecione Descoberta automatizada. A página Descoberta automatizada de dados confidenciais aparece e exibe suas configurações atuais. Nessa página, a seção S3 buckets lista os buckets do S3 que estão atualmente excluídos ou indica que todos os buckets estão incluídos no momento.
4. Na seção S3 buckets, selecione Editar.
5. Faça um dos seguintes procedimentos:

   - Para excluir um ou mais buckets do S3, selecione Adicionar buckets à lista de exclusão. Em seguida, na tabela de S3 buckets, marque a caixa de seleção para cada bucket que você deseja excluir. A tabela lista todos os buckets do S3 da sua conta na Região atual.
   - Para incluir um ou mais buckets do S3 que você excluiu anteriormente, selecione Remover buckets da lista de exclusão. Em seguida, na tabela de S3 buckets, marque a caixa de seleção para cada bucket que você deseja excluir. A tabela lista todos os buckets atualmente excluídos da descoberta automatizada de dados confidenciais.

   Para encontrar buckets específicos com mais facilidade, insira os critérios de pesquisa na caixa de pesquisa acima da tabela. Você também pode organizar a tabela por nome do bucket.
6. Ao terminar de selecionar buckets, selecione Adicionar ou Remover, dependendo da opção escolhida na etapa anterior.

Adicione ou remova identificadores de dados gerenciados das análises

Um identificador de dados gerenciados é um conjunto de critérios e técnica integrados que são projetados para detectar um tipo específico de dados sigilosos, como por exemplo, números de cartão de crédito, chaves de acesso secretas AWS ou números de passaporte para um determinado país ou região. Por padrão, o Macie analisa objetos do S3 usando o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. Para revisar a lista de identificadores incluídos nesse conjunto, consulte Configurações padrão para descoberta automatizada de dados confidenciais.

Você pode personalizar as análises para se concentrar em tipos específicos de dados confidenciais: adicionar identificadores de dados gerenciados para os tipos de dados confidenciais que você deseja que o Macie detecte e relate e remover identificadores de dados gerenciados para os tipos de dados confidenciais que você não deseja que o Macie detecte e relate. Se você remover um identificador de dados gerenciados, sua alteração não afetará as estatísticas e os detalhes da descoberta de dados confidenciais existentes para seus buckets do S3. Por exemplo, se você remover o identificador de

dados gerenciados que detecta chaves de acesso secretas AWS e o Macie já detectou esse tipo de dados confidenciais em um bucket, o Macie continuará relatando essas detecções para o bucket.

> **Tip**
>
> Em vez de remover um identificador de dados gerenciados das análises subsequentes de todos os buckets do S3, você pode excluir esse tipo de detecção da pontuação de sensibilidade de buckets específicos. Para obter mais informações, consulte Gerenciando a descoberta automatizada de dados confidenciais para buckets do S3 individuais.

Adicione ou remova identificadores de dados gerenciados

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja adicionar ou remover identificadores de dados gerenciados das análises de descobertas automatizadas.
3. No painel de navegação, em Configurações, selecione Descoberta automatizada. Na página Descoberta automatizada de dados confidenciais, a seção Identificadores de dados gerenciados exibe suas configurações atuais, organizadas em duas guias:
   - Adicionado ao padrão — essa guia lista os identificadores de dados gerenciados que você adicionou explicitamente. O Macie usa esses identificadores de dados gerenciados junto com os que estão no conjunto padrão e que você não removeu explicitamente.
   - Removido do padrão — essa guia lista os identificadores de dados gerenciados que você removeu explicitamente. O Macie não usa esses identificadores de dados gerenciados.
4. Na seção Identificadores de dados gerenciados, selecione Editar.
5. Faça o seguinte:
   - Para adicionar um ou mais identificadores de dados gerenciados, escolha a guia Adicionado ao padrão. Em seguida, na tabela, marque a caixa de seleção para cada identificador de dados gerenciados que você deseja adicionar. Se uma caixa de seleção já estiver marcada, você já adicionou esse identificador.
   - Para remover um ou mais identificadores de dados gerenciados, selecione a guia Removido do padrão. Em seguida, na tabela, marque a caixa de seleção para cada identificador de dados gerenciados que você deseja remover. Se uma caixa de seleção já estiver marcada, você já adicionou esse identificador.

Em cada guia, a tabela exibe uma lista de todos os identificadores de dados gerenciados que o Macie fornece atualmente. Na tabela, cada ID de um identificador de dados gerenciados descreve o tipo de dados confidenciais que o identificador foi projetado para detectar; por exemplo, USA_PASSPORT_NUMBER para números de passaportes dos EUA. Para encontrar buckets específicos com mais facilidade, insira os critérios de pesquisa na caixa de pesquisa acima da tabela. É possível, também, organizar as linhas na tabela escolhendo o cabeçalho de uma coluna. Para obter detalhes sobre cada identificador, consulte Usar identificadores de dados gerenciados.

6. Ao concluir, escolha Save.

Adicione ou remova identificadores de dados gerenciados das análises

O identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais. Os critérios consistem em uma expressão regular (regex) que define um padrão de texto a ser correspondido e, opcionalmente, sequências de caracteres e uma regra de proximidade que refinam os resultados. Para saber mais, consulte Criar identificadores de dados personalizados.

Por padrão, o Amazon Macie não usa identificadores de dados personalizados ao realizar a descoberta automatizada de dados confidenciais. Se você quiser que o Macie use identificadores de dados personalizados específicos, você pode adicioná-los às análises. O Macie, então, usa os identificadores de dados personalizados, além de quaisquer identificadores de dados gerenciados que você também configurou para que o Macie use.

Se você adicionar um identificador de dados personalizado às análises, você poderá removê-lo posteriormente. Se você remover um identificador de dados gerenciados, sua alteração não afetará as estatísticas e os detalhes da descoberta de dados confidenciais existentes para seus buckets do S3. Por exemplo, se você remover um identificador de dados personalizado que anteriormente produzia detecções para um bucket, o Macie continuará relatando essas detecções para o bucket. No entanto, considere excluir esse tipo de detecção da pontuação de sensibilidade de buckets específicos em vez de remover o identificador das análises subsequentes de todos os buckets. Para obter mais informações, consulte Gerenciando a descoberta automatizada de dados confidenciais para buckets do S3 individuais.

Adicione ou remova identificadores de dados personalizados

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja adicionar ou remover identificadores de dados personalizados das análises de descobertas automatizadas.
3. No painel de navegação, em Configurações, selecione Descoberta automatizada. A página Descoberta automatizada de dados confidenciais aparece e exibe suas configurações atuais. Nessa página, a seção Identificadores de dados personalizados lista os identificadores de dados personalizados que você adicionou ou indica que você não selecionou nenhum identificador de dados personalizado para descoberta automática.
4. Na seção Identificadores de dados personalizados, selecione Editar.
5. Faça o seguinte:

   - Na página Selecionar identificadores de dados personalizados, marque a caixa de seleção para cada identificador de dados personalizado que você deseja que o trabalho use. Se uma caixa de seleção já estiver marcada, você já adicionou esse identificador.
   - Na página Selecionar identificadores de dados personalizados, marque a caixa de seleção para cada identificador de dados personalizado que você deseja que o trabalho use. Se uma caixa de seleção já estiver desmarcada, o Macie não usa esse identificador ao realizar a descoberta automatizada atualmente.

   > **Tip**
   >
   > Para revisar ou testar as configurações de um identificador de dados personalizado antes de adicioná-lo ou removê-lo, selecione o ícone de link ( ) ao lado do nome do identificador. O Macie abrirá uma página que exibe as configurações do identificador.
   > Você também pode usar essa página para testar o identificador com dados de amostra. Para fazer isso, insira até mil caracteres de texto na caixa Dados da amostra e selecione Teste. O Macie avalia os dados da amostra usando o identificador e, em seguida, relata o número de correspondências.

6. Ao concluir, escolha Save.

Adicione ou remova listas de permissões das análises

No Amazon Macie, uma lista de permissões define um texto ou um padrão de texto específicos que o Macie deverá ignorar ao inspecionar objetos S3 em busca de dados sigilosos. Se o texto corresponder a uma entrada ou padrão em uma lista de permissões, o Macie não reportará o texto, mesmo que o texto corresponda aos critérios de um identificador de dados gerenciado ou de um identificador de dados personalizados. Para saber mais, consulte Como definir exceções de dados sigilosos com listas de permissões.

Por padrão, o Amazon Macie não usa identificadores de dados personalizados ao realizar a descoberta automatizada de dados confidenciais. Se você quiser que o Macie use listas de permissões específicas, você pode adicioná-las às análises. Se você adicionar uma lista de permissões às análises, você poderá removê-la posteriormente.

Para adicionar ou remover listas de permissões

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja adicionar ou remover listas de permissões das análises de descobertas automatizadas.
3. No painel de navegação, em Configurações, selecione Descoberta automatizada. A página Descoberta automatizada de dados confidenciais aparece e exibe suas configurações atuais. Nessa página, a seção Listas de permissões indica quais listas de permissões você adicionou ou indica que você não selecionou nenhuma lista de permissões para descoberta automática.
4. Na seção Listas e permissões, selecione Editar.
5. Faça o seguinte:

   - Para adicionar uma ou mais listas de permissão, marque a caixa de seleção para cada lista de permissões que você deseja adicionar. Se uma caixa de seleção já estiver marcada, você já adicionou esse identificador.
   - Para adicionar uma ou mais listas de permissão, marque a caixa de seleção para cada lista de permissões que você deseja adicionar. Se uma caixa de seleção já estiver desmarcada, o Macie não usa essa lista ao realizar a descoberta automatizada atualmente.

> **Tip**
>
> Para revisar as configurações de uma lista de permissões antes de adicioná-la ou removê-la, selecione o ícone do link () ao lado do nome da lista. O Macie abrirá uma página que exibe as configurações da lista.

6. Ao concluir, escolha Save.

Desabilitando a descoberta automatizada de dados confidenciais em sua conta

Você pode desabilitar a descoberta automatizada de dados confidenciais de sua conta a qualquer momento. Se você desabilitar a descoberta automática de dados confidenciais, o Macie interrompe todas as atividades de descoberta automatizada em sua conta antes do início do próximo ciclo de avaliação e análise, normalmente em 24 horas. Além disso, você perde o acesso a todos os dados estatísticos, dados de inventário e outras informações que a Macie produziu e forneceu diretamente durante a execução dessas atividades. Por exemplo, seu inventário de buckets do S3 não incluirá mais as pontuações de sensibilidade e visualizações, nem analisará as estatísticas e os detalhes de buckets individuais do S3.

Você pode continuar acessando as descobertas de dados confidenciais que o Macie produziu enquanto realiza a descoberta automatizada para a sua conta. O Macie armazena suas descobertas por 90 dias. Além disso, os dados que você armazenou ou publicou em outros Serviços da AWS permanecem intactos e não são afetados, como os resultados de descoberta de dados confidenciais no Amazon S3 e localização de eventos no Amazon EventBridge.

Se você desabilitar a descoberta automatizada de dados confidenciais de sua conta, você poderá habilitá-la novamente. O Macie, então, retoma todas as atividades de descobertas automatizadas da sua conta. Se você reativá-la em 30 dias, você recuperará o acesso a todos os dados estatísticos, dados de inventário e outras informações que a Macie produziu anteriormente e forneceu diretamente durante a execução dessas atividades. Se você não reativá-la em 30 dias, o Macie excluirá permanentemente os dados estatísticos e outras informações que ele produziu anteriormente e forneceu diretamente.

Siga estas etapas para desabilitar a descoberta automatizada de dados confidenciais para a sua conta usando o console do Amazon Macie. Para desabilitar a descoberta automatizada de forma programática, use a operação UpdateAutomatedDiscoveryConfiguration da API do Amazon Macie.

Desabilitando a descoberta automatizada de dados confidenciais em sua conta

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja desabilitar a descoberta automatizada de dados confidenciais.
3. No painel de navegação, em Configurações, selecione Descoberta automatizada.
4. Na seção Status, selecione Desabilitar.
5. Quando a confirmação for solicitada, escolha Desabilitar.

Gerenciando a descoberta automatizada de dados confidenciais para buckets do S3 individuais

Ao revisar e avaliar suas estatísticas e resultados automatizados de descoberta de dados confidenciais, você pode ajustar a pontuação de confidencialidade e outras configurações para buckets individuais do Amazon Simple Storage Service (Amazon S3). Ao ajustar essas configurações, você pode ajustar as avaliações de confidencialidade do seu estado geral de dados do Amazon S3 e dos buckets específicos dentro dele. Você também pode capturar os resultados das investigações que você realiza para buckets específicos.

Você pode ajustar as configurações automatizadas de descoberta de dados confidenciais para um bucket do S3 das seguintes maneiras.

Atribuir pontuação de confidencialidade

Por padrão, o Amazon Macie calcula automaticamente a pontuação de confidencialidade de um bucket. A pontuação é baseada principalmente na quantidade de dados confidenciais que Macie encontrou em um bucket e na quantidade de dados que Macie analisou em um bucket. Para obter mais informações, consulte Pontuação de confidencialidade para buckets do S3.

Você pode substituir a pontuação calculada de um bucket e atribuir manualmente a pontuação máxima (100), que também aplica o rótulo Confidencial ao bucket. Se você fizer isso, o Macie continuará realizando a descoberta automatizada do bucket. No entanto, as análises subsequentes não afetam a pontuação do bucket. Para calcular a pontuação automaticamente novamente, altere a configuração novamente.

Excluir ou incluir tipos específicos de dados confidenciais na pontuação de confidencialidade

Se calculada automaticamente, a pontuação de confidencialidade de um bucket é baseada parcialmente na quantidade de dados confidenciais que o Macie encontrou no bucket. Isso deriva principalmente da natureza e do número de tipos de dados confidenciais que o Macie encontrou no bucket e do número de ocorrências de cada tipo. Por padrão, o Macie inclui ocorrências de todos os tipos de dados confidenciais ao calcular a pontuação de confidencialidade de um bucket.

Você pode ajustar o cálculo excluindo ou incluindo tipos específicos de dados confidenciais na pontuação de um bucket. Por exemplo, se o Macie detectou endereços de correspondência em um bucket e você determinar que isso é aceitável, você pode excluir todas as ocorrências de endereços de correspondência da pontuação do bucket. Se você excluir um tipo de dados confidenciais, o Macie continuará inspecionando o bucket em busca desse tipo de dados e relatando as ocorrências encontradas. No entanto, essas ocorrências não afetam a pontuação calculada do bucket. Para incluir novamente um tipo de dados confidenciais no armazenamento calculado, altere a configuração novamente.

Exclua ou inclua o bucket em análises subsequentes

Como padrão, o Macie realiza uma descoberta automática para todos os buckets do S3 monitorados e analisados para sua conta. Se você for o administrador do Macie em uma organização, isso inclui objetos nos buckets do S3 que as contas de seus membros possuem. Você pode excluir buckets específicos das análises. Por exemplo, você pode excluir buckets que normalmente armazenam dados de log da AWS, como registros de AWS CloudTrail eventos.

Se você excluir um bucket, as estatísticas de descoberta de dados confidenciais existentes e os detalhes do bucket persistirão — por exemplo, a pontuação de confidencialidade atual do bucket permanecerá inalterada. No entanto, o Macie para de analisar objetos no bucket quando realiza a descoberta automática da sua conta. Depois de excluir um bucket, você poderá incluí-lo novamente.

Se você alterar uma configuração que afeta a pontuação de confidencialidade de um bucket do S3, o Macie imediatamente começa a recalcular e atualizar estatísticas relevantes de descoberta de dados confidenciais e outras informações que ele fornece sobre seus dados do Amazon S3. Por exemplo, se você atribuir a pontuação máxima a um bucket, o Macie incrementa a contagem de buckets sensíveis nas estatísticas agregadas da sua conta.

Siga estas etapas para alterar configurações usando o console do Amazon Macie. Para alterar uma configuração programaticamente, você pode usar as seguintes operações da API do Amazon

Macie: UpdateResourceProfile, para atribuir uma pontuação de confidencialidade a um bucket; UpdateResourceProfileDetections, para excluir ou incluir posteriormente tipos de dados confidenciais na pontuação de um bucket; e UpdateClassificationScope para excluir ou incluir um bucket em análises subsequentes.

Como alterar as configurações de descoberta de dados confidenciais automatizados para um bucket do S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Bucketsdo S3.
3. Na página Buckets do S3, escolha o bucket do S3 cujas configurações você deseja alterar. Você pode escolher o bucket usando a visualização da tabela ( ) ou o mapa interativo ( ).
4. Na página de detalhes, siga um destes procedimentos:

   - Para substituir a pontuação calculada e atribuir manualmente uma pontuação de confidencialidade ao bucket, ative Atribuir pontuação máxima ( ). Isso altera a pontuação do compartimento para 100 e aplica o rótulo Confidencial ao bucket.

     Para atribuir uma pontuação que o Macie calcula automaticamente, desative Atribuir pontuação máxima ( ).
   - Para excluir o bucket das análises subsequentes, ative Excluir da descoberta automática ( ).

     Se você excluiu anteriormente o bucket das análises, desative Excluir da descoberta automática ( ) para incluí-lo novamente.
   - Para excluir ou incluir ocorrências de tipos específicos de dados confidenciais na pontuação de confidencialidade do bucket, selecione a guia confidencialidade. Na tabela Detecções, marque a caixa de seleção do tipo de dados confidenciais a ser excluído ou incluído. Em

seguida, no menu Ações, selecione Excluir da pontuação para excluir o tipo ou selecione Incluir na pontuação para incluir o tipo.

Na tabela, o campo Tipo de dados confidenciais especifica o identificador (ID) exclusivo do identificador de dados gerenciados que detectou os dados ou o nome do identificador de dados personalizado que detectou os dados. O ID de um identificador de dados gerenciados descreve o tipo de dados confidenciais que o identificador foi projetado para detectar; por exemplo, USA_PASSPORT_NUMBER para números de passaportes dos EUA. Para obter detalhes sobre cada identificador de dados gerenciados, consulte Usar identificadores de dados gerenciados.

Se você alterou uma configuração que afeta a pontuação de confidencialidade do bucket do S3, o Macie começará imediatamente a recalcular e atualizar estatísticas relevantes de descoberta de dados confidenciais e outras informações sobre o bucket S3.

Como avaliar a cobertura da descoberta automatizada de dados confidenciais

À medida que a descoberta automatizada de dados confidenciais progride na sua conta, o Amazon Macie fornece estatísticas e detalhes para ajudar você a avaliar e monitorar a cobertura do seu patrimônio de dados no Amazon Simple Storage Service (Amazon S3). Com esses dados, você pode verificar o status das análises automáticas de dados confidenciais no seu patrimônio de dados geral e de buckets individuais do S3 no seu inventário de buckets. Você também pode identificar problemas que impediram o Macie de analisar objetos em buckets específicos. Se você corrigir os problemas, poderá aumentar a cobertura dos dados do Amazon S3 durante os ciclos de análise subsequentes.

Os dados de cobertura fornecem uma visão geral do status atual da descoberta automatizada de dados confidenciais para seus buckets S3 na Região da AWS atual. Se você for o administrador do Macie em uma organização, isso inclui buckets do S3 que as contas de seus membros possuem. Para cada bucket, os dados indicam se ocorreram problemas quando o Macie tentou analisar objetos no bucket. Se houve problemas, os dados indicam a natureza de cada problema e, em certos casos, o número de ocorrências. Os dados são atualizados à medida que a descoberta automática de dados confidenciais progride em sua conta a cada dia. Se o Macie analisar ou tentar analisar um ou mais objetos em um bucket durante um ciclo de análise diário, o Macie atualiza a cobertura e outros dados para refletir os resultados.

Para certos tipos de problemas, você pode revisar os dados agregados de todos os seus buckets do S3 e, opcionalmente, aprofundá-los para obter detalhes adicionais sobre cada bucket. Por exemplo, os dados de cobertura podem ajudar você a identificar rapidamente todos os buckets que o Macie não tem permissão para acessar na sua conta. Os dados de cobertura também relatam problemas no nível de objeto em que ocorreram. Esses problemas, chamados de erros de classificação, impediram que o Macie analisasse objetos específicos em um bucket. Por exemplo, você pode determinar quantos objetos o Macie não conseguiu analisar em um bucket porque os objetos são criptografados com uma chave AWS Key Management Service (AWS KMS) que não está mais disponível.

Se você usa o console do Amazon Macie para analisar os dados de cobertura, sua visão dos dados inclui orientações para remediar cada tipo de problema. Os tópicos seguintes nesta seção também fornecem orientações de remediação para cada tipo.

Tópicos

Revisão dos dados da cobertura de descoberta automatizada de dados confidenciais

Para revisar e avaliar a cobertura automatizada de descoberta de dados confidenciais da sua conta, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Tanto o console quanto a API fornecem dados que indicam o status atual das análises dos seus buckets do Amazon Simple Storage Service (Amazon S3) na Região da AWS atual. Os dados incluem informações sobre questões que criam lacunas nas análises:

- Buckets do S3 que o Macie não tem permissão para acessar. O Macie não pode analisar objetos nesses buckets porque as configurações de permissões dos buckets impedem que o Macie acesse os buckets e os objetos dos buckets.

- Buckets do S3 que não armazenam objetos classificáveis. O Macie não pode analisar nenhum objeto nesses buckets porque todos os objetos usam classes de armazenamento do Amazon S3 que o Macie não suporta, ou porque eles têm extensões de nome de arquivo para formatos de arquivo ou armazenamento que o Macie não suporta.
- Buckets do S3 que o Macie ainda não conseguiu analisar devido a erros de classificação no nível de objeto. O Macie tentou analisar um ou mais objetos nesses buckets. No entanto, o Macie não conseguiu analisar os objetos devido a problemas com as configurações de permissões no nível do objeto, conteúdo do objeto ou cotas.

Os dados de cobertura são atualizados à medida que a descoberta automática de dados confidenciais progride em sua conta a cada dia. Se você for o administrador do Macie em uma organização, os dados incluem informações sobre os buckets do S3 que as contas de seus membros possuem.

> **Note**
>
> Os dados de cobertura não incluem explicitamente os resultados para trabalhos descoberta de confidenciais que você criou e executou. No entanto, a correção de problemas de cobertura que afetam seus resultados automatizados de descoberta de dados confidenciais provavelmente aumentará também a cobertura de trabalhos de descoberta de dados confidenciais que você executará posteriormente. Para avaliar a cobertura de um trabalho, revise as estatísticas e os resultados do trabalho. Se os eventos de log de um trabalho ou outros resultados indicarem problemas de cobertura, a orientação de remediação apresentada posteriormente nesta seção poderá ajudar você a resolver alguns dos problemas.

Revisão dos dados da cobertura de descoberta automatizada de dados confidenciais

Para analisar os dados de cobertura para sua conta ou organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie. No console, uma única página fornece uma visão unificada dos dados de cobertura de todos os seus buckets do S3, incluindo um conjunto de problemas que ocorreram recentemente em cada bucket. A página também fornece opções para revisar grupos de dados por tipo de problema. Para monitorar sua investigação de problemas em buckets específicos, você pode exportar dados da página para um arquivo de valores separados por vírgula (CSV).

Console

Siga estas etapas para analisar a cobertura automatizada de descoberta de dados confidenciais usando o console do Amazon Macie.

Revisar dados da cobertura

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Cobertura de recursos.
3. Na página Cobertura de recursos, escolha a guia do tipo de dados de cobertura que você deseja revisar:

   - Tudo – Lista todos os buckets do S3 que o Macie monitora e analisa para a sua conta.

     Para cada bucket, o campo Problemas indica se os problemas impediram o Macie de analisar objetos no bucket. Se o valor desse campo for Nenhum, o Macie analisou pelo menos um dos objetos do bucket, ou o Macie ainda não tentou analisar nenhum dos objetos do bucket. Se houver problemas, esse campo indica a natureza dos problemas e como corrigi-los. Para erros de classificação no nível de objeto, ele também pode indicar o número de ocorrências do erro (entre parênteses).
   - Acesso negado – Exibe em lista os buckets do S3 que o Macie não tem permissão para acessar. As configurações de permissões a esses buckets impedem que o Macie acesse os buckets e os objetos dos buckets. Consequentemente, o Macie não consegue analisar nenhum objeto nesses buckets.
   - Erro de classificação – Exibe os buckets do S3 que o Macie ainda não analisou devido a erros de classificação no nível de objeto – problemas com configurações de permissões no nível de objeto, conteúdo de objeto ou cotas.

     Para cada bucket, o campo Problemas indica a natureza de cada tipo de erro que ocorreu e impediu que o Macie analisasse um objeto no bucket. Também indica como corrigir cada tipo de erro. Dependendo do erro, ele também pode indicar o número de ocorrências do erro (entre parênteses).
   - Inclassificável – Lista os buckets do S3 que o Macie não pode analisar porque não armazenam nenhum objeto classificável. Todos os objetos nesses buckets usam classes de armazenamento Amazon S3 não suportadas ou têm extensões de nome de arquivo para formatos de arquivo ou armazenamento incompatíveis. Consequentemente, o Macie não consegue analisar nenhum objeto nesses buckets.

4. Para detalhar e analisar os dados de suporte de um bucket do S3, escolha o nome do bucket. Em seguida, consulte o painel de detalhes do bucket para obter estatísticas e outras informações sobre o bucket.
5. Para exportar a tabela para um arquivo CSV, escolha Exportar para CSV na parte superior da página. O arquivo CSV resultante contém um subconjunto de metadados para cada bucket do S3 na tabela, para até 50.000 buckets. O arquivo inclui um campo de Problemas de cobertura. O valor neste campo indica se problemas impediram que o Macie de analisar objetos no bucket e, em caso positivo, a natureza dos problemas.

API

Para revisar os dados de cobertura de forma programática, especifique os critérios de filtro nas consultas que você envia usando a operação DescribeBuckets da API do Amazon Macie. Essa operação retorna uma matriz de objetos. Cada objeto contém dados estatísticos e outras informações sobre um bucket do S3 que corresponde aos critérios do filtro.

Nos critérios de filtro, inclua uma condição para o tipo de dados de cobertura que você deseja revisar:

- Para identificar buckets que o Macie não tem permissão para acessar devido às configurações de permissões dos buckets, inclua uma condição em que o valor do campo `errorCode` seja igual a `ACCESS_DENIED`.
- Para identificar buckets que o Macie tem permissão para acessar e ainda não analisou, inclua condições em que o valor do campo `sensitivityScore` seja igual a `50` e o valor do campo `errorCode` não seja igual a `ACCESS_DENIED`.
- Para identificar buckets que o Macie não pode analisar porque todos os objetos dos buckets usam classes ou formatos de armazenamento incompatíveis, inclua condições em que o valor do campo `classifiableSizeInBytes` seja igual a `0` e o valor do campo `sizeInBytes` seja maior que `0`.
- Para identificar buckets para os quais o Macie analisou pelo menos um objeto, inclua condições em que o valor do campo `sensitivityScore` esteja dentro do intervalo de 1 a 99, mas não seja igual a `50`. Para incluir também buckets nos quais você atribuiu manualmente a pontuação máxima, o intervalo deve ser de 1 a 100.
- Para identificar buckets que o Macie ainda não analisou devido a erros de classificação no nível de objetos, inclua uma condição em que o valor do campo `sensitivityScore` seja igual `-1`.

Em seguida, para analisar um detalhamento dos tipos e do número de erros que ocorreram em um determinado bucket, use a operação GetResourceProfile.

Se você estiver usando o AWS Command Line Interface(AWS CLI), especifique os critérios de filtro nas consultas enviadas executando o comando describe-buckets. Para analisar um detalhamento dos tipos e do número de erros que ocorreram em um determinado bucket S3, use o comando get-resource-profile.

Por exemplo, os comandos AWS CLI a seguir usam critérios de filtro para recuperar os detalhes de todos os buckets do S3 que o Macie não tem permissão para acessar devido às configurações de permissões dos buckets.

Este exemplo é formatado para for Linux, macOS, ou Unix:

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Este exemplo é formatado para Microsoft Windows:

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

Se a sua solicitação for realizada com êxito, o Macie retornará um array `buckets`. O array contém um objeto para cada bucket do S3 que está no Região da AWS atual e corresponde aos critérios do filtro.

Se nenhum bucket do S3 corresponder aos critérios do filtro, o Macie retornará um array `buckets` vazio.

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

Para obter mais informações sobre a especificação de critérios de filtro em consultas, incluindo exemplos de critérios comuns, consulte Como filtrar o seu inventário de buckets do S3.

Corrigindo problemas de cobertura para descoberta automatizada de dados confidenciais

O Amazon Macie relata vários tipos de problemas que reduzem a cobertura de descoberta de dados confidenciais automatizados dos seus dados do Amazon Simple Storage Service (Amazon S3). As informações a seguir podem ajudar você a investigar e corrigir esses problemas.

Tipos e detalhes do problema

- Acesso negado
- Erro de classificação: conteúdo inválido
- Erro de classificação: criptografia inválida
- Erro de classificação: chave KMS inválida
- Erro de classificação: permissão negada
- Inclassificável

> **Tip**
>
> Para investigar erros de classificação no nível de objeto em um bucket do S3, comece analisando a lista de amostras de objetos do bucket. Essa lista indica quais objetos o Macie analisou ou tentou analisar no bucket para até 100 objetos.
> Para revisar a lista no console do Amazon Macie, escolha o bucket na página de buckets do S3 e, em seguida, escolha a guia Amostras de objetos no painel de detalhes do bucket. Para revisar a lista programaticamente, use a operação ListResourceProfileArtifacts da API do Amazon Macie. Se o status da análise de um objeto for Skipped (`SKIPPED`), o objeto pode ter causado o erro.

Acesso negado

Esse problema indica que as configurações de permissões de um bucket do S3 impedem que o Macie acesse o bucket ou os objetos do bucket. O Macie não consegue recuperar e analisar nenhum objeto nesse buckets.

Detalhes

A causa mais comum desse tipo de problema é uma política restritiva de bucket. Uma política de bucket é uma política do (IAM) AWS Identity and Access Management baseada em recursos

que especifica quais ações uma entidade principal (usuário, conta, serviço ou outra entidade) pode realizar em um bucket do S3, bem como as condições em que uma entidade principal pode realizar essas ações. Uma política restritiva de bucket usa `Allow` explícitas ou declarações `Deny` que concedem ou restringem o acesso aos dados de um bucket com base em condições específicas. Por exemplo, uma política de buckets pode conter uma declaração `Allow` ou `Deny` que nega acesso a um bucket, a menos que endereços IP de origem específicos sejam usados para acessar o bucket.

Se a política de buckets para um bucket do S3 contiver uma declaração `Deny` explícita com uma ou mais condições, o Macie pode não ter permissão para recuperar e analisar os objetos do bucket para detectar dados confidenciais. O Macie pode fornecer somente um subconjunto de informações sobre o bucket, como o nome e a data de criação do bucket.

Orientação de remediação

Para corrigir esse problema, atualize a política de bucket para o bucket S3. Certifique-se de que a política permita que o Macie acesse o bucket e os objetos do bucket. Para permitir esse acesso, adicione uma condição para a função vinculada ao serviço do Macie (`AWSServiceRoleForAmazonMacie`) à política. A condição deve impedir que a função vinculada ao serviço do Macie corresponda à restrição `Deny` na política. Ela pode fazer isso usando a chave de contexto de condição global `aws:PrincipalArn` e o nome do recurso da Amazon (ARN) da função vinculada ao serviço Macie para sua conta.

Se você atualizar a política do bucket e o Macie obtiver acesso ao bucket do S3, o Macie detectará a alteração. Quando isso ocorre, o Macie atualizará estatísticas, dados de inventário e outras informações que fornece sobre seus dados Amazon S3. Além disso, os objetos do bucket terão maior prioridade para análise durante um ciclo de análise subsequente.

Referência adicional

Para obter mais informações sobre a atualização de uma política de bucket do S3 para permitir que o Macie acesse um bucket, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3. Para obter informações sobre como usar políticas de buckets para controlar o acesso aos buckets, consulte as Políticas de buckets e políticas de usuário e Como o Amazon S3 autoriza uma solicitação no Guia do Usuário do Serviço Amazon Simple Storage.

Erro de classificação: conteúdo inválido

Esse tipo de erro de classificação ocorre quando o Macie tenta analisar um objeto em um bucket do S3 e o objeto está malformado ou contém conteúdo que excede uma cota de descoberta de dados confidenciais. O Macie não consegue analisar o objeto.

Detalhes

Esse erro geralmente ocorre porque um objeto do S3 é um arquivo malformado ou corrompido. Consequentemente, o Macie não consegue analisar todos os dados no arquivo.

Esse erro também pode ocorrer se a análise de um objeto do S3 exceder uma cota de descoberta de dados confidenciais para um arquivo individual. Por exemplo, o tamanho de armazenamento do objeto excede a cota de tamanho desse tipo de arquivo.

Em ambos os casos, o Macie não consegue concluir a análise do objeto S3 e o status da análise do objeto é Ignorado (`SKIPPED`).

Orientação de remediação

Para investigar esse erro, baixe o objeto S3 e verifique a formatação e o conteúdo do arquivo. Avalie também o conteúdo do arquivo em relação às cotas do Macie para descoberta de dados confidenciais.

Se você não corrigir esse erro, o Macie tentará analisar outros objetos no bucket do S3. Se o Macie analisar outro objeto com sucesso, o Macie atualizará os dados de cobertura e outras informações que ele fornece sobre o bucket.

Referência adicional

Para obter uma lista de cotas de descoberta de dados confidenciais, incluindo as cotas para determinados tipos de arquivos, consulte Cotas do Amazon Macie. Para obter informações sobre como o Macie atualiza as pontuações de sensibilidade e outras informações que ele fornece sobre buckets do S3, consulte Como funciona a descoberta automatizada de dados confidenciais.

Erro de classificação: criptografia inválida

Esse tipo de erro de classificação ocorre quando o Macie tenta analisar um objeto em um bucket do S3 e o objeto é criptografado com uma chave fornecida pelo cliente. O objeto usa criptografia SSE-C, o que significa que o Macie não pode recuperar e analisar o objeto.

Detalhes

O Amazon S3 oferece suporte a várias opções de criptografia para objetos do S3. Para a maioria dessas opções, o Macie pode descriptografar um objeto usando a função vinculada ao serviço do Macie para a sua conta. No entanto, isso depende do tipo de criptografia usada.

Para que o Macie descriptografe um objeto do S3, o objeto deve ter sido criptografado com uma chave que o Macie possa acessar e usar. Se um objeto for criptografado com uma chave fornecida pelo cliente, o Macie não poderá fornecer o material de chave necessário para recuperar o objeto do Amazon S3. Consequentemente, o Macie não consegue analisar o objeto e o status da análise do objeto é Ignorado (`SKIPPED`).

Orientação de remediação

Para corrigir esse erro, criptografe objetos do S3 com chaves gerenciadas ou chaves do Amazon S3 ou chaves AWS Key Management Service (AWS KMS). Se você preferir usar chaves AWS KMS, elas podem ser chaves KMS gerenciadas pela AWS ou chaves KMS gerenciadas pelo cliente que o Macie tem permissão para usar.

Para criptografar objetos S3 existentes com chaves que o Macie possa acessar e usar, você pode alterar as configurações de criptografia dos objetos. Para criptografar novos objetos com chaves que o Macie possa acessar e usar, altere as configurações de criptografia do bucket S3. Além disso, certifique-se de que a política do bucket não exija que novos objetos sejam criptografados com uma chave fornecida pelo cliente.

Se você não corrigir esse erro, o Macie tentará analisar outros objetos no bucket do S3. Se o Macie analisar outro objeto com sucesso, o Macie atualizará os dados de cobertura e outras informações que ele fornece sobre o bucket.

Referência adicional

Para obter informações sobre os requisitos e as opções de uso do Macie para analisar objetos criptografados do S3, consulte Análise de objetos criptografados do Amazon S3 com o Amazon Macie. Para saber mais sobre as configurações e opções de criptografia para buckets S3, consulte Proteção de dados por criptografia e Definindo o comportamento de criptografia padrão no lado do cliente para buckets do S3 no Guia do usuário do Amazon Simple Storage Service.

Erro de classificação: chave KMS inválida

Esse tipo de erro de classificação ocorre quando o Macie tenta analisar um objeto em um bucket do S3 e o objeto é criptografado com uma chave AWS Key Management Service (AWS KMS) que não está mais disponível. O Macie não consegue recuperar e analisar o objeto.

Detalhes

AWS KMS fornece opções para desativar e excluir o gerenciamento AWS KMS keys pelo cliente. Se um objeto do S3 for criptografado com uma chave KMS desativada, agendada para exclusão ou excluída, o Macie não poderá recuperar e descriptografar o objeto. Consequentemente, o Macie não consegue analisar o objeto e o status da análise do objeto é Ignorado (`SKIPPED`). Para que o Macie analise um objeto criptografado, o objeto deve ser criptografado com uma chave que o Macie possa acessar e usar.

Orientação de remediação

Para corrigir esse erro, reative ou cancele a exclusão programada da AWS KMS key aplicável, dependendo do status atual da chave. Se a chave aplicável já tiver sido excluída, esse erro não poderá ser corrigido.

Para determinar qual AWS KMS key foi usada para criptografar um objeto do S3, você pode começar usando o Macie para revisar as configurações de criptografia do lado do servidor para o bucket do S3. Se as configurações de criptografia padrão do bucket estiverem configuradas para usar uma chave KMS, os detalhes do bucket indicarão qual chave será usada. Em seguida, você pode verificar o status dessa chave. Como alternativa, você pode usar o Amazon S3 para revisar as configurações de criptografia do bucket e dos objetos individuais no bucket.

Se você não corrigir esse erro, o Macie tentará analisar outros objetos no bucket do S3. Se o Macie analisar outro objeto com sucesso, o Macie atualizará os dados de cobertura e outras informações que ele fornece sobre o bucket.

Referência adicional

Para obter informações sobre como usar o Macie para revisar as configurações de criptografia do lado do servidor para um bucket do S3, consulte Analisar os detalhes dos buckets do S3. Para obter informações sobre como reativar ou cancelar a exclusão programada de uma AWS KMS key, consulte Ativação e desativação de chaves e Agendamento e cancelamento da exclusão de chaves no Guia do desenvolvedor AWS Key Management Service.

Erro de classificação: permissão negada

Esse tipo de erro de classificação ocorre quando o Macie tenta analisar um objeto em um bucket do S3 e não consegue recuperar ou descriptografar o objeto devido às configurações para o objeto ou às configurações das permissões à chave que foi usada para criptografar o objeto. O Macie não consegue recuperar e analisar o objeto.

Detalhes

Esse erro geralmente ocorre porque um objeto do S3 é criptografado com uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente que o Macie não tem permissão para usar. Se um objeto for criptografado com uma AWS KMS key gerenciada pelo cliente, a política de chaves deve permitir que o Macie decifre os dados usando a chave.

Esse erro também pode ocorrer se as configurações de permissões do Amazon S3 impedirem o Macie de recuperar um objeto do S3. A política de buckets do S3 bucket pode restringir o acesso a objetos específicos do bucket ou permitir que somente algumas entidades principais (usuários, contas, serviços ou outras entidades) acessem os objetos. Ou a lista de controle de acesso (ACL) a um objeto pode restringir o acesso ao objeto. Consequentemente, pode ser que o Macie não tenha permissão para acessar o objeto.

Nesses casos descritos acima, o Macie não consegue recuperar e analisar o objeto e, por isso, o status da análise do objeto é Ignorado (`SKIPPED`).

Orientação de remediação

Para corrigir esse erro, determine se o objeto do S3 está criptografado com uma AWS KMS key gerenciada pelo cliente. Se estiver, certifique-se de que a política de chave permita que a função vinculada ao serviço (`AWSServiceRoleForAmazonMacie`) do Macie decifre dados com a chave. A forma como você permite esse acesso depende se a conta proprietária da AWS KMS key também é proprietária do bucket do S3 que armazena o objeto. Se a mesma conta possuir a chave KMS e o bucket, um usuário da conta precisará atualizar a política de chaves. Se uma conta possuir a chave KMS e outra conta diferente possuir o bucket, um usuário da conta que possui a chave deve permitir o acesso entre contas à chave.

> **Tip**
>
> Você pode gerar automaticamente uma lista de todas as AWS KMS keys gerenciadas por clientes de que o Macie precisa para acessar ao analisar objetos nos buckets do S3 da sua conta. Para fazer isso, execute o script do Analisador de Permissões AWS KMS

que está disponível no repositório dos Amazon Macie Scripts no GitHub. O script também pode gerar um script adicional de comandos AWS Command Line Interface (AWS CLI). Opcionalmente, você pode executar esses comandos para atualizar as configurações e políticas necessárias para as chaves KMS que você especificar.

Se o Macie já tiver permissão para usar a AWS KMS key aplicável ou se o objeto do S3 não estiver criptografado com uma chave KMS gerenciada pelo cliente, certifique-se de que a política do bucket permita que o Macie acesse o objeto. Verifique também se a ACL do objeto permite que o Macie leia os dados e os metadados do objeto.

Para a política de bucket, você pode permitir esse acesso adicionando à política uma condição para a função vinculada ao serviço do Macie. A condição deve impedir que a função vinculada ao serviço do Macie corresponda à restrição `Deny` na política. Ela pode fazer isso usando a chave de contexto de condição global `aws:PrincipalArn` e o nome do recurso da Amazon (ARN) da função vinculada ao serviço Macie para sua conta.

Para a ACL do objeto, você pode permitir esse acesso trabalhando com o proprietário do objeto para adicionar sua Conta da AWS como beneficiário com permissões `READ` para o objeto. O Macie pode usar a função vinculada ao serviço na sua conta para recuperar e analisar o objeto. Considere também alterar as configurações de propriedade do objeto para o bucket. Você pode usar essas configurações para desativar as ACLs para todos os objetos no bucket e conceder permissões de propriedade à conta proprietária do bucket.

Se você não corrigir esse erro, o Macie tentará analisar outros objetos no bucket do S3. Se o Macie analisar outro objeto com sucesso, o Macie atualizará os dados de cobertura e outras informações que ele fornece sobre o bucket.

Referência adicional

Para obter mais informações sobre como permitir que o Macie decodifique dados com um AWS KMS key gerenciado pelo cliente, consulte Permitir que o Amazon Macie use um AWS KMS key gerenciado pelo cliente . Para obter mais informações sobre a atualização de uma política de bucket do S3 para permitir que o Macie acesse um bucket, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Para obter informações sobre como atualizar uma política de chaves, consulte Alterar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service. Para obter informações sobre o uso gerenciado pelo cliente do AWS KMS keys para criptografar objetos do

S3, consulte Uso da criptografia do lado do servidor com chavesAWS KMS no Guia do usuário do Amazon Simple Storage Service.

Para obter informações sobre como usar políticas de buckets para controlar o acesso aos buckets do S3, consulte as Políticas de buckets e políticas de usuário e Como o Amazon S3 autoriza uma solicitação no Guia do Usuário do Serviço Amazon Simple Storage. Para obter informações sobre o uso de ACLs ou configurações de propriedade de objetos para controlar o acesso aos objetos do S3, consulte Gerenciamento de acesso com ACLs e Controle da propriedade de objetos e desativação de ACLs para seu bucket no Guia do usuário do serviço de armazenamento do Amazon Simple.

Inclassificável

Esse problema indica que todos os objetos em um bucket do S3 são armazenados usando classes de armazenamento do Amazon S3 não suportadas ou formatos de arquivo ou armazenamento incompatíveis. O Macie não consegue analisar nenhum objeto no bucket.

Detalhes

Para ser elegível para seleção e análise, um objeto do S3 deve usar uma classe de armazenamento Amazon S3 compatível com o Macie. O objeto também deve ter uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível com o Macie. Se um objeto não atender a esses critérios, ele será tratado como um objeto inclassificável. O Macie não tenta recuperar ou analisar dados em objetos inclassificáveis.

Se todos os objetos em um bucket do S3 forem objetos inclassificáveis, o bucket geral será um bucket inclassificável. O Macie não pode realizar a descoberta automatizada de dados confidenciais para o bucket.

Orientação de remediação

Para resolver esse problema, revise as regras de configuração do ciclo de vida e outras configurações que determinam quais classes de armazenamento são usadas para armazenar objetos no bucket do S3. Considere ajustar essas configurações para usar as classes de armazenamento suportadas pelo Macie. Você também pode alterar a classe de armazenamento dos objetos existentes no bucket.

Avalie também os formatos de arquivo e de armazenamento de objetos existentes no bucket do S3. Para analisar os objetos, considere transferir os dados, de modo temporário ou permanente, para novos objetos que usem um formato compatível.

Se os objetos forem adicionados ao bucket do S3 e usarem uma classe e um formato de armazenamento compatíveis, o Macie detectará os objetos na próxima vez em que avaliar seu inventário do bucket. Quando isso acontecer, o Macie deixará de relatar que o bucket não é classificável em estatísticas, dados de cobertura e outras informações que ele fornece sobre seus dados do Amazon S3. Além disso, os novos objetos terão maior prioridade para análise durante um ciclo de análise subsequente.

Referência adicional

Para obter informações sobre as classes de armazenamento do Amazon S3 e os formatos de arquivo e armazenamento compatíveis com o Macie, consulte Classes e formatos de armazenamento suportados pelo Amazon Macie. Para obter informações sobre as regras de configuração do ciclo de vida e opções de classe de armazenamento que o Amazon S3 fornece, consulte Gerenciando o ciclo de vida do seu armazenamento e Usando as classes de armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Analisando estatísticas e resultados automatizados de descoberta de dados confidenciais

Quando a descoberta automática de dados confidenciais é habilitada para sua conta, o Amazon Macie gera e mantém automaticamente dados adicionais de inventário, estatísticas e outras informações sobre os buckets do Amazon Simple Storage Service (Amazon S3) que ele monitora e analisa para sua conta. Se você for o administrador do Macie em uma organização, isso inclui objetos nos buckets do S3 que as contas de seus membros possuem.

As informações adicionais capturam os resultados das atividades automatizadas de descoberta de dados confidenciais que a Macie realizou até agora em sua conta. Também complementa outras informações que o Macie fornece sobre seus dados do Amazon S3, como acesso público e configurações de criptografia para buckets do S3 individuais. Além de metadados e estatísticas, o Macie produz registros dos dados confidenciais que encontra e da análise que realiza, descobertas de dados confidenciais e resultados de descobertas de dados confidenciais.

À medida que a descoberta automatizada de dados confidenciais analisa o progresso da sua conta, os seguintes atributose dados podem ajudar você a analisar e avaliar os resultados:

- Painel de resumo — Fornece estatísticas agregadas para sua propriedade de dados do Amazon S3. As estatísticas incluem dados de métricas importantes, como o número total de buckets nos quais o Macie encontrou dados confidenciais e quantos desses buckets estão acessíveis ao

público. Eles também incluem dados sobre problemas que afetam a cobertura do seu patrimônio de dados.

- Mapa de calor de buckets do S3 — Fornece uma representação visual interativa da confidencialidade dos dados em todo o seu estado de dados, agrupados por Conta da AWS. Para cada conta, o mapa inclui estatísticas de confidencialidade agregadas e usa cores para indicar a pontuação de confidencialidade atual de cada bucket que a conta possui. O mapa também usa símbolos para ajudar você a identificar buckets que são acessíveis ao público, que não podem ser analisados pelo Macie e muito mais.
- Tabela de buckets do S3 — Fornece informações resumidas para cada bucket do S3 em seu inventário. Para cada bucket, a tabela inclui dados como o nome do bucket e a pontuação de confidencialidade atual, o número de objetos que o Macie pode analisar no bucket e se você configurou algum trabalho confidencial de descoberta de dados para analisar periodicamente objetos no bucket. Você pode, opcionalmente, exportar dados da tabela para um arquivo de valores separados por vírgulas (CSV).
- Painel de detalhes — Fornece detalhes e estatísticas de um bucket do S3 que você escolhe no mapa de calor ou na tabela. Os detalhes incluem uma lista de objetos que o Macie analisou no bucket e um detalhamento dos tipos e do número de ocorrências de dados confidenciais que o Macie encontrou no bucket. Você também pode usar o painel para gerenciar as configurações de descoberta automatizada para buckets individuais.
- Descobertas de dados confidenciais — Forneça relatórios detalhados de dados confidenciais que o Macie encontra em objetos individuais do S3. Os detalhes incluem quando o Macie encontrou os dados confidenciais e os tipos e número de ocorrências dos dados confidenciais que o Macie encontrou. Os detalhes também incluem informações sobre o bucket e o objeto do S3 afetados, incluindo as configurações de acesso público do bucket e quando o objeto foi alterado pela última vez.
- Resultados confidenciais da descoberta de dados — Forneça registros da análise que o Macie realiza para objetos individuais do S3. Isso inclui objetos nos quais o Macie não encontra dados confidenciais e, portanto, não produz descobertas de dados confidenciais, e objetos que o Macie não pode analisar devido a erros ou problemas.

Com esses dados, você pode avaliar a confidencialidade dos dados em todo o seu conjunto de dados do Amazon S3 e detalhar para avaliar e investigar buckets e objetos individuais do S3. Combinado com as informações que o Macie fornece sobre a segurança e a privacidade dos seus dados do Amazon S3, você também pode identificar casos em que uma remediação imediata possa

ser necessária — por exemplo, um bucket acessível ao público no qual o Macie encontrou dados confidenciais.

Dados adicionais podem ajudá-lo a avaliar e monitorar a cobertura do seu patrimônio de dados do Amazon S3. Com os dados de cobertura, você pode verificar o status das análises de seu patrimônio de dados geral e de buckets do S3 individuais em seu inventário de buckets. Você também pode identificar problemas que impediram o Macie de analisar objetos em buckets específicos. Se você corrigir os problemas, poderá aumentar a cobertura dos dados do Amazon S3 durante os ciclos de análise subsequentes. Para ter mais informações, consulte Como avaliar a cobertura da descoberta automatizada de dados confidenciais.

Tópicos

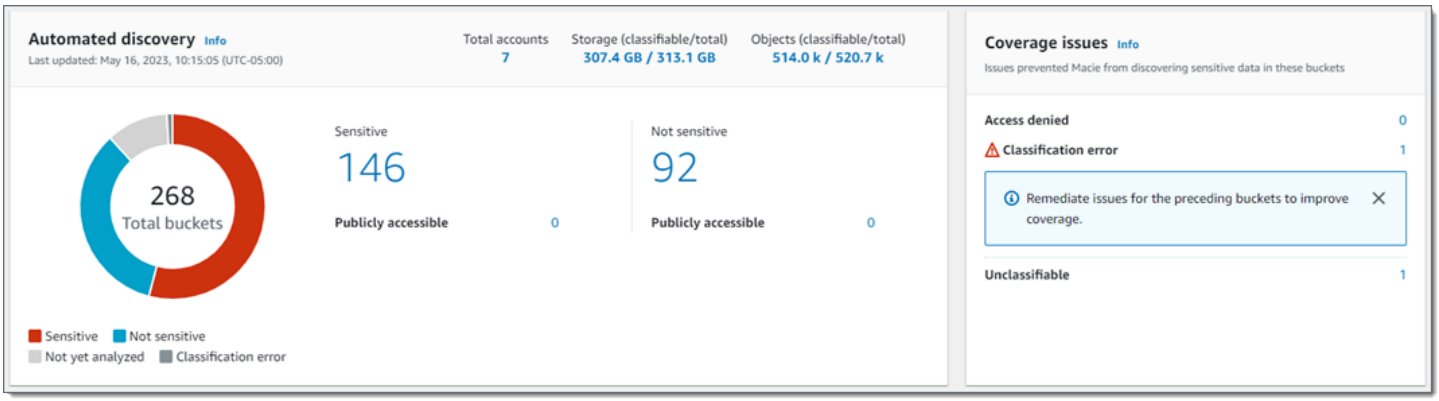
Revisando estatísticas agregadas de confidencialidade de dados no painel de resumo

No console do Amazon Macie, o painel de resumo fornece um instantâneo das estatísticas agregadas e dos dados de descobertas dos dados do Amazon Simple Storage Service (Amazon S3) na Região da AWS atual. Ele foi projetado para ajudar você a avaliar a postura geral de segurança dos dados do Amazon S3.

As estatísticas do painel incluem dados das principais métricas de segurança, como o número de buckets do S3 acessíveis ao público ou compartilhados com outras Contas da AWS. O painel também exibe grupos de dados agregados de descobertas da sua conta, por exemplo, os buckets do S3 que geraram mais descobertas nos sete dias anteriores. Se você for o administrador do Macie de uma organização, o painel fornece estatísticas e dados agregados para todas as contas da sua organização. Opcionalmente, você pode filtrar os dados por conta.

Se a descoberta automatizada de dados confidenciais estiver ativada em sua conta, o painel de resumo incluirá estatísticas automatizadas de descoberta de dados confidenciais. As estatísticas

capturam o status e os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora para seus dados do Amazon S3. Por exemplo: .



As estatísticas na seção Descoberta automatizada fornecem uma visão geral do status atual e dos resultados das atividades automatizadas de descoberta de dados confidenciais. Os dados não incluem os resultados de trabalhos confidenciais de descoberta de dados que você criou e executou.

As estatísticas na seção Problemas de cobertura indicam se os problemas impedem o Macie de analisar objetos em buckets individuais do S3. Essas estatísticas não incluem explicitamente dados de trabalhos confidenciais de descoberta de dados que você criou e executou. No entanto, a correção de problemas de cobertura que afetam seus resultados automatizados de descoberta de dados confidenciais provavelmente também aumentará a cobertura das tarefas que você executará posteriormente.

Tópicos

- Exibindo o painel Resumo
- Entendendo as estatísticas automatizadas de descoberta de dados confidenciais no painel de resumo

Exibindo o painel Resumo

Siga estas etapas para exibir o painel de resumo no console do Amazon Macie. Se você preferir consultar as estatísticas programaticamente, você pode usar a GetBucketStatisticsoperação da API do Amazon Macie.

Para exibir o painel de resumo

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Resumo. O Macie exibe o painel Resumo.

3. Para detalhar e revisar os dados de suporte de um item no painel, selecione o item.

Se você for o administrador do Macie de uma organização, o painel fornece estatísticas e dados agregados para a sua conta e as contas-membro da sua organização. Para filtrar o painel e exibir dados apenas de uma conta específica, insira o ID da conta na caixa Conta acima do painel.

Entendendo as estatísticas automatizadas de descoberta de dados confidenciais no painel de resumo

O painel de resumo no console do Amazon Macie inclui estatísticas agregadas que podem ajudar você a monitorar a descoberta automática de dados confidenciais para seus dados do Amazon S3. Por exemplo, você pode usar estatísticas do painel para determinar rapidamente em quantos buckets do S3 o Amazon Macie encontrou dados confidenciais e quantos desses buckets estão acessíveis publicamente. O painel fornece um instantâneo do status atual e dos resultados das análises dos dados do Amazon S3 na Região da AWS atual.

Você também pode usar estatísticas do painel para avaliar a cobertura dos seus dados do Amazon S3 e identificar problemas que impedem o Macie de analisar objetos em buckets do S3 individuais. Por exemplo, você pode determinar quantos buckets Macie não tem permissão para acessar em sua conta.

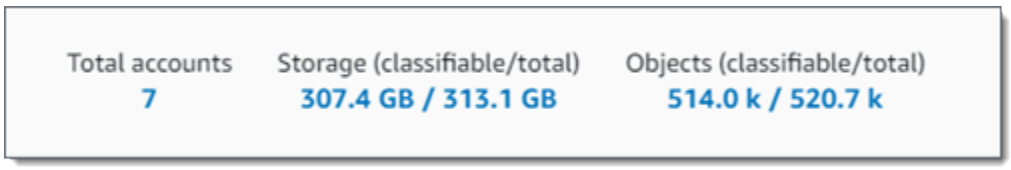
No painel, as estatísticas automatizadas de descoberta de dados confidenciais são organizadas principalmente nas seguintes seções:

- Armazenamento e descoberta de dados confidenciais
- Descoberta automatizada
- Problemas de cobertura

As estatísticas individuais em cada seção são as seguintes. Para obter informações sobre estatísticas em outras seções do painel Resumo, consulte Entendendo os componentes do painel Resumo.

Armazenamento e descoberta de dados confidenciais

Na parte superior da seção Descoberta automatizada, você encontrará estatísticas que indicam quantos dados você armazena no Amazon S3 e quanto desses dados o Macie pode analisar para detectar dados confidenciais. Por exemplo: .



Nesta seção:

- Total de contas — O número total desses Contas da AWS próprios buckets em seu inventário de buckets do S3. Se você for o administrador do Macie de uma organização, esse é o número total de contas do Macie que você gerencia para sua organização. Se você tiver uma conta independente do Macie, esse valor será 1.
- Armazenamento
  - Classificável – O tamanho total de armazenamento de todos os objetos que o Macie pode analisar nos buckets.
  - Total — O tamanho total de armazenamento de todos os objetos nos buckets, incluindo objetos que o Macie não consegue analisar.

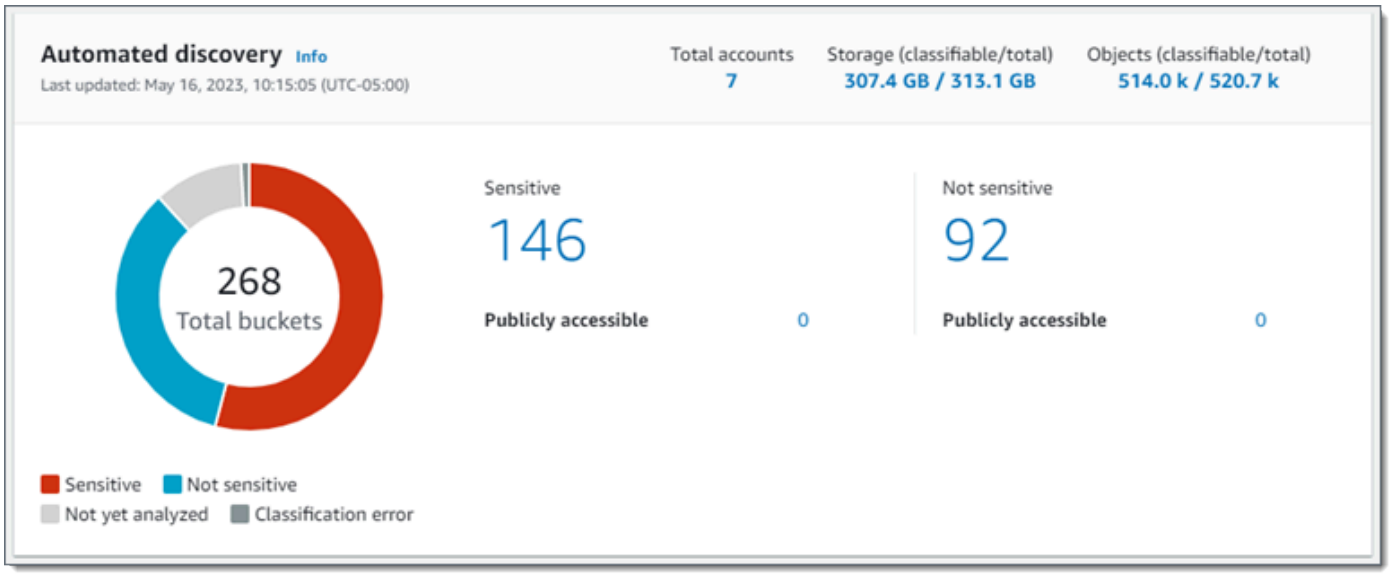
  Se algum dos objetos for um arquivo compactado, esses valores não refletirão o tamanho real desses arquivos depois de serem descompactados. Se o versionamento estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto classificável no bucket.
- Objetos
  - Classificável – O número total de objetos que o Macie pode analisar nos buckets.
  - Total – O tamanho total de armazenamento de todos os objetos nos buckets, incluindo objetos que o Macie não consegue analisar.

Nas estatísticas anteriores, dados e objetos serão classificáveis se usarem uma classe de armazenamento compatível do Amazon S3 e tiverem uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

Observe que as estatísticas Armazenamento e Objetos não incluem dados sobre objetos em buckets que o Macie não tem permissão para acessar. Para identificar buckets em que esse é o caso, selecione a estatística Acesso negado na seção Problemas de cobertura do painel.

Descoberta automatizada

As estatísticas primeiramente capturam o status e os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora para seus dados do Amazon S3. Por exemplo:



As estatísticas individuais nesta seção são as seguintes.

Total de buckets

O gráfico de rosca indica o número total de buckets em seu inventário de buckets do S3. O gráfico agrupa os buckets em categorias com base na pontuação de confidencialidade atual de cada bucket:

- Sigilosos (vermelho) — O número total de buckets cuja pontuação de confidencialidade varia de 51 a 100.
- Não sigilosos (azul) — O número total de buckets cuja pontuação de confidencialidade varia de 1 a 49.
- Ainda não analisados (cinza claro) — O número total de buckets cuja pontuação de confidencialidade é 50.
- Erro de classificação (cinza escuro) — O número total de buckets cuja pontuação de confidencialidade é -1.

Para obter detalhes sobre a faixa de pontuações de confidencialidade e rótulos que Macie define, consulte Pontuação de confidencialidade para buckets do S3.

Para revisar estatísticas adicionais de um grupo, passe o mouse sobre o grupo:

- Buckets – O número total de buckets.
- Acessível publicamente — o número total de buckets que permitem que o público em geral tenha acesso de leitura ou gravação ao bucket.
- Bytes classificáveis – O tamanho total de armazenamento de todos os objetos que o Macie pode analisar nos buckets. Esses objetos usam classes de armazenamento compatíveis do Amazon S3 e têm extensões de nome de arquivo para formatos de arquivo ou armazenamento compatíveis. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.
- Total de bytes — O tamanho total de armazenamento de todos os buckets.

Nas estatísticas anteriores, os valores do tamanho de armazenamento são baseados no tamanho de armazenamento da versão mais recente de cada objeto nos buckets. Se algum dos objetos for um arquivo compactado, esses valores não refletirão o tamanho real desses arquivos depois de serem descompactados.

Sigilosos

Essa área indica o número total de buckets do S3 que atualmente têm uma pontuação de confidencialidade que varia de 51 a 100. Dentro desse grupo, Acessível publicamente indica o número total de buckets que permitem que o público em geral tenha acesso de leitura ou gravação ao bucket.

Não sigilosos

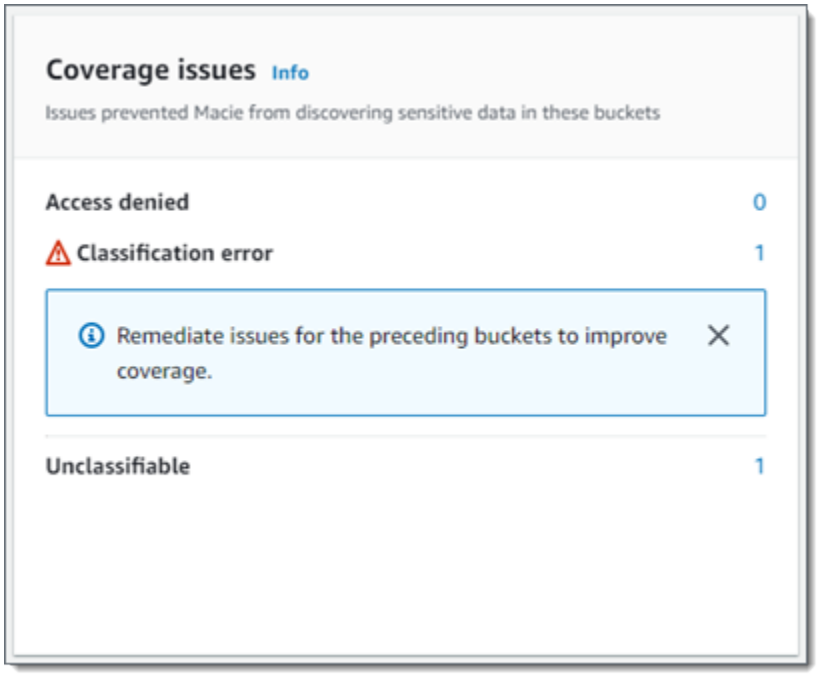
Essa área indica o número total de buckets do S3 que atualmente têm uma pontuação de confidencialidade que varia de 1 a 49. Dentro desse grupo, Acessível publicamente indica o número total de buckets que permitem que o público em geral tenha acesso de leitura ou gravação ao bucket.

Para determinar e calcular valores para as estatísticas Acessíveis publicamente, o Macie analisa uma combinação de configurações em nível de conta e de bucket para cada bucket, como as configurações de bloqueio de acesso público para a conta e o bucket, e a política de bucket para o bucket. Para ter mais informações, consulte Como o Macie monitora a segurança de dados do Amazon S3.

Observe que as estatísticas na seção Descoberta automatizada não incluem os resultados de trabalhos confidenciais de descoberta de dados que você criou e executou.

Problemas de cobertura

Essas estatísticas indicam se determinados tipos de problemas impedem o Macie de analisar objetos em buckets S3 individuais. Por exemplo: .



Nesta seção:

- Acesso negado — O número total de buckets que o Macie não tem permissão para acessar. Macie não consegue analisar nenhum objeto nesses buckets. As configurações de permissões dos buckets impedem que o Macie acesse os buckets e os objetos dos buckets.
- Erro de classificação — O número total de buckets que o Macie ainda não analisou devido a erros de classificação a nível de objeto. Macie tentou analisar um ou mais objetos nesses buckets. No entanto, Macie não conseguiu analisar os objetos devido a problemas com as configurações de permissões no nível do objeto, o conteúdo do objeto ou as cotas.
- Não classificáveis — O número total de buckets que não armazenam nenhum objeto classificável. Macie não consegue analisar nenhum objeto nesses buckets. Todos os objetos usam classes de armazenamento do Amazon S3 que o Macie não suporta, ou têm extensões de nome de arquivo para formatos de arquivo ou armazenamento que o Macie não suporta.

Escolha o valor de uma estatística para exibir detalhes adicionais e, conforme aplicável, orientação de remediação. Se você corrigir problemas de acesso e erros de classificação, poderá aumentar a cobertura dos dados do Amazon S3 durante os ciclos de análise subsequentes. Para ter mais informações, consulte Como avaliar a cobertura da descoberta automatizada de dados confidenciais.

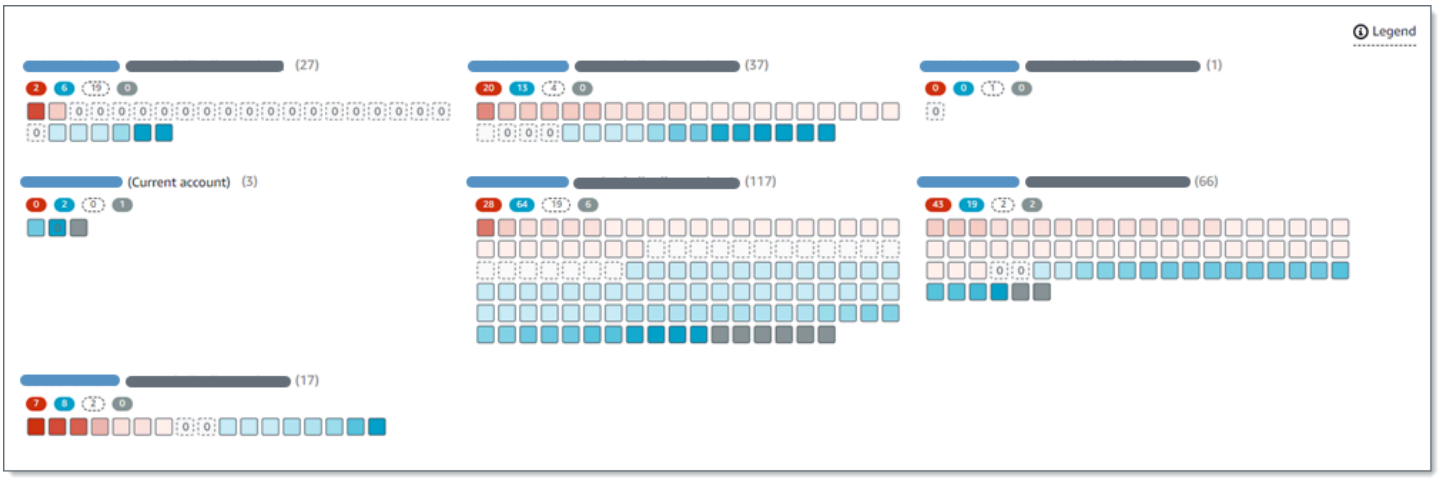
Observe que as estatísticas na seção Problemas de cobertura não incluem explicitamente dados de trabalhos confidenciais de descoberta de dados que você criou e executou. No entanto, a correção de problemas de cobertura que afetam seus resultados automatizados de descoberta de dados confidenciais provavelmente também aumentará a cobertura das tarefas que você executará posteriormente.

Para obter informações sobre outras seções do painel Resumo, consulte Entendendo os componentes do painel Resumo.

Como visualizar a confidencialidade dos dados com o mapa de buckets do S3

No console do Amazon Macie, o mapa de calor de buckets do S3 fornece uma representação visual e interativa da confidencialidade dos dados em todo o seu estado de dados atual do Amazon Simple Storage Service (Amazon S3). Região da AWS Ele captura os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora em sua conta.

Se você for o administrador do Macie de uma organização, o mapa inclui resultados para buckets do S3 que suas contas membros possuem, agrupados Conta da AWS e classificados por ID da conta. Por exemplo: .



Cada página do mapa exibe dados de até 99 contas ou 1.000 buckets, dependendo do tamanho da sua organização ou do patrimônio de dados do Amazon S3.

No painel de navegação, selecione Buckets do S3 no painel de navegação do console. Depois escolha o mapa

( )

na parte superior da página. O mapa estará disponível somente se a descoberta automática de

dados confidenciais estiver atualmente habilitada para sua conta. Ela não inclui resultados de trabalhos confidenciais de descoberta de dados que você criou e executou.

Tópicos

- Interpretação de dados no mapa de buckets do S3
- Interagir com o mapa de buckets do S3

Interpretação de dados no mapa de buckets do S3

No mapa de Buckets do S3, cada quadrado representa um bucket do S3 no seu inventário do buckets. A cor de um quadrado representa a pontuação de confidencialidade atual de um bucket, que mede a interseção de duas dimensões principais: a quantidade de dados confidenciais que o Macie encontrou no bucket e a quantidade de dados que o Macie analisou no bucket. A intensidade da tonalidade da cor representa onde a pontuação de um bucket cai em uma faixa de valores de confidencialidade de dados, conforme mostrado na imagem a seguir.

Em geral, você pode interpretar a intensidade da cor e do matiz da seguinte forma:

- Azul — Se a pontuação de confidencialidade atual de um bucket variar de 1 a 49, o quadrado do bucket será azul, e o rótulo de confidencialidade do bucket será Não confidencial. A intensidade do tom azul reflete o número de objetos únicos que o Macie analisou no bucket em relação ao número total de objetos únicos no bucket. Um tom mais escuro indica uma pontuação de confidencialidade mais baixa.
- Sem cor — Se a pontuação de confidencialidade atual de um bucket for 50, o quadrado do bucket não estará colorido, e o rótulo de confidencialidade do bucket será Ainda não analisados. Além disso, o quadrado tem uma borda tracejada.
- Vermelho — Se a pontuação de confidencialidade atual de um bucket varia de 51 a 100, o quadrado do bucket é vermelho e o rótulo de confidencialidade do bucket é Confidencial. A intensidade do tom vermelho reflete a quantidade de dados confidenciais que o Macie encontrou no bucket. Um tom mais escuro indica uma pontuação de confidencialidade mais alta.

- Cinza — Se a pontuação de confidencialidade atual de um bucket for -1, o quadrado do bucket será cinza escuro, e o rótulo de confidencialidade do bucket será Erro na classificação. A intensidade da tonalidade não varia.

Para obter detalhes sobre a faixa de pontuações de confidencialidade e rótulos que Macie define, consulte Pontuação de confidencialidade para buckets do S3.

No mapa, o quadrado de um bucket do S3 também pode conter um símbolo. O símbolo indica um erro, problema ou outro tipo de consideração que pode afetar sua avaliação da confidencialidade de um bucket. Um símbolo também pode indicar um possível problema com a segurança do bucket; por exemplo, o bucket está acessível ao público. A tabela a seguir lista os símbolos que o Macie usa para notificá-lo sobre esses casos.

Símbolo	Definição	Descrição
	Acesso negado	O Macie não tem permissão para acessar o bucket ou os objetos do bucket. Consequentemente, o Macie não pode analisar nenhum objeto no bucket. Esse problema geralmente ocorre porque um bucket tem uma política restritiva de bucket. Para obter informações sobre como resolver esse problema, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.
	Publicly accessible	O público em geral tem acesso de leitura e gravação ao bucket. Para fazer essa determinação, o Macie analisa uma combinação de configurações

Símbolo	Definição	Descrição
		em nível de conta e de bucket para cada bucket, como as configurações de bloqueio de acesso público para a conta e o bucket, e a política de bucket para o bucket. Para obter mais informaçõ es, consulte Como o Macie monitora a segurança de dados do Amazon S3.
	Não classificáveis	O Macie não consegue analisar nenhum objeto no bucket. Todos os objetos do bucket usam classes de armazenamento do Amazon S3 que o Macie não suporta, ou têm extensões de nome de arquivo para formatos de arquivo ou de armazenamento que o Macie não suporta. Para o Macie analisar um objeto, ele deve usar uma classe de armazenamento do compatível e ter uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatíve l. Para ter mais informações, consulte Classes e formatos de armazenamento suportado s.

Símbolo	Definição	Descrição
0	Zero bytes	O bucket não contém nenhum objeto para Macie analisar. O bucket está vazio ou todos os objetos no bucket contêm zero (0) bytes de dados.

Interagir com o mapa de buckets do S3

Ao revisar o mapa de buckets do S3, você pode interagir com ele de diferentes maneiras para revelar e avaliar dados e detalhes adicionais de contas e buckets individuais. Siga estas etapas para exibir o mapa no console do Amazon Macie e interagir com vários atributos que o mapa fornece.

Para interagir com o mapa de buckets do S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Bucketsdo S3. A página de buckets do S3 exibe um mapa do seu inventário de buckets. Se, em vez disso, a página exibir seu inventário em formato tabular, escolha mapa () na parte superior da página.
3. Na parte superior da página, escolha opcionalmente atualizar () para recuperar os metadados mais recentes do bucket a partir do Amazon S3.
4. No mapa de buckets do S3, faça o seguinte:

   - Para determinar quantos baldes têm uma etiqueta de sensibilidade específica, consulte os emblemas coloridos imediatamente abaixo de um Conta da AWS ID. Os emblemas exibem contagens agregadas de buckets, divididas por rótulo de confidencialidade.

     Por exemplo, o emblema vermelho informa o número total de buckets que pertencem à conta e têm o rótulo Confidencial. A pontuação de confidencialidade desses buckets varia de 51 a 100. Por exemplo, o emblema azul informa o número total de buckets que pertencem à conta e têm o rótulo Confidencial. A pontuação de confidencialidade desses buckets varia de 1 a 49.

- Para revisar um subconjunto de informações sobre um compartimento, passe o mouse sobre o quadrado do bucket. Um popover exibe o nome do bucket e a pontuação de confidencialidade atual.

  O popover também exibe o número total de objetos que o Macie pode analisar no bucket e o tamanho total de armazenamento da versão mais recente desses objetos. Esses objetos são classificáveis. Eles usam classes de armazenamento compatíveis do Amazon S3 e têm extensões de nome de arquivo para formatos de arquivo ou armazenamento compatíveis. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.
- Para filtrar o mapa e exibir somente os buckets que têm um valor específico para um campo, coloque o cursor na caixa de filtro e, em seguida, adicione uma condição de filtro para o campo. O Macie aplica seus critérios de condições e os exibe abaixo da caixa do filtro. Para refinar ainda mais os resultados, adicione condições de filtro para campos adicionais. Para ter mais informações, consulte Como filtrar o seu inventário de buckets do S3.
- Para detalhar e exibir somente os buckets pertencentes a uma conta específica, escolha o ID da conta. Macie abre uma nova guia que filtra e exibe dados somente dessa conta.

5. Para revisar todas as estatísticas confidenciais de descoberta de dados e outras informações que o Macie fornece sobre um determinado bucket, selecione o quadrado do bucket e, em seguida, consulte o painel de detalhes. Para ter mais informações, consulte Analisando detalhes de confidencialidade de dados para buckets do S3 individuais.

> **Tip**
>
> Na guia Detalhes do bucket do painel, você pode dinamizar e detalhar muitos dos campos. Para mostrar buckets que têm o mesmo valor para um campo, selecione
>
> no campo. Para mostrar buckets que têm o mesmo valor para um campo, escolha
> 
> no campo.

Como avaliar a confidencialidade dos dados com a tabela de buckets do S3

No console do Amazon Macie, a tabela de buckets do S3 exibe informações resumidas sobre cada um dos seus buckets do Amazon Simple Storage Service (Amazon S3) na Região da AWS atual. Se você for o administrador do Macie em uma organização, isso inclui informações sobre buckets do

S3 que as contas de seus membros possuem. Se preferir acessar os dados de forma programática, você pode usar a DescribeBucketsoperação da API Amazon Macie.

No console, é possível classificar e filtrar a tabela para personalizar a exibição. Você também pode exportar dados da tabela para um arquivo de valores separados por vírgulas (CSV). Se você escolher um bucket do S3 na tabela, o painel de detalhes exibirá informações adicionais sobre o bucket. Isso inclui detalhes e estatísticas que capturam os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie executou para o bucket até o momento. Também inclui dados para configurações e métricas que fornecem informações sobre a segurança e a privacidade dos dados do bucket. Além de revisar os detalhes de um bucket, você pode usar o painel de detalhes para ajustar as configurações automatizadas de descoberta de dados confidenciais do bucket. Para saber como, consulte Gerenciando a descoberta automatizada de dados confidenciais para buckets do S3 individuais.

Para avaliar a confidencialidade dos dados com a tabela de buckets do S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Bucketsdo S3.
3. Na página Buckets do S3, escolha a tabela
   ( )
   na parte superior da página. O Macie exibe o número de buckets em seu inventário e uma tabela dos buckets.
4. Na parte superior da página, escolha opcionalmente atualizar
   ( )
   para recuperar os metadados mais recentes do bucket a partir do Amazon S3.

   Se o ícone de informações
   ( )
   aparecer ao lado de qualquer nome de bucket, recomendamos que você faça isso. Esse ícone indica que um bucket foi criado nas últimas 24 horas, possivelmente após a última vez que Macie recuperou os metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização.
5. Na tabela de Buckets do S3, analise as informações resumidas sobre cada bucket em seu inventário:

- Confidencialidade — A pontuação de confidencialidade atual do bucket. Para obter informações sobre a faixa de pontuações de confidencialidade que Macie define, consulte Pontuação de confidencialidade para buckets do S3.
- Bucket – O nome do bucket.
- Conta — O ID da conta do Conta da AWS proprietário do bucket.
- Objetos classificáveis – O número total de objetos que o Macie pode analisar para detectar dados confidenciais no bucket.
- Tamanho classificável – O tamanho total de armazenamento de todos os objetos que o Macie pode analisar para detectar dados confidenciais nos buckets.

  Esse valor não reflete o tamanho real de qualquer objeto compactado depois que ele é descompactado. Além disso, se o versionamento estiver habilitado para o bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto no bucket.
- Monitorado por trabalho — especifica se algum trabalho confidencial de descoberta de dados está configurado para analisar periodicamente objetos no bucket diariamente, semanalmente ou mensalmente.

  Se o valor desse campo for Sim, o bucket será incluído explicitamente em um trabalho periódico ou corresponderá aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.
- Última execução do trabalho — se algum trabalho de descoberta de dados confidenciais único ou periódico estiver configurado para analisar objetos no bucket, o valor desse campo indicará a data e a hora mais recentes em que um desses trabalhos começou a ser executado. Caso contrário, esse campo fica vazio.

Nos dados anteriores, os objetos serão classificáveis se usarem uma classe de armazenamento compatível do Amazon S3 e tiverem uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. Você pode detectar dados confidenciais nos objetos usando Macie. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

6. Para analisar o inventário usando a tabela, siga um destes procedimentos:

- Para classificar a tabela por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna.
- Para filtrar a tabela e exibir somente os buckets que têm um valor específico para um campo, coloque o cursor na caixa de filtro e, em seguida, adicione uma condição de filtro para o campo. O Macie aplica seus critérios de condições e os exibe abaixo da caixa do filtro. Para refinar ainda mais os resultados, adicione condições de filtro para campos adicionais. Para ter mais informações, consulte Como filtrar o seu inventário de buckets do S3.
- Para revisar detalhes e estatísticas de um bucket específico, escolha o nome do bucket na tabela e consulte o painel de detalhes. Para ter mais informações, consulte Analisando detalhes do bucket do S3.

> **Tip**
>
> Na guia Detalhes do bucket do painel, você pode dinamizar e detalhar muitos dos campos. Para mostrar buckets que têm o mesmo valor para um campo, selecione
> 
> no campo. Para mostrar buckets que têm o mesmo valor para um campo, escolha
> 
> no campo.

7. Para exportar dados da tabela para um arquivo CSV, marque a caixa de seleção para cada linha que você deseja exportar ou marque a caixa de seleção no título da coluna de seleção para selecionar todas as linhas. Em seguida, selecione Exportar para CSV na parte superior da página. Você pode exportar até 50.000 linhas da tabela.
8. Para realizar uma análise mais profunda e imediata dos objetos em um ou mais buckets, marque a caixa de seleção de cada bucket e escolha Criar tarefa. Para ter mais informações, consulte Criar um trabalho de descoberta de dados confidenciais.

Analisando detalhes de confidencialidade de dados para buckets do S3 individuais

No console do Amazon Macie, você pode usar o painel de detalhes na página Buckets do S3 para revisar estatísticas e outras informações sobre buckets individuais do Amazon Simple Storage Service (Amazon S3) que o Macie monitora e analisa para sua conta. Se você for o administrador do Macie em uma organização, isso inclui objetos nos buckets do S3 que as contas de seus membros possuem.

As estatísticas e as informações incluem detalhes que fornecem informações sobre a segurança e a privacidade dos dados de um bucket do S3. Se a descoberta automatizada de dados confidenciais estiver ativada em sua conta, eles também capturarão os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora em um bucket. Por exemplo, você pode encontrar uma lista de objetos que o Macie analisou em um bucket e um detalhamento dos tipos e do número de ocorrências de dados confidenciais que o Macie encontrou em um bucket. Observe que os dados não incluem os resultados de trabalhos de descoberta de dados confidenciais que você criou e executou.

O Macie recalcula e atualiza automaticamente essas estatísticas e detalhes enquanto realiza a descoberta automática de dados confidenciais em sua conta. Por exemplo: .

- Se o Macie não encontrar dados confidenciais em um objeto do S3, o Macie diminui a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário. O Macie também adiciona o objeto à lista de objetos que são analisados no bucket.
- Se o Macie encontrar dados confidenciais em um objeto do S3, o Macie adiciona essas ocorrências ao detalhamento dos tipos de dados confidenciais que o Macie encontrou no bucket. O Macie também aumenta a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário. Além disso, o Macie adiciona o objeto à lista de objetos que são analisados no bucket. Essas tarefas são adicionais à criação de uma descoberta de dados confidenciais para o objeto.
- Se o Macie encontrar dados confidenciais em um objeto do S3 que é posteriormente alterado ou excluído, o Macie remove as ocorrências de dados confidenciais desse objeto da divisão de tipos de dados confidenciais do bucket. O Macie também diminui a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário. Além disso, o Macie remove o objeto da lista de objetos que são analisados no bucket.
- Se o Macie tentar analisar um objeto do S3, mas um problema ou erro impedir que o Macie faça isso, o Macie adiciona o objeto à lista de objetos analisados no bucket e indica que não conseguiu analisar o objeto.

Além de revisar as estatísticas e detalhes, você pode usar o painel para ajustar as configurações automatizadas de descoberta de dados confidenciais de um bucket do S3. Por exemplo, você pode incluir ou excluir tipos específicos de dados confidenciais da pontuação de um bucket. Para ter mais informações, consulte Gerenciando a descoberta automatizada para buckets do S3 individuais.

Para analisar detalhes de confidencialidade de dados para um bucket do S3

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Bucketsdo S3. A página de buckets do S3 exibe um mapa interativo do seu inventário de buckets. Opcionalmente, selecione a tabela ( ) na parte superior da página para exibir seu inventário em formato tabular.
3. No mapa ou tabela Buckets do S3, escolha o nome do bucket do S3 cujos detalhes você deseja revisar. O painel de detalhes exibe estatísticas e outras informações sobre o bucket.

A parte superior do painel mostra informações gerais sobre o bucket: o nome do bucket e o ID da conta do Conta da AWS proprietário do bucket. Ele também fornece opções para alterar determinadas configurações automatizadas de descoberta de dados confidenciais para o bucket. Configurações e informações adicionais sobre o bucket estão organizadas nas seguintes guias:

- Confidencialidade
- Detalhes do bucket
- Amostras de objeto
- Descoberta de dados confidenciais

As configurações e informações individuais em cada guia são as seguintes.

Confidencialidade

Essa guia mostra a pontuação de confidencialidade atual do bucket, variando de -1 a 100. Para obter informações sobre a faixa de pontuações de confidencialidade que Macie define, consulte Pontuação de confidencialidade para buckets do S3.

A guia também fornece um detalhamento dos tipos de dados confidenciais que o Macie encontrou nos objetos do bucket e o número de ocorrências de cada tipo:

- Tipo de dados sigilosos – O identificador (ID) exclusivo do identificador de dados gerenciados que detectou os dados, ou o nome do identificador de dados personalizado que detectou os dados.

  O ID de um identificador de dados gerenciados descreve o tipo de dados confidenciais que o identificador foi projetado para detectar; por exemplo, USA_PASSPORT_NUMBER para

números de passaportes dos EUA. Para obter detalhes sobre cada identificador de dados gerenciados, consulte Usar identificadores de dados gerenciados.

- Contagem — O número total de ocorrências dos dados que o identificador de dados gerenciado ou personalizado detectou.
- Status da pontuação — Especifica se as ocorrências dos dados são incluídas ou excluídas da pontuação de confidencialidade do bucket.

  Se você configurou o Macie para calcular a pontuação do bucket automaticamente, você pode ajustar o cálculo incluindo ou excluindo tipos específicos de dados confidenciais da pontuação do bucket: marque a caixa de seleção do identificador de dados que você deseja incluir ou excluir e, em seguida, escolha a opção desejada no menu Ações. Para ter mais informações, consulte Gerenciando a descoberta automatizada para buckets do S3 individuais.

Se o Macie não encontrou dados confidenciais em objetos que o bucket armazena atualmente, esta seção mostra a mensagem Nenhuma detecção encontrada.

Observe que a guia confidencialidade não inclui dados de objetos que o Macie analisou e que foram posteriormente alterados ou excluídos. Se os objetos forem alterados ou excluídos de um bucket após a análise do Macie, o Macie recalcula e atualiza automaticamente as estatísticas e os dados apropriados para excluir os objetos.

Detalhes do bucket

Essa guia fornece detalhes sobre as configurações do bucket, incluindo configurações de privacidade e segurança de dados. Por exemplo, você pode analisar os detalhamentos das configurações de acesso público do bucket e determinar se o bucket replica objetos ou é compartilhado com outras Contas da AWS.

Vale ressaltar que o campo Última atualização indica quando o Macie recuperou mais recentemente os metadados do Amazon S3 para o bucket ou os objetos do bucket. O campo Última execução de descoberta automatizada indica quando Macie analisou objetos no bucket mais recentemente enquanto realizava a descoberta automatizada.

A guia também fornece estatísticas em nível de objeto que podem ajudá-lo a avaliar a quantidade de dados que o Macie pode analisar no bucket. Também indica se algum trabalho confidencial de descoberta de dados está configurado para analisar objetos no bucket. Se houver, você poderá acessar detalhes sobre o trabalho executado mais recentemente e, opcionalmente, exibir as descobertas que o trabalho produziu.

Para obter detalhes adicionais sobre as informações nessa guia, consulte Analisar os detalhes dos buckets do S3.

Amostras de objeto

Essa guia lista os objetos que o Macie analisou no bucket enquanto realizava a descoberta automatizada de dados confidenciais. Opcionalmente, selecione o nome do objeto para abrir o console do Amazon S3 e exibir as propriedades do objeto.

A lista inclui dados de até 100 objetos. A lista é preenchida com base no valor do campo confidencialidade do objeto: Confidencial, seguido por Não confidencial, seguido por objetos que o Macie não conseguiu analisar.

Na lista, o campo confidencialidade do objeto indica se o Macie encontrou dados confidenciais em um objeto:

- Confidencial — Macie encontrou pelo menos uma ocorrência de dados confidenciais no objeto.
- Não confidencial — Macie não encontrou dados confidenciais no objeto.
- — (traço) — Macie não conseguiu concluir a análise do objeto devido a um problema ou erro.

O campo Resultado da classificação indica se Macie conseguiu analisar um objeto:

- Concluído – O Macie concluiu a análise do objeto.
- Parcial — Macie analisou somente um subconjunto de dados no objeto devido a um problema ou erro. Por exemplo, o objeto é um arquivo que contém arquivos em um formato incompatível.
- Ignorado — Macie não conseguiu analisar nenhum dado no objeto devido a um problema ou erro. Por exemplo, o objeto é criptografado com uma chave que Macie não tem permissão de usar.

Observe que a lista não inclui objetos que foram alterados ou excluídos depois que Macie os analisou ou tentou analisá-los. O Macie remove automaticamente um objeto da lista se o objeto for alterado ou excluído posteriormente.

Descoberta de dados confidenciais

Essa guia fornece estatísticas agregadas e automatizadas de descoberta de dados confidenciais para o bucket:

- Bytes analisados — A quantidade total de dados, em bytes, que o Macie analisou no bucket.
- Bytes classificáveis – O tamanho total de armazenamento, em bytes, de todos os objetos que o Macie pode analisar no bucket. Esses objetos usam classes de armazenamento compatíveis do Amazon S3 e têm extensões de nome de arquivo para formatos de arquivo

ou armazenamento compatíveis. Para ter mais informações, consulte Classes e formatos de armazenamento suportados.

- Total de detecções — O número total de ocorrências de dados confidenciais que o Macie encontrou no bucket. Isso inclui ocorrências atualmente suprimidas pelas configurações de pontuação de confidencialidade do bucket.

O gráfico Objetos analisados indica o número total de objetos que Macie analisou no bucket. Ele também fornece uma representação visual do número de objetos nos quais Macie encontrou ou não dados confidenciais. A legenda abaixo do gráfico mostra um detalhamento desses resultados:

- Objetos confidenciais (vermelho) — O número total de objetos no quais o Macie encontrou pelo menos uma ocorrência de dados confidenciais.
- Objetos não confidenciais (azul) — O número total de objetos nos quais Macie não encontrou dados confidenciais.
- Objetos ignorados (cinza escuro) — O número total de objetos que o Macie não conseguiu analisar devido a um problema ou erro.

A área abaixo da legenda do gráfico fornece um detalhamento dos casos em que Macie não conseguiu analisar objetos porque ocorreram certos tipos de problemas de permissão ou erros criptográficos:

- Ignorado: criptografia inválida — O número total de objetos criptografados com chaves fornecidas pelo cliente. Macie não consegue acessar essas chaves.
- Ignorado: KMS inválido — O número total de objetos criptografados com chaves AWS Key Management Service (AWS KMS) que não estão mais disponíveis. Esses objetos são criptografados com os AWS KMS keys que foram desativados, programados para exclusão ou excluídos. Macie não pode usar essas chaves.
- Ignorado: permissão negada — O número total de objetos que o Macie não tem permissão para acessar devido às configurações de permissões do objeto ou às configurações de permissões da chave usada para criptografar o objeto.

Para obter detalhes sobre esses e outros tipos de problemas e erros que podem ocorrer, consulteCorrigindo problemas de cobertura para descoberta automatizada de dados confidenciais. Se você corrigir os problemas e erros, poderá aumentar a cobertura dos dados do bucket durante os ciclos de análise subsequentes.

As estatísticas na guia Descoberta de dados confidenciais não incluem dados de objetos que foram alterados ou excluídos depois que Macie os analisou ou tentou analisá-los. Se os objetos

forem alterados ou excluídos de um bucket após o Macie analisar ou tentar analisá-los, o Macie recalculará e atualizará automaticamente essas estatísticas para excluir os objetos.

Analisando descobertas de dados confidenciais produzidas pela descoberta automatizada

Ao realizar descobertas automatizadas de dados confidenciais, o Amazon Macie cria uma descoberta de dados confidenciais para cada objeto do Amazon Simple Storage Service (Amazon S3) no qual encontra dados confidenciais. Uma descoberta de dados confidenciais é um relatório detalhado de dados confidenciais que o Macie encontrou em um objeto do S3. Cada descoberta de dados confidenciais fornece uma classificação de gravidade e detalhes como:

- A data e a hora em que Macie encontrou os dados confidenciais.
- A categoria e os tipos de dados confidenciais que Macie encontrou.
- O número de ocorrências de cada tipo de dado confidencial que Macie encontrou.
- Como Macie encontrou os dados confidenciais, a descoberta automatizada de dados confidenciais ou um trabalho de descoberta de dados confidenciais.
- O nome, as configurações de acesso público, o tipo de criptografia e outras informações sobre o bucket e o objeto do S3 afetados.

Dependendo do tipo de arquivo ou formato de armazenamento do objeto S3 afetado, os detalhes também podem incluir a localização de até 15 ocorrências dos dados confidenciais encontrados por Macie. Uma descoberta de dados confidenciais não inclui os dados confidenciais que Macie encontrou. Em vez disso, ele fornece informações que você pode usar para investigação e remediação adicionais, conforme necessário.

O Macie armazena suas descobertas de dados confidenciais por 90 dias. Você pode acessá-las usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode monitorar e processar descobertas usando outros aplicativos, serviços e sistemas. Para ter mais informações, consulte Analisando descobertas.

Para analisar descobertas produzidas pela descoberta automatizada de dados confidenciais

Para identificar e analisar as descobertas de dados confidenciais que o Macie cria enquanto realiza a descoberta automática de dados confidenciais em sua conta, você pode filtrar suas descobertas. Com filtros, você usa atributos específicos das descobertas para criar visualizações e consultas

personalizadas para as descobertas. Você pode usar o console do Amazon Macie para filtrar descobertas ou enviar consultas programaticamente usando a API do Amazon Macie.

Console

Siga estas etapas para identificar e analisar as descobertas usando o console do Amazon Macie.

Para analisar descobertas produzidas pela descoberta automatizada

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. (Opcional) Para exibir descobertas que foram suprimidas por uma regra de supressão, altere a configuração de Status da descoberta. Escolha Tudo para exibir descobertas suprimidas e não suprimidas, ou escolha Arquivado para exibir apenas descobertas suprimidas. Para ocultar novamente as descobertas suprimidas, escolha Atual.
4. Coloque o cursor na caixa Critérios de filtro. Na lista de campos exibida, escolha Tipo de origem.

   Este campo especifica como o Macie encontrou os dados confidenciais que produziram uma descoberta, uma descoberta automatizada de dados confidenciais ou um trabalho de descoberta de dados confidenciais. Para localizar esse campo na lista de campos de filtro, você pode navegar pela lista completa ou inserir parte do nome do campo para restringir a lista de campos.
5. Selecione AUTOMATED_SENSITIVE_DATA_DISCOVERY como o valor do campo e, em seguida, selecione Aplicar. O Macie aplica seus critérios de filtros e os adiciona a um filtro de token na caixa Critérios de filtro.
6. (Opcional) Para refinar os resultados, adicione condições de filtro para campos adicionais — por exemplo, Criado em para o intervalo de tempo em que uma descoberta foi criada, nome do bucket do S3 para o nome de um bucket afetado, ou Tipo de detecção de dados confidenciais para o tipo de confidencialidade que foi detectado e gerou uma descoberta. Para ter mais informações, consulte Filtrar descobertas.

Se quiser usar esse conjunto de condições novamente posteriormente, você pode salvar o conjunto como uma regra de filtro. Para fazer isso, escolha Salvar regra na caixa Critérios de filtro. Em seguida, insira um nome e, se preferir, uma descrição para a regra. Ao concluir, selecione Salvar.

API

Para identificar e analisar as descobertas de forma programática, especifique os critérios de filtro nas consultas que você envia usando a GetFindingStatisticsoperação ListFindingsou da API do Amazon Macie. A operação ListFindings retorna uma matriz de IDs de descoberta, uma ID para cada descoberta que corresponda aos critérios de filtro. Em seguida, você pode usar esses IDs para recuperar os detalhes de cada descoberta. A operação GetFindingStatistics retorna dados estatísticos agregados sobre todas as descobertas que correspondem aos critérios de filtro, agrupados por um campo que você especifica em sua solicitação. Para obter mais informações sobre como filtrar descobertas programaticamente, consulte Filtrar descobertas

Nos critérios de filtro, inclua uma condição para o campo `originType`. Este campo especifica como o Macie encontrou os dados confidenciais que produziram uma descoberta, uma descoberta automatizada de dados confidenciais ou um trabalho de descoberta de dados confidenciais. O valor desse campo é `AUTOMATED_SENSITIVE_DATA_DISCOVERY` se uma descoberta foi produzida durante a realização da descoberta automatizada.

Para identificar e analisar as descobertas usando o AWS Command Line Interface (AWS CLI), execute o comando list-findings ou get-finding-statistics. Os exemplos a seguir usam o comando list-findings para recuperar IDs de descoberta para todas as descobertas de alta gravidade produzidas pela descoberta automatizada de dados confidenciais na Região da AWS atual.

Para Linux, macOS ou Unix, usando o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Para Microsoft Windows, usando o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

Em que:

- `classificationDetails.originType` especifica o nome JSON do campo Tipo de origem e:
  - `eq` especifica o operador igual.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY` é um valor enumerado para o campo.
- *`severity.description`* especifica o nome JSON do campo Severidade, e:
  - *`eq`* especifica o operador igual.
  - *`High`* é um valor enumerado para o campo.

Se o comando for executado com sucesso, o Macie retornará uma matriz `findingIds`. A matriz lista o identificador exclusivo de cada descoberta que corresponde aos critérios de filtro, conforme mostrado no exemplo a seguir.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Se nenhuma descoberta corresponder aos critérios de filtro, o Macie retornará uma matriz `findingIds` vazia.

```
{
    "findingIds": []
}
```

Acessando resultados de descoberta de dados confidenciais produzidos pela descoberta automatizada

O Amazon Macie cria um registro de análise para cada objeto do Amazon Simple Storage Service (Amazon S3) que ele seleciona para análise enquanto realiza descobertas automatizadas de dados confidenciais para sua conta ou organização. Esses registros, chamados de resultados confidenciais da descoberta de dados, registram detalhes sobre a análise que o Macie realiza em objetos individuais do S3. Isso inclui objetos nos quais o Macie não detecta dados confidenciais e,

portanto, não produz descobertas, e objetos que o Macie não consegue analisar devido a erros ou problemas como configurações de permissões ou uso de um arquivo ou formato de armazenamento não compatível.

Se o Macie detectar dados confidenciais em um objeto do S3, o resultado da descoberta de dados confidenciais incluirá dados da descoberta correspondente. Ele também fornece informações adicionais, como a localização de até mil ocorrências de cada tipo de dado confidencial que Macie encontrou no objeto. Por exemplo: .

- O número da coluna e da linha de uma célula ou campo em uma pasta de trabalho do Microsoft Excel, arquivo CSV ou arquivo TSV
- O caminho para um campo ou matriz em um arquivo JSON ou JSON Lines
- O número da linha de uma linha em um arquivo de texto não binário que não seja um arquivo CSV, JSON, JSON Lines ou TSV; por exemplo, um arquivo HTML, TXT ou XML
- O número da página de uma página em um arquivo Adobe Portable Document Format (PDF)
- O índice do registro e o caminho para um campo em um registro em um contêiner de objetos Apache Avro ou arquivo Apache Parquet

Se o objeto do S3 afetado for um arquivo de arquivamento, como um arquivo.tar ou .zip, o resultado da descoberta de dados confidenciais também fornecerá dados de localização detalhados para ocorrências de dados confidenciais em arquivos individuais que o Macie extrai do arquivamento. O Macie não inclui essas informações nas descobertas de dados confidenciais para arquivos arquivados. Para relatar dados de localização, os resultados confidenciais da descoberta de dados usam um esquema JSON padronizado.

Um resultado de descoberta de dados confidenciais não inclui os dados confidenciais que o Macie encontrou. Em vez disso, ele fornece um registro de análise que pode ser útil para auditorias ou investigações de privacidade e proteção de dados.

O Macie armazena seus resultados confidenciais de descoberta de dados por 90 dias. Você não pode acessá-los diretamente no console do Amazon Macie ou com a API do Amazon Macie. Em vez disso, você configura o Macie para criptografar e armazená-los em um bucket do S3. O bucket pode servir como um repositório definitivo e de longo prazo para todos os seus resultados confidenciais de descoberta de dados. Em seguida, você pode, se preferir, acessar e consultar os resultados nesse repositório.

Para determinar onde esse repositório está para sua conta, escolha Resultados da descoberta no painel de navegação no console do Amazon Macie. Para fazer isso programaticamente, use a

GetClassificationExportConfigurationoperação da API Amazon Macie. Se você não configurou esse repositório para sua conta, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais para saber como.

Depois de configurar o Macie para armazenar seus resultados confidenciais de descoberta de dados em um bucket do S3, o Macie grava os resultados em arquivos JSON Lines (.jsonl), criptografa e adiciona esses arquivos ao bucket como arquivos GNU Zip (.gz). Para a descoberta automatizada de dados confidenciais, o Macie adiciona os arquivos a uma pasta nomeada automated-sensitive-data-discoveryno bucket.

Como é o caso das descobertas de dados confidenciais, os resultados da descoberta de dados confidenciais seguem um esquema padronizado. Isso pode ajudá-lo opcionalmente a consultá-los, monitorá-los e processá-los usando outros aplicativos, serviços e sistemas.

> **Tip**
>
> Para obter um exemplo detalhado e instrutivo de como você pode consultar e usar resultados de descoberta de dados confidenciais para analisar e relatar possíveis riscos de segurança de dados, consulte a postagem do blog Como consultar e visualizar os resultados da descoberta de dados confidenciais do Macie com o Amazon Athena e a Amazon QuickSight no blog de segurança.AWS
> Para ver exemplos de consultas do Athena que você pode usar para analisar resultados de descobertas de dados confidenciais, visite o repositório Amazon Macie Results Analytics em. GitHub Esse repositório também fornece instruções para configurar o Athena para recuperar e descriptografar seus resultados e scripts para criar tabelas para os resultados.

Pontuação de confidencialidade para buckets do S3

Se a descoberta automática de dados confidenciais estiver habilitada para sua conta, o Amazon Macie calcula e atribui automaticamente uma pontuação de confidencialidade a cada bucket do Amazon Simple Storage Service (Amazon S3) que ele monitora e analisa para sua conta. Uma pontuação de confidencialidade é uma representação quantitativa da quantidade de dados confidenciais que um bucket do S3 pode conter. Com base nessa pontuação, Macie também atribui uma etiqueta de confidencialidade a cada bucket. Um rótulo de confidencialidade é uma representação qualitativa da pontuação de confidencialidade de um bucket. Esses valores podem servir como pontos de referência para determinar onde os dados confidenciais podem residir no seu

conjunto de dados do Amazon S3 e identificar e monitorar possíveis riscos de segurança para esses dados.

Por padrão, a pontuação e o rótulo de confidencialidade de um bucket do S3 refletem os resultados das atividades automatizadas de descoberta de dados confidenciais que o Macie realizou até agora para o bucket. Eles não refletem os resultados dos trabalhos confidenciais de descoberta de dados que você criou e executou. Além disso, nem a pontuação nem o rótulo implicam ou indicam a criticidade ou a importância que um bucket ou os objetos de um bucket podem ter para sua organização. No entanto, você pode substituir a pontuação calculada de um bucket atribuindo manualmente a pontuação máxima (100) ao bucket, que também atribui o rótulo Confidencial ao bucket.

Tópicos

Dimensões e intervalos de pontuação de confidencialidade

Se calculada pelo Amazon Macie, a pontuação de confidencialidade de um bucket do S3 é uma medida quantitativa da interseção de duas dimensões principais:

- A quantidade de dados confidenciais que Macie encontrou no bucket. Isso deriva principalmente da natureza e do número de tipos de dados confidenciais que o Macie encontrou no bucket e do número de ocorrências de cada tipo.
- A quantidade de dados que o Macie analisou no bucket. Isso deriva principalmente do número de objetos exclusivos que Macie analisou no bucket em relação ao número total de objetos exclusivos no bucket.

A pontuação de confidencialidade de um bucket do S3 também determina qual rótulo de confidencialidade Macie atribui ao bucket. O rótulo de confidencialidade é uma representação qualitativa da pontuação; por exemplo, Confidencial ou Não confidencial. No console do Amazon Macie, a pontuação de confidencialidade de um bucket também determina qual cor o Macie usa para representar o bucket nas visualizações de dados, conforme mostrado na imagem a seguir.

As pontuações de confidencialidade variam de -1 a 100, conforme descrito na tabela a seguir. Para avaliar as entradas da pontuação de um bucket do S3, você pode consultar estatísticas confidenciais de descoberta de dados e outros detalhes que o Macie fornece sobre o bucket.

Pontuação de confidencialidade	Rótulo de confidencialidade	Informações adicionais
-1	Erro de classificação	O Macie ainda não analisou nenhum dos objetos do bucket devido a erros de classificação no nível do objeto; problemas com configurações de permissões no nível do objeto, conteúdo do objeto ou cotas. Quando Macie tentou analisar um ou mais objetos no bucket, ocorreram erros. Por exemplo, um objeto é um arquivo malformado ou um objeto está criptografado com uma chave que o Macie não pode acessar ou não tem permissão para usar. Os dados de cobertura do bucket podem ajudá-lo a investigar e corrigir os erros. Para obter mais informações, consulte Como avaliar a cobertura da descobert

Pontuação de confidenc ialidade	Rótulo de confidencialidade	Informações adicionais
		a automatizada de dados confidenciais. Macie continuará tentando analisar objetos no bucket. Se o Macie analisar um objeto com sucesso, o Macie atualizará a pontuação de confidencialidade e o rótulo do bucket para refletir os resultados da análise.

Pontuação de confidenc ialidade	Rótulo de confidencialidade	Informações adicionais
1-49	Não sigilosos	Nesse intervalo, uma pontuação mais alta, como 49, indica que o Macie analisou relativamente poucos objetos no bucket. Uma pontuação mais baixa, como 1, indica que Macie analisou muitos objetos no bucket (em relação ao número total de objetos no bucket) e detectou relativam ente poucos tipos e ocorrênci as de dados confidenciais nesses objetos. Uma pontuação de 1 também pode indicar que o bucket não contém nenhum objeto ou que todos os objetos no bucket contêm zero (0) bytes de dados. As estatísticas do objeto nos detalhes do bucket podem ajudá-lo a determinar se esse é o caso. Para obter mais informações, consulte Analisando detalhes do bucket do S3.

Pontuação de confidenc ialidade	Rótulo de confidencialidade	Informações adicionais
50	Ainda não analisado	Macie ainda não tentou analisar nem analisar nenhum dos objetos do bucket. Macie atribui automaticamente essa pontuação a um bucket quando você habilita inicialme nte a descoberta automática para sua conta ou quando um bucket é adicionado ao seu inventário de bucket. Uma pontuação de 50 também pode indicar que as configurações de permissõe s do bucket impedem que o Macie acesse o bucket ou os objetos do bucket. Isso geralmente ocorre devido a uma política de bucket restritiva. Os detalhes do bucket podem ajudá-lo a determinar se esse é o caso, pois o Macie pode fornecer somente um subconjunto de informações sobre o bucket. Para obter informações sobre como resolver esse problema, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Pontuação de confidenc ialidade	Rótulo de confidencialidade	Informações adicionais
51 a 99	Sigilosos	Nesse intervalo, uma pontuação mais baixa, como 99, indica que Macie analisou muitos objetos no bucket (em relação ao número total de objetos no bucket) e detectou relativamente poucos tipos e ocorrências de dados confidenciais nesses objetos. Uma pontuação mais baixa, como 51, indica que Macie analisou um número moderado de objetos no bucket (em relação ao número total de objetos no bucket) e detectou relativamente poucos tipos e ocorrências de dados confidenciais nesses objetos.
100	Sigilosos	A pontuação foi atribuída manualmente ao bucket, substituindo a pontuação calculada. Macie não atribui essa pontuação aos buckets.

Pontuações de confidencialidade de monitoramento

Quando você habilita inicialmente a descoberta automática de dados confidenciais para sua conta, o Amazon Macie atribui automaticamente uma pontuação de confidencialidade de 50 a cada bucket do S3. Macie também atribui essa pontuação a um bucket quando o bucket é adicionado ao seu inventário de bucket. Com base nessa pontuação, a etiqueta de confidencialidade de cada bucket ainda não foi analisada. A exceção é um bucket vazio, que é um bucket que não contém nenhum objeto ou todos os objetos no bucket contêm zero (0) bytes de dados. Se esse for o caso

de um bucket, Macie atribui uma pontuação de 1 ao bucket, e o rótulo de confidencialidade do compartimento será Não confidencial.

À medida que a descoberta automatizada de dados confidenciais progride em sua conta a cada dia, o Macie atualiza as pontuações e rótulos de confidencialidade de seus buckets do S3 para refletir os resultados da análise. Por exemplo:

- Se o Macie não encontrar dados confidenciais em um objeto, o Macie diminui a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se o Macie encontrar dados confidenciais em um objeto, o Macie aumentará a pontuação de confidencialidade do bucket e atualizará o rótulo de confidencialidade do bucket conforme necessário.
- Se o Macie encontrar dados confidenciais em um objeto que é alterado posteriormente, o Macie remove as detecções de dados confidenciais do objeto da pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se o Macie encontrar dados confidenciais em um objeto que é excluído posteriormente, o Macie remove as detecções de dados confidenciais do objeto da pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se um objeto for adicionado a um bucket que estava vazio anteriormente e o Macie encontrar dados confidenciais no objeto, o Macie aumenta a pontuação de confidencialidade do bucket e atualiza o rótulo de confidencialidade do bucket conforme necessário.
- Se as configurações de permissões de um bucket impedirem o Macie de recuperar informações ou acessar o bucket ou os objetos do bucket, o Macie alterará a pontuação de confidencialidade do bucket para 50 e alterará o rótulo de confidencialidade do bucket para Ainda não analisados.

Dependendo da quantidade de dados que você armazena no Amazon S3, os resultados da análise podem começar a aparecer dentro de 48 horas após a ativação da descoberta automática de dados confidenciais em sua conta.

Você pode ajustar as configurações de pontuação de confidencialidade da sua conta, o que altera as configurações para análises subsequentes de todos os seus buckets do S3. Você também pode ajustar as configurações de buckets S3 individuais. Para configurações no nível da conta, você pode começar a incluir ou excluir listas de permissões específicas, identificadores de dados personalizados ou identificadores de dados gerenciados das análises. Você também pode excluir

buckets específicos das análises. Para obter mais informações, consulte Configurando a descoberta automatizada para sua conta.

Para ajustar as configurações de pontuação de um determinado bucket, você pode incluir ou excluir tipos específicos de dados confidenciais da pontuação do bucket. Também é possível especificar se deseja atribuir uma pontuação calculada automaticamente para o bucket. Para obter mais informações, consulte Gerenciando a descoberta automatizada para buckets do S3 individuais.

Configurações padrão para descoberta automatizada de dados confidenciais

Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta, o Amazon Macie selecionará e analisará automaticamente objetos de amostra de todos os buckets do Amazon Simple Storage Service (Amazon S3) que ele monitora e analisa para sua conta. Se você for o administrador do Macie de uma organização, isso inclui buckets do S3 que suas contas de membro possuem. Para refinar o escopo das análises, você pode excluir buckets específicos da descoberta automatizada de dados confidenciais. Você pode fazer isso de duas maneiras: alterando as configurações automatizadas de descoberta de dados confidenciais da sua conta e alterando as configurações de descoberta automatizada de dados confidenciais para buckets individuais.

Por padrão, o Macie analisa objetos do S3 usando somente o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. O Macie não usa nenhum identificador de dados personalizado nem lista de permissões que você tenha definido. Para personalizar as análises, você pode configurar o Macie para usar identificadores de dados gerenciados específicos, identificadores de dados personalizados e listas de permissões. Você pode fazer isso alterando as configurações automatizadas de descoberta de dados confidenciais da sua conta.

Tópicos

- Identificadores de dados gerenciados padrão para descoberta automatizada de dados confidenciais
- Atualizações nas configurações padrão para descoberta automatizada de dados confidenciais

Identificadores de dados gerenciados padrão para descoberta automatizada de dados confidenciais

Por padrão, o Amazon Macie analisa objetos do S3 usando somente o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. Esse conjunto padrão de identificadores de dados gerenciados foi projetado para detectar categorias e tipos comuns de dados confidenciais. Com base em nossa pesquisa, ele pode detectar categorias gerais e tipos de dados confidenciais e, ao mesmo tempo, otimizar seus resultados de descoberta automatizada ao reduzir o ruído.

O conjunto padrão é dinâmico. À medida que lançamos novos identificadores de dados gerenciados, os adicionamos ao conjunto padrão, caso seja provável que otimizem ainda mais seus resultados automatizados de descoberta de dados confidenciais. Com o tempo, também podemos adicionar ou remover identificadores de dados gerenciados existentes do conjunto. A remoção de um identificador de dados gerenciados não afeta as estatísticas e os detalhes de descoberta de dados confidenciais existentes para seus buckets do S3. Por exemplo, se removermos o identificador de dados gerenciados de um tipo de dado confidencial que o Macie detectou anteriormente em um bucket, o Macie continuará relatando essas detecções para o bucket. Se adicionarmos ou removermos um identificador de dados gerenciados do conjunto padrão, atualizaremos esta página para indicar a natureza e o momento da alteração. Para receber alertas automáticos sobre alterações realizadas nesta página, inscreva-se no feed RSS na página Histórico de documentos do Macie.

Os tópicos a seguir listam os identificadores de dados gerenciados que estão atualmente no conjunto padrão, organizados por categoria e tipo de dados sigilosos. Eles especificam o identificador exclusivo (ID) para cada identificador de dados gerenciados no conjunto. Esse ID descreve o tipo de dados sigilosos que um identificador de dados gerenciados foi projetado para detectar, por exemplo: `PGP_PRIVATE_KEY` para chaves privadas PGP e `USA_PASSPORT_NUMBER` para números de passaportes dos EUA. Se você alterar as configurações automatizadas de descoberta de dados confidenciais da sua conta, poderá usar essa ID para excluir explicitamente um identificador de dados gerenciados das análises subsequentes.

Tópicos

Para obter detalhes sobre identificadores de dados gerenciados específicos ou uma lista completa de todos os identificadores de dados gerenciados que o Macie fornece atualmente, consulte. Usar identificadores de dados gerenciados

Credenciais

Para detectar ocorrências de dados de credenciais em objetos do S3, o Macie usa os seguintes identificadores de dados gerenciados por padrão.

Tipo de dados sigilosos	ID do identificador de dados gerenciados
Chave de acesso secreta da AWS	`AWS_CREDENTIALS`
Cabeçalho de autorização básica de HTTP	`HTTP_BASIC_AUTH_HEADER`
Chave privada OpenSSH	`OPENSSH_PRIVATE_KEY`
Chave privada PGP	`PGP_PRIVATE_KEY`
Chave privada do padrão de criptografia de chave pública (Public Key Cryptography Standard - PKCS)	`PKCS`
Chave privada PuTTY	`PUTTY_PRIVATE_KEY`

Informações financeiras

Para detectar ocorrências de informações financeiras em objetos do S3, o Macie usa os seguintes identificadores de dados gerenciados por padrão.

Tipo de dados sigilosos	ID do identificador de dados gerenciados
Dados da faixa magnética do cartão de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Números de cartão de crédito	`CREDIT_CARD_NUMBER` (para números de cartão de crédito próximos a uma palavra-chave)

Informações de identificação pessoal (PII)

Para detectar ocorrências de informações de identificação pessoal (PII) em objetos do S3, o Macie usa os seguintes identificadores de dados gerenciados por padrão.

Tipo de dados sigilosos	ID do identificador de dados gerenciados
Número de identificação da carteira de habilitação	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (para os EUA), `UK_DRIVERS_LICENSE`
Número de registro eleitoral	`UK_ELECTORAL_ROLL_NUMBER`
Número de identificação nacional	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Número do Seguro Nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Número de passaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Número do Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número da Previdência Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`
Identificação do contribuinte ou número de referência	`AUSTRALIA_TAX_FILE_NUMBER`, `BRAZIL_CPF_NUMBER`, `FRANCE_TAX_IDENTIFICATION_NUMBER`, `GERMANY_TAX_IDENTIFICATION_NUMBER`, `SPAIN_NIE_NUMBER`, `SPAIN_NIF_NUMBER`, `SPAIN_TAX`

Tipo de dados sigilosos	ID do identificador de dados gerenciados
	`_IDENTIFICATION_NUMBER`, `USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Atualizações nas configurações padrão para descoberta automatizada de dados confidenciais

A tabela a seguir descreve as alterações das configurações que o Amazon Macie usa por padrão para a descoberta automatizada de dados confidenciais. Para receber alertas automáticos sobre alterações realizadas nesta página, inscreva-se no feed RSS na página Histórico de documentos do Macie.

Alteração	Descrição	Data
Implementou um novo conjunto dinâmico de identificadores de dados gerenciados padrão	As novas configurações automatizadas de descoberta de dados confidenciais agora são baseadas em um conjunto padrão dinâmico de identificadores de dados gerenciados. Se você ativar a descoberta automatizada de dados confidenciais pela primeira vez nessa data ou após essa data, sua configuração será baseada no conjunto dinâmico. Se você ativou a descoberta automatizada de dados confidenciais pela primeira vez antes dessa data, sua configuração é baseada em um conjunto diferente de identificadores de dados	2 de agosto de 2023

Alteração	Descrição	Data
	gerenciados. Consulte as notas depois dessa tabela para mais informações.	
Disponibilidade geral	Lançamento inicial da descoberta automatizada de dados confidenciais.	28 de novembro de 2022

Se você ativou inicialmente a descoberta automatizada de dados confidenciais em sua conta antes de 2 de agosto de 2023, sua configuração não se baseia no conjunto dinâmico de identificadores de dados gerenciados padrão. Em vez disso, sua configuração é baseada em um conjunto estático de identificadores de dados gerenciados que definimos para a versão inicial da descoberta automatizada de dados confidenciais, conforme listado na tabela abaixo.

Para determinar quando você habilitou inicialmente a descoberta automatizada de dados confidenciais para a conta, escolha Descoberta automatizada no painel de navegação do console do Amazon Macie e, em seguida, consulte a data de ativação na seção Status. Para fazer isso programaticamente, use a operação GetAutomatedDiscoveryConfiguration da API Amazon Macie e consulte o valor do campo `firstEnabledAt`. Se a data for anterior a 2 de agosto de 2023 e você quiser começar a usar o conjunto dinâmico de identificadores de dados gerenciados padrão, entre em contato AWS Support para obter ajuda.

A tabela a seguir lista todos os identificadores de dados gerenciados que estão no conjunto estático. A tabela é classificada primeiro por categoria de dados confidenciais e depois por tipo de dados sigilosos. Para obter detalhes sobre identificadores específicos de dados gerenciados, consulteUsar identificadores de dados gerenciados.

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Credenciais	Chave de acesso secreta da AWS	`AWS_CREDENTIALS`
Credenciais	Cabeçalho de autorização básica de HTTP	`HTTP_BASIC_AUTH_HEADER`

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Credenciais	Chave privada OpenSSH	`OPENSSH_PRIVATE_KEY`
Credenciais	Chave privada PGP	`PGP_PRIVATE_KEY`
Credenciais	Chave privada do padrão de criptografia de chave pública (Public Key Cryptography Standard - PKCS)	`PKCS`
Credenciais	Chave privada PuTTY	`PUTTY_PRIVATE_KEY`
Informações financeiras	Número de conta bancária	`BANK_ACCOUNT_NUMBER` (para números de contas bancárias do Canadá e dos EUA), `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Informações financeiras	Data de validade do cartão de crédito	`CREDIT_CARD_EXPIRATION`
Informações financeiras	Dados da faixa magnética do cartão de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Informações financeiras	Números de cartão de crédito	`CREDIT_CARD_NUMBER` (para números de cartão de crédito próximos a uma palavra-chave)

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Informações financeiras	Código de verificação do cartão de crédito	`CREDIT_CARD_SECURITY_CODE`
Informações pessoais: informações de saúde pessoal (Personal health information - PHI)	Número de registro da Agência Antidrogas (Drug Enforcement Agency - DEA)	`US_DRUG_ENFORCEMENT_AGENCY_NUMBER`
Informações pessoais: PHI	Health Insurance Claim Number (HICN)	`USA_HEALTH_INSURANCE_CLAIM_NUMBER`
Informações pessoais: PHI	Número de identificação médica ou do seguro de saúde	`CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER`
Informações pessoais: PHI	Código do Healthcare Common Procedure Coding System (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Informações pessoais: PHI	National Drug Code (NDC)	`USA_NATIONAL_DRUG_CODE`
Informações pessoais: PHI	National Provider Identifier (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Informações pessoais: PHI	Identificador exclusivo de dispositivo (UDI)	`MEDICAL_DEVICE_UDI`

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Informações pessoais: informações de identificação pessoal (PII)	Datas de nascimento	`DATE_OF_BIRTH`

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Informações pessoais: PII	Número de identificação da carteira de habilitação	`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 os EUA), `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`,

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
		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
Informações pessoais: PII	Número de registro eleitoral	UK_ELECTORAL_ROLL_NUMBER
Informações pessoais: PII	Nome completo	NAME
Informações pessoais: PII	Coordenadas do sistema de posicionamento global (GPS)	LATITUDE_LONGITUDE
Informações pessoais: PII	Endereço postal	ADDRESS, BRAZIL_CEP_CODE
Informações pessoais: PII	Número de identificação nacional	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Informações pessoais: PII	Número do Seguro Nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Informações pessoais: PII	Número de passaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Informações pessoais: PII	Número de residência permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Informações pessoais: PII	Número de telefone	`BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (para o Canadá e os EUA), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Informações pessoais: PII	Número do Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Informações pessoais: PII	Número da Previdência Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Categoria de dados confidenciais	Tipo de dados sigilosos	ID do identificador de dados gerenciados
Informações pessoais: PII	Identificação do contribuinte ou número de referência	`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`
Informações pessoais: PII	Número de identificação de veículo (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Executando trabalhos de descoberta de dados confidenciais no Amazon Macie

Com o Amazon Macie, é possível criar e executar trabalhos de descoberta de dados confidenciais para automatizar a descoberta, o registro e a emissão de relatórios de dados confidenciais nos buckets do Amazon Simple Storage Service (Amazon S3). Um trabalho de descoberta de dados confidenciais, é uma série de tarefas automatizadas de processamento e análise que o Macie executa para detectar e relatar dados confidenciais em objetos do S3. Cada trabalho fornece relatórios detalhados dos dados confidenciais que o Macie encontra e da análise que o Macie realiza. Ao criar e executar trabalhos, você pode criar e manter uma visão abrangente dos dados armazenados pela organização no Amazon S3 e dos riscos de segurança ou conformidade desses dados.

Para ajudá-lo a atender e manter a conformidade com seus requisitos de segurança e privacidade de dados, o Macie oferece várias opções para agendar e definir o escopo de um trabalho. Você pode configurar um trabalho para ser executado somente uma vez para análise e avaliação sob demanda, ou de forma recorrente para análise, avaliação e monitoramento periódicos. Você também define a amplitude e a profundidade da análise de um trabalho — buckets do S3 específicos que você seleciona ou buckets que correspondem a critérios específicos. Opcionalmente, você pode refinar o escopo dessa análise escolhendo opções adicionais. As opções incluem critérios personalizados que derivam das propriedades dos objetos do S3, como tags, prefixos e quando um objeto foi modificado pela última vez.

Para cada trabalho, você também especifica os tipos de dados confidenciais para que o Macie detecte e relate. Você pode configurar um trabalho para usar identificadores de dados gerenciados fornecidos pelo Macie, identificadores de dados personalizados que você define ou uma combinação dos dois. Ao selecionar identificadores de dados gerenciados e personalizados específicos para um trabalho, você pode adaptar a análise para se concentrar em tipos específicos de dados confidenciais. Para ajustar a análise, você também pode configurar um trabalho para usar listas de permissões definidas por você. As listas de permissões especificam texto e padrões de texto que você deseja que o Macie ignore, geralmente exceções de dados confidenciais para cenários ou ambientes específicos de sua organização.

Cada trabalho produz registros dos dados confidenciais que o Macie descobre e da análise que ele realiza — descobertas de dados confidenciais e resultados das descobertas de dados confidenciais Uma descoberta de dados confidenciais é um relatório detalhado de dados confidenciais que o Macie descobriu em um objeto do S3. Um resultado de descoberta de dados confidenciais é um registro de detalhes sobre a análise de um objeto do S3. O Macie cria um resultado de descoberta de dados confidenciais para cada objeto que você configurar para que o trabalho analise. Isso inclui objetos nos quais o Macie não encontra dados confidenciais e, portanto, não produz descobertas de dados confidenciais, e objetos que o Macie não pode analisar devido a erros ou problemas. Cada tipo de registro segue um esquema padronizado, que pode ajudá-lo a consultar, monitorar e processar os registros para atender aos requisitos de segurança e conformidade.

Tópicos

- Prever e monitorar os custos para a tarefas de descoberta de dados confidenciais
- Identificadores de dados gerenciados recomendados para trabalhos de descoberta de dados sigilosos

Opções de escopo para trabalhos de descoberta de dados confidenciais

Com trabalhos de descoberta de dados confidenciais, você define o escopo dos dados do Amazon Simple Storage Service (Amazon S3) que o Amazon Macie analisa para detectar e relatar dados confidenciais. Para ajudá-lo a fazer isso, o Macie fornece várias opções específicas do trabalho que você pode escolher ao criar e configurar um trabalho.

Opções de escopo

- Buckets do S3
- Inclua objetos S3 existentes
- Profundidade da amostragem
- Critérios de objeto do S3

Buckets do S3

Ao criar um trabalho de descoberta de dados confidenciais, agora você pode especificar quais identificadores de dados gerenciados você deseja que o trabalho use ao analisar objetos do S3. Você pode fazer isso de duas maneiras: selecionando buckets do S3 específicos do seu inventário de buckets ou especificando critérios personalizados que derivam das propriedades dos buckets do S3.

Selecione buckets específicos

> Selecionar buckets específicos — Com essa opção, você seleciona explicitamente cada bucket do S3 que deseja que o trabalho analise. Então, quando o trabalho é executado, ele analisa objetos somente nos buckets que você selecionou. Se você configurar o trabalho para ser executado diariamente, semanalmente ou mensalmente, o trabalho analisará objetos nesses mesmos buckets sempre que for executado.
>
> Essa configuração é útil nos casos em que você prefere realizar uma análise direcionada de um conjunto específico de dados. Ele oferece um controle preciso e previsível sobre quais buckets um trabalho analisa.

Especificar critérios de bucket

Com essa opção, você define critérios de runtime que determinam quais buckets do S3 o trabalho analisa. Os critérios consistem em uma ou mais condições derivadas das propriedades do bucket, como configurações de acesso público e tags. Quando o trabalho é executado, ele identifica os buckets que correspondem aos seus critérios e, em seguida, analisa os objetos nesses buckets. Se você configurar o trabalho para ser executado periodicamente, o trabalho fará isso toda vez que for executado. Consequentemente, o trabalho pode analisar objetos em diferentes buckets cada vez que é executado, dependendo das alterações no inventário do bucket e dos critérios definidos por você.

Essa configuração é útil nos casos em que você deseja que o escopo da análise do trabalho se adapte dinamicamente às mudanças no inventário do bucket. Se você configurar um trabalho para usar critérios de bucket e ser executado periodicamente, o trabalho identificará automaticamente novos buckets que correspondam aos critérios e inspeciona esses buckets em busca de dados confidenciais.

Os tópicos desta seção fornecem detalhes adicionais sobre cada opção.

Tópicos

Selecionando buckets do Amazon S3

Se você optar por selecionar explicitamente cada bucket do S3 que deseja que um trabalho analise, o Macie fornece um inventário completo de seus buckets na Região da AWS atual. Em seguida, você pode revisar seu inventário e selecionar os buckets desejados. Para saber como o Macie gera e mantém esse inventário para você, consulte Como o Macie monitora a segurança de dados do Amazon S3.

Se você for o administrador do Macie de uma organização, o inventário inclui buckets que pertencem à contas-membro da sua organização. Você pode selecionar até mil desses buckets, abrangendo até mil contas.

Para ajudar a fazer suas seleções de bucket, o inventário fornece detalhes e estatísticas para cada bucket. Isso inclui a quantidade de dados que um trabalho pode analisar em cada bucket — objetos classificáveis são objetos que usam uma classe de armazenamento compatível com o Amazon S3 e

têm uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. O inventário também indica se algum trabalho existente está configurado para analisar objetos em um bucket. Esses detalhes podem ajudá-lo a estimar a amplitude de um trabalho e refinar suas seleções de bucket.

Na tabela de inventário:

- Sensibilidade — indica a pontuação de sensibilidade atual de um bucket, se a descoberta automática de dados confidenciais estiver ativada para sua conta.
- Objetos classificáveis – indica o número total de objetos que o trabalho pode analisar em um bucket.
- Tamanho classificável – indica o tamanho total de armazenamento de todos os objetos que o trabalho pode analisar em um bucket.

  Se o bucket contiver objetos compactados, esse valor não reflete o tamanho real desses objetos depois que eles forem descompactados. Se o controle de versão estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto no bucket.
- Monitorado por trabalho — indica se algum trabalho existente está configurado para analisar periodicamente objetos em um bucket diariamente, semanalmente ou mensalmente.

  Se o valor desse campo for Sim, o bucket será incluído explicitamente em um trabalho periódico ou corresponderá aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.
- Última execução do trabalho — se os trabalhos periódicos ou únicos existentes estiverem configurados para analisar objetos em um bucket, esse campo indicará a data e a hora mais recentes em que um desses trabalhos começou a ser executado. Caso contrário, esse campo estará vazio.

Se o ícone de informações
()
aparecer ao lado do nome de qualquer bucket na tabela, recomendamos que você recupere os metadados mais recentes do bucket do Amazon S3. Para fazer isso, selecione atualizar
()
acima da tabela. O ícone de informações indica que um bucket foi criado nas últimas 24 horas, possivelmente após a última vez que o Macie recuperou os metadados do bucket e do objeto

do Amazon S3 como parte do ciclo diário de atualização. Para obter mais informações, consulte Atualizações de dados.

Se o ícone de aviso
(⚠)
for exibido ao lado do nome de um bucket, o Macie não poderá acessar o bucket. O Macie só pode fornecer um subconjunto de informações sobre o bucket, como o nome do bucket. Isso significa que o trabalho não poderá analisar objetos no bucket. Para investigar o problema, revise as configurações de políticas e permissões do bucket no Amazon S3. Por exemplo, o bucket pode ter uma política restritiva de bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Para personalizar sua visualização do inventário e encontrar buckets específicos com mais facilidade, você pode filtrar a tabela inserindo critérios de filtro na caixa de filtro. A tabela a seguir oferece alguns exemplos.

Para mostrar todos os buckets que…	Aplique este filtro…
São propriedade de uma conta específica	ID da conta = *o ID de 12 dígitos da conta*
São acessíveis ao público	Permissão efetiva = Pública
Não estão incluídos em nenhum trabalho periódico	Monitorado ativamente por trabalho = Falso
Não estão incluídos em nenhum trabalho periódico	Definido no trabalho = Falso
Têm uma chave de tag especifica*	Chave de tag = *a tag da chave*
Têm um valor de tag específico*	Valor da tag = *o valor da tag*
Contenham objetos não criptografados (ou usem criptografia do lado do cliente)	Contagem de objetos por criptografia é Sem criptografia e De = 1

As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Você precisa especificar um valor completo e válido para o campo. Você não pode especificar valores parciais nem usar caracteres curinga nos valores.

Para exibir os detalhes de um bucket, selecione o bucket e consulte o painel de detalhes. Nessa página, você também pode:

- Dinamizar e fazer uma busca detalhada em determinados campos escolhendo uma lupa para o campo. Seleciona

  para mostrar buckets com o mesmo valor ou selecione

  para mostrar buckets com outros valores.
- Recupere os metadados mais recentes dos objetos no bucket. Isso pode ser útil se você criou um bucket recentemente ou fez alterações significativas nos objetos do bucket nas últimas 24 horas. Para recuperar os dados, selecione atualizar () na seção Estatísticas do objeto do painel. Essa opção está disponível para buckets que contêm trinta mil objetos ou menos.

Especificando critérios de bucket do S3

Se você optar por especificar critérios de bucket para um trabalho, o Macie fornece opções para definir e testar os critérios. Esses são critérios de runtime que determinam quais buckets do S3 contêm objetos para serem analisados pelo trabalho. Sempre que o trabalho é executado, ele identifica os buckets que correspondem aos seus critérios e, em seguida, analisa os objetos nos buckets apropriados. Se você for o administrador do Macie de uma organização, isso inclui buckets que pertencem a contas-membro em sua organização.

Definindo critérios de bucket

Os critérios de bucket consistem em uma ou mais condições que derivam das propriedades dos buckets do S3. Cada condição, também chamada de critério, consiste em três partes:

- Um campo baseado em propriedades, como o ID da conta ou Permissão efetiva.
- Um operador, iguala (`eq`) ou não iguala (`neq`).
- Um ou mais valores.
- Uma instrução de inclusão ou exclusão que indica se você deseja que o trabalho analise (inclua) ou ignore (exclua) buckets que correspondam à condição.

Se você especificar mais de um valor para um campo, o Macie usa a lógica OR para unir os valores. Se você especificar mais de uma condição para os critérios, o Macie usa a lógica AND para unir as condições. Além disso, as condições de exclusão têm precedência sobre as condições de inclusão. Por exemplo, se você incluir buckets acessíveis ao público e excluir buckets com tags específicas, o trabalho analisará os objetos em qualquer bucket que esteja acessível ao público, a menos que o bucket tenha uma das tags especificadas.

Você pode definir condições que derivam de qualquer um dos seguintes campos baseados em propriedades para buckets do S3.

ID da conta

O identificador (ID) exclusivo da Conta da AWS à qual o bucket pertence. Para especificar vários valores para esse campo, insira o ID de cada conta e separe cada entrada com uma vírgula.

Observe que o Macie não é compatível com o uso de caracteres curinga ou valores parciais para esse campo.

Bucket name

O nome de um bucket. Esse campo está correlacionado ao campo Nome, não ao campo Nome do recurso da Amazon, no Amazon S3. Para especificar vários valores para esse campo, insira o nome de cada bucket e separe cada entrada com uma vírgula.

Observe que os valores diferenciam entre maiúsculas e minúsculas. Além disso, o Macie não é compatível com o uso de caracteres curinga ou valores parciais para esse campo.

Permissões efetivas

Especifica se um bucket é publicamente acessível. Você pode escolher um ou mais dos seguintes valores para esse campo:

- Não público — o público em geral não tem acesso de leitura ou gravação ao bucket.
- Público — o público em geral tem acesso de leitura ou gravação ao bucket.
- Desconhecido — o Macie não conseguiu avaliar as configurações de acesso público do bucket.

Para determinar esse valor para um bucket, o Macie analisa uma combinação de configurações em nível de conta e de bucket para o bucket: as configurações de bloqueio de acesso público da conta; as configurações de bloqueio de acesso público do bucket; a política de bucket do bucket e a lista de controle de acesso (ACL) do bucket.

Acesso compartilhado

Especifica se um bucket é compartilhado com outra Conta da AWS, uma identidade do acesso de origem (OAI) do Amazon CloudFront ou um controle de acesso de origem (OAC) do Amazon CloudFront. Você pode escolher um ou mais dos seguintes valores para esse campo:

- Externo — o bucket é compartilhado com um ou mais dos itens a seguir ou com qualquer combinação deles: um OAI do CloudFront, um OAC do CloudFront ou uma conta externa (que não faz parte da) sua organização.
- Interno — o bucket é compartilhado com uma ou mais contas internas à (parte da) sua organização. Ele não é compartilhado com um OAI ou OAC do CloudFront.
- Não compartilhado — o bucket não é compartilhado com outra conta, com um OAI do CloudFront ou com um OAC do CloudFront.
- Desconhecido — o Macie não conseguiu avaliar as configurações de acesso compartilhado do bucket.

Para determinar se um bucket é compartilhado com outra Conta da AWS, o Macie analisa a política do bucket e a ACL do bucket. Além disso, uma organização é definida como um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio do AWS Organizations ou por convite do Macie. Para obter informações sobre as opções de compartilhamento de buckets do Amazon S3, consulte Identity and Access Management no Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Para determinar se um bucket é compartilhado com um OAI ou OAC do CloudFront, o Macie analisa a política de bucket do bucket. Um OAI ou OAC do CloudFront permite que os usuários acessem os objetos de um bucket por meio de uma ou mais distribuições específicas do CloudFront. Para obter informações sobre os OAIs e OACs do CloudFront, consulte Restringindo o acesso ao conteúdo do Amazon S3 no Guia do desenvolvedor do Amazon CloudFront.

Tags

As tags associadas a um bucket. As tags são rótulos que você pode definir e atribuir a determinados tipos de recursos AWS, incluindo os buckets do S3. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Para obter informações sobre a marcação de buckets do S3, consulte Usando tags de buckets do S3 para alocação de custos no Guia do usuário do Amazon Simple Storage Service.

Para um trabalho de descoberta de dados confidenciais, você pode usar esse tipo de condição para incluir ou excluir buckets que tenham uma chave de tag específica, um valor de tag específico ou uma chave e um valor de tag específicos (como um par). Por exemplo:

- Se você especificar **`Project`** como uma chave de tag e não especificar nenhum valor de tag para uma condição, qualquer bucket que tenha a chave de tag Project corresponderá aos critérios da condição, independentemente dos valores de tag associados a essa chave de tag.
- Se você especificar **`Development`** e **`Test`** como valores de tag e não especificar nenhuma chave de tag para uma condição, qualquer bucket que tenha o valor de tag **`Development`** ou **`Test`** corresponderá aos critérios da condição, independentemente das chaves de tag associadas a esses valores de tag.

Para especificar várias chaves de tag em uma condição, insira cada chave de tag no campo Chave e separe cada entrada com uma vírgula. Para especificar vários valores de tag em uma condição, insira cada valor de tag no campo Valor e separe cada entrada com uma vírgula.

Observe que as chaves e os valores de tags diferenciam maiúsculas de minúsculas. Além disso, o Macie não é compatível com o uso de caracteres curinga ou valores parciais em condições de tag.

Critérios de teste do bucket

Ao definir os critérios do bucket, você pode testar e refinar os critérios pré-visualizando os resultados. Para fazer isso, expanda a seção Pré-visualize os resultados dos critérios que é exibida abaixo dos critérios no console. Essa seção exibe uma tabela com todos os buckets que atualmente correspondem aos critérios.

A tabela também fornece informações sobre a quantidade de dados que o trabalho pode analisar em cada bucket — objetos classificáveis são objetos que usam uma classe de armazenamento compatível com o Amazon S3 e têm uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível. O inventário também indica se algum trabalho existente está configurado para analisar objetos em um bucket.

Na tabela:

- Sensibilidade — indica a pontuação de sensibilidade atual de um bucket, se a descoberta automática de dados confidenciais estiver ativada para sua conta.
- Objetos classificáveis – indica o número total de objetos que o trabalho pode analisar em um bucket.
- Tamanho classificável – indica o tamanho total de armazenamento de todos os objetos que o trabalho pode analisar em um bucket.

Se o bucket contiver objetos compactados, esse valor não reflete o tamanho real desses objetos depois que eles forem descompactados. Se o controle de versão estiver habilitado para um bucket, esse valor será baseado no tamanho de armazenamento da versão mais recente de cada objeto no bucket.

- Monitorado por trabalho — indica se algum trabalho existente está configurado para analisar periodicamente objetos em um bucket diariamente, semanalmente ou mensalmente.

  Se o valor desse campo for Sim, o bucket será incluído explicitamente em um trabalho periódico ou corresponderá aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.

Se o ícone de aviso
(⚠)
for exibido ao lado do nome do bucket, o Macie não poderá acessar o bucket ou os objetos do bucket. O Macie só pode fornecer um subconjunto de informações sobre o bucket, como o nome do bucket. Isso significa que o trabalho não poderá analisar objetos no bucket. Para investigar o problema, revise as configurações de políticas e permissões do bucket no Amazon S3. Por exemplo, o bucket pode ter uma política restritiva de bucket. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Para refinar os critérios do bucket para o trabalho, use as opções de filtro para adicionar, alterar ou remover condições dos critérios. Em seguida, o Macie atualiza a tabela para refletir suas alterações.

Inclua objetos S3 existentes

Você pode usar trabalhos de descoberta de dados confidenciais para realizar análises contínuas e incrementais de objetos nos buckets do S3. Se você configurar um trabalho para ser executado periodicamente, o Macie fará isso automaticamente — cada execução analisa apenas os objetos criados ou alterados após a execução anterior. Com a opção Incluir objetos existentes, você escolhe o ponto de partida para o primeiro incremento:

- Para analisar todos os objetos existentes imediatamente após a criação do trabalho, marque a caixa de seleção para essa opção.
- Para esperar e analisar apenas os objetos criados ou alterados após a criação do trabalho e antes da primeira execução, desmarque a caixa de seleção dessa opção.

Desmarcar essa caixa de seleção é útil nos casos em que você já analisou os dados e deseja continuar a analisá-los periodicamente. Por exemplo, se já usou outro serviço ou aplicativo para classificar dados e recentemente começou a usar o Macie, você pode usar essa opção para garantir a descoberta e a classificação contínuas de seus dados sem incorrer em custos desnecessários ou duplicar os dados de classificação.

Cada execução subsequente de um trabalho periódico analisa automaticamente apenas os objetos criados ou alterados após a execução anterior.

Para trabalhos periódicos e únicos, você também pode configurar um trabalho para analisar apenas os objetos criados ou alterados antes ou depois de um determinado período ou durante um determinado intervalo de tempo. Para fazer isso, adicione critérios de objeto que usem a data da última modificação dos objetos.

Profundidade da amostragem

Com essa opção, você especifica a porcentagem de objetos elegíveis do S3 que você deseja que o Macie analise quando um trabalho de descoberta de dados confidenciais é executado. Objetos elegíveis são objetos que: usam uma classe de armazenamento compatível com o Amazon S3, têm uma extensão de nome de arquivo para um arquivo ou formato de armazenamento compatível e correspondem a outros critérios que você especifica para o trabalho.

Se esse valor for menor que 100%, o Macie selecionará os objetos elegíveis a serem analisados aleatoriamente, até a porcentagem especificada, e analisará todos os dados nesses objetos. Por exemplo, se você configurar um trabalho para analisar 10.000 objetos e especificar uma profundidade de amostragem de 20%, o trabalho analisará aproximadamente 2.000 objetos elegíveis, selecionados aleatoriamente.

Reduzindo a profundidade da amostragem de um trabalho pode reduzir os custos e a duração de um trabalho. É útil nos casos em que os dados nos objetos são altamente consistentes e você deseja determinar se um bucket do S3, em vez de cada objeto, contém dados confidenciais.

Observe que essa opção controla a porcentagem de objetos que são analisados, não a porcentagem de bytes que são analisados. Se você inserir uma profundidade de amostragem menor que 100%, o Macie analisará todos os dados em cada objeto selecionado, não a porcentagem dos dados em cada objeto selecionado.

Critérios de objeto do S3

Para ajustar o escopo de um trabalho de descoberta de dados confidenciais, você também pode definir critérios personalizados que determinam quais objetos do S3 o Macie inclui ou exclui da análise de um trabalho. Os critérios de bucket consistem em uma ou mais condições que derivam das propriedades dos buckets do S3. As condições se aplicam aos objetos em todos os buckets do S3 que um trabalho está configurado para analisar. Se um bucket contiver várias versões de um objeto, as condições se aplicarão à versão mais recente do objeto.

Se você definir várias condições como critérios do objeto, o Macie usa a lógica AND para unir as condições. Além disso, as condições de exclusão têm precedência sobre as condições de inclusão. Por exemplo, se você incluir objetos com a extensão de nome de arquivo .pdf e excluir objetos maiores que 5 MB, o trabalho analisará qualquer objeto que tenha a extensão de nome de arquivo .pdf, a menos que o objeto seja maior que 5 MB.

Você pode definir condições que derivam de qualquer um dos seguintes campos baseados em propriedades para buckets do S3.

Extensões do nome do arquivo

Isso se correlaciona com a extensão do nome do arquivo de um objeto do Amazon S3. Você pode usar esse tipo de condição para incluir ou excluir objetos com base no tipo de arquivo. Para fazer isso para vários tipos de arquivos, insira a extensão de nome de arquivo para cada tipo e separe cada entrada com uma vírgula, como, por exemplo: **`docx,pdf,xlsx`**. Se você inserir várias extensões de nome de arquivo como valores para uma condição, o Macie usa a lógica OR para unir os valores.

Observe que os valores diferenciam entre maiúsculas e minúsculas. Além disso, o Macie não é compatível com o uso de valores parciais ou caracteres curinga nesse tipo de condição.

Para obter informações sobre os tipos de arquivo que o Macie pode analisar, consulte Formatos de arquivo e armazenamento suportados.

Última modificação

Isso se correlaciona com o campo Última modificação do Amazon S3. No Amazon S3, esse campo armazena a data e a hora em que um objeto do S3 foi criado ou alterado pela última vez, o que for mais recente.

Para um trabalho de descoberta de dados confidenciais, essa condição pode ser uma data específica, uma data e uma hora específicas ou um intervalo de tempo exclusivo:

- Para analisar objetos que foram modificados pela última vez após uma determinada data ou data e hora, insira os valores nos campos De.
- Para analisar objetos que foram modificados pela última vez antes de uma determinada data ou data e hora, insira os valores nos campos Até.
- Para analisar objetos que foram modificados pela última vez durante um determinado intervalo de tempo, use os campos De para inserir os valores da primeira data ou data e hora no intervalo de tempo. Use os campos Até para inserir os valores da última data ou data e hora no intervalo de tempo.
- Para analisar objetos que foram modificados pela última vez a qualquer momento durante um determinado dia, insira a data no campo de data De. Insira a data do dia seguinte no campo de data Até. Em seguida, verifique se os dois campos de hora estão em branco. (Macie trata um campo de tempo em branco como `00:00:00`.) Por exemplo, para analisar objetos que foram alterados em 9 de agosto de 2022, insira **`2022/08/09`** no campo de data De, insira **`2022/08/10`** no campo da data Até e não insira um valor em nenhum dos campos de hora.

Insira qualquer valor de tempo no Tempo Universal Coordenado (UTC) e use a notação de 24 horas.

Prefixo

Isso se correlaciona com o campo Chave do Amazon S3. No Amazon S3, esse campo armazena o nome de um objeto do S3, incluindo o prefixo do objeto. Um prefixo é semelhante a um caminho de diretório dentro de um bucket. Ele permite agrupar objetos semelhantes em um bucket, da mesma forma que você pode armazenar arquivos semelhantes em uma pasta em um sistema de arquivos. Para obter informações sobre prefixos de objeto e pastas no Amazon S3, consulte Organizando objetos no console do Amazon S3 usando pastas no Guia do usuário do Amazon Simple Storage Service.

Você pode usar esse tipo de condição para incluir ou excluir objetos cujas chaves (nomes) comecem com um determinado valor. Por exemplo, para excluir todos os objetos cuja chave começa com AWSLogs, insira **`AWSLogs`** como valor para uma condição de Prefixo e, em seguida, selecione Excluir.

Se você inserir vários prefixos como valores para uma condição, o Macie usa a lógica OR para unir os valores. Por exemplo, se você inserir **`AWSLogs1`** e **`AWSLogs2`** como valores para uma condição, qualquer objeto cuja chave comece com AWSLogs1 ou AWSLogs2 corresponderá aos critérios da condição.

Ao inserir um valor para uma condição de Prefixo, lembre-se do seguinte:

- Os valores diferenciam maiúsculas de minúsculas.
- O Macie não é compatível com o uso de caracteres curinga nesses valores.
- No Amazon S3, a chave de um objeto não inclui o nome do bucket que contém o objeto. Por esse motivo, não especifique nomes de buckets nesses valores.
- Se um prefixo incluir um delimitador, inclua o delimitador no valor. Por exemplo, insira **`AWSLogs/eventlogs`** para definir uma condição para todos os objetos cuja chave comece com AWSLogs/EventLogs. O Macie é compatível com o delimitador padrão do Amazon S3, que é uma barra (/), e delimitadores personalizados.

Observe, também, que um objeto corresponde aos critérios de uma condição somente se a chave do objeto corresponder exatamente ao valor inserido, começando com o primeiro caractere na chave do objeto. Além disso, o Macie aplica uma condição ao valor completo da chave de um objeto, incluindo o nome do arquivo do objeto.

Por exemplo, se a chave de um objeto for AWSLogs/eventlogs/testlog.csv e você inserir qualquer um dos seguintes valores para uma condição, o objeto corresponderá aos critérios da condição:

- **`AWSLogs`**
- **`AWSLogs/event`**
- **`AWSLogs/eventlogs/`**
- **`AWSLogs/eventlogs/testlog`**
- **`AWSLogs/eventlogs/testlog.csv`**

No entanto, se você inserir **`eventlogs`**, o objeto não corresponderá aos critérios — o valor da condição não inclui a primeira parte da chave, AWSLogs/. Da mesma forma, se você inserir **`awslogs`**, o objeto não corresponderá aos critérios devido às diferenças de maiúsculas e minúsculas.

Tamanho de armazenamento

Isso se correlaciona com o campo Tamanho do Amazon S3. No Amazon S3, esse campo indica o tamanho total de armazenamento de um objeto do S3. Se um objeto for um arquivo compactado, esse valor não refletirá o tamanho real do arquivo depois que o arquivo for descompactado.

Você pode usar esse tipo de condição para incluir ou excluir objetos menores que um determinado tamanho, maiores que um determinado tamanho ou que estejam dentro de uma determinada faixa de tamanho. O Macie aplica esse tipo de condição a todos os tipos de objetos, incluindo arquivos compactados ou arquivados e os arquivos que eles contêm. Para obter

informações sobre restrições baseadas em tamanho para cada formato compatível, consulte Cotas do Amazon Macie.

Tags

As tags associadas a um bucket. As tags são rótulos que você pode definir e atribuir a determinados tipos de recursos AWS, incluindo os buckets do S3. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. Para obter informações sobre a marcação de objetos do S3, consulte Categorizando o armazenamento usando tags no Guia do usuário do Amazon Simple Storage Service.

Para um trabalho de descoberta de dados confidenciais, você pode usar esse tipo de condição para incluir ou excluir objetos que tenham uma tag específica. Isso pode ser uma chave de tag específica ou uma chave e valor de tag específicos (como um par). Se você inserir vários prefixos como valores para uma condição, o Macie usa a lógica OR para unir os valores. Por exemplo, se você especificar **`Project1`** e **`Project2`** como chaves de tag para uma condição, qualquer objeto que tenha a chave de tag Project1 ou Project2 corresponderá aos critérios da condição.

Observe que as chaves e os valores de tags diferenciam maiúsculas de minúsculas. Além disso, o Macie não é compatível com o uso de valores parciais ou caracteres curinga nesse tipo de condição.

Criar um trabalho de descoberta de dados confidenciais

Com o Amazon Macie, é possível criar e executar trabalhos de descoberta de dados confidenciais para automatizar a descoberta, o registro e a emissão de relatórios de dados confidenciais nos buckets do Amazon Simple Storage Service (Amazon S3). Um trabalho de descoberta de dados confidenciais é uma série de tarefas automatizadas de processamento e análise que o Macie executa para detectar e relatar dados confidenciais em objetos do Amazon S3. À medida que a análise avança, o Macie fornece relatórios detalhados dos dados confidenciais encontrados e da análise que realiza: descobertas de dados confidenciais, que relatam dados confidenciais que Macie encontra em objetos individuais do S3, e resultados confidenciais da descoberta de dados, que registram detalhes sobre a análise de objetos individuais do S3. Para obter mais informações, consulte Analisando estatísticas e resultados de um trabalho.

Ao criar um trabalho, você começa especificando quais buckets do S3 contêm objetos que você deseja que o Macie analise quando o trabalho é executado — buckets específicos que você seleciona ou buckets que correspondem a critérios específicos. Em seguida, você especifica com que frequência executar o trabalho — uma vez ou periodicamente, diariamente, semanalmente ou

mensalmente. Você também pode escolher opções para refinar o escopo da análise do trabalho. As opções incluem critérios personalizados que derivam das propriedades dos objetos do S3, como tags, prefixos e quando um objeto foi modificado pela última vez.

Depois de definir o cronograma e o escopo do trabalho, você especifica quais identificadores de dados gerenciados e identificadores de dados personalizados você deseja que o trabalho use:

- Um identificador de dados personalizado é um conjunto de critérios e técnicas integrados projetados para detectar um tipo específico de dados confidenciais – por exemplo, números de cartão de crédito, chaves de acesso secretas AWS ou números de passaporte de um determinado país ou região. Esses identificadores podem detectar uma lista grande e crescente de tipos de dados confidenciais para muitos países e regiões, incluindo vários tipos de dados de credenciais, informações financeiras e informações de identificação pessoal (PII). Para obter mais informações, consulte Usar identificadores de dados gerenciados.
- O identificador de dados personalizado é um conjunto de critérios que você define para detectar dados confidenciais. Com identificadores de dados personalizados, você pode detectar dados confidenciais que refletem determinados cenários, propriedade intelectual ou dados proprietários de sua organização — por exemplo, IDs de funcionários, números de conta de cliente ou classificações de dados internas. Você pode complementar os identificadores de dados gerenciados fornecidos pelo Macie. Para obter mais informações, consulte Criar identificadores de dados personalizados.

Em seguida, opcionalmente, você seleciona as listas de permissões que deseja que o trabalho use. Uma lista de permissões especifica um texto ou um padrão de texto que você deseja que o Macie ignore, geralmente exceções de dados confidenciais para seus cenários ou ambientes específicos — por exemplo, nomes públicos ou números de telefone da sua organização ou dados de amostra que sua organização usa para testes. Para obter mais informações, consulte Como definir exceções de dados sigilosos com listas de permissões.

Ao terminar de escolher essas opções, você estará pronto para inserir as configurações gerais do trabalho, como o nome e a descrição do trabalho. Em seguida, você poderá revisar e salvar o trabalho.

Tarefas

- Antes de começar
- Etapa 1: escolher buckets do S3
- Etapa 2: revisar as seleções ou critérios de bucket do S3

- Etapa 3: Definir o cronograma e refinar o escopo
- Etapa 4: selecionar identificadores de dados gerenciados
- Etapa 4: selecionar identificadores de dados gerenciados
- Etapa 6: selecionar listas de permissões
- Etapa 7: inserir configurações gerais
- Etapa 8: Revisar e criar

Antes de começar

Antes de criar um trabalho, é uma boa ideia seguir as seguintes etapas:

- Verifique se você configurou o Macie para armazenar os resultados de descoberta de dados confidenciais em um bucket do S3. Para fazer isso, escolha Resultados do Discovery no painel de navegação no console do Amazon Macie. Em seguida, verifique se você inseriu as configurações. Para saber mais sobre essas configurações, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.
- Crie os identificadores de dados personalizados que você deseja que o trabalho use. Para saber como, consulte Criar identificadores de dados personalizados.
- Crie todas as listas de permissões que você deseja que o trabalho use. Para saber como, consulte Criação e gerenciamento de listas de permissões.
- Se você quiser analisar objetos do S3 criptografados, certifique-se de que o Macie possa acessar e usar as chaves de criptografia apropriadas. Para obter mais informações, consulte Analisando objetos criptografados do S3.
- Se você quiser analisar objetos em um bucket do S3 que tenha uma política restritiva de bucket, certifique-se de que o Macie tenha permissão para acessar os objetos. Para obter mais informações, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Se você fizer essas coisas antes de criar um trabalho, você simplificará a criação do trabalho e ajudar a garantir que o trabalho possa analisar os dados desejados.

Etapa 1: escolher buckets do S3

A primeira etapa na criação de um trabalho é especificar quais buckets do S3 contêm objetos que você deseja que o Macie analise quando o trabalho for executado. Para esta etapa, você tem duas opções:

- Selecionar buckets específicos — Com essa opção, você seleciona explicitamente cada bucket do S3 que deseja que o trabalho analise. Então, quando o trabalho é executado, ele analisa objetos somente nos buckets que você selecionou.
- Especificar critérios de bucket — Com essa opção, você define critérios de runtime que determinam quais buckets do S3 o trabalho analisa. Os critérios consistem em uma ou mais condições derivadas das propriedades do bucket. Em seguida, quando o trabalho é executado, ele identifica os buckets que correspondem aos seus critérios e analisa os objetos nesses buckets.

Para obter informações detalhadas sobre essas opções, consulte Opções de escopo para trabalhos.

As seções a seguir fornecem instruções para escolher e configurar cada opção. Escolha a seção da opção desejada.

Selecionar buckets específicos

Se você optar por selecionar explicitamente cada bucket do S3 que deseja que o trabalho analise, o Macie fornece um inventário completo de seus buckets no Região da AWS atual. Em seguida, você pode usar esse inventário para selecionar um ou mais buckets para análise do trabalho. Para saber mais sobre esse inventário, consulte Selecionando buckets do Amazon S3.

Se você for o administrador do Macie de uma organização, o inventário incluirá buckets que são de propriedade de contas-membro em sua organização. Você pode configurar o trabalho para analisar objetos em até 1.000 desses buckets, abrangendo até 1.000 contas.

Para selecionar buckets específicos para o trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Escolha Create job (Criar trabalho).
4. Para a etapa Escolher buckets do S3, escolha Selecionar buckets específicos. O Macie exibe uma tabela de todos os buckets do da sua conta na região atual.
5. Na seção Selecionar buckets do S3, escolha opcionalmente atualizar
   ()
   para recuperar os metadados mais recentes do bucket do Amazon S3.

   Se o ícone de informações
   ()

aparecer ao lado de qualquer nome de bucket, recomendamos que você faça isso. Esse ícone indica que um bucket foi criado nas últimas 24 horas, possivelmente após a última vez que Macie recuperou os metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização.

6. Em seguida, na tabela, marque a caixa de seleção para cada bucket no S3 que você deseja que o trabalho revise.

> **Tip**
>
> - Para encontrar buckets específicos com mais facilidade, insira critérios de filtro na caixa de filtros acima da tabela. Você também pode classificar a tabela escolhendo um título de coluna.
> - Para determinar se você já configurou um trabalho para analisar periodicamente objetos em um bucket, consulte o campo Monitorado por trabalho. Se Sim aparecer em um campo, o bucket será incluído explicitamente em um trabalho periódico ou o bucket correspondeu aos critérios de um trabalho periódico nas últimas 24 horas. Além disso, o status de pelo menos um desses trabalhos não é Cancelado. Macie atualiza esses dados diariamente.
> - Para determinar quando um trabalho existente, periódico ou único, analisou mais recentemente objetos em um bucket, consulte o campo Última execução do trabalho. Para obter informações adicionais sobre esse trabalho, consulte os detalhes do bucket.
> - Para exibir os detalhes de um bucket, escolha o bucket. Além das informações relacionadas ao trabalho, o painel de detalhes fornece estatísticas e outras informações sobre o bucket, como as configurações de acesso público do bucket. Para saber mais sobre estes dados, consulte Analisar seu inventário de buckets do S3.

7. Ao terminar de selecionar os buckets, escolha Avançar.

Na próxima etapa, você revisará e verificar suas seleções.

Especificar critérios de bucket

Se você optar por especificar critérios de runtime que determinem quais buckets do S3 o trabalho analisa, o Macie fornece opções para ajudá-lo a escolher campos, operadores e valores para

condições individuais nos critérios. Para saber mais sobre essas opções, consulte Especificando critérios de bucket do S3.

Para especificar critérios de bucket para o trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Escolha Create job (Criar trabalho).
4. Para a etapa Escolher buckets do S3, escolha Selecionar buckets específicos.
5. Em Especificar critérios do bucket, faça o seguinte para adicionar uma condição aos critérios:

   a. Coloque o cursor na caixa de filtro e escolha a propriedade do bucket a ser usada para a condição.

   b. Na primeira caixa, escolha um operador para a condição, Igual ou Não igual.

   c. Na próxima caixa, insira um ou mais valores para a propriedade.

      Dependendo do tipo e da natureza da propriedade do bucket, o Macie exibe opções diferentes para inserir valores. Por exemplo, se você escolher a propriedade de permissão efetiva, o Macie exibirá uma lista de valores para escolher. Se você escolher a propriedade ID da conta, o Macie exibirá uma caixa de texto na qual você poderá inserir uma ou mais IDs Conta da AWS. Para inserir vários valores em uma caixa de texto, insira cada valor e separe cada entrada com uma vírgula.

   d. Escolha Apply (Aplicar). Macie adiciona a condição e a exibe abaixo da caixa do filtro.

      Por padrão, o Macie adiciona a condição com uma declaração de inclusão. Isso significa que o trabalho está configurado para analisar (incluir) objetos em buckets que correspondam à condição. Para ignorar (excluir) buckets que correspondam à condição, escolha Incluir para a condição e, em seguida, escolha Excluir.

   e. Repita as etapas anteriores para cada condição adicional que você deseja adicionar aos critérios.

6. Para testar seus critérios, expanda a seção Visualizar os resultados dos critérios. Essa seção exibe uma tabela com todos os buckets que atualmente correspondem aos critérios.
7. Para refinar seus critérios, siga um destes procedimentos:

   - Para remover uma condição, selecione X para a condição.

- Para alterar uma condição, remova a condição escolhendo X para a condição. Em seguida, adicione uma condição que tenha as configurações corretas.
- Para remover todas as condições, escolha Limpar filtros.

Macie atualiza a tabela de resultados dos critérios para refletir suas alterações.

8. Ao terminar de especificar os critérios do bucket, escolha Avançar.

Na próxima etapa, você revisará e verificar suas seleções.

Etapa 2: revisar as seleções ou critérios de bucket do S3

Nesta etapa, verifique se você escolheu as configurações corretas na etapa anterior:

- Revise suas seleções de buckets - Se você selecionou buckets S3 específicos para o trabalho, revise a tabela de buckets e altere suas seleções de buckets conforme necessário. A tabela fornece informações sobre o escopo projetado e o custo da análise do trabalho. Os dados são baseados no tamanho e nos tipos de objetos atualmente armazenados em um bucket.

  Na tabela, o campo Custo estimado indica o custo total estimado (em USD) da análise de objetos em um bucket do S3. Cada estimativa reflete a quantidade projetada de dados não compactados que o trabalho analisará em um bucket. Se algum objeto for compactado ou arquivado, a estimativa pressupõe que os arquivos usem uma taxa de compactação de 3:1 e que a tarefa possa analisar todos os arquivos extraídos. Para obter mais informações, consulte Previsão e monitoramento dos custos do trabalho.
- Revise seus critérios de bucket - Se você especificou critérios de bucket para o trabalho, revise cada condição nos critérios. Para alterar os critérios, escolha Anterior e use as opções de filtro na etapa anterior para inserir os critérios corretos. Ao terminar, escolha Avançar.

Ao terminar de revisar e verificar as configurações do trabalho, escolha Avançar.

Etapa 3: Definir o cronograma e refinar o escopo

Em seguida, você especifica com que frequência deseja executar o trabalho — uma vez ou periodicamente, diariamente, semanalmente ou mensalmente. Você também pode escolher opções para refinar o escopo da análise do trabalho. Para saber mais sobre estas opções, consulte Opções de escopo para trabalhos.

Etapa 3: Definir o cronograma e refinar o escopo

1. Na página Refinar o escopo, especifique com que frequência você deseja que o trabalho seja executado:

   - Para executar o trabalho somente uma vez, imediatamente após terminar de criá-lo, escolha Trabalho único.
   - Para executar o trabalho periodicamente de forma recorrente, escolha Trabalho agendado. Em Atualizar frequência, escolha se deseja executar o trabalho diariamente, semanalmente ou mensalmente. Em seguida, use a opção Incluir objetos existentes para definir o escopo da primeira execução do trabalho:
     - Marque esta caixa de seleção para analisar todos os objetos existentes imediatamente após terminar de criar o trabalho. Cada execução subsequente analisa apenas os objetos criados ou alterados após a execução anterior.
     - Desmarque esta caixa de seleção para ignorar a análise de todos os objetos existentes. A primeira execução do trabalho analisa apenas os objetos que são criados ou alterados após a conclusão da criação do trabalho e antes do início da primeira execução. Cada execução subsequente analisa apenas os objetos criados ou alterados após a execução anterior.

       Desmarcar essa caixa de seleção é útil nos casos em que você já analisou os dados e deseja continuar a analisá-los periodicamente. Por exemplo, se já usou outro serviço ou aplicativo para classificar dados e recentemente começou a usar o Macie, você pode usar essa opção para garantir a descoberta e a classificação contínuas de seus dados sem incorrer em custos desnecessários ou duplicar os dados de classificação.
2. (Opcional) Para especificar a porcentagem de objetos que você deseja que a tarefa analise, insira a porcentagem na caixa Profundidade de amostragem.

   Se esse valor for menor que 100%, o Macie selecionará os objetos a serem analisados aleatoriamente, até a porcentagem especificada, e analisará todos os dados nesses objetos. O valor padrão é 100%.
3. (Opcional) Para adicionar critérios específicos que determinem quais objetos do S3 são incluídos ou excluídos da análise do trabalho, expanda a seção Configurações adicionais e insira os critérios. Esses critérios consistem em condições individuais que são derivados de propriedades de objetos:

   - Para analisar (incluir) objetos que atendam a uma condição específica, insira o tipo e o valor da condição e escolha Incluir.

- Para ignorar (excluir) objetos que atendam a uma condição específica, insira o tipo e o valor da condição e escolha Excluir.

Repita essa etapa para cada condição de inclusão ou exclusão desejada.

Se você inserir várias condições, todas as condições de exclusão terão precedência sobre as condições de inclusão. Por exemplo, se você incluir objetos com a extensão de nome de arquivo .pdf e excluir objetos maiores que 5 MB, o trabalho analisará qualquer objeto que tenha a extensão de nome de arquivo .pdf, a menos que o objeto seja maior que 5 MB.

4. Ao terminar, escolha Avançar.

Etapa 4: selecionar identificadores de dados gerenciados

Nesta etapa, especifique quais identificadores de dados gerenciados você deseja que o trabalho use ao analisar objetos do S3. Você tem duas opções:

- Use as configurações recomendadas - Com essa opção, o trabalho analisa objetos do S3 usando o conjunto de identificadores de dados gerenciados que recomendamos para trabalhos. Esse conjunto foi projetado para detectar categorias e tipos comuns de dados confidenciais. Para revisar uma lista de identificadores de dados gerenciados que estão atualmente no conjunto, consulte Identificadores de dados gerenciados recomendados para trabalhos. Atualizamos essa lista sempre que adicionamos ou removemos um identificador de dados gerenciados do conjunto.
- Use as configurações recomendadas - Com essa opção, o trabalho analisa objetos do S3 usando o conjunto de identificadores de dados gerenciados que recomendamos para trabalhos. Isso pode ser todos ou apenas alguns dos identificadores de dados gerenciados que estão disponíveis atualmente. Você também pode configurar o trabalho para não usar nenhum identificador de dados gerenciados. Em vez disso, o trabalho pode usar somente identificadores de dados personalizados que você selecionar na próxima etapa. Para revisar uma lista de identificadores de dados gerenciados que estão atualmente no conjunto, consulte Referência rápida: identificadores de dados gerenciados pelo Amazon Macie. Atualizamos essa lista sempre que adicionamos ou removemos um identificador de dados gerenciados do conjunto.

Quando você escolhe qualquer uma das opções, o Macie exibe uma tabela de identificadores de dados gerenciados. Na tabela, o campo Tipo de dados confidenciais especifica o identificador exclusivo (ID) de um identificador de dados gerenciados. Essa ID descreve o tipo de dados confidenciais que o identificador de dados gerenciados foi projetado para detectar, por exemplo:

USA_PASSPORT_NUMBER para números de passaporte dos EUA, CREDIT_CARD_NUMBER para números de cartão de crédito e PGP_PRIVATE_KEY para chaves privadas PGP. Para encontrar identificadores específicos mais rapidamente, você pode classificar e filtrar a tabela por categoria ou tipo de dados confidenciais.

Para selecionar identificadores de dados gerenciados para o trabalho

1. Na página Selecionar identificadores de dados gerenciados, em Opções de identificador de dados gerenciados, faça o seguinte:

   - Para usar o conjunto de identificadores de dados gerenciados que recomendamos para trabalhos, escolha Recomendado.

     Se você escolher essa opção e configurar o trabalho para ser executado mais de uma vez, cada execução usará automaticamente todos os identificadores de dados gerenciados que estão no conjunto recomendado quando a execução é iniciada. Isso inclui novos identificadores de dados gerenciados que lançamos e adicionamos ao conjunto. Ela exclui identificadores de dados gerenciados que removemos do conjunto e que não são mais recomendados para trabalhos.
   - Para usar somente identificadores de dados gerenciados específicos que você selecionar, escolha Personalizado e, em seguida, escolha Usar identificadores de dados gerenciados específicos. Em seguida, na tabela, marque a caixa de seleção para cada bucket no S3 que você deseja que o trabalho revise.

     Se você escolher essa opção e configurar o trabalho para ser executado mais de uma vez, cada execução usará somente os identificadores de dados gerenciados que selecionar. Em outras palavras, a tarefa usa esses mesmos identificadores de dados gerenciados sempre que é executada.
   - Para usar todos os identificadores de dados gerenciados atualmente oferecidos por Macie, escolha Personalizado e, em seguida, escolha Usar identificadores de dados gerenciados específicos. Em seguida, na tabela, marque a caixa de seleção no título da coluna de seleção para selecionar todas as linhas.

     Se você escolher essa opção e configurar o trabalho para ser executado mais de uma vez, cada execução usará somente os identificadores de dados gerenciados que selecionar. Em outras palavras, a tarefa usa esses mesmos identificadores de dados gerenciados sempre que é executada.

- Para não usar nenhum identificador de dados gerenciados e usar somente identificadores de dados personalizados, escolha Personalizado e, em seguida, escolha Não usar nenhum identificador de dados gerenciados. Em seguida, na próxima etapa, selecione os identificadores de dados personalizados a serem usados.

2. Ao terminar, escolha Avançar.

Etapa 4: selecionar identificadores de dados gerenciados

Para esta etapa, selecione quaisquer identificadores de dados personalizados que você deseja que o trabalho use ao analisar objetos do S3. A tarefa usará os identificadores selecionados além de quaisquer identificadores de dados gerenciados que você configurou para usar na tarefa. Para saber mais sobre identificadores de dados personalizados, consulte Criar identificadores de dados personalizados.

Para selecionar identificadores de dados gerenciados para o trabalho

1. Na página Selecionar identificadores de dados personalizados, marque a caixa de seleção para cada identificador de dados personalizado que você deseja que o trabalho use. Você pode selecionar até 30 identificadores de dados personalizados.

> **Tip**
>
> Para revisar ou testar as configurações de um identificador de dados personalizado antes de selecioná-lo, escolha o ícone do link () próximo ao nome do identificador. O Macie abrirá uma página que exibe as configurações do identificador.
> Você também pode usar essa página para testar o identificador com dados de amostra. Para fazer isso, insira até mil caracteres de texto na caixa Dados da amostra e selecione Teste. O Macie avalia os dados da amostra usando o identificador e, em seguida, relata o número de correspondências.

2. Ao terminar de selecionar identificadores de dados personalizados, escolha Avançar.

Etapa 6: selecionar listas de permissões

Para esta etapa, selecione quaisquer identificadores de dados personalizados que você deseja que o trabalho use ao analisar objetos do S3. Para saber mais sobre listas de permissões, consulte Como definir exceções de dados sigilosos com listas de permissões.

Para selecionar listas de permissões para o trabalho

1. Na página Selecionar listas de permissões, marque a caixa de seleção para cada lista de permissões que você deseja que o trabalho use. Você pode selecionar até 10 listas.

   > **Tip**
   >
   > Para revisar as configurações de uma lista de permissões antes de selecioná-la, escolha o ícone de link ( ) ao lado do nome da lista. O Macie abrirá uma página que exibe as configurações da lista.
   >
   > Se a lista especificar uma expressão regular (regex), você também poderá usar essa página para testar a regex com dados de amostra. Para fazer isso, insira até mil caracteres de texto na caixa Dados da amostra e selecione Teste. Macie avalia os dados da amostra usando o regex e, em seguida, relata o número de correspondências.

2. Ao terminar de selecionar os listas, escolha Avançar.

Etapa 7: inserir configurações gerais

Para essa etapa, especifique um nome e, opcionalmente, uma descrição do trabalho.

Você também pode atribuir tags ao trabalho. Uma tag é um rótulo que você define e atribui a determinados tipos de atributos AWS. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional. As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.

Para inserir as configurações gerais do trabalho

1. Na página Inserir configurações gerais, insira um nome para o trabalho na caixa Nome do trabalho. Um nome pode conter até 500 caracteres.

2. (Opcional) Em Descrição do trabalho, insira uma breve descrição da tarefa. A descrição pode conter até 200 caracteres.
3. (Opcional) Em Tags, escolha Adicionar tag e, em seguida, insira até 50 tags para atribuir ao trabalho.
4. Ao terminar, escolha Avançar.

Etapa 8: Revisar e criar

Para esta etapa final, revise as definições de configuração do trabalho e verifique se elas estão corretas. Esta é uma etapa importante. Depois de criar um trabalho, você não poderá alterar nenhuma dessas configurações. Isso ajuda a garantir que você tenha um histórico imutável de descobertas de dados sigilosos e resultados de descoberta para auditorias de privacidade de dados e proteção de dados ou investigações que você realiza.

Dependendo das configurações do trabalho, você também pode revisar o custo total estimado (em dólares americanos) para executar o trabalho uma vez. Se você selecionou buckets S3 específicos para o trabalho, a estimativa é baseada no tamanho e nos tipos de objetos nos compartimentos selecionados e na quantidade desses dados que o trabalho pode analisar. Se você selecionou buckets S3 específicos para o trabalho, a estimativa é baseada no tamanho e nos tipos de objetos em até 500 buckets que correspondam atualmente aos critérios e na quantidade desses dados que o trabalho pode analisar. Para saber mais sobre essa estimativa, consulte Previsão e monitoramento dos custos do trabalho.

Revisar e criar a tarefa

1. Na página Revisar e criar, revise cada configuração e verifique se está correta. Para alterar uma configuração, escolha Editar na seção que contém a configuração e insira a configuração correta. Você também pode usar as guias de navegação para acessar a página que contém uma configuração.
2. Ao concluir a verificação das configurações, escolha Enviar para criar e salvar o trabalho. Macie verifica as configurações e notifica você sobre quaisquer problemas a serem resolvidos.

> **Note**
>
> Se você não configurou um repositório para os resultados confidenciais da descoberta de dados, o Macie exibe um aviso e não salva o trabalho. Para resolver esse problema, escolha Configurar na seção Repositório para

resultados de descoberta de dados confidenciais. Em seguida, insira as configurações do repositório. Para saber como, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais. Depois de inserir as configurações, retorne à página Revisar e criar e escolha atualizar () na seção Repositório para resultados de descoberta de dados confidenciais da página. Não é recomendável, mas você pode substituir temporariamente o requisito de repositório e salvar o trabalho. Se você fizer isso, corre o risco de perder os resultados da descoberta do trabalho — Macie reterá os resultados por apenas 90 dias. Para substituir temporariamente o requisito, marque a caixa de seleção da opção de substituição.

3. Se o Macie notificar você sobre problemas a serem resolvidos, resolva os problemas e escolha Enviar novamente para criar e salvar o trabalho.

Se você configurou o trabalho para ser executado uma vez, diariamente ou no dia da semana ou do mês atual, o Macie começará a executar o trabalho imediatamente após salvá-lo. Caso contrário, Macie se preparará para executar a tarefa no dia da semana ou do mês especificado. Para monitorar o trabalho, você pode verificar o status do trabalho.

Analisando estatísticas e resultados de descobertas de dados confidenciais

Quando você executa um trabalho de descoberta de dados confidenciais, o Amazon Macie calcula e relata, automaticamente, determinados dados estatísticos do trabalho. Por exemplo, o Macie relata o número de vezes que o trabalho foi executado e o número aproximado de objetos do Amazon Simple Storage Service (Amazon S3) que o trabalho ainda não processou durante sua execução atual. O Macie também produz vários tipos de resultados para o trabalho: eventos de log, descobertas de dados confidenciais e resultados de descobertas de dados confidenciais.

Tópicos

- Tipos de resultados para trabalhos de descoberta de dados confidenciais
- Analisando estatísticas e resultados das descobertas automatizadas de dados confidenciais

Tipos de resultados para trabalhos de descoberta de dados confidenciais

À medida que um trabalho de descoberta de dados confidenciais progride, o Amazon Macie produz os seguintes tipos de resultados para o trabalho.

Evento de log

Esse é um registro de um evento que ocorreu durante a execução do trabalho. O Macie registra e publica automaticamente os dados de determinados eventos automaticamente no Amazon CloudWatch Logs. Os dados nesses logs fornecem um registro das alterações no progresso ou no status do trabalho, como a data e a hora exatas em que o trabalho começou ou parou de ser executado. Os dados também fornecem detalhes sobre quaisquer erros no nível da conta ou do bucket que ocorreram durante a execução do trabalho.

Os eventos de logs podem ajudá-lo a monitorar um trabalho e resolver todos os problemas que impediram o trabalho de analisar os dados que você deseja. Se um trabalho usa critérios de runtime para determinar quais buckets do S3 analisar, os eventos de log também podem ajudá-lo a determinar se e quais buckets do S3 corresponderam aos critérios quando o trabalho foi executado.

É possível acessar os eventos de log usando o console do Amazon CloudWatch ou a API do Amazon CloudWatch Logs. Para ajudá-lo a navegar até os eventos de log de um trabalho, o console do Amazon Macie fornece um link para eles. Para obter mais informações, consulte Monitorar trabalhos.

Descobrindo dados confidenciais

Esse é um relatório detalhado dos dados confidenciais que o Macie encontrou em um objeto do S3. Cada descoberta fornece uma classificação de gravidade e detalhes como:

- A data e a hora em que Macie encontrou os dados confidenciais.
- A categoria e os tipos de dados confidenciais que Macie encontrou.
- O número de ocorrências de cada tipo de dado confidencial que Macie encontrou.
- O identificador exclusivo do trabalho que produziu a descoberta.
- O nome, as configurações de acesso público, o tipo de criptografia e outras informações sobre o bucket e o objeto do S3 afetados.

Dependendo do tipo de arquivo ou formato de armazenamento do objeto S3 afetado, os detalhes também podem incluir a localização de até 15 ocorrências dos dados confidenciais encontrados

por Macie. Para relatar os dados de localização, a descoberta de dados confidenciais usa um esquema JSON padronizado.

Uma descoberta de dados confidenciais não inclui os dados confidenciais que Macie encontrou. Em vez disso, ele fornece informações que você pode usar para investigação e remediação adicionais, conforme necessário.

O Macie armazena as descobertas de dados confidenciais por 90 dias. Você pode acessá-las usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode monitorá-los e processá-los usando outros aplicativos, serviços e sistemas. Para obter mais informações, consulte Analisando descobertas.

Resultado da descoberta de dados confidenciais

Esse é um registro de detalhes sobre a análise de um objeto do S3. O Macie cria um resultado de descoberta de dados confidenciais automaticamente para para cada objeto que você configurar um trabalho para analisar. Isso inclui objetos nos quais o Macie não encontra dados confidenciais e, portanto, não produz descobertas de dados confidenciais, e objetos que o Macie não pode analisar devido a erros ou problemas, como configuração de permissões ou uso de um formato de arquivo ou armazenamento não compatível.

Se o Macie descobrir dados confidenciais em um objeto do S3, o resultado da descoberta de dados confidenciais incluirá dados da descoberta de dados confidenciais correspondente. Ele também fornece informações adicionais, como a localização de até mil ocorrências de cada tipo de dado confidencial que Macie encontrou no objeto. Por exemplo:

- O número da coluna e da linha de uma célula ou campo em uma pasta de trabalho do Microsoft Excel, arquivo CSV ou arquivo TSV
- O caminho para um campo ou matriz em um arquivo JSON ou JSON Lines
- O número da linha de uma linha em um arquivo de texto não binário que não seja um arquivo CSV, JSON, JSON Lines ou TSV; por exemplo, um arquivo HTML, TXT ou XML
- O número da página de uma página em um arquivo Adobe Portable Document Format (PDF)
- O índice do registro e o caminho para um campo em um registro em um contêiner de objetos Apache Avro ou arquivo Apache Parquet

Se o objeto do S3 afetado for um arquivo de arquivamento, como um arquivo.tar ou .zip, o resultado da descoberta de dados confidenciais também fornecerá dados de localização detalhados para ocorrências de dados confidenciais em arquivos individuais que o Macie extrai do arquivamento. O Macie não inclui essas informações nas descobertas de dados confidenciais

para arquivos arquivados. Para relatar dados de localização, os resultados confidenciais da descoberta de dados usam um esquema JSON padronizado.

O resultado de uma descoberta de dados confidenciais não inclui os dados confidenciais que o Macie encontrou. Em vez disso, ele fornece um registro de análise que pode ser útil para auditorias ou investigações de privacidade e proteção de dados.

O Macie armazena seus resultados confidenciais de descoberta de dados por 90 dias. Você não pode acessá-los diretamente no console do Amazon Macie ou com a API do Amazon Macie. Em vez disso, você configura o Macie para criptografá-los e armazená-los em um bucket do S3. O bucket pode servir como um repositório definitivo e de longo prazo para todos os seus resultados confidenciais de descoberta de dados. Em seguida, você pode, opcionalmente, acessar e consultar os resultados nesse repositório. Para saber mais sobre como definir essas configurações, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Depois de definir as configurações, o Macie grava seus resultados da descoberta de dados confidenciais em arquivos JSON Lines (.jsonl) e criptografa e adiciona esses arquivos ao bucket do S3 como arquivos GNU Zip (.gz). Para ajudá-lo a navegar até os eventos de log de um trabalho, o console do Amazon Macie fornece um link para eles.

Tanto as descobertas de dados confidenciais quanto os resultados de descobertas de dados confidenciais seguem esquemas padronizados. Isso pode ajudá-lo opcionalmente a consultá-los, monitorá-los e processá-los usando outros aplicativos, serviços e sistemas.

> **Tip**
>
> Para obter um exemplo detalhado e instrutivo de como você pode consultar e usar resultados de descoberta de dados confidenciais para analisar e relatar possíveis riscos de segurança de dados, consulte a postagem do blog Como consultar e visualizar os resultados de descoberta de dados confidenciais do Macie com o Amazon Athena e o Amazon QuickSight do Blog de segurança AWS.
> Para exemplos de consultas do Amazon Athena que você pode usar para analisar resultados de descoberta de dados confidenciais, visite o repositório Repositório de análise de resultados do Amazon Macie no GitHub. Esse repositório também fornece instruções para configurar o Athena para recuperar e descriptografar seus resultados e scripts para criar tabelas para os resultados.

Analisando estatísticas e resultados das descobertas automatizadas de dados confidenciais

Para analisar as estatísticas de processamento e os resultados de determinados trabalhos de descoberta de dados confidenciais, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Siga estas etapas para analisar as estatísticas e resultados de um trabalho usando o console.

Para acessar as estatísticas de processamento de um trabalho de forma programática, use a operação DescribeClassificationJob da API do Amazon Macie. Para acesso programático às descobertas que um trabalho produziu, use a operação ListFindings da API do Amazon Macie e especifique o identificador exclusivo do trabalho em uma condição de filtro para o campo `classificationDetails.jobId`. Para saber como, consulte Como criar e aplicar filtros às descobertas. Em seguida, você pode usar a operação GetFindings para recuperar os detalhes dessas descobertas.

Para revisar estatísticas e resultados de um trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Na página Tarefas, selecione o nome do trabalho cujas estatísticas e resultados você deseja revisar. O painel de detalhes exibe estatísticas, configurações e outras informações sobre o trabalho.
4. No painel de detalhes, siga um destes procedimentos:

   - Para revisar as estatísticas de processamento do trabalho, consulte a seção Estatísticas do painel. Essa seção exibe estatísticas, como o número de vezes que a tarefa foi executada e o número aproximado de objetos que a tarefa ainda não processou durante a execução atual.
   - Para revisar os eventos de log do trabalho, selecione Exibir resultados na parte superior do painel e, em seguida, selecione Exibir logs do CloudWatch. O Macie abre o console do Amazon CloudWatch e exibe uma tabela dos eventos de log que o Macie publicou para o trabalho.
   - Para revisar todas as descobertas de dados confidenciais que o trabalho produziu, selecione Mostrar resultados na parte superior do painel e, em seguida, selecione Mostrar descobertas. O Macie abrirá a página Descobertas e exibirá todas as descobertas do trabalho. Para rever os detalhes de uma determinada descoberta, selecione a descoberta e, em seguida, consulte o painel de detalhes.

> **Tip**
>
> No painel de detalhes da descoberta, você pode usar o link no campo Localização detalhada do resultado para navegar até o resultado correspondente da descoberta de dados confidenciais no Amazon S3:
>
> - Se a descoberta se aplicar a um arquivo grande ou a um arquivo compactado, o link exibirá a pasta que contém os resultados da descoberta para o arquivo. Um arquivo compactado ou arquivado é grande se gerar mais de cem resultados de descoberta.
> - Se a descoberta se aplicar a um arquivo pequeno ou a um arquivo compactado, o link exibirá o arquivo que contém os resultados da descoberta do arquivo. Um arquivo compactado ou arquivado é pequeno se gerar cem resultados ou menos de descoberta.
> - Se a descoberta se aplicar a um arquivo pequeno ou a um arquivo compactado, o link exibirá o arquivo que contém os resultados da descoberta do arquivo.

- Para rever todos os resultados da descoberta de dados confidenciais que o trabalho produziu, selecione Mostrar resultados na parte superior do painel e, em seguida, selecione Mostrar classificações. O Macie abrirá o console do Amazon S3 e exibirá a pasta que contém todos os resultados da descoberta para o trabalho. Essa opção só estará disponível depois de configurar o Macie para armazenar os resultados da descoberta de dados confidenciais em um bucket do S3.

Monitorar trabalhos de descoberta de dados sigilosos com o Amazon CloudWatch Logs

Além de monitorar o status geral de um trabalho de descoberta de dados sigilosos, você pode monitorar e analisar eventos específicos que ocorrem à medida que o trabalho progride. Você pode fazer isso usando dados de log quase em tempo real que o Amazon Macie publica automaticamente no Amazon CloudWatch Logs. Os dados nesses logs fornecem um registro das alterações no progresso ou no status de um trabalho, como a data e a hora exatas em que um trabalho começou a ser executado, foi pausado ou terminou a execução.

Os dados de log também fornecem detalhes sobre quaisquer erros no nível da conta ou do bucket que ocorram durante a execução de um trabalho. Por exemplo, se as configurações de permissões de um bucket do S3 impedirem que um trabalho analise objetos no bucket, o Macie registra um

evento. O evento indica quando o erro ocorreu e identifica o bucket afetado e a conta proprietária do bucket. Os dados desses tipos de eventos podem ajudá-lo a identificar, investigar e solucionar erros que impedem o Macie de analisar os dados que você deseja.

Com o Amazon CloudWatch Logs, é possível monitorar, armazenar e acessar os arquivos de log de vários sistemas, aplicativos e Serviços da AWS, incluindo o Macie. Você também pode consultar e analisar dados de log e configurar o CloudWatch Logs para notificá-lo quando determinados eventos ocorrerem ou se os limites forem atingidos. O CloudWatch Logs também fornece atributos para arquivar dados de log e exportar os dados para o Amazon S3. Para obter mais informações sobre o CloudWatch Logs, consulte o Guia do usuário do Amazon CloudWatch Logs.

Tópicos

Como o log funciona para trabalhos de descoberta de dados sigilosos

Quando você começa a executar trabalhos sigilosos de descoberta de dados, o Macie cria e configura automaticamente os recursos apropriados no Amazon CloudWatch Logs para registrar eventos de logs para todos os seus trabalhos Região da AWS atuais. Em seguida, o Macie publica dados de eventos nesses recursos automaticamente quando seus trabalhos são executados. A política de permissões para a função vinculada ao serviço Macie para a sua conta permite que o Macie execute essas tarefas em seu nome. Você não precisa tomar nenhuma medida para criar ou configurar recursos no CloudWatch Logs ou para registrar dados de eventos de logs para seus trabalhos.

No CloudWatch Logs, os logs são organizados em grupos de logs. Cada grupo de logs contém fluxos de logs. Cada fluxo de logs contém eventos de logs. O objetivo geral de cada um desses recursos é o seguinte:

- Um grupo de logs corresponde a uma coleção de fluxos de log que compartilham as mesmas configurações de retenção, monitoramento e controle de acesso, por exemplo, a coleção de logs de todos os trabalhos de descoberta de dados sigilosos.
- Um fluxo de log é uma sequência de eventos de log que compartilham a mesma origem, por exemplo, um trabalho de descoberta de dados sigilosos individual.

- Um evento de log é um registro de uma atividade que foi registrada por um aplicativo ou recurso, por exemplo, um evento individual que o Macie registrou e publicou para um trabalho específico de descoberta de dados sigilosos.

O Macie publica eventos para todos os trabalhos de descoberta de dados sigilosos em um grupo de logs, e cada trabalho tem um fluxo de log exclusivo nesse grupo de logs. O grupo de logs tem o seguinte prefixo e nome:

```
/aws/macie/classificationjobs
```

Se esse grupo de logs já existir, o Macie o usará para armazenar eventos de log para seus trabalhos. Isso pode ser útil se a sua organização usa a configuração automática, como o AWS CloudFormation, para criar grupos de logs com períodos de retenção de log predefinidos, configurações de criptografia, tags, filtros de métrica e assim por diante para eventos de trabalho.

Se esse grupo de logs não existir, o Macie o criará com as configurações padrão que o CloudWatch Logs usa para novos grupos de logs. As configurações incluem um período de retenção de logs de Nunca expirar, o que significa que o CloudWatch Logs armazena os logs indefinidamente. Para alterar o período de retenção do grupo de logs, use o console do Amazon CloudWatch, ou a API do Amazon CloudWatch Logs. Para obter mais informações, consulte Como trabalhar com grupos de logs e fluxos de logs no Guia do usuário do Amazon CloudWatch Logs.

Dentro desse grupo de logs, o Macie cria um fluxo de logs exclusivo para cada trabalho executado, na primeira vez em que o trabalho é executado. O nome do fluxo de logs é o identificador exclusivo do trabalho, como `85a55dc0fa6ed0be5939d0408example`, no formato a seguir.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Cada fluxo de log contém todos os eventos de log que o Macie registrou e publicou para o trabalho correspondente. Para trabalhos periódicos, isso inclui eventos para todas as execuções do trabalho. Se você excluir o fluxo de log de um trabalho periódico, o Macie criará o fluxo novamente na próxima vez em que o trabalho for executado. Se você excluir o fluxo de logs de um trabalho único, não poderá restaurá-lo.

Observe que o log está ativado por padrão para todos os trabalhos. Você não pode desativá-lo ou impedir que o Macie publique eventos de trabalho no CloudWatch Logs. Se você não quiser armazenar os logs, poderá reduzir o período de retenção do grupo de logs para apenas um dia.

Ao final do período de retenção, o CloudWatch Logs exclui automaticamente os dados de eventos expirados do grupo de logs.

Analisar logs para trabalhos de descoberta de dados sigilosos

Você pode revisar os logs dos trabalhos de descoberta de dados sigilosos usando o console do Amazon CloudWatch ou a API do Amazon CloudWatch Logs. Tanto o console, quanto a API, fornecem atributos projetados para ajudar você a revisar e analisar dados de log. Você pode usar esses atributos para trabalhar com fluxos de log e eventos para seus trabalhos da mesma forma que trabalharia com qualquer outro tipo de dados de log no CloudWatch Logs.

Por exemplo, você pode pesquisar e filtrar dados agregados para identificar tipos específicos de eventos que ocorreram em todos os seus trabalhos durante um período específico. Ou você pode realizar uma análise direcionada de todos os eventos que ocorreram em um determinado trabalho. O CloudWatch Logs também fornece opções para monitorar dados de log, definir filtros de métricas e criar alarmes personalizados.

> **Tip**
>
> Para navegar até os eventos de log de um trabalho específico usando o console do Amazon Macie, faça o seguinte: Na página Trabalhos, selecione o nome do trabalho. Na parte superior do painel de detalhes, selecione Mostrar resultados e, em seguida, selecione Mostrar logs do CloudWatch. Macie abre o console do Amazon CloudWatch e exibe uma tabela de eventos de log para o trabalho.

Para revisar os logs de seus trabalhos (console do Amazon CloudWatch)

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a região na qual você executou trabalhos dos quais deseja revisar os logs.
3. No painel de navegação, escolha Logs e, em seguida, escolha Grupos de log.
4. Na página Grupos de logs, selecione o grupo de logs /aws/macie/classificationjobs.. O CloudWatch Logs exibe uma tabela de fluxos de log para os trabalhos que você executou. Há um fluxo exclusivo para cada trabalho. O nome de cada fluxo está correlacionado ao identificador exclusivo de um trabalho.
5. Em Fluxos de logs, siga um destes procedimentos:

- Para revisar os eventos de log de um trabalho específico, selecione o fluxo de log do trabalho. Para encontrar o fluxo com mais facilidade, insira o identificador exclusivo do trabalho na caixa de filtro acima da tabela. Depois de escolher o fluxo de logs, o CloudWatch Logs exibe uma tabela de eventos de log para o trabalho.
- Para revisar os eventos de log de todos os seus trabalhos, selecione Pesquisar todos os fluxos de logs. O CloudWatch Logs exibe uma tabela de eventos de log para todos os seus trabalhos.

6. (Opcional) Na caixa de filtro acima da tabela, insira termos, frases ou valores que especifiquem as características de eventos específicos a serem revisados. Para obter mais informações, consulte Pesquisar dados de log usando padrões de filtro no Guia do usuário do Amazon CloudWatch Logs.
7. Para revisar os detalhes de um evento de log específico, selecione a seta para a direita ( ) na linha do evento. O CloudWatch Logs exibe os detalhes do evento no formato JSON.

Ao se familiarizar com os dados nos eventos de log, você também pode realizar tarefas como criar filtros de métricas que transformam dados de log em métricas numéricas do CloudWatch e criar alarmes personalizados que facilitam a identificação e a resposta a eventos de log específicos. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

Esquema de eventos de log para trabalhos de descoberta de dados sigilosos

Cada evento de log para um trabalho confidencial de descoberta de dados é um objeto JSON que está em conformidade com o esquema de eventos do Amazon CloudWatch Logs e contém um conjunto padrão de campos. Alguns tipos de eventos têm campos adicionais que fornecem informações particularmente úteis para esse tipo de evento. Por exemplo, eventos de erros no nível da conta incluem o ID da conta para a Conta da AWS afetada. Os eventos de erros no nível do bucket incluem o nome do bucket do S3 afetado. Para obter uma lista detalhada dos eventos de trabalho que o Macie publica no CloudWatch Logs, consulte Tipos de eventos de log para trabalhos.

O exemplo a seguir mostra o esquema de eventos de log para trabalhos de descoberta de dados sigilosos. Neste exemplo, o evento relata que Macie não conseguiu analisar nenhum objeto em um bucket do S3 porque o Amazon S3 negou acesso ao 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"
    }
}
```

No exemplo anterior, Macie tentou listar os objetos no bucket usando a operação ListObjectsV2 da API do Amazon S3. Quando Macie enviou a solicitação para o Amazon S3, o Amazon S3 negou o acesso ao bucket.

Os campos a seguir são comuns a todos os eventos de log para trabalhos sigilosos de descoberta de dados:

- `adminAccountId` – O identificador para a Conta da AWS que criou o trabalho.
- `jobId` – O identificador exclusivo para o trabalho.
- `eventType` – O tipo de evento que ocorreu. Para obter listas completas dos valores possíveis e uma descrição de cada um, consulte Tipos de eventos de log para trabalhos.
- `occurredAt` – A data e a hora, no formato Tempo Universal Coordenado (UTC) e ISO 8601 estendido, quando o evento ocorreu.
- `description` – Uma breve descrição do evento.
- `jobName` – O nome personalizado do trabalho.

Dependendo do tipo e da natureza de um evento, um evento de logs também pode conter os seguintes campos:

- `affectedAccount` – O identificador único para o Conta da AWS que é proprietário do recurso afetado.
- `affectedResource` – Um objeto que fornece detalhes sobre o recurso afetado. No objeto, o campo `type` especifica um campo que armazena metadados sobre um recurso. O campo `value` especifica o valor para o campo (`type`).

- `operation` – A operação que Macie tentou realizar e causou o erro.
- `runDate` – A data e a hora, no formato Tempo Universal Coordenado (UTC) e ISO 8601 estendido, quando o começou o trabalho ou a execução do trabalho aplicável.

Tipos de eventos de log para trabalhos de descoberta de dados sigilosos

O Macie publica eventos de log para três categorias de eventos:

- Eventos de status do trabalho, que registram alterações no status ou no progresso de um trabalho ou da execução de um trabalho.
- Eventos de erro no nível da conta, que registram erros que impediram o Macie de analisar dados do Amazon S3 para um Conta da AWS específico.
- Eventos de erro no nível de bucket, que registram erros que impediram o Macie de analisar dados do Amazon S3 para um bucket específico.

Os tópicos desta seção listam e descrevem os tipos de eventos que o Macie publica para cada categoria.

Tópicos

Eventos de status de trabalho

Um evento de status do trabalho registra uma alteração no status, no progresso de um trabalho ou uma execução de um trabalho. Para trabalhos periódicos, o Macie registra e publica esses eventos tanto para o trabalho geral, quanto para as execuções individuais. Para obter mais informações sobre como determinar o status geral do trabalho, consulte Verificação do status de trabalhos de descoberta de dados sigilosos.

O exemplo a seguir usa dados de amostra para mostrar a estrutura e a natureza dos campos em um evento de status do trabalho. Neste exemplo, um evento `SCHEDULED_RUN_COMPLETED` indica que a execução programada de um trabalho periódico terminou de ser executada. A execução começou em 14 de abril de 2021, às 17:09:30 UTC, conforme indicado pelo campo `runDate`. A execução começou em 14 de abril de 2021, às 17:16:30 UTC, conforme indicado pelo 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"
}
```

A tabela a seguir lista e descreve os tipos de eventos de status de trabalho que o Macie registra e publica no CloudWatch Logs. A coluna Tipo de evento indica o nome de cada evento conforme ele aparece no campo `eventType` de um evento. A coluna Descrição fornece uma breve descrição do evento conforme ele aparece no campo `description` de um evento. As informações adicionais fornecem informações sobre o tipo de trabalho ao qual o evento se aplica. A tabela é classificada primeiro pela ordem cronológica geral na qual os eventos podem ocorrer e, em seguida, em ordem alfabética crescente por tipo de evento.

Tipo de evento	Descrição	Informações adicionais
JOB_CREATED	O trabalho foi criado.	Aplica-se a trabalhos únicos e periódicos.
ONE_TIME_JOB_STARTED	O trabalho começou a ser executado.	Aplica-se somente a trabalhos únicos.
SCHEDULED_RUN_STARTED	A execução agendada do trabalho começou a ser executada.	Aplica-se somente a trabalhos periódicos. Para registrar o início de um trabalho único, o Macie publica um evento ONE_TIME_JOB_STARTED, não esse tipo de evento.
BUCKET_MATCHED_THE_CRITERIA	O bucket afetado correspondia aos critérios do bucket especificados para o trabalho.	Aplica-se a trabalhos únicos e periódicos que usam critérios de runtime bucket para

Tipo de evento	Descrição	Informações adicionais
		determinar quais buckets do S3 devem ser analisados. O objeto `affectedResource` especifica o nome do bucket que correspondeu aos critérios e foi incluído na análise do trabalho.
NO_BUCKETS_MATCHED_THE_CRITERIA	O trabalho começou a ser executado, mas nenhum bucket atualmente correspon de aos critérios de buckets especificados para o trabalho. O trabalho não analisou nenhum dado.	Aplica-se a trabalhos únicos e periódicos que usam critérios de runtime bucket para determinar quais buckets do S3 devem ser analisados.
EXECUÇÃO_PROGRAMADA_CONCLUÍDA	A execução agendada do trabalho terminou de ser executada.	Aplica-se somente a trabalhos periódicos. Para registrar a conclusão de um trabalho único, o Macie publica um evento JOB_COMPLETED, não esse tipo de evento.
JOB_PAUSED_BY_USER	O trabalho foi pausado por um usuário.	Aplica-se a trabalhos únicos e periódicos que você interrompeu temporariamente (pausados).

Tipo de evento	Descrição	Informações adicionais
JOB_RESUMED_BY_USER	O trabalho foi retomado por um usuário.	Aplica-se a trabalhos únicos e periódicos que você interrompeu temporari amente (pausados) e retomou subsequentemente.
JOB_PAUSED_BY_MACI E_SERVICE_QUOTA_MET	O trabalho foi pausado pelo Macie. A conclusão do trabalho excederia a cota mensal para a conta afetada.	Aplica-se a trabalhos únicos e periódicos que o Macie interrompeu temporariamente (pausados). O Macie pausa automatic amente uma tarefa quando o processamento adicional da tarefa ou da execução de uma tarefa excede a cota mensal de descoberta de dados sigilosos de uma ou mais contas para as quais a tarefa analisa dados. Para evitar esse problema, considere aumentar a cota das contas afetadas.

Tipo de evento	Descrição	Informações adicionais
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	O trabalho foi retomado pelo Macie. A cota de serviço mensal foi levantada para a conta afetada.	Aplica-se a trabalhos únicos e periódicos que o Macie interrompeu temporariamente (pausados) e retomou subsequentemente. Se o Macie pausar automaticamente um trabalho único, o Macie retomará automaticamente o trabalho quando o mês seguinte começar ou a cota mensal de descoberta de dados sigilosos for aumentada para todas as contas afetadas, o que ocorrer primeiro. Se o Macie pausar automaticamente um trabalho periódico, o Macie retomará automaticamente o trabalho quando a próxima execução estiver programada para começar ou o mês subsequente começar, o que ocorrer primeiro.

Tipo de evento	Descrição	Informações adicionais
JOB_CANCELLED	O trabalho foi cancelado.	Aplica-se a trabalhos únicos e periódicos que você interrompeu permanent emente (cancelados) ou, no caso de trabalhos únicos, pausados e que não foram retomados em 30 dias. Se você suspender ou desativar o Macie, esse tipo de evento também se aplica aos trabalhos que estavam ativos ou pausados quando você suspendeu ou desativou o Macie. O Macie cancela automaticamente seus trabalhos em um Região da AWS se você suspender ou desativar o Macie na região.
JOB_COMPLETED	O trabalho terminou de ser executado.	Aplica-se somente a trabalhos únicos. Para registrar a conclusão de um trabalho único, o Macie publica um evento SCHEDULED _RUN_COMPLETED, não esse tipo de evento.

Eventos de erro no nível da conta

Um evento de erro no nível da conta registra um erro que impediu o Macie de analisar objetos em buckets do S3 que são de propriedade de uma Conta da AWS específica. O campo `affectedAccount` em cada evento especifica o ID para aquela conta.

O exemplo a seguir usa dados de amostra para exibir a estrutura e a natureza dos campos em um evento de erro em nível de conta. Neste exemplo, um evento `ACCOUNT_ACCESS_DENIED` indica que o Macie não conseguiu analisar objetos em nenhum bucket do S3 pertencente à conta `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"
}
```

A tabela a seguir lista e descreve os tipos de eventos de erros em nível de conta que o Macie registra e publica no CloudWatch Logs. A coluna Tipo de evento indica o nome de cada evento conforme ele aparece no campo `eventType` de um evento. A coluna Descrição fornece uma breve descrição do evento conforme ele aparece no campo `description` de um evento. A coluna Informações adicionais fornece todas as dicas aplicáveis para investigar ou solucionar o erro que ocorreu. A tabela é classificada em ordem alfabética crescente por tipo de evento.

Tipo de evento	Descrição	Informações adicionais
ACCOUNT_ACCESS_DENIED	O Macie não tem permissão para acessar os dados do bucket do S3 da conta afetada.	Isso geralmente ocorre porque os buckets que pertencem à conta têm políticas restritivas de bucket. Para obter informações sobre como resolver esse problema, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3.

Tipo de evento	Descrição	Informações adicionais
		O valor do campo `operation` no evento pode ajudá-lo a determinar quais configurações de permissões impediram o Macie de acessar os dados do S3 da conta. Esse campo indica a operação do Amazon S3 que o Macie tentou realizar quando o erro ocorreu.
ACCOUNT_DISABLED	O trabalho ignorou recursos que são de propriedade da conta afetada. O Macie foi desativado para a conta.	Para resolver esse problema, reative o Macie para a conta no mesmo Região da AWS.
ACCOUNT_DISASSOCIATED	O trabalho ignorou recursos que são de propriedade da conta afetada. A conta não está mais associada à sua conta de administrador do Macie como conta de membro.	Isso ocorre se você, como administrador do Macie de uma organização, configurar um trabalho para analisar dados de uma conta de membro associada e a conta de membro for posteriormente removida da sua organização. Para resolver esse problema, associe novamente a conta afetada à sua conta de administrador do Macie como conta de membro. Para obter mais informações, consulte Gerenciar várias contas da .

Tipo de evento	Descrição	Informações adicionais
ACCOUNT_ISOLATED	O trabalho ignorou recursos que são de propriedade da conta afetada. O Conta da AWS foi isolado.	–
ACCOUNT_REGION_DISABLED	O trabalho ignorou recursos que são de propriedade da conta afetada. O Conta da AWS não está ativo na Região da AWS atual.	–
ACCOUNT_SUSPENDED	O trabalho cancelou ou ignorou recursos que são de propriedade da conta afetada. O Macie foi suspenso pela conta.	Se a conta especificada for sua própria conta, o Macie cancelou automaticamente o trabalho quando você suspendeu Macie na mesma região. Para resolver o problema, reative o Macie na Região. Se a conta especificada for uma conta de membro, reative o Macie para essa conta na mesma região.
ACCOUNT_TERMINATED	O trabalho ignorou recursos que são de propriedade da conta afetada. O Conta da AWS foi encerrado.	–

Eventos de erro em nível de bucket

Um evento de erro no nível da conta registra um erro que impediu o Macie de analisar objetos em bucket S3 específico. O campo `affectedAccount` em cada evento especifica o ID da cont para o Conta da AWS proprietário daquele bucket. O objeto `affectedResource` em cada evento especifica o nome do bucket.

O exemplo a seguir usa dados de amostra para exibir a estrutura e a natureza dos campos em um evento de erro em nível de bucket. Neste exemplo, um evento `BUCKET_ACCESS_DENIED` indica que o Macie não conseguiu analisar objetos em nenhum bucket do S3 de nome `DOC-EXAMPLE-BUCKET`. No exemplo anterior, Macie tentou listar os objetos no bucket usando a operação ListObjectsV2 da API do Amazon S3, o Amazon S3 negou acesso ao 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"
    }
}
```

A tabela a seguir lista e descreve os tipos de eventos de erros em nível de bucket que o Macie registra e publica no CloudWatch Logs. A coluna Tipo de evento indica o nome de cada evento conforme ele aparece no campo `eventType` de um evento. A coluna Descrição fornece uma breve descrição do evento conforme ele aparece no campo `description` de um evento. A coluna Informações adicionais fornece todas as dicas aplicáveis para investigar ou solucionar o erro que ocorreu. A tabela é classificada em ordem alfabética crescente por tipo de evento.

Tipo de evento	Descrição	Informações adicionais
BUCKET_ACCESS_DENIED		

Tipo de evento	Descrição	Informações adicionais
	O Macie não tem permissão para acessar o bucket do S3 afetado.	Isso geralmente ocorre porque um bucket tem uma política restritiva de bucket. Para obter informações sobre como resolver esse problema, consulte Permitindo que o Amazon Macie acesse buckets e objetos do S3. O valor do campo `operation` no evento pode ajudá-lo a determinar quais configurações de permissões impediram o Macie de acessar o bucket. Esse campo indica a operação do Amazon S3 que o Macie tentou realizar quando o erro ocorreu.

Tipo de evento	Descrição	Informações adicionais
BUCKET_DETAILS_UNAVAILABLE	Um problema temporário impediu que o Macie recuperasse detalhes sobre o bucket e sobre os objetos do bucket.	Isso ocorre se um problema transitório impediu que o Macie recuperasse os metadados do bucket e do objeto necessários para analisar os objetos de um bucket. Por exemplo, uma exceção do Amazon S3 ocorreu quando o Macie tentou verificar se tinha permissão para acessar o bucket. Para resolver o problema de um trabalho único, considere criar e executar um novo trabalho único para analisar objetos no bucket. Para um trabalho agendado, o Macie tentará recuperar os metadados novamente durante a próxima execução do trabalho.
BUCKET_DOES_NOT_EXIST	O bucket S3 afetado não existe mais.	Isso geralmente ocorre porque um bucket foi excluído.
BUCKET_IN_DIFFERENT_REGION	O bucket do S3 afetado foi movido para um Região da AWS diferente.	–

Tipo de evento	Descrição	Informações adicionais
BUCKET_OWNER_CHANGED	O proprietário do bucket S3 afetado foi alterado. O Macie não tem mais permissão para acessar o bucket.	Isso normalmente ocorre se a propriedade de um bucket foi transferida para um Conta da AWS que não faz parte da sua organização. O campo `affectedAccount` no evento indica a ID da conta para a conta que anteriormente possuía o bucket.

Como gerenciar trabalhos de descoberta de dados sigilosos

Para ajudá-lo a gerenciar seus trabalhos de descoberta de dados sigilosos, o Amazon Macie fornece um inventário completo de seus trabalhos em cada Região da AWS. Com esse inventário, você pode gerenciar seus trabalhos como uma única coleção e acessar as definições de configuração, o status e as estatísticas de processamento de trabalhos individuais. Você também pode acessar as descobertas de dados sigilosos e outros resultados que cada trabalho produziu.

Além dessas tarefas, você pode criar variações personalizadas de trabalhos individuais, como copiar um trabalho existente, ajustar as configurações da cópia e depois salvar a cópia como um novo trabalho. Isso pode ser útil nos casos em que você deseja analisar diferentes conjuntos de dados da mesma forma ou o mesmo conjunto de dados de maneiras diferentes. Ou se desejar ajustar as configurações de um trabalho existente — cancele o trabalho existente, copie-o e, em seguida, ajuste e salve a cópia como um novo trabalho.

Tópicos

- Revisão do seu inventário de trabalhos de descoberta de dados sigilosos
- Verificação das configurações de trabalho de descoberta de dados sigilosos
- Verificação do status de trabalhos de descoberta de dados sigilosos
- Pausar, retomar ou cancelar trabalhos sigilosos de descoberta de dados
- Copiar trabalhos de descoberta de dados sigilosos

Revisão do seu inventário de trabalhos de descoberta de dados sigilosos

A página Trabalhos no console do Amazon Macie fornece informações sobre todos os trabalhos de descoberta de dados sigilosos da sua conta no Região da AWS atual. Para cada trabalho, a tabela exibe informações resumidas que incluem: o status atual do trabalho; se o trabalho é executado de forma programada e periódica, e se o trabalho analisa um número específico de buckets do S3 ou analisa os buckets do S3 que correspondem aos critérios de runtime. Se você escolher um trabalho na tabela, o painel de detalhes exibirá as definições de configuração e outras informações sobre o trabalho.

Para revisar o seu inventário de trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas). A página Trabalhos é aberta e exibe o número de trabalhos em seu inventário e uma tabela desses trabalhos.
3. Para encontrar um trabalho específico mais rapidamente, siga um destes procedimentos:
   - Para classificar a tabela por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna.
   - Para exibir somente os trabalhos que têm um valor específico para um campo, coloque o cursor na caixa de filtro. No menu exibido, escolha o campo a ser usado para o filtro e insira o valor do filtro. Em seguida, escolha Aplicar.
   - Para ocultar somente os trabalhos que têm um valor específico para um campo, coloque o cursor na caixa de filtro. No menu exibido, escolha o campo a ser usado para o filtro e insira o valor do filtro. Em seguida, escolha Aplicar. Na caixa do filtro, selecione o ícone de igual (●) para o filtro. Isso altera o operador do filtro de igual a para não igual a (⊘).
   - Para remover um filtro, escolha o ícone de remover filtro (⊗) para que o filtro seja removido.
4. Para revisar as definições de configuração e outros detalhes de um trabalho específico, selecione o nome do trabalho na tabela e, em seguida, consulte o painel de detalhes.

Verificação das configurações de trabalho de descoberta de dados sigilosos

No console do Amazon Macie, você pode usar o painel de detalhes na página Trabalhos para revisar as definições de configuração e outras informações sobre trabalhos individuais de descoberta de dados sigilosos. Por exemplo, você pode revisar uma lista dos buckets do S3 que um trabalho está configurado para analisar e quais identificadores de dados gerenciados um trabalho usa para analisar objetos nesses buckets.

> **Note**
>
> Não é possível alterar as configurações de um trabalho existente. Isso ajuda a garantir que você tenha um histórico imutável de descobertas de dados sigilosos e resultados de descoberta para auditorias de privacidade de dados e proteção de dados ou investigações que você realiza. Se você quiser alterar um trabalho existente, cancele o trabalho. Em seguida, copie o trabalho, defina a cópia para usar as configurações desejadas e salve a cópia como um novo trabalho.
>
> Se você fizer isso, também deverá tomar medidas para garantir que o novo trabalho não analise os dados existentes da mesma forma novamente. Para fazer isso, anote a data e a hora em que você cancela o trabalho existente. Em seguida, configure o escopo do novo trabalho para incluir apenas os objetos criados ou alterados após o cancelamento do trabalho original. Por exemplo, use critérios de objeto para adicionar uma condição de exclusão da última modificação que especifica a data e a hora em que você cancelou o trabalho original.

Para revisar as configurações de um trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. 0Na página Trabalhos, na escolha o nome do trabalho cujas configurações você deseja revisar. O painel de detalhes exibirá as definições de configuração e outras informações sobre o trabalho. Dependendo das configurações do trabalho, o painel contém as seguintes seções.

   Informações gerais

   Esta seção fornece informações gerais sobre o trabalho, por exemplo, o nome do recurso da Amazon (ARN) do trabalho, quando o trabalho começou a ser executado mais recentemente

e o status atual do trabalho. Se você pausou o trabalho, esta seção também indica quando você pausou o trabalho e quando o trabalho ou a última execução do trabalho expirou ou expirará se você não retomá-lo.

Estatísticas

Esta seção mostra as estatísticas de processamento da tarefa, por exemplo, o número de vezes que a tarefa foi executada e o número aproximado de objetos que a tarefa ainda não processou durante a execução atual.

Scope

Esta seção indica a frequência com que o trabalho é executado. Também mostra configurações que refinam o escopo do trabalho, por exemplo, a profundidade da amostragem e qualquer critério de objeto que inclua ou exclua objetos do S3 da análise do trabalho.

Buckets do S3

Essa seção aparecerá no painel se o trabalho estiver configurado para analisar buckets que você selecionou explicitamente ao criar o trabalho. Ele indica o número do Contas da AWS para o qual o trabalho está configurado para analisar dados. Também indica o número de buckets que o trabalho está configurado para analisar e os nomes desses buckets (agrupados por conta).

Para mostrar a lista completa de contas e buckets no formato JSON, selecione o número no campo Total de buckets.

Critérios de bucket S3

Essa seção aparecerá no painel se o trabalho usar critérios de runtime para determinar quais buckets analisar. Ele lista os critérios que o trabalho está configurado para usar.

Para mostrar os critérios no formato JSON, selecione Detalhes e, em seguida, selecione a guia Critérios na janela exibida.

Para revisar uma tabela de buckets que atualmente corresponda aos critérios, selecione Detalhes e, em seguida, selecione a guia Combinando buckets na janela exibida. Opcionalmente, selecione atualizar () para recuperar os dados mais recentes.

> **Tip**
>
> Se o trabalho já tiver sido executado, você também poderá determinar se algum bucket correspondeu aos critérios quando o trabalho foi executado e, em caso afirmativo, aos nomes desses buckets. Para fazer isso, revise os eventos de log do trabalho: selecione Exibir resultados na parte superior do painel e, em seguida, selecione Exibir logs do CloudWatch. Macie abre o console do Amazon CloudWatch e exibe uma tabela de eventos de log para o trabalho. Os eventos incluem um evento `BUCKET_MATCHED_THE_CRITERIA` para cada bucket que correspondeu aos critérios e foi incluído na análise do trabalho. Para obter mais informações, consulte Monitorar trabalhos.

Identificadores de dados personalizados

Essa seção aparece no painel se a tarefa estiver configurada para usar um ou mais identificadores de dados personalizados. Ele especifica os nomes desses identificadores de dados personalizados.

Lista de permissões

Essa seção aparece no painel se a tarefa estiver configurada para usar uma ou mais Lista de permissões. Ele especifica os nomes dessas listas. Para revisar as configurações de uma lista de permissões antes de selecioná-la, selecione o ícone de link ( ) ao lado do nome da lista.

Identificadores de dados gerenciados

Esta seção indica quais identificadores de dados gerenciados o trabalho está configurado para usar. Isso é determinado pelo tipo de seleção do identificador de dados gerenciados para o trabalho:

- Recomendado – Use os identificadores de dados gerenciados que estão no conjunto recomendado quando o trabalho é executado.
- Incluir os selecionados – Use somente os identificadores de dados gerenciados listados na seção Seleções.
- Incluir tudo – Use todos os identificadores de dados gerenciados que estão disponíveis quando o trabalho é executado.

- Excluir os selecionados – Use todos os identificadores de dados gerenciados que estão disponíveis quando o trabalho é executado, exceto os listados na seção Seleções.
- Excluir tudo – não use nenhum identificador de dados gerenciados. Use somente os identificadores de dados personalizados especificados.

Para revisar essas configurações no formato JSON, selecione Detalhes.

Tags

Essa seção aparece no painel se as tags estiverem associadas ao trabalho. Ele lista essas tags.

Uma tag é um rótulo que você define e atribui a determinados tipos de recursos AWS. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.

4. Para revisar e salvar as configurações do trabalho no formato JSON, selecione o identificador exclusivo do trabalho (Job ID) na parte superior do painel e selecione Download.

Verificação do status de trabalhos de descoberta de dados sigilosos

Quando você cria um trabalho de descoberta de dados sigilosos, o seu status inicial é Ativo (em execução) ou Ativo (Inativo), dependendo do tipo e do cronograma do trabalho. Em seguida, o trabalho passa por estados adicionais, que você pode monitorar à medida que o trabalho progride.

> **Tip**
>
> Além de monitorar o status geral de um trabalho, você pode monitorar eventos específicos que ocorrem à medida que o trabalho progride. Você pode fazer isso usando dados de log que o Macie publica automaticamente no Amazon CloudWatch Logs. Os dados nesses logs fornecem um registro das alterações no status de um trabalho e detalhes sobre quaisquer erros no nível da conta ou do bucket que ocorram durante a execução de um trabalho. Para obter mais informações, consulte Monitorar trabalhos.

Para verificar o status de um trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. No painel de navegação, escolha Jobs (Tarefas).
3. Na página Trabalhos, localize o trabalho cujo status você deseja verificar. O campo Status indica o status atual de um trabalho.

   Ativo (inativo)

   Para um trabalho periódico, a execução anterior está concluída e a próxima execução programada está pendente. Esse valor não se aplica a trabalhos únicos.

   Ativo (em execução)

   Para um trabalho único, o trabalho está em andamento no momento. Para um trabalho periódico, uma execução programada está em andamento.

   Cancelado

   Para qualquer tipo de trabalho, o trabalho foi interrompido permanentemente (cancelado).

   Um trabalho tem esse status se você o cancelou explicitamente ou, se for um trabalho único, você pausou o trabalho e não o retomou em 30 dias. Um trabalho também pode ter esse status se você suspendeu o Macie anteriormente no Região da AWS atual.

   Concluído

   Para um trabalho único, o trabalho foi executado com êxito e agora está concluído. Esse valor não se aplica a trabalhos periódicos. Em vez disso, o status de um trabalho periódico muda para Ativo (Inativo) quando cada execução é concluída com êxito.

   Pausado (pelo Macie)

   Para qualquer tipo de trabalho, o trabalho foi interrompido temporariamente (pausado) pelo Macie.

   Um trabalho tem esse status se a conclusão do trabalho ou a execução de um trabalho exceder a cota mensal de descoberta de dados sigilosos para a sua conta. Quando isso acontece, o Macie pausa o trabalho automaticamente. O Macie retoma automaticamente o trabalho quando o próximo mês civil começa (e a cota mensal é redefinida para a sua conta) ou se você aumenta a cota da sua conta.

   Se você for o administrador do Macie de uma organização e tiver configurado o trabalho para analisar dados das contas-membro, o trabalho também poderá ter esse status se a

conclusão do trabalho ou a execução de um trabalho exceder a cota mensal de descoberta de dados sigilosos de uma conta-membro.

Se um trabalho estiver em execução e a análise de objetos elegíveis atingir essa cota para uma conta-membro, o trabalho interromperá a análise de objetos pertencentes à conta. Quando o trabalho termina de analisar os objetos de todas as outras contas que não atingiram a cota, o Macie pausa o trabalho automaticamente. Se for um trabalho único, o Macie retomará automaticamente o trabalho quando o mês seguinte começar ou a cota mensal de descoberta de dados sigilosos for aumentada para todas as contas afetadas, o que ocorrer primeiro. Se for um trabalho periódico, o Macie retomará o trabalho automaticamente quando a próxima execução estiver programada para começar ou o mês subsequente começar, o que ocorrer primeiro. Se uma execução programada começar antes do início do próximo mês civil ou se a cota for aumentada para uma conta afetada, o trabalho não analisará objetos pertencentes à conta.

Pausado (pelo usuário)

Para qualquer tipo de trabalho, o trabalho foi interrompido temporariamente (pausado) por você.

Se você pausar um trabalho único e não retomá-lo em 30 dias, o trabalho expira e Macie o cancela. Se você pausar um trabalho periódico enquanto ele estiver em execução e não retomá-lo em 30 dias, a execução do trabalho expirará e o Macie cancelará a execução. Para verificar a data de expiração de um trabalho pausado ou execução de um trabalho, selecione o nome do trabalho na tabela e, em seguida, consulte o campo Expira na seção Detalhes do status do painel de detalhes.

Se um trabalho for cancelado ou pausado, você poderá consultar os detalhes do trabalho para determinar se o trabalho começou a ser executado ou, para um trabalho periódico, se foi executado pelo menos uma vez antes de ser cancelado ou pausado. Para fazer isso, selecione o nome do trabalho na tabela e, em seguida, consulte o painel de detalhes. No painel, o campo Número de execuções indica o número de vezes que o trabalho foi executado. O campo Último horário de execução indica a data e a hora mais recentes quando o trabalho começou a ser executado.

Dependendo do status atual do trabalho, você pode, opcionalmente, pausar, retomar ou cancelar o trabalho.

Pausar, retomar ou cancelar trabalhos sigilosos de descoberta de dados

Depois de criar um trabalho de descoberta de dados sigilosos, você pode pausá-lo temporariamente ou cancelá-lo permanentemente. Quando você pausa um trabalho que está sendo executado ativamente, o Macie imediatamente começa a pausar todas as tarefas de processamento do trabalho. Quando você pausa um trabalho que está sendo executado ativamente, o Macie imediatamente começa a pausar todas as tarefas de processamento do trabalho. Você não pode retomar ou reiniciar um trabalho depois que ele for cancelado.

Se você pausar um trabalho único, poderá retomá-lo em 30 dias. Quando você retomar o trabalho, o Macie retoma imediatamente o processamento a partir do ponto em que você pausou o trabalho; o Macie não reinicia o trabalho desde o início. Se você não retomar um trabalho único e em 30 dias depois de pausá-lo, o trabalho expira e o Macie o cancela.

Se você pausar um trabalho periódico, poderá retomá-lo a qualquer momento. Se você retomar um trabalho periódico e o trabalho estiver inativo quando você o pausou, o Macie retomará o trabalho de acordo com o cronograma e outras definições de configuração que você escolheu ao criar o trabalho. Se você retomar um trabalho periódico e o trabalho estiver em execução quando você o pausou, a forma como Macie retoma o trabalho depende de quando você retomar o trabalho:

- Quando você retomar o trabalho dentro de 30 dias depois de pausá-lo, o Macie retoma imediatamente a execução programada a partir do ponto em que você pausou o trabalho; o Macie não reinicia o trabalho desde o início.
- Se você não retomar o trabalho dentro de 30 dias após a pausa, a última execução agendada expirará e o Macie cancelará todas as tarefas de processamento restantes da execução. Se você retomar o trabalho subsequentemente, o Macie retomará o trabalho de acordo com o cronograma e outras definições de configuração que você escolheu ao criar o trabalho.

Para ajudá-lo a determinar quando um trabalho pausado ou a execução de um trabalho expirará, o Macie adiciona uma data de expiração aos detalhes do trabalho enquanto o trabalho está pausado. Para verificar essa data, escolha o nome do trabalho na tabela na página Trabalhos e, em seguida, consulte o campo Expira na seção Detalhes do status do painel de detalhes. Além disso, notificamos você aproximadamente sete dias antes da expiração do trabalho ou da execução do trabalho. Notificaremos você novamente quando o trabalho ou a execução do trabalho expirar e for cancelado. Para notificá-lo, enviamos um email para o endereço que está associado ao seu Conta da AWS. Também criamos AWS Health eventos e Amazon CloudWatch Events para a sua conta.

Para pausar, retomar ou cancelar um trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Na página Trabalhos, marque a caixa de seleção do trabalho que você deseja pausar, retomar ou cancelar e, em seguida, faça o seguinte no menu Ações:
   - Para pausar o trabalho temporariamente, selecione Pausar. Essa opção estará disponível somente se o status atual da tarefa for Ativo (Inativo), Ativo (Em execução) ou Pausado (Pelo Macie).
   - Para retomar o trabalho, selecione Retomar. Essa opção estará disponível somente se o status atual do trabalho for Pausado (pelo usuário).
   - Para cancelar a operação, selecione Cancelar. Se escolher essa opção, não será possível continuar ou reiniciar o trabalho posteriormente.

Copiar trabalhos de descoberta de dados sigilosos

Para criar rapidamente um novo trabalho de descoberta de dados sigilosos semelhante a um trabalho existente, você pode criar uma cópia do trabalho, editar as configurações da cópia e depois salvar a cópia como um novo trabalho. Isso pode ser útil nos casos em que você deseja criar uma variação personalizada de um trabalho existente. Ou você deseja ajustar as configurações de uma tarefa existente ao cancelar o trabalho, copie-o e, em seguida, ajuste e salve as configurações como um novo trabalho.

Para copiar um trabalho

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, escolha Jobs (Tarefas).
3. Marque a caixa de seleção ao lado do trabalho que você deseja copiar.
4. No menu Ações, selecione Copiar para novo.
5. Conclua as etapas no console para revisar e ajustar as configurações da cópia do trabalho. Para a etapa Refinar o escopo, considere escolher opções que evitem que o trabalho analise os dados existentes da mesma forma novamente:
   - Para um trabalho único, use critérios de objeto para incluir somente os objetos que foram criados ou alterados após um determinado período. Por exemplo, se você estiver criando

uma cópia de um trabalho que cancelou, adicione uma condição de Última modificação que especifique a data e a hora em que você cancelou o trabalho existente.

- Para um trabalho periódico, desmarque a caixa de seleção Incluir objetos existentes. A primeira execução do trabalho analisa apenas os objetos que são criados ou alterados após a conclusão da criação do trabalho e antes do início da primeira execução. Você também pode usar critérios de objeto para excluir objetos que foram modificados pela última vez antes de uma determinada data e hora.

Para obter detalhes adicionais sobre essa e outras etapas, consulte Criar um trabalho de descoberta de dados confidenciais.

6. Ao terminar, selecione Enviar para salvar a cópia como um novo trabalho.

Prever e monitorar os custos para a tarefas de descoberta de dados confidenciais

Os preços do Amazon Macie são baseados parcialmente na quantidade de dados que você analisa executando trabalhos confidenciais de descoberta de dados. Para prever e monitorar seus custos previstos para executar trabalhos de descoberta de dados confidenciais, você pode revisar as estimativas de custo que o Macie fornece quando você cria um trabalho e depois de começar a executar trabalhos.

Para revisar e monitorar seus custos reais, você pode usar a AWS Billing and Cost Management. A AWS Billing and Cost Management fornece atributos projetados para ajudar você a rastrear e analisar seus custos para o Serviços da AWS e gerenciar orçamentos para a sua conta ou organização. Ele também fornece atributos que podem ajudar você a prever os custos de uso com base em dados históricos. Para saber mais, consulte o Manual do usuário do AWS Billing.

Para informações sobre a definição de preços do Macie, consulte a definição de preços do Amazon Macie.

Tópicos

- Prever o custo de um trabalho de descoberta de dados confidenciais
- Monitorando os custos estimados para tarefas de descoberta de dados confidenciais

Prever o custo de um trabalho de descoberta de dados confidenciais

Quando você cria um trabalho de descoberta de dados confidenciais, o Amazon Macie pode calcular e exibir os custos aproximados em duas etapas principais no processo de criação do trabalho: quando você revisa a tabela de buckets do S3 que você selecionou para o trabalho (etapa 2) e quando você revisa todas as configurações do trabalho (etapa 8). Essas estimativas podem ajudar você a determinar se deve ajustar as configurações da tarefa antes de salvar o trabalho. A disponibilidade e a natureza das estimativas dependem das configurações que você escolher para o trabalho.

Análise dos custos estimados para buckets individuais (etapa 2)

Se você selecionar explicitamente buckets individuais para um trabalho de análise, você poderá revisar o custo estimado da análise de objetos em cada um desses buckets. O Macie exibe essas estimativas durante a etapa 2 do processo de criação do trabalho, quando você revisa as seleções do seu bucket. Na tabela dessa etapa, o campo Custo estimado indica o custo total estimado (em USD) da execução do trabalho uma vez ao analisar os objetos em um bucket.

Cada estimativa reflete a quantidade prevista de dados não compactados que o trabalho analisará em um bucket, com base no tamanho e nos tipos de objetos atualmente armazenados no bucket. A estimativa também reflete os preços do Macie para a Região da AWS atual.

Somente objetos classificáveis são incluídos na estimativa de custo de um bucket. Um objeto classificável é um objeto S3 que usa uma classe de armazenamento compatível do Amazon S3 e tem uma extensão de arquivo para um arquivo ou formato de armazenamento compatível. Se quaisquer objetos classificáveis forem itens compactados ou arquivados, a estimativa pressupõe que os arquivos usam uma taxa de compactação de 3:1 e que a tarefa possa analisar todos os arquivos extraídos.

Revisando o custo total estimado de um trabalho (etapa 8)

Se você criar um trabalho avulso ou criar e configurar um trabalho periódico para incluir objetos S3 existentes, o Macie calcula e exibe o custo total estimado do trabalho durante a última etapa do processo de criação do trabalho. Você pode revisar essa estimativa enquanto revisa e verifica todas as configurações selecionadas para o trabalho.

Essa estimativa indica o custo total projetado (em USD) da execução do trabalho uma vez na Região atual. A estimativa reflete a quantidade projetada de dados não compactados que o trabalho irá analisar. Ela se baseia no tamanho e nos tipos de objetos atualmente armazenados

em buckets que você selecionou explicitamente para o trabalho ou em até 500 buckets que atualmente correspondem aos critérios de buckets que você especificou para o trabalho, dependendo das configurações do trabalho.

Observe que essa estimativa não reflete nenhuma opção que você selecionou para refinar e reduzir o escopo do trabalho. Por exemplo, uma menor profundidade de amostragem ou critérios que excluam determinados objetos S3 do trabalho. Ela também não reflete sua cota mensal de descoberta de dados confidenciais, o que pode limitar o escopo e o custo da análise do trabalho, ou quaisquer descontos que poderiam se aplicar à sua conta.

Além do custo total estimado do trabalho, a estimativa fornece dados agregados que oferecem uma visão sobre o escopo e o custo projetados do trabalho:

- Os valores de tamanho indicam o tamanho total de armazenamento dos objetos que o trabalho pode ou não analisar.
- Os valores de contagem de objetos indicam o número total de objetos que o trabalho pode ou não analisar.

Nesses valores, um objeto Classificável é um objeto S3 que usa uma classe de armazenamento compatível do Amazon S3 e tem uma extensão de arquivo para um arquivo ou formato de armazenamento compatível. Somente objetos classificáveis são incluídos na estimativa de custo. Um objeto Inclassificável é um objeto que não utiliza uma classe de armazenamento ou não possui uma extensão de nome de arquivos suportados ou um formato de armazenamento compatível. Esses objetos não são incluídos na estimativa de custo.

A estimativa fornece dados agregados adicionais para objetos do S3 que são arquivos compactados ou arquivados. O valor Compactado indica o tamanho total de armazenamento dos objetos que usam uma classe de armazenamento do Amazon S3 e têm uma extensão de nome de arquivo para um tipo compatível de arquivo compactado ou de arquivamento. O valor Descompactado indica o tamanho aproximado desses objetos se eles estiverem descompactados, com base em uma taxa de compactação especificada. Esses dados são relevantes devido à forma como o Macie analisa arquivos compactados e arquivados.

Quando o Macie analisa um arquivo compactado ou arquivado, ele inspeciona o arquivo completo e o conteúdo do arquivo. Para inspecionar o conteúdo do arquivo, o Macie descompacta o arquivo e, em seguida, inspeciona cada arquivo extraído que usa um formato compatível. A quantidade real de dados que um trabalho analisa, portanto, depende do seguinte:

- Se um arquivo usa compactação e, em caso afirmativo, a taxa de compactação que ele usa.

- O número, tamanho e formato dos arquivos extraídos.

Por default, o Macie assume o seguinte ao calcular as estimativas de custo de um trabalho:

- Todos os arquivos compactados e arquivados usam uma taxa de compactação de 3:1.
- Todos os arquivos extraídos usam um formato de arquivo ou armazenamento compatível.

Essas suposições podem resultar em uma estimativa de tamanho maior para o escopo dos dados que o trabalho analisará e, consequentemente, uma estimativa de custo mais alta para o trabalho.

Você pode recalcular o custo total estimado do trabalho com base em uma taxa de compressão diferente. Para fazer isso, escolha a taxa na lista Escolha uma taxa de compressão estimada na seção Custo estimado. Em seguida, o Macie atualiza a estimativa para corresponder à sua seleção.

Para obter mais informações sobre como o Macie calcula os custos estimados, consulte Entender como os custos de uso estimados são calculados.

Monitorando os custos estimados para tarefas de descoberta de dados confidenciais

Se você já estiver executando trabalhos confidenciais de descoberta de dados, a página de Uso no console do Amazon Macie pode ajudá-lo a monitorar o custo estimado desses trabalhos. A página mostra seus custos estimados (em USD) do uso do Macie na Região da AWS atual durante o mês corrente do calendário. Para obter mais informações sobre como o Macie calcula custos estimados, consulte Entender como os custos de uso estimados são calculados.

Para revisar seus custos estimados de execução de trabalhos

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja rever seus custos estimados.
3. No painel de navegação, escolha Uso.
4. Na página Uso, consulte o detalhamento dos custos estimados da sua conta. O item Trabalhos de descoberta de dados confidenciais relata o custo total estimado dos trabalhos que você executou até agora durante o mês atual na Região.

   Se você for o administrador do Macie de uma organização, a seção Custos estimados mostra os custos estimados para a sua organização em geral para o mês atual na Região atual. Para exibir o custo total estimado dos trabalhos que foram executados para uma conta específica,

escolha a conta na tabela. Em seguida, a seção Custos estimados mostra um detalhamento dos custos estimados da conta, incluindo o custo estimado dos trabalhos que foram executados. Para mostrar esses dados de uma conta diferente, escolha a conta na tabela. Para limpar a seleção da conta, escolha X ao lado da ID da conta.

Para revisar e monitorar seus custos reais, use AWS Billing and Cost Management.

Identificadores de dados gerenciados recomendados para trabalhos de descoberta de dados sigilosos

Para otimizar os resultados de seus trabalhos de descoberta de dados sigilosos, você pode configurar trabalhos individuais para usar automaticamente o conjunto de identificadores de dados gerenciados que recomendamos para trabalhos. Um identificador de dados gerenciados é um conjunto de critérios e técnica integrados que são projetados para detectar um tipo específico de dados sigilosos, como por exemplo, chaves de acesso secretas AWS, números de cartão de crédito, ou números de passaporte para um determinado país ou região.

O conjunto recomendado de identificadores de dados gerenciados foi projetado para detectar categorias e tipos comuns de dados sigilosos. Com base em nossa pesquisa, ele pode detectar categorias gerais e tipos de dados sigilosos e, ao mesmo tempo, otimizar os resultados do seu trabalho ao reduzir o ruído. À medida que lançamos novos identificadores de dados gerenciados, nós os adicionamos a esse conjunto se for provável que otimizem ainda mais os resultados do seu trabalho. Com o tempo, também podemos adicionar ou remover identificadores de dados gerenciados existentes do conjunto. Se adicionarmos ou removermos um identificador de dados gerenciados do conjunto recomendado, atualizaremos esta página para indicar a natureza e o momento da alteração. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na página do Histórico de documentos do Macie.

Ao criar um trabalho de descoberta de dados sigilosos, você especifica quais identificadores de dados gerenciados deseja que o trabalho use para analisar objetos nos buckets do Amazon Simple Storage Service (Amazon S3). Para configurar um trabalho para usar o conjunto recomendado de identificadores de dados gerenciados, selecione a opção Recomendado ao criar o trabalho. O trabalho então usará automaticamente todos os identificadores de dados gerenciados que estão no conjunto recomendado quando o trabalho começar a ser executado. Se você escolher essa opção e configurar o trabalho para ser executado mais de uma vez, cada execução usará automaticamente todos os identificadores de dados gerenciados que estão no conjunto recomendado quando a execução é iniciada.

Os tópicos a seguir listam os identificadores de dados gerenciados que estão atualmente no conjunto recomendado, organizados por categoria e tipo de dados sigilosos. Eles especificam o identificador exclusivo (ID) para cada identificador de dados gerenciados no conjunto. Esse ID descreve o tipo de dados sigilosos que um identificador de dados gerenciados foi projetado para detectar, por exemplo: `PGP_PRIVATE_KEY` para chaves privadas PGP e `USA_PASSPORT_NUMBER` para números de passaportes dos EUA.

Tópicos

Para obter detalhes sobre identificadores de dados gerenciados específicos ou uma lista completa de todos os identificadores de dados gerenciados que o Macie fornece atualmente, consulte Usar identificadores de dados gerenciados.

Credenciais

Para detectar ocorrências de dados de credenciais em objetos do S3, o conjunto recomendado usa os seguintes identificadores de dados gerenciados.

Tipo de dado sigiloso	ID do identificador de dados gerenciados
Chave de acesso secreta da AWS	`AWS_CREDENTIALS`
Cabeçalho de autorização básica HTTP	`HTTP_BASIC_AUTH_HEADER`
Chave privada OpenSSH	`OPENSSH_PRIVATE_KEY`
Chave privada PGP	`PGP_PRIVATE_KEY`
Chave privada do padrão de criptografia de chave pública (Public Key Cryptography Standard, PKCS)	`PKCS`
Chave privada PuTTY	`PUTTY_PRIVATE_KEY`

Informações financeiras

Para detectar ocorrências de dados de informações financeiras em objetos do S3, o conjunto recomendado usa os seguintes identificadores de dados gerenciados.

Tipo de dado sigiloso	ID do identificador de dados gerenciados
Dados da faixa magnética do cartão de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Números de cartão de crédito	`CREDIT_CARD_NUMBER` (para números de cartão de crédito próximos a uma palavra-chave)

Informações de identificação pessoal (PII)

Para detectar ocorrências de informações de identificação pessoal (PII) em objetos do S3, o conjunto recomendado usa os seguintes identificadores de dados gerenciados.

Tipo de dado sigiloso	ID do identificador de dados gerenciados
Número de identificação da carteira de habilitação	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (para os EUA), `UK_DRIVERS_LICENSE`
Número de registro eleitoral	`UK_ELECTORAL_ROLL_NUMBER`
Número de identificação nacional	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Número do Seguro Nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Número de passaporte	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUM`

Tipo de dado sigiloso	ID do identificador de dados gerenciados
	`BER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER`
Número do Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número da Previdência Social (SSN)	`SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER`
Identificação do contribuinte ou número de referência	`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`

Atualizações para o conjunto recomendado

A tabela a seguir descreve as alterações no conjunto de identificadores de dados gerenciados que recomendamos para trabalhos sigilosos de descoberta de dados. Para receber alertas automáticos sobre alterações realizadas nesta página, inscreva-se no feed RSS na página Histórico de documento do Macie.

Alteração	Descrição	Data
Disponibilidade geral	Lançamento inicial do conjunto recomendado.	27 de junho de 2023

Análise de objetos criptografados do Amazon S3 com o Amazon Macie

Quando você habilita o Amazon Macie para o seu Conta da AWS, o Macie cria uma função vinculada ao serviço que concede ao Macie as permissões necessárias para chamar o Amazon Simple Storage Service (Amazon S3) e outros Serviços da AWS em seu nome. Uma função vinculada ao serviço simplifica o processo de configuração de AWS service (Serviço da AWS) porque você não precisa adicionar permissões manualmente para que o serviço conclua ações em seu nome. Para saber mais sobre esse tipo de função, consulte Usando funções vinculadas a serviços no Guia do AWS Identity and Access Managementusuário.

A política de permissões para a função vinculada ao serviço do Macie (`AWSServiceRoleForAmazonMacie`) permite que o Macie execute ações que incluem recuperar informações sobre seus buckets e objetos do S3 e recuperar e analisar objetos nos buckets do S3. Se a conta for a conta de administrador do Macie de uma organização, a política também permitirá que o Macie execute essas ações em seu nome para contas-membro na organização.

Se um objeto do S3 for criptografado, a política de permissões para a função vinculada ao serviço do Macie normalmente concede ao Macie as permissões necessárias para descriptografar o objeto. No entanto, isso depende do tipo de criptografia usada. Também pode depender de o Macie ter permissão para usar a chave de criptografia apropriada.

Tópicos

- Opções de criptografia para objetos do Amazon S3
- Permitir que o Amazon Macie use um AWS KMS key gerenciado pelo cliente

Opções de criptografia para objetos do Amazon S3

O Amazon S3 oferece suporte a várias opções de criptografia para objetos do S3. Para a maioria dessas opções, o Amazon Macie pode descriptografar um objeto usando a função vinculada ao serviço Macie para sua conta. No entanto, isso depende do tipo de criptografia usado para criptografar um objeto.

Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

> Se um objeto for criptografado usando criptografia do lado do servidor com uma chave gerenciada do Amazon S3 (SSE-S3), o Macie poderá descriptografar o objeto.

Para saber mais sobre esse tipo de criptografia, consulte Usar criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Criptografia do lado do servidor com AWS KMS keys (DSSE-KMS e SSE-KMS)

Se um objeto for criptografado usando criptografia de camada dupla do lado do servidor ou criptografia do lado do servidor com um dispositivo AWS gerenciado AWS KMS key (DSSE-KMS ou SSE-KMS), o Macie poderá descriptografar o objeto.

Se um objeto for criptografado usando criptografia de camada dupla do lado do servidor ou criptografia do lado do servidor com um cliente gerenciado AWS KMS key (DSSE-KMS ou SSE-KMS), o Macie só poderá descriptografar o objeto se você permitir que o Macie use a chave. Esse é o caso de objetos criptografados com chaves KMS gerenciadas inteiramente dentro AWS KMS e chaves KMS em um repositório de chaves externo. Se o Macie não tiver permissão para usar a chave KMS aplicável, o Macie só poderá armazenar e relatar metadados do objeto.

Para saber mais sobre esses tipos de criptografia, consulte Usando criptografia do lado do servidor de camada dupla com AWS KMS keys e Usando criptografia do lado do servidor com AWS KMS keys no Guia do usuário do Amazon Simple Storage Service.

> **Tip**
>
> Você pode gerar automaticamente uma lista de todas as AWS KMS keys gerenciadas por clientes de que o Macie precisa para acessar ao analisar objetos nos buckets do S3 da sua conta. Para fazer isso, execute o script do Analisador de AWS KMS Permissões, que está disponível no repositório Amazon Macie Scripts em. GitHub O script também pode gerar um script adicional de comandos AWS Command Line Interface (AWS CLI). Opcionalmente, você pode executar esses comandos para atualizar as configurações e políticas necessárias para as chaves KMS que você especificar.

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Se um objeto for criptografado usando criptografia do lado do servidor com uma chave fornecida pelo cliente (SSE-C), o Macie não conseguirá descriptografar o objeto. O Macie só pode armazenar e relatar metadados do objeto.

Para saber mais sobre esse tipo de criptografia, consulte Usar criptografia do lado do servidor com chaves fornecidas pelo cliente no Guia do usuário do Amazon Simple Storage Service.

Criptografia do lado do cliente

Se um objeto for criptografado usando criptografia do lado do cliente, o Macie não poderá descriptografar o objeto. O Macie só pode armazenar e relatar metadados do objeto. Por exemplo, o Macie pode relatar o tamanho do objeto e as tags associadas ao objeto.

Para saber mais sobre esse tipo de criptografia no contexto do Amazon S3, consulte Proteção de dados usando criptografia do lado do cliente no Guia do usuário do Amazon Simple Storage Service.

Você pode filtrar seu inventário de buckets no Macie para determinar quais buckets do S3 armazenam objetos que usam determinados tipos de criptografia. Você também pode determinar quais buckets usam certos tipos de criptografia do lado do servidor por padrão ao armazenar novos objetos. A tabela a seguir fornece exemplos de filtros que você pode aplicar ao seu inventário de bucket para encontrar essas informações.

Para mostrar buckets que...	Aplique este filtro…
Armazenar objetos com criptografia SSE-C	A contagem de objetos por criptografia é fornecida pelo cliente e de = 1
Armazene objetos que usam criptografia DSSE-KMS ou SSE-KMS	A contagem de objetos por criptografia é AWS KMSgerenciada e De = 1
Armazenar objetos com criptografia SSE-S3	A contagem de objetos por criptografia é gerenciada pelo Amazon S3 e From = 1
Armazenar objetos com criptografia do lado do cliente (ou sem criptografia)	Contagem de objetos por criptografia é Sem criptografia e De = 1
Criptografe novos objetos por padrão usando a criptografia DSSE-KMS	Criptografia padrão = aws:kms:dsse
Criptografe novos objetos por padrão usando a criptografia SSE-KMS	Criptografia padrão = aws:kms
Criptografe novos objetos por padrão usando a criptografia SSE-KMS	Criptografia padrão = AES256

Se um bucket estiver configurado para criptografar novos objetos por padrão usando criptografia DSSE-KMS ou SSE-KMS, você também poderá determinar qual deles será usado. AWS KMS key Para fazer isso, selecione o bucket na página de buckets do S3. No painel de detalhes do bucket, em Criptografia do lado do servidor, consulte o campo. AWS KMS key Esse campo exibe o nome do recurso da Amazon (ARN) ou o identificador exclusivo (ID da chave) da chave.

Permitir que o Amazon Macie use um AWS KMS key gerenciado pelo cliente

Se um objeto do Amazon S3 for criptografado usando criptografia de camada dupla do lado do servidor ou criptografia do lado do servidor com um cliente gerenciado (DSSE-KMS AWS KMS key ou SSE-KMS), o Amazon Macie poderá descriptografar o objeto somente se tiver permissão para usar a chave. A forma de fornecer esse acesso depende de a conta que possui a chave também possuir o bucket do S3 que armazena o objeto:

- Se a mesma conta for proprietária da AWS KMS key e do bucket, um usuário da conta precisará atualizar a política da chave.
- Se uma conta for proprietária da AWS KMS key e outra conta diferente for proprietária do bucket, um usuário da conta proprietária da chave deverá permitir o acesso entre contas à chave.

Este tópico descreve como realizar essas tarefas e fornece exemplos para ambos os cenários. Para saber mais sobre como permitir o acesso ao serviço gerenciado pelo clienteAWS KMS keys, consulte Autenticação e controle de acesso AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Permitir acesso da mesma conta a uma chave gerenciada pelo cliente

Se a mesma conta for proprietária da AWS KMS key e do bucket do S3, um usuário da conta precisará adicionar uma declaração à política da chave. A declaração adicional deverá permitir que o perfil vinculado a serviço do Macie para a conta decifre dados usando a chave. Para obter informações detalhadas sobre como atualizar uma política principal, consulte Alterar uma política de chave no Guia do desenvolvedor AWS Key Management Service.

Na declaração:

- O elemento `Principal` deverá especificar o nome do recurso da Amazon (ARN) do perfil vinculado a serviço do Macie para a conta proprietária da AWS KMS key e do bucket do S3.

Se a conta estiver em uma Região da AWS opcional, o ARN também deverá incluir o código de região adequado para a região. Por exemplo, se a conta estiver na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, o `Principal` elemento deverá especificar`arn:aws:iam::123456789012:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, onde *123456789012* é o ID da conta. Para obter uma lista códigos das regiões nas quais o Macie está disponível, consulte Endpoints e cotas do Amazon Macie no Referência geral da AWS.

- O array `Action` deve especificar a ação `kms:Decrypt`. Essa é a única ação do AWS KMS para a qual o Macie deve ter permissão para descriptografar um objeto do S3 que foi criptografado com a chave.

Veja a seguir um exemplo da declaração a ser adicionada à política para uma 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": "*"
}
```

No exemplo anterior:

- O campo `AWS` no elemento `Principal` especifica o ARN da função vinculada ao serviço Macie (`AWSServiceRoleForAmazonMacie`) para a conta. Isso permite que a função vinculada ao serviço do Macie execute a ação especificada na declaração de política. *123456789012* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta proprietária da chave do KMS e do bucket do S3.
- A matriz `Action` especifica a ação que o perfil vinculado a serviço do Macie pode realizar usando a chave do KMS: descriptografar o texto cifrado que foi criptografado com a chave.

O local em que você adiciona essa declaração a uma política de chave depende da estrutura e dos elementos que a política contém atualmente. Ao adicionar a instrução, certifique-se de que a sintaxe seja válida. As políticas de chaves usam o formato JSON. Isso significa que você também precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política.

Permitir acesso entre contas a uma chave gerenciada pelo cliente

Se uma conta for proprietária da AWS KMS key (proprietária da chave) e outra conta for proprietária do bucket do S3 (proprietária do bucket), o proprietário da chave deverá fornecer ao proprietário do bucket acesso entre contas à chave do KMS. Para fazer isso, o proprietário da chave primeiro garante que a política de chave permita que o proprietário do bucket use a chave e crie uma concessão para a chave. Em seguida, o proprietário do bucket cria uma concessão para a chave. Uma concessão é um instrumento de política que permite que as AWSentidades principais usem chaves KMS em operações criptográficas se as condições especificadas pela concessão forem atendidas. Nesse caso, a concessão delegará as permissões relevantes ao perfil vinculado a serviço do Macie para a conta do proprietário do bucket.

Para obter informações detalhadas sobre como atualizar uma política principal, consulte Alterar uma política de chave no Guia do desenvolvedor AWS Key Management Service. Para saber mais sobre concessões, consulte Subsídios AWS KMS no AWS Key Management ServiceGuia do desenvolvedor.

Etapa 1: atualizar a política de chave

Na política de chave, o proprietário da chave deve garantir que a política inclua duas declarações:

- A primeira instrução permite que o proprietário do bucket use a chave para descriptografar dados.
- A segunda declaração permite que o proprietário do bucket crie uma concessão para o perfil vinculado a serviço do Macie para a própria conta (o proprietário do bucket).

Na primeira declaração, o elemento `Principal` deve especificar o ARN da conta do proprietário do bucket. O array `Action` deve especificar a ação `kms:Decrypt`. Essa é a única ação do AWS KMS para a qual o Macie deve ter permissão para descriptografar um objeto que foi criptografado com a chave. Veja a seguir um exemplo dessa declaração na política para uma AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
```

```
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

No exemplo anterior:

- O campo `AWS` no elemento `Principal` especifica o ARN da conta do proprietário do bucket (111122223333). Isso permite que o proprietário do bucket execute a ação especificada na declaração de política. *123456789012* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta do proprietário do bucket.
- A matriz `Action` especifica a ação que o proprietário do bucket pode realizar usando a chave do KMS: descriptografar o texto cifrado que foi criptografado com a chave.

A segunda declaração na política de chave permite que o proprietário do bucket crie uma concessão para a função vinculada ao serviço Macie para sua conta. Na primeira declaração, o elemento `Principal` deve especificar o ARN da conta do proprietário do bucket. O array `Action` deve especificar a ação `kms:CreateGrant`. Um elemento `Condition` pode filtrar o acesso à ação `kms:CreateGrant` especificada na instrução. Veja a seguir um exemplo dessa declaração na política para uma 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"
        }
```

```
    }
}
```

No exemplo anterior:

- O campo `AWS` no elemento `Principal` especifica o ARN da conta do proprietário do bucket (111122223333). Isso permite que o proprietário do bucket execute a ação especificada na declaração de política. *123456789012* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta do proprietário do bucket.
- O array `Action` especifica a ação que o proprietário do bucket pode realizar na chave KMS — criar uma concessão para a chave.
- O elemento `Condition` usa o operador de condição `StringEquals` e a chave de condição `kms:GranteePrincipal`para filtrar o acesso à ação especificada pela declaração de política. Nesse caso, o proprietário do bucket poderá criar uma concessão somente para o `GranteePrincipal` especificado, que é o ARN do perfil vinculado a serviço do Macie para a própria conta. Nesse ARN, *111122223333* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta do proprietário do bucket.

  Se a conta do proprietário do bucket estiver em uma Região da AWS opcional, inclua também o código de região adequado no ARN do perfil vinculado a serviço do Macie. Por exemplo, se a conta estiver na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, `macie.amazonaws.com` substitua pelo ARN. `macie.me-south-1.amazonaws.com` Para obter uma lista códigos das regiões nas quais o Macie está disponível, consulte Endpoints e cotas do Amazon Macie no Referência geral da AWS.

O local em que você adiciona essa declaração a uma política de chave depende da estrutura e dos elementos que a política contém atualmente. Ao adicionar as declarações, o proprietário da chave deverá garantir que a sintaxe seja válida. As políticas de chave usam o formato JSON. Isso significa que o proprietário da chave também precisa adicionar uma vírgula antes ou depois de cada declaração, dependendo de onde ele adicionar a declaração à política.

Etapa 2: criar uma concessão

Depois que o proprietário da chave atualizar a política de chave conforme necessário, o proprietário do bucket deve criar uma concessão para a chave. A concessão delega as permissões relevantes à função vinculada ao serviço Macie da conta do proprietário do bucket. Antes de o proprietário do bucket criar a concessão, ele deve verificar se tem permissão para realizar a ação

`kms:CreateGrant` em sua conta. Essa ação permite que ele adicione uma concessão a uma AWS KMS key existente gerenciada pelo cliente.

Para criar a concessão, o proprietário do bucket pode usar a CreateGrantoperação da AWS Key Management Service API. Quando o proprietário do bucket cria a concessão, ele deve especificar os seguintes valores para os parâmetros necessários:

- `KeyId`: o ARN da chave do KMS. Para acesso entre contas a uma chave do KMS, esse valor deve ser um ARN. Não pode ser um ID de chave.
- `GranteePrincipal`: o ARN do perfil vinculada a serviço do Macie (`AWSServiceRoleForAmazonMacie`) para a conta dele. Esse valor deve ser `arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, em que *`111122223333`* é o ID da conta do proprietário do bucket.

  Se a conta dele estiver em uma região opcional, o ARN deverá incluir o código de região adequado. Por exemplo, se a conta dele estiver na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, o ARN deverá ser `arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`, onde *`111122223333`* é o ID da conta para a conta do proprietário do bucket.
- `Operations`: a ação de descriptografia do AWS KMS (`Decrypt`). Essa é a única ação do AWS KMS para a qual o Macie deve ter permissão para descriptografar um objeto que foi criptografado com a chave do KMS.

Para criar uma concessão para uma chave do KMS gerenciada pelo cliente usando a AWS Command Line Interface (AWS CLI), execute o comando create-grant. O exemplo a seguir mostra como. O exemplo está formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
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"
```

Em que:

- `key-id` especifica o ARN da chave do KMS à qual aplicar a concessão.

- `grantee-principal` especifica o ARN do perfil vinculado a serviço do Macie para a conta que tem permissão para realizar a ação especificada pela concessão. Esse valor deve corresponder ao ARN especificado pela condição `kms:GranteePrincipal` da segunda declaração na política de chave.
- `operations` especifica a ação que a concessão permite que a entidade principal especificada execute: descriptografar o texto cifrado que foi criptografado com a chave do KMS.

Se o comando for executado com sucesso, você receberá um resultado semelhante ao seguinte.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Onde `GrantToken` é uma string única, não secreta, de comprimento variável e codificada em base64 que representa a concessão que foi criada e `GrantId` é o identificador exclusivo da concessão.

Armazenamento e retenção de resultados de descoberta de dados confidenciais com o Amazon Macie

Quando você executa um trabalho de descoberta de dados confidenciais ou o Amazon Macie realiza uma descoberta automática de dados confidenciais, o Macie cria um registro de análise para cada objeto do Amazon Simple Storage Service (Amazon S3) incluído no escopo da análise. Esses registros, chamados de resultados confidenciais da descoberta de dados, registram detalhes sobre a análise de objetos individuais do S3. Isso inclui objetos nos quais o Macie não detecta dados confidenciais e, portanto, não produz descobertas, e objetos que o Macie não pode analisar devido a erros ou problemas. Se o Macie detectar dados confidenciais em um objeto, o registro incluirá dados da descoberta correspondente, bem como informações adicionais. Os resultados confidenciais da descoberta de dados fornecem registros de análise que podem ser úteis para auditorias ou investigações de privacidade e proteção de dados.

O Macie armazena seus resultados confidenciais de descoberta de dados por apenas 90 dias. Para acessar seus resultados e permitir o armazenamento e a retenção a longo prazo deles, configure o Macie para criptografar os resultados com uma chave AWS Key Management Service (AWS KMS) e armazená-los em um bucket do S3. O bucket pode servir como um repositório definitivo e de longo

prazo para todos os seus resultados confidenciais de descoberta de dados. Em seguida, você pode, se preferir, acessar e consultar os resultados nesse repositório.

Este tópico orienta você pelo processo de uso do AWS Management Console para configurar um repositório para seus resultados confidenciais de descoberta de dados. A configuração é uma combinação de um AWS KMS key que criptografa os resultados, um bucket do S3 que armazena os resultados e configurações do Macie que indicam qual chave e bucket usar. Se você preferir definir as configurações do Macie programaticamente, poderá usar a PutClassificationExportConfigurationoperação da API do Amazon Macie.

Quando você define as configurações no Macie, suas escolhas se aplicam somente à Região da AWS atual. Se você for o administrador do Macie de uma organização, suas escolhas se aplicam somente à sua conta. Eles não se aplicam a nenhuma conta de membro associada.

Se você usa o Macie em vários Regiões da AWS, defina as configurações do repositório para cada região na qual você usa o Macie. Como opção, você pode armazenar resultados de descoberta de dados confidenciais para várias regiões no mesmo bucket do S3. No entanto, observe os seguintes requisitos:

- Para armazenar os resultados de uma região que AWS habilita por padrão para Contas da AWS, como a região Leste dos EUA (Norte da Virgínia), você precisa escolher um bucket em uma região que esteja habilitada por padrão. Não é possível armazenar os resultados em um bucket em uma região opcional (região desabilitada por padrão).
- Para armazenar os resultados de uma região opcional, como a região do Oriente Médio (Bahrein), você precisa escolher um bucket na mesma região ou uma região que seja habilitada por padrão. Não é possível armazenar os resultados em um bucket em outra região opcional.

Para determinar se uma região é habilitada por padrão, consulte Regiões e endpoints no Guia de usuário do AWS Identity and Access Management . Além dos requisitos anteriores, considere também se você deseja recuperar amostras de dados confidenciais que o Macie relata em descobertas individuais. Para recuperar amostras de dados confidenciais de um objeto do S3 afetado, todos os seguintes recursos e dados devem ser armazenados na mesma região: o objeto afetado, a descoberta aplicável e o resultado correspondente da descoberta de dados confidenciais.

Tarefas

- Visão geral
- Etapa 1: verifique suas permissões

- Etapa 2: configurar o AWS KMS key
- Etapa 3: Selecione um bucket do S3

Visão geral

O Amazon Macie cria automaticamente um resultado de descoberta de dados confidenciais para cada objeto do Amazon S3 que ele analisa ou tenta analisar quando você executa um trabalho de descoberta de dados confidenciais ou quando o serviço realiza uma descoberta automática de dados confidenciais para sua conta ou organização. Isso inclui:

- Objetos nos quais o Macie detecta dados confidenciais e, portanto, também produzem descobertas de dados confidenciais.
- Objetos nos quais o Macie não detecta dados confidenciais e, portanto, não produzem descobertas de dados confidenciais.
- Objetos que o Macie não consegue analisar devido a erros ou problemas, como configurações de permissões ou uso de um arquivo ou formato de armazenamento não suportado.

Se o Macie detectar dados sigilosos em um objeto do S3, o resultado da descoberta de dados sigilosos incluirá dados da descoberta de dados sigilosos correspondente. Ele também fornece informações adicionais, como a localização de até mil ocorrências de cada tipo de dado confidencial que Macie encontrou no objeto. Por exemplo: .

- O número da coluna e da linha de uma célula ou campo em uma pasta de trabalho do Microsoft Excel, arquivo CSV ou arquivo TSV
- O caminho para um campo ou matriz em um arquivo JSON ou JSON Lines
- O número da linha de uma linha em um arquivo de texto não binário que não seja um arquivo CSV, JSON, JSON Lines ou TSV; por exemplo, um arquivo HTML, TXT ou XML
- O número da página de uma página em um arquivo Adobe Portable Document Format (PDF)
- O índice do registro e o caminho para um campo em um registro em um contêiner de objetos Apache Avro ou arquivo Apache Parquet

Se o objeto do S3 afetado for um arquivo de arquivamento, como um arquivo.tar ou .zip, o resultado da descoberta de dados confidenciais também fornecerá dados de localização detalhados para ocorrências de dados confidenciais em arquivos individuais que o Macie extrai do arquivamento. O Macie não inclui essas informações nas descobertas de dados confidenciais para arquivos

arquivados. Para relatar dados de localização, os resultados confidenciais da descoberta de dados usam um esquema JSON padronizado.

Um resultado de descoberta de dados confidenciais não inclui os dados confidenciais que Macie encontrou. Em vez disso, ele fornece um registro de análise que pode ser útil para auditorias ou investigações.

O Macie armazena seus resultados confidenciais de descoberta de dados por 90 dias. Você não pode acessá-los diretamente no console do Amazon Macie ou com a API do Amazon Macie. Em vez disso, siga as etapas deste tópico para configurar o Macie para criptografar seus resultados com um AWS KMS key que você especificar e armazenar os resultados em um bucket do S3 que você também especificar. Em seguida, o Macie grava os resultados em arquivos JSON Lines (.jsonl), adiciona os arquivos ao bucket como arquivos GNU Zip (.gz) e criptografa os dados usando a criptografia SSE-KMS. Desde 8 de novembro de 2023, o Macie também assina os objetos resultantes do S3 com uma AWS KMS key de código de autenticação de mensagens por hash (HMAC).

Após você configurar o Macie para armazenar os resultados de descoberta de dados confidenciais em um bucket do S3, o bucket poderá servir como um repositório definitivo e de longo prazo para os resultados. Em seguida, você pode, se preferir, acessar e consultar os resultados nesse repositório.

> **Tip**
>
> Para obter um exemplo detalhado e instrutivo de como você pode consultar e usar resultados de descoberta de dados confidenciais para analisar e relatar possíveis riscos de segurança de dados, consulte a postagem do blog Como consultar e visualizar os resultados da descoberta de dados confidenciais do Macie com o Amazon Athena e a Amazon QuickSight no blog de segurança.AWS
> Para exemplos de consultas do Amazon Athena que você pode usar para analisar resultados confidenciais de descoberta de dados, visite o repositório Amazon Macie Results Analytics em. GitHub Esse repositório também fornece instruções para configurar o Athena para recuperar e descriptografar seus resultados e scripts para criar tabelas para os resultados.

Etapa 1: verifique suas permissões

Antes de configurar um repositório para os resultados confidenciais da descoberta de dados, verifique se você tem as permissões necessárias para criptografar e armazenar os resultados. Para verificar suas permissões, use AWS Identity and Access Management (IAM) para revisar as políticas

do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações nessas políticas com a seguinte lista de ações que você deve ter permissão para realizar para configurar o repositório.

Amazon Macie

Para Macie, verifique se você tem permissão para realizar a seguinte ação:

`macie2:PutClassificationExportConfiguration`

Essa ação permite que você adicione ou altere as configurações do repositório no Macie.

Amazon S3

Para o Amazon S3, verifique se você tem permissão para executar as seguintes ações:

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Essas ações permitem que você acesse e configure um bucket do S3 que pode servir como repositório.

AWS KMS

Para usar o console do Amazon Macie para adicionar ou alterar as configurações do repositório, verifique também se você tem permissão para realizar as seguintes ações do AWS KMS :

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

Essas ações permitem que você recupere e exiba informações sobre o AWS KMS keys para a sua conta. Em seguida, você pode escolher uma dessas chaves para criptografar os resultados confidenciais da descoberta de dados.

Se você planeja criar um novo AWS KMS key para criptografar os dados, você também precisa ter permissão para realizar as seguintes ações: `kms:CreateKeykms:GetKeyPolicy`, e. `kms:PutKeyPolicy`

Se você não tiver permissão para realizar as ações necessárias, peça ajuda ao AWS administrador antes de prosseguir para a próxima etapa.

Etapa 2: configurar o AWS KMS key

Depois de verificar suas permissões, determine quais AWS KMS key você deseja que o Macie use para criptografar seus resultados de descoberta de dados confidenciais. A chave deve ser uma chave KMS de criptografia simétrica e gerenciada pelo cliente que esteja habilitada da Região da AWS mesma forma que o bucket do S3 em que você deseja armazenar os resultados.

A chave pode ser uma existente AWS KMS key de sua própria conta ou uma existente AWS KMS key de propriedade de outra conta. Se você planeja usar uma nova chave para as descobertas do KMS, crie uma chave antes de prosseguir. Se você desejar usar uma chave existente de propriedade de outra conta da, obtenha o nome do recurso da Amazon (ARN) da chave. Você precisará inserir esse ARN ao definir as configurações de repositório no Macie. Para obter informações sobre como criar e revisar as configurações das chaves KMS, consulte Gerenciando chaves no Guia do desenvolvedor do AWS Key Management Service .

> **Note**
>
> A chave pode estar AWS KMS key em um armazenamento de chaves externo. No entanto, a chave pode, então, ser mais lenta e menos confiável do que uma chave totalmente gerenciada no AWS KMS. Você pode reduzir esse risco armazenando os resultados de descoberta de dados confidenciais em um bucket do S3 configurado para usar a chave como uma chave de bucket do S3. Isso reduz o número de solicitações do AWS KMS que devem ser feitas para criptografar os resultados confidenciais da descoberta de dados.
> Para obter informações sobre o uso de chaves KMS em repositórios de chaves externos, consulte Repositórios de chaves externos no Guia do desenvolvedor do AWS Key Management Service . Para obter informações sobre o uso de chaves de bucket do S3, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Depois de determinar qual chave KMS você deseja que o Macie use, dê permissão ao Macie para usar a chave. Caso contrário, o Macie não conseguirá criptografar nem armazenar seus resultados no repositório. Para dar permissão ao Macie para usar a chave, atualize a política de chaves para a chave. Para obter informações detalhadas sobre políticas de chaves e gerenciamento do acesso às

chaves do KMS, consulte Políticas de chave no AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

Atualizar a política de chaves

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. Selecione a chave que deseja que o Macie use para criptografar os resultados de descoberta de dados confidenciais.
4. Na guia Política de chave, selecione Editar.
5. Copie a seguinte instrução para sua área de transferência e adicione-a à 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/*"
             ]
         }
    }
}
```

Ao adicionar a instrução, verifique se a sintaxe é válida. As políticas usam o formato JSON. Isso significa que você também precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a instrução à política. Se você adicionar a instrução como a última instrução, adicione uma vírgula após o colchete de fechamento para a instrução anterior.

Se você adicioná-la como a primeira instrução ou adicioná-la entre duas instruções existentes, adicione uma vírgula após o colchete de fechamento para a instrução.

6. Atualize a instrução com os valores corretos para seu ambiente:

   - Nos campos `Condition`, substitua os valores do espaço reservado, onde:
     - *`111122223333`* é o ID da sua Conta da AWS.
     - A *`região`* é a região Região da AWS em que você está usando o Macie e deseja permitir que o Macie use a chave.

       Se você usa o Macie em várias regiões e deseja permitir que o Macie use a chave em outras regiões, adicione condições `aws:SourceArn` para cada região adicional. Por exemplo: .

       ```
       "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, você pode permitir que o Macie use a chave em todas as regiões. Para fazer isso, substitua o valor do espaço reservado pelo caractere curinga (*). Por exemplo: .

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:*:111122223333:export-configuration:*",
           "arn:aws:macie2:*:111122223333:classification-job/*"
       ]
       ```

   - Se você estiver usando o Macie em uma região opcional, adicione o código de região adequado ao valor do campo `Service`. Por exemplo, se você estiver usando Macie na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, substitua `macie.amazonaws.com` por `macie.me-south-1.amazonaws.com`. Para obter uma lista de regiões onde o Macie está disponível atualmente e o código de região de cada uma, consulte Endpoints e cotas do Amazon Macie no arquivo Referência geral da AWS.

Observe que os campos `Condition` usam duas chaves de condição globais do IAM:

- aws: SourceAccount — Essa condição permite que o Macie execute as ações especificadas somente para sua conta. Mais especificamente, ele determina qual conta pode realizar as ações especificadas para os recursos e ações especificadas pela condição `aws:SourceArn`.

  Para permitir que o Macie execute as ações especificadas para contas adicionais, adicione o ID da conta de cada conta adicional a essa condição. Por exemplo: .

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

- aws: SourceArn — Essa condição impede que outras pessoas Serviços da AWS executem as ações especificadas. Também impede que Macie use a chave enquanto realiza outras ações na sua conta. Em outras palavras, isso permite que o Macie criptografe objetos do S3 com a chave somente se os objetos forem resultados de descoberta de dados confidenciais e somente se esses resultados forem para descoberta automatizada de dados confidenciais ou trabalhos de descoberta de dados confidenciais criados pela conta especificada na região especificada.

  Para permitir que o Macie execute as ações especificadas para contas adicionais, adicione ARNs para cada conta adicional a essa condição. Por exemplo: .

  ```
  "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/*"
  ]
  ```

  As contas especificadas pelas condições `aws:SourceAccount` e `aws:SourceArn` devem ser correspondentes.

  Essas condições ajudam a evitar que Macie seja usada como representante confusa durante transações com AWS KMS. Embora não o recomendemos, você pode remover essas condições da instrução.

7. Ao terminar de adicionar e atualizar a instrução, selecione Salvar alterações.

Etapa 3: Selecione um bucket do S3

Depois de verificar suas permissões e configurar o AWS KMS key, você estará pronto para especificar qual bucket do S3 deseja usar como repositório para seus resultados confidenciais de descoberta de dados. Você tem duas opções:

- Use um novo bucket do S3 criado pelo Macie — Se você escolher essa opção, o Macie criará automaticamente um novo bucket do S3 no atual Região da AWS para os resultados da sua descoberta. O Macie também aplica uma política de bucket ao bucket. A política permite que o Macie adicione objetos ao bucket. Isso também exige que os objetos sejam criptografados com a AWS KMS key que você especifica, usando a criptografia SSE-KMS. Para revisar a política, escolha Visualizar política no console do Amazon Macie depois de especificar um nome para o bucket e a chave do KMS que será utilizada.
- Use um bucket do S3 existente criado por você — Se você preferir armazenar os resultados da descoberta em um determinado bucket do S3 criado por você, crie o bucket antes de continuar. Em seguida, verifique as configurações do bucket e atualize a política do bucket para garantir que o Macie possa adicionar objetos ao bucket. Este tópico explica quais configurações verificar e como atualizar a política. Ele também fornece exemplos de instruções a serem adicionadas à política.

As seções a seguir dão instruções para cada opção. Escolha a seção da opção que deseja.

Use um novo bucket S3 criado por Macie

Se você preferir usar um novo bucket do S3 que o Macie cria para você, a etapa final do processo é definir as configurações do repositório no Macie.

Para definir as configurações do repositório no Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Resultados da descoberta.
3. Em Repositório para resultados de descoberta de dados confidenciais, selecione Criar bucket.
4. Na caixa Criar um bucket, insira um nome para o bucket.

   O nome deve ser exclusivo em todos os buckets no S3. Além disso, o nome pode consistir apenas em letras minúsculas, números, pontos (.) e hífens (-). Para requisitos adicionais de nomenclatura, consulte Regras de nomenclatura de buckets no Guia do usuário do Amazon Simple Storage Service.

5. Expanda a seção Advanced.
6. (Opcional) Para especificar um prefixo a ser usado no caminho para um local no bucket, insira o prefixo na caixa Prefixo do resultado da descoberta de dados.

   Quando você insere um valor, o Macie atualiza o exemplo abaixo da caixa para mostrar o caminho até o local do bucket onde ele armazenará os resultados da descoberta.
7. Em Bloquear todo o acesso público, selecione Sim para ativar todas as configurações de bloqueio de acesso público para o bucket.

   Para obter informações sobre essas configurações, consulte Blocking public access to your Amazon S3 storage do Guia do usuário do Amazon Simple Storage Service.
8. Em Configurações de criptografia, especifique o AWS KMS key que deseja que o Macie use para criptografar os resultados:

   - Para usar uma chave da sua própria conta, selecione Selecione uma chave em sua conta. Em seguida, na lista AWS KMS key, selecione a chave a ser usada. A lista exibe chaves KMS de criptografia simétrica e gerenciadas pelo cliente para sua conta.
   - Para usar uma chave que outra conta possui, selecione Inserir o ARN de uma chave de outra conta. Em seguida, na caixa AWS KMS key ARN, insira o nome do recurso da Amazon (ARN) da chave a ser utilizada — por exemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.
9. Após terminar de inserir configurações, escolha Salvar.

   O Macie testa as configurações para verificar se elas estão corretas. Se alguma configuração estiver incorreta, o Macie exibirá uma mensagem de erro para ajudar a resolver o problema.

Depois de salvar as configurações do repositório, o Macie adiciona os resultados de descoberta existentes dos 90 dias anteriores ao repositório. Macie também começa a adicionar novos resultados de descoberta ao repositório.

Use um bucket do S3 existente que você criou

Se você preferir armazenar seus resultados confidenciais de descoberta de dados em um determinado bucket do S3, crie e configure o bucket antes de definir as configurações do repositório no Macie. Ao criar o bucket, observe os seguintes requisitos:

- Se você habilitar o bloqueio de objetos para o bucket, precisará desabilitar a configuração de retenção padrão para esse recurso. Caso contrário, o Macie não poderá adicionar os resultados de

descoberta ao bucket. Para obter informações sobre esta configuração, consulte Usar o S3 Object Lock no Guia do usuário do Amazon Simple Storage Service.

- Para armazenar os resultados da descoberta em uma região habilitada por padrão para Contas da AWS, como a região Leste dos EUA (Norte da Virgínia), o bucket precisa estar em uma região habilitada por padrão. Não é possível armazenar os resultados em um bucket em uma região opcional (região desabilitada por padrão).
- Para armazenar seus resultados de descoberta de uma região opcional, como a região do Oriente Médio (Bahrein), o bucket precisa estar na mesma região ou em uma região que seja habilitada por padrão. Não é possível armazenar os resultados em um bucket em outra região opcional.

Para determinar se uma região é habilitada por padrão, consulte Regiões e endpoints no Guia de usuário do AWS Identity and Access Management .

Depois de criar o bucket, atualize a política do bucket para permitir que o Macie recupere informações sobre o bucket e adicione objetos ao bucket. Em seguida, você pode definir as configurações do repositório no Macie.

Como atualizar a política de bucket para o bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o bucket no qual você deseja armazenar os resultados da descoberta.
3. Escolha a aba Permissions.
4. Na seção Bucket policy, selecione Edit.
5. Copie o exemplo de política a seguir para a área de transferência:

```
{
    "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. Cole o exemplo de política no editor Política do bucket no console do Amazon S3.
7. Atualize o exemplo de política com os valores corretos para seu ambiente:
   - Na instrução opcional que nega cabeçalhos de criptografia incorretos:
     - *myBucketName*Substitua pelo nome do bucket.
     - Na `StringNotEquals` condição, substitua *ARN:aws:kms:region:111122223333:key/kms KeyId* pelo Amazon Resource Name (ARN) do a ser usado para criptografar os resultados da descoberta. AWS KMS key
   - Em todas as outras instruções, substitua os valores do espaço reservado, onde:

- *myBucketName*é o nome do bucket.
- *111122223333* é o ID da sua Conta da AWS.
- A *região* é a Região da AWS em que você está usando o Macie e deseja permitir que o Macie adicione resultados de descoberta ao bucket.

  Se você usa o Macie em várias regiões e deseja permitir que o Macie adicione resultados ao bucket para regiões adicionais, adicione condições `aws:SourceArn` para cada região adicional. Por exemplo: .

  ```
  "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, você pode permitir que o Macie adicione resultados ao bucket para todas as regiões nas quais você usa o Macie. Para fazer isso, substitua o valor do espaço reservado pelo caractere curinga (*). Por exemplo: .

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:*:111122223333:export-configuration:*",
      "arn:aws:macie2:*:111122223333:classification-job/*"
  ]
  ```

- Se você estiver usando o Macie em uma região opcional, adicione o código de região adequado ao valor do campo `Service` em cada declaração que especifica a entidade principal de serviço do Macie. Por exemplo, se você estiver usando o Macie na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, `macie.amazonaws.com` substitua por em cada instrução aplicável. `macie.me-south-1.amazonaws.com` Para obter uma lista de regiões onde o Macie está disponível atualmente e o código de região de cada uma, consulte Endpoints e cotas do Amazon Macie no arquivo Referência geral da AWS.

Observe que o exemplo de política inclui declarações que permitem ao Macie determinar em qual região o bucket reside (`GetBucketLocation`) e adicionar objetos ao bucket (`PutObject`). Essas instruções definem condições que usam duas chaves de condição globais do IAM:

- aws: SourceAccount — Essa condição permite que o Macie adicione resultados confidenciais de descoberta de dados ao bucket somente para sua conta. Isso impede que o Macie adicione resultados de descoberta de outras contas ao bucket. Mais especificamente, a condição especifica qual conta pode usar o bucket para os recursos e ações especificados pela condição `aws:SourceArn`.

  Para armazenar resultados de contas adicionais no bucket, adicione o ID da conta de cada conta adicional a essa condição. Por exemplo: .

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

- aws: SourceArn — Essa condição restringe o acesso ao bucket com base na origem dos objetos que estão sendo adicionados ao bucket. Isso impede que outras Serviços da AWS pessoas adicionem objetos ao bucket. Isso também impede que o Macie adicione objetos ao bucket enquanto realiza outras ações na sua conta. Mais especificamente, a condição permite que o Macie adicione objetos ao bucket somente se os objetos forem resultados de descoberta de dados confidenciais e somente se esses resultados forem para descoberta automatizada de dados confidenciais ou trabalhos de descoberta de dados confidenciais criados pela conta especificada na região especificada.

  Para permitir que o Macie execute as ações especificadas para contas adicionais, adicione ARNs para cada conta adicional a essa condição. Por exemplo: .

  ```
  "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/*"
  ]
  ```

  As contas especificadas pelas condições `aws:SourceAccount` e `aws:SourceArn` devem corresponder.

  Ambas as condições ajudam a evitar que Macie seja usado como um representante confuso durante transações com o Amazon S3. Embora não seja recomendável, você pode remover essas condições da política de bucket.

8. Quando terminar de atualizar a política do bucket, escolha Salvar alterações.

Agora é possível definir as configurações do repositório no Macie.

Para definir as configurações do repositório no Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, em Configurações, selecione Resultados da descoberta.
3. Em Repositório para resultados de descoberta de dados confidenciais, selecione Bucket existente.
4. Em Escolher um bucket, selecione o bucket no qual você deseja armazenar os resultados de descoberta.
5. (Opcional) Para especificar um prefixo a ser usado no caminho para um local no bucket, expanda a seção Avançado. Em seguida, em Prefixo do resultado da descoberta de dados, insira o prefixo a ser usado.

   Quando você insere um valor, o Macie atualiza o exemplo abaixo da caixa para mostrar o caminho até o local do bucket onde ele armazenará os resultados da descoberta.
6. Em Configurações de criptografia, especifique o AWS KMS key que deseja que o Macie use para criptografar os resultados:

   - Para usar uma chave da sua própria conta, selecione Selecione uma chave em sua conta. Em seguida, na lista AWS KMS key, selecione a chave a ser usada. A lista exibe chaves KMS de criptografia simétrica e gerenciadas pelo cliente para sua conta.
   - Para usar uma chave que outra conta possui, selecione Inserir o ARN de uma chave de outra conta. Em seguida, na caixa AWS KMS key ARN, insira o ARN da chave a ser usada — por exemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.
7. Após terminar de inserir configurações, selecione Salvar.

   O Macie testa as configurações para verificar se elas estão corretas. Se alguma configuração estiver incorreta, o Macie exibirá uma mensagem de erro para ajudar a resolver o problema.

Depois de salvar as configurações do repositório, o Macie adiciona os resultados de descoberta existentes dos 90 dias anteriores ao repositório. Macie também começa a adicionar novos resultados de descoberta ao repositório.

> **Note**
>
> Se você alterar posteriormente a configuração Prefixo do resultado da descoberta de dados, atualize também a política de bucket no Amazon S3. As declarações de política que especificam o caminho anterior devem especificar o novo caminho. Caso contrário, o Macie não terá permissão para adicionar os resultados de descoberta ao bucket.

> **Tip**
>
> Para reduzir os custos de criptografia do lado do servidor, configure também o bucket do S3 para usar uma chave do bucket do S3 e especifique a AWS KMS key que você configurou para criptografia dos resultados confidenciais da descoberta de dados. O uso de uma chave de bucket do S3 reduz o número de chamadas para AWS KMS, o que pode reduzir os custos da AWS KMS solicitação. Se a chave KMS estiver em um armazenamento de chaves externo, o uso de uma chave de bucket do S3 também pode minimizar o impacto no desempenho do uso da chave. Para sabre mais, consulte Redução do custo do SSE-KMS com chaves de bucket do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Classes e formatos de armazenamento suportados pelo Amazon Macie

Para ajudá-lo a descobrir dados confidenciais em seu conjunto de dados do Amazon Simple Storage Service (Amazon S3), o Amazon Macie oferece suporte à maioria das classes de armazenamento do Amazon S3 e a uma grande variedade de formatos de arquivo e armazenamento. Essa compatibilidade se aplica ao uso de identificadores de dados gerenciados e ao uso de identificadores de dados personalizados para analisar objetos do S3.

Para que o Macie analise um objeto do S3, o objeto precisa estar armazenado diretamente no bucket de uso geral do Amazon S3 usando uma classe de armazenamento compatível. O objeto também precisa usar um formato de arquivo ou armazenamento compatível. Os tópicos desta seção listam as classes de armazenamento e os formatos de arquivo e armazenamento que o Macie suporta atualmente.

> **Tip**
>
> Embora o Macie seja otimizado para o Amazon S3, você pode usá-lo para descobrir dados confidenciais em recursos que você atualmente armazena em outro lugar. Você pode fazer isso movendo os dados para o Amazon S3 temporariamente ou permanentemente. Por exemplo, exporte os snapshots do Serviço do banco de dados relacional Amazon ou do Amazon Aurora para o Amazon S3 no formato Apache Parquet. Ou exporte uma tabela do Amazon DynamoDB para o Amazon S3. Em seguida, você pode criar um trabalho confidencial de descoberta de dados para analisar os dados no Amazon S3.

Tópicos

Classes de armazenamento do Amazon S3 compatíveis

Para a descoberta de dados confidenciais, o Amazon Macie oferece suporte às seguintes classes de armazenamento do Amazon S3:

- Redundância reduzida (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 não analisa objetos do S3 que usem outras classes de armazenamento do Amazon S3, como o S3 Glacier Deep Archive ou S3 Express One Zone. Além disso, o Macie não analisa objetos que estejam armazenados em buckets de diretório do Amazon S3.

Se você configurar um trabalho confidencial de descoberta de dados para analisar objetos do S3 que não usam uma classe de armazenamento compatível do Amazon S3, o Macie ignora esses objetos quando o trabalho é executado. O Macie não tenta recuperar ou analisar dados nos objetos — os objetos são tratados como objetos inclassificáveis. Um objeto inclassificável é um objeto que não usa

uma classe de armazenamento compatível ou um formato de arquivo ou armazenamento compatível. O Macie analisa somente os objetos que usam uma classe de armazenamento e um arquivo ou formato de armazenamento compatível.

Da mesma forma, se você configurar o Macie para realizar a descoberta automatizada de dados confidenciais, objetos inclassificáveis não serão elegíveis para seleção e análise. O Macie seleciona somente os objetos que usam uma classe de armazenamento do Amazon S3 compatível e um arquivo ou formato de armazenamento compatível.

Para identificar buckets do S3 que contêm objetos inclassificáveis, você pode filtrar seu inventário de buckets do S3. Para cada bucket em seu inventário, há campos que relatam o número e o tamanho total de armazenamento de objetos inclassificáveis no bucket.

Para obter informações detalhadas sobre as classes de armazenamento que o Amazon S3 fornece, consulte Usando classes de armazenamento do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Formatos de arquivo e armazenamento suportados

Quando o Amazon Macie analisa um objeto do S3, o Macie recupera a versão mais recente do objeto do Amazon S3 e, em seguida, realiza uma inspeção profunda do conteúdo do objeto. Essa inspeção leva em consideração o formato de arquivo ou armazenamento dos dados. O Macie pode analisar dados em vários formatos diferentes, incluindo formatos de compactação e arquivamento comumente usados.

Quando o Macie analisa dados em um arquivo compactado ou arquivado, o Macie inspeciona o arquivo completo e o conteúdo do arquivo. Para inspecionar o conteúdo do arquivo, o Macie descompacta o arquivo e, em seguida, inspeciona cada arquivo extraído que usa um formato compatível. O Macie pode fazer isso para até 1.000.000 de arquivos e até uma profundidade aninhada de 10 níveis. Para obter informações sobre cotas adicionais que se aplicam à descoberta de dados confidenciais, consulte Cotas do Amazon Macie.

A tabela a seguir lista e descreve os tipos de arquivos e formatos de armazenamento que o Macie pode analisar para detectar dados confidenciais. Para cada tipo suportado, a tabela também lista as extensões de nome de arquivo aplicáveis.

Tipo de arquivo ou armazenamento	Descrição	Extensões de nome de arquivo
Big data	Contêineres de objetos Apache Avro e arquivos Apache Parquet	.avro, .parquet
compactação ou arquivamento	Arquivos compactados GNU Zip, arquivos TAR e arquivos compactados ZIP	.gz, .gzip, .tar, .zip
Documento	Arquivos em formato de documento portátil da Adobe, pastas de trabalho do Microsoft Excel e documentos do Microsoft Word	.doc, .docx, .pdf, .xls, .xlsx
Mensagem de e-mail	Arquivos de correio eletrônico cujo conteúdo está em conformidade com os requisitos especificados por uma RFC da IETF para mensagens de correio eletrônico, como a RFC 2822	.eml
Texto	Arquivos de texto não binários, como arquivos de valores separados por vírgula (CSV), arquivos HTML (Hypertext Markup Language), arquivos JavaScript Object Notation (JSON), arquivos de linhas JSON, documentos de texto sem formatação, arquivos de valores separados por tabulação (TSV) e	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, . e outros (dependendo do tipo de arquivo de texto não binário)

Tipo de arquivo ou armazenamento	Descrição	Extensões de nome de arquivo
	arquivos XML (Extensible Markup Language)	

O Macie não analisa dados em imagens, áudio, vídeo e outros tipos de conteúdo multimídia.

Se você configurar um trabalho de descoberta de dados confidenciais para analisar objetos do S3 que não usam uma classe de armazenamento compatível do Amazon S3, o Macie ignora esses objetos quando o trabalho é executado. O Macie não tenta recuperar ou analisar dados nos objetos — os objetos são tratados como objetos inclassificáveis. Um objeto inclassificável é um objeto que não usa uma classe de armazenamento compatível do Amazon S3 ou um formato de arquivo ou armazenamento compatível. O Macie analisa somente os objetos que usam uma classe de armazenamento e um arquivo ou formato de armazenamento compatível.

Da mesma forma, se você configurar o Macie para realizar a descoberta automatizada de dados confidenciais, objetos inclassificáveis não serão elegíveis para seleção e análise. O Macie seleciona somente os objetos que usam uma classe de armazenamento do Amazon S3 compatível e um arquivo ou formato de armazenamento compatível.

Para identificar buckets do S3 que contêm objetos inclassificáveis, você pode filtrar seu inventário de buckets do S3. Para cada bucket em seu inventário, há campos que relatam o número e o tamanho total de armazenamento de objetos inclassificáveis no bucket.

Analisando as descobertas do Amazon Macie

O Amazon Macie gera descobertas quando detecta possíveis violações de políticas ou problemas com a segurança ou a privacidade de seus buckets do Amazon Simple Storage Service (Amazon S3) ou detecta dados confidenciais em objetos do S3. Uma descoberta é um relatório detalhado de um possível problema do ou dados confidenciais encontrados por Macie. Cada descoberta fornece detalhes como uma classificação de gravidade, informações sobre o recurso afetado e quando o Macie encontrou os dados ou o problema. O Macie armazena sua política e as descobertas de dados confidenciais por 90 dias.

Você pode revisar, analisar e gerenciar suas descobertas das seguintes maneiras.

Console Amazon Macie

: As páginas de descobertas no console do Amazon Macie listam suas descobertas e fornecem informações detalhadas para descobertas individuais. Essas páginas também fornecem opções para agrupar, filtrar e classificar descobertas e para criar e gerenciar regras de supressão. As regras de supressão podem ajudá-lo a simplificar a análise das descobertas.

API do Amazon Macie

: Com a API do Amazon Macie, você pode consultar e recuperar dados de descobertas usando uma ferramenta de linha de comando da AWS ou um SDK da AWS, ou enviando solicitações HTTPS diretamente para o Macie. Para consultar os dados, você envia uma solicitação para a API do Amazon Macie e usa parâmetros compatíveis para especificar quais descobertas você deseja recuperar. Depois de enviar sua solicitação, o Macie retorna os resultados em uma resposta JSON. Em seguida, você pode passar os resultados para outro serviço ou aplicativo para uma análise mais aprofundada, armazenamento de longo prazo ou relatórios. Para obter mais informações, consulte a Referência da API do Amazon Macie.

Amazon EventBridge

: Para apoiar ainda mais a integração com outros serviços e sistemas, como sistemas de monitoramento ou gerenciamento de eventos, Macie publica as descobertas no Amazon EventBridge como eventos. O EventBridge, anteriormente Amazon CloudWatch Events, é um serviço de barramento de eventos com tecnologia sem servidor que pode fornecer um fluxo de dados em tempo real de suas próprias aplicações, de aplicações de software como serviço (SaaS) e Serviços da AWS, como o Macie. Ele pode encaminhar esses dados para destinos como funções AWS Lambda, tópicos do Amazon Simple Notification Service e fluxos do Amazon

Kinesis para processamento adicional e automatizado. O uso do EventBridge também ajuda a garantir a retenção de longo prazo dos dados das descobertas. Para saber mais sobre o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

Macie publica automaticamente eventos no EventBridge para novas descobertas. Ele também publica eventos automaticamente para ocorrências subsequentes de descobertas de políticas existentes. Como os dados das descobertas são estruturados como eventos do EventBridge, você pode monitorar, analisar e agir de acordo com as descobertas com mais facilidade usando outros serviços e ferramentas. Por exemplo, você pode usar o EventBridge para enviar automaticamente tipos específicos de novas descobertas para uma função AWS Lambda que, por sua vez, processa e envia os dados para seu sistema de gerenciamento de incidentes e eventos de segurança (SIEM). Se você integrar as Notificações de Usuários da AWS com o Macie, também poderá usar os eventos para ser notificado das descobertas automaticamente por meio dos canais de entrega que você especificar. Para saber mais sobre o uso de eventos do EventBridge para monitorar e processar descobertas, consulte Integração do Amazon Macie com o Amazon Eventbridge.

AWS Security Hub

Para uma análise adicional e mais ampla da postura de segurança da sua organização, você também pode publicar as descobertas em AWS Security Hub. O Security Hub é um serviço que coleta dados de segurança dos Serviços da AWS e soluções de segurança AWS Partner Network suportadas para fornecer uma visão abrangente do estado de segurança em todo o ambiente da AWS. O Security Hub também ajuda a verificar o ambiente de acordo com os padrões e as melhores práticas do setor de segurança. Para saber mais sobre o Security Hub, consulte o Guia do usuário da AWS Security Hub. Para saber mais sobre o uso do Security Hub para monitorar e processar descobertas, consulte Integração do Amazon Macie com o AWS Security Hub.

Além das descobertas, o Macie cria resultados de descoberta de dados confidenciais para objetos do S3 que ele analisa para descobrir dados confidenciais. Um resultado de descoberta de dados confidenciais é um registro de detalhes sobre a análise de um objeto. Isso inclui objetos nos quais o Macie não encontra dados confidenciais e, portanto, não produz descobertas, e objetos que o Macie não pode analisar devido a erros ou problemas. Os resultados confidenciais da descoberta de dados fornecem registros de análise que podem ser úteis para auditorias ou investigações de privacidade e proteção de dados. Você não pode acessar resultados confidenciais da descoberta de dados diretamente no console do Amazon Macie ou com a API do Amazon Macie. Em vez disso, você configura o Macie para armazenar os resultados em um bucket do S3. Em seguida, você pode, opcionalmente, acessar e consultar os resultados nesse bucket. Para saber como configurar o Macie

para armazenar os resultados, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Tópicos

Tipos de descobertas do Amazon Macie

O Amazon Macie gera duas categorias de descobertas: descobertas de políticas e descobertas de dados confidenciais. Uma descoberta de políticas é um relatório detalhado de uma possível violação da política ou problema na segurança ou na privacidade de um bucket do Amazon Simple Storage Service (Amazon S3). O Macie gera descobertas de políticas como parte de suas atividades contínuas para avaliar e monitorar seus buckets do S3 para fins de segurança e controle de acesso. Uma descoberta de dados confidenciais é um relatório detalhado de dados confidenciais que o Macie detectou em um objeto do S3. O Macie gera descobertas de dados confidenciais como parte das atividades que ele executa quando você executa trabalhos de descoberta de dados confidenciais ou realiza a descoberta automática de dados confidenciais na sua conta.

Dentro de cada categoria, há tipos específicos. O tipo de descoberta fornece informações sobre a natureza do problema ou dos dados confidenciais encontrados pelo Macie. Cada descoberta fornece detalhes como uma classificação de gravidade, informações sobre o recurso afetado e informações, como quando e como o Macie encontrou o problema ou os dados confidenciais. A gravidade e os detalhes de cada descoberta variam de acordo com o tipo e a natureza da descoberta.

Tópicos

> **Tip**
>
> Para explorar e aprender sobre as diferentes categorias e tipos de descobertas que o Macie pode gerar, crie amostras de descobertas. Amostras de descobertas usam dados de exemplo e valores de espaço reservado para demonstrar os tipos de informações que cada tipo de descoberta pode conter.

Tipos de descobertas de políticas

O Amazon Macie gera uma descoberta de políticas quando as políticas ou configurações de um bucket do S3 são alteradas de uma forma que reduz a segurança ou a privacidade do bucket e dos objetos do bucket. Para obter informações sobre como o Macie detecta essas alterações, consulte Como o Macie monitora a segurança de dados do Amazon S3.

O Macie gera uma descoberta de política somente se a alteração ocorrer após você habilitar o Macie para seu Conta da AWS. Por exemplo, se as configurações de bloqueio de acesso público forem desativadas para um bucket do S3 depois que você habilitar o Macie, o Macie gerará uma descoberta BlockPublicAccessDisabledPolicy:iamUser/S3 para o bucket. No entanto, se as configurações de bloqueio de acesso público foram desativadas para um bucket quando você habilitou o Macie e elas continuarem desativadas, o Macie não gerará uma descoberta BlockPublicAccessDisabledPolicy:iamUser/s3 para o bucket.

Descobertas atualizadas – Se o Macie detectar uma ocorrência posterior de uma descoberta de política existente, o Macie atualizará a descoberta existente adicionando detalhes sobre a ocorrência posterior e incrementando a contagem de ocorrências. O Macie armazena as descobertas da política por 90 dias.

O Macie pode gerar os seguintes tipos de descobertas de políticas para um bucket do S3.

Policy:IAMUser/S3BlockPublicAccessDisabled

Todas as configurações de bloqueio de acesso público ao bloco no nível de bucket foram desabilitadas para o bucket. O acesso ao bucket é controlado pelas configurações de bloqueio de acesso público para a conta, pelas listas de controle de acesso (ACLs) e pela política de buckets para o bucket.

Para saber mais sobre as configurações de bloqueio de acesso público para buckets do S3, consulte Bloqueio do acesso público ao seu armazenamento no Amazon S3 no Guia do Usuário do Amazon Simple Storage Service.

Policy:IAMUser/S3BucketEncryptionDisabled

As configurações de criptografia padrão do bucket foram redefinidas para o comportamento padrão de criptografia do Amazon S3, que consiste em criptografar novos objetos automaticamente com uma chave gerenciada do Amazon S3.

A partir de 5 de janeiro de 2023, o Amazon S3 aplica automaticamente a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para objetos adicionados aos buckets. Opcionalmente, você pode definir as configurações de criptografia padrão de um bucket para, em vez disso, usar a criptografia do lado do servidor com uma AWS KMS chave (SSE-KMS) ou a criptografia do lado do servidor de camada dupla com uma chave (DSSE-KMS). AWS KMS Para saber mais sobre as configurações e opções de criptografia padrão para buckets S3, consulte Como definir o comportamento padrão de criptografia do lado do servidor para buckets S3 no Guia do usuário do Amazon Simple Storage Service.

Se o Macie gerou esse tipo de descoberta antes de 5 de janeiro de 2023, a descoberta indica que as configurações de criptografia padrão foram desativadas para o bucket afetado. Isso significava que as configurações do bucket não especificavam o comportamento padrão de criptografia do lado do servidor para novos objetos. A capacidade de desativar as configurações de criptografia padrão para um bucket não é mais suportada pelo Amazon S3.

Policy:IAMUser/S3BucketPublic

Uma política de bucket ou ACL para o bucket foi alterada para permitir o acesso de usuários anônimos ou de todas as identidades AWS Identity and Access Management (IAM) autenticadas.

Para saber mais sobre políticas de buckets e ACLs para buckets S3, consulte o Gerenciamento de identidade e acesso no Amazon S3 no Guia do Usuário do Amazon Simple Storage Service.

Policy:IAMUser/S3BucketReplicatedExternally

A replicação foi habilitada e configurada para replicar objetos do bucket para um bucket de uma Conta da AWS que é externa e não faz parte da sua organização. Uma organização é um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio do AWS Organizations ou por convite do Macie.

Em certas condições, o Macie pode gerar esse tipo de descoberta para um bucket que não está configurado para replicar objetos em um bucket para uma Conta da AWS externa. Isso pode ocorrer se o bucket de destino tiver sido criado em um local Região da AWS diferente durante as 24 horas anteriores, depois que o Macie recuperou os metadados do bucket e do objeto do Amazon S3 como parte do ciclo diário de atualização. Para investigar a descoberta, comece atualizando seus dados de inventário. Em seguida, revise os detalhes do bucket. Os detalhes indicam se o bucket está configurado para replicar objetos em outros buckets. Se o bucket estiver configurado para fazer isso, os detalhes incluirão o ID cada conta que possui um bucket de destino.

Para saber mais sobre as configurações de replicação para buckets do S3, consulte a Replicação de objetos no Guia do usuário do Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedExternally

Uma política de ACL ou bucket para esse bucket foi alterada para permitir que o bucket fosse compartilhado com uma Conta da AWS externa à sua organização (ou que não faz parte dela). Uma organização é um conjunto de contas do Macie que são gerenciadas centralmente como um grupo de contas relacionadas por meio do AWS Organizations ou por convite do Macie.

Em certos casos, o Macie pode gerar esse tipo de descoberta para um bucket que não é compartilhado com uma conta AWS externa. Isso pode ocorrer se o Macie não conseguir avaliar totalmente a relação entre o elemento `Principal` na política do bucket e determinadas chaves de contexto de condição global AWS ou chaves de condição do Amazon S3 no elemento `Condition` da política. As chaves de condição aplicáveis são: `aws:PrincipalAccount`, `aws:PrincipalArn`, `aws:PrincipalOrgID`, `aws:PrincipalOrgPaths`, `aws:PrincipalTag`, `aws:PrincipalType`, `aws:SourceAccount`, `aws:SourceArn`, `aws:userid`, `s3:DataAccessPointAccount` e `s3:DataAccessPointArn`. Recomendamos que você analise a política do bucket para determinar se esse acesso é intencional e seguro.

Para saber mais sobre políticas de buckets e ACLs para buckets S3, consulte o Gerenciamento de identidade e acesso no Amazon S3 no Guia do Usuário do Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedWithCloudFront

A política do bucket foi alterada para permitir que o bucket seja compartilhado com uma identidade de acesso de CloudFront origem da Amazon (OAI), um controle de acesso de CloudFront origem (OAC) ou um CloudFront OAI e um OAC. CloudFront Um CloudFront OAI ou OAC permite que os usuários acessem os objetos de um bucket por meio de uma ou mais distribuições especificadas CloudFront.

Para saber mais sobre CloudFront OAIs e OACs, consulte Restringir o acesso a uma origem do Amazon S3 no Amazon Developer Guide. CloudFront

> **Note**
>
> Em certos casos, o Macie gera uma descoberta policy:iamuser/s3 em vez de uma BucketSharedExternally descoberta policy:iamuser/s3 para um bucket. BucketSharedWithCloudFront Nesses casos:
>
> - O bucket é compartilhado com um Conta da AWS externo à sua organização, além de um CloudFront OAI ou OAC.
> - A política do bucket especifica um ID de usuário canônico, em vez do Amazon Resource Name (ARN), de um OAI. CloudFront
>
> Isso produz a descoberta de uma política de severidade mais alta para o bucket.

Tipos de descobertas de dados confidenciais

O Macie gera uma descoberta de dados confidenciais ao detectar dados confidenciais em um objeto do S3 que ele analisa para descobrir dados confidenciais. Isso inclui a análise que o Macie realiza quando você executa um trabalho de descoberta de dados confidenciais e quando ele executa uma descoberta automatizada de dados confidenciais.

Por exemplo, se você criar e executar um trabalho confidencial de descoberta de dados e o Macie detectar números de contas bancárias em um objeto do S3, o Macie gerará uma descoberta financeira do objeto: SensitiveData S3Object/Financial. Da mesma forma, se o Macie detectar números de contas bancárias em um objeto do S3 que ele analisa durante um ciclo automatizado de descoberta de dados confidenciais, o Macie gera uma constatação financeira do objeto: S3. SensitiveData

Se o Macie detectar dados confidenciais no mesmo objeto do S3 durante uma execução de trabalho subsequente ou um ciclo automatizado de descoberta de dados confidenciais, o Macie gerará uma nova descoberta de dados confidenciais para o objeto. Diferentemente das descobertas de políticas, todas as descobertas de dados confidenciais são tratadas como novas (únicas). O Macie armazena as descobertas de dados confidenciais por 90 dias.

O Macie pode gerar os seguintes tipos de descobertas de dados confidenciais para um objeto do S3.

SensitiveData:S3Object/Credentials

O objeto contém dados confidenciais de credenciais, como chaves de acesso AWS secretas ou chaves privadas.

SensitiveData:S3Object/CustomIdentifier

O objeto contém texto que corresponde aos critérios de detecção de um ou mais identificadores de dados personalizados. O objeto pode conter mais de um tipo de dados confidenciais.

SensitiveData:S3Object/Financial

O objeto contém informações financeiras confidenciais, como números de contas bancárias ou números de cartão de crédito.

SensitiveData:S3Object/Multiple

O objeto contém mais de uma categoria de dados confidenciais — qualquer combinação de dados de credenciais, informações financeiras, informações pessoais ou texto que corresponda aos critérios de detecção de um ou mais identificadores de dados personalizados.

SensitiveData:S3Object/Personal

O objeto contém informações pessoais confidenciais — informações de identificação pessoal (PII), como números de passaporte ou números de identificação da carteira de motorista, informações pessoais de saúde (PHI), como números de seguro saúde ou de identificação médica, ou uma combinação de PII e PHI.

Para obter informações sobre os tipos de dados confidenciais que o Macie pode detectar usando técnicas e critérios incorporados, consulte Usar identificadores de dados gerenciados. Para obter informações sobre os tipos de objetos do S3 que o Macie pode analisar, consulte Classes e formatos de armazenamento suportados.

Trabalhando com exemplos de descobertas no Amazon Macie

Para explorar e aprender sobre os diferentes tipos de descobertas que o Amazon Macie pode gerar, você pode criar amostras de descobertas. Amostras de descobertas usam dados de exemplo e valores de espaço reservado para demonstrar os tipos de informações que cada tipo de descoberta pode conter.

Por exemplo, o exemplo de descoberta Policy:iamUser/S3BucketPublic contém detalhes sobre um bucket fictício do Amazon Simple Storage Service (Amazon S3). Os detalhes da descoberta incluem

dados de exemplo sobre um ator e uma ação que alteraram a lista de controle de acesso (ACL) do bucket e tornaram o bucket acessível ao público. Da mesma forma, a descoberta de amostra SensitiveData:S3Object/Multiple contém detalhes sobre uma pasta de trabalho fictícia do Microsoft Excel. Os detalhes da descoberta incluem exemplos de dados sobre os tipos e a localização de dados confidenciais na pasta de trabalho.

Além de se familiarizar com as informações que diferentes tipos de descobertas podem conter, você pode usar exemplos de descobertas para testar a integração com outros aplicativos, serviços e sistemas. Dependendo das regras de supressão da sua conta, o Macie pode publicar exemplos de descobertas no Amazon EventBridge como eventos. Ao usar os dados de exemplo nos exemplos de descobertas, você pode desenvolver e testar soluções automatizadas para monitorar e processar esses eventos. Dependendo das configurações de publicação da sua conta, o Macie também publica as descobertas no AWS Security Hub. Isso significa que você também pode usar exemplos de descobertas para desenvolver e testar soluções para monitorar e processar descobertas do Macie no Security Hub. Para obter informações sobre a publicação de descobertas nesses serviços, consulte Monitoramento e processamento de descobertas.

Tópicos

Como gerar amostras de descobertas

Você pode criar amostras de descobertas usando o console do Amazon Macie ou a API do Amazon Macie. Se você usa o console, o Macie gera automaticamente um exemplo de descoberta para cada tipo de descoberta compatível com o Macie. Se você usar a API, poderá criar um exemplo para cada tipo ou somente para determinados tipos que você especificar.

Console

Siga estas etapas para criar amostras de descobertas usando o console do Amazon Macie.

Para criar exemplos de descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Settings (configurações).
3. Em Sample findings, escolha Generate sample findings.

API

Para criar exemplos de descobertas de forma programática, use a operação CreateSampleFindings da API do Amazon Macie. Ao enviar sua solicitação, opcionalmente use o parâmetro `findingTypes` para especificar somente determinados tipos de descobertas de amostra a serem criadas. Para criar automaticamente exemplos de todos os tipos, não inclua esse parâmetro na sua solicitação.

Para criar amostras de descobertas usando o AWS Command Line Interface (AWS CLI), execute o comando create-sample-findings. Para criar automaticamente amostras de todos os tipos de descobertas, não inclua o parâmetro `finding-types`. Para criar exemplos somente de determinados tipos de descobertas, inclua esse parâmetro e especifique os tipos de exemplos de descobertas a serem criados. Por exemplo:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

Onde *`SensitiveData:S3Object/Multiple`* é um tipo de descoberta de dados confidenciais a ser criada e *`Policy:IAMUser/S3BucketPublic`* é um tipo de descoberta de política a ser criada.

Se o comando for executado com sucesso, o Macie retornará uma resposta vazia.

Revisando exemplos de descobertas

Para ajudá-lo a identificar os exemplos de descobertas que você criou, o Macie define o valor do campo Exemplo de cada exemplo de descoberta como Verdadeiro. Além disso, o nome do bucket do S3 afetado é o mesmo para todas as descobertas de amostra: macie-sample-finding-bucket. Se você analisar amostras de descobertas usando as páginas de descobertas no console do Amazon Macie, o Macie também exibirá o prefixo [EXEMPLO] no campo Tipo de descoberta para cada exemplo de descoberta.

Console

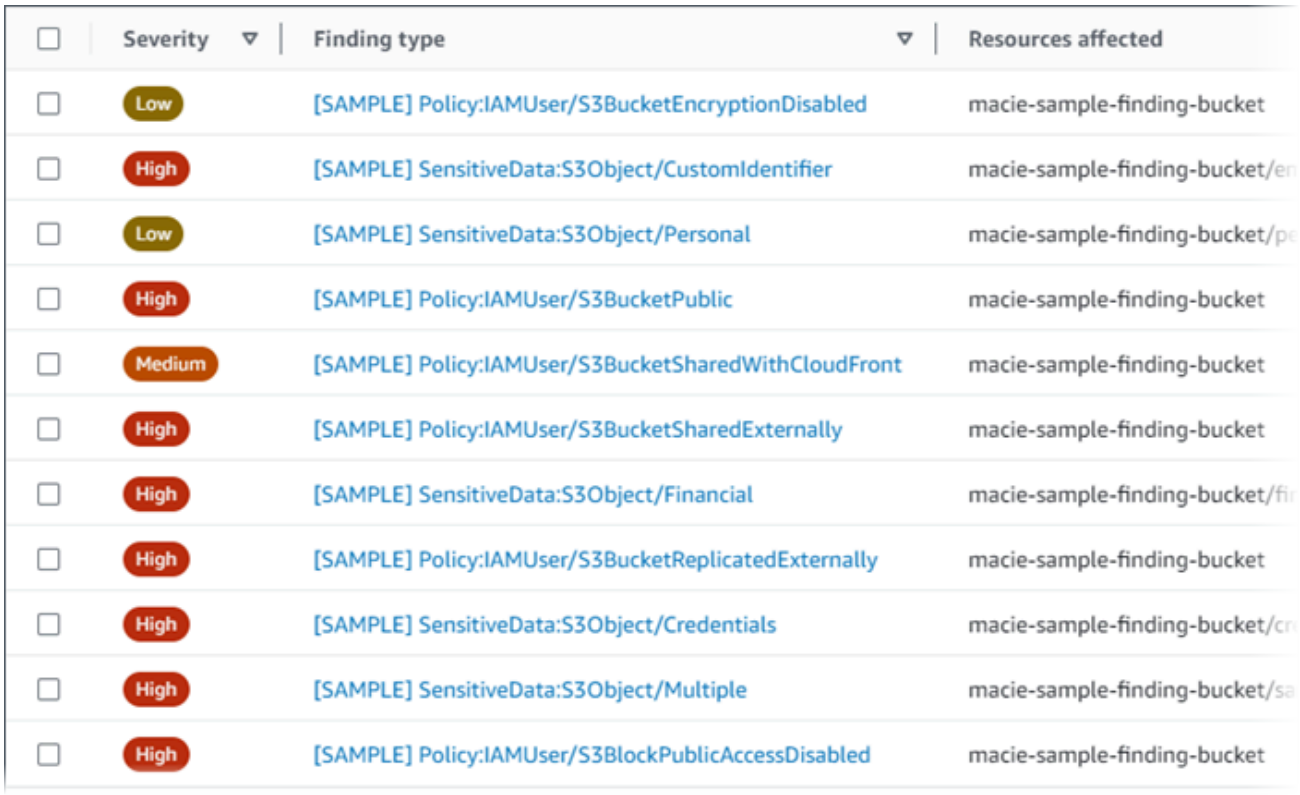
Siga estas etapas para revisar amostras de descobertas usando o console do Amazon Macie.

Para revisar amostras de descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. No painel de navegação, selecione Descobertas.
3. Na página Descobertas siga um destes procedimentos:

   - Na coluna Tipo de descoberta, localize descobertas cujo tipo comece com [EXEMPLO], conforme mostrado na imagem a seguir.



   - Usando a caixa Critérios de filtro acima da tabela, filtre a tabela para exibir somente descobertas de exemplos. Para fazer isso, coloque o cursor na caixa. Na lista de campos exibida, selecione Exemplo. Selecione Verdadeiro e, em seguida, selecione Aplicar. Isso adiciona a seguinte condição de filtro à tabela:

4. Para revisar os detalhes de um exemplo de descoberta específico, selecione a descoberta. O painel de detalhes exibirá informações sobre a descoberta.

Você também pode baixar e salvar os detalhes de um ou mais exemplos de descobertas como um arquivo JSON. Como fazer isso, marque a caixa de seleção para cada exemplo de descoberta que você deseja baixar e salvar. Em seguida, selecione Exportar (JSON) no menu Ações na parte superior da página Descobertas. Na janela exibida, selecione Baixar. Para

obter descrições detalhadas dos campos JSON que uma descoberta pode incluir, consulte Descobertas na Referência de API do Amazon Macie.

API

Para analisar as descobertas de amostras de forma programática, primeiro use a operação ListFindings da API do Amazon Macie para recuperar o identificador exclusivo (`findingId`) para cada descoberta de amostra que você criou. Em seguida, use a operação GetFindings para recuperar os detalhes dessas descobertas.

Ao enviar a solicitação de ListFindings, você pode especificar critérios de filtro para incluir somente resultados de amostra nos resultados. Para fazer isso, adicione uma condição de filtro onde o valor do campo `sample` seja `true`. Se você estiver usando o AWS CLI, execute o comando list-findings e use o parâmetro `finding-criteria` para especificar a condição do filtro. Por exemplo:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":
[\"true\"]}}}
```

Se a sua solicitação for realizada com êxito, o Macie retornará uma matriz `findingIds`. A matriz lista o identificador exclusivo de cada descoberta de exemplo para sua conta na Região da AWS atual.

Para então recuperar os detalhes das descobertas da amostra, especifique esses identificadores exclusivos em uma solicitação GetFindings ou, para o AWS CLI, ao executar o comando get-findings.

Como suprimir amostras de descobertas

Como outras descobertas, o Macie armazena exemplos de descobertas por 90 dias. Depois de concluir a revisão e a experimentação das amostras, você pode arquivá-las, opcionalmente, criando uma regra de supressão. Se você fizer isso, os exemplos de descobertas deixarão de aparecer por padrão no console e seu status mudará para arquivado.

Para arquivar amostras de descobertas usando o console do Amazon Macie, configure a regra para arquivar descobertas em que o valor do campo Amostra seja Verdadeiro. Para arquivar amostras de descobertas usando a API do Amazon Macie, configure a regra para arquivar descobertas em que o valor do campo `sample` seja `true`.

Analisar descobertas no console do Amazon Macie

O Amazon Macie monitora seu AWS ambiente e gera descobertas de políticas quando detecta possíveis violações de políticas ou problemas com a segurança ou a privacidade de seus buckets do Amazon Simple Storage Service (Amazon S3). O Macie gera descobertas de dados confidenciais quando detecta dados confidenciais em objetos do S3. O Macie armazena suas descobertas de políticas e dados confidenciais por 90 dias.

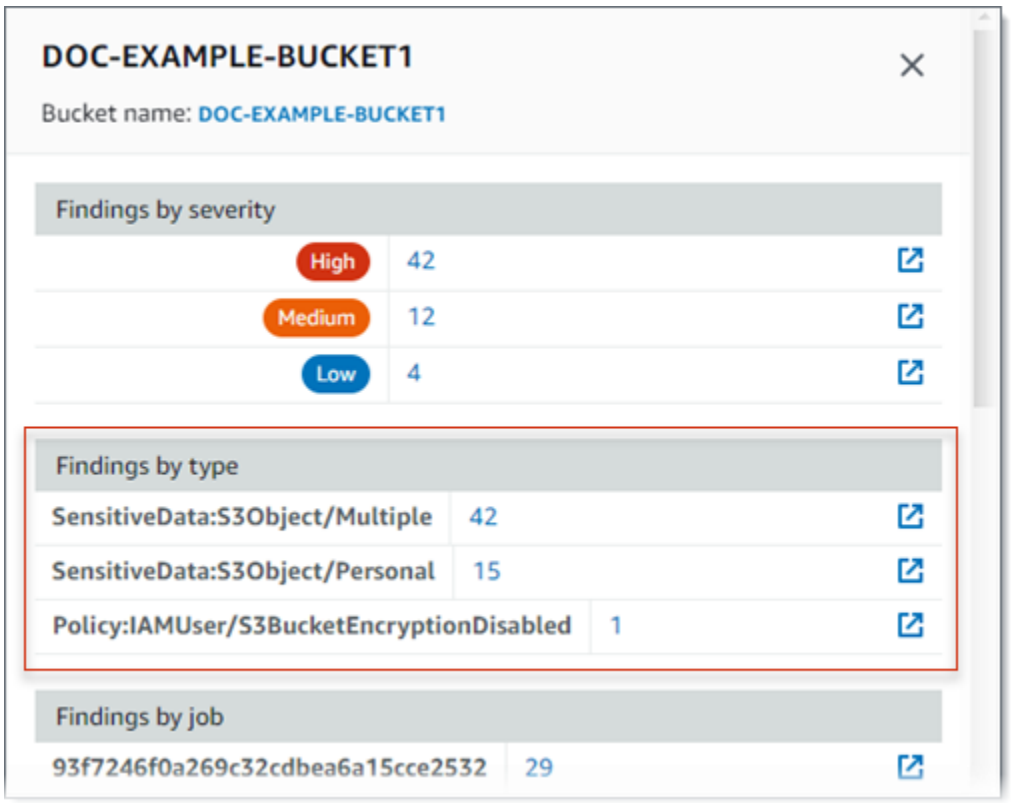
Cada descoberta especifica um tipo de descoberta e uma classificação de severidade. Detalhes adicionais incluem informações sobre o recurso afetado e quando e como Macie encontrou o problema ou dados confidenciais relatados pela descoberta. A severidade e os detalhes de cada descoberta variam de acordo com o tipo e a natureza da descoberta.

Ao usar o console do Amazon Macie, você pode revisar e analisar descobertas e acessar os detalhes de descobertas individuais. Você também pode exportar uma ou mais descobertas para um arquivo JSON. Para ajudá-lo a simplificar sua análise, o console oferece várias opções para criar visualizações personalizadas das descobertas.

Use agrupamentos predefinidos

Use páginas específicas para analisar as descobertas agrupadas por critérios, como bucket do S3 afetado, tipo de descoberta ou trabalho de descoberta de dados confidenciais. Com essas páginas, você pode analisar as estatísticas agregadas de cada grupo, como a contagem de descobertas por severidade. Você também pode detalhar para analisar os detalhes de descobertas individuais em um grupo e aplicar filtros para refinar sua análise.

Por exemplo, se você agrupar todas as descobertas por bucket do S3 e observar que um determinado bucket tem uma violação de política, você pode determinar rapidamente se também há descobertas de dados confidenciais para o bucket. Para fazer isso, selecione Por bucket no painel de navegação (em Descobertas) e, em seguida, selecione o bucket. No painel de detalhes exibido, a seção Descobertas por tipo lista os tipos de descobertas que se aplicam ao bucket, conforme mostrado na imagem a seguir.

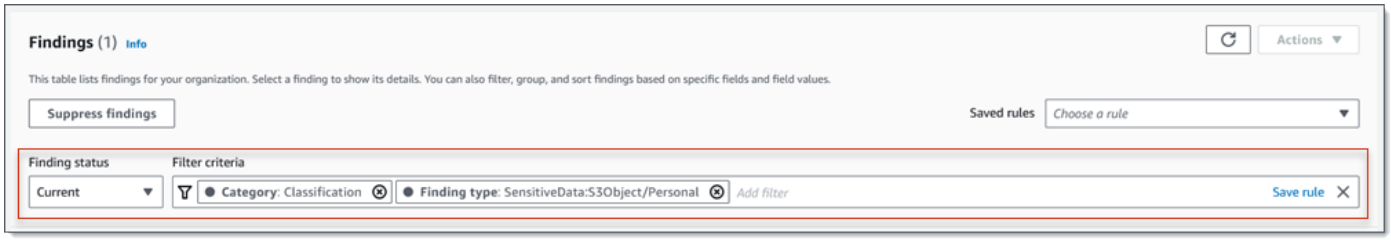


Para investigar um tipo específico, selecione o número do tipo. O Macie exibe uma tabela de todas as descobertas que correspondem ao tipo selecionado e se aplicam ao bucket. Para refinar os resultados, filtre a tabela.

Crie e aplique filtros

Use atributos de descoberta específicos para incluir ou excluir determinadas descobertas de uma tabela de descobertas. Atributo de descoberta é um campo que armazena dados específicos para uma descoberta, como tipo de descoberta, severidade ou nome do bucket do S3 afetado. Se você filtrar uma tabela, poderá identificar com mais facilidade as descobertas que têm características específicas. Em seguida, você pode analisar essas descobertas detalhadamente.

Por exemplo, para analisar todas as descobertas de dados confidenciais, adicione critérios de filtro ao campo Categoria. Para refinar os resultados e incluir somente um tipo específico de descoberta de dados confidenciais, adicione critérios de filtro para o campo Tipo de descoberta. Por exemplo:



Para depois analisar os detalhes de uma descoberta específica, selecione a descoberta. O painel de detalhes exibirá informações sobre a descoberta.

É possível classificar descobertas gerenciadas pelo cliente em ordem ascendente ou descendente pelos campos determinados. Para fazer isso, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna.

Como analisar descobertas no console

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas. A página Descobertas exibe descobertas que o Macie criou ou atualizou para sua conta na Região da AWS atual durante os últimos 90 dias. Por padrão, isso não inclui descobertas que foram suprimidas por uma regra de supressão.
3. Para articular e analisar as descobertas por meio de um grupo lógico predefinido, selecione Por bucket, Por tipo ou Por trabalho no painel de navegação (em Descobertas)). Em seguida, selecione um item na tabela. No painel de detalhes, selecione o link do campo para dinamizar.
4. Para filtrar as descobertas por critérios específicos, use as opções de filtro acima da tabela:

   - Para exibir descobertas que foram suprimidas por uma regra de supressão, use o menu Status da busca. Escolha Tudo para exibir descobertas suprimidas e não suprimidas, ou escolha Arquivado para exibir somente descobertas suprimidas. Para ocultar novamente as descobertas suprimidas, selecione Atual.
   - Para exibir somente as descobertas que têm um atributo específico, use a caixa Filtrar critérios. Coloque o cursor na caixa e adicione uma condição de filtro para o atributo. Para refinar ainda mais os resultados, adicione condições para atributos adicionais. Para então remover uma condição, selecione o ícone de remoção da condição (⊗) da condição a ser removida.

Para obter mais informações sobre filtragem, consulte Como criar e aplicar filtros às descobertas.

5. Para classificar as descobertas por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna.
6. Para visualizar os detalhes de uma determinada descoberta, selecione a descoberta. O painel de detalhes exibirá informações sobre a descoberta.

> **Tip**
>
> É possível usar o painel de detalhes para dinamizar e detalhar determinados campos. Para mostrar descobertas que tenham o mesmo valor para um campo, selecione
>
> 
>
> no campo. Ou escolha
>
> 
>
> mostrar descobertas que tenham outros valores para o campo.
> Para uma descoberta de dados confidenciais, você também pode usar o painel de detalhes para investigar dados confidenciais que Macie encontrou no objeto S3 afetado:
>
> - Para localizar ocorrências de um tipo específico de dados confidenciais, selecione o link numérico no campo para esse tipo de dados. O Macie exibe informações (no formato JSON) sobre onde o Macie encontrou os dados. Para obter mais informações, consulte Como localizar dados confidenciais.
> - Para recuperar amostras dos dados confidenciais que o Macie encontrou, selecione Analisar no campo Revelar amostras. Para obter mais informações, consulte Recuperando amostras de dados confidenciais.
> - Para navegar até o resultado correspondente da descoberta de dados confidenciais, selecione o link no campo Localização detalhada do resultado. Macie abre o console do Amazon S3 e exibe o arquivo ou pasta que contém o resultado da descoberta. Para obter mais informações, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

É possível também baixar e salvar os detalhes de uma ou mais descobertas como um arquivo JSON. Para fazer isso, marque a caixa de seleção para cada descoberta que você deseja baixar e salvar. Em seguida, selecione Exportar (JSON) no menu Ações na parte superior da página Descobertas.

Na janela exibida, selecione Baixar. Para obter descrições detalhadas dos campos JSON que uma descoberta pode incluir, consulte Descobertas na Referência de API do Amazon Macie.

Filtrar descobertas do Amazon Macie

Para realizar análises direcionadas e analisar as descobertas com mais eficiência, você pode filtrar as descobertas do Amazon Macie. Com filtros, você cria visualizações e consultas personalizadas para descobertas, o que pode ajudá-lo a identificar e enfocar descobertas com características específicas. Use o console do Amazon Macie para filtrar descobertas ou enviar consultas programaticamente usando a API do Amazon Macie.

Ao criar um filtro, você usa atributos específicos das descobertas para definir critérios para incluir ou excluir descobertas de uma exibição ou dos resultados da consulta. Atributo de descoberta é um campo que armazena dados específicos para uma descoberta, como gravidade, tipo ou nome do bucket do S3 ao qual a descoberta se aplica.

No Macie, um filtro consiste em uma ou mais condições. Cada condição, também chamada de critério, consiste em três partes:

- Um campo baseado em atributos, como Gravidade ou tipo de descoberta.
- Um operador, como igual a ou não igual a.
- Um ou mais valores. O tipo e o número de valores dependem do campo e do operador que você escolher.

Se você criar um filtro que queira usar novamente, poderá salvá-lo como uma regra de filtro. Uma regra de filtro é um conjunto de critérios de filtro que você cria e salva para reaplicar ao analisar as descobertas no console do Amazon Macie.

Você também pode salvar um filtro como regra de supressão. Uma regra de supressão é um conjunto de critérios de filtro que você cria e salva para arquivar automaticamente descobertas que correspondam aos critérios da regra. Para saber mais sobre regras de supressão, consulte Suprimir descobertas.

Tópicos

- Fundamentos da filtragem de descobertas
- Como criar e aplicar filtros às descobertas
- Como criar e gerenciar regras de filtro para descobertas

- Campos para filtrar descobertas

Fundamentos da filtragem de descobertas

Ao criar um filtro, lembre-se dos atributos e diretrizes a seguir. Observe também que os resultados filtrados estão limitados aos 90 dias anteriores e aos Região da AWS atuais. O Amazon Macie armazena suas descobertas por apenas 90 dias a cada Região da AWS.

Tópicos

- Uso de várias condições em um filtro
- Especificando valores para campos
- Especificando vários valores para um campo
- Usando operadores em condições

Uso de várias condições em um filtro

Um filtro pode incluir uma ou mais condições. Cada condição, também chamada de critério, consiste em três partes:

- Um campo baseado em atributos, como Gravidade ou tipo de descoberta. Para obter uma lista de campos que você pode usar, consulte Campos para filtrar descobertas.
- Um operador, como igual ou não igual. Para obter uma lista de operadores que você pode usar, consulte Usando operadores em condições.
- Um ou mais valores. O tipo e o número de valores dependem do campo e do operador que você escolher.

Se um filtro contiver várias condições, o Macie usa a lógica AND para unir as condições e avaliar os critérios do filtro. Isso significa que uma descoberta corresponde aos critérios do filtro somente se corresponder a todas as condições do filtro.

Por exemplo, se você adicionar uma condição para incluir somente descobertas de alta gravidade e adicionar outra condição para incluir somente descobertas de dados confidenciais, o Macie retornará todas as descobertas de dados confidenciais de alta gravidade. Em outras palavras, o Macie exclui todas as conclusões de políticas e todas as descobertas de dados confidenciais de gravidade média e baixa.

Você pode usar um campo somente uma vez em um filtro. No entanto, você pode especificar vários valores para vários campos.

Por exemplo, se uma condição usa o campo Gravidade para incluir somente descobertas de alta gravidade, você não pode usar o campo Gravidade em outra condição para incluir descobertas de gravidade média ou baixa. Em vez disso, especifique vários valores para a condição existente ou use um operador diferente para a condição existente. Por exemplo, para incluir todas as descobertas de gravidade média e alta, adicione uma condição Gravidade igual a Média, Alta ou adicione uma condição Gravidade não igual a Baixa.

Especificando valores para campos

Quando você especifica um valor para um campo, o valor precisa estar em conformidade com o tipo de dados subjacente do campo. Dependendo do campo, você pode especificar um dos seguintes tipos de valores.

Matriz de texto (sequências de caracteres)

Especifica uma lista de valores de texto (string) para um campo. Cada string se correlaciona a um valor predefinido ou existente para um campo — por exemplo, Alto para o campo Gravidade, SensitiveData:S3Object/Financial para o campo Tipo de descoberta ou o nome de um bucket do S3 para o campo de nome do bucket do S3.

Se você usar uma matriz, observe o seguinte:

- Os valores diferenciam maiúsculas de minúsculas.
- Você não pode especificar valores parciais nem usar caracteres curinga nos valores. Você precisa especificar um valor completo e válido para o campo.

Por exemplo, para filtrar as descobertas de um bucket do S3 chamado my-S3-bucket, insira **`my-S3-bucket`** como valor para o campo de nome do bucket do S3. Se você inserir qualquer outro valor, como **`my-s3-bucket`** ou **`my-S3`**, o Macie não retornará as descobertas para o bucket.

Para obter uma lista de valores válidos para cada campo, consulte Campos para filtrar descobertas.

Você pode especificar até 50 valores em uma matriz. A forma como você especifica os valores depende do uso do console do Amazon Macie ou da API do Amazon Macie, conforme discutido em Especificando vários valores para um campo.

Booleano

Especifica um dos dois valores mutuamente exclusivos para um campo.

Se você usar o console do Amazon Macie para especificar esse tipo de valor, o console fornecerá uma lista de valores para você escolher. Se você usa a API do Amazon Macie, especifique `true` ou `false` para o valor.

Data/hora (e intervalos de tempo)

Especifica uma data e hora absolutas para um campo. Se você especificar esse tipo de valor, precisará especificar uma data e uma hora.

No console do Amazon Macie, os valores de data e hora estão em seu fuso horário local e usam notação de 24 horas. Em todos os outros contextos, esses valores estão no Tempo Universal Coordenado (UTC) e no formato ISO 8601 estendido, por exemplo, `2020-09-01T14:31:13Z` para 14:31:13 UTC de 1º de setembro de 2020.

Se um campo armazenar um valor de data/hora, você poderá usar o campo para definir um intervalo de tempo fixo ou relativo. Por exemplo, você pode incluir somente as descobertas que foram criadas entre duas datas e horários específicos ou somente aquelas que foram criadas antes ou depois de uma data e hora específicas. A forma como você define um intervalo de tempo depende se você usa o console do Amazon Macie ou a API do Amazon Macie:

- No console, use um seletor de data ou insira o texto diretamente nas caixas De e Para.
- Com a API, defina um intervalo de tempo fixo adicionando uma condição que especifica a primeira data e hora no intervalo e adicione outra condição que especifica a última data e hora no intervalo. Se você fizer isso, Macie usa a lógica AND para unir as condições. Para definir um intervalo de tempo relativo, adicione uma condição que especifique a primeira ou a última data e hora no intervalo. Especifique os valores como timestamps Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

No console, os intervalos de tempo são inclusivos. Com a API, os intervalos de tempo podem ser inclusivos ou exclusivos, dependendo do operador que você escolher.

Número (e intervalos numéricos)

Especifica um número inteiro longo para um campo.

Se um campo armazenar um valor de data/hora, você poderá usar o campo para definir um intervalo de tempo fixo ou relativo. Por exemplo, você pode incluir somente as descobertas que

relatam de 50 a 90 ocorrências de dados confidenciais em um objeto do S3. A forma como você define um intervalo de tempo depende se você usa o console do Amazon Macie ou a API do Amazon Macie:

- No console, use as caixas De e Para para inserir os números mais baixos e mais altos no intervalo, respectivamente.
- Com a API, defina um intervalo de tempo fixo adicionando uma condição que especifica a primeira data e hora no intervalo e adicione outra condição que especifica a última data e hora no intervalo. Se você fizer isso, Macie usa a lógica AND para unir as condições. Para definir um intervalo numérico relativo, adicione uma condição que especifique o menor ou o maior número no intervalo.

No console, os intervalos de tempo são inclusivos. Com a API, os intervalos de tempo podem ser inclusivos ou exclusivos, dependendo do operador que você escolher.

Texto (string)

Especifica uma lista de valores de texto (string) para um campo. A string está correlacionada a um valor predefinido ou existente para um campo — por exemplo, Alto para o campo Gravidade, o nome de um bucket do S3 para o campo de nome do bucket do S3 ou o identificador exclusivo de um trabalho de descoberta de dados confidenciais para o campo Job ID.

Se você especificar uma única sequência de texto, observe o seguinte:

- Os valores diferenciam maiúsculas de minúsculas.
- Você não pode especificar valores parciais nem usar caracteres curinga nos valores. Você precisa especificar um valor completo e válido para o campo.

Por exemplo, para filtrar as descobertas de um bucket do S3 chamado my-S3-bucket, insira **`my-S3-bucket`** como valor para o campo de nome do bucket do S3. Se você inserir qualquer outro valor, como **`my-s3-bucket`** ou **`my-S3`**, o Macie não retornará as descobertas para o bucket.

Para obter uma lista de valores válidos para cada campo, consulte Campos para filtrar descobertas.

Especificando vários valores para um campo

Com determinados campos e operadores, você pode especificar vários valores para um campo. Se você fizer isso, Macie usa a lógica OR para unir os valores e avaliar os critérios do filtro. Isso significa que uma descoberta corresponde aos critérios se tiver algum dos valores do campo.

Por exemplo, se você adicionar uma condição para incluir descobertas em que o valor do campo Tipo de descoberta seja igual a SensitiveData:S3Object/Financial, SensitiveData:S3Object/Personal, o Macie retornará descobertas de dados confidenciais para objetos do S3 que contêm somente informações financeiras e objetos do S3 que contêm somente informações pessoais. Em outras palavras, Macie exclui todas as descobertas de políticas. O Macie também exclui todas as descobertas de dados confidenciais para objetos que contêm outros tipos de dados confidenciais ou vários tipos de dados confidenciais.

A exceção está nas condições que usam o operador eqExactMatch. Se você fizer isso, Macie usa a lógica OR para unir os valores e avaliar os critérios do filtro. Isso significa que uma descoberta corresponde aos critérios somente se tiver todos os valores para o campo e somente esses valores para o campo. Para saber mais sobre esse operador, consulte Usando operadores em condições.

A forma como você especifica os valores depende do uso do console do Amazon Macie ou da API do Amazon Macie, conforme discutido em . Com a API, você usa uma matriz que lista os valores.

No console, você normalmente escolhe os valores de uma lista. No entanto, para alguns campos, você precisa adicionar uma condição distinta para cada valor. Por exemplo, para incluir descobertas de dados que o Macie detectou usando determinados identificadores de dados personalizados, faça o seguinte:

1. Coloque o cursor na caixa Critérios de filtro e selecione o campo Nome do identificador de dados personalizado. Insira o nome de um identificador de dados personalizado e selecione Aplicar.
2. Repita a etapa anterior para cada identificador de dados personalizado adicional que você deseja especificar para o filtro.

Para obter uma lista dos campos para os quais você precisa fazer isso, consulte Campos para filtrar descobertas.

Usando operadores em condições

Você pode usar os seguintes tipos de operadores em condições individuais.

Igual a (eq)

> Corresponde (=) a qualquer valor especificado para o campo. Você pode usar o operador igual a com os seguintes tipos de valores: matriz de texto (cadeias de caracteres), booleano, data/hora, número e texto (sequência de caracteres).

Para muitos campos, você pode usar esse operador e especificar até 50 valores para o campo. Se você fizer isso, Macie usa a lógica AND para unir as condições. Isso significa que uma descoberta corresponde aos critérios se tiver algum dos valores do campo.

Por exemplo:

- Para incluir descobertas que relatam ocorrências de informações financeiras, informações pessoais ou informações financeiras e pessoais, adicione uma condição que use o campo Categoria de dados confidenciais e esse operador e especifique Informações financeiras e Informações pessoais como valores para o campo.
- Para incluir descobertas que relatam ocorrências de números de cartão de crédito, endereços de correspondência ou números de cartão de crédito e endereços de correspondência, adicione uma condição para o campo Tipo de detecção de dados confidenciais, use esse operador e especifique CREDIT_CARD_NUMBER e ADDRESS como valores para o campo.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Igual à correspondência exata (eqExactMatch)

Corresponde exclusivamente a todos os valores especificados para o campo. Você pode usar o operador de igual a correspondência exata com um conjunto selecionado de campos.

Se você usar esse operador e especificar vários valores para um campo, o Macie usa a lógica AND para unir os valores. Isso significa que uma descoberta corresponde aos critérios somente se tiver todos os valores para o campo e somente esses valores para o campo. Você pode especificar até 50 valores para o campo.

Por exemplo:

- Para incluir descobertas que relatam ocorrências de números de cartão de crédito e nenhum outro tipo de dado confidencial, adicione uma condição para o campo Tipo de detecção de dados confidenciais, use esse operador e especifique CREDIT_CARD_NUMBER como o único valor para o campo.
- Para incluir descobertas que relatam ocorrências de números de cartão de crédito e nenhum outro tipo de dado confidencial, adicione uma condição para o campo Tipo de detecção de dados confidenciais, use esse operador e especifique CREDIT_CARD_NUMBER e ADDRESS como valores para o campo.

Como o Macie usa a lógica AND para unir os valores de um campo, você não pode usar esse operador em combinação com outros operadores para o mesmo campo. Em outras palavras, se você usar o operador de igual a correspondência exata a um campo em uma condição, precisará usá-lo em todas as outras condições que usam o mesmo campo.

Como outros operadores, você pode usar o operador de igual a correspondência exata em mais de uma condição em um filtro. Se você fizer isso, Macie usa a lógica AND para unir as condições. Isso significa que uma descoberta corresponde aos critérios do filtro somente se tiver todos os valores especificados por todas as condições do filtro.

Por exemplo, para incluir descobertas que foram criadas após um certo tempo, relatar ocorrências de números de cartão de crédito e não relatar nenhum outro tipo de dado confidencial, faça o seguinte:

1. Adicione uma condição que use o campo Criado em, use o operador maior que e especifique a data e a hora de início do filtro.
2. Adicione outra condição que use o campo Tipo de detecção de dados confidenciais, use o operador de igual a correspondência exata e especifique CREDIT_CARD_NUMBER como o único valor para o campo.

Você pode usar o operador de igual a correspondência exata com os seguintes campos:

- Identificador de dados personalizado (`customDataIdentifiers.detections.arn`)
- Nome do identificador de dados personalizado (`customDataIdentifiers.detections.name`)
- Chave de tag de bucket S3 (`resourcesAffected.s3Bucket.tags.key`)
- Valor de tag de bucket S3 (`resourcesAffected.s3Bucket.tags.value`)
- Chave de tag de objeto S3 (`resourcesAffected.s3Object.tags.key`)
- Valor da tag de objeto S3 (`resourcesAffected.s3Object.tags.value`)
- Tipo de detecção de dados confidenciais (`sensitiveData.detections.type`)
- Categoria de dados confidenciais (`sensitiveData.category`)

Na lista anterior, o nome entre parênteses usa a notação de pontos para indicar o nome do campo nas representações JSON das descobertas e na API Amazon Macie.

Maior que (gt)

É maior que (**>**) o valor especificado para o campo. Você pode usar o operador maior que com valores numéricos e de data/hora.

Por exemplo, para incluir somente as descobertas que relatam mais de 90 ocorrências de dados confidenciais em um objeto do S3, adicione uma condição que use o campo Contagem total de dados confidenciais e esse operador e especifique 90 como o valor do campo. Para fazer isso no console do Amazon Macie, insira **91** na caixa De, não insira um valor na caixa Para e selecione Aplicar. As comparações numéricas e baseadas em tempo estão incluídas no console.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Maior ou igual a (gte)

É maior ou igual ao (**>=**) valor especificado para o campo. Você pode usar o operador maior que ou igual a com valores numéricos e de data/hora.

Por exemplo, para incluir somente as descobertas que relatam mais de 90 ocorrências de dados confidenciais em um objeto do S3, adicione uma condição que use o campo Contagem total de dados confidenciais e esse operador e especifique 90 como o valor do campo. Para fazer isso no console do Amazon Macie, insira **90** na caixa De, não insira um valor na caixa Para e selecione Aplicar.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Menor que (lt)

É menor que (**>**) o valor especificado para o campo. Você pode usar o operador menor que com valores numéricos e de data/hora.

Por exemplo, para incluir somente as descobertas que relatam mais de 90 ocorrências de dados confidenciais em um objeto do S3, adicione uma condição que use o campo Contagem total de dados confidenciais e esse operador e especifique 90 como o valor do campo. Para fazer isso no console do Amazon Macie, insira **89** na caixa De, não insira um valor na caixa Para e selecione Aplicar. As comparações numéricas e baseadas em tempo estão incluídas no console.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Menor ou igual a (lte)

É menor ou igual ao (**<=**) valor especificado para o campo. Você pode usar o operador menor que ou igual a com valores numéricos e de data/hora.

Por exemplo, para incluir somente as descobertas que relatam 90 ou menos ocorrências de dados confidenciais em um objeto do S3, adicione uma condição que use o campo Contagem total de dados confidenciais e esse operador e especifique 90 como o valor do campo. Para fazer isso no console do Amazon Macie, insira **`90`** na caixa Até, não insira um valor na caixa De e selecione Aplicar.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Não são iguais (neq)

Não corresponde (=) a qualquer valor especificado para o campo. Você pode usar o operador não igual a com os seguintes tipos de valores: matriz de texto (cadeias de caracteres), booleano, data/hora, número e texto (sequência de caracteres).

Para muitos campos, você pode usar esse operador e especificar até 50 valores para o campo. Se você fizer isso, Macie usa a lógica OR para unir as condições. Isso significa que uma descoberta corresponde aos critérios se tiver algum dos valores do campo.

Por exemplo:

- Para excluir descobertas que relatam ocorrências de informações financeiras, informações pessoais ou informações financeiras e pessoais, adicione uma condição que use o campo Categoria de dados confidenciais e esse operador e especifique Informações financeiras e Informações pessoais como valores para o campo.
- Para excluir descobertas que relatam ocorrências de números de cartão de crédito, adicione uma condição para o campo Tipo de detecção de dados confidenciais, use esse operador e especifique CREDIT_CARD_NUMBER como o único valor para o campo.
- Para excluir descobertas que relatam ocorrências de números de cartão de crédito, endereços de correspondência ou números de cartão de crédito e endereços de correspondência, adicione uma condição para o campo Tipo de detecção de dados confidenciais, use esse operador e especifique CREDIT_CARD_NUMBER e ADDRESS como valores para o campo.

Se você usar a API do Amazon Macie para definir uma condição que usa esse operador com um valor de data/hora, especifique o valor como um timestamp Unix em milissegundos — por exemplo, `1604616572653` para 22:49:32 UTC de 5 de novembro de 2020.

Como criar e aplicar filtros às descobertas

Para identificar e focar nas descobertas que têm características específicas, você pode filtrar as descobertas no console do Amazon Macie e nas consultas que envia programaticamente usando a API do Amazon Macie. Ao criar um filtro, você usa atributos específicos das descobertas para definir critérios para incluir ou excluir descobertas de uma exibição ou dos resultados da consulta. Atributo de descoberta é um campo que armazena dados específicos para uma descoberta, como gravidade, tipo ou nome do bucket do S3 ao qual a descoberta se aplica.

No Macie, um filtro consiste em uma ou mais condições. Cada condição, também chamada de critério, consiste em três partes:

- Um campo baseado em atributos, como Gravidade ou Tipo de descoberta.
- Um operador, como igual ou não igual.
- Um ou mais valores. O tipo e o número de valores dependem do campo e do operador que você escolher.

A forma como você define e aplica as condições do filtro depende do uso do console do Amazon Macie ou da API do Amazon Macie.

Tópicos

Como filtrar descobertas no console do Amazon Macie

Se você usa o console do Amazon Macie para filtrar as descobertas, o Macie oferece opções para ajudá-lo a escolher campos, operadores e valores para condições individuais. Você acessa essas opções usando as configurações de filtro nas páginas Descobertas, conforme mostrado na imagem a seguir.

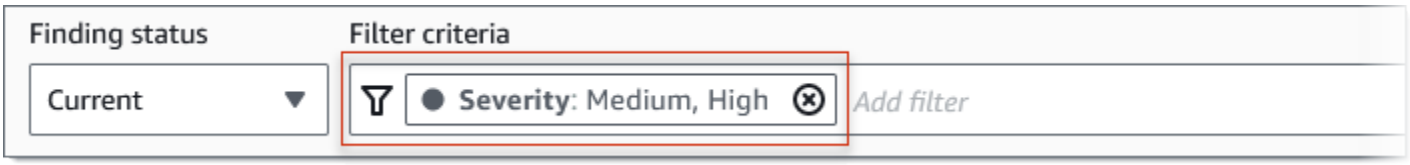
Ao usar o menu Status da descoberta, você pode especificar se deseja incluir descobertas que foram suprimidas (arquivadas automaticamente) por uma regra de supressão. Usando a caixa Critérios de filtro, você pode inserir as condições do filtro.

Quando você coloca o seu cursor na caixa Critérios de filtro, o Macie exibe uma lista de campos que você pode usar em condições do filtro. Os campos são organizados por categoria lógica. Por exemplo, a categoria Campos comuns inclui campos que se aplicam a qualquer tipo de descoberta, e a categoria Campos de classificação inclui campos que se aplicam somente a descobertas de dados confidenciais. Os campos são classificados em ordem alfabética dentro de cada categoria.

Para adicionar uma condição, comece escolhendo um campo na lista. Para encontrar um campo, navegue pela lista completa ou insira parte do nome do campo para restringir a lista de campos.

Dependendo do campo que você escolher, O Macie exibirá diferentes opções. As opções refletem o tipo e a natureza do campo escolhido. Por exemplo, se você escolher o campo Severidade, o Macie exibirá uma lista de valores para escolher: Baixa, Média e Alta. Se você escolher o campo Nome do bucket do S3, o Macie exibirá uma caixa de texto na qual você poderá inserir um nome do bucket. Seja qual for o campo escolhido, o Macie o guiará pelas etapas para adicionar uma condição que inclua as configurações necessárias para o campo.

Depois de adicionar uma condição, o Macie aplica os critérios para a condição e adiciona a condição a um token de filtro na caixa Critérios de filtro, conforme mostrado na imagem a seguir.



Neste exemplo, a condição é configurada para incluir todas as descobertas de severidade média e alta e para excluir todas as descobertas de baixa severidade. Ele retorna descobertas em que o valor do campo Severidade é igual a Médio ou Alto.

> **Tip**
>
> Para muitos campos, você pode alterar o operador de uma condição de igual para não igual escolhendo o ícone de igual (●) no token de filtro para a condição. Se você fizer isso, o Macie alterará o operador para não igual e exibirá o ícone diferente (⊘) no token. Para alternar novamente para o operador igual, selecione o ícone de não é igual.

À medida que você adiciona mais condições, o Macie aplica seus critérios e os adiciona aos tokens na caixa Critérios de filtro. Você pode consultar a caixa a qualquer momento para determinar quais critérios você aplicou. Para remover uma condição, selecione o ícone de remoção da condição (⊗) no token da condição.

Para filtrar descobertas usando o console

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. (Opcional) Para primeiro analisar e revisar as descobertas por um grupo lógico predefinido, selecione Por bucket, Por tipo ou Por trabalho no painel de navegação (em Descobertas). Em seguida, selecione um item na tabela. No painel de detalhes, selecione o link do campo a analisar.
4. (Opcional) Para exibir descobertas que foram suprimidas por uma regra de supressão, altere a configuração de Status do filtro. Selecione Arquivado para exibir somente descobertas suprimidas ou selecione Tudo para exibir descobertas suprimidas e não suprimidas. Para ocultar as descobertas suprimidas, selecione Atual.
5. Para adicionar uma condição de filtro:

    a. Coloque o cursor na caixa Critérios de filtro e selecione o campo a ser usado para a condição. Para obter mais informações sobre os campos que você pode usar, consulte Campos para filtrar descobertas.

    b. Insira o tipo de valor apropriado para o campo. Para obter informações detalhadas sobre os diferentes tipos de valores, consulte Especificando valores para campos.

Matriz de texto (string)

Para esse tipo de valor, o Macie geralmente fornece uma lista de valores para você escolher. Se for esse o caso, selecione cada valor que você deseja usar na condição.

Se o Macie não fornecer uma lista de valores, insira um valor completo e válido para o campo. Para especificar valores adicionais para o campo, selecione Aplicar e, em seguida, adicione outra condição para cada valor adicional.

Observe que valores diferenciam entre maiúsculas e minúsculas. Além disso, você não pode usar valores parciais ou caracteres curinga nos valores. Por exemplo, para filtrar as descobertas de um bucket do S3 chamado my-S3-bucket, insira como valor para o campo **`my-S3-bucket`**nome do bucket do S3. Se você inserir qualquer outro valor, como **`my-s3-bucket`** ou **`my-S3`**, o Macie não retornará as descobertas para o bucket.

Booleano

Para esse tipo de valor, o Macie fornece uma lista de valores para você escolher. Selecione o valor que deseja usar na condição.

Data/hora (intervalos de tempo)

Para esse tipo de valor, use as caixas De e Para para definir um intervalo de tempo inclusivo:

- Para definir um intervalo de tempo fixo, use as caixas De e Para para especificar a primeira data e hora e a última data e hora no intervalo, respectivamente.
- Para definir um intervalo de tempo relativo que começa em uma determinada data e hora e termina na hora atual, insira a data e a hora de início nas caixas De e exclua qualquer texto nas caixas Para.
- Para definir um intervalo de tempo relativo que termina em uma determinada data e hora, insira a data e a hora de término nas caixas Para e exclua qualquer texto nas caixas De.

Observe que os valores de tempo usam a notação de 24 horas. Se você usar o seletor de datas para escolher datas, poderá refinar os valores inserindo texto diretamente nas caixas De e Para.

Número (e intervalos numéricos)

Para esse tipo de valor, use as caixas De e Para para inserir um ou mais números inteiros que definam um intervalo numérico inclusivo, fixo ou relativo.

Valores de texto (string)

Para esse tipo de valor, insira um valor completo e válido para o campo.

Observe que valores diferenciam entre maiúsculas e minúsculas. Além disso, você não pode usar valores parciais ou caracteres curinga nos valores. Por exemplo, para filtrar as descobertas de um bucket do S3 chamado my-S3-bucket, insira como valor para o campo **`my-S3-bucket`**nome do bucket do S3. Se você inserir qualquer outro valor, como **`my-s3-bucket`** ou **`my-S3`**, o Macie não retornará as descobertas para o bucket.

c. Ao terminar de adicionar valores para o campo, selecione Aplicar. O Macie aplica seus critérios de filtro e adiciona a condição a um token de filtro na caixa Critérios de filtro.

6. Repita essa etapa 5 para cada condição que deseja adicionar.
7. Para remover uma condição, selecione o ícone de remoção da condição (⊗) no token de filtro da condição.
8. Para alterar uma condição, remova a condição escolhendo o ícone de remoção da condição (⊗) no token de filtro da condição. Em seguida, repita a etapa 5 para adicionar uma condição com as configurações corretas.

Se quiser usar esse conjunto de condições de novo posteriormente, você pode salvar o conjunto como uma regra de filtro. Para fazer isso, selecione Salvar regra na caixa Critérios de filtro. Então, informe um nome para a regra e, como opção, uma descrição. Ao concluir, selecione Salvar.

Como filtrar descobertas de forma programática com a API do Amazon Macie

Para filtrar as descobertas de forma programática, especifique os critérios de filtro nas consultas que você envia usando a operação ListFindings ou GetFindingStatistics da API Amazon do Macie. A operação ListFindings retorna uma matriz de IDs de descoberta, uma ID para cada descoberta que corresponda aos critérios do filtro. A operação GetFindingStatistics retorna dados estatísticos agregados sobre todas as descobertas que correspondem aos critérios do filtro, agrupados por um campo que você especifica em sua solicitação.

Observe que as operações ListFindings e GetFindingStatistics são diferentes das operações que você usa para suprimir descobertas. Ao contrário das operações de supressão, que também especificam critérios de filtro, as operações ListFindings e GetFindingStatistics consultam apenas os dados das descobertas. Eles não realizam qualquer ação nas descobertas que correspondam aos critérios de filtro. Para suprimir descobertas, use a operação CreateFindingsFilter do API da Amazon Macie.

Para especificar critérios de filtro em uma consulta, inclua um mapa das condições do filtro em sua solicitação. Para cada condição, você deve especificar um campo, um operador e um ou mais valores para o campo. O tipo e o número de valores dependem do campo e do operador que você escolher. Para obter informações sobre os campos, operadores e tipos de valores que você pode usar em uma condição, consulteCampos para filtrar descobertas, Usando operadores em condições e Especificando valores para campos.

Os exemplos a seguir mostram como especificar critérios de filtro nas consultas enviadas usando o AWS Command Line Interface(AWS CLI). Você também pode fazer isso usando uma versão atual de outra AWS ferramenta de linha de comando ou de um AWS SDK, ou enviando solicitações HTTPS diretamente para o Macie. Para obter mais informações sobre AWS ferramentas e SDKs, consulte Ferramentas para aproveitar AWS.

Exemplos

- Exemplo 1: filtro de descobertas baseado em severidade
- Exemplo 2: Descobertas de filtro baseadas categoria de dados confidenciais
- Exemplo 3: Filtrar descobertas com base em um intervalo de tempo fixo
- Exemplo 4: filtrar descobertas com base no status de supressão
- Exemplo 5: filtrar descobertas com base em vários campos e tipos de valores

Os exemplos usam o comando list-findings. Se um exemplo for executado com sucesso, o Macie retornará uma matriz `findingIds`. A matriz lista o identificador exclusivo de cada descoberta que corresponde aos critérios de filtro, conforme mostrado no exemplo a seguir.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
```

```
    ]
}
```

Se nenhuma descoberta corresponder aos critérios do filtro, o Macie retornará uma matriz `findingIds` vazia.

```
{
    "findingIds": []
}
```

Exemplo 1: filtro de descobertas baseado em severidade

Este exemplo usa o comando list-findings para recuperar IDs de descoberta para todas as suas descobertas atuais de alta e média severidade no Região da AWS atual.

Para Linux, macOS ou Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Para o Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

Onde:

- *severity.description* especifica o nome JSON do campo Severidade.
- *eq* especifica o operador igual.
- *Alto* e *Médio* são uma matriz de valores enumerados para o campo Severidade.

Exemplo 2: Descobertas de filtro baseadas categoria de dados confidenciais

Este exemplo usa o comando list-findings para recuperar IDs de descobertas de todas as suas descobertas de dados confidenciais que estão na região atual e relatar ocorrências de informações financeiras (e nenhuma outra categoria de dados confidenciais) em objetos do S3.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Para o Microsoft Windows, usando o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

Onde:

- *classificationDetails.result.sensitiveData.detections.type* especifica o nome JSON do campo de Categoria de dados confidenciais.
- *EqExactMatch* especifica o operador de correspondência exata igual.
- *FINANCIAL_INFORMATION* é um valor enumerado para o campo Categoria de dados confidenciais.

Exemplo 3: Filtrar descobertas com base em um intervalo de tempo fixo

Este exemplo usa o comando list-findings para recuperar IDs de descobertas de todas as suas descobertas que estão na região atual e foram criadas entre 07 horas UTC de 5 de outubro de 2020 e 07 horas UTC de 5 de novembro de 2020 (inclusive).

Para Linux, macOS ou Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Para o Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

Onde:

- *createdAt* especifica o nome JSON do campo Criado em.
- *gte* especifica o operador maior ou igual a .
- *1601881200000* é a primeira data e hora (como um timestamp Unix em milissegundos) no intervalo de tempo.
- *lte* especifica o operador menor ou igual a .
- *1604559600000* é a última data e hora (como um timestamp Unix em milissegundos) no intervalo de tempo.

Exemplo 4: filtrar descobertas com base no status de supressão

Este exemplo usa o comando list-findings para recuperar IDs de descobertas de todas as suas descobertas que estão na região atual e foram suprimidas (arquivadas automaticamente) por uma regra de supressão.

Para Linux, macOS ou Unix:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Para o Microsoft Windows:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

Onde:

- *archived* especifica o nome JSON do campo Arquivado.
- *eq* especifica o operador igual.
- *true* é um valor booleano para o campo Arquivado.

Exemplo 5: filtrar descobertas com base em vários campos e tipos de valores

Este exemplo usa o comando list-findings para recuperar IDs de descoberta de todas as descobertas de dados confidenciais que estão na região atual e que correspondem aos seguintes critérios: foram criadas entre 07 horas UTC de 5 de outubro de 2020 e 07 horas UTC de 5 de novembro de 2020 (exclusivamente); relatar ocorrências de dados financeiros e nenhuma outra categoria de dados

confidenciais em objetos do S3; e não foram suprimidas (arquivadas automaticamente) por uma regra de supressão.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade:

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Para o Microsoft Windows, usando o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade:

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

Onde:

- *createdAt* especifica o nome JSON para o campo Created at, e:
  - *gt* especifica o operador maior ou igual a .
  - *1601881200000* é a primeira data e hora (como um timestamp Unix em milissegundos) no intervalo de tempo.
  - *lt* especifica o operador menor ou igual a .
  - *1604559600000* é a última data e hora (como um timestamp Unix em milissegundos) no intervalo de tempo.
- *classificationDetails.result.sensitiveData.detections.type* especifica o nome JSON do campo de Categoria de dados confidenciais, e:
  - *EqExactMatch* especifica o operador de correspondência exata igual.
  - *FINANCIAL_INFORMATION* é um valor enumerado para o campo.
- *archived* especifica o nome JSON do campo Arquivado, e:
  - *eq* especifica o operador igual.
  - *false* é um valor booleano para o campo.

Como criar e gerenciar regras de filtro para descobertas

Uma regra de filtro é um conjunto de critérios de filtro que você cria e salva para usar novamente ao analisar as descobertas no console do Amazon Macie. As regras de filtro podem ajudá-lo a realizar uma análise consistente das descobertas que têm características específicas. Por exemplo, você pode criar uma regra de filtro para analisar todas as descobertas de políticas de alta severidade para buckets do S3 que contêm objetos não criptografados e outra regra de filtro para analisar todas as descobertas de dados confidenciais de alta severidade que relatam tipos específicos de dados confidenciais.

Observe que as regras de filtro são diferentes das regras de supressão. Uma regra de supressão é um conjunto de critérios de filtro que você cria e salva para arquivar automaticamente descobertas que correspondam aos critérios da regra. Embora os dois tipos de regras armazenem e apliquem critérios de filtro, uma regra de filtro não executa nenhuma ação nas descobertas que correspondam aos critérios da regra. Em vez disso, uma regra de filtro determina apenas quais descobertas aparecem no console depois que você aplica a regra. Para obter mais informações sobre regras de supressão, consulte Suprimir descobertas.

Para criar e gerenciar regras de filtros, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Os tópicos a seguir explicam como fazer isso. Para a API, os tópicos incluem exemplos de como realizar essas tarefas usando o AWS Command Line Interface (AWS CLI). Você também pode realizar essas tarefas usando uma versão atual de outra ferramenta de linha de comando da AWS ou de um SDK AWS, ou enviando solicitações HTTPS diretamente para o Macie. Para obter mais informações sobre AWS ferramentas e SDKs, consulte Ferramentas para aproveitar AWS.

Tópicos

Como criar regras de filtro

Ao criar uma regra de filtro, você especifica critérios de filtro, um nome e, opcionalmente, uma descrição da regra. Você pode criar uma regra de filtro usando o console do Amazon Macie ou a API do Amazon Macie.

Console

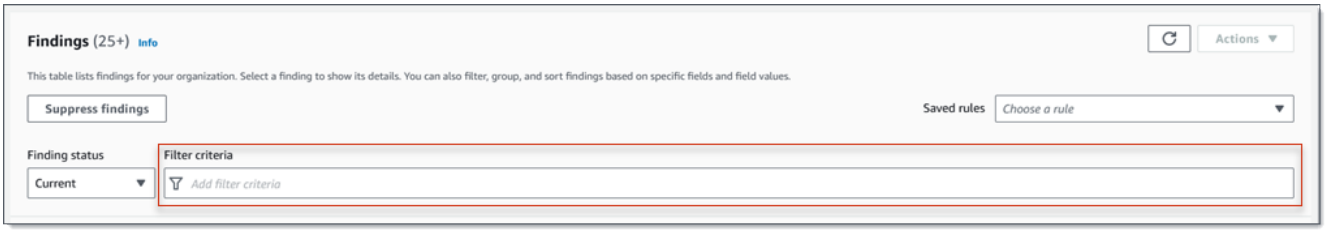
Siga estas etapas para criar uma regra de filtro usando o console do Amazon Macie.

Para criar uma regra de filtro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.

> **Tip**
>
> Para usar uma regra de filtro existente como ponto de partida, selecione a regra na lista Regras salvas.
> Você também pode simplificar a criação de uma regra ao analisar e detalhar antes as descobertas por meio de um grupo lógico predefinido. Se você fizer isso, o Macie criará e aplicará automaticamente as condições do filtro apropriadas, o que pode ser um ponto de partida útil para se criar uma regra. Para fazer isso, selecione Por bucket, Por tipo ou Por trabalho no painel de navegação (em Descobertas) e, em seguida, selecione um item na tabela. No painel de detalhes, selecione o link do campo a analisar.

3. Na caixa Critérios de filtro, adicione condições que definam os critérios de filtro para a regra.



Para saber como adicionar condições de filtro, consulte Como criar e aplicar filtros às descobertas.

4. Ao terminar de definir os critérios de filtro para a regra, selecione Salvar regra na caixa Critérios de filtro.

5. Em Regra de filtro, insira um nome e, opcionalmente, uma descrição da regra.
6. Escolha Salvar.

API

Para criar uma regra de filtro programaticamente, use a operação CreateFindingsFilter da API do Amazon Macie e especifique os valores apropriados para os parâmetros necessários:

- Para o parâmetro `action`, especifique `NOOP` para garantir que o Macie não suprima (arquive automaticamente) as descobertas que correspondam aos critérios da regra.
- Para o parâmetro `criterion`, especifique um mapa de condições que defina os critérios de filtro para a regra.

  No mapa, cada condição deve especificar um campo, um operador e um ou mais valores para o campo. O tipo e o número de valores dependem do campo e do operador que você escolher. Para obter informações sobre os campos, operadores e tipos de valores que você pode usar em uma condição, consulteCampos para filtrar descobertas, Usando operadores em condições e Especificando valores para campos.

Para criar uma regra de filtro usando AWS CLI, execute o comando create-findings-filter e especifique os valores apropriados para os parâmetros necessários. Os exemplos a seguir criam uma regra de supressão que retorna todas as descobertas de dados confidenciais que estão atualmente em Região da AWS e relatam ocorrências de informações pessoais (e nenhuma outra categoria de dados confidenciais) em objetos do S3.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade.

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

Este exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

Onde:

- *my_filter_rule* é o nome personalizado da regra.
- `criterion` é um mapa das condições do filtro para a regra:
  - *classificationDetails.result.sensitiveData.category* é o nome JSON do campo Categoria de dados confidenciais.
  - *EqExactMatch* especifica o operador de correspondência exata igual.
  - *PERSONAL_INFORMATION* é um valor enumerado para o campo Categoria de dados confidenciais.

Se o comando for executado com êxito, você receberá um resultado semelhante a este.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra de filtro que foi criada e `id` é o identificador exclusivo da regra.

Para obter exemplos adicionais de critérios de filtro, consulte Como filtrar descobertas de forma programática com a API do Amazon Macie.

Aplicação de regras de filtro

Quando você aplica uma regra de filtro, o Amazon Macie usa os critérios da regra para determinar quais descobertas incluir ou excluir da sua visualização das descobertas no console. O Macie também exibe os critérios para ajudá-lo a determinar quais critérios você aplicou.

Observe que as regras de filtro foram criadas para uso com o console do Amazon Macie. Você não pode usá-las diretamente em consultas enviadas programaticamente usando a API do Amazon Macie. No entanto, se você estiver usando a API para consultar descobertas, poderá recuperar os critérios de filtro de uma regra usando a operação GetFindingsFilter. Em seguida, você pode adicionar os critérios à sua consulta. Para obter informações sobre como especificar critérios de filtro em uma consulta, consulte Como criar e aplicar filtros às descobertas.

Siga estas etapas para filtrar as descobertas no console aplicando uma regra de filtro.

Para aplicar uma regra de filtro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na lista regras salvas, selecione a regra de filtro que você deseja aplicar. O Macie aplica os critérios da regra e exibe os critérios na caixa Filtrar critérios.
4. (Opcional) Para refinar os critérios, use a caixa Critérios de filtro para adicionar ou remover condições do filtro. Se fizer isso, suas alterações não afetarão as configurações da regra. O Macie não salvará nenhuma de suas alterações, a menos que você as salve explicitamente como uma nova regra.
5. Para aplicar uma regra de filtro diferente, repita a etapa 3.

Depois de aplicar uma regra de filtro, você pode remover rapidamente todos os critérios de filtro da sua exibição escolhendo o X na caixa Critérios de filtro.

Como alterar as regras de filtro

Você pode modificar as configurações de uma regra de filtro a qualquer momento usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode atribuir e gerenciar tags para a regra.

Uma tag é um rótulo que você define e atribui a determinados tipos de recursos AWS. Cada tag consiste em uma chave de tag necessária e em um valor de tag opcional. As tags podem ajudá-lo a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.

Console

Siga estas etapas para alterar as configurações de uma regra de filtro existente usando o console do Amazon Macie.

Para alterar uma regra de filtro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na lista Regras salvas, selecione o ícone de edição () ao lado da regra de filtro que deseja alterar.
4. Faça o seguinte:
   - Para alterar os critérios de filtro da regra, use a caixa Critérios de filtro para inserir condições para os critérios desejados. Para saber como, consulte Como criar e aplicar filtros às descobertas.
   - Para alterar o nome da regra, insira um novo nome na caixa Nome em Regra de filtro.
   - Para alterar a descrição da regra, insira uma nova descrição na caixa Descrição em Regra de filtro.
   - Para atribuir, analisar ou editar tags para a regra, selecione Gerenciar tags em Regra de filtro. Em seguida, revise altere as tags conforme necessário. Uma regra pode ter até 50 tags.
5. Quando terminar de fazer as alterações, escolha Salvar.

API

Para alterar uma regra de filtro programaticamente, use a operação UpdateFindingsFilter da API do Amazon Macie. Ao enviar sua solicitação, use os parâmetros compatíveis para especificar um novo valor para cada configuração que você deseja alterar.

Para o parâmetro `id`, especifique o identificador único da regra que será alterada. Você pode obter esse identificador usando a operação ListFindingsFilter para recuperar obter uma lista de regras de supressão e de filtro para a sua conta. Se estiver usando a AWS CLI, execute o comando list-findings-filters para recuperar essa lista.

Para alterar uma regra de filtro usando o AWS CLI, execute o comando update-findings-filter e use os parâmetros suportados para especificar um novo valor para cada configuração que você deseja alterar. Por exemplo, o comando a seguir altera o nome de uma regra de filtro existente.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

Onde:

- *9b2b4508-aa2f-4940-b347-d1451example* é o identificador exclusivo para a regra.
- *personal_information_only* é o novo nome para a regra.

Se o comando for executado com êxito, você receberá um resultado semelhante a este.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra que foi alterada e `id` é o identificador único e exclusivo da regra.

Da mesma forma, o exemplo a seguir converte uma regra de supressão para uma regra de filtro alterando o valor do parâmetro `action` de `ARCHIVE` para `NOOP`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

Onde:

- *8a1c3508-aa2f-4940-b347-d1451example* é o identificador exclusivo para a regra.
- *NOOP* é a nova ação que o Macie deve realizar em descobertas que correspondam aos critérios da regra — não execute nenhuma ação (não suprima as descobertas).

Se o comando for executado com êxito, você receberá um resultado semelhante ao seguinte:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra que foi alterada e `id` é o identificador único e exclusivo da regra.

Como excluir regras de filtro

Você pode excluir uma regra de filtro a qualquer momento usando o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para excluir uma regra de filtro usando o console do Amazon Macie.

Para excluir uma regra de filtro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na lista Regras salvas, selecione o ícone de edição () ao lado da regra de filtro que deseja excluir.
4. Em Regra de filtro, selecione Excluir.

API

Para excluir uma regra de filtro programaticamente, use a operação DeleteFindingsFilter da API do Amazon Macie. Para o parâmetro `id`, especifique o identificador único para a regra de filtro a excluir. Você pode obter esse identificador usando a operação ListFindingsFilter para recuperar obter uma lista de regras de supressão e de filtro para a sua conta. Se estiver usando a AWS CLI, execute o comando list-findings-filters para recuperar essa lista.

Para excluir uma regra de filtro usando o AWS CLI, execute o comando delete-findings-filter. Por exemplo:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

Onde *9b2b4508-aa2f-4940-b347-d1451example* é o identificador exclusivo da regra de filtro que será excluída.

Se o comando for executado com sucesso, o Macie retornará uma resposta HTTP 200 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500 que indica o motivo porque operação falhou.

Campos para filtrar descobertas

Para ajudar você a analisar as descobertas com mais eficiência, o console do Amazon Macie e a API do Amazon Macie fornecem acesso a vários conjuntos de campos para filtrar as descobertas:

- Campos comuns – Esses campos armazenam dados que se aplicam a qualquer tipo de descoberta. Eles se correlacionam com atributos comuns das descobertas, como gravidade, tipo de descoberta e ID da descoberta.
- Campos de recursos afetados – Esses campos armazenam dados sobre os recursos aos quais uma descoberta se aplica, como nome, tags e configurações de criptografia de um bucket ou objeto do S3 afetado.
- Campos de política – Esses campos armazenam dados específicos das descobertas da política, como a ação que produziu uma descoberta e a entidade que executou a ação.
- Campos de classificação de dados sigilosos – Esses campos armazenam dados específicos das descobertas de dados sigilosos, como a categoria e os tipos de dados sigilosos que Macie encontrou em um objeto do S3 afetado.

Um filtro pode usar uma combinação de campos de qualquer um dos conjuntos anteriores.

Os tópicos dessa seção listam e descrevem campos individuais que você pode usar para filtrar descobertas. Para obter detalhes adicionais sobre esses campos, incluindo quaisquer relações entre os campos, consulte Descobertas na Referência de API do Amazon Macie.

Tópicos

Campos comuns

A tabela a seguir lista e descreve os campos que você pode usar para filtrar descobertas com base em atributos de descoberta comuns. Esses campos armazenam dados que se aplicam a qualquer tipo de descoberta.

Na tabela, a coluna Campo indica o nome do campo no console do Amazon Macie. A coluna do campo JSON usa notação de pontos para indicar o nome do campo nas representações JSON das descobertas e na API Amazon Macie. A coluna Descrição fornece uma breve descrição dos dados que o campo armazena e indica quaisquer requisitos para valores de filtro. A tabela é classificada em ordem alfabética crescente por campo e, em seguida, por campo JSON.

Campo	Campo JSON	Descrição
ID da conta*	`accountId`	O identificador exclusivo para o Conta da AWS ao qual a descoberta se aplica. Normalmente, essa é a conta que é proprietária do recurso afetado.
—	`archived`	Um valor booleano que especifica se a descobert a foi suprimida (arquivada automaticamente) por uma regra de supressão. Para usar esse campo em um filtro no console, selecione uma opção no menu Status da descoberta Menu: Arquivado (somente suprimido), Atual (somente não suprimido) ou Tudo (suprimido e não suprimido).
Categoria	`category`	A categoria da descoberta. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Na API, os valores válidos são: `CLASSIFICATION` , para

Campo	Campo JSON	Descrição
		uma descoberta de dados sigilosos; e, `POLICY`, para uma descoberta de política.
—	`count`	O número total de ocorrências da descoberta. Para descobertas de dados sigilosos, esse valor é sempre 1. Todas as descobertas de dados sigilosos são consideradas únicas. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.
Criado em	`createdAt`	A data e a hora em que o Macie criou a descoberta. Você pode usar esse campo para definir um intervalo de tempo para um filtro.
ID* da descoberta	`id`	O identificador único para a descoberta. Essa é uma sequência aleatória que o Macie gera e atribui a uma descoberta ao criar a descoberta.

Campo	Campo JSON	Descrição
Tipo* de descoberta	`type`	O tipo da descoberta — por exemplo, `SensitiveData:S3Object/Personal` ou `Policy:IAMUser/S3BucketPublic` . O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos na API, consulte FindingTypea Referência de API do Amazon Macie.
Região	`region`	A Região da AWS em que a Macie criou a descoberta, por exemplo exemplo, ou `us-east-1` ou `ca-central-1`

Campo	Campo JSON	Descrição
Amostra	`sample`	Um valor booleano que especifica se a descoberta é uma amostra de descoberta. Uma amostra de descobert a é uma descoberta que usa dados de exemplo e valores de marcadores para demonstrar os tipos de informações que uma descoberta pode conter. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro.
Gravidade	`severity.description`	A representação qualitativa da gravidade da descoberta. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Na API, os valores válidos são `Low`, `Medium` e `High`.

Campo	Campo JSON	Descrição
Atualizado em	`updatedAt`	A data e a hora em que a descoberta foi atualizada pela última vez. Para descobert as de dados sigilosos, esse valor é igual ao valor do campo Criado em. Todas as descobertas de dados sigilosos são consideradas novas (únicas). Você pode usar esse campo para definir um intervalo de tempo para um filtro.

* Para especificar vários valores para esse campo no console, adicione uma condição que use o campo e que especifique um valor distinto para o filtro, e então, repita essa etapa para cada valor adicional. Para fazer isso com a API, use uma matriz que lista os valores a serem usados para o filtro.

Campos de recursos afetados

Os tópicos a seguir listam e descrevem os campos que você pode usar para filtrar as descobertas com base no recurso ao qual uma descoberta se aplica. Os tópicos são organizados por tipo de recurso.

Tópicos

- Bucket do S3
- objeto do S3

Bucket do S3

A tabela a seguir lista e descreve os campos que você pode usar para filtrar as descobertas com base nas características do Bucket do S3 ao qual uma descoberta se aplica.

Na tabela, a coluna Campo indica o nome do campo no console do Amazon Macie. A coluna do campo JSON usa notação de pontos para indicar o nome do campo nas representações JSON das descobertas e na API Amazon Macie. (Nomes de campo JSON mais longos usam a sequência de caracteres de nova linha (\n) para melhorar a legibilidade.) A coluna Descrição fornece uma breve descrição dos dados que o campo armazena e indica quaisquer requisitos para valores de filtro. A tabela é classificada em ordem alfabética crescente por campo e, em seguida, por campo JSON.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Bucket.createdAt`	A data e a hora em que o bucket afetado foi criado, ou alterações, como edições na política do bucket, foram feitas mais recentemente no bucket afetado. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.
Criptografia padrão para buckets do S3	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	O algoritmo de criptografia do lado do servidor usado por padrão para criptografar objetos que são adicionados ao bucket afetado. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos para a API, consulte a

Campo	Campo JSON	Descrição
		EncryptionTypeReferência de API do Amazon Macie.
Id da chave KMS com criptografia de bucket S3*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	O nome do recurso da Amazon (ARN) ou o identificador exclusivo (ID da chave) do AWS KMS key que é usado por padrão para criptografar objetos que são adicionados ao bucket afetado.
Criptografia de bucket do S3 necessária pela política de bucket	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	Especifica se a política de bucket para o bucket afetado exige criptografia de objetos no lado do servidor quando objetos são adicionados ao bucket. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos na API, consulte S3Bucket na Referência de API do Amazon Macie.
O nome do bucket do S3*	`resourcesAffected.s3Bucket.name`	O nome completo do bucket afetado.

Campo	Campo JSON	Descrição
Nome de exibição do proprietário do bucket S3*	`resourcesAffected.s3Bucket.owner.displayName`	O nome de exibição do AWS uauário proprietário do bucket afetado.
Permissão de acesso público ao bucket S3	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	Especifica se o bucket afetado pode ser acessado publicamente com base em uma combinação de configurações de permissões que se aplicam ao bucket. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos para a API, consulte a BucketPublicAccessReferência de API do Amazon Macie.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		Um valor booleano que especifica se o Amazon S3 bloqueia listas de controle de acesso (ACLs) públicas para o bucket afetado e objetos no bucket. Essa é uma configuração de bloqueio de acesso público em nível de conta para o bucket.
		
		Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Um valor booleano que especifica se o Amazon S3 bloqueia listas de controle de acesso públicas para o bucket afetado. Essa é uma configuração de bloqueio de acesso público em nível de conta para o bucket.
		
		Esse campo não está disponível como opção de filtro no console.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Um valor booleano que especifica se o Amazon S3 ignora ACLs públicas para o bucket afetado e objetos no bucket. Essa é uma configuração de bloqueio de acesso público em nível de conta para o bucket.
		
		Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Um valor booleano que especifica se o Amazon S3 restringe políticas públicas do bucket para o bucket afetado. Essa é uma configuração de bloqueio de acesso público em nível de conta para o bucket. Esse campo não está disponível como opção de filtro no console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	Um valor booleano que especifica se a ACL em nível de bucket para o bucket afetado concede ao público em geral permissões de acesso de leitura para o bucket. Esse campo não está disponível como opção de filtro no console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	Um valor booleano que especifica se a ACL em nível de bucket para o bucket afetado concede ao público em geral permissões de acesso de gravação para o bucket. Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAcls`	Um valor booleano que especifica se o Amazon S3 bloqueia ACLs públicas para o bucket afetado e objetos no bucket. Essa é uma configuração de bloqueio de acesso público em nível de bucket para o bucket. Esse campo não está disponível como opção de filtro no console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy`	Um valor booleano que especifica se o Amazon S3 bloqueia políticas públicas de bucket para o bucket afetado. Essa é uma configuração de bloqueio de acesso público em nível de bucket para o bucket. Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls`	Um valor booleano que especifica se o Amazon S3 ignora ACLs públicas para o bucket afetado e objetos no bucket. Essa é uma configuração de bloqueio de acesso público em nível de bucket para o bucket. Esse campo não está disponível como opção de filtro no console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Um valor booleano que especifica se o Amazon S3 restringe políticas públicas do bucket para o bucket afetado. Essa é uma configuração de bloqueio de acesso público em nível de bucket para o bucket. Esse campo não está disponível como opção de filtro no console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	Um valor booleano que especifica se a política do bucket afetado permite que o público em geral tenha acesso de leitura ao bucket. Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	Um valor booleano que especifica se a política do bucket afetado permite que o público em geral tenha acesso de gravação ao bucket. Esse campo não está disponível como opção de filtro no console.
Chave de tag do Bucket S3*	`resourcesAffected.s3Bucket.tags.key`	Uma chave de tag associada ao bucket afetado.
Valor do tag do Bucket*	`resourcesAffected.s3Bucket.tags.value`	Um valor de tag que é associado ao bucket afetado.

* Para especificar vários valores para esse campo no console, adicione uma condição que use o campo e que especifique um valor distinto para o filtro, e então, repita essa etapa para cada valor adicional. Para fazer isso com a API, use uma matriz que lista os valores a serem usados para o filtro.

objeto do S3

A tabela a seguir lista e descreve os campos que você pode usar para filtrar as descobertas com base nas características do Bucket do S3 ao qual uma descoberta se aplica.

Na tabela, a coluna Campo indica o nome do campo no console do Amazon Macie. A coluna do campo JSON usa notação de pontos para indicar o nome do campo nas representações JSON das descobertas e na API Amazon Macie. A coluna Descrição fornece uma breve descrição dos dados que o campo armazena e indica quaisquer requisitos para valores de filtro. A tabela é classificada em ordem alfabética crescente por campo e, em seguida, por campo JSON.

Campo	Campo JSON	Descrição

Campo	Campo JSON	Descrição
Id da chave KMS com criptografia de objeto S3*	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	O nome do recurso da Amazon (ARN) ou o identificador exclusivo (ID da chave) do AWS KMS key que é usado por padrão para criptografar o objeto afetado.
Tipo de criptografia de objetos S3	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	O algoritmo de criptografia do lado do servidor usado para criptografar o objeto afetado. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos para a API, consulte a EncryptionTypeReferência de API do Amazon Macie.
—	`resourcesAffected.s3Object.extension`	A extensão do nome do arquivo do objeto afetado. Para objetos que não têm uma extensão de nome de arquivo, especifique "" como o valor do filtro. Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`resourcesAffected.s3Object.lastModified`	A data e a hora em que o objeto afetado foi criado ou alterado pela última vez, o que for mais recente. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.
Chave de objeto S3*	`resourcesAffected.s3Object.key`	O nome completo (chave) do objeto afetado, incluindo o prefixo do objeto, se aplicável.
—	`resourcesAffected.s3Object.path`	O caminho completo para o objeto afetado, incluindo o nome do bucket afetado e o nome do objeto (chave). Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
acesso público ao objeto S3	`resourcesAffected.s3Object.publicAccess`	Um valor booleano que especifica se o bucket afetado pode ser acessado publicamente com base em uma combinação de configurações de permissões que se aplicam ao bucket. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro.
Chave de tag de objeto S3*	`resourcesAffected.s3Object.tags.key`	Uma chave de tag associada ao bucket afetado.
Valor da tag de objeto S3*	`resourcesAffected.s3Object.tags.value`	Um valor de tag que é associado ao objeto afetado.

* Para especificar vários valores para esse campo no console, adicione uma condição que use o campo e que especifique um valor distinto para o filtro, e então, repita essa etapa para cada valor adicional. Para fazer isso com a API, use uma matriz que lista os valores a serem usados para o filtro.

Campos de política

A tabela a seguir lista e descreve os campos que você pode usar para filtrar descobertas de políticas. Esses campos armazenam dados específicos das descobertas de políticas.

Na tabela, a coluna Campo indica o nome do campo no console do Amazon Macie. A coluna do campo JSON usa notação de pontos para indicar o nome do campo nas representações JSON das descobertas e na API Amazon Macie. (Nomes de campo JSON mais longos usam a sequência de caracteres de nova linha (\n) para melhorar a legibilidade.) A coluna Descrição fornece uma breve

descrição dos dados que o campo armazena e indica quaisquer requisitos para valores de filtro. A tabela é classificada em ordem alfabética crescente por campo e, em seguida, por campo JSON.

Campo	Campo JSON	Descrição
Tipo de ação	`policyDetails.action.actionType`	O tipo de ação que produziu a descoberta. O único valor válido é para este campo é `AWS_API_CALL` .
Nome da chamada de API*	`policyDetails.action.apiCallDetails.api`	O nome da operação que foi invocada mais recentemente e produziu a descoberta — por exemplo, `PutBucketPublicAccessBlock` .
Nome do serviço de API*	`policyDetails.action.apiCallDetails.apiServiceName`	O URL do AWS service (Serviço da AWS) que fornece a operação que foi invocada e produziu a descoberta, por exemplo, `s3.amazonaws.com` .
—	`policyDetails.action.apiCallDetails.firstSeen`	A primeira data e hora em que qualquer operação foi invocada e produziu a descoberta. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.
—	`policyDetails.action.apiCallDetails.lastSeen`	A data e a hora mais recentes em que a operação especificada (nome da chamada de

Campo	Campo JSON	Descrição
		API ou `api`) foi invocada e produziu a descoberta. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.
—	`policyDetails.actor.domainDetails.domainName`	O nome de domínio do dispositivo usado para realizar a ação. Esse campo não está disponível como opção de filtro no console.
Cidade IP*	`policyDetails.actor.ipAddressDetails.ipCity.name`	O nome da cidade de origem do endereço IP do dispositivo que foi usado para realizar a ação.
País IP*	`policyDetails.actor.ipAddressDetails.ipCountry.name`	O nome da cidade de origem do endereço IP do dispositivo que foi usado para realizar a ação, poe exemplo, `United States`.

Campo	Campo JSON	Descrição
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	O Número de Sistema Autônomo (ASN) do sistema autônomo que incluía o endereço IP do dispositivo usado para realizar a ação. Esse campo não está disponível como opção de filtro no console.
Proprietário do IP ASN org*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	O identificador da organização associado ao ASN do sistema autônomo que inclui o endereço IP do dispositivo usado para realizar a ação.
ISP proprietário do IP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	O nome do provedor de serviços de Internet (ISP) que possuía o endereço IP do dispositivo usado para realizar a ação.
Endereço de IP V4*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	O endereço IPv4 (Internet Protocol versão 4) do dispositivo que foi usado para realizar a ação.

Campo	Campo JSON	Descrição
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `AssumeRole` do API AWS STS, a ID da chave de acesso AWS que identifica as credenciais. Esse campo não está disponível como opção de filtro no console.
Identidade do usuário, função assumida, ID da conta*	`policyDetails.actor.userIdentity.assumedRole.accountId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `AssumeRole` do API AWS STS, o identificador único Conta da AWS que é proprietário da entidade que foi usada para obter as credenciais.
ID da entidade principal assumida plea identidade do usuário*	`policyDetails.actor.userIdentity.assumedRole.principalId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `AssumeRole` do API AWS STS, o identificador único para a entidade que foi usada para obter as credenciais.

Campo	Campo JSON	Descrição
Identidade do usuário, função assumida, ARN da sessão*	`policyDetails.actor.userIdentity.assumedRole.arn`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `AssumeRole` do API AWS STS, o nome do recurso da Amazon (ARN) do conta fonte, usuário do IAM, ou a função que foi usada para obter as credenciais.

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a `AssumeRole` operação da API AWS STS, a origem das credenciais de segurança temporárias — por exemplo, `Root`, `IAMUser` ou `Role`.
		
		Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.userName`
		Para uma ação realizada com credenciais de segurança temporárias obtidas usando a operação `AssumeRole` da API AWS STS, o nome ou apelido do usuário ou função que emitiu a sessão. Observe que esse valor é nulo se as credenciais foram obtidas de uma conta raiz que não tem um apelido.
		
		Esse campo não está disponível como opção de filtro no console.

ID da conta AWS de identidade do usuário*	`policyDetails.actor.userIdentity.awsAccount.accountId`	Para uma ação realizada usando as credenciais para outra Conta da AWS, o identificador único da conta.
Identidade do usuário ID da entidade principal da conta AWS*	`policyDetails.actor.userIdentity.awsAccount.principalId`	Para uma ação realizada usando as credenciais para outra Conta da AWS, o identificador único para a entidade que realizou a ação.
Serviço de identidade de usuário AWS invocado por	`policyDetails.actor.userIdentity.awsService.invokedBy`	Para uma ação realizada por uma conta que pertence a um AWS service (Serviço da AWS), o nome do serviço.

Campo	Campo JSON	Descrição
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `GetFederationToken` da API AWS STS, a ID da chave de acesso AWS que identifica as credenciais. Esse campo não está disponível como opção de filtro no console.
Identidade federada do usuário da sessão ARN*	`policyDetails.actor.userIdentity.federatedUser.arn`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `GetFederationToken` da API AWS STS, a ARN da entidade que foi usada para obter as credenciais.
Identidade do usuário ID da conta de usuário federada*	`policyDetails.actor.userIdentity.federatedUser.accountId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `GetFederationToken` da API AWS STS, o identificador único Conta da AWS que é proprietário da entidade que foi usada para obter as credenciais.

Campo	Campo JSON	Descrição
ID principal do usuário da entidade principal federada*	`policyDetails.actor.userIdentity.federatedUser.principalId`	Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `GetFederationToken` da API AWS STS, o identificador único para a entidade que foi usada para obter as credencias.

—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n`
	
	`sessionIssuer.type`
		Para uma ação realizada com credenciais de segurança temporárias que foram obtidas usando a operação `GetFederationToken` da API AWS STS, a origem das credenciais de segurança temporárias — por exemplo, `Root`, `IAMUser` ou `Role`.
		
		Esse campo não está disponível como opção de filtro no console.

Campo	Campo JSON	Descrição
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	Para uma ação realizada com credenciais de segurança temporárias obtidas usando a operação `GetFederationToken` da API AWS STS, o nome ou apelido do usuário ou função que emitiu a sessão. Observe que esse valor é nulo se as credenciais foram obtidas de uma conta raiz que não tem um apelido. Esse campo não está disponível como opção de filtro no console.
Identidade da conta do usuário do IAM*	`policyDetails.actor.userIdentity.iamUser.accountId`	Para uma ação realizada usando as credenciais de um usuário do IAM, o identificador único para a entidade Conta da AWS que é associada com o usuário do IAM que realizou a ação.
Identidade do usuário ID da entidade principal do IAM*	`policyDetails.actor.userIdentity.iamUser.principalId`	Para uma ação realizada usando as credenciais de um usuário do IAM, o identificador único para o usuário do IAM que realizou a ação.
Identidade de usuário Nome de usuário do IAM *	`policyDetails.actor.userIdentity.iamUser.userName`	Para uma ação realizada usando as credenciais de um usuário do IAM, o nome de usuário do usuário do IAM que realizou a ação.

Campo	Campo JSON	Descrição
ID da conta raiz da identidade do usuário*	`policyDetails.actor.userIdentity.root.accountId`	Para uma ação realizada usando as credenciais para sua Conta da AWS, o identificador único para a conta.
ID da entidade principal raiz da identidade do usuário*	`policyDetails.actor.userIdentity.root.principalId`	Para uma ação realizada usando as credenciais para a sua Conta da AWS, o identificador único para a entidade que realizou a ação.
User identity type	`policyDetails.actor.userIdentity.type`	O tipo de entidade que realizou a ação que produziu a descoberta. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos para a API, consulte a UserIdentityTypeReferência de API do Amazon Macie.

* Para especificar vários valores para esse campo no console, adicione uma condição que use o campo e que especifique um valor distinto para o filtro, e então, repita essa etapa para cada valor adicional. Para fazer isso com a API, use uma matriz que lista os valores a serem usados para o filtro.

Campos de classificação de dados sigilosos

A tabela a seguir lista e descreve campos que você pode usar para filtrar descobertas de dados sigilosos. Esses campos armazenam dados específicos para descobertas de dados sigilosos.

Na tabela, a coluna Campo indica o nome do campo no console do Amazon Macie. A coluna do campo JSON usa notação de pontos para indicar o nome do campo nas representações JSON das

descobertas e na API Amazon Macie. A coluna Descrição fornece uma breve descrição dos dados que o campo armazena e indica quaisquer requisitos para valores de filtro. A tabela é classificada em ordem alfabética crescente por campo e, em seguida, por campo JSON.

Campo	Campo JSON	Descrição
ID do identificador de dados personalizados*	`classificationDetails.result.customDataIdentifiers.detections.arn`	O identificador exclusivo do identificador de dados personalizados que detectou os dados e produziu a descoberta.
Nome do identificador de dados personalizados*	`classificationDetails.result.customDataIdentifiers.detections.name`	O nome do identificador de dados personalizados que detectou os dados e produziu a descoberta.
Contagem total de identificadores de dados personalizados	`classificationDetails.result.customDataIdentifiers.detections.count`	O número total de ocorrências de dados que foram detectadas por identificadores de dados personalizados e produziram a descoberta. Você pode usar esse campo para definir um intervalo numérico para um filtro.
ID do trabalho*	`classificationDetails.jobId`	O identificador exclusivo do trabalho de descoberta de dados sigilosos que produziu a descoberta.
Tipo da origem	`classificationDetails.originType`	Como o Macie encontrou os dados sigilosos que produziram a descoberta: `AUTOMATED_SENSITIVE_DATA_DI`

Campo	Campo JSON	Descrição
		`SCOVERY` ou `SENSITIVE_DATA_DISCOVERY_JOB` .
—	`classificationDetails.result.mimeType`	O tipo de conteúdo, como um tipo MIME, ao qual a descoberta se aplica; por exemplo, `text/csv` para um arquivo CSV ou `application/pdf` para um arquivo Adobe Portable Document Format. Esse campo não está disponível como opção de filtro no console.
—	`classificationDetails.result.sizeClassified`	O tamanho total do armazenamento, em bytes, do objeto S3 ao qual a descoberta se aplica. Esse campo não está disponível como opção de filtro no console. Com a API, você pode usar esse campo para definir um intervalo numérico para um filtro.

Campo	Campo JSON	Descrição
Código de status do resultado*	`classificationDetails.result.status.code`	O status da descoberta. Os valores válidos são: • `COMPLETE` – O Macie concluiu sua análise do objeto. • `PARTIAL` – O Macie analisou somente um subconjunto dos dados do objeto. Por exemplo, o objeto é um arquivo que contém arquivos em um formato incompatível. • `SKIPPED` – O Macie não conseguiu analisar o objeto. Por exemplo, o objeto é um arquivo malformado.
Categoria de dados confidenciais	`classificationDetails.result.sensitiveData.category`	A categoria de dados sigilosos que foram detectados e produziram a descoberta. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Na API, os valores válidos são: `CREDENTIALS` , `FINANCIAL_INFORMATION` e `PERSONAL_INFORMATION` .

Campo	Campo JSON	Descrição
Tipo de detecção de dados sigilosos	`classificationDetails.result.sensitiveData.detections.type`	O tipo de dados sigilosos que foram detectados e produziram a descoberta. O console fornece uma lista de valores para escolher quando você adiciona esse campo a um filtro. Para obter uma lista de valores válidos para o console e a API, consulte Detecção de dados sigilosos.
Contagem total de dados sigilosos	`classificationDetails.result.sensitiveData.detections.count`	O número total de ocorrências dos dados sigilosos que foram detectados e produziram a descoberta. Você pode usar esse campo para definir um intervalo numérico para um filtro.

* Para especificar vários valores para esse campo no console, adicione uma condição que use o campo e que especifique um valor distinto para o filtro, e então, repita essa etapa para cada valor adicional. Para fazer isso com a API, use uma matriz que lista os valores a serem usados para o filtro.

Detecção de dados sigilosos

Os tópicos a seguir listam valores que você pode especificar para o campo Tipo de detecção de dados sigilosos em um filtro. (O nome JSON desse campo é `classificationDetails.result.sensitiveData.detections.type`.) Os tópicos são organizados pelas categorias de dados sigilosos que o Macie pode detectar usando identificadores de dados gerenciados.

Categorias

- Credenciais
- Informações financeiras
- Informações pessoais: informações de saúde pessoal (Personal health information - PHI)
- Informações pessoais: informações de identificação pessoal (PII)

Para saber mais sobre o identificador de dados gerenciados para um tipo específico de dados sigilosos, consulte Referência detalhada: identificadores de dados gerenciados pelo Amazon Macie.

Credenciais

Você pode especificar os valores a seguir para filtrar descobertas que relatam ocorrências de dados de credenciais em objetos do S3.

Tipo de dado sigiloso	Valor do filtro
Chave de acesso secreta da AWS	`AWS_CREDENTIALS`
Chave da API do Google Cloud	`GCP_API_KEY`
Cabeçalho de autorização básica HTTP	`HTTP_BASIC_AUTH_HEADER`
JSON Web Token (JWT)	`JSON_WEB_TOKEN`
Chave privada OpenSSH	`OPENSSH_PRIVATE_KEY`
Chave privada PGP	`PGP_PRIVATE_KEY`
Chave privada do padrão de criptografia de chave pública (PKCS)	`PKCS`
Chave privada PuTTY	`PUTTY_PRIVATE_KEY`
Chave da API Stripe	`STRIPE_CREDENTIALS`

Informações financeiras

Você pode especificar os valores a seguir para filtrar descobertas que relatam ocorrências de informações financeiras em objetos do S3.

Tipo de dado sigiloso	Valor do filtro
Número de conta bancária	`BANK_ACCOUNT_NUMBER` (para o Canadá e os EUA)
Número básico da conta bancária (BBAN)	Dependendo do país ou região: `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Data de validade do cartão de crédito	`CREDIT_CARD_EXPIRATION`
Dados da faixa magnética do cartão de crédito	`CREDIT_CARD_MAGNETIC_STRIPE`
Números de cartão de crédito	`CREDIT_CARD_NUMBER` (para números de cartão de crédito próximos a uma palavra-chave), `CREDIT_CARD_NUMBER_(NO_KEYWORD)` (para números de cartão de crédito que não estejam próximos de uma palavra-chave)
Código de verificação do cartão de crédito	`CREDIT_CARD_SECURITY_CODE`
Número internacional de conta bancária (IBAN)	Dependendo do país ou região: `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_NUMB`

Tipo de dado sigiloso	Valor do filtro
	ER, 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,

Tipo de dado sigiloso	Valor do filtro
	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 as Ilhas Virgens Britânicas)

Informações pessoais: informações de saúde pessoal (Personal health information - PHI)

Você pode especificar os valores a seguir para filtrar descobertas que relatam ocorrências de informações pessoais de saúde (PHI) em objetos do S3.

Tipo de dado sigiloso	Valor do filtro
Número de registro da Agência Antidrogas (DEA)	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Health Insurance Claim Number (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
Número de identificação médica ou do seguro de saúde	Dependendo do país ou região: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Tipo de dado sigiloso	Valor do filtro
Código do Healthcare Common Procedure Coding System (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
National Drug Code (NDC)	`USA_NATIONAL_DRUG_CODE`
National Provider Identifier (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Identificador exclusivo de dispositivo (UDI)	`MEDICAL_DEVICE_UDI`

Informações pessoais: informações de identificação pessoal (PII)

Você pode especificar os valores a seguir para filtrar descobertas que relatam ocorrências de informações de identificação pessoal (PII) em objetos do S3.

Tipo de dado sigiloso	Valor do filtro
Datas de nascimento	`DATE_OF_BIRTH`
Número de identificação da carteira de habilitação	Dependendo do país ou região: `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 os EUA), `ESTONIA_DRIVERS_LICENSE`, `FINLAND_DRIVERS_LICENSE`, `FRANCE_DRIVERS_LICENSE`, `GERMANY_DRIVERS_LICENSE`, `GREECE_DRIVERS_LICENSE`, `HUNGARY_DRIVERS_LICENSE`, `INDIA_DRIVERS_LICENSE`, `IRELAND_DRIVERS_LI`

Tipo de dado sigiloso	Valor do filtro
	`CENSE, ITALY_DRIVERS_LICEN SE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLAN DS_DRIVERS_LICENSE, POLAND _DRIVERS_LICENSE, PORTUGAL_ DRIVERS_LICENSE, ROMANIA_D RIVERS_LICENSE, SLOVAKIA_ DRIVERS_LICENSE, SLOVENIA_ DRIVERS_LICENSE, SPAIN_DRI VERS_LICENSE, SWEDEN_DRIVE RS_LICENSE, UK_DRIVERS_LICENSE`
Número de registro eleitoral	`UK_ELECTORAL_ROLL_NUMBER`
Nome completo	`NAME`
Coordenadas do sistema de posicionamento global (GPS)	`LATITUDE_LONGITUDE`
Cookie HTTP	`HTTP_COOKIE`
Endereço postal	`ADDRESS, BRAZIL_CEP_CODE`
Número de identificação nacional	Dependendo do país ou região: `BRAZIL_RG _NUMBER, FRANCE_NATIONAL_I DENTIFICATION_NUMBER, GERM ANY_NATIONAL_IDENTIFICATION _NUMBER, INDIA_AADHAAR_NUM BER, ITALY_NATIONAL_IDENTIFICATI ON_NUMBER, SPAIN_DNI_NUMBER`
Número do Seguro Nacional (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`

Tipo de dado sigiloso	Valor do filtro
Número de passaporte	Dependendo do país ou região: `CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Número de residência permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Número de telefone	Dependendo do país ou região: `BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (para o Canadá e os EUA), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Número do Seguro Social (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Número da Previdência Social (SSN)	Dependendo do país ou região: `SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Tipo de dado sigiloso	Valor do filtro
Identificação do contribuinte ou número de referência	Dependendo do país ou região: `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 identificação de veículo (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Como investigar dados confidenciais com as descobertas do Amazon Macie

Quando você executa trabalhos de descoberta de dados confidenciais ou o Amazon Macie realiza uma descoberta automática de dados confidenciais, o Macie captura detalhes sobre a localização de cada ocorrência de dados confidenciais em objetos do Amazon Simple Storage Service (Amazon S3) que ele acha. Isso inclui dados confidenciais que o Macie detectou usando identificadores de dados gerenciados e dados que correspondem aos critérios dos identificadores de dados personalizados que você configurou para um trabalho ou para o Macie usar.

Com as descobertas de dados confidenciais, você pode analisar esses detalhes de até 15 ocorrências de dados confidenciais que o Macie encontrou em objetos individuais do S3. Os detalhes fornecem informações sobre as categorias e os tipos de dados confidenciais que buckets e objetos específicos do S3 podem conter. Eles podem ajudá-lo a localizar ocorrências individuais de dados confidenciais em objetos e determinar se é necessário realizar uma investigação mais profunda de buckets e objetos específicos.

Para obter informações adicionais, você pode, como opção, configurar e usar o Macie para recuperar amostras de dados confidenciais que o Macie relata em descobertas individuais. As amostras podem

ajudar você a verificar a natureza dos dados confidenciais que o Macie encontrou. Eles também podem ajudar você a personalizar sua investigação de um bucket e objeto do S3 afetados. Se você optar por recuperar amostras de dados confidenciais para uma descoberta, o Macie usa os dados na descoberta para localizar de 1 a 10 ocorrências de cada tipo de dado confidencial relatado pela descoberta. Em seguida, o Macie extrai essas ocorrências de dados confidenciais do objeto afetado e exibe os dados para você analisar.

Se um objeto do S3 contiver muitas ocorrências de dados confidenciais, uma descoberta também pode ajudar a navegar até o resultado correspondente da descoberta de dados confidenciais. Ao contrário de uma descoberta de dados confidenciais, um resultado de descoberta de dados confidenciais fornece dados de localização detalhados para até 1.000 ocorrências de cada tipo de dado confidencial que Macie encontrou em um objeto. O Macie usa o mesmo esquema para dados de localização em descobertas de dados confidenciais e resultados de descobertas de dados confidenciais. Para saber mais sobre os resultados da detecção de dados confidenciais, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Os tópicos desta seção explicam como localizar e, como opção, recuperar ocorrências de dados confidenciais relatadas por descobertas de dados confidenciais. Eles também explicam o esquema que o Macie usa para relatar a localização de ocorrências individuais de dados confidenciais que o Macie encontra.

Tópicos

Como localizar dados confidenciais com as descobertas do Amazon Macie

Quando você executa trabalhos de descoberta de dados confidenciais ou o Amazon Macie realiza uma descoberta automática de dados confidenciais, o Macie realiza uma inspeção profunda da versão mais recente de cada objeto do Amazon Simple Storage Service (Amazon S3) que ele analisa. Para cada execução de trabalho ou ciclo de análise, o Macie também usa um algoritmo de pesquisa em profundidade para preencher as descobertas resultantes com detalhes sobre a localização de ocorrências específicas de dados confidenciais que o Macie encontra nos objetos do S3. Essas ocorrências fornecem informações sobre as categorias e os tipos de dados confidenciais que um bucket e um objeto do S3 afetados podem conter. Os detalhes podem ajudá-lo a localizar

ocorrências individuais de dados confidenciais em objetos e determinar se é necessário realizar uma investigação mais profunda de buckets e objetos específicos.

Com as descobertas de dados confidenciais, você pode determinar a localização de até 15 ocorrências de dados confidenciais que o Macie encontrou em um objeto do S3 afetado. Isso inclui dados confidenciais que o Macie detectou usando identificadores de dados gerenciados e dados que correspondem aos critérios dos identificadores de dados personalizados que você configurou para um trabalho ou o Macie usar.

Uma descoberta de dados confidenciais pode fornecer detalhes como:

- O número da coluna e da linha de uma célula ou campo em uma pasta de trabalho do Microsoft Excel, arquivo CSV ou arquivo TSV.
- O caminho para um campo ou matriz em um arquivo JSON ou JSON Lines.
- O número da linha de uma linha em um arquivo de texto não binário que não seja um arquivo CSV, JSON, JSON Lines ou TSV; por exemplo, um arquivo HTML, TXT ou XML.
- O número da página de uma página em um arquivo Adobe Portable Document Format (PDF).
- O índice do registro e o caminho para um campo em um registro em um contêiner de objetos Apache Avro ou arquivo Apache Parquet.

Você pode acessar esses detalhes usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode acessar esses detalhes nas descobertas que Macie publica para outros Serviços da AWS, tanto no Amazon EventBridge, quanto no AWS Security Hub. Para saber mais sobre as estruturas JSON que o Macie usa para relatar esses detalhes, consulte Esquema JSON para locais de dados confidenciais. Para saber como acessar os detalhes das descobertas que Macie publica para outrosServiços da AWS, consulte Monitoramento e processamento de descobertas.

Se um objeto do S3 contiver muitas ocorrências de dados confidenciais, você também poderá usar uma descoberta para navegar até o resultado correspondente da descoberta de dados confidenciais. Ao contrário de uma descoberta de dados confidenciais, um resultado de detecção de dados confidenciais fornece dados de localização detalhados para até 1.000 ocorrências de cada tipo de dado confidencial que o Macie encontrou em um objeto. Se um objeto do S3 for um arquivo de arquivamento, como um arquivo.tar ou .zip, isso inclui ocorrências de dados confidenciais em arquivos individuais que o Macie extraiu do arquivo. (O Macie não inclui essas informações nas descobertas de dados confidenciais). Para saber mais sobre os resultados da detecção de dados confidenciais, consulte Armazenamento e retenção de resultados de descoberta de dados

confidenciais. O Macie usa o mesmo esquema para dados de localização em descobertas de dados confidenciais e resultados de descobertas de dados confidenciais.

Como localizar ocorrências de dados confidenciais

Para localizar ocorrências de dados confidenciais, você pode usar o console do Amazon Macie ou a API do Amazon Macie. As etapas a seguir explicam como localizar dados confidenciais usando o console.

Para fazer isso programaticamente, use a operação GetFindings da API do Amazon Macie. Se uma descoberta incluir detalhes sobre a localização de uma ou mais ocorrências de um tipo específico de dados confidenciais, os objetos `occurrences` na descoberta fornecerão esses detalhes. Para obter mais informações, consulte Esquema JSON para locais de dados confidenciais.

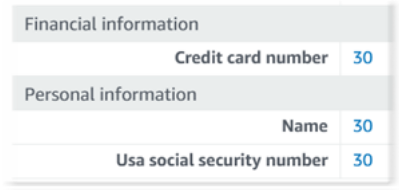
Para localizar ocorrências de dados confidenciais

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.

   > **Tip**
   >
   > Você pode usar a página Trabalhos para exibir todas as descobertas de um trabalho específico de detecção de dados confidenciais. No painel de navegação, selecione Trabalhos e, então, selecione o nome do trabalho. Na parte superior do painel de detalhes, selecione Exibir resultados e, em seguida, selecione Exibir descobertas.

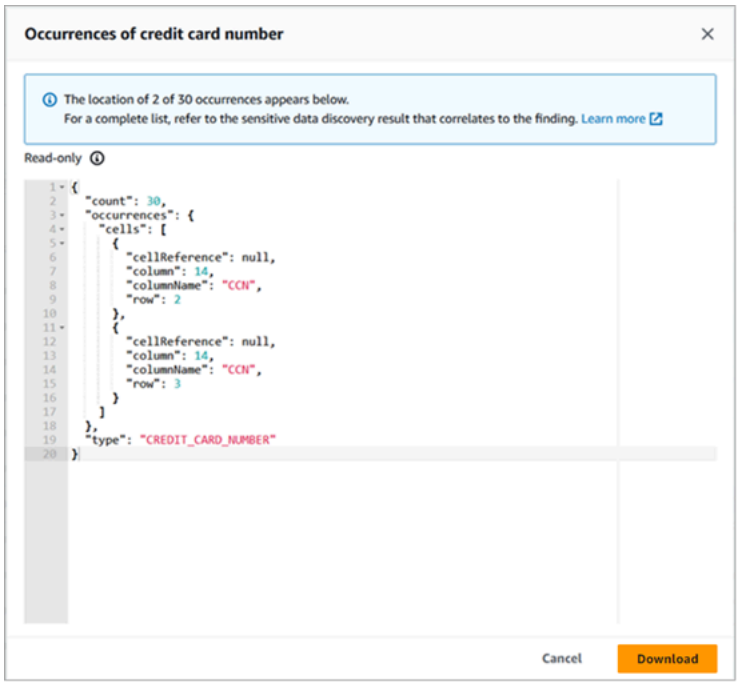
3. Na página Descobertas, selecione a descoberta dos dados confidenciais que deseja localizar. O painel de detalhes exibirá informações sobre a descoberta.
4. No painel de detalhes, vá até a seção Dados confidenciais. Esta seção fornece informações sobre as categorias e os tipos de dados confidenciais que o Macie encontrou no objeto do S3 afetado. Também indica o número de ocorrências de cada tipo de dado confidencial que o Macie encontrou.

   Por exemplo, a imagem a seguir mostra alguns detalhes de uma descoberta que relata 30 ocorrências de números de cartão de crédito, 30 ocorrências de nomes e 30 ocorrências de números do Seguro Social dos EUA.



Se uma descoberta incluir detalhes sobre a localização de uma ou mais ocorrências de um tipo específico de dado confidencial, o número de ocorrências será um link. Selecione o link para mostrar os detalhes. O Macie abre uma nova janela e exibe os detalhes no formato JSON.

Por exemplo, a imagem a seguir mostra a localização de duas ocorrências de números de cartão de crédito em um objeto do S3 afetado.



Para salvar os detalhes como um arquivo JSON, selecione Baixar e, em seguida, especifique um nome e um local para o arquivo.

5. (Opcional) Para salvar todos os detalhes da descoberta como um arquivo JSON, selecione o identificador da descoberta (ID da descoberta) na parte superior do painel de detalhes. O Macie abre uma nova janela e exibe todos os detalhes no formato JSON. Selecione Baixar e, em seguida, especifique um nome e um local para o arquivo.

Para acessar detalhes sobre a localização de até 1.000 ocorrências de cada tipo de dado confidencial no objeto afetado, consulte o resultado correspondente da detecção de dados confidenciais para a descoberta. Para fazer isso, vá até o início da seção Detalhes do painel. Em

seguida, selecione o link no campo Localização detalhada do resultado. O Macie abre o console do Amazon S3 e exibe o arquivo ou pasta que contém o resultado da descoberta correspondente.

Recuperando e revelando amostras de dados confidenciais com as descobertas do Amazon Macie

Para verificar a natureza dos dados confidenciais que o Amazon Macie relata nas descobertas, você pode, opcionalmente, configurar e usar o Macie para recuperar e revelar amostras de dados confidenciais relatados por determinadas descobertas. Isso inclui dados confidenciais que o Macie detectou usando identificadores de dados gerenciados e dados que correspondem aos critérios dos identificadores de dados personalizados. As amostras podem ajudar você a personalizar sua investigação sobre o objeto e o bucket afetados do Amazon Simple Storage Service (Amazon S3).

Se você recuperar e revelar amostras de dados confidenciais para uma descoberta, o Macie executará as seguintes tarefas gerais:

1. Verifica se a descoberta especifica a localização de determinadas ocorrências de dados confidenciais e a localização de um resultado da descoberta de dados confidenciais correspondente.
2. Avalia o resultado correspondente da descoberta de dados confidenciais, verificando a validade dos metadados do objeto afetado do S3 e os dados de localização para ocorrências de dados confidenciais no objeto.
3. Ao usar dados no resultado da descoberta de dados confidenciais, localiza as primeiras 1 a 10 ocorrências de dados confidenciais relatadas pela descoberta e extrai os primeiros 1 a 128 caracteres de cada ocorrência do objeto do S3 afetado. Se a descoberta relatar vários tipos de dados confidenciais, o Macie fará isso para até cem tipos.
4. Ele criptografa os dados extraídos com uma chave AWS Key Management Service (AWS KMS) que você especificar.
5. Armazena temporariamente os dados criptografados em um cache e exibe os dados para você revisar. Os dados são criptografados o tempo todo, tanto em trânsito quanto em repouso.
6. Logo após a extração e a criptografia, ele exclui permanentemente os dados do cache, a menos que uma retenção adicional seja temporariamente necessária para resolver um problema operacional.

Se você optar por recuperar e revelar amostras de dados confidenciais para uma descoberta novamente, o Macie repetirá essas tarefas para localizar, extrair, criptografar, armazenar e, por fim, excluir as amostras.

O Macie não usa o perfil vinculado a serviços do Macie em sua conta para realizar essas tarefas. Em vez disso, você usa sua identidade do AWS Identity and Access Management (IAM) ou permite que o Macie assuma um perfil do IAM em sua conta. É possível recuperar e revelar amostras de dados confidenciais para uma descoberta se você ou o perfil tiver permissão para acessar os recursos e dados necessários, e também para realizar as ações necessárias. Todas as ações necessárias estão registradas em AWS CloudTrail.

> **Important**
>
> Recomendamos que você restrinja o acesso a essa funcionalidade usando políticas personalizadas do IAM. Para controle de acesso adicional, recomendamos que você também crie um AWS KMS key dedicado para criptografia de amostras de dados confidenciais que são recuperadas e restrinja o uso da chave somente às entidade principais, que devem ter permissão para recuperar e revelar amostras de dados confidenciais.
> Para obter recomendações e exemplos de políticas que você pode usar para controlar o acesso a essa funcionalidade, consulte a postagem do blog Como usar o Amazon Macie para pré-visualizar dados confidenciais em buckets do S3 no blog de segurança AWS.

Os tópicos desta seção explicam como configurar e usar o Macie para recuperar e revelar amostras de dados confidenciais para as descobertas. Você pode realizar essas tarefas em todas as Regiões da AWS em que o Macie está atualmente disponível, exceto nas regiões Asia Pacific (Osaka) e Israel (Tel Aviv).

Tópicos

- Requisitos e opções de configuração para recuperar amostras de dados confidenciais com descobertas
- Configurar o Amazon Macie para recuperar e revelar amostras de dados confidenciais com descobertas
- Como recuperar e revelar amostras de dados confidenciais com descobertas

Requisitos e opções de configuração para recuperar amostras de dados confidenciais com descobertas

Como opção é possível configurar e usar o Amazon Macie para recuperar e revelar amostras de dados confidenciais que o Macie relata em descobertas individuais. Se você recuperar e revelar amostras de dados confidenciais para uma descoberta, o Macie vai usar os dados no resultado da descoberta de dados confidenciais correspondente para localizar ocorrências de dados confidenciais no objeto afetado do Amazon Simple Storage Service (Amazon S3). Em seguida, o Macie extrai amostras dessas ocorrências do objeto afetado. O Macie criptografa os dados extraídos com uma chave AWS Key Management Service (AWS KMS) que você especifica, armazena temporariamente os dados criptografados em um cache e retorna os dados em seus resultados da descoberta. Logo após a extração e a criptografia, o Macie exclui permanentemente os dados do cache, a menos que uma retenção adicional seja temporariamente necessária para resolver um problema operacional.

O Macie não usa o perfil vinculado a serviço do Macie em sua conta para localizar, recuperar, criptografar ou revelar amostras de dados confidenciais para objetos afetados do S3. Em vez disso, o Macie usa configurações e recursos que você configura para sua conta. Ao definir as configurações no Macie, você especifica como acessar os objetos afetados do S3. Você também especifica qual AWS KMS key deve ser usada para criptografar as amostras. É possível definir as configurações em todas as Regiões da AWS nas quais o Macie está atualmente disponível, exceto nas regiões Asia Pacific (Osaka) e Israel (Tel Aviv).

Você tem duas opções para acessar objetos afetados do S3 e recuperar amostras de dados confidenciais deles. É possível configurar o Macie para usar credenciais de usuário do AWS Identity and Access Management (IAM) ou assumir um perfil do IAM:

- Usar credenciais de usuário do IAM: com essa opção, cada usuário da sua conta usa sua identidade individual do IAM para localizar, recuperar, criptografar e revelar as amostras. Isso significa que um usuário pode recuperar e revelar amostras de dados confidenciais para uma descoberta se tiver permissão para acessar os recursos e dados necessários, e também para realizar as ações necessárias.
- Assumir um perfil do IAM: com essa opção, você cria um perfil do IAM que delega acesso ao Macie. Você também garante que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Posteriormente, o Macie vai assumir o perfil quando um usuário da sua conta optar por localizar, recuperar, criptografar e revelar amostras de dados confidenciais para uma descoberta.

Você pode usar qualquer uma das configurações com qualquer tipo de conta do Macie, ou seja, a conta delegada de administrador do Macie para uma organização, uma conta de membro do Macie em uma organização ou uma conta autônoma do Macie.

Os tópicos a seguir explicam as opções, os requisitos e os fatores que podem ajudar você a determinar como definir as configurações e os recursos para sua conta. Isso inclui as políticas de confiabilidade e permissão para anexar a um perfil do IAM. Para obter recomendações e exemplos adicionais de políticas que você pode usar para recuperar e revelar amostras de dados confidenciais, consulte a postagem Como usar o Amazon Macie para pré-visualizar dados confidenciais em buckets do S3 no blog de segurança da AWS.

Tópicos

Como determinar qual método de acesso usar

Ao determinar qual configuração é melhor para seu ambiente AWS, uma consideração importante é se seu ambiente inclui várias contas do Amazon Macie que são gerenciadas centralmente como uma organização. Se você for o administrador delegado do Macie de uma organização, configurar o Macie para assumir um perfil do IAM pode agilizar a recuperação de amostras de dados confidenciais de objetos do S3 afetados para contas em sua organização. Com essa abordagem, você cria um perfil do IAM em sua conta de administrador. Você também cria um perfil do IAM em cada conta de membro aplicável. O perfil na sua conta de administrador delega acesso ao Macie. O perfil em uma conta de membro delega o acesso entre contas ao perfil em sua conta de administrador. Se implementado, você poderá usar o encadeamento de perfis para acessar objetos do S3 afetados para as contas de membros.

Considere também quem tem acesso direto às descobertas individuais por padrão. A fim de recuperar e revelar amostras de dados confidenciais para uma descoberta, primeiro o usuário deve ter acesso à descoberta:

- Trabalhos de descoberta de dados confidenciais: somente a conta que cria um trabalho pode acessar as descobertas produzidas pelo trabalho. Se você tiver uma conta de administrador do

Macie, poderá configurar um trabalho para analisar objetos em buckets do S3 para qualquer conta em sua organização. Portanto, seus trabalhos podem produzir descobertas para objetos em buckets pertencentes às suas contas de membros. Se você tiver uma conta de membro ou uma conta autônoma do Macie, poderá configurar um trabalho para analisar objetos somente nos buckets pertencentes à sua conta.

- Descoberta automatizada de dados confidenciais: somente a conta de administrador do Macie pode acessar descobertas que o processo automatizado de descoberta produz para contas na organização. As contas de membros não podem acessar essas descobertas. Se você tiver uma conta autônoma do Macie, só poderá acessar as descobertas que a descoberta automatizada produz para sua própria conta.

Se você planeja acessar objetos afetados do S3 usando uma perfil do IAM, considere também o seguinte:

- Para localizar ocorrências de dados confidenciais em um objeto, é necessário armazenar o resultado correspondente da descoberta de dados confidenciais para uma descoberta em um objeto do S3 que o Macie tenha assinado com uma AWS KMS key de código de autenticação de mensagens por hash (HMAC). O Macie deve ser capaz de verificar a integridade e a autenticidade do resultado da descoberta de dados confidenciais. Caso contrário, o Macie não assumirá o perfil do IAM para recuperar amostras de dados confidenciais. Essa é uma barreira de proteção adicional que visa restringir o acesso a dados em objetos do S3 para uma conta.
- Para recuperar amostras de dados confidenciais de um objeto criptografado com uma AWS KMS key gerenciada pelo cliente, o perfil do IAM deve ter permissão para descriptografar dados com a chave. Mais especificamente, a política da chave deve permitir que o perfil execute a ação `kms:Decrypt`. Para outros tipos de criptografia no lado do servidor, é necessário ter permissões ou recursos adicionais para descriptografar um objeto afetado. Para obter mais informações, consulte Como descriptografar objetos afetados do S3.
- Para recuperar amostras de dados confidenciais de um objeto para outra conta, você deve ser o administrador delegado do Macie para a conta na Região da AWS aplicável. Além disso:
  - No momento, o Macie deve estar habilitado para a conta de membro na região aplicável.
  - A conta de membro deve ter um perfil do IAM que delegue o acesso entre contas a um perfil do IAM na sua conta de administrador do Macie. O nome do perfil deve ser o mesmo em sua conta de administrador do Macie e na conta de membro.
  - A política de confiança para o perfil do IAM na conta de membro deve incluir uma condição que especifique o ID externo correto para sua configuração. Esse ID é uma string alfanumérica

exclusiva que o Macie gera automaticamente depois que você define as configurações da sua conta de administrador do Macie. Para obter mais informações sobre o uso de IDs externos em políticas de confiabilidade, consulte Como usar um ID externo ao conceder acesso aos seus recursos da AWS a terceiros no Guia do usuário do AWS Identity and Access Management.

- Se o perfil do IAM na conta de membro atender a todos os requisitos do Macie, a conta de membro não precisará definir e ativar as configurações do Macie para que você recupere amostras de dados confidenciais dos objetos da conta. O Macie usará somente as configurações e o perfil do IAM na sua conta de administrador do Macie e o perfil do IAM na conta de membro.

> **Tip**
>
> Se sua conta integrar uma grande organização, considere usar um modelo do AWS CloudFormation e um conjunto de pilhas para provisionar e gerenciar os perfis do IAM para contas de membro em sua organização. Para obter informações sobre como criar e usar modelos e conjuntos de pilhas, consulte o Guia do usuário do AWS CloudFormation.
> você pode usar o console do Amazon Macie para analisar e, opcionalmente, baixar um modelo do CloudFormation que possa servir como ponto de partida. No painel de navegação no console, em Configurações, selecione Revelar amostras. Escolha Editar e, em seguida, escolha Exibir permissões de perfil de membro e modelo do CloudFormation.

Os tópicos subsequentes desta seção fornecem detalhes e considerações adicionais para cada tipo de configuração. Para perfis do IAM, isso inclui as políticas de confiabilidade e permissão para anexar a um perfil. Se você não tiver certeza sobre qual tipo de configuração é a melhor para seu ambiente, peça ajuda ao seu administrador da AWS.

Como usar credenciais de usuário do IAM para acessar objetos afetados do S3

Se você configurar o Amazon Macie para recuperar amostras de dados confidenciais usando credenciais de usuário do IAM, cada usuário da sua conta do Macie usará a própria identidade do IAM para localizar, recuperar, criptografar e revelar amostras para descobertas individuais. Isso significa que um usuário pode recuperar e revelar amostras de dados confidenciais para uma descoberta se a identidade do IAM dele tiver permissão para acessar os recursos e dados necessários, e também para realizar as ações necessárias. Todas as ações necessárias estão registradas em AWS CloudTrail.

Para recuperar e revelar amostras de dados confidenciais de uma descoberta específica, o usuário precisa ter permissão para acessar os seguintes dados e recursos: a descoberta; o resultado correspondente da descoberta de dados confidenciais, o bucket afetado do S3 e o objeto afetado do S3. O usuário também deverá ter permissão para usar a AWS KMS key empregada para criptografar o objeto afetado, se for o caso, e a AWS KMS key que você configurou para o Macie usar na criptografia de amostras de dados confidenciais. Se alguma política do IAM, política de recursos ou outras configurações de permissões negar o acesso necessário, o usuário não conseguirá recuperar e revelar nenhuma amostra para a descoberta.

Para definir esse tipo de configuração, conclua as seguintes tarefas gerais:

1. Verifique se você configurou um repositório para os resultados da descoberta de dados confidenciais.
2. Configure a AWS KMS key para uso na criptografia de amostras de dados confidenciais.
3. Verifique suas permissões para definir as configurações no Macie.
4. Configure e ative as configurações no Macie.

Para obter informações sobre como realizar essas tarefas, consulte Configurar o Amazon Macie para recuperar e revelar amostras de dados confidenciais com descobertas.

Assumir um perfil do IAM para acessar objetos afetados do S3

Para configurar o Amazon Macie para recuperar amostras de dados confidenciais assumindo um perfil do IAM, comece criando um perfil do IAM que delegue acesso ao Macie. Garanta que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Quando um usuário da sua conta do Macie optar por recuperar e revelar amostras de dados confidenciais para uma descoberta, o Macie assumirá a função de recuperar as amostras do objeto afetado do S3. O Macie só assume o perfil quando um usuário opta por recuperar e revelar amostras para uma descoberta. Para assumir o perfil, o Macie usa a operação AssumeRole da API AWS Security Token Service (AWS STS). Todas as ações necessárias estão registradas em AWS CloudTrail.

Para recuperar e revelar amostras de dados confidenciais para uma descoberta específica, o usuário deve ter permissão para acessar a descoberta, o resultado correspondente da descoberta de dados confidenciais e a AWS KMS key que você define para o Macie usar a fim de criptografar amostras de dados confidenciais. O perfil do IAM deve permitir que o Macie acesse o bucket afetado do S3 e o objeto afetado do S3. O perfil também deve ter permissão para usar a AWS KMS key que foi usada

para criptografar o objeto afetado, se aplicável. Se alguma política do IAM, política de recursos ou outras configurações de permissões negar o acesso necessário, o usuário não conseguirá recuperar e revelar nenhuma amostra para a descoberta.

Para definir esse tipo de configuração, conclua as seguintes tarefas gerais. Se você tiver uma conta de membro em uma organização, trabalhe com o administrador do Macie para determinar se e como definir as configurações e os recursos da sua conta.

1. Defina o seguinte:
   - O nome do perfil do IAM que você deseja que o Macie assuma. Se sua conta fizer parte de uma organização, esse nome deverá ser o mesmo para a conta de administrador delegada do Macie e para cada conta de membro aplicável na organização. Caso contrário, o administrador do Macie não poderá acessar os objetos afetados do S3 para uma conta de membro aplicável.
   - O nome da política de permissão do IAM para anexar ao perfil do IAM. Se sua conta fizer parte de uma organização, recomendamos que você use o mesmo nome de política para cada conta de membro aplicável na organização. Isso pode simplificar o provisionamento e o gerenciamento do perfil nas contas dos membros.
2. Verifique se você configurou um repositório para os resultados da descoberta de dados confidenciais.
3. Configure a AWS KMS key para uso na criptografia de amostras de dados confidenciais.
4. Verifique suas permissões para criar perfis do IAM e definir as configurações no Macie.
5. Se você for o administrador delegado do Macie para uma organização ou se tiver uma conta autônoma no Macie:
   a. Crie e configure o perfil do IAM para sua conta. Garanta que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Para obter detalhes sobre esses requisitos, consulte o próximo tópico.
   b. Configure e ative as configurações no Macie. Em seguida, o Macie vai gerar um ID externo para a configuração. Se você for o administrador do Macie para uma organização, anote esse ID. A política de confiança para o perfil do IAM em cada uma das suas contas de membro aplicáveis deve especificar esse ID.
6. Se você tiver uma conta de membro em uma organização:
   a. Peça ao administrador do Macie o ID externo a ser especificado na política de confiança do perfil do IAM em sua conta. Além disso, verifique o nome do perfil do IAM e a política de permissões a ser criada.

b. Crie e configure o perfil do IAM para sua conta. Garanta que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o seu administrador do Macie assuma o perfil. Para obter detalhes sobre esses requisitos, consulte o próximo tópico.
c. (Opcional) Se você quiser recuperar e revelar amostras de dados confidenciais de objetos afetados do S3 para sua própria conta, defina e ative as configurações no Macie. Se você quiser que o Macie assuma uma perfil do IAM para recuperar as amostras, comece criando e configurando um perfil adicional do IAM em sua conta. Garanta que as políticas de confiança e permissões para esse perfil adicional atendam a todos os requisitos para que o Macie assuma o perfil. Em seguida, defina as configurações no Macie e especifique o nome desse perfil adicional. Para obter detalhes sobre os requisitos de política para o perfil, consulte o próximo tópico.

Para obter informações sobre como realizar essas tarefas, consulte Configurar o Amazon Macie para recuperar e revelar amostras de dados confidenciais com descobertas.

Configurar um perfil do IAM para acessar objetos afetados do S3

Para acessar os objetos afetados do S3 usando um perfil do IAM, comece criando e configurando um perfil que delegue acesso ao Amazon Macie. Garanta que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o Macie assuma o perfil. A maneira de fazer isso dependerá do seu tipo de conta Macie.

As seções a seguir fornecem detalhes sobre as políticas de confiança e permissões a serem anexadas ao perfil do IAM para cada tipo de conta do Macie. Escolha a seção para o tipo de conta que você tem.

> **Note**
>
> Se você tiver uma conta de membro em uma organização, talvez seja necessário criar e configurar dois perfis do IAM para sua conta:
>
> - Para permitir que seu administrador do Macie recupere e revele amostras de dados confidenciais de objetos afetados do S3 para sua conta, crie e configure um perfil que a conta do seu administrador possa assumir. Para obter esses detalhes, escolha a seção de conta de membro do Macie.
> - Para recuperar e revelar amostras de dados confidenciais de objetos afetados do S3 para sua própria conta, crie e configure um perfil que seu Macie possa assumir. Para obter esses detalhes, escolha a seção de conta autônoma do Macie.

> Antes de criar e configurar qualquer perfil do IAM, trabalhe com o administrador do Macie para determinar a configuração adequada para sua conta.

Para obter informações detalhadas sobre como usar o IAM para criar o perfil, consulte Como criar um perfil usando políticas personalizadas de confiança no Guia do usuário do AWS Identity and Access Management.

Conta de administrador do Macie

Se você for o administrador delegado do Macie de uma organização, comece usando o editor de políticas do IAM para criar a política de permissões para o perfil do IAM. A política deve seguir o exemplo abaixo.

```
{
    "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"
        }
    ]
}
```

Onde *IAMRoleName* é o nome do perfil do IAM que o Macie deve assumir ao recuperar amostras de dados confidenciais dos objetos afetados do S3 para as contas da sua organização. Substitua

esse valor pelo nome do perfil que você está criando para sua conta e planeja criar para contas de membros aplicáveis em sua organização. Esse nome deve ser o mesmo para sua conta de administrador do Macie e para cada conta de membro aplicável.

> **Note**
>
> Na política de permissões anterior, o elemento `Resource` na primeira instrução usa um caractere curinga (*). Isso permite que uma entidade do IAM anexada recupere objetos de todos os buckets do S3 que sua organização possui. Para permitir esse acesso apenas a buckets específicos, substitua o caractere curinga pelo nome do recurso da Amazon (ARN) de cada bucket. Por exemplo, para permitir o acesso somente a objetos em um bucket chamado DOC-EXAMPLE-BUCKET, altere o elemento para: `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> Também é possível restringir o acesso a objetos em buckets específicos do S3 para contas individuais. Para fazer isso, especifique os ARNs do bucket no elemento `Resource` da política de permissões para o perfil do IAM em cada conta aplicável. Para obter mais informações e exemplos, consulte Elementos da política JSON do IAM: recurso no Guia do usuário do AWS Identity and Access Management.

Após criar a política de permissões para o perfil do IAM, crie e configure o perfil. Se você fizer isso usando o console do IAM, escolha Política de confiança personalizada como o Tipo de entidade confiável para o perfil. Especifique o seguinte para a política de confiança que define entidades confiáveis para o perfil.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
```

```
        }
    ]
}
```

Onde *accountId* é o ID de conta da sua Conta da AWS. Substitua esse valor pelo seu ID de conta com 12 dígitos.

Na política de confiança anterior:

- O elemento `Principal` especifica a entidade principal de serviço que o Macie usa ao recuperar amostras de dados confidenciais dos objetos afetados do S3, `reveal-samples.macie.amazonaws.com`.
- O elemento `Action` especifica a ação que a entidade principal do serviço pode realizar, a operação AssumeRole da API do AWS Security Token Service (AWS STS).
- O elemento `Condition` define uma condição que usa a chave de contexto de condição global aws:SourceAccount. Essa condição determina qual conta pode realizar a ação especificada. Nesse caso, ele permite que o Macie assuma o perfil somente para a conta especificada (*accountID*). A condição ajuda a evitar que o Macie seja usado em um ataque de representante confuso durante transações com o AWS STS.

Após definir a política de confiança para o perfil do IAM, anexe a política de permissões ao perfil. Essa deve ser a política de permissões que você criou antes de começar a criar o perfil. Em seguida, conclua as etapas restantes no IAM para concluir a criação e a configuração do perfil. Ao terminar, defina e ative as configurações no Macie.

Conta de membro do Macie

Se você tiver uma conta de membro do Macie e quiser permitir que seu administrador do Macie recupere e revele amostras de dados confidenciais dos objetos afetados do S3 para sua conta, comece solicitando as seguintes informações ao administrador do Macie:

- O nome do perfil do IAM a ser criado. O nome deve ser igual para sua conta e para a conta de administrador do Macie da sua organização.
- O nome da política de permissão do IAM para anexar ao perfil.
- O ID externo para especificar na política de confiabilidade do perfil. Esse ID deve ser o ID externo que o Macie gerou para a configuração do administrador do Macie.

Após receber essas informações, use o editor de políticas do IAM para criar a política de permissões para o perfil. A política deve seguir o exemplo abaixo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

A política de permissão anterior permite que uma entidade do IAM anexada recupere objetos de todos os buckets do S3 da sua conta. Isso acontece porque o elemento `Resource` na política usa um caractere curinga (*). Para permitir esse acesso apenas a buckets específicos, substitua o caractere curinga pelo nome do recurso da Amazon (ARN) de cada bucket. Por exemplo, para permitir o acesso somente a objetos em um bucket chamado DOC-EXAMPLE-BUCKET2, altere o elemento para:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

Para obter mais informações e exemplos, consulte Elementos da política JSON do IAM: recurso no Guia do usuário do AWS Identity and Access Management.

Após criar a política de permissões para o perfil do IAM, crie o perfil. Se você criar o perfil usando o console do IAM, escolha Política de confiança personalizada como o Tipo de entidade confiável para o perfil. Especifique o seguinte para a política de confiança que define entidades confiáveis para o perfil.

```
{
    "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}"
                }
            }
        }
    ]
}
```

Na política anterior, substitua os valores do espaço reservado pelos valores corretos para seu ambiente AWS, no qual:

- *administratorAccountID* é o ID da conta com 12 dígitos para a conta do seu administrador do Macie.
- *IAMRoleName* é o nome do perfil do IAM na conta do seu administrador do Macie. Deve ser o nome que você recebeu do administrador do Macie.
- *ExternalID* é o ID externo que você recebeu do administrador do Macie.

Em geral, a política de confiança permite que o administrador do Macie assuma o perfil para recuperar e revelar amostras de dados confidenciais de objetos afetados do S3 para sua conta. O elemento `Principal` especifica o ARN de um perfil do IAM na sua conta de administrador do Macie. Esse é o perfil que o administrador do Macie usa para recuperar e revelar amostras de dados confidenciais das contas da sua organização. O bloco `Condition` define duas condições que determinam adicionalmente quem pode assumir o perfil:

- A primeira condição especifica um ID externo exclusivo para a configuração da sua organização. Para saber mais sobre IDs externos, consulte Como usar um ID externo ao conceder acesso aos seus recursos da AWS a terceiros no Guia do usuário do AWS Identity and Access Management.
- A segunda condição usa a chave de contexto de condição global aws:PrincipalOrgID. O valor da chave é uma variável dinâmica que representa o identificador exclusivo de uma organização no AWS Organizations (`${aws:ResourceOrgID}`). A condição restringe o acesso somente às contas que fazem parte da mesma organização no AWS Organizations. Se você tiver ingressado na sua organização aceitando um convite no Macie, remova essa condição da política.

Após definir a política de confiança para o perfil do IAM, anexe a política de permissões ao perfil. Essa deve ser a política de permissões que você criou antes de começar a criar o perfil. Em seguida, conclua as etapas restantes no IAM para concluir a criação e a configuração do perfil. Não defina nem insira configurações para o perfil no Macie.

Conta autônoma do Macie

Se você tiver uma conta autônoma do Macie ou uma conta de membro do Macie e quiser recuperar e revelar amostras de dados confidenciais dos objetos afetados do S3 para sua própria conta, comece usando o editor de políticas do IAM para criar a política de permissões para o perfil do IAM. A política deve seguir o exemplo abaixo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Na política de permissões anterior, o elemento `Resource` usa um caractere curinga (*). Isso permite que uma entidade do IAM anexada recupere objetos de todos os buckets do S3 da sua conta. Para permitir esse acesso apenas a buckets específicos, substitua o caractere curinga pelo nome do recurso da Amazon (ARN) de cada bucket. Por exemplo, para permitir o acesso somente a objetos em um bucket chamado DOC-EXAMPLE-BUCKET3, altere o elemento para:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

Para obter mais informações e exemplos, consulte Elementos da política JSON do IAM: recurso no Guia do usuário do AWS Identity and Access Management.

Após criar a política de permissões para o perfil do IAM, crie o perfil. Se você criar o perfil usando o console do IAM, escolha Política de confiança personalizada como o Tipo de entidade confiável para

o perfil. Especifique o seguinte para a política de confiança que define entidades confiáveis para o perfil.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Onde *accountId* é o ID de conta da sua Conta da AWS. Substitua esse valor pelo seu ID de conta com 12 dígitos.

Na política de confiança anterior:

- O elemento `Principal` especifica a entidade principal de serviço que o Macie usa ao recuperar e revelar amostras de dados confidenciais dos objetos afetados do S3, `reveal-samples.macie.amazonaws.com`.
- O elemento `Action` especifica a ação que a entidade principal do serviço pode realizar, a operação AssumeRole da API do AWS Security Token Service (AWS STS).
- O elemento `Condition` define uma condição que usa a chave de contexto de condição global aws:SourceAccount. Essa condição determina qual conta pode realizar a ação especificada. Ela permite que o Macie assuma o perfil somente para a conta especificada (*accountID*). A condição ajuda a evitar que o Macie seja usado em um ataque de representante confuso durante transações com o AWS STS.

Após definir a política de confiança para o perfil do IAM, anexe a política de permissões ao perfil. Essa deve ser a política de permissões que você criou antes de começar a criar o perfil. Em seguida,

conclua as etapas restantes no IAM para concluir a criação e a configuração do perfil. Ao terminar, defina e ative as configurações no Macie.

Como descriptografar objetos afetados do S3

O Amazon S3 oferece suporte a várias opções de criptografia para objetos do S3. Para a maioria dessas opções, não é necessário ter nenhum recurso ou permissão adicional para que um perfil ou usuário do IAM decodifique e recupere amostras de dados confidenciais de um objeto afetado. Esse é o caso para um objeto criptografado usando criptografia no lado do servidor com uma chave gerenciada pelo Amazon S3 ou uma AWS KMS key gerenciada pela AWS.

No entanto, se um objeto do S3 for criptografado com uma AWS KMS key gerenciada pelo cliente, será necessário ter permissões adicionais para descriptografar e recuperar amostras de dados confidenciais do objeto. Mais especificamente, a política de chave da chave KMS deverá permitir que o perfil ou usuário do IAM execute a ação `kms:Decrypt`. Caso contrário, ocorrerá um erro e o Macie não recuperará nenhuma amostra do objeto. Para saber como fornecer esse acesso a um usuário do IAM, consulte Autenticação e controle de acesso para o AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

A forma de fornecer esse acesso para um perfil do IAM dependerá de a conta proprietária da AWS KMS key também ser proprietária do perfil:

- Se a mesma conta for proprietária da chave KMS e do perfil, um usuário da conta precisará atualizar a política da chave.
- Se uma conta for proprietária da chave KMS e outra conta diferente for proprietária do perfil, um usuário da conta proprietária da chave deverá permitir o acesso entre contas à chave.

Este tópico descreve como realizar essas tarefas para um perfil do IAM que você criou para recuperar amostras de dados confidenciais de objetos do S3. Ele também fornece exemplos para os dois cenários. Para obter informações sobre como permitir o acesso à AWS KMS keys gerenciada pelo cliente em outros cenários, consulte Autenticação e controle de acesso para o AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Permitir acesso da mesma conta a uma chave gerenciada pelo cliente

Se a mesma conta for proprietária da AWS KMS key e do perfil do IAM, um usuário da conta precisará adicionar uma declaração à política da chave. A declaração adicional deverá permitir que o perfil do IAM decifre dados usando a chave. Para obter informações detalhadas sobre como atualizar

uma política principal, consulte Alterar uma política de chave no Guia do desenvolvedor AWS Key Management Service.

Na declaração:

- O elemento `Principal` precisará especificar o nome do recurso da Amazon (ARN) do perfil do IAM.
- O array `Action` deve especificar a ação `kms:Decrypt`. Essa é a única ação do AWS KMS para a qual o perfil do IAM deverá ter permissão de realizar para descriptografar um objeto que foi criptografado com a chave.

Veja a seguir um exemplo da instrução a ser adicionada à política de uma chave do 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": "*"
}
```

No exemplo anterior:

- O campo `AWS` no elemento `Principal` especifica o ARN do perfil do IAM na conta. Isso permite que o perfil execute a ação especificada na declaração de política. *123456789012* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta proprietária do perfil e da chave do KMS. *IAMRoleName* é um nome de exemplo. Substitua esse valor pelo nome do perfil do IAM na conta.
- A matriz `Action` especifica a ação que o perfil do IAM pode realizar usando a chave do KMS: descriptografar o texto cifrado que foi criptografado com a chave.

O local em que você adiciona essa declaração a uma política de chave depende da estrutura e dos elementos que a política contém atualmente. Ao adicionar a instrução, certifique-se de que a sintaxe seja válida. As políticas de chaves usam o formato JSON. Isso significa que você também

precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política.

Permitir acesso entre contas a uma chave gerenciada pelo cliente

Se uma conta for proprietária da AWS KMS key (proprietária da chave) e outra conta for proprietária do perfil do IAM (proprietária do perfil), o proprietário da chave deverá fornecer ao proprietário do perfil acesso entre contas à chave. Uma maneira de fazer isso é usando uma concessão Uma concessão é um instrumento de política que permite que as AWSentidades principais usem chaves KMS em operações criptográficas se as condições especificadas pela concessão forem atendidas. Para saber mais sobre concessões, consulte Subsídios AWS KMS no AWS Key Management ServiceGuia do desenvolvedor.

Com essa abordagem, primeiro o proprietário da chave garante que a política da chave permita que o proprietário do perfil crie uma concessão para a chave. Em seguida, o proprietário do perfil criará uma concessão para a chave. A concessão delega as permissões relevantes ao perfil do IAM em sua conta. Ele permite que o perfil decifre objetos do S3 que são criptografados com a chave.

Etapa 1: atualizar a política de chave

Na política de chave, o proprietário da chave deve garantir que a política inclua uma declaração que permita ao proprietário do perfil criar uma concessão para o perfil do IAM na conta dele (do proprietário do perfil). Nessa declaração, o elemento `Principal` deverá especificar o ARN da conta do proprietário do perfil. O array `Action` deve especificar a ação `kms:CreateGrant`. Um bloco `Condition` pode filtrar o acesso à ação especificada. Veja a seguir um exemplo da instrução a ser adicionada à política de uma chave do 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"
        }
    }
}
```

No exemplo anterior:

- O campo `AWS` no elemento `Principal` especifica o ARN da conta do proprietário do perfil. Isso permite que a conta execute a ação especificada na declaração de política. *111122223333* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta do proprietário do perfil.
- A matriz `Action` especifica a ação que o proprietário do perfil pode realizar na chave do KMS: criar uma concessão para a chave.
- O bloco `Condition` usa operadores de condição e as seguintes chaves de condição para filtrar o acesso à ação que o proprietário do perfil tem permissão para executar na chave do KMS:
  - kms:GranteePrincipal: essa condição permite que o proprietário do perfil crie uma concessão somente para a entidade principal beneficiária especificada, que é o ARN do perfil do IAM em sua conta. Nesse ARN, *111122223333* é um exemplo de ID de conta. Substitua esse valor pelo ID da conta do proprietário do perfil. *IAMRoleName* é um nome de exemplo. Substitua esse valor pelo nome do perfil do IAM na conta do proprietário do perfil.
  - kms:GrantOperations: essa condição permite que o proprietário do perfil crie uma concessão somente para delegar permissão para realizar a ação `Decrypt` do AWS KMS (descriptografar texto cifrado que foi criptografado com a chave). Isso impede que o proprietário do perfil crie concessões que deleguem permissões para realizar outras ações na chave do KMS. A ação `Decrypt` é a única ação do AWS KMS para a qual o perfil do IAM deverá ter permissão de realizar para descriptografar um objeto que foi criptografado com a chave.

O local no qual o proprietário adicionará essa declaração a uma política de chave dependerá da estrutura e dos elementos atualmente contidos na política. Quando o proprietário da chave adiciona a declaração, ele deve garantir que a sintaxe seja válida. As políticas de chaves usam o formato JSON. Isso significa que você também precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política. Para obter informações detalhadas sobre como atualizar uma política principal, consulte Alterar uma política de chave no Guia do desenvolvedor AWS Key Management Service.

Etapa 2: criar uma concessão

Depois que o proprietário da chave atualizar a política de chave conforme necessário, o proprietário do perfil criará uma concessão para a chave. A concessão delega as permissões relevantes ao perfil do IAM na conta dele (o proprietário do perfil). Antes que o proprietário do perfil crie a concessão, ele deverá verificar se tem permissão para realizar a ação `kms:CreateGrant`. Essa ação permite que ele adicione uma concessão a uma AWS KMS key existente gerenciada pelo cliente.

Para criar a concessão, o proprietário do perfil pode usar a operação CreateGrant da API do AWS Key Management Service. Quando o proprietário do perfil criar a concessão, ele deverá especificar os seguintes valores para os parâmetros necessários:

- `KeyId`: o ARN da chave do KMS. Para acesso entre contas a uma chave do KMS, esse valor deve ser um ARN. Não pode ser um ID de chave.
- `GranteePrincipal`: o ARN do perfil do IAM na conta dele. Esse valor deve ser `arn:aws:iam::`*`111122223333`*`:role/`*`IAMRoleName`*, no qual *`111122223333`* é o ID da conta do proprietário do perfil e *`IAMRoleName`* é o nome do perfil.
- `Operations`: a ação de descriptografia do AWS KMS (`Decrypt`). Essa é a única ação do AWS KMS para a qual o perfil do IAM deverá ter permissão de realizar para descriptografar um objeto que foi criptografado com a chave do KMS.

Se o proprietário do perfil estiver usando a AWS Command Line Interface (AWS CLI), ele poderá executar o comando create-grant para criar a concessão. O exemplo a seguir mostra como. O exemplo está formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
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"
```

Em que:

- `key-id` especifica o ARN da chave do KMS à qual aplicar a concessão.
- `grantee-principal` especifica o ARN do perfil do IAM que tem permissão para realizar a ação especificada pela concessão. Esse valor deve corresponder ao ARN especificado pela condição `kms:GranteePrincipal` na política de chave.
- `operations` especifica a ação que a concessão permite que a entidade principal especificada execute: descriptografar o texto cifrado que foi criptografado com a chave.

Se o comando for executado com sucesso, você receberá um resultado semelhante ao seguinte.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Onde `GrantToken` é uma string única, não secreta, de comprimento variável e codificada em base64 que representa a concessão que foi criada e `GrantId` é o identificador exclusivo da concessão.

Configurar o Amazon Macie para recuperar e revelar amostras de dados confidenciais com descobertas

Como opção é possível configurar e usar o Amazon Macie para recuperar e revelar amostras de dados confidenciais que o Macie relata em descobertas individuais de dados confidenciais. As amostras podem ajudar você a verificar a natureza dos dados confidenciais que o Macie encontrou. Eles podem ajudar você a personalizar sua investigação sobre o objeto e o bucket afetados do Amazon Simple Storage Service (Amazon S3). Você pode recuperar e revelar amostras de dados confidenciais em todas as Regiões da AWS nas quais o Macie está atualmente disponível, salvo nas regiões Asia Pacific (Osaka) e Israel (Tel Aviv).

Quando você recupera e revela amostras de dados confidenciais de uma descoberta, o Macie usa dados no resultado correspondente da descoberta de dados confidenciais para localizar ocorrências de dados confidenciais no objeto do S3 afetado. Em seguida, o Macie extrai amostras dessas ocorrências do objeto afetado. O Macie criptografa os dados extraídos com uma chave AWS Key Management Service (AWS KMS) que você especifica, armazena temporariamente os dados criptografados em um cache e retorna os dados em seus resultados da descoberta. Logo após a extração e a criptografia, o Macie exclui permanentemente os dados do cache, a menos que uma retenção adicional seja temporariamente necessária para resolver um problema operacional.

Para recuperar e revelar amostras de dados confidenciais para descobertas, primeiro você precisa definir e habilitar as configurações da sua conta no Macie. Você também precisa configurar recursos de apoio e permissões para sua conta. Os tópicos desta seção orientam você no processo de configuração do Macie para recuperar e revelar amostras de dados confidenciais e no gerenciamento do status da configuração da sua conta.

Tópicos

- Antes de começar

- Como definir e habilitar as configurações do Amazon Macie
- Como desabilitar configurações do Amazon Macie

> **Tip**
>
> Para obter recomendações e exemplos de políticas que você pode usar para controlar o acesso a essa funcionalidade, consulte a postagem do blog Como usar o Amazon Macie para pré-visualizar dados confidenciais em buckets do S3 no blog de segurança AWS.

Antes de começar

Antes de configurar o Amazon Macie para recuperar e revelar amostras de dados confidenciais de descobertas, execute as tarefas a seguir para garantir que você tenha os recursos e as permissões necessários.

Tarefas

- Etapa 1: configurar um repositório para resultados de descoberta de dados confidenciais
- Etapa 2: determinar como acessar os objetos afetados do S3
- Etapa 3: configurar o AWS KMS key
- Etapa 4: verificar suas permissões

Essas tarefas são opcionais se você já tiver configurado o Macie para recuperar e revelar amostras de dados confidenciais e só quiser alterar suas configurações.

Etapa 1: configurar um repositório para resultados de descoberta de dados confidenciais

Quando você recupera e revela amostras de dados confidenciais de uma descoberta, o Macie usa dados no resultado correspondente da descoberta de dados confidenciais para localizar ocorrências de dados confidenciais no objeto do S3 afetado. Portanto, é importante verificar se você configurou um repositório para os resultados de descoberta de dados confidenciais. Caso contrário, o Macie não conseguirá localizar amostras de dados confidenciais que você deseja recuperar e revelar.

Para determinar se você configurou esse repositório para a sua conta, é possível usar o console do Amazon Macie: escolha Resultados da descoberta (em Configurações) no painel de navegação. Para fazer isso programaticamente, use a operação GetClassificationExportConfiguration da API do Amazon Macie. Para saber mais sobre os resultados de descoberta de dados confidenciais e como

configurar esse repositório, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Etapa 2: determinar como acessar os objetos afetados do S3

Você tem duas opções para acessar objetos afetados do S3 e recuperar amostras de dados confidenciais deles. Você pode configurar o Macie para usar suas credenciais de usuário do AWS Identity and Access Management (IAM). Como alternativa, é possível configurar o Macie para assumir um perfil do IAM que delegue acesso ao Macie. Você pode usar qualquer uma das configurações com qualquer tipo de conta do Macie, ou seja, a conta delegada de administrador do Macie para uma organização, uma conta de membro do Macie em uma organização ou uma conta autônoma do Macie. Antes de definir as configurações no Macie, determine qual método de acesso deseja usar. Para obter detalhes sobre as opções e os requisitos de cada método, consulte Requisitos e opções de configuração para recuperar amostras de dados confidenciais com descobertas.

Se você planeja usar um perfil do IAM, crie e configure a função antes de definir as configurações no Macie. Além disso, garanta que as políticas de confiança e permissões do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Se sua conta integrar uma organização que gerencie centralmente várias contas do Macie, trabalhe com o administrador do Macie para determinar primeiro se e como configurar o perfil para a sua conta.

Etapa 3: configurar o AWS KMS key

Quando você recupera e revela amostras de dados confidenciais para uma descoberta, o Macie criptografa as amostras com uma chave do AWS Key Management Service (AWS KMS) que você especifica. Portanto, você precisa determinar qual AWS KMS key deseja usar para criptografar as amostras. A chave pode ser uma chave do KMS existente na sua própria conta ou uma chave do KMS existente que outra conta possui. Se você desejar usar uma chave que outra conta possui, obtenha o nome do recurso da Amazon (ARN) da chave. Você precisará especificar esse ARN ao inserir as configurações no Macie.

A chave do KMS deve ser uma chave do KMS de criptografia simétrica e gerenciada pelo cliente. Também deve ser uma chave de região única habilitada na mesma Região da AWS que sua conta no Macie. A chave do KMS pode estar em um repositório de chaves externo. No entanto, a chave pode, então, ser mais lenta e menos confiável do que uma chave totalmente gerenciada no AWS KMS. Se a latência ou um problema de disponibilidade impedir o Macie de criptografar amostras de dados confidenciais que você deseja recuperar e revelar, ocorre um erro e o Macie não retorna nenhuma amostra para a descoberta.

Além disso, a política de chaves para a chave deve permitir que as entidades principais adequadas (perfis do IAM, usuários do IAM ouContas da AWS) realizem as seguintes ações:

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> Como uma camada adicional de controle de acesso, recomendamos que você crie uma chave do KMS dedicada para criptografia de amostras de dados confidenciais que são recuperadas e restrinja o uso da chave somente às entidades principais que devem ter permissão para recuperar e revelar amostras de dados confidenciais. Se um usuário não tiver permissão para realizar as ações anteriores para a chave, o Macie vai rejeitar a solicitação de recuperar e revelar amostras de dados confidenciais. O Macie não retornará nenhuma amostra para a descoberta.

Para obter informações sobre como criar e configurar chaves do KMS, consulte Gerenciamento de chaves no Guia do desenvolvedor do AWS Key Management Service. Para obter informações sobre o uso de políticas de chaves para gerenciar o acesso às chaves do KMS, consulte Políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Etapa 4: verificar suas permissões

Antes de definir as configurações no Macie, verifique também se você tem as permissões necessárias. Para verificar suas permissões, use o AWS Identity and Access Management (IAM) para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações dessas políticas com a seguinte lista de ações que você deve ter permissão para realizar.

Amazon Macie

Verifique também se você tem permissão para realizar as seguintes ações:

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

A primeira ação permite que você acesse sua conta no Macie. A segunda ação permite que você altere suas configurações para recuperar e revelar amostras de dados confidenciais. Isso inclui habilitar e desabilitar a configuração.

Opcionalmente, verifique se você também tem permissão para realizar a ação `macie2:GetRevealConfiguration`. Essa ação permite que você recupere suas configurações atuais e o status atual da configuração para sua conta.

AWS KMS

Se você planeja usar o console do Amazon Macie para inserir as definições de configuração, verifique também se tem permissão para realizar as seguintes ações do AWS Key Management Service (AWS KMS):

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

Essas ações permitem que você recupere informações sobre o AWS KMS keys para a sua conta. Em seguida, você pode escolher uma dessas chaves ao inserir as configurações.

IAM

Se você planeja configurar o Macie para assumir um perfil do IAM para recuperar e revelar amostras de dados confidenciais, verifique também se tem permissão para realizar a seguinte ação do IAM: `iam:PassRole`. Essa ação permite que você transmita o perfil para o Macie, o que permitirá que o Macie assuma o perfil. Quando você inserir as configurações da sua conta, o Macie também poderá verificar se o perfil existe na sua conta e está configurada corretamente.

Se você não tiver permissão para realizar as ações necessárias, peça ajuda ao seu administrador AWS.

Como definir e habilitar as configurações do Amazon Macie

Após verificar se você tem os recursos e as permissões necessários, você poderá definir as configurações no Amazon Macie e habilitar a configuração da sua conta.

Se sua conta integrar uma organização que gerencie centralmente várias contas do Macie, observe o seguinte antes de configurar ou alterar posteriormente as configurações da sua conta:

- Se você tiver uma conta de membro, trabalhe com o administrador do Macie para determinar se e como definir as configurações da sua conta. Seu administrador do Macie poderá ajudar a determinar as configurações corretas para sua conta.

- Se você tiver uma conta de administrador do Macie e alterar suas configurações para acessar objetos afetados do S3, suas alterações poderão afetar outras contas e recursos da sua organização. Isso dependerá de o Macie estar ou não configurado para assumir um perfil do AWS Identity and Access Management (IAM) para recuperar amostras de dados confidenciais. Se estiver e você reconfigurar o Macie para usar as credenciais de usuário do IAM, o Macie excluirá permanentemente as configurações existentes do perfil do IAM: o nome do perfil e o ID externo da sua configuração. Posteriormente, se sua organização optar por usar os perfis do IAM novamente, você precisará especificar um novo ID externo na política de confiança para o perfil em cada conta de membro aplicável.

Para obter detalhes sobre as opções de configuração para os tipos de conta, consulte Requisitos e opções de configuração para recuperar amostras de dados confidenciais com descobertas.

Para definir as configurações no Macie e habilitar a configuração da sua conta, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para definir e habilitar as configurações usando o console do Amazon Macie.

Para definir e habilitar as configurações do Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor Região da AWS no canto superior direito da página, selecione a região na qual deseja configurar e habilitar o Macie para recuperar e revelar amostras de dados confidenciais.
3. No painel de navegação, em Configurações, selecione Revelar amostras.
4. Na seção Configurações, escolha Editar.
5. Em Status, escolha Enabled (Habilitado).
6. Em Acesso, especifique o método de acesso e as configurações que deseja usar ao recuperar amostras de dados confidenciais dos objetos afetados do S3:

   - Para usar um perfil do IAM que delegue acesso ao Macie, escolha Assumir um perfil do IAM. Se você escolher essa opção, o Macie recuperará as amostras assumindo o perfil do IAM que você criou e configurou na sua Conta da AWS. Na caixa Nome do perfil, insira o nome do perfil.

- Para usar as credenciais do usuário do IAM que solicita as amostras, escolha Usar credenciais do usuário do IAM. Se você escolher essa opção, cada usuário da sua conta usará sua identidade individual do IAM para recuperar as amostras.

7. Em Criptografia, especifique a AWS KMS key que deseja usar para criptografar as amostras de dados confidenciais que forem recuperadas:

   - Para usar uma chave do KMS da sua própria conta, escolha Selecionar uma chave da sua conta. Em seguida, na lista AWS KMS key, selecione a chave a ser usada. A lista exibe as chaves do KMS de criptografia simétrica existentes para sua conta.
   - Para usar uma chave do KMS de outra conta, selecione Inserir o ARN de uma chave de outra conta. Em seguida, na caixa AWS KMS key ARN, insira o nome do recurso da Amazon (ARN) da chave a ser utilizada — por exemplo, **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**.

8. Após terminar de inserir configurações, escolha Salvar.

O Macie testa as configurações e verifica se elas estão corretas. Se você tiver configurado o Macie para assumir um perfil do IAM, o Macie também verificará se o perfil existe na sua conta e se as políticas de confiança e permissões estão configuradas corretamente. Se houver algum problema, o Macie exibirá uma mensagem descrevendo o problema.

Para resolver um problema com a AWS KMS key, consulte os requisitos no tópico anterior e especifique uma chave do KMS que atenda aos requisitos. Para resolver um problema com o perfil do IAM, comece verificando se você inseriu o nome correto do perfil. Se o nome estiver correto, certifique-se de que as políticas do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Para obter esses detalhes, consulte Configurar um perfil do IAM para acessar objetos afetados do S3. Após corrigir qualquer erro, você poderá salvar e habilitar as configurações.

> **Note**
>
> Se você for o administrador do Macie para uma organização e tiver configurado o Macie para assumir um perfil do IAM, o serviço vai gerar e exibir um ID externo depois que você salvar as configurações da sua conta. Anote esse ID. A política de confiança para o perfil do IAM em cada uma das suas contas de membro aplicáveis deve especificar esse ID. Caso contrário, não será possível recuperar amostras de dados confidenciais de objetos do S3 de propriedade da conta.

API

Para definir e habilitar as configurações de maneira programática, use a operação UpdateRevealConfiguration da API do Amazon Macie. Em sua solicitação, especifique os valores adequados para os parâmetros compatíveis:

- Para os parâmetros de `retrievalConfiguration`, especifique o método de acesso e as configurações que deseja usar ao recuperar amostras de dados confidenciais dos objetos afetados do S3:
  - Para assumir um perfil do IAM que delegue acesso ao Macie, especifique `ASSUME_ROLE` para o parâmetro `retrievalMode` e especifique o nome do perfil do parâmetro `roleName`. Se você especificar essas configurações, o Macie recuperará as amostras assumindo o perfil do IAM que você criou e configurou na sua Conta da AWS.
  - Para usar as credenciais do usuário do IAM que solicita as amostras, especifique `CALLER_CREDENTIALS` para o parâmetro `retrievalMode`. Se você especificar essa configuração, cada usuário da sua conta usará sua identidade individual do IAM para recuperar as amostras.

  > **Important**
  >
  > Se você não especificar valores para esses parâmetros, o Macie definirá o método de acesso (`retrievalMode`) como `CALLER_CREDENTIALS`. Se o Macie estiver configurado para usar um perfil do IAM para recuperar as amostras, o Macie também excluirá permanentemente o nome do perfil atual e o ID externo da sua configuração. Para manter essas configurações em uma configuração existente, inclua os parâmetros `retrievalConfiguration` em sua solicitação e especifique suas configurações atuais para esses parâmetros. Para recuperar suas configurações atuais, use a operação GetRevealConfiguration ou, se estiver usando a AWS Command Line Interface (AWS CLI), execute o comando get-reveal-configuration.

- Para o parâmetro `kmsKeyId`, especifique a AWS KMS key que deseja usar para criptografar as amostras de dados confidenciais que forem recuperadas:
  - Para usar uma chave do KMS da sua própria conta, especifique o nome do recurso da Amazon (ARN), o ID ou o alias da chave. Se você especificar um alias, inclua o prefixo `alias/` — por exemplo, `alias/ExampleAlias`.
  - Para usar uma chave do KMS que outra conta possui, especifique o ARN da chave — por exemplo, `arn:aws:kms:us-`

`east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. Ou especifique o ARN do alias da chave, por exemplo, `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`.

- Para o parâmetro `status`, especifique `ENABLED` para habilitar a configuração da sua conta Macie.

Em sua solicitação, não se esqueça de especificar também a Região da AWS na qual deseja habilitar e usar a configuração.

Para definir e habilitar as configurações usando a AWS CLI, execute o comando update-reveal-configuration e especifique os valores adequados para os parâmetros compatíveis. Por exemplo, se estiver usando a AWS CLI no Microsoft Windows, execute o seguinte 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\"}
```

Em que:

- *us-east-1* é a região na qual habilitar e usar a configuração. Neste exemplo, a Região Leste dos EUA (Norte da Virgínia).
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias* é o ARN do alias da AWS KMS key a ser utilizada. Neste exemplo, a chave pertence a outra conta.
- `ENABLED` é o status da configuração.
- *ASSUME_ROLE* é o método de acesso a ser usado. Neste exemplo, assuma o perfil do IAM especificado.
- *MacieRevealRole* é o nome do perfil do IAM que o Macie deve assumir ao recuperar amostras de dados confidenciais.

O exemplo anterior usa o caractere circunflexo (^) de continuação de linha para melhorar a legibilidade.

Quando você envia sua solicitação, o Macie testa as configurações. Se você tiver configurado o Macie para assumir um perfil do IAM, o Macie também verificará se o perfil existe na sua conta

e se as políticas de confiança e permissões estão configuradas corretamente. Se houver algum problema, sua solicitação vai falhar e o Macie retornará uma mensagem descrevendo o erro. Para resolver um problema com a AWS KMS key, consulte os requisitos no tópico anterior e especifique uma chave do KMS que atenda aos requisitos. Para resolver um problema com o perfil do IAM, comece verificando se você especificou o nome correto do perfil. Se o nome estiver correto, certifique-se de que as políticas do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Para obter esses detalhes, consulte Configurar um perfil do IAM para acessar objetos afetados do S3. Reenvie sua solicitação após resolver o problema.

Se a sua solicitação for realizada com êxito, o Macie habilitará a configuração da sua conta na Região especificada e você receberá um resultado semelhante ao seguinte.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Onde `kmsKeyId` especifica a AWS KMS key a ser usada para criptografar amostras de dados confidenciais recuperadas e `status` é o status da configuração da sua conta do Macie. Os valores `retrievalConfiguration` especificam o método de acesso e as configurações a serem usadas ao recuperar as amostras.

> **Note**
>
> Se você for o administrador do Macie de uma organização e tiver configurado o Macie para assumir um perfil do IAM, anote o ID externo (`externalId`) na resposta. A política de confiança para o perfil do IAM em cada uma das suas contas de membro aplicáveis deve especificar esse ID. Caso contrário, não será possível recuperar amostras de dados confidenciais de objetos afetados do S3 de propriedade da conta.

Para verificar posteriormente as configurações ou o status da configuração da sua conta, use a operação getRevealConfiguration ou, para o AWS CLI, execute o comando get-reveal-configuration.

Como desabilitar configurações do Amazon Macie

É possível desabilitar a qualquer momento as configurações da sua conta do Amazon Macie. Se você desabilitar a configuração, o Macie manterá a configuração que especifica qual AWS KMS key usar para criptografar as amostras de dados confidenciais que forem recuperadas. O Macie excluirá permanentemente as configurações de acesso do Amazon S3 para a configuração.

> **Warning**
>
> Ao desabilitar as configurações da sua conta do Macie, você também exclui permanentemente as configurações atuais que especificam como acessar os objetos afetados do S3. Se o Macie estiver configurado para acessar objetos afetados assumindo um perfil do AWS Identity and Access Management (IAM), isso incluirá: o nome do perfil e o ID externo que o Macie gerou para a configuração. Essas configurações não podem ser recuperadas depois de excluídas.

Para desabilitar as configurações da sua conta do Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para desabilitar as configurações da sua conta usando o console do Amazon Macie.

Para desabilitar as configurações do Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor de Região da AWS no canto superior direito da página, selecione a região na qual você deseja desabilitar as configurações para sua conta do Macie.
3. No painel de navegação, em Configurações, selecione Revelar amostras.
4. Na seção Configurações, escolha Editar.
5. Em Status, escolha Desabilitar.

6. Escolha Save (Salvar).

API

Para desabilitar as configurações de maneira programática, use a operação UpdateRevealConfiguration da API do Amazon Macie. Em sua solicitação, não se esqueça de especificar a Região da AWS na qual deseja desabilitar a configuração. Para o parâmetro `status`, especifique `DISABLED`.

Para desabilitar as configurações usando a AWS Command Line Interface (AWS CLI), execute o comando update-reveal-configuration. Use o parâmetro `region` para especificar a região na qual deseja desabilitar a configuração. Para o parâmetro `status`, especifique `DISABLED`. Por exemplo, se estiver usando a AWS CLI no Microsoft Windows, execute o seguinte comando:

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

Em que:

- *`us-east-1`* é a região na qual deseja desabilitar a configuração. Neste exemplo, a Região Leste dos EUA (Norte da Virgínia).
- `DISABLED` é o novo status da configuração.

Se a sua solicitação for realizada com êxito, o Macie desabilitará a configuração da sua conta na Região especificada e você receberá um resultado semelhante ao seguinte.

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

Onde `status` é o novo status da configuração da sua conta do Macie.

Se o Macie tiver sido configurado para assumir um perfil do IAM para recuperar amostras de dados confidenciais, você poderá excluir o perfil e a política de permissões do perfil de maneira opcional. O Macie não exclui esses recursos quando você desabilita as configurações da sua conta. Além

disso, o Macie não usa esses recursos para realizar nenhuma outra tarefa na sua conta. Para excluir o perfil e sua política de permissão, é possível usar o console do IAM ou a API do IAM. Para obter mais informações, consulte Excluir perfis no Guia do usuário do AWS Identity and Access Management.

Como recuperar e revelar amostras de dados confidenciais com descobertas

Com o Amazon Macie, é possível recuperar e revelar amostras de dados confidenciais que o Macie relata em descobertas individuais de dados confidenciais. Isso inclui dados confidenciais que o Macie detectou usando identificadores de dados gerenciados e dados que correspondem aos critérios dos identificadores de dados personalizados. As amostras podem ajudar você a verificar a natureza dos dados confidenciais que o Macie encontrou. Eles podem ajudar você a personalizar sua investigação sobre o objeto e o bucket afetados do Amazon Simple Storage Service (Amazon S3). Você pode recuperar e revelar amostras de dados confidenciais em todas as regiões Regiões da AWS onde o Macie está disponível atualmente, exceto nas regiões Ásia-Pacífico (Osaka) e Israel (Tel Aviv).

Se você recuperar e revelar amostras de dados confidenciais para uma descoberta, o Macie usa os dados no resultado correspondente da descoberta de dados confidenciais para localizar as primeiras 1 a 10 ocorrências de dados confidenciais relatadas pela descoberta. Em seguida, p Macie extrai os primeiros 1 a 128 caracteres de cada ocorrência do objeto do S3 afetado. Se uma descoberta relata vários tipos de dados confidenciais, o Macie faz isso para até cem tipos de dados confidenciais relatados pela descoberta.

Quando o Macie extrai dados confidenciais de um objeto do S3 afetado, o Macie criptografa os dados com uma chave AWS Key Management Service (AWS KMS) especificada por você, armazena temporariamente os dados criptografados em um cache e retorna os dados em seus resultados para a descoberta. Logo após a extração e a criptografia, o Macie exclui permanentemente os dados do cache, a menos que uma retenção adicional seja temporariamente necessária para resolver um problema operacional.

Se você optar por recuperar e revelar amostras de dados confidenciais para uma descoberta novamente, o Macie repetirá o processo para localizar, extrair, criptografar, armazenar e, por fim, excluir as amostras.

Para uma demonstração de como você pode recuperar e revelar amostras de dados confidenciais usando o console do Amazon Macie, assista ao seguinte vídeo: Recuperação e revelação de amostras de dados confidenciais com o Amazon Macie.

Tópicos

Antes de começar

Antes que possa recuperar e revelar amostras de dados confidenciais para descobertas, você precisará definir e habilitar as configurações da sua conta do Amazon Macie. Você também precisa trabalhar com seu AWS administrador para verificar se você tem as permissões e os recursos necessários.

Quando você recupera e revela amostras de dados confidenciais para uma descoberta, o Macie executa uma série de tarefas para localizar, recuperar, criptografar e revelar as amostras. O Macie não usa o perfil vinculado a serviços do Macie em sua conta para realizar essas tarefas. Em vez disso, você usa sua identidade AWS Identity and Access Management (IAM) ou permite que Macie assuma uma função do IAM em sua conta.

Para recuperar e revelar amostras de dados confidenciais para uma descoberta, você deve ter acesso à descoberta, ao resultado correspondente da descoberta de dados confidenciais e ao AWS KMS key que você configurou o Macie para usar para criptografar amostras de dados confidenciais. Além disso, você ou o perfil do IAM deve ter permissão para acessar o bucket afetado do S3 e o objeto afetado do S3. Você ou a função também devem ter permissão para usar o AWS KMS key que foi usado para criptografar o objeto afetado, se aplicável. Se alguma política do IAM, política de recursos ou outras configurações de permissões negar o acesso necessário, haverá um erro e o Macie não retornará nenhuma amostra para a descoberta.

Você também precisa ter permissão para realizar as seguintes ações do Macie:

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

As três primeiras ações permitem que você acesse sua conta do Macie e recupere os detalhes das descobertas. A última ação permite que você recupere e revele amostras de dados confidenciais das descobertas.

Para usar o console do Amazon Macie a fim de recuperar e revelar amostras de dados confidenciais, você também deve ter permissão para realizar a seguinte ação: `macie2:GetSensitiveDataOccurrencesAvailability`. Essa ação permite determinar se as amostras estão disponíveis para descobertas individuais. Você não precisa de permissão para realizar essa ação para recuperar e revelar amostras de forma programática. No entanto, ter essa permissão pode agilizar sua recuperação de amostras.

Se você for o administrador delegado do Macie de uma organização e tiver configurado o Macie para assumir um perfil do IAM para recuperar amostras de dados confidenciais, também deverá ter permissão para realizar a seguinte ação: `macie2:GetMember`. Essa ação permite que você recupere informações sobre a associação entre sua conta e uma conta afetada. Ela permite que o Macie verifique se você é atualmente o administrador do Macie para a conta afetada.

Se você não tiver permissão para realizar as ações necessárias ou acessar os dados e recursos necessários, peça ajuda ao AWS administrador.

Como determinar se as amostras de dados confidenciais estão disponíveis para uma descoberta

Para recuperar e revelar amostras de dados confidenciais para uma descoberta, a descoberta precisa atender a determinados critérios. Ele deve incluir dados de localização para ocorrências específicas de dados confidenciais. Além disso, ele precisa especificar a localização de um resultado de descoberta de dados confidenciais válido e correspondente. O resultado da descoberta de dados confidenciais deve ser armazenado da Região da AWS mesma forma que a descoberta. Se você configurou o Amazon Macie para acessar os objetos afetados do S3 assumindo uma função AWS Identity and Access Management (IAM), o resultado da descoberta de dados confidenciais também deve ser armazenado em um objeto do S3 que o Macie assinou com um Código de Autenticação de Mensagens (HMAC) baseado em Hash. AWS KMS key

O objeto do S3 afetado também precisa atender a determinados critérios. O tipo de MIME do objeto deve ser um dos seguintes:

- application/avro, para um arquivo de contêiner de objetos Apache Avro (.avro)
- application/gzip, para um arquivo compactado GNU Zip (.gz ou .gzip)
- application/json, para um arquivo JSON ou JSON Lines (.json ou .jsonl)
- application/parquet, para um arquivo Apache Parquet (.parquet)
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, para um arquivo de pasta de trabalho do Microsoft Excel (.xlsx)

- application/zip, para um arquivo compactado GNU Zip (.gz ou .gzip)
- text/csv, para um arquivo CSV (.csv)
- text/plain, para um arquivo de texto não binário diferente de um arquivo CSV, JSON, JSON Lines ou TSV
- text/tab-separated-values, para um arquivo CSV (.csv)

Além disso, o conteúdo do objeto do S3 deve ser o mesmo de quando a descoberta foi criada. O Macie verifica a tag de entidade do objeto (ETag) para determinar se ela corresponde à ETag especificada pela descoberta. Além disso, o tamanho de armazenamento do objeto não pode exceder a cota de tamanho aplicável para recuperar e revelar amostras de dados confidenciais. Para obter uma lista das cotas aplicáveis, consulteCotas do Amazon Macie.

Se uma descoberta e o objeto do S3 afetado atenderem aos critérios anteriores, amostras de dados confidenciais estarão disponíveis para a descoberta. Opcionalmente, você pode determinar se esse é o caso de uma descoberta específica antes de tentar recuperar e revelar amostras da descoberta.

Determinando se as amostras de dados confidenciais estão disponíveis para descobertas

Você pode usar o console do Amazon Macie ou a API do Amazon Macie para determinar se amostras de dados confidenciais estão disponíveis para uma descoberta.

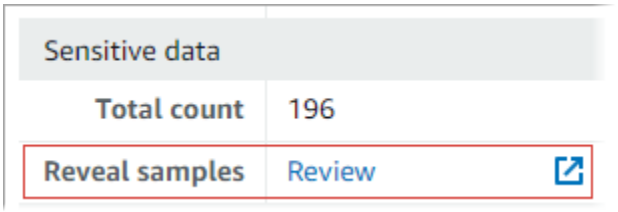
Console

Siga essas etapas no console do Amazon Macie para determinar se existem amostras de dados confidenciais disponíveis para uma descoberta.

Determinando se as amostras de dados confidenciais estão disponíveis para descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na página Descobertas, selecione a descoberta. O painel de detalhes exibirá informações sobre a descoberta.
4. No painel de detalhes, vá até a seção Dados confidenciais. Em seguida, consulte o campo Revelar amostras.

   Se houver amostras de dados confidenciais disponíveis para a descoberta, um link Revisar será exibido no campo, conforme mostrado na seguinte imagem.



Se não houver amostras de dados confidenciais disponíveis para a descoberta, o campo Revelar amostras exibirá um texto indicando o motivo:

- Conta fora da organização: você não tem permissão para acessar o objeto afetado do S3 usando o Macie. A conta afetada não faz parte da sua organização. Ou a conta faz parte da sua organização, mas o Macie não está habilitado para a conta na Região da AWS atual.
- Resultado inválido de classificação: não há um resultado correspondente de descoberta de dados confidenciais para a descoberta. Ou o resultado correspondente da descoberta de dados confidenciais não está disponível no Região da AWS atual, está malformado ou corrompido ou usa um formato de armazenamento incompatível. O Macie não consegue verificar a localização dos dados confidenciais a serem recuperados.
- Assinatura de resultado inválida: o resultado correspondente da descoberta de dados confidenciais é armazenado em um objeto do S3 que não foi assinado pelo Macie. O Macie não consegue verificar a integridade e a autenticidade do resultado da descoberta de dados confidenciais. Portanto, o Macie não consegue verificar a localização dos dados confidenciais a serem recuperados.
- Perfil de membro muito permissivo: a política de confiança ou de permissões para o perfil do IAM na conta de membro afetada não atende aos requisitos do Macie para restringir o acesso ao perfil. Ou a política de confiança do perfil não especifica o ID externo correto para sua organização. O Macie não pode assumir o perfil para recuperar os dados confidenciais.
- GetMember Permissão ausente — Você não tem permissão para recuperar informações sobre a associação entre sua conta e a conta afetada. O Macie não consegue determinar se você não tem permissão para acessar o objeto afetado do S3 como administrador delegado do Macie para a conta afetada.
- Objeto excede a cota de tamanho: o tamanho de armazenamento do objeto afetado do S3 excede a cota de tamanho para recuperar e revelar amostras de dados confidenciais desse tipo de arquivo.

- Objeto indisponível: o objeto afetado do S3 não está disponível. O objeto foi renomeado, movido ou excluído, ou seu conteúdo foi alterado depois que o Macie criou a descoberta. Ou o objeto está criptografado com uma AWS KMS key que está atualmente desabilitada.
- Resultado não assinado: o resultado correspondente da descoberta de dados confidenciais está armazenado em um objeto do S3 que não foi assinado. O Macie não consegue verificar a integridade e a autenticidade do resultado da descoberta de dados confidenciais. Portanto, o Macie não consegue verificar a localização dos dados confidenciais a serem recuperados.
- Perfil muito permissivo: sua conta está configurada para recuperar ocorrências de dados confidenciais usando um perfil do IAM cuja política de confiança ou permissões não atende aos requisitos do Macie para restringir o acesso ao perfil. O Macie não pode assumir o perfil para recuperar os dados confidenciais.
- Tipo de objeto incompatível: o objeto afetado do S3 usa um formato de arquivo ou armazenamento não compatível com o Macie para recuperar e revelar amostras de dados confidenciais. O tipo MIME do objeto afetado do S3 não é um dos valores na lista anterior.

Se houver um problema com o resultado da descoberta de dados confidenciais, as informações no campo Localização detalhada do resultado da descoberta poderão ajudar você a investigar o problema. Esse campo especifica o caminho original para o resultado no Amazon S3. Para investigar um problema com um perfil do IAM, certifique-se de que as políticas do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Para obter esses detalhes, consulte Configurar um perfil do IAM para acessar objetos afetados do S3.

API

Para determinar programaticamente se amostras de dados confidenciais estão disponíveis para uma descoberta, use a GetSensitiveDataOccurrencesAvailabilityoperação da API Amazon Macie. Ao enviar sua solicitação, use o parâmetro `findingId` para especificar o identificador exclusivo da descoberta. Para obter esse identificador, você pode usar a ListFindingsoperação.

Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando get-sensitive-data-occurrences-availability e use o `finding-id` parâmetro para especificar o identificador exclusivo para a descoberta. Para obter esse identificador, você pode usar a operação ListFindings.

Se sua solicitação tiver êxito e as amostras estiverem disponíveis para a descoberta, você receberá um resultado semelhante a este:

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

Se sua solicitação tiver êxito e as amostras não estiverem disponíveis para a descoberta, o valor do campo `code` será `UNAVAILABLE` e a matriz `reasons` especificará o motivo. Por exemplo: .

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

Se houver um problema com o resultado da descoberta de dados confidenciais, as informações no campo `classificationDetails.detailedResultsLocation` da descoberta poderão ajudar você a investigar o problema. Esse campo especifica o caminho original para o resultado no Amazon S3. Para investigar um problema com um perfil do IAM, certifique-se de que as políticas do perfil atendam a todos os requisitos para que o Macie assuma o perfil. Para obter esses detalhes, consulte Configurar um perfil do IAM para acessar objetos afetados do S3.

Como recuperar e revelar amostras de dados confidenciais para uma descoberta

Para recuperar e revelar amostras de dados confidenciais de uma descoberta, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

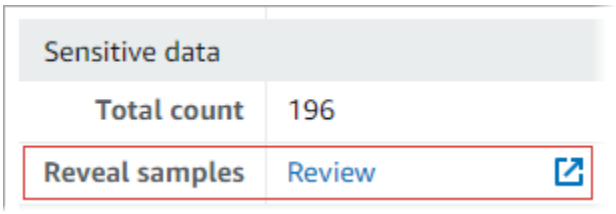
Console

Siga estas etapas para recuperar e revelar amostras de dados confidenciais de uma descoberta usando o console do Amazon Macie.

Para recuperar e revelar amostras de dados confidenciais de uma descoberta

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.

3. Na página Descobertas, selecione a descoberta. O painel de detalhes exibirá informações sobre a descoberta.
4. No painel de detalhes, vá até a seção Dados confidenciais. Em seguida, no campo Revelar amostras, selecione Revisar:

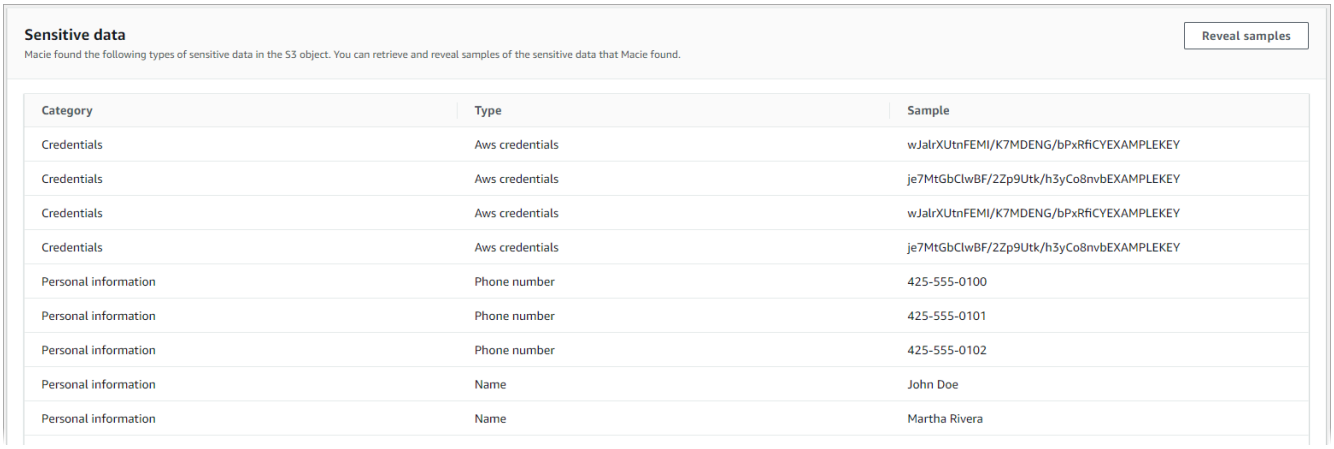


> **Note**
>
> Se o link Revisar não aparecer no campo Revelar amostras, as amostras de dados confidenciais não estarão disponíveis para a descoberta. Para obter informações sobre porque esse é o caso, consulte o tópico anterior.

Depois de selecionar Revisar, o Macie exibe uma página que resume os principais detalhes da descoberta. Os detalhes incluem as categorias, os tipos e o número de ocorrências de dados confidenciais que o Macie encontrou no objeto do S3 afetado.

5. Na seção Dados confidenciais da página, selecione Revelar amostras. Em seguida, o Macie vai recuperar e revelar amostras das primeiras 1 a 10 ocorrências de dados confidenciais relatadas pela descoberta. Cada amostra contém os primeiros 1 a 128 caracteres de uma ocorrência de dados confidenciais. A recuperação e revelação das amostras pode demorar vários minutos.

   Se a descoberta relatar vários tipos de dados confidenciais, o Macie recupera e revela amostras de até cem tipos. Por exemplo, a imagem a seguir mostra amostras que abrangem várias categorias e tipos de dados confidenciais:AWS credenciais, números de telefone dos EUA e nomes de pessoas.



Sensitive data

Macie found the following types of sensitive data in the S3 object. You can retrieve and reveal samples of the sensitive data that Macie found.

Reveal samples

Category	Type	Sample
Credentials	Aws credentials	wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Credentials	Aws credentials	wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Credentials	Aws credentials	je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
Personal information	Phone number	425-555-0100
Personal information	Phone number	425-555-0101
Personal information	Phone number	425-555-0102
Personal information	Name	John Doe
Personal information	Name	Martha Rivera

As amostras são organizadas, primeiro, por categoria de dados confidenciais e, depois, por tipo de dados confidenciais.

API

Para recuperar e revelar amostras de dados confidenciais para uma descoberta de forma programática, use a GetSensitiveDataOccurrencesoperação da API do Amazon Macie. Ao enviar sua solicitação, use o parâmetro `findingId` para especificar o identificador exclusivo da descoberta. Para obter esse identificador, você pode usar a ListFindingsoperação.

Para recuperar e revelar amostras de dados confidenciais usando o AWS Command Line Interface (AWS CLI), execute o get-sensitive-data-occurrencescomando e use o `finding-id` parâmetro para especificar o identificador exclusivo da descoberta. Por exemplo: .

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

Onde *1f1c2d74db5d8caa76859ec52example* é o identificador exclusivo da descoberta. Para obter esse identificador usando o AWS CLI, você pode executar o comando list-findings.

Se a sua solicitação for realizada com êxito, o Macie começará a processar sua solicitação e você receberá um resultado semelhante a este:

```
{
    "status": "PROCESSING"
}
```

Pode demorar vários minutos para processar a sua solicitação. Em alguns minutos, envie sua solicitação novamente.

Se o Macie puder localizar, recuperar e criptografar as amostras de dados confidenciais, o Macie retornará as amostras em um mapa `sensitiveDataOccurrences`. O mapa especifica de 1 a 100 tipos de dados confidenciais relatados pela descoberta e, para cada tipo, de 1 a 10 amostras. Cada amostra contém os primeiros 1 a 128 caracteres de uma ocorrência de dados confidenciais relatada pela descoberta.

No mapa, cada chave é o ID do identificador de dados gerenciados que detectou os dados confidenciais, ou o nome e o identificador exclusivo do identificador de dados personalizado que detectou os dados confidenciais. Os valores são exemplos do identificador de dados gerenciados ou do identificador de dados personalizado especificado. Por exemplo, a resposta a seguir fornece três amostras de nomes de pessoas e duas amostras de chaves de acesso AWS secretas que foram detectadas por identificadores de dados gerenciados (`NAME`e`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"
}
```

Se sua solicitação tiver êxito, mas não houver amostras de dados confidenciais disponíveis para a descoberta, você receberá uma mensagem `UnprocessableEntityException` indicando porque as amostras não estão disponíveis. Por exemplo: .

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

No exemplo anterior, o Macie tentou recuperar amostras do objeto afetado do S3, mas o objeto não estava mais disponível. O conteúdo do objeto mudou depois que o Macie criou a descoberta.

Se sua solicitação tiver êxito, mas outro tipo de erro tiver impedido o Macie de recuperar e revelar amostras de dados confidenciais para a descoberta, você receberá uma saída semelhante à seguinte:

```
{
    "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"
}
```

O valor do campo `status` é `ERROR` e o campo `error` descreve o erro que ocorreu. As informações do tópico anterior podem ajudar você a investigar o erro.

Esquema JSON para locais de dados confidenciais

O Amazon Macie usa estruturas JSON padronizadas para armazenar informações sobre onde encontra dados confidenciais nos objetos do Amazon Simple Storage Service (Amazon S3). As estruturas são usadas por descobertas de dados confidenciais e resultados de detecções de dados confidenciais. Para descobertas de dados confidenciais, as estruturas fazem parte do esquema JSON para descobertas. Para analisar o esquema JSON completo das descobertas, consulte Descobertas na Referência de API do Amazon Macie. Para saber mais sobre os resultados da detecção de dados confidenciais, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Tópicos

- Visão geral do esquema JSON para locais de dados confidenciais

- Detalhes e exemplos de esquemas JSON para localizações de dados confidenciais

Visão geral do esquema JSON para locais de dados confidenciais

Para relatar a localização de dados confidenciais que o Amazon Macie encontrou em um objeto do S3 afetado, o esquema JSON para descobertas de dados confidenciais e resultados de descobertas de dados confidenciais inclui um objeto `customDataIdentifiers` e um objeto `sensitiveData`. O `customDataIdentifiers` objeto fornece detalhes sobre os dados que o Macie detectou usando identificadores de dados personalizados. O `sensitiveData` objeto fornece detalhes sobre os dados que o Macie detectou usando identificadores de dados gerenciados.

Cada objeto `customDataIdentifiers` e `sensitiveData` contém uma ou mais matrizes `detections`:

- Em um objeto `customDataIdentifiers`, a matriz `detections` indica quais identificadores de dados personalizados detectaram os dados e produziram a descoberta. Para cada identificador de dados personalizado, a matriz também indica o número de ocorrências dos dados que o identificador detectou. Também pode indicar a localização dos dados que o identificador detectou.
- Em um objeto `sensitiveData`, uma matriz `detections` indica os tipos de dados confidenciais que o Macie detectou usando identificadores de dados gerenciados. Para cada tipo de dado confidencial, a matriz também indica o número de ocorrências dos dados e pode indicar a localização dos dados.

Para uma descoberta de dados confidenciais, uma matriz `detections` pode incluir de 1 a 15 objetos `occurrences`. Cada objeto `occurrences` especifica onde o Macie detectou ocorrências individuais de um tipo específico de dados confidenciais.

Por exemplo, a matriz `detections` a seguir indica a localização de três ocorrências de dados confidenciais (números do Seguro Social dos EUA) que Macie encontrou em um arquivo 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"
       }
```

A localização e o número de objetos `occurrences` em uma matriz `detections` variam com base nas categorias, tipos e número de ocorrências de dados confidenciais que o Macie detecta durante um ciclo automatizado de análise de descoberta de dados confidenciais ou a execução de um trabalho de descoberta de dados confidenciais. Para cada execução de trabalho ou ciclo de análise, o Macie também usa um algoritmo de pesquisa detalhada para preencher as descobertas resultantes com detalhes sobre os dados de localização de 1 a 15 ocorrências específicas de dados confidenciais que o Macie detecta nos objetos do S3. Essas ocorrências são indicativas das categorias e dos tipos de dados confidenciais que um bucket e um objeto do S3 afetados podem conter.

Um objeto `occurrences` pode conter qualquer uma das seguintes estruturas, dependendo do tipo de arquivo ou formato de armazenamento do objeto S3 afetado:

- matriz `cells` – Essa matriz se aplica às pastas de trabalho do Microsoft Excel, arquivos CSV e arquivos TSV. Um objeto nessa matriz especifica uma célula ou campo em que o Macie detectou uma ocorrência de dados confidenciais.
- Matriz `lineRanges` – Essa matriz se aplica a arquivos de mensagens de e-mail (EML) e arquivos de texto não binários que não sejam arquivos CSV, JSON, JSON Lines e TSV; por exemplo,

arquivos HTML, TXT e XML. Um objeto nessa matriz especifica uma linha ou um intervalo inclusivo de linhas em que o Macie detectou uma ocorrência de dados confidenciais e a posição dos dados na linha ou linhas especificadas.

Em certos casos, um objeto em uma matriz `lineRanges` especifica a localização de uma detecção de dados confidenciais em um tipo de arquivo ou formato de armazenamento compatível com outro tipo de matriz. Esses casos são: uma detecção em uma seção não estruturada de um arquivo estruturado no geral, como um comentário em um arquivo; uma detecção em um arquivo malformado que o Macie analisa como texto sem formatação; e um arquivo CSV ou TSV que tem um ou mais nomes de coluna nos quais o Macie detectou dados confidenciais.

- Matriz `offsetRanges` – Isso está reservado para uso futuro. Se essa matriz estiver presente, o valor dela será nulo.
- matriz `pages` – Essa matriz se aplica aos arquivos Adobe Portable Document Format (PDF). Um objeto nessa matriz especifica uma página em que o Macie detectou uma ocorrência de dados confidenciais.
- matriz `records` – Essa matriz se aplica a contêineres de objetos Apache Avro, arquivos Apache Parquet, arquivos JSON e arquivos JSON Lines. Para contêineres de objetos Avro e arquivos Parquet, um objeto nessa matriz especifica um índice de registro e o caminho para um campo em um registro no qual o Macie detectou uma ocorrência de dados confidenciais. Para arquivos JSON e JSON Lines, um objeto nessa matriz especifica um caminho para um campo ou matriz no qual o Macie detectou uma ocorrência de dados confidenciais. Para arquivos JSON Lines, ele também especifica o índice da linha que contém os dados.

O conteúdo dessas matrizes varia de acordo com o tipo de arquivo ou formato de armazenamento do objeto S3 afetado e seu conteúdo.

Detalhes e exemplos de esquemas JSON para localizações de dados confidenciais

O Amazon Macie adapta o conteúdo das estruturas JSON que ele usa para indicar onde detectou dados confidenciais em tipos específicos de arquivos e de conteúdo. Os tópicos a seguir explicam e fornecem exemplos dessas estruturas.

Tópicos

- Matriz de registros

Para obter uma lista completa das estruturas JSON que podem ser incluídas em uma descoberta de dados confidenciais, consulte Descobertas na Referência de API do Amazon Macie.

Matriz de células

Aplica-se a: livros de trabalho do Microsoft Excel, arquivos CSV e arquivos TSV

Em uma matriz `cells`, um objeto `Cell` especifica uma célula ou campo em que o Macie detectou uma ocorrência de dados confidenciais. A tabela a seguir descreve a finalidade de cada campo em um objeto `Cell`.

Campo	Tipo	Descrição
`cellReference`	String	A localização da célula, como referência absoluta da célula, que contém a ocorrênci a. Esse campo se aplica somente às pastas de trabalho do Excel. Esse valor é nulo para arquivos CSV e TSV.
`column`	Inteiro	O número da coluna que contém a ocorrência. Para uma pasta de trabalho do Excel, esse valor se correlaci ona com os caracteres alfabéticos de um identific ador de coluna; por exemplo, 1 para a coluna A, 2 para a coluna B e assim por diante.
`columnName`	String	O nome da coluna que contém a ocorrência, se disponível.
`row`	Inteiro	O número da linha que contém a ocorrência.

O exemplo a seguir mostra a estrutura de um objeto `Cell` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo CSV.

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais no campo na quinta linha da terceira coluna (chamada SSN) do arquivo.

O exemplo a seguir mostra a estrutura de um objeto `Cell` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em uma pasta de trabalho do Excel.

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais na planilha chamada Planilha2 na pasta de trabalho. Nessa planilha, o Macie detectou dados confidenciais na célula na quinta linha da terceira coluna (coluna C, chamada SSN).

Matriz LineRanges

Aplica-se a: arquivos de mensagens de e-mail (EML) e arquivos de texto não binários que não sejam arquivos CSV, JSON, JSON Lines e TSV; por exemplo, arquivos HTML, TXT e XML

Em uma matriz `lineRanges`, um objeto `Range` especifica uma linha ou um intervalo inclusivo de linhas em que o Macie detectou uma ocorrência de dados confidenciais e a posição dos dados na linha ou nas linhas especificadas.

Esse objeto geralmente está vazio para tipos de arquivo compatíveis com outros tipos de matrizes em objetos `occurrences`. As exceções são:

- Dados em seções não estruturadas de um arquivo estruturado no geral, como um comentário em um arquivo.
- Dados em um arquivo malformado que o Macie analisa como texto sem formatação.
- Um arquivo CSV ou TSV que tem um ou mais nomes de coluna nos quais o Macie detectou dados confidenciais.

A tabela a seguir descreve a finalidade de cada campo em um objeto `Range` de uma matriz `lineRanges`.

Campo	Tipo	Descrição
`end`	Inteiro	O número de linhas desde o início do arquivo até o final da ocorrência.
`start`	Inteiro	O número de linhas desde o início do arquivo até o começo da ocorrência.
`startColumn`	Inteiro	O número de caracteres, com espaços e começando em 1, desde o início da primeira linha que contém a ocorrência (`start`) até o início da ocorrência.

O exemplo a seguir mostra a estrutura de um objeto `Range` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo TXT.

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou uma ocorrência completa de dados confidenciais (um endereço postal) na primeira linha do arquivo. O primeiro caractere na ocorrência tem 119 caracteres (com espaços) a partir do início dessa linha.

O exemplo a seguir mostra a estrutura de um objeto `Range` que especifica a localização de uma ocorrência de dados confidenciais que engloba várias linhas em um arquivo TXT.

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou uma ocorrência completa de dados confidenciais (um endereço postal) no intervalo das linhas 51 a 54 do arquivo. O primeiro caractere na ocorrência é o primeiro caractere na linha 51 do arquivo.

Matriz de páginas

Aplica-se a: arquivos Adobe Portable Document Format (PDF)

Em uma matriz `pages`, um objeto `Page` especifica uma página em que o Macie detectou uma ocorrência de dados confidenciais. O objeto contém um campo `pageNumber`. O campo `pageNumber` armazena um número inteiro que especifica o número da página que contém a ocorrência.

O exemplo a seguir mostra a estrutura de um objeto `Page` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo PDF.

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

No exemplo anterior, a descoberta indica que a página 10 do arquivo contém a ocorrência.

Matriz de registros

Aplica-se a: contêineres de objetos Apache Avro, arquivos Apache Parquet, arquivos JSON e arquivos JSON Lines

Para um contêiner de objetos Avro ou um arquivo Parquet, um objeto `Record` em uma matriz `records` especifica um índice de registro e o caminho para um campo em um registro no qual o Macie detectou uma ocorrência de dados confidenciais. Para arquivos JSON e JSON Lines, um objeto `Record` especifica um caminho para um campo ou matriz no qual o Macie detectou uma ocorrência de dados confidenciais. Para arquivos JSON Lines, ele também especifica o índice da linha que contém a ocorrência.

A tabela a seguir descreve a finalidade de cada campo em um objeto `Record`.

Campo	Tipo	Descrição
`jsonPath`	String	O caminho, como uma expressão JSONPath, até a ocorrência. Para um contêiner de objeto Avro ou um arquivo Parquet, esse é o caminho para o campo no registro (`recordIndex`) que contém a ocorrência. Para um arquivo JSON ou JSON Lines, esse é o caminho para o campo ou matriz que contém a ocorrência. Se os dados forem um valor em uma matriz, o caminho também indicará qual valor contém a ocorrência. Se o Macie detectar dados confidenciais no nome de qualquer elemento no caminho, o Macie omite o

Campo	Tipo	Descrição
		campo `jsonPath` de um objeto `Record`. Se o nome de um elemento de caminho exceder 240 caracteres, o Macie truncará o nome removendo caracteres do início do nome. Se o caminho completo resultante exceder 250 caracteres, o Macie também truncará o caminho, começando com o primeiro elemento no caminho, até que o caminho contenha 250 caracteres ou menos.
`recordIndex`	Inteiro	Para um contêiner de objeto Avro ou um arquivo Parquet, o índice do registro, começando em 0, para o registro que contém a ocorrência. Para um arquivo JSON Lines, o índice da linha, começando em 0, para a linha que contém a ocorrência. Esse valor é sempre `0` para arquivos JSON.

O exemplo a seguir mostra a estrutura de um objeto `Record` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo Parquet.

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
```

```
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais no registro do índice 7663 (registro número 7664). Naquele registro, o Macie detectou dados confidenciais no campo nomeado `abcdefghijklmnopqrstuvwxyz`. O caminho JSON completo para o campo no registro é `$.abcdefghijklmnopqrstuvwxyz`. O campo é descendente direto do objeto raiz (nível externo).

O exemplo a seguir também mostra a estrutura de um objeto `Record` para uma ocorrência de dados confidenciais que o Macie detectou em um arquivo Parquet. No entanto, neste exemplo, o Macie truncou o nome do campo que contém a ocorrência porque o nome excede o limite de caracteres.

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

No exemplo anterior, o campo é descendente direto do objeto raiz (nível externo).

No exemplo a seguir, também para uma ocorrência de dados confidenciais que o Macie detectou em um arquivo Parquet, o Macie truncou o caminho completo para o campo que contém a ocorrência. O caminho completo excede o limite de caracteres.

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais no registro do índice 2335 (registro número 2336). Naquele registro, o Macie detectou dados confidenciais no campo nomeado `abcdefghijklmnopqrstuvwxyz`. O caminho JSON completo para o campo no registro é:

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

O exemplo a seguir mostra a estrutura de um objeto `Record` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo JSON. Neste exemplo, a ocorrência é um valor específico em uma matriz.

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais no segundo valor de uma matriz chamada. `key` A matriz é filha de um objeto chamado`access`.

O exemplo a seguir mostra a estrutura de um objeto `Record` que especifica a localização de uma ocorrência de dados confidenciais que o Macie detectou em um arquivo JSON Lines.

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

No exemplo anterior, a descoberta indica que o Macie detectou dados confidenciais no terceiro valor (linha) no arquivo. Naquela linha, a ocorrência está em um campo chamado `key`, que é filho de um objeto chamado `access`.

Suprimir descobertas do Amazon Macie

Para simplificar sua análise das descobertas, você pode criar e usar regras de supressão. Uma regra de supressão é um conjunto de critérios de filtro baseados em atributos que define os casos em que você deseja que o Amazon Macie arquive as descobertas automaticamente. As regras de supressão são úteis em situações em que você revisou uma classe de descobertas e não quer ser notificado sobre elas novamente.

Por exemplo, você pode decidir permitir que os buckets do S3 contenham endereços de correspondência se os buckets não permitirem acesso público e criptografarem novos objetos automaticamente com um AWS KMS key particular. Nesse caso, você pode criar uma regra de supressão que especifique critérios de filtro para os seguintes campos: tipo de detecção de dados

confidenciais, permissão de acesso público ao bucket S3 e ID da chave KMS de criptografia do bucket S3. A regra suprime descobertas futuras que correspondam aos critérios do filtro.

Se você suprimir descobertas com uma regra de supressão, o Macie continuará gerando descobertas para ocorrências subsequentes de dados confidenciais e possíveis violações de políticas que correspondam aos critérios da regra. Porém, o Macie altera automaticamente o status das descobertas para arquivadas. Isso significa que as descobertas não aparecem por padrão no console do Amazon Macie, mas persistem no Macie até expirarem. O Macie armazena as descobertas por 90 dias.

Além disso, o Macie não publica descobertas suprimidas no Amazon EventBridge como eventos ou para o AWS Security Hub. No entanto, o Macie continua a criar e armazenar resultados de descoberta de dados confidenciais que se correlacionam com descobertas de dados confidenciais que você suprime. Isso ajuda a garantir que você tenha um histórico imutável de descobertas de auditorias de privacidade e de proteção de dados ou investigações que você realiza.

> **Note**
>
> Se a sua conta fizer parte de uma organização que gerencia de forma centralizada várias contas do Macie, as regras de supressão podem funcionar de forma diferente para a sua conta. Isso depende da categoria de descobertas que você deseja suprimir e se você tem uma conta de administrador ou membro do Macie:
>
> - Descobertas de políticas – Somente um administrador do Macie pode suprimir descobertas de políticas para as contas da organização.
>
>   Se você tiver uma conta de administrador no Macie e criar uma regra de supressão, o Macie aplicará a regra às descobertas de políticas de todas as contas da sua organização, a menos que você configure a regra para excluir contas específicas. Se você tiver uma conta de membro do Macie e quiser suprimir as descobertas da política para sua conta, entre em contato com o administrador do Macie.
> - Descobertas de dados confidenciais – Um administrador do Macie e membros individuais podem suprimir descobertas de dados confidenciais que seus trabalhos de descoberta de dados confidenciais produzem. Um administrador do Macie também pode suprimir as descobertas que o Macie gera ao realizar a descoberta automatizada de dados confidenciais para a organização.
>
>   Somente a conta que cria um trabalho de descoberta de dados confidenciais pode suprimir ou acessar as descobertas de dados confidenciais que o trabalho produzir. Somente

a conta de administrador do Macie de uma organização pode suprimir ou acessar os resultados que a descoberta automatizada de dados confidenciais produz para contas na organização.

Para obter mais informações sobre as tarefas que administradores e membros podem realizar, consulte Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Para criar e gerenciar regras de supressão, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Os tópicos a seguir explicam como fazer isso. Para a API, os tópicos incluem exemplos de como realizar essas tarefas usando o AWS Command Line Interface (AWS CLI). Você também pode realizar essas tarefas usando um versionamento atual de outra ferramenta de linha de comando da AWS ou de um SDK AWS, ou enviando solicitações HTTPS diretamente para o Macie. Para obter mais informações sobre as ferramentas e SDKs da AWS, consulte as Ferramentas de criação em AWS

Tópicos

Criar regras de supressão

Antes de criar uma regra de supressão, é importante observar que você não pode restaurar (desarquivar) descobertas suprimidas usando uma regra de supressão. Porém, você pode revisar as descobertas suprimidas no console do Amazon Macie e acessar as descobertas suprimidas com a API do Amazon Macie.

Ao criar uma regra de supressão, você especifica critérios de filtro, um nome e, opcionalmente, uma descrição da regra. Você pode criar uma regra de supressão usando o console do Amazon Macie ou a API do Amazon Macie.

Console

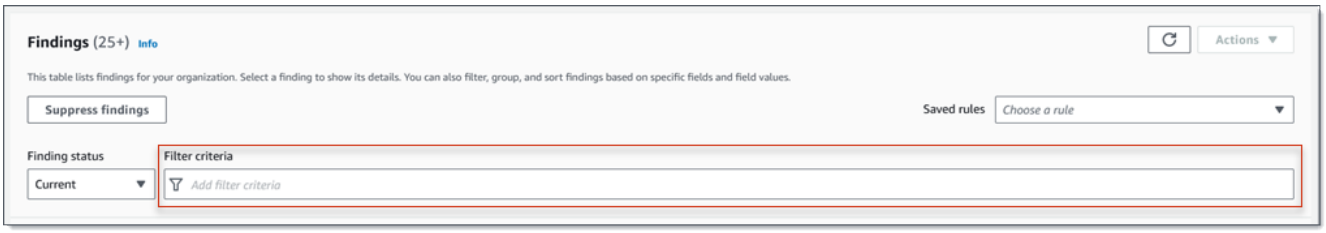
Siga estas etapas para criar uma regra de supressão usando o console do Amazon Macie.

Como criar uma regra de supressão

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.

> **Tip**
>
> Para usar uma regra de supressão ou filtro existente como ponto de partida, selecione a regra na lista Regras salvas.
> Você também pode simplificar a criação de uma regra ao analisar e detalhar antes as descobertas por meio de um grupo lógico predefinido. Se você fizer isso, o Macie criará e aplicará automaticamente as condições do filtro apropriadas, o que pode ser um ponto de partida útil para se criar uma regra. Para fazer isso, selecione Por bucket, Por tipo ou Por trabalho no painel de navegação (em Descobertas) e, em seguida, selecione um item na tabela. No painel de detalhes, selecione o link do campo a utilizar.

3. Na caixa Critérios de filtro, adicione condições de filtro que especifiquem os atributos das descobertas que você deseja que a regra suprima.



Para saber como adicionar condições de filtro, consulte Como criar e aplicar filtros às descobertas.

4. Ao terminar de adicionar condições de filtro para a regra, selecione Suprimir descobertas.
5. Em Regra de supressão, insira um nome e, opcionalmente, uma descrição da regra.
6. Escolha Save (Salvar).

API

Para criar uma regra de supressão programaticamente, use a operação CreateFindingsFilter da API do Amazon Macie e especifique os valores apropriados para os parâmetros necessários:

- Para o parâmetro `action`, especifique `ARCHIVE` para garantir que o Macie suprima as descobertas que correspondam aos critérios da regra.
- Para o parâmetro `criterion`, especifique um mapa de condições que defina os critérios de filtro para a regra.

  No mapa, cada condição deve especificar um campo, um operador e um ou mais valores para o campo. O tipo e o número de valores dependem do campo e do operador que você escolher. Para obter informações sobre os campos, operadores e tipos de valores que você pode usar em uma condição, consulteCampos para filtrar descobertas, Usando operadores em condições e Especificando valores para campos.

Para criar uma regra de supressão usando AWS CLI, execute o comando create-findings-filter e especifique os valores apropriados para os parâmetros necessários. Os exemplos a seguir criam uma regra de supressão que retorna todas as descobertas de dados confidenciais que estão atualmente em Região da AWS e relatam ocorrências de endereços de correspondência (e nenhum outro tipo de dados confidenciais) em objetos do S3.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

Este exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

Onde:

- *my_suppression_rule* é o nome personalizado da regra.
- `criterion` é um mapa das condições do filtro para a regra:
  - *classificationDetails.result.sensitiveData.detections.type* é o nome JSON do campo de Tipo de detecção de dados confidenciais.
  - *EqExactMatch* especifica o operador de correspondência exata igual.
  - *ENDEREÇO* é um valor enumerado para o campo de Tipo de detecção de dados confidenciais.

Se o comando for executado com sucesso, você receberá um resultado semelhante a este.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra de supressão que foi criada e `id` é o identificador exclusivo da regra.

Para obter exemplos adicionais de critérios de filtro, consulte Como filtrar descobertas de forma programática com a API do Amazon Macie.

Como revisar descobertas suprimidas

Por padrão, o Macie não exibe descobertas suprimidas no console do Amazon Macie. No entanto, você pode revisar essas descobertas no console alterando suas configurações do filtro.

Para revisar as descobertas suprimidas no console

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas. A página Descobertas exibe descobertas que o Macie criou ou atualizou para sua conta na região Região da AWS atual durante os últimos 90 dias. Por padrão, isso não inclui descobertas que foram suprimidas por uma regra de supressão.
3. Para Descoberta de status, faça um dos seguintes procedimentos:
   - Para exibir somente descobertas suprimidas, selecione Arquivado.
   - Para exibir descobertas suprimidas e não suprimidas, selecione Tudo.

- Para ocultar novamente as descobertas suprimidas, selecione Atual.

Você também pode acessar descobertas suprimidas usando a API do Amazon Macie. Para recuperar uma lista de descobertas suprimidas, use a operação ListFindings e inclua uma condição de filtro que especifique `true` para o campo `archived`. Para ver um exemplo de como fazer isso usando a AWS CLI, consulte Como filtrar descobertas de forma programática. Em seguida, para recuperar os detalhes de uma ou mais descobertas suprimidas, use a operação GetFindings e especifique o identificador exclusivo para cada descoberta a ser recuperada.

Modificando regras de supressão

Você pode modificar as configurações de uma regra de supressão a qualquer momento usando o console do Amazon Macie ou a API do Amazon Macie. Você também pode atribuir e gerenciar tags para a regra.

Uma tag é um rótulo que você define e atribui a determinados tipos de recursos AWS. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. As tags podem ajudar você a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Para saber mais, consulte Marcar recursos do Amazon Macie.

Console

Siga estas etapas para alterar as configurações de uma regra de supressão existente usando o console do Amazon Macie.

Para alterar uma regra de supressão

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na lista Regras salvas, selecione o ícone de edição () ao lado da regra de supressão que você deseja alterar.
4. Faça o seguinte:
   - Para alterar os critérios da regra, use a caixa Filtrar critérios para inserir condições que especificam os atributos das descobertas que você deseja que a regra suprima. Para saber como, consulte Como criar e aplicar filtros às descobertas.

- Para alterar o nome da regra, insira um novo nome na caixa Nome em Regra de supressão.
- Para alterar a descrição da regra, insira uma nova descrição na caixa Descrição em Regra de supressão.
- Para atribuir, revisar ou editar tags para a regra, selecione Gerenciar tags em Regra de supressão. Em seguida, revise e altere as tags conforme necessário. Uma regra pode ter até 50 tags.

5. Quando terminar de fazer as alterações, escolha Salvar.

API

Para alterar uma regra de supressão programaticamente, use a operação UpdateFindingsFilter da API do Amazon Macie. Ao enviar sua solicitação, use os parâmetros compatíveis para especificar um novo valor para cada configuração que você deseja alterar.

Para o parâmetro `id`, especifique o identificador único para a alteração da regra. Você pode obter esse identificador usando a operação ListFindingsFilter para obter uma lista de regras de supressão e de filtro para sua conta. Se estiver usando o AWS CLI, execute o comando list-findings-filters para recuperar essa lista.

Para alterar uma regra de supressão usando o AWS CLI, execute o comando update-findings-filter e use os parâmetros suportados para especificar um novo valor para cada configuração que você deseja alterar. Por exemplo, o comando a seguir altera o nome de uma regra de supressão existente.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

Onde:

- *8a3c5608-aa2f-4940-b347-d1451example* é o identificador exclusivo da regra.
- *mailing_addresses_only* é o novo nome da regra.

Se o comando for executado com sucesso, você receberá um resultado semelhante ao seguinte.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
```

```
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra de supressão que foi criada e `id` é o identificador exclusivo da regra.

Da mesma forma, o exemplo a seguir converte uma regra de filtro em uma regra de supressão, alterando o valor do parâmetro `action` de `NOOP` para `ARCHIVE`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

Onde:

- *`8a3c5608-aa2f-4940-b347-d1451example`* é o identificador exclusivo da regra.
- *`ARCHIVE`* é a nova ação que o Macie deve realizar com base em descobertas que correspondam aos critérios da regra — suprimir as descobertas.

Se o comando for executado com êxito, você receberá um resultado semelhante ao seguinte:

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) para a regra que foi alterada e `id` é o identificador único e exclusivo da regra.

Deletando as regras de supressão

Você pode deletar uma regra de supressão a qualquer momento usando o console do Amazon Macie ou a API do Amazon Macie. Se você deletar uma regra de supressão, o Macie deixará de suprimir ocorrências novas e subsequentes de descobertas que correspondam aos critérios da regra e não sejam suprimidas por outras regras. Observe, no entanto, que o Macie pode continuar suprimindo as descobertas que estiver processando atualmente e que correspondam aos critérios da regra.

Depois que você exclui uma regra de supressão, ocorrências novas e subsequentes de descobertas que correspondam aos critérios da regra têm o status atual (não arquivado). Isso significa que elas aparecem por padrão no console do Amazon Macie. Além disso, o Macie publica essas descobertas no Amazon EventBridge como eventos. Dependendo das configurações de publicação da sua conta, o Macie também publica as descobertas em AWS Security Hub.

Console

Siga estas etapas para deletar uma regra de supressão usando o console do Amazon Macie.

Excluir uma regra de supressão

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Descobertas.
3. Na lista de Regras salvas, selecione o ícone de edição () ao lado da regra de supressão que você deseja excluir.
4. Em Regra de supressão, selecione Excluir.

API

Para excluir uma regra de supressão programaticamente, use a operação DeleteFindingsFilter da API do Amazon Macie. Para o parâmetro `id`, especifique o identificador único para a regra de supressão a excluir. Você pode obter esse identificador usando a operação ListFindingsFilter para obter uma lista de regras de supressão e de filtro para a sua conta. Se estiver usando a AWS CLI, execute o comando list-findings-filters para recuperar essa lista.

Para excluir uma regra de supressão usando o AWS CLI, execute o comando delete-findings-filter. Por exemplo:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

Onde *8a3c5608-aa2f-4940-b347-d1451example* é o identificador exclusivo para que a regra de supressão apague.

Se o comando for executado com êxito, o Macie retornará uma resposta HTTP 200 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500 que indica o motivo de a operação ter falhado.

Pontuação de severidade das descobertas do Amazon Macie

Quando o Amazon Macie gera uma descoberta de política ou de dados confidenciais, ele atribui automaticamente uma severidade à descoberta. A severidade de uma descoberta reflete as principais características da descoberta e pode ajudá-lo a avaliar e priorizar suas descobertas. A severidade de uma descoberta não implica nem indica a criticidade ou a importância que um recurso afetado pode ter para a sua organização.

Para as descobertas de política, a severidade se baseia na natureza de um possível problema com a segurança ou a privacidade dos dados do Amazon Simple Storage Service (Amazon S3). Para descobertas de dados confidenciais, a severidade é baseada na natureza e no número de ocorrências de dados confidenciais que o Macie encontrou em um objeto do S3.

No Macie, a severidade de um achado é representada de duas maneiras.

Nível de severidade

Essa é uma representação qualitativa da severidade. Os níveis de severidade variam de Low, para menos severo, até High, para mais severo.

Os níveis de severidade aparecem diretamente no console do Amazon Macie. Eles também estão disponíveis em representações JSON de descobertas no console do Macie, da API Amazon Macie e em resultados de descobertas de dados confidenciais que se correlacionam com descobertas de dados confidenciais. Os níveis de severidade também estão incluídos na busca de eventos que o Macie publica no Amazon EventBridge e nas descobertas que o Macie publica para AWS Security Hub.

Pontuação de severidade

Essa é uma representação numérica da severidade. As pontuações de severidade variam de 1 a 3 e são mapeadas diretamente para os níveis de severidade:

Pontuação de severidade	Nível de severidade
1	Baixo
2	Médio
3	Alto

As pontuações de severidade não aparecem diretamente no console do Amazon Macie. No entanto, eles estão disponíveis em representações JSON de descobertas no console do Macie, da API Amazon Macie e em resultados de descobertas de dados confidenciais que se correlacionam com descobertas de dados confidenciais. As pontuações de severidade também estão incluídas em eventos de descobertas que o Macie publica no Amazon EventBridge. Eles não estão incluídos nas descobertas que o Macie publica em AWS Security Hub.

Os tópicos desta seção indicam como o Macie determina a severidade das descobertas de políticas e de dados confidenciais.

Tópicos

Pontuação de severidade das descobertas de políticas

A severidade de uma descoberta de política é baseada na natureza de um possível problema com a segurança ou a privacidade de um bucket do S3. A tabela a seguir lista os níveis de severidade que o Macie atribui a cada tipo de descoberta de política. Para obter uma descrição de cada tipo, consulte Tipos de descobertas.

Tipo de descoberta	Nível de severidade
Policy:IAMUser/S3BlockPublicAccessDisabled	Alto
Policy:IAMUser/S3BucketEncryptionDisabled	Baixo
Policy:IAMUser/S3BucketPublic	Alto
Policy:IAMUser/S3BucketReplicatedExternally	Alto
Policy:IAMUser/S3BucketSharedExternally	Alto
Policy:IAMUser/S3BucketSharedWithCloudFront	Médio

A severidade de uma descoberta de política não muda com base no número de ocorrências da descoberta.

Pontuação de severidade de descobertas de dados confidenciais

A severidade de descobertas de dados confidenciais é baseada na natureza e no número de ocorrências de dados confidenciais que o Macie encontrou em um objeto do S3. Os tópicos a seguir indicam como o Macie determina a severidade de cada tipo de descoberta de dados confidenciais:

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Para obter informações detalhadas sobre os tipos de dados confidenciais que o Macie pode detectar e relatar em descobertas de dados confidenciais, consulte Usar identificadores de dados gerenciados e Criar identificadores de dados personalizados.

SensitiveData:S3Object/Credentials

Uma descoberta de SensitiveData:S3Object/Credentials indica que um objeto S3 contém dados confidenciais de credenciais. Para esse tipo de descoberta, o Macie determina a severidade com base no tipo e no número de ocorrências dos dados de credenciais que o Macie encontrou no objeto.

A tabela a seguir indica os níveis de severidade que o Macie atribui às descobertas que relatam ocorrências de dados de credenciais em um objeto do S3.

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Chave de acesso secreta da AWS	Alto	Alto	Alto
Chave da API do Google Cloud	Alto	Alto	Alto

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Cabeçalho de autorização básica HTTP	Alto	Alto	Alto
JSON Web Token (JWT)	Alto	Alto	Alto
Chave privada OpenSSH	Alto	Alto	Alto
Chave privada PGP	Alto	Alto	Alto
Chave privada do padrão de criptografia de chave pública (PKCS)	Alto	Alto	Alto
Chave privada PuTTY	Alto	Alto	Alto
Chave da API Stripe	Alto	Alto	Alto

SensitiveData:S3Object/CustomIdentifier

Uma descoberta SensitiveData:S3Object/CustomIdentifier indica que um objeto do S3 contém texto que corresponde aos critérios de detecção de um ou mais identificadores de dados personalizados. O objeto pode conter mais de um tipo de dados confidenciais.

Por padrão, o Macie atribui o nível de severidade Médio a esse tipo de descoberta; se o objeto do S3 contiver pelo menos uma ocorrência de texto que corresponda aos critérios de detecção de pelo menos um identificador de dados personalizado, o Macie atribuirá automaticamente o nível de severidade Médio à descoberta. A severidade da descoberta não muda com base no número de ocorrências de texto que correspondem aos critérios de um identificador de dados personalizado.

No entanto, a severidade desse tipo de descoberta pode variar se você definir configurações de severidade personalizadas para um identificador de dados personalizado que produziu a descoberta. Se for esse o caso, o Macie determina a severidade da seguinte forma:

- Se o objeto do S3 contiver texto que corresponda aos critérios de detecção de apenas um identificador de dados personalizado, o Macie determinará a severidade da descoberta com base nas configurações de severidade para aquele identificador.
- Se o objeto do S3 contiver texto que corresponda aos critérios de detecção de mais de um identificador de dados personalizado, o Macie determinará a severidade da descoberta avaliando as configurações de severidade de cada identificador de dados personalizado, determinando qual dessas configurações produz a maior severidade e, em seguida, atribuindo aquela maior severidade à descoberta.

Para analisar as configurações de severidade de um identificador de dados personalizado, selecione Identificadores de dados personalizados no painel de navegação do console do Amazon Macie. Em seguida, selecione o nome do identificador de dados personalizado. A seção Severidade mostra as configurações. Para obter mais informações, consulte Definindo configurações de gravidade de busca para identificadores de dados personalizados.

SensitiveData:S3Object/Financial

Uma descoberta do SensitiveData:S3Object/Financial indica que um objeto do S3 contém informações financeiras confidenciais. Para esse tipo de descoberta, o Macie determina a severidade com base no tipo e no número de ocorrências das informações financeiras que o Macie encontrou no objeto.

A tabela a seguir indica os níveis de severidade que o Macie atribui às descobertas que relatam ocorrências de dados financeiros em um objeto do S3.

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Número da conta bancária [1]	Alto	Alto	Alto
Data de validade do cartão de crédito	Baixo	Médio	Alto
	Alto	Alto	Alto

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Dados da faixa magnética do cartão de crédito			
Números de cartão de crédito [2]	Alto	Alto	Alto
Código de verificação do cartão de crédito	Médio	Alto	Alto

1. Os níveis de severidade são os mesmos para qualquer tipo de número de conta bancária; um Número Básico de Conta Bancária (BBAN), um Número Internacional de Conta Bancária (IBAN) ou um número de conta bancária do Canadá ou dos EUA.
2. Os níveis de severidade são os mesmos para números de cartão de crédito que estão ou não próximos a uma palavra-chave.

Se uma descoberta relata vários tipos de informações financeiras em um objeto, o Macie determina a severidade da descoberta calculando a severidade de cada tipo de informação financeira encontrada por Macie, determinando qual tipo produz a maior severidade e atribuindo a maior severidade à descoberta. Por exemplo, se o Macie detectar 10 datas de vencimento do cartão de crédito (nível de severidade Médio) e 10 números de cartão de crédito de (Alto nível de severidade) em um objeto, o Macie atribuirá um nível de severidade Alto à descoberta.

SensitiveData:S3Object/Personal

Uma descoberta do SensitiveData:S3Object/Personal indica que um objeto do S3 contém informações pessoais confidenciais; informações pessoais de saúde (PHI), informações de identificação pessoal (PII) ou uma combinação das duas. Para esse tipo de descoberta, o Macie determina a severidade com base no tipo e no número de ocorrências dos dados de informações pessoais que o Macie encontrou no objeto.

A tabela a seguir indica os níveis de severidade que o Macie atribui às descobertas que relatam ocorrências de dados de confidenciais de PHI em um objeto do S3.

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Número de registro da Agência Antidrogas (DEA)	Alto	Alto	Alto
Número de reivindicação de seguro saúde (HICN)	Alto	Alto	Alto
Número de identificação médica ou do seguro de saúde	Alto	Alto	Alto
Código do Healthcare Common Procedure Coding System (HCPCS)	Alto	Alto	Alto
Código Nacional de Medicamentos (NDC)	Alto	Alto	Alto
Identificador do provedor nacional (NPI)	Alto	Alto	Alto
Identificador exclusivo de dispositivo (UDI)	Baixo	Médio	Alto

A tabela a seguir indica os níveis de severidade que o Macie atribui às descobertas de dados confidenciais que relatam ocorrências de PII em um objeto do S3.

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
	Baixo	Médio	Alto

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Datas de nascimento			
Número de identificação da carteira de habilitação	Baixo	Médio	Alto
Número de registro eleitoral	Alto	Alto	Alto
Nome completo	Baixo	Médio	Alto
Coordenadas do sistema de posicionamento global (GPS)	Baixo	Médio	Médio
Cookie HTTP	Baixo	Médio	Alto
Endereço postal	Baixo	Médio	Alto
Número de identificação nacional	Alto	Alto	Alto
Número do Seguro Nacional (NINO)	Alto	Alto	Alto
Número de passaporte	Médio	Alto	Alto
Número de residência permanente	Alto	Alto	Alto
Número de telefone	Baixo	Médio	Alto
Número do Seguro Social (SIN)	Alto	Alto	Alto

Tipo de dado confidencial	1 ocorrência	2 a 99 ocorrências	100 ou mais ocorrências
Número da Previdência Social (SSN)	Alto	Alto	Alto
Identificação do contribuinte ou número de referência	Alto	Alto	Alto
Número de identificação de veículo (VIN)	Baixo	Baixo	Médio

Se uma descoberta relatar vários tipos de informações de PHI, PII ou PHI e PII em um objeto, o Macie determinará a severidade da descoberta calculando a severidade de cada tipo de informação, determinando qual tipo produz a maior severidade e atribuindo a maior severidade à descoberta.

Por exemplo, se o Macie detectar 10 nomes completos (nível de severidade Médio) e 5 números de passaportes (nível de severidade Alto) em um objeto, o Macie atribuirá um nível de severidade Alto à descoberta. Igualmente, se o Macie detectar 10 nomes completos (nível de severidade Médio) e 10 números de identificação de seguro saúde (nível de severidade Alto) em um objeto, o Macie atribuirá um nível de severidade Alto à descoberta.

SensitiveData:S3Object/Multiple

Uma descoberta SensitiveData:S3Object/Multiple indica que um objeto do S3 contém dados abrangendo várias categorias de dados confidenciais; qualquer combinação de dados de credenciais, informações financeiras, informações pessoais ou texto que corresponda aos critérios de detecção de um ou mais identificadores de dados personalizados.

Para esse tipo de descoberta, o Macie determina a severidade calculando a severidade de cada tipo de dado confidencial encontrado pelo Macie (conforme indicado nos tópicos anteriores), determinando qual tipo produz a maior severidade e atribuindo a maior severidade à descoberta.

Por exemplo, se o Macie detectar 10 nomes completos (nível de severidade Médio) e 10 AWSchaves de acesso secreto (nível de severidade Alto) em um objeto, o Macie atribuirá um nível de severidade Alto à descoberta.

Monitoramento e processamento de descobertas do Amazon Macie

Para dar suporte à integração com outros aplicativos, serviços e sistemas, como os sistemas de monitoramento ou de gerenciamento de eventos, o Amazon Macie publica automaticamente descobertas de políticas e de dados confidenciais no Amazon EventBridge como eventos. Para fornecer mais suporte e uma análise mais ampla da postura de segurança da sua organização, você também pode configurar o Macie para publicar políticas e descobertas de dados confidenciais em AWS Security Hub.

Amazon EventBridge

O Amazon EventBridge, antes chamado de Amazon CloudWatch Events, é um serviço de barramento de eventos sem servidor que fornece um fluxo de dados em tempo real de aplicações e serviços e roteia esses dados para destinos como perfis AWS Lambda, tópicos do Amazon Simple Notification Service e streams do Amazon Kinesis. Com o EventBridge, você pode automatizar o monitoramento e o processamento de certos tipos de eventos, incluindo eventos que o Macie publica para as descoberta. Para saber mais sobre o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

Se você integrar as Notificações de Usuários da AWS com o Macie, também poderá usar os eventos do EventBridge para gerar notificações automaticamente sobre eventos que o Macie publica para descobertas. Com as notificações do usuário, você pode configurar regras personalizadas e canais de entrega para receber notificações sobre determinados tipos de eventos do Amazon EventBridge. Os canais de entrega incluem e-mail, notificações por chat AWS Chatbot e notificações por push AWS Console Mobile Application. Você também pode rever as notificações em um local central no AWS Management Console. Para saber mais sobre notificações de usuários, consulte o Guia do usuário de Notificações de Usuários da AWS.

AWS Security Hub

O AWS Security Hub é um serviço de segurança que fornece uma visão abrangente do seu estado de segurança no seu ambiente AWS. Ele coleta dados de segurança de Serviços da AWS e de soluções de segurança AWS Partner Network compatíveis e ajuda a verificar o ambiente de acordo com os padrões e as melhores práticas do setor de segurança. Ele também ajuda você a analisar as tendências de segurança e a identificar os problemas de segurança de maior prioridade. Com o Security Hub, é possível rever as descobertas do Macie como parte

de uma análise mais ampla da postura de segurança da sua organização. Também é possível agregar descobertas de várias Regiões da AWS e monitorar e processar dados de descobertas agregadas de uma única região. Para saber mais sobre o Security Hub, consulte o Guia do usuário do AWS Security Hub.

Quando o Macie cria uma descoberta, ele automaticamente publica a descoberta no EventBridge como um novo evento. Dependendo das configurações de publicação que você escolher para a sua conta, o Macie também publica a descoberta no Security Hub. O Macie publica cada descoberta nova imediatamente após a conclusão do processamento da descoberta. Se o Macie detectar uma ocorrência subsequente de uma descoberta de política existente, ele publica uma atualização no evento do EventBridge existente para a descoberta. Dependendo das configurações de publicação que você escolher para a sua conta, o Macie também publica a descoberta no Security Hub. O Macie publica essas atualizações de forma recorrente, usando uma frequência de publicação que você especifica nas configurações de publicação da sua conta.

Tópicos

Como definir as configurações de publicação para as descobertas do Amazon Macie

Para apoiar a integração com outros aplicativos, serviços e sistemas, o Amazon Macie publica automaticamente descobertas de políticas e descobertas de dados confidenciais na Amazon EventBridge como eventos. Para obter informações sobre como você pode usar EventBridge para monitorar e processar descobertas, consulteIntegração do Amazon Macie com o Amazon Eventbridge.

Você AWS Security Hub também pode configurar o Macie para publicar automaticamente as descobertas, usando as opções de destino que você especifica nas configurações de publicação da sua conta. Com essas opções, você pode configurar o Macie para publicar somente descobertas de políticas, somente descobertas de dados confidenciais ou descobertas de políticas e dados

confidenciais no Security Hub. Você também pode configurar o Macie para parar de publicar qualquer descoberta no Security Hub. Para obter informações sobre como você pode usar o Security Hub para monitorar e processar descobertas, consulte Integração do Amazon Macie com o AWS Security Hub.

Para descobertas de políticas, o momento em que o Macie publica uma descoberta para outra AWS service (Serviço da AWS) depende do fato de a descoberta ser nova e da frequência de publicação que você especificar para a sua conta. Para descobertas de dados confidenciais, o momento é sempre imediato; o Macie publica uma descoberta de dados confidenciais imediatamente após concluir o processamento da descoberta. Diferentemente das descobertas de políticas, o Macie trata todas as descobertas de dados confidenciais como novas (únicas).

Observe que o Macie não publica descobertas de políticas ou de dados confidenciais que são arquivadas automaticamente por uma regra de supressão. Em outras palavras, o Macie não publica descobertas suprimidas em outras Serviços da AWS.

Tópicos

- Como escolher destinos de publicação para descobertas
- Como determinar a frequência de publicação das descobertas
- Como alterar a frequência de publicação das descobertas

Como escolher destinos de publicação para descobertas

Você pode configurar o Amazon Macie para publicar automaticamente descobertas de políticas e dados confidenciais, AWS Security Hub além da Amazon. EventBridge Por padrão, o Macie publica somente descobertas de políticas novas e atualizadas para o Security Hub. Para alterar ou estender a configuração padrão, ajuste as configurações de destino da publicação para a sua conta.

Ao ajustar suas configurações de destino, você escolhe as categorias de descobertas que deseja que o Macie publique no Security Hub — somente descobertas de políticas, somente descobertas de dados confidenciais ou descobertas de políticas e dados confidenciais. Você também pode optar por parar de publicar qualquer categoria de descoberta no Security Hub.

Se você alterar as suas configurações de destino, a sua alteração se aplicará somente às Região da AWSatuais. Se você for o administrador do Macie de uma organização, a sua alteração se aplicará somente à sua conta. Ela não se aplicará a nenhuma conta de membro associada. Para ter mais informações, consulte Gerenciar várias contas da .

Para escolher destinos de publicação para descobertas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Configurações.
3. Na seção Publicação de descobertas, em Destinos, selecione entre as seguintes opções:

   - Publicar descobertas de políticas no Security Hub — Marque essa caixa de seleção para começar a publicar automaticamente descobertas de políticas novas e atualizadas no Security Hub. Para parar de publicar descobertas de políticas novas e atualizadas no Security Hub, desmarque essa caixa de seleção.

     Se você marcar essa caixa de seleção e tiver descobertas de políticas existentes, o Macie não as publicará automaticamente no Security Hub. Em vez disso, o Macie publica somente as descobertas de políticas que ele cria ou atualiza depois que você salva sua alteração.
   - Publicar descobertas de dados confidenciais no Security Hub — Marque essa caixa de seleção para começar a publicar novas descobertas de dados confidenciais no Security Hub automaticamente. Para parar de publicar novas descobertas de dados confidenciais no Security Hub, desmarque essa caixa de seleção.

     Se você marcar essa caixa de seleção e tiver descobertas de dados confidenciais existentes, o Macie não as publicará automaticamente no Security Hub. Em vez disso, o Macie publica somente as descobertas de dados confidenciais que ele cria depois que você salva sua alteração.
4. Escolha Salvar.

Se você optar por publicar qualquer categoria de descoberta no Security Hub, certifique-se de habilitar também o Security Hub na região atual e configurá-lo para aceitar descobertas do Macie. Caso contrário, não será possível acessar as descobertas no Security Hub. Para saber como aceitar descobertas no Security Hub, consulte Como gerenciar integrações de produtos no Guia do UsuárioAWS Security Hub .

Como determinar a frequência de publicação das descobertas

No Amazon Macie, cada descoberta tem um identificador exclusivo. O Macie usa esse identificador para determinar quando publicar uma descoberta para outra AWS service (Serviço da AWS):

- Novas descobertas – Quando o Macie cria uma nova política ou uma descoberta de dados confidenciais, ele atribui um identificador exclusivo à descoberta como parte do processamento

da descoberta. Imediatamente após a Macie terminar de processar a descoberta, ela publica a descoberta como um novo evento da Amazon. EventBridge Dependendo das configurações de publicação da sua conta, o Macie também publica as descobertas em AWS Security Hub.

- Descobertas atualizadas – Se o Macie detectar uma ocorrência posterior de uma descoberta de política existente, o Macie atualizará a descoberta existente adicionando detalhes sobre a ocorrência posterior e incrementando a contagem de ocorrências. O Macie também publica essas atualizações no EventBridge evento existente e, dependendo das configurações de publicação da sua conta, na descoberta existente do Security Hub. O Macie faz isso apenas para descobertas de políticas. Diferentemente das descobertas de políticas, todas as descobertas de dados confidenciais são tratadas como novas (únicas).

  Por padrão, o Macie publica descobertas atualizadas a cada 15 minutos como parte de um ciclo de publicação recorrente. Isso significa que todas as descobertas de políticas que forem atualizadas após o ciclo de publicação mais recente serão mantidas, atualizadas novamente conforme necessário e incluídas no próximo ciclo de publicação (aproximadamente 15 minutos depois). Você pode alterar essa programação escolhendo uma frequência de publicação diferente. Por exemplo, se você configurar o Macie para publicar descobertas atualizadas a cada hora e uma publicação ocorrer às 12 horas, todas as atualizações que ocorrerem depois das 12 horas serão publicadas às 13 horas.

Observe que nenhum desses casos se aplica às descobertas que são arquivadas automaticamente por uma regra de supressão. Macie não publica descobertas suprimidas para outras pessoas. Serviços da AWS

Como alterar a frequência de publicação das descobertas

Você pode alterar a programação que o Amazon Macie usa para publicar atualizações das descobertas de políticas existentes em outros. Serviços da AWSPor padrão, o Macie publica descobertas atualizadas a cada 15 minutos. Se você alterar essa programação, a sua alteração se aplicará somente à Região da AWSatual. Se você for o administrador do Macie de uma organização, a alteração também será aplicada a todas as contas-membro associadas na região. Para ter mais informações, consulte Gerenciar várias contas da .

Como configurar a frequência de publicação das descobertas atualizadas

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. No painel de navegação, selecione Configurações.

3. Na seção Publicação de descobertas, em Frequência de atualização das descobertas de políticas, escolha com que frequência você deseja que o Macie publique descobertas de políticas atualizadas em outras Serviços da AWS.
4. Selecione Salvar.

Integração do Amazon Macie com o Amazon Eventbridge

O Amazon EventBridge, anteriormente Amazon CloudWatch Events, é um serviço de barramento de eventos sem servidor. O EventBridge fornece um stream de dados em tempo real de aplicações e serviços e roteia esses dados para destinos como AWS Lambda funções, tópicos do Amazon Simple Notification Service (Amazon SNS) e streams do Amazon Kinesis. Para saber mais sobre o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

Com o EventBridge, você pode automatizar o monitoramento e o processamento de certos tipos de eventos. Isso inclui eventos que o Amazon Macie publica automaticamente para novas descobertas de políticas e descobertas de dados confidenciais. Isso também inclui eventos que o Macie publica automaticamente para ocorrências subsequentes de descobertas de políticas existentes. Para obter detalhes sobre como e quando Macie publica esses eventos, consulte. Como definir as configurações de publicação para as descobertas

Ao usar o EventBridge e os eventos que o Macie publica para as descobertas, você pode monitorar e processar as descobertas quase em tempo real. Em seguida, você pode agir de acordo com as descobertas usando outros aplicativos e serviços. Por exemplo, você pode usar o EventBridge para enviar tipos específicos de novas descobertas para uma AWS Lambda função. A função do Lambda pode então processar e enviar os dados para o sistema de gerenciamento de incidentes e eventos de segurança (SIEM). Se você integrar a notificação de usuários da empresa com o Macie, também poderá usar os eventos para ser notificado das descobertas automaticamente por meio dos canais de entrega que você especificar.

Além do monitoramento e processamento automatizados, o uso do EventBridge permite a retenção de longo prazo dos dados de suas descobertas. Macie armazena as descobertas por 90 dias. Com o EventBridge, você pode enviar dados de descobertas para sua plataforma de armazenamento preferida e armazenar os dados pelo tempo que quiser.

> **Note**
>
> Para retenção de longo prazo, configure também o Macie para armazenar os resultados de descoberta de dados confidenciais em um bucket do S3. Um resultado de descoberta

de dados confidenciais é um registro de detalhes sobre a análise que Macie realizou em um objeto do S3 para determinar se o objeto contém dados confidenciais. Para saber mais, consulte Armazenamento e retenção de resultados de descoberta de dados confidenciais.

Tópicos

Trabalhar com o Amazon EventBridge

Com o Amazon EventBridge, você cria regras para especificar quais eventos deseja monitorar e quais alvos você quer para realizar ações automatizadas para esses eventos. Um destino é um destino para o qual o EventBridge envia eventos.

Para automatizar as tarefas de monitoramento e processamento de descobertas, você pode criar uma regra do EventBridge que detecta automaticamente eventos de busca do Amazon Macie e envia esses eventos para outro aplicativo ou serviço para processamento ou outra ação. Você pode personalizar a regra para enviar somente os eventos que atendam a determinados critérios. Para fazer isso, especifique os critérios que derivam doEsquema de eventos do EventBridge para descobertas.

Por exemplo, você pode criar uma regra que envia tipos específicos de novas descobertas para uma AWS Lambda função. A função do Lambda pode então realizar tarefas como: processar e enviar os dados para seu sistema SIEM; aplicar automaticamente um certo tipo de criptografia do lado do servidor para um objeto do S3; ou restringir o acesso a um objeto do S3 alterando a lista de controle de acesso (ACL) do objeto. Ou você pode criar uma regra que envia automaticamente novas descobertas de alta severidade para um tópico do Amazon SNS, que então notifica sua equipe de resposta a incidentes sobre a descoberta.

Além de invocar funções do Lambda e notificar tópicos do Amazon SNS, o EventBridge oferece suporte a outros tipos de destinos e ações, como retransmissão de eventos para o Amazon Kinesis Streams, ativação de máquinas de estado do AWS Step Functions e invocação do comando de execução AWS Systems Manager. Para obter informações sobre destinos compatíveis, consulte Destinos do Amazon EventBridge no Manual do usuário do Amazon EventBridge.

Criar regras do Amazon EventBridge para descobertas

Os procedimentos a seguir explicam como usar o console do Amazon EventBridge e o AWS Command Line Interface(AWS CLI) para criar uma regra do EventBridge para as descobertas do Amazon Macie. A regra detecta eventos do EventBridge que usam o esquema e o padrão de evento para descobertas do Macie e envia esses eventos para uma função AWS Lambda para processamento.

O AWS Lambda é um serviço de computação que pode ser usado para executar código sem provisionamento ou gerenciamento de servidores. Você empacota o código e faz upload dele no AWS Lambda como uma função do Lambda. O AWS Lambda então executa a função quando ela é invocada. Uma função pode ser invocada manualmente por você, automaticamente em resposta a eventos ou em resposta a solicitações de aplicações ou serviços. Para obter mais informações sobre criar e invocar as funções do Lambda, consulte o AWS LambdaGuia do desenvolvedor.

Console

Esse procedimento explica como usar o console do Amazon EventBridge para criar uma regra que envia automaticamente todos os eventos de descoberta do Macie para uma função do Lambda para processamento. A regra usa configurações padrão para regras que são executadas quando eventos específicos são recebidos. Para obter detalhes sobre as configurações de regras ou para saber como criar uma regra que usa configurações personalizadas, consulte Criação de regras que reagem a eventos no Guia do usuário do Amazon EventBridge.

> **Tip**
>
> Você também pode criar uma regra que usa um padrão de evento personalizado para detectar e agir apenas em um subconjunto de eventos de descoberta do Macie. Esse subconjunto pode ser baseado em campos específicos que o Macie inclui em um evento de descoberta. Para saber mais sobre os campos disponíveis, consulteEsquema de eventos do EventBridge para descobertas. Para saber como criar esse tipo de regra, consulte Filtragem de conteúdo em padrões de eventos no Guia do usuário do Amazon EventBridge.

Antes de criar essa regra, crie a função do Lambda que deseja que a regra use como destino. Ao criar a regra, você precisará especificar essa função como o destino da regra.

Para criar uma regra de evento usando o console

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, em Events (Eventos), escolha Rules (Regras).
3. Na seção Rules (Regras), escolha Create rule (Criar regra).
4. Em Definir detalhe da regra, faça o seguinte:
   - Em Name (Nome), insira um nome para a regra.
   - (Opcional) Em Descrição, insira uma breve descrição da regra.
   - Para Barramento de eventos, verifique se o padrão está selecionado e Habilitar a regra nos barramentos de eventos selecionados está ligado.
   - Em Rule type (Tipo de regra), escolha Rule with an event pattern (Regra com um padrão de evento).
5. Ao terminar, escolha Avançar.
6. Em Criar padrão de evento, faça o seguinte:
   - Em Origem do evento, selecione AWS eventos ou parceiro do EventBridge.
   - (Opcional) Em Exemplo de evento, analise um evento de busca de amostra para Macie para saber o que um evento pode conter. Para fazer isso, selecione AWSeventos. Em seguida, em Eventos de amostra, selecione Macie Finding.
   - Na seção Padrão de evento, selecione Formulário de padrão de evento. Depois insira as seguintes configurações:
     - Para Event source (Origem do evento), escolha Serviços da AWS.
     - Para AWS service (Serviço da AWS), insira Macie.
     - Em Tipo de evento, insira Macie Finding.
7. Ao terminar, escolha Avançar.
8. Na página Selecione destinos, faça o seguinte:
   - Em Target types (Tipos de destino), escolha AWS service (Serviço da AWS).
   - Em Selecionar um destino, insira Função do Lambda. Então, para Função, selecione a função para a qual deseja enviar eventos.
   - Em Configurar versão/alias, insira as configurações de versão e alias para a função do Lambda de destino.

- (Opcional) Para Configurações adicionais, insira configurações personalizadas para especificar quais dados de eventos você deseja enviar para a função do Lambda. Você também pode especificar como lidar com eventos que não são entregues à função com sucesso.

9. Ao terminar, escolha Avançar.
10. Na página Configurar tags, insira opcionalmente uma ou mais tags a serem atribuídas à regra. Em seguida, escolha Next (Próximo).
11. Na página Revisar e criar, analise as configurações da regra e verifique se estão corretas.

    Para alterar uma configuração, selecione Editar para a configuração e insira a configuração correta. Você também pode usar as guias de navegação para acessar a página que contém uma configuração.
12. Depois de inserir configurações para a regra, selecione Criar.

AWS CLI

Este procedimento explica como usar o AWS CLI para criar uma regra do EventBridge que envia todos os eventos de busca do Macie para uma função do Lambda para processamento. A regra usa configurações padrão para regras que são executadas quando eventos específicos são recebidos. No procedimento, os comandos são formatados para o Microsoft Windows. Para Unix, Linux e macOS, substitua o caractere de continuação de linha circunflexo (^) por uma barra invertida (\).

Antes de criar essa regra, crie a função do Lambda que deseja que a regra use como destino. Ao criar a função, preste atenção o nome do recurso da Amazon (ARN) da função. Você precisará fornecer esse ARN ao especificar o destino da regra.

Para criar uma regra de evento usando o AWS CLI

1. Crie uma regra que detecte eventos para todas as descobertas que Macie publica no EventBridge. Para fazer isso, use o comando put-rule do EventBridge. Por exemplo:

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

   Onde *MacieFindings* é o nome que você deseja para a regra.

Se o comando for executado com êxito, o EventBridge responderá com o ARN da regra. Anote esse ARN. Ele será necessário na etapa 3.

> **Tip**
>
> Você também pode criar uma regra que usa um padrão de evento personalizado para detectar e agir apenas em um subconjunto de eventos de descoberta do Macie. Esse subconjunto pode ser baseado em campos específicos que o Macie inclui em um evento de descoberta. Para saber mais sobre os campos disponíveis, consulteEsquema de eventos do EventBridge para descobertas. Para saber como criar esse tipo de regra, consulte Filtragem de conteúdo em padrões de eventos no Guia do usuário do Amazon EventBridge.

2. Especifique a função do Lambda a ser usada como destino para a regra. Para fazer isso, use o comando put-targets do EventBridge. Por exemplo:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-findings-function
```

Onde *MacieFindings* for o nome que você especificou para a regra na etapa 1, e o valor para o parâmetro `Arn` for o ARN da função que você quer que a regra use como destino.

3. Adicione permissões que permitem que a regra chame a função do Lambda de destino. Para fazer isso, use o comando Lambda add-permission. Por exemplo:

```
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
```

Onde:

- *my-findngs-function* for o nome da função do Lambda que deseja que a regra use como destino.

- *Sid* é um identificador exclusivo que você define para descrever a instrução na política de função do Lambda.
- `source-arn` é o ARN da regra do EventBridge.

Se o comando for executado com êxito, você receberá um resultado semelhante a:

```
{
  "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\"}}}"
}
```

O valor `Statement` é uma versão da string JSON da instrução adicionada à política da função do Lambda.

Integração do Amazon Macie com o AWS Security Hub

AWS Security Hub é um serviço que fornece uma visão abrangente da sua postura de segurança em todo o seu ambiente AWS e ajuda a verificar seu ambiente em relação aos padrões e práticas recomendadas do setor de segurança. Ele faz isso em parte consumindo, agregando, organizando e priorizando suas descobertas de vários Serviços da AWS e soluções de segurança do AWS Partner Network. O Security Hub ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de prioridade mais alta. Com o Security Hub, também é possível agregar descobertas de várias Regiões da AWS e então monitorar e processar todos os dados de descobertas agregadas de uma única região. Para saber mais sobre o Security Hub, consulte o Guia do usuário da AWS Security Hub.

O Amazon Macie se integra ao Security Hub, o que significa que você pode publicar descobertas do Macie no Security Hub automaticamente. O Security Hub pode então incluir tais descobertas na análise feita sobre a seu procedimento de segurança. Além disso, você pode usar o Security Hub para monitorar e processar descobertas de políticas e dados confidenciais como parte de um

conjunto maior e agregado de dados de descobertas para seu AWS ambiente. Em outras palavras, você pode analisar as descobertas do Macie enquanto realiza análises mais amplas da postura de segurança da sua organização e corrigir as descobertas conforme necessário. O Security Hub elimina a complexidade de abordar grandes volumes de descobertas de vários provedores. Além disso, ele usa um formato padrão para todas as descobertas, incluindo as descobertas de Macie. O uso desse formato, o AWS Security Finding Format (ASFF), elimina a necessidade de realizar esforços demorados de conversão de dados.

Tópicos

Como o Amazon Macie publica as descobertas no AWS Security Hub

No AWS Security Hub, os problemas de segurança são rastreados como descobertas. Algumas descobertas provêm de problemas que são detectados por Serviços da AWS, como o Amazon Macie, ou por soluções de segurança AWS Partner Network compatíveis. O Security Hub também tem um conjunto de regras que ele usa para detectar problemas de segurança e gerar descobertas.

O Security Hub fornece ferramentas para gerenciar descobertas de todas essas fontes. Você pode revisar e filtrar listas de descobertas e revisar os detalhes de descobertas individuais. Para saber como, consulte Exibição de listas de descobertas e detalhes no Guia do usuário do AWS Security Hub. Você também pode rastrear o status de uma investigação em uma descoberta. Para saber como, consulte Tomar medidas sobre descobertas no Guia do usuário do AWS Security Hub.

Todas as descobertas no Security Hub usam um formato JSON padrão chamado AWS Security Finding Format (ASFF). O ASFF inclui detalhes sobre a origem de um problema, os recursos afetados e o status atual de uma descoberta. Para obter mais informações, consulte AWS Security Finding Format (ASFF) no Manual do usuário do AWS Security Hub.

Tipos de descobertas que o Macie o publica

Dependendo das configurações de publicação que você escolher para sua conta do Macie, o Macie pode publicar todas as descobertas criadas no Security Hub, tanto descobertas de dados confidenciais quanto descobertas de políticas. Para obter informações sobre essas configurações e como alterá-las, consulte Como definir as configurações de publicação para as descobertas. Por

padrão, o Macie publica somente descobertas de políticas novas e atualizadas para o Security Hub. Macie não o publicará descobertas de dados confidenciais no Security Hub.

Descobertas de dados confidenciais

Se você configurar o Macie para publicar descobertas de dados confidenciais no Security Hub, o Macie publicará automaticamente cada descoberta de dados confidenciais criada para sua conta e o fará imediatamente após concluir o processamento da descoberta. O Macie faz isso para todas as descobertas de dados confidenciais que não são arquivadas automaticamente por uma regra de supressão.

Se você for o administrador do Macie de uma organização, a publicação se limita às descobertas de trabalhos de descoberta de dados confidenciais que você executou e às atividades automatizadas de descoberta de dados confidenciais que o Macie realizou para sua organização. Somente a conta que cria um trabalho pode publicar as descobertas de dados confidenciais que o trabalho produz. Somente a conta de administrador do Macie pode publicar descobertas de dados confidenciais que a descoberta automatizada de dados confidenciais produz para sua organização.

Quando o Macie publica descobertas de dados confidenciais no Security Hub, ele usa o AWS Security Finding Format (ASFF), que é o formato padrão para todas as descobertas no Security Hub. No ASFF, o campo `Types` indica o tipo de descoberta. Esse campo usa uma taxonomia ligeiramente diferente da taxonomia do tipo de descoberta em Macie.

A tabela a seguir lista o tipo de descoberta ASFF para cada tipo de descoberta de dados confidenciais que o Macie pode criar.

Tipo de descoberta	Tipo de descoberta do 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	

Tipo de descoberta	Tipo de descoberta do ASFF
	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

Descobertas de política

Se você configurar o Macie para publicar descobertas de política no Security Hub, o Macie publicará automaticamente cada nova descoberta de política criada e fará isso imediatamente após concluir o processamento da descoberta. Se o Macie detectar uma ocorrência subsequente de uma descoberta de política existente, o publicará automaticamente uma atualização da descoberta existente no Security Hub, usando uma frequência de publicação especificada para sua conta. O Macie executa essas tarefas para todas as descobertas de políticas que não são arquivadas automaticamente por uma regra de supressão.

Se você for o administrador do Macie de uma organização, a publicação se limita às descobertas de políticas para buckets do S3 que pertencem diretamente à sua conta. O Macie não publica descobertas de políticas que ele cria ou atualiza para contas de membros em sua organização. Isso ajuda a garantir que você não tenha dados de descobertas duplicados no Security Hub.

Como é o caso das descobertas de dados confidenciais, o Macie usa o AWS Security Finding Format (ASFF) ao publicar descobertas de políticas novas e atualizadas no Security Hub. No ASFF, o campo `Types` usa uma taxonomia ligeiramente diferente da taxonomia do tipo de descoberta no Macie.

A tabela a seguir lista o tipo de descoberta ASFF para cada tipo de descoberta de política que o Macie pode criar. Se Macie criou ou atualizou uma descoberta de política no Security Hub em ou após 28 de janeiro de 2021, a descoberta tem um dos seguintes valores para o campo `Types` ASFF no Security Hub.

Tipo de descoberta	Tipo de descoberta do ASFF
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled

Tipo de descoberta	Tipo de descoberta do 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

Se o Macie criou ou atualizou uma descoberta de política antes de 28 de janeiro de 2021, a descoberta tem um dos seguintes valores para o campo ASFF `Types` no Security Hub:

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

Os valores na lista anterior são mapeados diretamente para valores do campo Tipo de descoberta (`type`) no Macie.

> **Note**
>
> Ao analisar e processar as descobertas de políticas no Security Hub, observe as seguintes exceções:
>
> - Em certezas Regiões da AWS, o Macie começou a usar os tipos de descoberta ASFF para descobertas novas e atualizadas já em 25 de janeiro de 2021.
> - Se você agiu de acordo com uma descoberta de política no Security Hub antes de Macie começar a usar os tipos de descoberta ASFF em sua Região da AWS, o valor do campo `Types` ASFF da descoberta será um dos tipos de descoberta do Macie na lista anterior. Não será um dos tipos de descoberta do ASFF na tabela anterior. Isso vale para as constatações de políticas nas quais você agiu usando o console AWS Security Hub ou a operação BatchUpdateFindings da API do AWS Security Hub.

Latência para publicar descobertas

Quando o Macie cria uma nova política ou uma descoberta de dados confidenciais, ele publica a descoberta no Security Hub imediatamente após concluir o processamento da descoberta.

Quando o Macie detecta uma ocorrência subsequente de uma descoberta de política existente, ele publica uma atualização para a descoberta existente do Security Hub. O momento da atualização depende da frequência de publicação que você escolher para sua conta Macie. Por padrão, o Macie publica atualizações a cada 15 minutos. Para obter mais informações, inclusive como alterar a configuração da sua conta, consulte Como definir as configurações de publicação para as descobertas.

Tentar novamente a publicação quando o Security Hub não estiver disponível

Se o Security Hub não estiver disponível, o Macie cria uma fila de descobertas que não foram recebidas pelo Security Hub. Quando o sistema é restaurado, Macie tenta publicar novamente até que as descobertas sejam recebidas pelo Security Hub.

Atualizar as descobertas do existentes no Security Hub

Depois que Macie publica uma descoberta de política no Security Hub, Macie atualiza a descoberta para refletir quaisquer ocorrências adicionais da descoberta ou atividade de descoberta. O Macie faz isso apenas para descobertas de políticas. Diferentemente das descobertas de políticas, todas as descobertas de dados confidenciais são tratadas como novas (únicas).

Quando o Macie publica uma atualização em uma descoberta de política, o Macie atualiza o valor do campo Atualizado em (`UpdatedAt`) da descoberta. Você pode usar esse valor para determinar quando o Macie detectou mais recentemente uma ocorrência subsequente da possível violação de política ou problema que produziu a descoberta.

O Macie também pode atualizar o valor do campo Tipos (`Types`) de uma descoberta se o valor existente do campo não for um Tipo de descoberta ASFF. Isso depende se você agiu de acordo com a descoberta no Security Hub. Se você não agiu de acordo com a descoberta, Macie altera o valor do campo para o tipo de descoberta ASFF apropriado. Se você agiu de acordo com a descoberta, usando o console AWS Security Hub ou a operação BatchUpdateFindings da API do AWS Security Hub, o Macie não altera o valor do campo.

Exemplos de descobertas do Amazon Macie em AWS Security Hub

Quando o Amazon Macie publica descobertas no AWS Security Hub, ele usa o AWS Security Finding Format (ASFF). Esse é o formato padrão para todas as descobertas no Security Hub. Os exemplos a seguir usam exemplos de dados para demonstrar a estrutura e a natureza dos dados de descobertas que o Macie publica no Security Hub nesse formato:

- Exemplo de uma descoberta de dados confidenciais
- Exemplo de uma descoberta de política

Exemplo de uma descoberta de dados confidenciais no Security Hub

Aqui está um exemplo de uma descoberta de dados confidenciais que Macie publicou no Security Hub usando o 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"
```

```
}
```

Exemplo de uma descoberta de política no Security Hub

Aqui está um exemplo de uma descoberta de política que o Macie publicou no Security Hub usando o 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
}
```

Habilitar e configurar a integração do AWS Security Hub

Para integrar o Amazon Macie comAWS Security Hub, habilite o Security Hub para seu. Conta da AWS Para saber como, consulte Habilitando o Security Hub no Guia AWS Security Hub do Usuário.

Ao habilitar tanto o Macie quanto o Security Hub, a integração é habilitada automaticamente. Por padrão, o Macie começa a publicar automaticamente descobertas de políticas novas e atualizadas no Security Hub. Você não precisa realizar etapas adicionais para configurar a integração. Se você tiver descobertas de políticas existentes quando a integração estiver habilitada, o Macie não as publicará no Security Hub. Em vez disso, o Macie publica somente as descobertas de políticas que ele cria ou atualiza após a ativação da integração.

Opcionalmente, você pode personalizar sua configuração escolhendo a frequência com que o Macie publica atualizações das descobertas de políticas no Security Hub. Você também pode optar por publicar descobertas de dados confidenciais no Security Hub. Para saber como, consulte Como definir as configurações de publicação para as descobertas.

Interrompendo a publicação de descobertas para AWS Security Hub

Para parar de publicar as descobertas no AWS Security Hub, você pode alterar as configurações de publicação da sua conta do Amazon Macie. Para saber como, consulte Como escolher destinos de publicação para descobertas. Você também pode fazer isso usando o console do Security Hub ou a API do Security Hub. Para saber como, consulte Desabilitar e habilitar o fluxo de descobertas de uma integração (console) ou Desabilitar o fluxo de descobertas de uma integração (API do Security Hub, AWS CLI) no Guia do usuário do AWS Security Hub.

Integração do Amazon Macie com as Notificações de Usuários da AWS

Notificações de Usuários da AWS é um serviço que atua como um local central para suas AWS notificações na AWS Management Console. Isso inclui notificações como alarmes do Amazon

CloudWatch, casos AWS Support e comunicações de outras Serviços da AWS. Com as notificações do usuário, você pode configurar regras personalizadas e canais de entrega para receber notificações sobre determinados tipos de eventos do Amazon EventBridge. Os canais de entrega incluem e-mail, notificações por chat AWS Chatbot e notificações por push AWS Console Mobile Application. Você também pode revisar as notificações no console de notificações de usuários da AWS. Para saber mais sobre notificações de usuários, consulte o Guia do usuário de Notificações de Usuários da AWS.

O Macie se integra às Notificações de Usuários da AWS, o que significa que você pode configurar notificações de usuário para notificá-lo sobre eventos que o Macie publica no EventBridge para descobertas de políticas e dados confidenciais. Se um evento de descoberta corresponder aos critérios que você especificou, as Notificações do Usuário gerarão uma notificação. A notificação inclui detalhes importantes da descoberta associada, como o tipo e a gravidade da descoberta e o nome do recurso afetado. As notificações do usuário também podem enviar a notificação para um ou mais canais de entrega que você especificar. Você pode personalizar sua escolha de canais de entrega para se alinhar aos seus fluxos de trabalho de segurança e conformidade.

Por exemplo, você pode configurar as notificações do usuário para gerar notificações para tipos específicos de descobertas novas e de alta gravidade. Você também pode especificar AWS Chatbot como um canal de entrega para essas notificações. As Notificações de Usuário, então, detectam eventos do EventBridge para as descobertas, geram notificações que incluem dados das descobertas e enviam as notificações para AWS Chatbot. AWS Chatbot pode, então, encaminhar as notificações para um canal do Slack ou uma sala de bate-papo do Amazon Chime para notificar sua equipe de resposta a incidentes.

Tópicos

- Como trabalhar com Notificações de Usuários da AWS
- Habilitar e configurar Notificações de Usuários da AWS para descobertas do Amazon Macie
- Mapeando campos de Notificações de Usuários da AWS para campos de localização do Amazon Macie
- Alterar as configurações de notificações de usuários da AWS para as descobertas do Amazon Macie
- Alterar as configurações de notificações de usuários da AWS para as descobertas do Amazon Macie

Como trabalhar com Notificações de Usuários da AWS

Com o Notificações de Usuários da AWS, você cria regras para especificar os tipos de eventos do Amazon EventBridge que você deseja monitorar e receber notificações. Uma regra define os critérios que um evento do EventBridge deve corresponder para gerar uma notificação. Você também pode escolher um ou mais canais de entrega para uma regra. Os canais de entrega especificam onde você deseja receber notificações de eventos que correspondam aos critérios de uma regra.

Se as Notificações de Usuário detectarem um evento do EventBridge que corresponda aos critérios de uma regra, executarão as seguintes tarefas gerais:

1. Extrair um subconjunto de dados do evento.
2. Gerar uma notificação que contém os dados extraídos.
3. Enviar a notificação para os canais de entrega que você especifica para esse tipo de evento.

O design e a estrutura da notificação são otimizados para cada canal de entrega para o qual ela é enviada.

Para controlar a frequência ou o número de notificações que você recebe, você pode definir as configurações de agregação para uma regra. Se você habilitar essas configurações, as Notificações de Usuário combinarão dados de vários eventos em uma única notificação. Você pode optar por enviar notificações agregadas de eventos com rapidez e frequência, o que talvez você queira fazer para encontrar eventos de alta severidade. Ou envie-as com menos frequência para receber menos notificações, o que talvez você queira fazer para eventos de descoberta de baixa gravidade. Se você combinar dados de eventos, poderá detalhar para analisar os detalhes de cada evento agregado usando o console de Notificações de Usuários da AWS. A partir daí, você também pode navegar até cada descoberta associada no console do Amazon Macie.

Habilitar e configurar Notificações de Usuários da AWS para descobertas do Amazon Macie

Para permitir que Notificações de Usuários da AWS gere notificações para as descobertas do Amazon Macie, crie uma configuração de notificação para o Macie em Notificações de Usuários. Uma configuração de notificação especifica os critérios para uma regra. Também especifica canais de entrega e outras configurações para monitorar e enviar notificações sobre eventos do Amazon EventBridge que correspondam aos critérios da regra. Para obter informações detalhadas sobre

a criação de uma configuração de notificação, consulte Introdução às Notificações de Usuários da AWS no Guia do usuário de Notificações de Usuários da AWS.

Para criar uma configuração de notificação para as descobertas do Macie, selecione as seguintes opções para a regra do evento:

- Para AWS service (Serviço da AWS)Nome, selecione Macie.
- Em Tipo de evento, selecione Descoberta Macie .
- Para Regiões, selecione cada uma Região da AWS em que você usa o Macie e deseja ser notificado sobre as descobertas.

Com essa configuração, as Notificações de Usuários monitoram os eventos do EventBridge para seu Conta da AWS e geram notificações para todos os eventos que o Macie encontra nas regiões que você selecionou. Os eventos atendem aos seguintes critérios:

- `source` igual a `aws.macie`
- `detail-type` igual a `Macie Finding`

O padrão JSON subjacente para a regra do evento é:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

Para refinar a regra e gerar notificações somente para um subconjunto de descobertas, você pode personalizar o padrão JSON para a regra. Para fazer isso, especifique critérios adicionais que derivam do esquema de eventos do EventBridge para as descobertas do Macie.

Se você criar uma regra que usa um padrão JSON personalizado, poderá criar várias configurações de notificação para as descobertas do Macie. Em seguida, você pode personalizar os canais de entrega e outras configurações de cada configuração para se alinharem aos seus fluxos de trabalho de segurança e conformidade para tipos específicos de descobertas.

Por exemplo, você pode criar uma regra que o notifique se o Macie gerar ou atualizar uma Policy:IAMUser/S3BucketPublicdescoberta. Nesse caso, o padrão da regra pode ser:

```
{
```

```
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

E você pode criar outra regra que o notifique se o Macie gerar uma descoberta de dados confidenciais para um bucket do S3 que esteja acessível ao público. Nesse caso, o padrão da regra pode ser:

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Se você criar várias configurações de notificação para as descobertas do Macie, é uma boa ideia garantir que a regra para cada configuração seja exclusiva. Caso contrário, você poderá receber notificações duplicadas para descobertas individuais.

Para saber mais sobre a personalização de padrões de eventos para regras, consulte Como usar padrões de eventos JSON personalizados no Guia do usuário de Notificações de Usuários da AWS.

Mapeando campos de Notificações de Usuários da AWS para campos de localização do Amazon Macie

Quando Notificações de Usuários da AWS - AWS User Notifications - gera uma notificação para uma descoberta do Amazon Macie, ele preenche a notificação com dados de um subconjunto de campos no evento correspondente do Amazon EventBridge. Esses campos oferecem detalhes importantes da descoberta associada, como o tipo e a gravidade da descoberta e o nome do recurso afetado.

Se você analisar uma notificação no console de Notificações de Usuários da AWS, a notificação incluirá todos os dados desse subconjunto de campos. Ela também fornece um link para a descoberta associada no console do Amazon Macie. Se você analisar uma notificação em outros

canais de entrega, ela poderá conter dados de apenas alguns dos campos. Isso ocorre porque as Notificações de Usuários adaptam o design e a estrutura de suas notificações para funcionar com cada tipo de canal de entrega suportado.

A tabela a seguir lista os campos que podem ser incluídos em uma notificação para uma descoberta. Na tabela, a coluna Campo de notificação descreve (em itálico) ou indica o nome de um campo em uma notificação. A coluna do campo evento de descoberta usa notação de ponto para indicar o nome do campo JSON correspondente em um evento do EventBridge para uma descoberta. A coluna Descrição descreve os dados armazenados no campo.

Campo de notificação	Campo evento de descoberta	Descrição
Título da mensagem	`detail.type`	O tipo de descoberta Por exemplo: `Policy:IAMUser/S3BucketPublic` ou `Sensitive Data:S3Object/Financial` .
Resumo	`detail.title`	Uma breve descrição da descoberta Por exemplo: `The S3 object contains financial information.`
Descrição	`detail.description`	Descrição completa da descoberta. Por exemplo: `The S3 object contains financial information such as bank account numbers or credit card numbers.`

Campo de notificação	Campo evento de descoberta	Descrição
Gravidade	`detail.severity.description`	A representação qualitativa da gravidade do achado: `Low`, `Medium` ou `High`.
ID da descoberta	`detail.id`	O identificador exclusivo da descoberta.
Criado	`detail.createdAt`	A data e a hora em que Macie criou a descoberta.
Atualizado	`detail.updatedAt`	A data e a hora em que Macie atualizou a descoberta mais recentemente. Para descobertas de dados confidenciais, esse valor é igual ao valor do campo Criado (`detail.createdAt`). Todas as descobertas de dados sigilosos são consideradas novas (únicas).
Bucket do S3 afetado	`detail.resourcesAffected.s3Bucket.arn`	O Nome do recurso da Amazon (ARN) do bucket do S3.
Objeto do S3 afetado	`detail.resourcesAffected.s3Object.path`	O nome (chave) do objeto S3 afetado, incluindo o nome do bucket que armazena o objeto e, se aplicável, o prefixo do objeto. Esse campo não está incluído nas notificações de descobertas de políticas.

Campo de notificação	Campo evento de descoberta	Descrição

Detecção de dados confidenciais	`detail.classificationDetails.result.sensitiveData.detections...`
	
	E/Ou
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		Essa é uma concatenação de vários campos em um evento para uma descoberta de dados confidenciais. Esse campo não está incluído nas notificações de descobertas de políticas.
		
		Se um identificador de dados gerenciados detectou os dados confidenciais, esse campo especifica a categoria, o tipo e o número (`count`) das ocorrências dos dados confidenciais que foram detectados. Por exemplo: `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences .`
		
		Se um identificador de dados personalizado detectou os dados confidenciais, esse campo especifica o nome do identificador de dados personalizado e o número (`count`) de ocorrências dos dados confidenciais que foram detectados. Por exemplo: `Employee ID 20 occurrences .`
		
		Se uma descoberta relatar vários tipos de dados

Campo de notificação	Campo evento de descoberta	Descrição
		confidenciais, a notificação incluirá dados de até quatro tipos. Os dados são preenchid os primeiro por qualquer identificador de dados personalizado aplicável e, em seguida, por qualquer identific ador de dados gerenciado aplicável.

Alterar as configurações de notificações de usuários da AWS para as descobertas do Amazon Macie

Você pode alterar suas configurações de notificações de usuário da AWS para as descobertas do Amazon Macie quando quiser. Para fazer isso, edite a configuração da notificação em Notificações do usuário. Para saber como, consulte Gerenciamento de configurações de notificação no Guia do usuário de Notificações de Usuários da AWS.

Se você tiver várias configurações de notificação para as descobertas do Macie, alterar as configurações de uma configuração não afetará as configurações das outras configurações. Você pode editar todas ou apenas algumas de suas configurações.

Alterar as configurações de notificações de usuários da AWS para as descobertas do Amazon Macie

Para permitir que Notificações de Usuários da AWS gere notificações para as descobertas do Amazon Macie, crie uma configuração de notificação para o Macie em Notificações de Usuários. Para saber como, consulte Gerenciamento de configurações de notificação no Guia do usuário de Notificações de Usuários da AWS.

Se você tiver várias configurações de notificação para as descobertas do Macie, alterar as configurações de uma configuração não afetará as configurações das outras configurações. Você pode editar todas ou apenas algumas de suas configurações.

Esquema de eventos do Amazon EventBridge para descobertas do Amazon Macie

Para dar um suporte maior à integração com outros aplicativos, serviços e sistemas, como sistemas de monitoramento ou de gerenciamento de eventos, o Amazon Macie publica automaticamente as descobertas no Amazon EventBridge como eventos. O EventBridge, antigo Amazon CloudWatch Events, é um serviço de barramento de eventos sem servidor que fornece um fluxo de dados em tempo real de aplicativos e outros Serviços da AWS para destinos como perfis AWS Lambda, tópicos do Amazon Simple Notification Service e streams do Amazon Kinesis. Para saber mais sobre o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

> **Note**
>
> Se você já usa o CloudWatch Events, observe que o EventBridge e o CloudWatch Events são o mesmo serviço subjacente e API. No entanto, o EventBridge inclui recursos adicionais que permitem que você receba eventos de aplicações de software como serviço (SaaS) e de suas próprias aplicações. Como o serviço subjacente e a API são os mesmos, o esquema de eventos das descobertas do Macie também é o mesmo.

O Macie publica automaticamente eventos para todas as novas descobertas e ocorrências subsequentes às descobertas de políticas existentes, com exceção das descobertas arquivadas automaticamente por uma regra de supressão. Os eventos são objetos JSON que estão em conformidade com o esquema do EventBridge para eventos da AWS. Cada evento contém uma representação em JSON de uma descoberta específica. Como os dados são estruturados como um evento do EventBridge, você pode monitorar, processar e atuar mais facilmente em uma descoberta usando outras aplicações, serviços e ferramentas. Para obter detalhes sobre como e quando o Macie publica os eventos para descobertas, consulte Como definir as configurações de publicação para as descobertas.

Tópicos

Esquema de eventos

O exemplo a seguir mostra o esquema de um evento do Amazon EventBridge para uma descoberta do Amazon Macie. Para obter descrições detalhadas dos campos que podem ser incluídos em um evento de descoberta, consulte Descobertas na Referência de API do Amazon Macie. A estrutura e os campos de um evento de descoberta são mapeados de maneira próxima ao objeto Descoberta da API do Amazon Macie.

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "Conta da AWS ID (string)",
    "time": "event timestamp (string)",
    "region": "Região da 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
}
```

Exemplo de evento para uma descoberta de política

O exemplo a seguir usa dados de amostra para demonstrar a estrutura e a natureza dos objetos e campos em um evento do Amazon EventBridge para uma descoberta de política.

Neste exemplo, o evento relata uma ocorrência subsequente a uma descoberta de política existente: as configurações de bloqueio de acesso público foram desabilitadas para um bucket do S3. Os campos e valores a seguir podem ajudá-lo a determinar se esse é o caso:

- O campo `type` está definido como `Policy:IAMUser/S3BlockPublicAccessDisabled`.
- Os valores dos campos `createdAt` e `updatedAt` têm valores diferentes. Esse é um indicador de que o evento relata uma ocorrência subsequente a uma descoberta de política existente. Os valores desses campos seriam os mesmos se o evento relatasse uma nova descoberta.

- O campo `count` está definido como 2, o que indica que essa é a segunda ocorrência da descoberta.
- O campo `category` está definido como `POLICY`.
- O valor do campo `classificationDetails` é `null`, o que ajuda a diferenciar esse evento para uma descoberta de política de um evento de uma descoberta de dados confidenciais. Para uma descoberta de dados confidenciais, esse valor seria um conjunto de objetos e campos que fornecem informações sobre como e quais dados confidenciais foram encontrados.

Observe também que o valor do campo `sample` é `true`. Esse valor enfatiza que esse é um exemplo de evento para uso na documentação.

```
{
    "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
    }
}
```

Exemplo de evento para uma descoberta de dados confidenciais

O exemplo a seguir usa dados de amostra para demonstrar a estrutura e a natureza dos objetos e campos em um evento do Amazon EventBridge para uma descoberta de política.

Neste exemplo, o evento relata uma nova descoberta de dados confidenciais: o Amazon Macie encontrou mais de uma categoria de dados confidenciais em um objeto do S3. Os campos e valores a seguir podem ajudá-lo a determinar se esse é o caso:

- O campo `type` está definido como `SensitiveData:S3Object/Multiple`.
- Os campos `createdAt` e `updatedAt` têm os mesmos valores. Ao contrário das descobertas de políticas, esse é sempre o caso das descobertas de dados confidenciais. Todas as descobertas de dados confidenciais são consideradas novas.
- O campo `count` está definido como `1`, o que indica que essa é uma nova descoberta. Ao contrário das descobertas de políticas, esse é sempre o caso das descobertas de dados confidenciais. Todas as descobertas de dados confidenciais são consideradas novas.
- O campo `category` está definido como `CLASSIFICATION`.
- O valor do campo `policyDetails` é `null`, o que ajuda a diferenciar esse evento de descoberta de dados confidenciais de um evento de descoberta de política. Para uma descoberta de política, esse valor seria um conjunto de objetos e campos que fornecem informações sobre uma possível violação de política ou problema com a segurança ou a privacidade de um bucket do S3.

Observe também que o valor do campo `sample` é `true`. Esse valor enfatiza que esse é um exemplo de evento para uso na documentação.

```
{
    "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
    }
}
```

Previsão e monitoramento dos custos do Amazon Macie

Para ajudá-lo a prever e monitorar seus custos de uso do Amazon Macie, o Macie calcula e fornece custos de uso estimados para sua conta. Com esses dados, você pode determinar se pretende ajustar o uso do serviço ou as cotas da conta. Se você está participando atualmente de um teste gratuito de 30 dias do Macie, você pode usar esses dados para estimar seus custos de uso do Macie após o término do teste gratuito. Você também pode conferir o status do teste.

Você pode analisar seus custos de uso estimados no console do Amazon Macie e acessá-los programaticamente com a API do Amazon Macie. Se você for o administrador do Macie de uma organização, poderá analisar e acessar os dados agregados da sua organização e os detalhamentos dos dados das contas da sua organização.

Além dos custos de uso estimados que o Macie fornece, você pode analisar e monitorar seus custos reais usandoAWS Billing and Cost Management. AWS Billing and Cost Managementfornece recursos projetados para ajudá-lo a rastrear e analisar seus custos de Serviços da AWS e gerenciar orçamentos para sua conta ou organização. Ele também fornece atributos que podem ajudar você a prever os custos de uso com base em dados históricos. Para saber mais, consulte o Manual do usuário do AWS Billing.

Tópicos

- Entender como os custos de uso estimados são calculados para o Amazon Macie
- Analisar os custos estimados de uso do Amazon Macie
- Participar do teste gratuito do Amazon Macie

Entender como os custos de uso estimados são calculados para o Amazon Macie

Os preços do Amazon Macie são baseados nas seguintes dimensões.

Monitoramento de controle preventivo

> Esses custos são derivados da manutenção do inventário de buckets do Amazon Simple Storage Service (Amazon S3), e da avaliação e monitoramento dos buckets em relação à segurança e ao controle de acesso. Para obter mais informações, consulte Como o Macie monitora a segurança de dados do Amazon S3.

Você é cobrado com base no número total de buckets do S3 que o Macie monitora em sua conta. As cobranças são rateadas por dia.

Monitoramento de objetos para descoberta automatizada de dados confidenciais

Esses custos derivam do monitoramento e da avaliação do inventário de buckets do S3 para identificar objetos do S3 que são qualificados para análise por meio da descoberta automatizada de dados confidenciais. Para obter mais informações, consulte Como funciona a descoberta automatizada de dados confidenciais.

Você é cobrado com base no número total de objetos do S3 que o Macie monitora em sua conta. As cobranças são rateadas por dia.

Análise de objetos por trabalhos de descoberta de dados confidenciais e descoberta automatizada de dados confidenciais

Esses custos derivam da análise de objetos do S3 e do relatório de dados confidenciais que Macie encontra nos objetos. Isso inclui análises e relatórios por trabalhos de descoberta de dados confidenciais e por descoberta automatizada de dados confidenciais.

Você é cobrado com base na quantidade de dados não compactados que o Macie analisa nos objetos do S3. Não há cobrança por objetos que o Macie não possa analisar por motivos como uso de uma classe de armazenamento Amazon S3 não suportada, uso de um formato de arquivo ou armazenamento não suportado ou configurações de permissões. Para obter mais informações, consulte Descobrir dados confidenciais. Além disso, esses custos não variam com base no número de descobertas de dados confidenciais produzidas por seus trabalhos ou pela descoberta automatizada de dados confidenciais.

Para gerenciar os custos da descoberta automatizada de dados confidenciais, você pode excluir buckets individuais do S3 das análises. Por exemplo, você pode excluir buckets que são conhecidos por atenderem aos requisitos de segurança e conformidade da sua organização. Para excluir buckets, você pode atualizar as definições de configuração da sua conta. Você também pode excluir buckets caso a caso enquanto analisa os detalhes de buckets individuais em seu inventário de buckets.

Os custos de trabalhos de descoberta de dados confidenciais são restritos pela cota mensal de descoberta de dados confidenciais de sua conta. (A cota padrão é de 5 TB de dados.) Se um trabalho estiver em execução e a análise dos objetos qualificados atingir essa cota, o Macie pausa automaticamente o trabalho até o início do próximo mês civil (e a cota mensal seja redefinida para sua conta) ou você aumenta a cota da sua conta.

Se você for o administrador do Macie de uma organização, os custos dos trabalhos de descoberta de dados confidenciais são restritos pela cota mensal de descoberta de dados confidenciais de cada conta para a qual você analisa dados. A cota de uma conta de membro define a quantidade máxima de dados que suas vagas e as vagas da conta de membro podem analisar para a conta durante um mês civil. Se um trabalho estiver em execução e a análise de objetos qualificados atingir essa cota para uma conta de membro, o Macie interrompe a análise de objetos pertencentes à conta. Quando o Macie acaba de analisar os objetos de todas as outras contas que não atingiram a cota, o Macie pausa automaticamente o trabalho. Se for um trabalho único, o Macie retomará automaticamente o trabalho quando o mês seguinte começar ou a cota mensal de descoberta de dados sigilosos for aumentada para todas as contas afetadas, o que ocorrer primeiro. Se for um trabalho periódico, o Macie retoma automaticamente o trabalho quando a próxima execução estiver programada para começar ou o próximo mês civil começar, o que ocorrer primeiro. Se uma execução programada começar antes do início do próximo mês civil ou se a cota for aumentada para uma conta afetada, o Macie não analisará objetos pertencentes à conta.

> **Tip**
>
> Para obter dicas úteis sobre como gerenciar ou reduzir os custos de descoberta de dados confidenciais, consulte a postagem do blog Como usar o Amazon Macie para reduzir o custo da descoberta de dados confidenciais no AWS blog de segurança.

Para obter informações detalhadas e exemplos de custos de uso, consulte os preços do Amazon Macie.

Ao usar o Macie para analisar seus custos de uso estimados, é importante entender como as estimativas de custo são calculadas. Considere o seguinte:

- As estimativas são relatadas em dólares americanos e são Região da AWS apenas para o momento. Se você usa o Macie em várias regiões, os dados não são agregados para todas as regiões nas quais você usa o Macie.
- No console, as estimativas são inclusivas para o mês atual do calendário até o momento. Se você consultar os dados programaticamente com a API do Amazon Macie, poderá escolher um intervalo de tempo inclusivo para as estimativas. Isso pode ser um intervalo de tempo contínuo dos 30 dias anteriores ou do mês atual até o momento.

- As estimativas não refletem todos os descontos que podem ser aplicados à sua conta. A exceção são os descontos que derivam dos níveis regionais de preços por volume, conforme descrito nos preços do Amazon Macie. Se sua conta se qualificar para esse tipo de desconto, as estimativas refletem esse desconto.
- Se você for o administrador do Macie de uma organização, as estimativas não refletem os descontos combinados por volume de uso da sua organização. Para obter informações sobre esses descontos, consulte Descontos por volume no Guia AWS Billing do usuário.
- Para o monitoramento preventivo de controles, a estimativa é baseada no custo médio diário para o intervalo de tempo aplicável. O custo é rateado por dia.
- Para a descoberta automatizada de dados confidenciais, a estimativa geral é baseada no custo médio diário do monitoramento de objetos (proporcional por dia) e na quantidade de dados não compactados que Macie analisou até agora durante o intervalo de tempo aplicável. Se você é o administrador do Macie de uma organização e analisa os dados de uma conta de membro, os custos estimados dessas atividades são incluídos nas estimativas de cada conta aplicável.
- Para trabalhos de descoberta de dados confidenciais, a estimativa é baseada na quantidade de dados não compactados que seus trabalhos analisaram até agora durante o intervalo de tempo aplicável. Se você é o administrador do Macie de uma organização e executa trabalhos que analisam dados de uma conta de membro, o custo estimado desses trabalhos é incluído na estimativa da conta de membro aplicável.
- Se sua conta for uma conta membro de uma organização e seu administrador do Macie realizar a descoberta automatizada de dados confidenciais ou executar trabalhos de descoberta de dados confidenciais que analisam seus dados, os custos estimados dessas atividades serão incluídos nas estimativas de sua conta.
- As estimativas não incluem os custos incorridos pelo uso de outros Serviços da AWS com determinados recursos do Macie. Por exemplo, usar o Customer Managed AWS KMS keys para descriptografar objetos do S3 que você deseja inspecionar em busca de dados confidenciais.

Observe também que o Macie fornece um nível gratuito mensal para análise de objetos do S3 por meio de trabalhos de descoberta de dados confidenciais e descoberta automatizada de dados confidenciais. Todo mês, não há cobrança para analisar até 1 GB de dados para descobrir e relatar dados confidenciais em objetos do S3. Se mais de 1 GB de dados forem analisados durante um determinado mês, as cobranças de descoberta de dados confidenciais começarão a ser acumuladas em sua conta após os primeiros 1 GB de dados. Se menos de 1 GB de dados for analisado em um mês, a alocação restante não será transferida para o próximo mês. Se sua conta fizer parte de uma organização com faturamento consolidado, o nível gratuito se aplica à quantidade combinada de

dados analisados para sua organização. Em outras palavras, não há cobrança para analisar até 1 GB de dados por mês para todas as contas da sua organização.

Analisar os custos estimados de uso do Amazon Macie

Para analisar seus custos atuais estimados de uso do Amazon Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Tanto o console quanto a API fornecem custos estimados para as dimensões de preços do Macie. Se você está participando atualmente de um teste gratuito de 30 dias, você pode usar esses dados para estimar seus custos de uso do Macie após o término do teste gratuito. Para obter informações sobre as dimensões e considerações de preços do Macie, consulte. Entender como os custos de uso estimados são calculados Para obter informações detalhadas e exemplos de custos de uso, consulte os preços do Amazon Macie.

No Macie, os custos de uso estimados são relatados em dólares americanos e se aplicam somente aos atuaisRegião da AWS. Se você usar o console para analisar os dados, as estimativas de custo são para o mês atual do calendário até o momento (inclusive). Se você consultar os dados programaticamente com a API do Amazon Macie, poderá especificar um intervalo de tempo inclusivo para as estimativas, seja um período contínuo dos 30 dias anteriores ou o atual mês do calendário até o momento.

Tópicos

- Analisar os custos de uso estimados no console do Amazon Macie
- Consultar os custos de uso estimados com a API do Amazon Macie

Analisar os custos de uso estimados no console do Amazon Macie

No console do Amazon Macie, as estimativas de custo são organizadas da seguinte forma:

- Monitoramento de controle preventivo — Esse é o custo estimado de manter seu inventário de buckets do Amazon Simple Storage Service (Amazon S3) e avaliar e monitorar os buckets para segurança e controle de acesso.
- Trabalhos de descoberta de dados confidenciais — Esse é o custo estimado dos trabalhos de descoberta de dados confidenciais que você executou.
- Descoberta automatizada de dados confidenciais — Esses são os custos estimados de realizar a descoberta automatizada de dados confidenciais. Isso inclui monitorar e avaliar seu inventário de buckets do S3 para identificar objetos do S3 que são qualificados para análise. Também inclui

analisar objetos qualificados e relatar dados confidenciais, estatísticas, descobertas e outros tipos de resultados.

Siga estas etapas para analisar seus custos de uso estimados usando o console do Amazon Macie.

Para analisar seus custos estimados de uso no console

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja rever seus custos estimados.
3. No painel de navegação, escolha Uso.

Se você tiver uma conta autônoma do Macie ou se sua conta for uma conta membro de uma organização, a página Uso exibirá um detalhamento dos custos de uso estimados da sua conta.

Se você for o administrador do Macie de uma organização, a página Uso lista as contas em sua organização:

- Na tabela, o campo Total indica o custo total estimado para cada conta.
- A seção Custos estimados mostra o custo total estimado para sua organização e um detalhamento desses custos.

Para analisar o detalhamento dos custos estimados para uma conta específica da organização, escolha a conta na tabela. Em seguida, a seção Custos estimados mostra esse detalhamento. Para mostrar esses dados para outra conta, escolha a conta na tabela. Para limpar a seleção de conta, escolha X ao lado do ID da conta.

Consultar os custos de uso estimados com a API do Amazon Macie

Para consultar programaticamente seus custos de uso estimados, você pode usar as seguintes operações da API do Amazon Macie:

- GetUsageTotals— Essa operação retorna os custos totais estimados de uso da sua conta, agrupados por métrica de uso. Se você for o administrador do Macie de uma organização, essa operação retornará estimativas de custo agregadas para todas as contas da sua organização. Para saber mais sobre essa operação, consulte Totais de uso na Referência de API do Amazon Macie.

- GetUsageStatistics— Essa operação retorna estatísticas de uso e dados relacionados à sua conta, agrupados por conta e, em seguida, por métrica de uso. Os dados incluem os custos totais de uso estimados e as cotas da conta corrente. Conforme aplicável, também indica quando seu teste gratuito de 30 dias começou para o Macie e para a descoberta automatizada de dados confidenciais. Se você for o administrador do Macie de uma organização, essa operação retornará um detalhamento dos dados de todas as contas da sua organização. Você pode personalizar sua consulta classificando e filtrando os resultados da consulta. Para saber mais sobre essa operação, consulte Estatísticas de uso na Referência de API do Amazon Macie.

Ao usar qualquer operação, você pode, opcionalmente, especificar um intervalo de tempo inclusivo para os dados. Esse intervalo de tempo pode ser um intervalo contínuo dos 30 dias anteriores (`PAST_30_DAYS`) ou do mês do calendário atual até a data (`MONTH_TO_DATE`). Se você não especificar um intervalo de datas, o Macie retornará os dados para os 30 dias corridos anteriores.

Os exemplos a seguir mostram como consultar estatísticas e custos de uso estimados usando o AWS Command Line Interface(AWS CLI). Você também pode consultar os dados usando uma versão atual de outra ferramenta de linha de AWS comando ou de um AWS SDK, ou enviando solicitações HTTPS diretamente para o Macie. Para obter mais informações sobre as ferramentas e SDKs, consulte AWSFerramentas para criar na .AWS

Exemplos

- Exemplo 1: Consultar os custos totais de uso estimados
- Exemplo 2: Consultar estatísticas de uso

Exemplo 1: Consultar os custos totais de uso estimados

Para consultar os custos totais de uso estimados usando oAWS CLI, execute o comando get-usage-totals e, opcionalmente, especifique um intervalo de tempo para os dados. Por exemplo:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Onde *`MONTH_TO_DATE`*especifica o mês atual do calendário até o momento como o intervalo de tempo para os dados.

Se o comando for executado com êxito, você receberá um resultado semelhante a este.

```
{
    "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"
        }
    ]
}
```

Onde `estimatedCost` está o custo total de uso estimado para a métrica de uso associada (`type`):

- `SENSITIVE_DATA_DISCOVERY`, para analisar objetos do S3 com trabalhos de descoberta de dados confidenciais.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, para analisar objetos do S3 com descoberta automatizada de dados confidenciais.
- `DATA_INVENTORY_EVALUATION`, para monitorar e avaliar buckets do S3 em relação à segurança e ao controle de acesso.
- `AUTOMATED_OBJECT_MONITORING`, para avaliar e monitorar seu inventário de buckets do S3 para identificar objetos do S3 que são qualificados para análise por meio da descoberta automatizada de dados confidenciais.

Exemplo 2: Consultar estatísticas de uso

Para consultar estatísticas de uso usando oAWS CLI, execute o comando get-usage-statistics. Opcionalmente, você pode classificar, filtrar e especificar um intervalo de tempo para os resultados

da consulta. O exemplo a seguir recupera estatísticas de uso de uma conta de administrador do Macie nos últimos 30 dias. Os resultados são classificados em ordem crescente por Conta da AWS ID.

Para Linux, macOS ou Unix, use o caractere de continuação de linha com barra invertida (\) para melhorar a legibilidade:

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Para Microsoft Windows, usando o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade:

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

Onde:

- *AccountId* especifica o campo a ser usado para classificar os resultados.
- *ASC* é a ordem de classificação a ser aplicada aos resultados, com base no valor do campo especificado (*AccountId*).
- *PAST_30_DAYS*especifica os 30 dias anteriores como o intervalo de tempo dos dados.

Se o comando for executado com êxito, Macie retornará uma `records` matriz. A matriz contém um objeto para cada conta incluída nos resultados da consulta. Por exemplo:

```
{
    "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"
}
```

Onde `estimatedCost` está o custo total de uso estimado para a métrica de uso associada (`type`) de uma conta:

- `DATA_INVENTORY_EVALUATION`, para monitorar e avaliar buckets do S3 em relação à segurança e ao controle de acesso.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, para analisar objetos do S3 com descoberta automatizada de dados confidenciais.
- `SENSITIVE_DATA_DISCOVERY`, para analisar objetos do S3 com trabalhos de descoberta de dados confidenciais.
- `AUTOMATED_OBJECT_MONITORING`, para avaliar e monitorar o inventário de buckets do S3 da conta para identificar objetos do S3 que são qualificados para análise por meio da descoberta automatizada de dados confidenciais.

Participar do teste gratuito do Amazon Macie

Ao habilitar o Amazon Macie pela primeira vez, sua Conta da AWS será inscrita automaticamente em uma avaliação gratuita de 30 dias do Macie. Isso inclui contas de membros individuais em uma AWS Organizations organização.

Durante o teste gratuito, não há cobrança pelo uso do Macie de forma específica Região da AWS para:

- Realizar monitoramento de controle preventivo — Isso inclui gerar e manter um inventário de seus buckets do Amazon Simple Storage Service (Amazon S3) na região. Isso também inclui avaliar

e monitorar esses buckets em relação à segurança e ao controle de acesso. Para obter mais informações, consulte Como o Macie monitora a segurança de dados do Amazon S3.

- Realize a descoberta automatizada de dados confidenciais — Isso inclui monitorar e avaliar seu inventário de buckets do S3 na região para identificar objetos do S3 que são qualificados para análise. Também inclui analisar objetos qualificados e relatar dados confidenciais, estatísticas, descobertas e outros tipos de resultados. Para obter mais informações, consulte Como funciona a descoberta automatizada de dados confidenciais.

  A descoberta automatizada de dados confidenciais está disponível somente para contas de administrador do Macie e contas autônomas do Macie. Se você tiver uma conta de administrador do Macie, poderá usar esse recurso para analisar objetos nos buckets do S3 pertencentes às suas contas membros.

Para obter uma lista de todas as regiões onde o Macie está disponível no momento, consulte endpoints do Amazon Macie e cotas no Referência geral da AWS.

O teste gratuito dura 30 dias consecutivos. Você não pode pausá-lo depois que ele começa. Após o término do teste gratuito, as cobranças começam a ser acumuladas pela realização do monitoramento preventivo de controles. As cobranças também começam a ser acumuladas pela realização de descobertas automatizadas de dados confidenciais. Se você for o administrador do Macie de uma organização, as cobranças serão acumuladas conforme aplicável para cada conta em sua organização. Você pode usar o Macie para analisar os detalhamentos dos custos estimados de uso de contas individuais em sua organização.

> **Note**
>
> O teste gratuito não inclui a análise de objetos do S3 por trabalhos de descoberta de dados confidenciais. Você incorrerá em cobranças se criar e executar trabalhos de descoberta de dados confidenciais que analisem mais de 1 GB de dados não compactados durante o teste gratuito. (O Macie fornece um nível gratuito mensal para descoberta de dados confidenciais. A cada mês, não há cobrança para analisar até 1 GB de dados não compactados em objetos do S3. Após os primeiros 1 GB de dados, os custos aumentam.) Você também pode incorrer em cobranças por outros Serviços da AWS que você usa com determinados recursos do Macie, por exemplo, usando AWS KMS keys gerenciados pelo cliente para descriptografar objetos do S3 que você deseja inspecionar em busca de dados confidenciais.

Para verificar seu status e os custos estimados durante o teste gratuito

Durante o teste gratuito, você pode verificar o status do teste e analisar os custos estimados de uso da sua conta. As estimativas de custo são baseadas no uso do Macie até o momento durante o teste gratuito. Eles podem ajudar você a entender quais podem ser alguns dos seus custos de uso após o término do teste. Para obter detalhes sobre como o Macie calcula esses valores, consulte. Entender como os custos de uso estimados são calculados

Siga estas etapas para verificar o status do seu teste e analisar seus custos de uso estimados no console do Amazon Macie. Você também pode acessar esses dados programaticamente usando a operação GetUsageStatistics da API do Amazon Macie.

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região da na qual você quer conferir o status do teste gratuito e os custos estimados de uso.
3. No painel de navegação, escolha Uso.

A página Uso indica o número de dias restantes em seu teste gratuito. Também mostra um detalhamento de seus custos de uso estimados em dólares americanos:

- Monitoramento de controle preventivo — Esse é o custo total projetado para manter seu inventário de buckets de S3 e avaliar e monitorar os buckets para segurança e controle de acesso após o término do teste gratuito.
- Trabalhos de descoberta de dados confidenciais — Esse é o custo total estimado de todos os trabalhos de descoberta de dados confidenciais que você executou. Trabalhos confidenciais de descoberta de dados não estão incluídos no teste gratuito.
- Descoberta automatizada de dados confidenciais — Esses são os custos totais projetados para realizar a descoberta automatizada de dados confidenciais após o término do teste gratuito, divididos por dimensão de preço — monitoramento de objetos e análise de objetos.

Se você for o administrador do Macie de uma organização, a página Uso fornece detalhes sobre as contas do Macie em sua organização:

- Na tabela, os campos de Avaliação gratuita indicam se uma conta está atualmente participando da avaliação gratuita para monitoramento preventivo de controles ou descoberta automatizada de dados confidenciais. Um campo Avaliação gratuita estará vazio se a avaliação gratuita aplicável tiver terminado para uma conta. O campo Total indica o custo total estimado para cada conta.

- A seção Custos estimados mostra os custos estimados da organização em geral.

Para analisar o detalhamento dos custos estimados para uma conta específica da organização, escolha a conta na tabela. Em seguida, a seção Custos estimados mostra esse detalhamento. Para mostrar esses dados para outra conta, escolha a conta na tabela. Para limpar a seleção de conta, escolha X ao lado do ID da conta.

> **Note**
>
> Se uma conta armazenar mais de 150 TB de dados no Amazon S3, os custos estimados e reais da conta para a descoberta automatizada de dados confidenciais podem ser maiores do que as projeções de custo que a Macie fornece durante o teste gratuito de 30 dias. Isso ocorre porque a análise de objetos pela descoberta automatizada de dados confidenciais é pausada quando 150 GB de dados não compactados são analisados para uma conta que está inscrita na avaliação gratuita. A análise de objetos da conta é retomada após o término da avaliação gratuita.
>
> Para obter assistência na previsão de custos para uma conta que armazena mais de 150 TB de dados no Amazon S3, entre em contato com AWS Support. Para gerenciar os custos de descobertas automatizadas de dados confidenciais após o término do teste gratuito, você pode excluir buckets de S3 individuais das análises subsequentes. Para excluir buckets, você pode atualizar as definições de configuração da sua conta. Você também pode excluir buckets caso a caso enquanto analisa os detalhes de buckets individuais em seu inventário de buckets.

Como gerenciar várias contas do Amazon Macie

Se o seu ambiente AWS tiver várias contas, você poderá associar as contas do Amazon Macie ao seu ambiente e gerenciá-las centralmente como uma organização no Macie. Com essa configuração, um administrador designado do Macie pode avaliar e monitorar a postura geral de segurança do patrimônio de dados do Amazon Simple Storage Service (Amazon S3) da sua organização e descobrir dados sigilosos nos buckets S3 da sua organização. O administrador também pode realizar várias tarefas de gerenciamento e administração de contas em grande escala, como monitorar os custos de uso estimados e avaliar as cotas da conta.

No Macie, uma organização consiste de uma conta de administrador designada do Macie e uma ou mais contas de membros associados. Você pode associar as contas de duas maneiras: integrando o Macie com AWS Organizations ou enviando e aceitando convites de associação do Macie. Recomendamos que você integre o Macie com o AWS Organizations

AWS Organizations é um serviço global de gerenciamento de contas que permite aos administradores de AWS consolidar e gerenciar centralmente várias Contas da AWS. Ele fornece os atributos de faturamento consolidado e gerenciamento de contas, projetados para atender às necessidades orçamentárias, de segurança e de conformidade. É oferecido sem custo adicional e se integra a vários Serviços da AWS, incluindo o Macie, AWS Security Hub e o Amazon GuardDuty. Para saber mais, consulte o Manual do usuário do AWS Organizations.

Se você preferir gerenciar centralmente várias contas do Macie sem usar AWS Organizations, você pode usar convites para membros em vez disso. Se você enviar um convite e ele for aceito por outra conta, a sua conta se tornará a conta de administrador do Macie da outra conta. Se você receber e aceitar um convite, a sua conta se tornará uma conta-membro do Macie e a conta do administrador do Macie poderá acessar e gerenciar determinadas configurações, dados e recursos para a sua conta do Macie.

Tópicos

Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro

Se você gerencia centralmente várias contas do Amazon Macie como uma organização, o administrador do Macie tem acesso aos dados de inventário do Amazon Simple Storage Service (Amazon S3), às descobertas das políticas e a determinadas configurações e recursos do Macie para contas associadas aos membros. O administrador também pode realizar a descoberta automatizada de dados confidenciais e executar trabalhos de descoberta de dados confidenciais para detectar dados confidenciais nos buckets do S3 que as contas dos membros possuem. Support para tarefas específicas varia de acordo com o fato de uma conta de administrador do Macie estar associada a uma conta de membro por meio de AWS Organizations ou por convite.

A tabela a seguir fornece detalhes sobre o relacionamento entre o administrador do Macie e as contas dos membros. Ela indica as permissões padrão para cada tipo de conta. Para restringir ainda mais o acesso aos atributos e operações do Macie, você pode usar AWS Identity and Access Managementpolíticas do IAM personalizadas.

Na tabela:

- Próprio indica que a conta não pode realizar a tarefa em nenhuma conta associada.
- Qualquer indica que a conta não pode realizar a tarefa em nenhuma conta associada.
- Tudo indica que a conta pode realizar a tarefa e a tarefa se aplica a todas as contas associadas.

Um traço (—) indica que a conta não pode realizar a tarefa.

Tarefa	Através AWS Organizations		Por convite	
	Administrador	Membro	Administrador	Membro
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. O administrador de uma organização em AWS Organizations pode revisar todas as contas na organização, incluindo contas que não habilitaram o Macie. O administrador de uma organização baseada em convite pode revisar somente as contas adicionadas ao inventário.

2. Somente um administrador pode suprimir as descobertas de políticas. Se um administrador criar uma regra de supressão, o Macie aplicará a regra às descobertas de políticas de todas as contas na organização, a menos que a regra esteja configurada para excluir contas específicas. Se um membro criar uma regra de supressão, o Macie não a aplica às descobertas da política da conta do membro.

3. Somente a conta que possui um recurso afetado pode publicar as descobertas da política para o recursoAWS Security Hub. Tanto as contas de administrador quanto as de membros publicam automaticamente as descobertas da política de um recurso afetado no Amazon EventBridge.

4. Um membro pode configurar um trabalho para analisar objetos somente nos buckets do S3 que sua conta possui. Um membro pode configurar um trabalho para analisar objetos somente nos buckets do S3 que sua conta possui. Para obter informações sobre como as cotas são aplicadas e os custos são calculados para trabalhos em várias contas, consulte Entender como os custos de uso estimados são calculados.

5. Somente a conta que cria um trabalho pode acessar os detalhes do trabalho. Isso inclui detalhes relacionados ao trabalho no inventário do bucket do S3.

6. Somente a conta que cria um trabalho pode acessar, suprimir ou publicar descobertas de dados confidenciais que o trabalho produz. Somente um administrador pode acessar, suprimir ou publicar descobertas de dados confidenciais que a descoberta automatizada de dados confidenciais produz.

7. Se uma descoberta de dados confidenciais for aplicável a um objeto do S3 de propriedade de uma conta de membro, o administrador poderá recuperar amostras de dados confidenciais relatados pela descoberta. Isso dependerá da origem da descoberta, das configurações e dos recursos na conta do administrador e na conta do membro. Para obter mais informações, consulte Opções de configuração e requisitos para recuperar amostras de dados confidenciais.

8. Para que um administrador suspenda o Macie por sua própria conta, o administrador deve primeiro desassociar sua conta de todas as contas de membros.

9. Para que um administrador desative o Macie para sua própria conta, o administrador deve primeiro desassociar sua conta de todas as contas de membros e excluir as associações entre sua conta e todas essas contas. O administrador de uma organização no AWS Organizations

pode fazer isso trabalhando com a conta de gerenciamento da organização para designar uma conta diferente como a conta de administrador.

Para que um membro de uma organização do AWS Organizations desative o Macie, primeiro o administrador deve desassociar a conta do membro de sua conta de administrador. Em uma organização baseada em convite, o membro pode desassociar sua conta da conta de administrador e, em seguida, desabilitar o Macie.

10. O administrador de uma organização em AWS Organizations pode excluir uma associação com uma conta de membro depois de desassociar a conta de sua conta de administrador. A conta continua aparecendo no inventário da conta do administrador, mas seu status indica que não é uma conta de membro. Em uma organização baseada em convite, o administrador e um membro de uma organização podem excluir uma associação com uma conta de membro depois de desassociar a conta de sua conta de administrador. A outra conta, então, deixa de aparecer no inventário da conta.

Gerenciando contas do Amazon Macie ao AWS Organizations

Se você usa AWS Organizations para gerenciar centralmente várias Contas da AWS, você pode integrar o Amazon Macie com o AWS Organizations, e, em seguida, gerenciar centralmente o Macie para contas em sua organização. Com essa configuração, um administrador designado do Macie pode habilitar e gerenciar o Macie para até dez mil contas. O administrador também pode acessar os dados de inventário do Amazon Simple Storage Service (Amazon S3) e descobrir os dados confidenciais nos buckets do S3 de propriedade da conta. Para obter detalhes sobre as tarefas que o administrador pode realizar, consulte Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Para integrar o Macie ao AWS Organizations, você começa designando uma conta como a conta delegada de administrador do Macie para a organização. O administrador do Macie, então, habilita o Macie para outras contas na organização, adiciona essas contas como contas-membro do Macie e define as configurações e os recursos do Macie para as contas.

> **Tip**
>
> Se você já associou uma conta de administrador do Macie às contas-membro usando convites, você pode designar essa conta como a conta delegada de administrador do Macie para sua organização em AWS Organizations. Se você fizer isso, todas as contas-membro atualmente associadas permanecerão como membros e você poderá aproveitar ao

máximo os benefícios de gerenciar contas usando o AWS Organizations. Para obter mais informações, consulte Transição de uma organização baseada em convites.

Os tópicos desta seção explicam como integrar o Macie ao AWS Organizations e como administrar e gerenciar o Macie para contas em uma organização.

Tópicos

Considerações e recomendações para usar o Amazon Macie com AWS Organizations

Antes de integrar o Amazon Macie AWS Organizations e configurar sua organização no Macie, considere os seguintes requisitos e recomendações. Também certifique-se de entender a relação entre o administrador do Macie e as contas de membros.

Tópicos

Como designar uma conta de administrador do Macie

Ao determinar qual conta deve ser a conta delegada de administrador do Macie para a sua organização, lembre-se do seguinte:

- Uma organização só pode ter uma conta de administrador do Macie delegada.

- Uma conta não pode ser uma conta de administrador do Macie e uma conta-membro ao mesmo tempo.
- Somente a conta AWS Organizations de gerenciamento de uma organização pode designar a conta de administrador delegada do Macie para a organização, e somente a conta de gerenciamento pode posteriormente alterar ou remover essa designação.
- A conta AWS Organizations de gerenciamento de uma organização também pode ser a conta delegada de administrador do Macie para a organização. No entanto, não recomendamos essa configuração com base nas melhores práticas AWS de segurança e no princípio do privilégio mínimo. Os usuários que têm acesso à conta de gerenciamento para fins de cobrança provavelmente são diferentes dos usuários que precisam acessar o Macie para fins de segurança da informação.

  Se preferir essa configuração, você deve habilitar o Macie para a conta de gerenciamento da organização em pelo menos uma Região da AWS antes de designar a conta como a conta delegada de administrador do Macie. Caso contrário, a conta não conseguirá acessar e gerenciar configurações e recursos do Macie para contas de membros.
- Ao contrário AWS Organizations, o Macie é um serviço regional. Isso significa que a designação de uma conta de administrador do Macie é uma designação regional. Isso também significa que as associações entre contas de administrador e de membros do Macie são regionais. Por exemplo, se a conta de gerenciamento designar uma conta de administrador do Macie na região Leste dos EUA (Norte da Virgínia), o administrador do Macie poderá gerenciar o Macie para contas de membros somente nessa região.

  Para gerenciar centralmente contas do Macie em várias Regiões da AWS, a conta de gerenciamento deve entrar em cada região em que a organização atualmente usa ou usará o Macie e, em seguida, designar a conta de administrador do Macie em cada uma dessas regiões. O administrador do Macie pode então configurar a organização em cada uma dessas regiões. Para obter uma lista de todas as regiões onde o está disponível no momento, consulte os endpoints e quotas do Amazon Macie no Referência geral da AWS.
- Uma conta pode ser associada apenas a uma conta de administrador do Macie por vez. Se a sua organização usa o Macie em várias regiões, a conta de administrador designado do Macie deve ser a mesma em todas essas regiões. No entanto, a conta de gerenciamento da sua organização deve designar a conta de administrador separadamente em cada região.
- Uma conta pode ser a conta delegada de administrador do Macie para apenas uma organização por vez. Se você gerencia várias organizações em AWS Organizations, deverá designar uma

conta de administrador do Macie diferente para cada organização. Isso ocorre devido a um AWS Organizations requisito: uma conta só pode ser membro de uma organização por vez.

- Se as contas do administrador do Conta da AWS Macie forem suspensas, isoladas ou fechadas, todas as contas associadas aos membros do Macie serão automaticamente removidas como contas de membros do Macie, mas o Macie não será desativado para as contas.

Como alterar ou remover a designação de uma conta de administrador do Macie

Somente a conta AWS Organizations de gerenciamento de uma organização pode alterar ou remover a designação de uma conta de administrador delegada do Macie para a organização.

Se a conta de gerenciamento remover a designação, todas as contas de membros associadas serão removidas como contas de membros do Macie, mas o Macie não será desativado para as contas. Para que uma conta também pause ou pare de usar o Macie, um usuário da conta deve suspender (pausar) ou desativar (parar) o Macie para a conta.

Como adicionar e remover contas de membros do Macie

Ao adicionar, remover ou gerenciar contas de membros da sua organização, lembre-se do seguinte:

- Uma conta de administrador do Macie pode ser associada a no máximo 10.000 contas de membros ativas (habilitadas) do Macie em cada Região da AWS. Se a sua organização exceder essa cota, o administrador do Macie não poderá adicionar contas de membros até remover o número necessário de contas de membros existentes na região.

  Quando uma organização atinge essa cota, notificamos o administrador do Macie criando CloudWatch eventos AWS Health da Amazon para sua conta. Também enviamos um e-mail para o endereço de e-mail do cliente associado à sua conta.

  Se você for o administrador do Macie de uma organização, poderá determinar quantas contas de membros ativas estão atualmente associadas à sua conta usando a página Contas no console do Amazon Macie ou DescribeOrganizationConfigurationa operação da API do Amazon Macie. Para ter mais informações, consulte Como revisar contas do Amazon Macie para uma organização.
- Uma conta pode ser associada apenas a uma conta de administrador do Macie por vez. Isso significa que uma conta não pode aceitar um convite do Macie de outra conta se já estiver associada à conta de administrador do Macie de uma organização em AWS Organizations.

Da mesma forma, se uma conta já aceitou um convite, o administrador do Macie de uma organização não AWS Organizations poderá adicionar a conta como conta de membro do Macie. A conta deve primeiro ser desassociada de sua conta de administrador atual, baseada em convite.

- Para adicionar a conta AWS Organizations de gerenciamento como uma conta de membro do Macie, um usuário da conta de gerenciamento deve primeiro habilitar o Macie para a conta. O administrador do Macie não tem permissão para habilitar o Macie para a conta de gerenciamento.
- Uma conta-membro não pode se desassociar da conta de administrador do Macie. Somente o administrador do Macie pode remover uma conta como conta de membro do Macie.
- Se o administrador do Macie remover uma conta de membro do Macie, o Macie continuará habilitado para a conta. Para que uma conta também pause ou pare de usar o Macie, um usuário da conta deve suspender (pausar) ou desativar (parar) o Macie para a conta.

Transição de uma organização baseada em convites

Se você já associou uma conta de administrador do Macie às contas dos membros usando os convites para membros do Macie, recomendamos que você designe essa conta como a conta delegada do administrador do Macie para sua organização em AWS Organizations. Isso simplifica a transição de uma organização baseada em convites.

Se você fizer isso, todas as contas de membros atualmente associadas continuarão sendo membros. Se uma conta de membro fizer parte da sua organização em AWS Organizations, a associação da conta mudará automaticamente de Por convite para Via AWS Organizations in Macie. Se a conta de um membro não fizer parte da sua organização AWS Organizations, a associação da conta continuará sendo Por convite. Nos dois casos, as contas continuam associadas à conta delegada de administrador do Macie como contas de membros.

Recomendamos essa abordagem porque uma conta não pode ser associada a mais de uma conta de administrador do Macie ao mesmo tempo. Se você designar uma conta diferente como a conta de administrador do Macie para sua organização em AWS Organizations, o administrador designado não poderá gerenciar contas que já estejam associadas a outra conta de administrador do Macie por convite. Cada conta de membro deve primeiro ser desassociada de sua conta de administrador atual, baseada em convite. O administrador do Macie da sua organização em AWS Organizations pode então adicionar a conta como uma conta de membro do Macie e começar a gerenciar a conta.

Depois de integrar o Macie AWS Organizations e configurar sua organização no Macie, você pode, opcionalmente, designar uma conta de administrador do Macie diferente para a organização. Você

também pode continuar usando convites para associar e gerenciar contas de membros que não fazem parte da sua organização em AWS Organizations.

Integrando e configurando uma organização no Amazon Macie

Para começar a usar o Amazon Macie com o AWS Organizations, AWS Organizations a conta de gerenciamento da organização designa uma conta como conta de administrador delegada do Macie para a organização. Isso permite que o Macie seja um serviço confiável em AWS Organizations. Também habilita o Macie na conta atual Região da AWS do administrador designado e permite que a conta do administrador designada habilite e gerencie o Macie para outras contas na organização nessa região. Para obter informações sobre como essas permissões são concedidas, consulte Usando o AWS Organizations com outros Serviços da AWS no Guia do usuário do AWS Organizations.

O administrador delegado do Macie então configura a organização no Macie, principalmente adicionando as contas da organização como contas de membros do Macie na Região. O administrador pode então acessar determinadas configurações, dados e recursos do Macie para essas contas naquela região.

Este tópico explica como designar um administrador delegado do Macie para uma organização e como adicionar as contas da organização como contas de membros do Macie. Antes de executar essas tarefas, certifique-se de compreender o relacionamento entre contas de administrador e membros. Também é uma boa ideia revisar as considerações e recomendações para usar o Macie com AWS Organizations.

Tarefas

- Etapa 1: verifique suas permissões
- Etapa 2: designar a conta de administrador delegada do Macie para a organização
- Etapa 3: habilitar e adicionar novas contas da organização automaticamente como contas-membro do Macie
- Etapa 4: habilitar e adicionar contas de organização existentes como contas-membros do Macie

Para integrar e configurar a organização em várias regiões, a conta AWS Organizations de gerenciamento e o administrador delegado do Macie repetem essas etapas em cada região adicional.

Etapa 1: verifique suas permissões

Antes de designar a conta de administrador delegada do Macie para sua organização, verifique se você (como usuário da conta de AWS Organizations gerenciamento) tem permissão para realizar a seguinte ação do Macie: `macie2:EnableOrganizationAdminAccount`. Essa ação permite que você designe a conta de administrador delegada do Macie para sua organização usando o Macie.

Verifique também se você tem permissão para realizar as seguintes AWS Organizations ações:

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Essas ações permitem que você: recupere informações sobre sua organização; integre o Macie com AWS Organizations; recupere informações sobre as quais Serviços da AWS você se integrou AWS Organizations; e designe uma conta de administrador delegada do Macie para sua organização.

Para conceder essas permissões, inclua a seguinte instrução em uma política AWS Identity and Access Management (IAM) da sua conta:

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

Antes de designar sua conta de gerenciamento do AWS Organizations como a conta de administrador delegada do Macie para a organização, sua conta também precisará ter permissão para realizar a seguinte ação do IAM: `CreateServiceLinkedRole`. Essa ação permite que você habilite o Macie para a conta de gerenciamento. No entanto, com base nas melhores práticas de AWS segurança e no princípio do privilégio mínimo, não recomendamos que você faça isso.

Se você decidir conceder essa permissão, adicione a instrução a seguir à política do IAM para a sua conta AWS Organizations de gerenciamento:

```
{
   "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"
      }
   }
}
```

Na instrução, substitua *111122223333* pelo ID da conta de gerenciamento.

Se você quiser administrar o Macie em uma Região da AWS opcional (região desabilitada por padrão), atualize também o valor da entidade principal de serviço do Macie no elemento `Resource` e na condição `iam:AWSServiceName`. O valor deve especificar o código da região. Por exemplo, para administrar o Macie na região do Oriente Médio (Bahrein), que tem o código de região me-south-1, faça o seguinte:

- Para o elemento `Resource`, substitua

  `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`

  Onde *111122223333* especifica o ID da conta de gerenciamento e *me-south-1* especifica o código da região para a região.
- Na condição `iam:AWSServiceName`, substitua `macie.amazonaws.com` por `macie.me-south-1.amazonaws.com`, onde *me-south-1* especifica o código da região para a região.

Para obter uma lista de regiões onde o Macie está disponível atualmente e o código de região de cada uma, consulte Endpoints e cotas do Amazon Macie no arquivo Referência geral da AWS. Para obter informações sobre regiões opcionais, consulte Como especificar quais Regiões da AWS sua conta pode usar no Guia de referência do AWS Account Management.

Etapa 2: designar a conta de administrador delegada do Macie para a organização

Depois de verificar suas permissões, você (como usuário da conta de gerenciamento do AWS Organizations) pode designar a conta de administrador delegada do Macie para sua organização.

Para designar a conta de administrador delegada do Macie para uma organização

Para designar a conta de administrador delegada do Macie para sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Somente um usuário da conta de gerenciamento do AWS Organizations pode realizar essa tarefa.

Console

Siga estas etapas para designar a conta de administrador delegada do Macie usando o console do Amazon Macie.

Para designar a conta de administrador delegada do Macie

1. Faça login no AWS Management Console usando sua conta de gerenciamento do AWS Organizations.
2. Usando o seletor de Região da AWS no canto superior direito da página, selecione a região na qual deseja designar a conta de administrador delegado do Macie para sua organização.
3. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
4. Siga um destes procedimentos, dependendo de o Macie estar habilitado para sua conta de gerenciamento na região atual:
   - Se o Macie não estiver habilitado, selecione Iniciar na página de boas-vindas.
   - Se o Macie estiver ativado, escolha Configurações no painel de navegação.
5. Em Administrador delegado, insira o ID da conta de 12 dígitos para a Conta da AWS que você deseja designar como a nova conta de administrador do Macie.
6. Escolha Delegar.

Repita as etapas anteriores em cada região adicional da qual deseja integrar a organização ao Macie. Você deve designar a mesma conta de administrador do Macie em cada uma dessas regiões.

API

Para designar programaticamente a conta delegada do administrador do Macie, use a operação EnableOrganizationAdminAccount da API do Amazon Macie. Para designar a conta em várias regiões, envie a designação para cada região na qual você deseja integrar sua organização ao Macie. Você deve designar a mesma conta de administrador do Macie em cada uma dessas regiões.

Ao enviar a designação, use o parâmetro `adminAccountId` necessário para especificar o ID da conta de 12 dígitos para a Conta da AWS a ser designada como a conta de administrador do Macie para a organização. Além disso, certifique-se de especificar a região à qual a designação se aplica.

Para designar a conta de administrador do Macie usando o AWS Command Line Interface (AWS CLI), execute o comando enable-organization-admin-account. Para o parâmetro `admin-account-id`, especifique o ID da conta de 12 dígitos para a Conta da AWS a ser designada. Use o parâmetro `region` para especificar a região à qual a designação se aplica. Por exemplo:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 111122223333
```

Onde *us-east-1* é a região à qual a designação se aplica (a região Leste dos EUA (Norte da Virgínia)) e *111122223333* é a ID da conta a ser designada.

Depois de designar a conta de administrador do Macie para sua organização, o administrador do Macie pode começar a configurar a organização no Macie.

Etapa 3: habilitar e adicionar novas contas da organização automaticamente como contas-membro do Macie

Por padrão, o Macie não é habilitado automaticamente para novas contas quando as contas são adicionadas à sua organização no AWS Organizations. Além disso, as contas não são adicionadas automaticamente como contas de membros do Macie. As contas aparecem no inventário de contas do administrador do Macie. No entanto, o Macie não está necessariamente habilitado para as contas

e o administrador do Macie não pode necessariamente acessar as configurações, os dados e os recursos do Macie para as contas.

Se você for o administrador delegado do Macie para a organização, poderá alterar essa configuração para sua organização. Se você ativar a configuração de ativação automática, o Macie será ativado automaticamente para novas contas quando as contas forem adicionadas à sua organização no AWS Organizations, e as contas serão automaticamente associadas à sua conta de administrador do Macie como contas de membros. A habilitação dessa configuração não afeta as contas existentes na sua organização. Para habilitar e gerenciar o Macie para contas existentes, você deve adicionar manualmente as contas como contas de membros do Macie. A próxima etapa explica como fazer isso.

> **Note**
>
> Se você ativar a configuração de ativação automática, observe as seguintes exceções:
>
> - Se uma nova conta já estiver associada a uma conta de administrador diferente do Macie, o Macie não adicionará automaticamente a conta como conta membro em sua organização.
>
> A conta deve se desassociar de sua conta de administrador atual do Macie antes que possa fazer parte da sua organização no Macie. Em seguida, você pode adicionar manualmente a conta. Para identificar contas em que esse é o caso, você pode revisar o inventário de contas da sua organização.
> - Se sua organização atingir a cota de 10.000 contas de membros do Macie em uma Região da AWS, o Macie desativará automaticamente essa configuração na Região.
>
> Se isso acontecer, notificaremos você criando eventos AWS Health e do Amazon CloudWatch para sua conta de administrador do Macie. Também enviamos e-mails para o endereço associado a essa conta. Se o número total de contas diminuir posteriormente para menos de 10.000 contas, o Macie ativará automaticamente a configuração novamente.

Para habilitar e adicionar automaticamente novas contas da organização como contas de membros do Macie

Para habilitar e adicionar automaticamente novas contas como contas de membros do Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Somente o administrador delegado do Macie para a organização pode executar esta tarefa.

Console

Para realizar esta tarefa usando o console, você deve ter permissão para realizar a seguinte ação do AWS Organizations: `organizations:ListAccounts`. Essa ação permite que você recupere as informações sobre as contas da sua organização. Se você tiver essas permissões, siga estas etapas para ativar e adicionar automaticamente novas contas da organização como contas de membros do Macie.

Para ativar e adicionar automaticamente novas contas da organização

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor de Região da AWS no canto superior direito da página, selecione a região na qual você deseja habilitar e adicionar automaticamente novas contas como contas de membro do Macie.
3. No painel de navegação, em Settings, selecione Accounts.
4. Na página Contas, ao lado de Adicionar contas, ative a configuração de Ativação automática.

Repita as etapas anteriores em cada região adicional na qual deseja configurar a organização no Macie.

Para alterar essa configuração posteriormente e parar de ativar e adicionar novas contas automaticamente, repita as etapas anteriores e desative a configuração de ativação automática.

API

Para habilitar e adicionar automaticamente novas contas de membros do Macie de forma programática, use a operação UpdateOrganizationConfiguration da API do Amazon Macie. Ao enviar sua solicitação, defina o valor do parâmetro `autoEnable` como `true`. (O valor padrão é `false`.) Além disso, certifique-se de especificar a região à qual sua solicitação se aplica. Para ativar e adicionar automaticamente novas contas em outras regiões, envie a solicitação para cada região adicional.

Se você usar o AWS CLI para enviar a solicitação, execute o comando update-organization-configuration e especifique o parâmetro `auto-enable` para ativar e adicionar novas contas automaticamente. Por exemplo:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

Onde *us-east-1* é a região na qual habilitar e adicionar automaticamente novas contas, a região Leste dos EUA (Norte da Virgínia).

Para alterar essa configuração posteriormente e parar de ativar e adicionar novas contas automaticamente, execute o mesmo comando novamente e use o parâmetro `no-auto-enable`, em vez do parâmetro `auto-enable`, em cada região aplicável.

Etapa 4: habilitar e adicionar contas de organização existentes como contas-membros do Macie

Quando você integra o Macie com o AWS Organizations, o Macie não é habilitado automaticamente para todas as contas existentes em sua organização. Além disso, as contas não são associadas automaticamente à conta delegada de administrador do Macie como contas de membros do Macie.

Portanto, a etapa final de integrar e configurar sua organização no Macie é adicionar contas existentes da organização como contas de membros do Macie. Quando você adiciona uma conta existente como conta de membro do Macie, o Macie é automaticamente ativado para a conta e você (como administrador delegado do Macie) obtém acesso a determinadas configurações, dados e recursos do Macie para a conta.

Observe que você não pode adicionar uma conta atualmente associada a outra conta de administrador do Macie. Para adicionar a conta, trabalhe com o proprietário da conta para primeiro desassociar a conta da conta de administrador atual. Além disso, você não pode adicionar uma conta existente se o Macie estiver atualmente suspenso da conta. O proprietário da conta deve primeiro rehabilitar o Macie para a conta. Finalmente, se você quiser adicionar a conta de gerenciamento do AWS Organizations como uma conta de membro, um usuário dessa conta deve primeiro habilitar o Macie para a conta.

Para habilitar e adicionar contas de organização existentes como contas-membros do Macie

Para habilitar e adicionar contas organizacionais existentes como contas de membros do Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Somente o administrador delegado do Macie para a organização pode executar esta tarefa.

Console

Para realizar esta tarefa usando o console, você deve ter permissão para realizar a seguinte ação do AWS Organizations: `organizations:ListAccounts`. Essa ação permite que você recupere as informações sobre as contas da sua organização. Se você tiver essas permissões, siga estas etapas para ativar e adicionar contas existentes como contas de membros do Macie.

Para habilitar e adicionar contas existentes da organização

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor de Região da AWS no canto superior direito da página, selecione a região na qual você deseja habilitar e adicionar contas existentes como contas de membro do Macie.
3. No painel de navegação, em Settings, selecione Accounts.

   A página Contas é aberta e exibe uma tabela das contas associadas à sua conta Macie. Se uma conta fizer parte da sua organização no AWS Organizations, o tipo será Via AWS Organizations. Se uma conta não for uma conta-membro do Macie, o status será Não membro.
4. Na tabela Contas, selecione a caixa de seleção para cada conta que deseja adicionar como conta-membro do Macie.

   > **Tip**
   >
   > Para identificar mais facilmente as contas a serem adicionadas, você pode filtrar a tabela. Para fazer isso, coloque o cursor na caixa de filtro acima da tabela e selecione Status. Em seguida, escolha Status = Não é um membro.
5. No menu Ações, selecione Adicionar membro.
6. Confirme que deseja adicionar as contas selecionadas como contas-membro.

Depois de confirmar a adição das contas selecionadas, o status das contas muda para Criando/Habilitando e, em seguida, Habilitado.

Repita as etapas anteriores em cada região adicional na qual deseja configurar a organização no Macie.

API

Para habilitar e adicionar programaticamente uma ou mais contas existentes como contas de membro do Macie, use a operação CreateMember da API do Amazon Macie. Ao enviar sua solicitação, use os parâmetros compatíveis para especificar o ID da conta de 12 dígitos e o endereço de e-mail de cada uma Conta da AWS para ativar e adicionar. Especifique também a região à qual a solicitação se aplica. Para ativar e adicionar contas existentes em outras regiões, envie a solicitação para cada região adicional.

Para recuperar o ID da conta e o endereço de e-mail de uma Conta da AWS para habilitar e adicionar, você pode, opcionalmente, usar a operação ListMembers da API do Amazon Macie. Essa operação fornece detalhes sobre as contas associadas à sua conta do Macie, incluindo contas que não são contas de membros do Macie. Se o valor da propriedade `relationshipStatus` de uma conta não for `Enabled`, a conta não é uma conta de membro do Macie.

Para ativar e adicionar uma ou mais contas existentes usando o AWS CLI, execute o comando create-member. Use o parâmetro `region` para especificar a região na qual ativar e adicionar as contas. Use os parâmetros `account` para especificar o ID da conta e o endereço de e-mail de cada Conta da AWS a ser adicionada. Por exemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Onde *us-east-1* é a região na qual ativar e adicionar a conta como uma conta de membro do Macie (a região Leste dos EUA (Norte da Virgínia)) e os parâmetros `account` especificam o ID da conta (*123456789012*) e o endereço de e-mail (*janedoe@example.com*) da conta.

Se a sua solicitação for realizada com êxito, o status (`relationshipStatus`) da conta especificada será alterado para `Enabled` no inventário da sua conta.

Como revisar contas do Amazon Macie para uma organização

Depois que uma organização AWS Organizations é integrada e configurada no Amazon Macie, o administrador delegado do Macie da organização pode acessar um inventário das contas da organização no Macie. Como administrador do Macie de uma organização, você pode usar esse inventário para revisar estatísticas e detalhes das contas do Macie da sua organização em uma Região da AWS. Você também pode usar esse inventário para gerenciar contas de membros do Macie em uma região.

Para revisar as contas do Macie de uma organização

Para analisar as contas em sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para analisar as contas do Macie da sua organização usando o console do Amazon Macie.

Para revisar as contas da sua organização

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja revisar as contas de sua organização.
3. No painel de navegação, em Configurações, selecione Contas.

A página Contas é aberta e exibe estatísticas agregadas e uma tabela das contas associadas à sua conta Macie no Região da AWS atual.

Na parte superior da página Contas, você encontrará as seguintes estatísticas agregadas.

Via AWS Organizations

Ativo informa o número total de contas associadas à sua conta através do AWS Organizations e que atualmente são contas-membro do Macie na sua organização. O Macie está habilitado para essas contas e você é o administrador Macie das contas.

Tudo relata o número total de contas associadas à sua conta por meio de AWS Organizations, incluindo contas que atualmente não são contas de membros do Macie.

Por convite

Ativo informa o número total de contas associadas à sua conta pelo convite do Macie e que atualmente são contas-membro do Macie. (Essas contas não estão associadas à sua conta por meio de AWS Organizations.) O Macie está habilitado para essas contas e você é o administrador das contas do Macie porque eles aceitaram seu convite de associação.

Tudo relata o número total de contas associadas à sua conta por convite do Macie, incluindo contas que não responderam a um convite seu.

Ativo/Tudo

Ativo relata o número total de contas que atualmente são contas de membros do Macie em sua conta, por meio do AWS Organizations ou por convite. O Macie está habilitado para essas contas e você é o administrador Macie das contas.

Tudo relata o número total de contas associadas à sua conta, por meio do AWS Organizations ou por convite. Isso inclui contas que fazem parte da sua organização AWS Organizations e que atualmente não são contas de membros do Macie e quaisquer contas que não tenham respondido a um convite de membro do Macie feito por você.

Na tabela, você encontrará detalhes sobre cada conta na região atual. A tabela inclui o número total de contas associadas à sua conta do Macie, por meio do AWS Organizations ou por convite do Macie.

ID da conta

A ID da conta e o endereço de e-mail para a Conta da AWS.

Nome

O nome da conta da Conta da AWS. Esse valor é normalmente N/A para contas que são associadas à sua conta por convite do Macie.

Type

Como a conta é associada à sua conta, por meio do AWS Organizations ou por convite do Macie.

Status

O status do relacionamento entre sua conta e a conta. Para uma conta em uma organização AWS Organizations (Tipo é Via AWS Organizations), os possíveis valores são:

- Conta suspensa – A Conta da AWS está suspensa.
- Criado/habilitando — O Macie está processando uma solicitação para habilitar e adicionar a conta como uma conta de membro do Macie.
- Habilitado – A conta é uma conta de membro do Macie. O Macie está habilitado para a conta e você é o administrador Macie da conta.
- Não é um membro — A conta faz parte da sua organização no AWS Organizations, mas não é uma conta de membro do Macie.

- Pausado (suspenso) – A conta é uma conta de membro, mas o Macie está atualmente suspenso para a conta.
- Região desabilitada — A conta faz parte da sua organização no AWS Organizations, mas a região atual está desativada para a Conta da AWS.
- Removido (desassociado) — A conta era anteriormente uma conta de membro do Macie, mas foi posteriormente removida como conta de membro. Você desassociou a conta de sua conta de administrador do Macie. Macie continua habilitado para a conta.

Última ação

Quando você ou a conta associada realizaram recentemente uma ação que afetou o relacionamento entre as suas contas.

Para classificar a tabela por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna. Para filtrar a tabela, coloque o cursor na caixa de filtro e adicione uma condição de filtro para um campo. Para refinar ainda mais os resultados, adicione condições de filtro para campos adicionais.

API

Para revisar as contas da sua organização de forma programática, use a operação ListMembers da API do Amazon Macie e certifique-se de especificar a região à qual sua solicitação se aplica. Para revisar os detalhes em outras regiões, envie a sua solicitação em cada região adicional.

Ao enviar sua solicitação, use o parâmetro `onlyAssociated` para especificar quais contas incluir na resposta. Por padrão, o Macie retorna detalhes somente sobre as contas que são contas de membros do Macie na região especificada, seja por meio do AWS Organizations ou por convite do Macie. Para recuperar esses detalhes de todas as contas associadas à sua conta do Macie, incluindo contas que não são contas-membro, inclua o parâmetro `onlyAssociated` na sua solicitação e defina o valor do parâmetro como `false`.

Para revisar as contas da sua organização usando o AWS Command Line Interface (AWS CLI), execute o comando list-members. Para o parâmetro `only-associated`, especifique se deseja incluir todas as contas associadas ou somente contas de membros do Macie. Para incluir somente contas de membros, omita esse parâmetro ou defina o valor do parâmetro para `true`. Para incluir todas as contas, defina esse valor como `false`. Por exemplo:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Onde *us-east-1* é a região da à qual a solicitação se aplica, a região Leste dos EUA (Norte da Virgínia).

Se a sua solicitação for realizada com êxito, o Macie retornará uma matriz `members`. A matriz contém um objeto `member` para cada conta que atenda aos critérios especificados na solicitação. Nesse objeto, o campo `relationshipStatus` indica o status atual da associação entre sua conta e a outra conta na região especificada. Para uma conta em uma organização baseada do AWS Organizations, os valores possíveis são:

- `AccountSuspended` – A Conta da AWS está suspensa.
- `Created` – O Macie está processando uma solicitação para habilitar e adicionar a conta como uma conta-membro do Macie.
- `Enabled` – A conta é uma conta-membro do Macie. O Macie está habilitado para a conta e você é o administrador Macie da conta.
- `Paused` – A conta é uma conta-membro do Macie, mas o Macie está atualmente suspenso (pausado) para a conta.
- `RegionDisabled` — A conta faz parte da sua organização no AWS Organizations, mas a região atual está desativada para a Conta da AWS.
- `Removed` — A conta era anteriormente uma conta-membro do Macie, mas foi posteriormente removida como conta-membro. Você desassociou a conta de sua conta de administrador do Macie. Macie continua habilitado para a conta.

Para obter informações sobre outros campos no objeto `member`, consulte Membros na referência de API do Amazon Macie.

Gerenciar contas de membros do Amazon Macie para uma organização

Depois que uma AWS Organizations organização é integrada e configurada no Amazon Macie, o administrador delegado do Macie da organização pode acessar determinadas configurações, dados e recursos do Macie para contas de membros.

Como administrador do Macie de uma organização, você pode realizar centralmente determinadas tarefas de gerenciamento e administração de contas no Macie. Por exemplo:

- Adicionar e remover contas de membros do Macie.

- Gerencie o status do Macie para contas individuais, como habilitar ou suspender o Macie para uma conta
- Monitore as cotas do Macie e os custos de uso estimados para contas individuais e para a organização em geral

Você também pode analisar dados de inventário do Amazon Simple Storage Service (Amazon S3) e resultados de políticas para contas de membro do Macie. E você pode descobrir dados confidenciais nos buckets do S3 que as contas possuem. Para obter uma lista detalhada das tarefas que você pode executar, consulteCompreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Por padrão, o Macie oferece visibilidade dos dados e dos recursos relevantes de todas as contas de membros do Macie em sua organização. Você também pode analisar dados e recursos de contas individuais detalhadamente. Por exemplo, se você usar o painel Resumo para avaliar a postura de segurança da sua organização no Amazon S3, você poderá filtrar os dados por conta. Da mesma forma, se você monitorar os custos de uso estimados, poderá acessar os detalhamentos dos custos estimados para contas de membros individuais.

Além das tarefas comuns às contas de administrador e membro, você pode realizar várias tarefas administrativas para sua organização.

Tarefas

- Adicionar contas de membros do Amazon Macie a uma organização
- Suspensão do Amazon Macie para contas de membros em uma organização
- Remover uma conta de membro do Amazon Macie de sua organização

Como administrador do Macie de uma organização, você pode realizar essas tarefas usando o console do Amazon Macie ou a API do Amazon Macie. Se preferir usar o console, observe que você deve ter permissão para realizar a seguinte AWS Organizations ação:`organizations:ListAccounts`. Essa ação permite que você recupere e exiba informações sobre contas de membros da sua organização emAWS Organizations.

Adicionar contas de membros do Amazon Macie a uma organização

Em alguns casos, pode ser necessário adicionar manualmente uma conta como conta de membro do Macie. Esse é o caso de contas que você removeu anteriormente (desassociou) como contas de

membros. Esse também é o caso se você não tiver configurado o Macie para habilitar e adicionar automaticamente novas contas como contas de membros quando as contas são adicionadas à sua organização emAWS Organizations.

Quando você adiciona uma conta como conta de membro do Macie, o Macie é habilitado para a conta atualRegião da AWS, se ainda não estiver habilitado nessa região, e a conta é associada à sua conta do administrador do Macie como conta de membro na região. A conta de membro não recebe um convite ou outra notificação de que você estabeleceu essa relação entre suas contas.

Observe que você não pode adicionar uma conta que já esteja associada a outra conta de administrador do Macie. A conta deve primeiro se desassociar de sua conta de administrador atual. Além disso, você não pode adicionar a conta AWS Organizations de gerenciamento como conta de membro, a menos que a conta de gerenciamento já tenha habilitado o Macie para a conta. Para saber mais sobre os requisitos adicionais, consulte Considerações e recomendações para usar o Amazon Macie com AWS Organizations.

Para adicionar uma conta de membro do Macie a uma organização

Para adicionar uma ou mais contas de membros do Macie à sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para adicionar uma ou mais contas de membro do Macie usando o console do Amazon Macie.

Para adicionar uma conta de membro do Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor Região da AWS no canto superior direito da página, selecione a região na qual você deseja adicionar uma conta de membro.
3. No painel de navegação, em Configurações, selecione Contas. A página Contas é aberta e exibe uma tabela das contas associadas à sua conta do Macie.
4. (Opcional) Para identificar mais facilmente contas que fazem parte da sua organização AWS Organizations e não são contas de membros do Macie, use a caixa de filtros acima da tabela para adicionar as seguintes condições de filtro:
   - Tipo: Organização
   - Status = Não é membro

Para também exibir contas que você removeu anteriormente e que talvez queira adicionar como contas de membros, adicione também uma condição de filtro Status = Removido.

5. Na tabela Contas, marque a caixa de seleção de cada conta que quiser adicionar como conta de membro.
6. No menu Ações, selecione Criar método.
7. Confirme se quer adicionar o número de contas selecionadas como contas de membros.

Depois de confirmar suas seleções, o status das contas selecionadas muda para Criada/Habilitada e, em seguida, Habilitadano inventário da sua conta.

Repita as etapas anteriores em cada região adicional onde você quer adicionar uma conta de membro.

API

Para adicionar uma ou mais contas de membro do Macie de forma programática, use a operação CreateMember da API do Amazon Macie.

Ao enviar sua solicitação, use os parâmetros compatíveis para especificar o ID da conta de 12 dígitos e o endereço de e-mail de cada um Conta da AWS que você deseja adicionar. Especifique também a região à qual a solicitação se aplica. Para adicionar uma conta em outras regiões, envie sua solicitação em cada região adicional.

Para recuperar o ID da conta e o endereço de e-mail de uma conta a ser adicionada, você pode correlacionar a saída da operação ListAccounts da API e a operação ListMembers da AWS Organizations API Amazon Macie. Para a ListMembers operação da API Macie, inclua o `onlyAssociated` parâmetro em sua solicitação e defina o valor do parâmetro como`false`. Se a operação for bem-sucedida, o Macie retornará uma `members` matriz que fornece detalhes sobre todas as contas associadas à sua conta de administrador do Macie na região especificada, incluindo contas que atualmente não são contas de membros. Observe o seguinte na matriz:

- Se o valor da `relationshipStatus` propriedade de uma conta não for`Enabled`, a conta está associada à sua conta, mas não é uma conta de membro do Macie.
- Se uma conta não estiver incluída na matriz, mas estiver incluída na saída da ListAccounts operação da AWS Organizations API, a conta faz parte da sua organização, AWS Organizations mas não está associada à sua conta e, portanto, não é uma conta membro do Macie.

Para adicionar uma conta de membro usando oAWS CLI, execute o comando create-member. Use o `region` parâmetro para especificar a região na qual adicionar a conta. Use os parâmetros `account` para especificar o ID da conta e o endereço de e-mail de cada a ser adicionada. Por exemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Onde us-east-1 é a região na qual adicionar a conta como conta membro (a região Leste dos EUA (Norte da Virgínia)) e account os parâmetros especificam o ID da conta (123456789012) e o endereço de e-mail (janedoe@example.com) da conta.

Se a sua solicitação for realizada com êxito, o status (`relationshipStatus`) da conta especificada será alterado para `Enabled` o inventário da sua conta.

Suspensão do Amazon Macie para contas de membros em uma organização

Como administrador do Macie de uma organização emAWS Organizations, você pode suspender o Macie para uma conta de membro em sua organização. Se você fizer isso, também poderá habilitar novamente o Macie para a conta posteriormente.

Quando você suspende o Macie para uma conta de membro:

- O Macie perde o acesso e deixa de fornecer metadados sobre os dados do Amazon S3 da conta no Região da AWS atual.
- O Macie interrompe a execução de todas as atividades da conta da região. Isso inclui o monitoramento de buckets do S3 quanto à segurança e o controle de acesso, a execução de descobertas automatizadas de dados confidenciais e os trabalhos de descoberta de dados confidenciais que estejam atualmente em andamento.
- O Macie cancela todos os trabalhos de descoberta de dados confidenciais que foram criadas pela conta na região. Um trabalho não pode ser retomado ou reiniciado depois de ser cancelado.

  Se você tiver criado empregos para analisar dados que a conta do membro possui, o Macie não cancela seus trabalhos. Em vez disso, os trabalhos ignoram recursos que são de propriedade da conta.

Enquanto uma conta é suspensa, o Macie retém o identificador de sessão, as configurações e os recursos do Macie para a conta na região aplicável. Por exemplo, as descobertas da conta permanecerão intactas e não serão afetadas por até 90 dias. Sua organização não incorre em cobranças de Macie pela conta na região aplicável, enquanto Macie está suspenso pela conta nessa região.

Para suspender o Macie de uma conta de membro em uma organização

Para suspender o Macie de uma conta membro em uma organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para suspender o Macie de uma conta-membro usando o console do Amazon Macie.

Para suspender o Macie de uma conta-membro

1. Abra o console do em https://console.aws.amazon.com/macie/.
2. Ao usar o Região da AWS seletor no canto superior direito da página, selecione a região onde você deseja suspender o Macie para a conta de membro.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas, marque a caixa de seleção da conta a ser suspensa.
5. No menu Ações, escolha Suspender Macie.
6. Confirme que você deseja suspender Macie da conta.

Depois de confirmar a suspensão, o status da conta muda para Suspensa no inventário da sua conta.

Repita as etapas anteriores em cada Região adicional na qual deseja suspender o Macie da conta.

API

Para suspender o Macie de uma conta-membro de forma programática, use a operação UpdateMemberSession da API do Amazon Macie.

Ao enviar sua solicitação, use o `id` parâmetro para especificar o ID da conta de 12 dígitos onde você deseja suspender o Conta da AWS Macie. Para o parâmetro `status`, especifique `PAUSED`

como o novo status da conta do Macie. Especifique também a região à qual a solicitação se aplica. Para suspender a conta em outras regiões, envie sua solicitação em cada região adicional.

Para recuperar o ID da conta a ser suspensa, você pode usar a operação ListMembers da API do Amazon Macie. Se você fizer isso, considere filtrar os resultados incluindo o `onlyAssociated` parâmetro na sua solicitação. Se você definir o valor desse parâmetro como`true`, o Macie retornará uma `members` matriz que fornece detalhes somente sobre as contas que atualmente são contas de membros.

Para suspender o Macie de uma conta-membro usando o AWS CLI, execute o comando update-member-session. Use o `region` parâmetro para especificar a região onde suspender o Macie e use o `id` parâmetro para especificar o ID da conta para a suspensão do Conta da AWS Macie. Para o parâmetro `status`, especifique `PAUSED`: Por exemplo:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Onde *`us-east-1`* é a região na qual suspender Macie (a região Leste dos EUA (Norte da Virgínia)), *`123456789012`* é a ID da conta pela qual suspender Macie e é o novo status de Macie para a conta. `PAUSED`

Se a sua solicitação for realizada com êxito, o Macie retornará uma resposta vazia e o status da conta especificada será alterado para `Paused` no inventário da sua conta.

Remover uma conta de membro do Amazon Macie de sua organização

Se você quiser parar de acessar as configurações, dados e recursos do Macie para uma conta de membro, você pode remover a conta como conta de membro do Macie. Você faz isso desassociando a conta da sua conta de administrador do Macie. Observe que somente você pode fazer isso com uma conta de membro. Uma AWS Organizations conta de membro não pode se desassociar da conta de administrador do Macie.

Quando você remove uma conta de membro do Macie, o Macie permanece habilitado para a conta atual. Região da AWS No entanto, a conta é desassociada da sua conta de administrador do Macie e se torna uma conta autônoma do Macie. Isso significa que você perde o acesso a todas as configurações, dados e recursos do Macie da conta, incluindo metadados e descobertas de políticas para os dados do Amazon S3 da conta. Isso também significa que você não pode mais usar o Macie para descobrir dados confidenciais nos buckets do S3 que a conta possui. Se você já criou trabalhos

de descoberta de dados confidenciais para fazer isso, os trabalhos ignoram os buckets que a conta tem.

Depois de remover uma conta de membro do Macie, a conta continua aparecendo no inventário da sua conta. Macie não notifica o proprietário da conta de que você removeu a conta.

Para remover uma conta de membro do Macie da sua organização

Para remover uma conta de membro do Macie da sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para remover uma conta de membro do Macie usando o console do Amazon Macie.

Para remover uma conta de membro do Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o Região da AWS seletor no canto superior direito da página, selecione a região da qual você deseja remover a conta de membro.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas marque a caixa de seleção da conta que deseja adicionar como conta de membro.
5. No menu Ações, escolha Desassociar conta.
6. Confirme que você deseja remover a conta selecionada como conta de membro.

Depois de confirmar sua seleção, o status da conta muda para Removida [desassociada] no inventário da sua conta.

Repita as etapas anteriores em cada região adicional onde deseja remover a conta de membro.

API

Para remover uma conta de membro do Macie de forma programática, use a operação disassociateMember da API do Amazon Macie.

Ao enviar sua solicitação, use o parâmetro `id` para especificar o ID Conta da AWS de 12 dígitos da conta-membro ser removida. Especifique também a região à qual a solicitação se aplica. Para remover a conta em outras Regiões, envie a sua solicitação em cada Região adicional.

Para recuperar o ID da conta de membro a ser removida, você pode usar a operação ListMembers da API do Amazon Macie. Se você fizer isso, considere filtrar os resultados incluindo o `onlyAssociated` parâmetro na sua solicitação. Se você definir o valor desse parâmetro como`true`, o Macie retornará uma `members` matriz que fornece detalhes somente sobre as contas que atualmente são contas de membros do Macie.

Para remover uma conta de membro do Macie usando oAWS CLI, execute o comando disassociate-member. Use o `region` parâmetro para especificar a região na qual remover a conta. Use o `id` parâmetro para especificar a ID da conta de membro a ser removida. Por exemplo:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Onde *`us-east-1`* é a região na qual remover a conta (a região Leste dos EUA (Norte da Virgínia)) e *`123456789012`* é a ID da conta a ser removida.

Se a sua solicitação for realizada com êxito, o Macie retornará uma resposta vazia e o status da conta especificada será alterado para `Removed` no inventário da sua conta.

Designar uma conta de administrador do Amazon Macie para uma organização

Depois que uma AWS Organizations organização é integrada e configurada no Amazon Macie, a conta de AWS Organizations gerenciamento pode designar uma conta diferente como a conta delegada de administrador do Macie para a organização.

Como usuário da conta de AWS Organizations gerenciamento de uma organização, verifique se você atende aos seguintes requisitos de permissões antes de designar outra conta de administrador do Macie para sua organização:

- Você deve ter as mesmas permissões necessárias para designar inicialmente uma conta de administrador do Macie para sua organização. Você também deve ter permissão para realizar a seguinte AWS Organizations ação:`organizations:DeregisterDelegatedAdministrator`. Essa ação adicional permite que você remova a designação atual.
- Se sua conta for atualmente uma conta de membro do Macie, o administrador atual do Macie deverá remover sua conta como conta de membro do Macie. Caso contrário, você não poderá acessar as operações do Macie para designar uma conta de administrador diferente. Depois de

designar uma nova conta de administrador, o novo administrador do Macie pode adicionar sua conta como conta de membro do Macie novamente.

Se sua organização usa o Macie em vários Regiões da AWS, certifique-se também de alterar a conta delegada do administrador do Macie em cada região em que sua organização usa o Macie — a conta delegada do administrador do Macie deve ser a mesma em todas essas regiões. Se você gerencia várias organizações em AWS Organizations, observe também que uma conta pode ser a conta delegada de administrador do Macie para apenas uma organização por vez. Para saber mais sobre os requisitos adicionais, consulte Considerações e recomendações para usar o Amazon Macie com AWS Organizations.

Para designar uma conta de administrador Macie diferente para sua organização

Para designar uma conta de administrador diferente do Macie para sua organização, você pode usar o console do Amazon Macie ou uma combinação do Amazon Macie e das APIs. AWS Organizations Somente um usuário da conta de AWS Organizations gerenciamento pode alterar a designação de sua organização.

Console

Para alterar a designação usando o console do Amazon Macie, siga estas etapas.

Para designar uma conta de administrador do Macie diferente

1. Faça login no AWS Management Console usando sua conta AWS Organizations de gerenciamento.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região na qual você deseja alterar a designação.
3. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
4. Siga um destes procedimentos, dependendo de o Macie estar habilitado para sua conta de gerenciamento na região atual:
   - Se o Macie não estiver habilitado, selecione Iniciar na página de boas-vindas.
   - Se o Macie estiver habilitado, selecione Configurações no painel de navegação.
5. Em Administrador delegado, selecione Remover. Para alterar a designação, primeiro você deve remover a designação atual.
6. Confirme que você deseja remover a designação atual.

7. Em Administrador delegado, insira o ID da conta de 12 dígitos para designar como Conta da AWS a nova conta de administrador do Macie para a organização.
8. Escolha Delegar.

Repita as etapas anteriores em cada região adicional na qual você integrou o Macie com AWS Organizations.

API

Para alterar a designação programaticamente, você usa duas operações da API Amazon Macie e uma operação da API. AWS Organizations Isso ocorre porque você precisa remover a designação atual no Macie e AWS Organizations antes de enviar a nova designação.

Para remover a designação atual:

1. Use a DisableOrganizationAdminAccountoperação da API Macie. Para o `adminAccountId` parâmetro necessário, especifique o ID da conta de 12 dígitos da Conta da AWS que está atualmente designada como a conta de administrador do Macie para a organização.
2. Use a DeregisterDelegatedAdministratoroperação da AWS Organizations API. Para o parâmetro `AccountId` necessário, especifique o ID da conta de 12 dígitos da conta que está atualmente designada como a conta de administrador do Macie para a organização. Esse valor deve corresponder ao ID da conta que você especificou na solicitação anterior do Macie. Para o parâmetro `ServicePrincipal`, especifique o principal de serviço do Macie (`macie.amazonaws.com`).

Depois de remover a designação atual, envie a nova designação usando a EnableOrganizationAdminAccountoperação da API Macie. Para o `adminAccountId` parâmetro necessário, especifique o ID da conta de 12 dígitos para designar como Conta da AWS a nova conta de administrador do Macie para a organização.

Para alterar a designação usando o AWS CLI, execute o disable-organization-admin-accountcomando da API Macie e o deregister-delegated-administratorcomando da AWS Organizations API. Esses comandos removem a designação atual em Macie e AWS Organizations, respectivamente. Para os `account-id` parâmetros `admin-account-id` e, especifique a ID da conta de 12 dígitos a ser removida como Conta da AWS a conta de administrador atual do Macie. Use o parâmetro `region` para especificar a região à qual deseja aplicar a remoção. Por exemplo: .

```
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
```

Em que:

- *us-east-1* é a região da à qual a solicitação se aplica, a região Leste dos EUA (Norte da Virgínia).
- *111122223333* é o ID da conta a ser removida como a conta de administrador do Macie.
- `macie.amazonaws.com` é o principal serviço da Macie.

Depois de remover a designação atual, envie a nova designação executando o enable-organization-admin-accountcomando da API do Macie. Para o `admin-account-id` parâmetro, especifique o ID da conta de 12 dígitos para designar como Conta da AWS a nova conta de administrador do Macie para a organização. Use o parâmetro `region` para especificar a região à qual a designação se aplica. Por exemplo: .

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

Onde *us-east-1* é a região à qual a designação se aplica (a região Leste dos EUA (Norte da Virgínia)) e *444455556666* é o ID da conta a ser designada como a nova conta de administrador do Macie.

Desativando a integração do Amazon Macie com AWS Organizations

Depois que uma AWS Organizations organização é integrada ao Amazon Macie, a conta AWS Organizations de gerenciamento pode posteriormente desativar a integração. Como usuário da conta de AWS Organizations gerenciamento, você pode fazer isso desativando o acesso a serviço confiável para o Macie em. AWS Organizations

Quando você desativa o acesso a serviços confiáveis para o Macie, ocorre o seguinte:

- Macie perde seu status de serviço confiável emAWS Organizations.
- A conta de administrador do Macie da organização perde o acesso a todas as configurações, dados e recursos do Macie para todas as contas dos membros do Macie. Regiões da AWS

- Todas as contas de membros do Macie se tornam contas autônomas do Macie. Se o Macie tiver sido ativado para uma conta de membro em uma ou mais regiões, o Macie continuará ativado para a conta nessas regiões. No entanto, a conta não estará mais associada a uma conta de administrador do Macie em nenhuma região.

Para obter informações adicionais sobre os resultados da desativação do acesso a serviços confiáveis, consulte Usar AWS Organizations com outros Serviços da AWS no Guia do AWS Organizations Usuário.

Para desabilitar acesso a serviço confiável

Para desativar o acesso a serviços confiáveis, você pode usar o AWS Organizations console ou a AWS Organizations API. Como usuário da conta AWS Organizations de gerenciamento, você pode fazer isso desativando o acesso a serviço confiável para o Macie em. Para obter detalhes sobre as permissões necessárias, consulte Permissões necessárias para desativar o acesso confiável no Guia do AWS Organizations usuário.

Antes de desativar o acesso a serviços confiáveis, opcionalmente, trabalhe com o administrador delegado do Macie da sua organização para suspender ou desativar o Macie para contas de membros e limpar os recursos do Macie para essas contas.

Console

Para desativar o acesso a serviços confiáveis usando o console AWS Organizations, siga estas etapas.

Para desabilitar acesso a serviço confiável

1. Faça login no AWS Management Console usando sua conta de gerenciamento do AWS Organizations.
2. Abra o console do AWS Organizations em https://console.aws.amazon.com/organizations/.
3. No painel de navegação, escolha Serviços.
4. Em Serviços integrados, escolha Amazon Macie.
5. Escolha Disable trusted access (Desabilitar acesso confiável).
6. Confirme que você deseja desativar o acesso confiável.

API

Para desativar programaticamente o acesso a serviços confiáveis, use a operação DisableAWSServiceAccess da API. AWS Organizations Para o parâmetro `ServicePrincipal`, especifique o principal de serviço do Macie (`macie.amazonaws.com`).

Para desativar o acesso confiável ao serviço usando o AWS Command Line Interface(AWS CLI), execute o comando disable-aws-service-access da API. AWS Organizations Para o parâmetro `service-principal`, especifique o principal de serviço do Macie (`macie.amazonaws.com`). Por exemplo:

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

Gerenciando contas do Amazon Macie por convite

Você pode gerenciar centralmente várias contas do Amazon Macie de duas maneiras: integrando o Macie a AWS Organizations ou usando convites para associação. Se você usar convites para associação, um administrador designado do Macie poderá gerenciar o Macie para até mil contas. O administrador também pode acessar os dados de inventário do Amazon Simple Storage Service (Amazon S3) e descobrir os dados confidenciais nos buckets do S3 de propriedade da conta. Para obter detalhes sobre as tarefas que os administradores podem realizar, consulte Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Em uma organização baseada em convites, você associa contas do Macie entre si enviando e aceitando convites de associação no Macie. Se você enviar um convite e ele for aceito por outra conta, você se tornará o administrador do Macie da outra conta e a outra conta se tornará uma conta-membro na sua organização. Se você receber e aceitar um convite, a sua conta se tornará uma conta-membro e o administrador do Macie poderá acessar determinadas configurações, dados e recursos do Macie para a sua conta.

> **Tip**
>
> Se você criar uma organização baseada em convites no Macie, você poderá, posteriormente, fazer a transição para usar AWS Organizations em vez disso. Você também pode usar os dois métodos ao mesmo tempo para gerenciar várias contas do Macie. Por exemplo, se seu

ambiente AWS incluir contas de teste, você poderá excluir as contas da sua organização em AWS Organizations e gerenciá-las separadamente por convite.

Os tópicos desta seção explicam como criar e participar de uma organização baseada em convites e como realizar várias tarefas administrativas para a organização.

Tópicos

Considerações e recomendações para organizações baseadas em convites no Amazon Macie

Antes de criar ou começar a gerenciar uma organização baseada em convites no Amazon Macie, considere os seguintes requisitos e recomendações. Também certifique-se de entender a relação entre o administrador do Macie e as contas de membros.

Tópicos

Escolhendo uma conta de administrador do Macie

Ao determinar qual conta deve ser a conta de administrador do Macie para a organização, lembre-se do seguinte:

- Uma organização só pode ter uma conta de administrador Macie.
- Uma conta não pode ser administrador do Macie e conta de membro ao mesmo tempo.

- Macie é um serviço regional. Isso significa que a associação entre uma conta de administrador do Macie e uma conta de membro é regional — a associação existe somente no Região da AWS em que um convite é enviado e aceito. Por exemplo, se o administrador do Macie Service enviar convites na região Leste dos EUA (Norte da Virgínia) e esses convites forem aceitos, ele poderá gerenciar as contas de membros apenas nessa região.

  Para gerenciar centralmente contas do Macie em várias Regiões da AWS, o administrador do Macie pode fazer login em cada região onde a organização usa atualmente ou usará o Macie e enviar convites para as contas apropriadas em cada uma dessas regiões. Para obter uma lista das regiões onde o Macie está disponível no momento, consulte Amazon Macie endpoints and cotas no Referência geral da AWS.
- Uma conta de membro só pode ser associada a uma conta de administrador do Macie por vez. Se sua organização usa o Macie em várias regiões, isso significa que a conta de administrador do Macie deve ser a mesma em todas essas regiões. No entanto, as contas de administrador e membro devem enviar e aceitar convites separadamente em cada região.
- Se a Conta da AWS do administrador do Macie for suspensa, isolada ou fechada, todas as contas de membros associadas serão automaticamente removidas como contas de membros, mas o Macie continuará ativado para essas contas.

Enviando convites e gerenciando contas de membros do Macie

Como administrador do Macie de uma organização baseada em convites, lembre-se do seguinte ao enviar convites e gerenciar contas na organização:

- Se você enviar um convite, os dados relacionados poderão ser transferidos entre Regiões da AWS. Esse é o caso porque o Macie verifica o endereço de e-mail da conta de recebimento usando um serviço de verificação de e-mail que opera somente na região Leste dos EUA (Norte da Virgínia).
- Você pode enviar um convite para qualquer Conta da AWS ativa, incluindo contas que não tenham habilitado o Macie. No entanto, para aceitar ou recusar um convite, a conta receptora deve habilitar o Macie na região de onde o convite foi enviado.
- Uma conta de administrador do Macie pode ser associada a no máximo 1.000 contas em cada Região da AWS. Isso inclui contas que ainda não responderam aos convites. Se sua conta atingir essa cota, você não poderá adicionar ou convidar outras contas até remover o número necessário de contas associadas, receber o número necessário de convites recusados ou uma combinação dos dois.

Para determinar quantas contas estão atualmente associadas à sua conta, você pode usar a página Contas no console do Amazon Macie ou a operação ListMembers da API do Amazon Macie. Para obter mais informações, consulte Como analisar contas do Amazon Macie para uma organização baseada em convites.

- Uma conta de membro só pode ser associada a uma conta de administrador do Macie por vez. Isso significa que uma conta não pode aceitar seu convite se já estiver associada a outra conta de administrador do Macie. A conta deve primeiro se desassociar de sua conta atual de administrador do Macie.
- Em uma organização baseada em convites, uma conta de membro pode se desassociar de sua conta de administrador do Macie a qualquer momento. Se isso acontecer, o Macie continuará ativado para a conta e a conta se tornará uma conta autônoma do Macie. Macie não notifica você se uma conta de membro se desassociar da sua conta de administrador. No entanto, a conta continua aparecendo no inventário da sua conta e tem o status de Membro desassociado.
- Se você remover uma conta de membro de sua organização, o Macie continuará ativado para a conta e a conta se tornará uma conta autônoma do Macie.

Respondendo e gerenciando convites de associação

Como destinatário de um convite ou membro de uma organização baseada em convites, lembre-se do seguinte ao responder e gerenciar os convites recebidos:

- Antes de enviar um convite, certifique-se de entender a relação entre o administrador do Macie e as contas dos membros.
- Uma conta de membro só pode ser associada a uma conta de administrador do Macie por vez. Se você aceitar um convite e, posteriormente, quiser se juntar a outra organização (por convite ou por meio de AWS Organizations), primeiro desassocie sua conta da conta de administrador atual do Macie. Em seguida, você pode se juntar à outra organização.
- Para aceitar ou recusar um convite, você precisa habilitar o Macie na Região da AWS de onde o convite foi enviado. A conta que enviou o convite não pode habilitar o Macie nessa região para você. Recusar um convite é opcional. Se recusar um convite, você pode, opcionalmente, desativar o Macie na região aplicável depois de recusar o convite.
- Se você for administrador do Macie, não poderá aceitar um convite para se tornar uma conta de membro — uma conta não pode ser de administrador e conta de membro do Macie ao mesmo tempo. Para se tornar uma conta de membro, você deve primeiro desassociar sua conta de todas as contas de membros removendo todas as contas de membros de sua organização atual.

- Macie é um serviço regional. Isso significa que a associação entre uma conta de administrador do Macie e uma conta de membro é regional — a associação existe somente no Região da AWS em que um convite é enviado e aceito.
- Se você usa o Macie em várias regiões, a conta de administrador do Macie deve ser a mesma em todas essas regiões. No entanto, o administrador do Macie precisa enviar convites para você separadamente em cada região, e você precisa aceitar os convites separadamente em cada região.
- Você pode desassociar sua conta de uma conta de administrador do Macie a qualquer momento. Se isso acontecer, o Macie continuará ativado para a conta e a conta se tornará uma conta autônoma do Macie.
- Se você remover uma conta de membro de sua organização, o Macie continuará ativado para a conta e a conta se tornará uma conta autônoma do Macie.

Fazendo a transição para AWS Organizations

Depois de criar uma organização baseada em convites no Macie, você pode fazer a transição para usar AWS Organizations. Para simplificar a transição, recomendamos que você designe a conta de administrador existente, baseada em convite, como a conta de administrador do Macie para a organização em AWS Organizations.

Se você fizer isso, todas as contas de membros atualmente associadas continuarão sendo membros. Se a conta de um membro fizer parte da organização em AWS Organizations, a associação da conta muda automaticamente de Por convite para Via AWS Organizations no Macie. Se a conta de um membro não fizer parte da organização em AWS Organizations, a associação da conta continuará sendo Por convite. Em ambos os casos, as contas continuam associadas à conta de administrador do Macie como contas de membros.

Uma conta de membro só pode ser associada a uma conta de administrador do Macie por vez. Se você designar uma conta diferente como conta de administrador do Macie para uma organização em AWS Organizations, o administrador designado não poderá gerenciar contas que já estejam associadas a outra conta de administrador do Macie por convite. Cada conta de membro deve primeiro se desassociar de sua conta de administrador atual, baseada em convite. Só então o administrador do Macie da organização AWS Organizations pode adicionar a conta do membro à organização e começar a gerenciar o Macie da conta.

Depois de integrar o Macie com AWS Organizations e configurar sua organização no Macie, você pode, como opção, designar uma conta de administrador do Macie diferente para a organização.

Você também pode continuar usando convites para associar e gerenciar contas de membros que não fazem parte da sua organização em AWS Organizations.

Criação e gerenciamento de uma organização baseada em convites no Amazon Macie

Para criar uma organização baseada em convites no Amazon Macie, você começa determinando qual conta deseja que seja a conta de administrador do Macie para a organização. Em seguida, você usa essa conta para adicionar contas-membro — você envia convites para associação para outras Contas da AWS, convidando as contas a ingressarem na organização como contas-membro do Macie na Região da AWS atual. Para criar a organização em várias Regiões, envie convites para associação de cada Região na qual as outras contas já usam ou irão usar o Macie.

Quando uma conta aceita um convite, ela se torna uma conta-membro do Macie associada à conta de administrador do Macie na região pertinente. A conta de administrador do Macie pode acessar determinadas configurações, dados e recursos do Macie da conta-membro naquela Região.

Como administrador do Macie de uma organização baseada em convites, você pode analisar dados de inventário do Amazon Simple Storage Service (Amazon S3) e descobertas de políticas para contas-membro. Você também pode realizar a descoberta automatizada de dados confidenciais e executar trabalhos de descoberta de dados confidenciais para detectar dados confidenciais nos buckets do S3 de propriedade das contas-membro. Para obter uma lista detalhada das tarefas que você pode executar, consulte Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Por padrão, o Macie oferece visibilidade dos dados e recursos relevantes para sua organização em geral. Você também pode se aprofundar mais para analisar dados e recursos para contas-membro da sua organização. Por exemplo, se você usar o painel Resumo para avaliar a postura de segurança da sua organização no Amazon S3, você poderá filtrar os dados por conta. Da mesma forma, se você monitorar os custos de uso estimados, você poderá acessar o detalhamento dos custos estimados para contas-membro individuais.

Além das tarefas que são comuns às contas de administrador e membro, você pode realizar, de forma centralizada, várias tarefas administrativas para sua organização. Antes de realizar essas tarefas, é uma boa ideia revisar as considerações e recomendações para gerenciamento de organizações baseadas em convites no Macie.

Tarefas

- Adicionando contas-membro do Amazon Macie a uma organização baseada em convites

- Suspendendo o Amazon Macie para contas-membro em uma organização baseada em convites
- Removendo contas-membro do Amazon Macie de uma organização baseada em convites
- Excluindo associações com outras contas

Adicionando contas-membro do Amazon Macie a uma organização baseada em convites

Como administrador do Macie de uma organização baseada em convites, você adiciona contas-membro à sua organização executando duas etapas primárias:

1. Adicione as contas ao seu inventário de contas do Macie. Isso associa as contas com a sua conta.
2. Envie convites para associação para as contas.

Depois que a conta aceitar seu convite, ela se torna uma conta-membro na sua organização.

Etapa 1: adicione as contas

Para adicionar uma ou mais contas ao seu inventário de contas, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Com o console do Amazon Macie, você pode adicionar uma conta por vez ou adicionar várias contas ao mesmo tempo fazendo o upload de um arquivo de valores separados por vírgula (CSV). Siga estas etapas para adicionar uma ou mais contas usando o console.

Para adicionar uma conta

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja adicionar uma conta.
3. No painel de navegação, em Configurações, selecione Contas.
4. Escolha Add accounts.
5. Na seção Inserir detalhes da conta, escolha a guia Adicionar conta. Então, faça o seguinte:
   - Em =ID da conta, insira o ID de 12 dígitos da conta Conta da AWS a ser adicionada.
   - Em Endereço de e-mail, insira o endereço de e-mail da Conta da AWS a ser adicionada.

6. Selecione Adicionar e, a seguir, selecione Avançar.

O Macie adiciona a conta ao inventário da sua conta. O tipo da conta é Por convite e seu status é Criada. Repita as etapas anteriores em cada Região adicional na qual você deseja adicionar a conta.

Para adicionar várias contas

1. Usando um editor de texto, crie um arquivo CSV da seguinte forma:

   a. Adicione o cabeçalho a seguir como a primeira linha do arquivo: `Account ID,Email`

   b. Para cada conta, crie uma nova linha com o ID de 12 dígitos da conta para a Conta da AWS a ser adicionada e o endereço de e-mail da conta. Separe as entradas com uma vírgula, por exemplo: `111111111111,janedoe@example.com`

      O endereço de e-mail deve corresponder ao endereço de e-mail associado à Conta da AWS.

   c. Verifique se o conteúdo do arquivo está formatado conforme mostrado no exemplo a seguir, que contém o cabeçalho e as informações necessários para três contas:

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

   d. Salve o arquivo no computador.

2. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
3. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja adicionar as contas.
4. No painel de navegação, em Configurações, selecione Contas.
5. Escolha Add accounts.
6. Na seção Inserir detalhes da conta, escolha a guia Carregar lista.
7. Selecione Procurar e, em seguida, selecione o arquivo CSV criado na etapa 1.
8. Selecione Adicionar contas e Avançar.

O Macie adiciona as contas ao seu inventário de contas. Seu tipo é Por convite e seu status é Criada. Repita as etapas de 3 a 8 em cada Região adicional na qual você deseja adicionar contas-membro.

API

Para adicionar uma ou mais contas de forma programática, use a operação CreateMember da API Amazon Macie. Ao enviar sua solicitação, use os parâmetros compatíveis para especificar o ID de 12 dígitos da conta e o endereço de e-mail de cada Conta da AWS a ser adicionada. Especifique também a Região à qual a solicitação se aplica. Para adicionar contas em outras Regiões, envie a solicitação em cada Região adicional.

Para adicionar contas usando o AWS Command Line Interface (AWS CLI), execute o comando create-member. Use o parâmetro `region` para especificar a Região na qual adicionar as contas. Use os parâmetros `account` para especificar o ID da conta e o endereço de e-mail de cada Conta da AWS a ser adicionada. Por exemplo:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

Onde *us-east-1* é a região na qual adicionar a conta (a região Leste dos EUA (Norte da Virgínia)) e os parâmetros `account` especificam o ID da conta (*111111111111*) e o endereço de e-mail (*janedoe@example.com*) da conta a ser adicionada.

Se sua solicitação for realizada com êxito, o Macie adicionará cada conta ao inventário da sua conta com o status de `Created` e você receberá um resultado semelhante ao seguinte:

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

Onde `arn` é o nome do recurso da Amazon (ARN) do recurso criado para a associação entre sua conta e a conta adicionada. Neste exemplo, `123456789012` é o ID da conta que criou a associação e `111111111111` é o ID da conta que foi adicionada.

Etapa 2: envie convites para associação para as contas-membro

Depois de adicionar uma conta ao inventário da sua conta, você pode convidar a conta para se juntar à sua organização como conta-membro do Macie. Para fazer isso, envie um convite para associação para a conta. Quando você envia um convite, um selo de Contas e uma notificação aparecem no

console do Amazon Macie para a conta do destinatário, se o Macie estiver habilitado para a conta. O Macie também cria um evento AWS Health para a conta.

Dependendo se você usa o console ou a API do Amazon Macie para enviar o convite, o Macie também envia o convite para o endereço de e-mail que você especificou para a conta do destinatário ao adicionar a conta. A mensagem de e-mail indica que você gostaria de se tornar o administrador da conta do Macie e inclui a ID da sua Conta da AWS e da Conta da AWS do destinatário. A mensagem também explica como acessar o convite. Opcionalmente, você pode adicionar texto personalizado à mensagem.

Para adicionar uma ou mais contas ao seu inventário de contas, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para enviar um convite para associação usando o console do Amazon Macie.

Para enviar um convite para associação

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja enviar o convite.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas, marque a caixa de seleção de cada conta para a qual você deseja enviar o convite.

   > **Tip**
   >
   > Para identificar com mais facilidade as contas que você adicionou e para as quais ainda não enviou convites, você pode filtrar a tabela. Para fazer isso, coloque o cursor na caixa de filtro acima da tabela e selecione Status. Em seguida, selecione Status = Criada.

5. No menu Ações, selecione Convidar.
6. (Opcional) Na caixa Mensagem, insira qualquer texto personalizado que você queira incluir na mensagem de e-mail que contém o convite. O texto pode conter até 80 caracteres alfanuméricos.
7. Escolha Invite.

Para enviar o convite em uma Regiões da AWS adicional, repita as etapas anteriores em cada Região adicional.

Depois de enviar o convite, o status da conta do destinatário muda para Verificação de e-mail em andamento no inventário da sua conta. Se o Macie puder verificar o endereço de e-mail de uma conta, o status da conta mudará, posteriormente, para Convidada. Se o Macie não conseguir verificar o endereço, o status da conta mudará para Verificação de e-mail falhou. Se isso acontecer, fale com o responsável pela conta para obter o endereço de e-mail correto. Em seguida, exclua a associação entre suas contas, adicione a conta novamente e envie o convite novamente.

Quando um destinatário aceita um convite, o status da conta do destinatário muda para Habilitada no inventário da sua conta. Se um destinatário recusar um convite, a conta do destinatário será desassociada da sua conta e removida do inventário da sua conta.

API

Para enviar um convite de forma programática, use a operação CreateInvitations da API do Amazon Macie. Ao enviar sua solicitação, use os parâmetros compatíveis para especificar o ID de 12 dígitos da conta para cada Conta da AWS para a qual enviar o convite. O ID da conta deve corresponder ao ID da conta no inventário da sua conta. Caso contrário, ocorrerá um erro. Especifique também a Região da qual enviar o convite. Para enviar o convite de outras Regiões, envie a solicitação em cada região adicional.

Em sua solicitação, você também pode especificar se deseja enviar o convite como uma mensagem de e-mail e se deseja incluir texto personalizado nessa mensagem. Se você optar por enviar uma mensagem de e-mail, o Macie enviará o convite para o endereço de e-mail que você especificou para uma conta quando você adicionou a conta ao inventário da sua conta. Para enviar o convite como uma mensagem de e-mail, omita o parâmetro `disableEmailNotification` ou defina o valor do parâmetro como `false`. (O valor padrão é `false`.) Para adicionar texto personalizado à mensagem, use o parâmetro `message` para especificar o texto a ser adicionado. O texto pode conter até 80 caracteres alfanuméricos.

Para enviar convites usando o AWS CLI, execute o comando create-invitations. Use o parâmetro `region` para especificar a Região da qual enviar o convite. Use o parâmetro `account-ids` para especificar o ID da conta para cada Conta da AWS para a qual enviar o convite. Por exemplo:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

Onde *us-east-1* é a Região da qual enviar o convite (a região Leste dos EUA (Norte da Virgínia)) e o parâmetro `account-ids` especifica os IDs de conta de três contas para as quais enviar o convite. Para enviar um convite também como mensagem de e-mail, inclua também o parâmetro `no-disable-email-notification` e, opcionalmente, inclua o `message` parâmetro para especificar o texto personalizado a ser adicionado à mensagem.

Depois de enviar o convite, o status da conta de cada destinatário muda para `EmailVerificationInProgress`. Se o Macie puder verificar o endereço de e-mail de uma conta, o status da conta será alterado posteriormente para `Invited`. Se o Macie não conseguir verificar o endereço, o status da conta mudará para `EmailVerificationFailed`. Se isso acontecer, fale com o responsável pela conta para obter o endereço de e-mail correto. Em seguida, exclua a associação entre suas contas, adicione a conta novamente e envie o convite novamente.

Quando um destinatário aceita um convite, o status da conta do destinatário muda para `Enabled` no inventário da sua conta. Se um destinatário recusar um convite, a conta do destinatário será desassociada da sua conta e removida do inventário da sua conta.

Suspendendo o Amazon Macie para contas-membro em uma organização baseada em convites

Como administrador do Macie de uma organização, você pode suspender o Macie em uma Região da AWS específica para determinados membros em sua organização. Observe, no entanto, que você não pode reativar o Macie para uma conta-membro depois de suspendê-la. Posteriormente, somente um usuário da conta poderá reabilitar o Macie para a conta.

Quando você suspende o Macie para uma conta-membro:

- o Macie perde o acesso e deixa de fornecer metadados sobre os dados da conta do Amazon S3 na Região.
- o Macie interrompe a execução de todas as atividades da conta naquela Região. Isso inclui o monitoramento de buckets do S3 quanto à segurança e o controle de acesso, a execução de descobertas automáticas de dados confidenciais e os trabalhos de descoberta de dados confidenciais que estejam atualmente em andamento.
- O Macie cancela todos os trabalhos de descoberta de dados confidenciais que foram criadas pela conta na região. Nenhum trabalho poderá ser retomado ou reiniciado depois que ele for cancelado.

Se você criou trabalhos para analisar dados que a conta-membro possui, o Macie não cancelará esses trabalhos. Em vez disso, os trabalhos ignorarão os recursos que são de propriedade da conta.

Enquanto uma conta estiver suspensa, o Macie reterá o identificador da sessão, as configurações e os recursos da conta na Região pertinente. Por exemplo, as descobertas da conta permanecerão intactas e não serão afetadas por até 90 dias. A conta não será cobrada pelo uso do Macie na região aplicável enquanto o Macie estiver suspenso da conta nessa Região.

Para suspender o Macie de uma conta-membro em uma organização baseada em convites

Para suspender o Macie de uma conta-membro em uma organização baseada em convites, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para suspender o Macie de uma conta-membro usando o console do Amazon Macie.

Para suspender o Macie de uma conta-membro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja suspender o Macie de uma conta-membro.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas, marque a caixa de seleção da conta a ser suspensa.
5. No menu Ações, selecione Suspender o Macie.
6. Confirme que você deseja suspender o Macie da conta selecionada.

Depois de confirmar a suspensão, o status da conta muda para Suspensa no inventário da sua conta.

Repita as etapas anteriores em cada Região adicional na qual deseja suspender o Macie da conta.

API

Para suspender o Macie de uma conta-membro de forma programática, use a operação UpdateMemberSession da API do Amazon Macie. Ao enviar sua solicitação, use o parâmetro `id` para especificar o ID de 12 dígitos da Conta da AWS da qual você deseja suspender o Macie. Para o parâmetro `status`, especifique `PAUSED` como o novo status da conta do Macie. Especifique também a Região à qual a solicitação se aplica. Para suspender o Macie em Regiões adicionais, envie sua solicitação em cada Região adicional.

Para recuperar o ID da conta-membro, você pode usar a operação ListMembers da API do Amazon Macie. Se você fizer isso, considere filtrar os resultados incluindo o parâmetro `onlyAssociated` na sua solicitação. Se você definir o valor desse parâmetro como `true`, o Macie retornará uma matriz `members` que fornece detalhes somente sobre as contas que atualmente são contas-membro da sua conta de administrador.

Para suspender o Macie de uma conta-membro usando o AWS CLI, execute o comando update-member-session. Use o parâmetro `region` para especificar a Região na qual suspender o Macie e use o parâmetro `id` para especificar o ID da conta para a qual suspender o Macie. Para o parâmetro `status`, especifique `PAUSED`: Por exemplo:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Onde *us-east-1* é a Região na qual suspender o Macie (a região Leste dos EUA (Norte da Virgínia)), *123456789012* é o ID da conta para a qual suspender o Macie e `PAUSED` é o novo status do Macie para a conta.

Se sua solicitação for realizada com êxito, o Macie retornará uma resposta vazia e o status da conta especificada será alterado para `Paused` no inventário da sua conta.

Removendo contas-membro do Amazon Macie de uma organização baseada em convites

Como administrador da conta do Macie, você pode remover uma conta-membro da organização. Você faz isso desassociando a conta da sua conta de administrador do Macie.

Se você remover uma conta-membro, o Macie continuará habilitado para a conta e a conta continuará sendo exibida no inventário da sua conta. No entanto, a conta se torna uma conta

autônoma do Macie. O Macie não notifica o proprietário da conta quando você a remove. Portanto, considere entrar em contato com o proprietário da conta para garantir que ele comece a gerenciar as configurações e os recursos da conta.

Ao remover uma conta-membro, você perde o acesso a todas as configurações, recursos e dados da conta do Macie. Isso inclui descobertas de políticas e metadados para buckets do S3 que a conta possui. Além disso, você não poderá mais usar o Macie para descobrir dados confidenciais nos buckets do S3 que a conta possui. Se você já criou trabalhos de descoberta de dados confidenciais para fazer isso, os trabalhos ignoram os buckets que a conta possui.

Depois de remover uma conta-membro, você poderá adicioná-la novamente à sua organização enviando um novo convite para a conta. Você também pode removê-la completamente do inventário da sua conta excluindo a associação entre suas contas.

Para remover uma conta-membro de uma organização baseada em convites

Para remover uma conta-membro da sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para remover uma conta-membro usando o console do Amazon Macie.

Para remover uma conta-membro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja remover a conta-membro.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas, marque a caixa de seleção da conta a ser removida.
5. No menu Ações, selecione Desassociar conta.
6. Confirme que você deseja remover a conta selecionada como uma conta-membro.

Depois de confirmar sua seleção, o status da conta muda para Removida [desassociada] no inventário da sua conta.

Repita as etapas anteriores em cada região adicional onde deseja remover a conta de membro.

API

Para remover uma conta-membro de forma programática, use a operação DisassociateMember da API Amazon Macie. Ao enviar sua solicitação, use o parâmetro `id` para especificar o ID Conta da AWS de 12 dígitos da conta-membro ser removida. Especifique também a Região à qual a solicitação se aplica. Para remover a conta em outras Regiões, envie a sua solicitação em cada Região adicional.

Para recuperar o ID da conta-membro, você pode usar a operação ListMembers da API do Amazon Macie. Se você fizer isso, considere filtrar os resultados incluindo o parâmetro `onlyAssociated` na sua solicitação. Se você definir o valor desse parâmetro como `true`, o Macie retornará uma matriz `members` que fornece detalhes somente sobre as contas que atualmente são contas-membro da sua conta.

Para remover uma conta-membro usando o AWS CLI, execute o comando disassociate-member. Use o parâmetro `region` para especificar a Região na qual remover a conta. Use o parâmetro `id` para especificar o ID da conta a ser removida. Por exemplo:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Onde *us-east-1* é a Região na qual remover a conta (a região Leste dos EUA (Norte da Virgínia)) e *123456789012* é o ID da conta a ser removida.

Se sua solicitação for realizada com êxito, o Macie retornará uma resposta vazia e o status da conta especificada será alterado para `Removed` no inventário da sua conta.

Excluindo associações com outras contas

Depois de adicionar uma conta ao inventário da sua conta, você pode excluir a associação entre sua conta e a outra conta. Você pode fazer isso com qualquer conta em seu inventário, exceto:

- Uma conta que seja parte da sua organização em AWS Organizations. Esse tipo de associação é controlado pelo AWS Organizations, não pelo Macie.
- Uma conta-membro que aceitou um convite de membro do Macie para se juntar à sua organização. Se for esse o caso, você deve remover a conta-membro antes de excluir a associação.

Quando você exclui uma associação, o Macie remove a conta do inventário da sua conta. Se você quiser restaurar a associação posteriormente, você precisará adicionar a conta novamente como se fosse uma conta completamente nova.

Para excluir uma associação com outra conta

Para excluir uma associação entre sua conta e outra conta, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Para usar o console do Amazon Macie para excluir uma associação com outra conta, siga estas etapas.

Para excluir uma associação

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja excluir a associação.
3. No painel de navegação, em Configurações, selecione Contas.
4. Na tabela Contas, marque a caixa de seleção da conta cuja associação você deseja excluir.
5. No menu Ações, selecione Excluir conta.
6. Confirme que você deseja excluir a associação selecionada.

Repita as etapas anteriores em cada Região adicional na qual deseja excluir a associação.

API

Para excluir uma associação com outra conta de forma programática, use a operação DeleteMember da API Amazon Macie. Ao enviar sua solicitação, use o parâmetro `id` para especificar o ID de 12 dígitos da Conta da AWS com a qual excluir a associação. Especifique também a Região à qual a solicitação se aplica. Para excluir a associação em outras Regiões, envie a sua solicitação em cada Região adicional.

Para recuperar o ID da conta-membro, você pode usar a operação ListMembers da API do Amazon Macie. Se você fizer isso, inclua o parâmetro `onlyAssociated` em sua solicitação e defina o valor do parâmetro como `false`. Se a operação for realizada com êxito, o Macie retornará uma matriz `members` que fornece detalhes sobre todas as contas associadas à sua conta, incluindo contas que não são contas-membros no momento.

Para excluir uma associação com outra conta usando o AWS CLI, execute o comando delete-member. Use o parâmetro `region` para especificar a Região na qual excluir a associação e o parâmetro `id` para especificar o ID da conta. Por exemplo:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

Onde *us-east-1* é a Região na qual excluir a associação com a outra conta (a região Leste dos EUA (Norte da Virgínia)) e *123456789012* é o ID da conta.

Se a sua solicitação for realizada com êxito, o Macie retornará uma resposta vazia e a associação entre sua conta e a outra conta será excluída. A conta associada anteriormente é removida do inventário da sua conta.

Como analisar contas do Amazon Macie para uma organização baseada em convites

Para ajudá-lo a gerenciar as contas em sua organização, o Amazon Macie fornece um inventário das contas associadas à sua conta do Macie em cada um dos Região da AWS em que você usa o Macie. Ao usar esse inventário, você pode verificar o status de contas individuais e analisar as estatísticas e os detalhes da conta para a sua organização. Você também pode gerenciar o status do relacionamento entre a sua conta e contas individuais.

Para analisar contas para uma organização baseada em convites

Para analisar as contas em sua organização, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para analisar as contas da sua organização usando o console do Amazon Macie.

Para analisar as contas da sua organização

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja analisar as contas de sua organização.
3. No painel de navegação, em Configurações, selecione Contas.

A página Contas será aberta e exibe estatísticas agregadas e uma tabela das contas associadas à sua conta do Macie no Região da AWS atual.

Na parte superior da página Contas, você encontrará as seguintes estatísticas agregadas.

Via AWS Organizations

Se você for o administrador do Macie de uma organização em AWS Organizations, o Ativo relata o número total de contas que estão associadas à sua conta por meio de AWS Organizations e que atualmente são contas de membros do Macie em sua organização. O Macie está habilitado para essas contas e você é o administrador Macie das contas.

Tudo relata o número total de contas associadas à sua conta por meio de AWS Organizations, incluindo contas que atualmente não são contas de membros do Macie.

Por convite

Ativo relata o número total de contas que atualmente são contas de membros do Macie em sua organização baseada em convites. O Macie está habilitado para essas contas e você é o administrador das contas do Macie porque eles aceitaram seu convite de associação.

Tudo relata o número total de contas associadas à sua conta por convite do Macie, incluindo contas que não responderam a um convite seu.

Ativo/Tudo

Ativo relata o número total de contas que atualmente são contas de membros do Macie em sua conta, por meio de AWS Organizations ou por convite. O Macie está habilitado para essas contas e você é o administrador Macie das contas.

Tudo relata o número total de contas associadas à sua conta, por meio de AWS Organizations ou por convite. Isso inclui contas que não aceitaram o seu convite de associação ao Macie. Isso também inclui contas que estão associadas à sua conta por meio do AWS Organizations e que não são atualmente contas de membros do Macie.

Na tabela, você encontrará detalhes sobre cada conta na região atual. A tabela inclui o número total de contas associadas à sua conta do Macie, por meio de convite do Macie ou por AWS Organizations.

ID da conta

A ID da conta e o endereço de e-mail para o Conta da AWS.

Nome

O nome da conta para o Conta da AWS. Esse valor é normalmente N/A para contas que são associadas à sua conta por convite.

Tipo

Como a conta é associada à sua conta, por convite ou por meio deAWS Organizations.

Status

O status do relacionamento entre a sua conta e a conta. Para uma conta em uma organização baseada em convites (o Tipo é Por convite), os valores possíveis são:

- Conta suspensa – A Conta da AWS está suspensa.
- Criado (Convite) – Você adicionou a conta, mas ainda não enviou um convite de associação para ela.
- Falha na verificação de e-mail – Você tentou enviar um convite de associação para a conta, mas o endereço de e-mail especificado não é válido para a conta.
- Verificação de e-mail em andamento – Você enviou um convite de associação para a conta e o Macie está processando a solicitação.
- Habilitado – A conta é uma conta de membro. O Macie está habilitado para essas contas e você é o administrador Macie da conta.
- Convidado – Você enviou um convite de associação para a conta e a conta não respondeu ao seu convite.
- Membro renunciou – Anteriormente, a conta era uma conta de membro. No entanto, a conta se desligou da sua organização ao se desassociar da sua conta.
- Pausada (suspenso) – A conta é uma conta de membro, mas o Macie está atualmente suspenso da conta.
- Região desativada – A região atual está desativada para o Conta da AWS.
- Removida (desassociada) – A conta era anteriormente uma conta de membro. No entanto, você a removeu como conta de membro ao desassociá-la da sua conta.

Última ação

Quando você ou a conta associada realizaram recentemente uma ação que afetou o relacionamento entre as suas contas.

Para classificar a tabela por um campo específico, clique no título da coluna do campo. Para alterar a ordem de classificação, clique novamente no título da coluna. Para filtrar a tabela, coloque o cursor na caixa de filtro e adicione uma condição de filtro para um campo. Para refinar ainda mais os resultados, inclua condições do filtro para campos adicionais.

API

Para analisar as contas da sua organização de forma programática, use a operação ListMembers da API do Amazon Macie e certifique-se de especificar a região à qual sua solicitação se aplica. Para analisar os detalhes em outras regiões, envie a sua solicitação em cada região adicional.

Ao enviar sua solicitação, use o parâmetro `onlyAssociated` para especificar quais contas incluir na resposta. Por padrão, o Macie retorna detalhes somente sobre as contas que são contas de membros na região especificada, seja por convite ou por meio de AWS Organizations. Para recuperar os detalhes de todas as contas associadas, incluindo contas que não são contas de membros, inclua o parâmetro `onlyAssociated` em sua solicitação e defina o valor do parâmetro como `false`.

Para analisar as contas da sua organização usando o AWS Command Line Interface(AWS CLI), execute o comando list-members. Para o parâmetro `only-associated`, especifique se deseja incluir todas as contas associadas ou somente contas de membros. Para incluir somente contas de membros, omita esse parâmetro ou defina o valor do parâmetro para `true`. Para incluir todas as contas, defina esse valor como `false`. Por exemplo:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Onde a *us-east-1* é a região à qual a solicitação se aplica, a região Leste dos EUA (Norte da Virgínia).

Se a sua solicitação for realizada com êxito, o Macie retornará uma matriz `members`. A matriz contém um objeto `member` para cada conta que atenda aos critérios especificados na solicitação. Nesse objeto, o campo `relationshipStatus` indica o status atual da associação entre sua conta e a outra conta na região especificada. Para uma conta em uma organização baseada em convites, os valores possíveis são:

- `AccountSuspended` – O Conta da AWS está suspenso.
- `Created` – Você adicionou a conta, mas não enviou um convite de associação para ela.
- `EmailVerificationFailed` – Você tentou enviar um convite de membro para a conta, mas o endereço de e-mail especificado não é válido para a conta.

- `EmailVerificationInProgress` – Você enviou um convite de associação para a conta e o Macie está processando a solicitação.
- `Enabled` – A conta-membro. O Macie está habilitado para essas contas e você é o administrador Macie da conta.
- `Invited` – Você enviou um convite de associação para a conta e a conta não respondeu ao seu convite.
- `Paused` – A conta é uma conta-membro, mas o Macie está atualmente suspenso (pausado) para a conta.
- `RegionDisabled` – A região atual está desativada para o Conta da AWS.
- `Removed` – Anteriormente, a conta era uma conta-membro. No entanto, você a removeu como conta de membro ao desassociá-la da sua conta.
- `Resigned` – Anteriormente, a conta era uma conta-membro. No entanto, a conta se desligou da sua organização ao se desassociar da sua conta.

Para obter informações sobre outros campos no objeto `member`, consulte Membros na referência de API do Amazon Macie.

Designação de uma conta de administrador do Amazon Macie para uma organização com base em convites

Depois de criar e estabelecer uma organização baseada em convites, você pode alterar a conta de administrador do Amazon Macie para a organização. Para fazer isso, os administradores e membros da organização devem seguir as seguintes etapas:

1. O administrador atual do Macie opcionalmente exporta o inventário atual de contas de membros ativos da organização. Isso simplifica a transição, ajudando você a identificar contas de membros que devem continuar fazendo parte da organização.
2. O administrador atual do Macie remove todas as contas dos membros da organização atual. Isso desassocia as contas da conta atual do administrador, mas o Macie continua habilitado para as contas.
3. O novo administrador do Macie adiciona as contas dos membros anteriores à nova organização. Isso associa as contas à nova conta de administrador.

4. Cada conta membro aceita o convite para se juntar à nova organização. Quando uma conta aceita o convite, ela se torna uma conta de membro ativa na nova organização. O novo administrador do Macie pode então acessar as configurações, os dados e os recursos do Macie para a conta.

Se sua organização usa o Macie em várias Regiões da AWS, execute as etapas anteriores em cada uma dessas regiões.

Para exportar o inventário atual de contas de membros ativas, o administrador atual do Macie pode usar o console do Amazon Macie ou a API do Amazon Macie. Com o console, o administrador atual pode exportar os dados para um arquivo de valores separados por vírgula (CSV). O novo administrador pode então usar o console para carregar o arquivo CSV e adicionar todas as contas (em massa) à nova organização.

Para exportar dados da conta do membro usando o console

1. Faça login no AWS Management Console usando a conta de administrador atual do Macie.
2. Ao usar o seletor de Região da AWS no canto superior direito da página, selecione a região da em que você deseja exportar os dados.
3. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
4. No painel de navegação, em Settings, selecione Accounts.
5. (Opcional) Para filtrar a tabela Contas e mostrar somente as contas que são contas de membros do Macie atualmente ativas na organização, use a caixa de filtro acima da tabela para adicionar as seguintes condições de filtro:
   - Tipo = Convite
   - Status = Habilitado
6. Na tabela Contas, marque a caixa de seleção de cada conta de membro ativa a ser incluída nos dados exportados.
7. Escolha Exportar CSV.
8. Especifique o local e o nome do arquivo.

Com a API do Amazon Macie, o administrador atual do Macie pode recuperar os dados no formato JSON. O novo administrador do Macie pode então usar esses dados para gerar a lista de IDs de conta e endereços de e-mail para as contas adicionarem e convidarem para a nova organização. Para recuperar os dados no formato JSON, use a operação ListMembers do API do Amazon Macie. Se a operação for bem-sucedida, o Macie retornará uma matriz `members` que fornece detalhes sobre

todas as contas associadas à conta do administrador. Se uma conta for uma conta ativa de membro do Macie na organização atual baseada em convite, o valor da propriedade `relationshipStatus` da conta é `Enabled` e a propriedade `invitedAt` especifica uma data e hora.

Gerenciando sua associação em uma organização baseada em convites no Amazon Macie

Se você for convidado para participar de uma organização no Amazon Macie, você pode, opcionalmente, aceitar ou recusar o convite. Em Macie, uma organização da é um conjunto de contas da que são gerenciadas centralmente como um grupo de contas relacionadas. Uma organização consiste em uma conta de administrador designada do Macie e uma ou mais contas de membros associadas.

Se você aceitar um convite, sua conta se tornará uma conta-membro da organização. Quando você aceita, a conta que enviou o convite se torna a conta de administrador do Macie da sua conta — você associa sua conta à outra conta e ativa uma relação administrador-membro entre as contas. A conta de administrador do Macie pode então acessar determinadas configurações, dados e recursos do Macie para sua conta no campo Região da AWS aplicável. Para obter mais informações, consulte Compreendendo a relação entre o administrador do Amazon Macie e as contas-membro.

Se você recusar um convite, o status e as configurações atuais da sua conta Macie não serão alterados.

Tópicos

- Respondendo a convites de associação para organizações
- Desassociar de uma conta de administrador do Amazon Macie

Respondendo a convites de associação para organizações

Quando você recebe um convite para participar de uma organização, Amazon Macie notifica você de várias maneiras. Por padrão, o Macie envia o convite para você como uma mensagem de e-mail. Macie também cria um evento AWS Health para sua Conta da AWS. Se você já usa o Macie no local Região da AWS de onde o convite foi enviado, o Macie também exibe um selo de Contas e uma notificação no console do Macie.

Depois de receber um convite, você pode, opcionalmente, aceitar ou recusar o convite. Antes de responder, observe o seguinte:

- Você pode ser membro de apenas uma organização por vez. Se receber vários convites, você só poderá aceitar um. Ou, se você já for membro de uma organização, precisará desassociar sua conta da conta atual de administrador do Macie antes de ingressar em uma organização diferente.
- Se você usa o Macie em várias regiões, sua conta precisa ter a mesma conta de administrador do Macie em todas essas regiões. O administrador do Macie precisa enviar convites para você separadamente de cada região, e você precisa aceitar os convites separadamente em cada região.
- Para aceitar ou recusar um convite, você precisa habilitar o Macie na região de onde o convite foi enviado. Recusar um convite é opcional. Se você permitir que o Macie recuse um convite, poderá desativar o Macie na Região depois de recusar o convite. Isso ajuda a garantir que você não incorra em cobranças desnecessárias pelo uso do Macie na região.

Para considerações adicionais, consulte Respondendo e gerenciando convites de associação.

Para responder a um convite de associação para uma organização

Para responder a um convite de associação, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para responder a um convite de associação usando o console do Amazon Macie.

Para responder a um convite de membro

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Ao usar o seletor de Região da AWS no canto superior direito da página, selecione a região da da na qual você recebeu o convite.
3. Se você não habilitou o Macie na região, escolha Começar e, em seguida, escolha Habilitar o Macie. Você precisa ativar o Macie antes de aceitar ou recusar um convite.
4. No painel de navegação, em Settings, selecione Accounts.
5. Em Conta do administrador, faça uma das seguintes ações:

   - Para aceitar o convite, ative Aceitar
     ()
     ao lado do convite. Em seguida, escolha Aceitar convite ou Atualizar, dependendo se você já aceitou outro convite.

- Para recusar o convite, escolha Recusar convite ao lado do convite e confirme que você deseja recusar o convite.

Se você recebeu e deseja responder ao convite em regiões adicionais, repita as etapas anteriores em cada região adicional.

API

Para responder a um convite de forma programática, use a operação AcceptInvitation ou DeclineInvitations da API do Amazon Macie, dependendo se você deseja aceitar ou recusar o convite. Ao enviar sua solicitação, não se esqueça de especificar a região da qual o convite foi enviado. Para responder ao convite em outras regiões, envie sua solicitação em cada região adicional.

Em uma solicitação `AcceptInvitation`, use o parâmetro `administratorAccountId` para especificar o ID da conta de 12 dígitos da Conta da AWS que enviou o convite. Use o parâmetro `invitationId` para especificar a ID exclusiva para aceitação do convite.

Em uma solicitação `DeclineInvitations`, use o parâmetro `accountIds` para especificar o ID da conta de 12 dígitos da Conta da AWS que enviou o convite para recusar.

Para recuperar as IDs, você pode usar a operação ListInvitations da API Amazon Macie. Se a operação for bem-sucedida, o Macie retornará uma matriz `invitations` que fornece detalhes sobre os convites que você recebeu, incluindo o ID da conta que enviou cada convite e o ID exclusivo de cada convite. Se o valor da propriedade `relationshipStatus` de um convite for `Invited`, você ainda não respondeu ao convite.

Para responder a um convite usando o AWS Command Line Interface (AWS CLI), execute o comando accept-invitation ou decline-invitations, dependendo se você deseja aceitar ou recusar o convite. Use o parâmetro `region` para especificar a região da qual o convite foi enviado. Por exemplo:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Onde *us-east-1* é a região da qual o convite foi enviado (a região Leste dos EUA (Norte da Virgínia)), *123456789012* é a ID da conta que enviou o convite, e *d8bdad0e203fd1242e0a4721bexample* é a ID exclusiva do convite a ser aceito.

Se uma solicitação para aceitar um convite for bem-sucedida, Macie retornará uma resposta vazia. Se uma solicitação para recusar um convite for bem-sucedida, o Macie retornará uma matriz `unprocessedAccounts` vazia.

Depois de recusar um convite, o convite persiste como um recurso para sua conta Macie. Opcionalmente, você pode excluí-lo usando a operação DeleteInvitations ou, para o AWS CLI, o comando delete-invitations.

Desassociar de uma conta de administrador do Amazon Macie

Se você aceitar um convite para participar de uma organização no Amazon Macie, poderá posteriormente se demitir da organização desassociando sua conta da conta atual de administrador do Macie. Observe que você não poderá fazer isso se sua conta for uma conta-membro de uma organização do AWS Organizations. Para se demitir de uma organização AWS Organizations, trabalhe com seu administrador do Macie para remover sua conta como conta de membro do Macie.

Se você desassociar sua conta da conta de administrador do Macie, o administrador do Macie perderá o acesso a todas as configurações, dados e recursos da sua conta do Macie. Isso inclui metadados e descobertas de políticas para dados do Amazon S3 que você possui. Isso também significa que o administrador não pode mais analisar seus dados do Amazon S3 executando a descoberta automática de dados confidenciais ou executando trabalhos de descoberta de dados confidenciais.

Quando você desassocia sua conta, o Macie continua habilitado para sua conta na região aplicável. No entanto, sua conta passará a ser uma conta Macie independente da região. O status da sua conta muda para Membro renunciado no inventário da conta do administrador.

Para se desassociar de uma conta de administrador do Macie

Para desassociar sua conta da conta atual de administrador do Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie.

Console

Siga estas etapas para desassociar sua conta da conta de administrador do Macie usando o console do Amazon Macie.

Para se desassociar de uma conta de administrador

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. Ao usar o seletor de Região da AWS no canto superior direito da página, selecione a região da na qual você quer desassociar sua conta da sua conta de administrador.
3. No painel de navegação, em Settings, selecione Contas.
4. Em Conta de administrador, desative Aceitar () ao lado do convite e escolha Atualizar.

A conta continua aparecendo na página Contas. Se você decidir se juntar novamente à organização, poderá usar esta página para aceitar o convite original novamente. Como alternativa, você pode recusar e excluir o convite, o que também exclui a associação entre sua conta e a outra conta. Para fazer isso, escolha Recusar convite.

Se você quiser desassociar sua conta da conta de administrador do Macie em regiões adicionais, repita as etapas anteriores em cada região adicional.

API

Para desassociar sua conta da conta de administrador do Macie de forma programática, use a operação disassociateFromAdministratorAccount da API do Amazon Macie. Ao enviar sua solicitação, não se esqueça de especificar a região à qual a solicitação se aplica. Para se desassociar da conta em outras regiões, envie sua solicitação em cada região adicional.

Para desassociar sua conta da conta de administrador do Macie usando o AWS CLI, execute o comando disassociate-from-administrator-account. Use o parâmetro `region` para especificar a região na qual se desassociar da conta.

Se a sua solicitação for realizada com êxito, Macie retornará uma resposta vazia.

Depois de se desassociar da conta, o convite original persiste como um recurso para sua conta Macie, a menos que você o exclua. Se você decidir se juntar novamente à organização, poderá usar esse recurso para aceitar o convite original novamente. Como alternativa, você pode excluir o convite usando a operação DeleteInvitations ou, para o AWS CLI, o comando delete-invitations. Se você excluir o convite, também excluirá a associação entre sua conta e a outra conta.

Segurança no Amazon Macie

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os Serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Macie, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo Serviços da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Macie. Os tópicos a seguir mostram como configurar o Macie para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros Serviços da AWS que ajudam você a monitorar e proteger os recursos do Macie.

Tópicos

Proteção de dados no Amazon Macie

O AWS modelo de responsabilidade compartilhada é aplicado à proteção de dados no Amazon Macie. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja asConta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os atributos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui trabalhar com o Macie ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os SDKs AWS. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

O Amazon Macie armazena com segurança seus dados em repouso usando soluções de criptografia AWS. O Macie criptografa dados, como descobertas, usando um Chave gerenciada pela AWS do AWS Key Management Service (AWS KMS).

Se você desabilitar o Macie, ele excluirá permanentemente todos os recursos que ele armazena ou mantém para você, como os trabalhos de descoberta de dados confidenciais, os identificadores de dados personalizados e as descobertas.

Criptografia em trânsito

O Macie criptografa todos os dados em trânsito entre Serviços da AWS.

O Amazon Macie analisa dados do Amazon S3 e exporta resultados de descobertas de dados confidenciais para um bucket do S3. Depois que o Macie obtém as informações de que precisa dos objetos do S3, elas são descartadas.

O Macie acessa o Amazon S3 usando um endpoint da VPC desenvolvido por AWS PrivateLink. Portanto, o tráfego entre o Macie e o Amazon S3 permanece na rede da Amazon e não passa pela Internet pública. Para obter mais informações, consulte AWS PrivateLink.

Gestão de acesso e identidade para o Amazon EKS

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Funções vinculadas ao serviço do Amazon Macie
- AWS políticas gerenciadas para o Amazon Macie
- Solução de problemas de identidade e acesso do Amazon Macie

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no .

Usuário do serviço – Se você usar o serviço do Macie para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do Macie para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Macie, consulte Solução de problemas de identidade e acesso do Amazon Macie.

Administrador do serviço – Se você for o responsável pelos recursos do Macie na empresa, provavelmente terá acesso total ao Macie. Cabe a você determinar quais funcionalidades e recursos do Macie os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Analise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Macie, consulte Como o Amazon Macie trabalha com AWS Identity and Access Management.

Administrador do IAM – Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao Macie. Para ver exemplos de políticas baseadas em identidade do Macie que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. Os usuários do AWS IAM Identity Center (IAM Identity Center), a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de

identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no ou no portal de acesso da AWS Management Console dependendo do tipo de usuário que você é.AWS Para obter mais informações sobre como fazer login na AWS, consulte How to sign in to your Conta da AWS (Como fazer login na conta da) no Início de Sessão da AWS User Guide (Guia do usuário do).

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulteAssinar AWSsolicitações de API da noGuia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer

usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar atributos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um

URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Uso de funções do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações.

Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada ao serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou atributo, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfil do AWS Management Console, da AWS CLI ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas embutidas são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em atributos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Como o Amazon Macie trabalha com AWS Identity and Access Management

Antes de usar o AWS Identity and Access Management (IAM) para gerenciar o acesso ao Amazon Macie, saiba quais recursos do IAM estão disponíveis para uso com o Macie.

Atributos do IAM que você pode usar com o Amazon Macie

atributo do IAM	Suporte do Macie
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
atributos de políticas	Sim
Chaves de condição de políticas	Sim
Listas de controle de acesso (ACLs)	Não
Controle de acesso por atributo (ABAC) – tags em políticas	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não

atributo do IAM	Suporte do Macie
Funções vinculadas ao serviço	Sim

Para uma visualização de alto nível de como o Macie e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon Macie

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

O Macie é compatível com políticas com base em identidade. Para ver exemplos, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Políticas baseadas em recursos no Amazon Macie

Oferece suporte a políticas baseadas em recurso	Não

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e

políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o atributo estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o atributo. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma outra política baseada em identidade será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em atributos no Guia do usuário do IAM.

O Macie não é compatível com Políticas baseadas em recursos. Ou seja, você não pode anexar uma política a um recurso do Macie diretamente.

Ações de políticas para o Amazon Macie

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de políticas para o Macie usam o seguinte prefixo antes da ação:

```
macie2
```

Por exemplo, para conceder a permissão a alguém para acessar informações sobre todos os identificadores de dados gerenciados que o Macie fornece, que é uma ação que corresponde à operação `ListManagedDataIdentifiers` na API do Amazon Macie, inclua a ação `macie2:ListManagedDataIdentifiers` na política:

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas. Por exemplo:

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

```
"Action": "macie2:List*"
```

No entanto, como prática recomendada, você deve criar políticas que sigam o princípio de privilégio mínimo. Em outras palavras, você deve criar políticas que incluem somente as permissões necessárias para executar uma tarefa específica.

Para obter uma lista de ações do Macie, consulte Ações definidas pelo Amazon Macie na Referência de autorização do serviço. Para obter exemplos de políticas que especificam ações do Macie, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Recursos de políticas para o Amazon Macie

Oferece suporte a atributos de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um atributo usando seu Nome do atributo da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

O Macie define os seguintes tipos de recursos:

- Lista de permissões
- Identificador de dados personalizado
- Regra de filtro ou supressão, também conhecidas como um filtro de descobertas
- Conta-membro
- Trabalho de descoberta de dados confidenciais, também conhecido como trabalho de classificação

Você pode especificar esses tipos de recurso nas políticas usando ARNs.

Por exemplo, para criar uma política para o trabalho de descoberta de dados confidenciais que tenha o ID do trabalho 3ce05dbb7ec5505def334104bexample, você pode usar o seguinte ARN:

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

Ou, para especificar todos os trabalhos de descoberta de dados confidenciais para uma determinada conta, use um caractere curinga (*):

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

Onde *123456789012* é o ID da conta para o Conta da AWS que criou os trabalhos. No entanto, como prática recomendada, você deve criar políticas que sigam o princípio de privilégio mínimo. Em outras palavras, você deve criar políticas que incluem somente as permissões necessárias para executar uma tarefa específica em um recurso específico.

Algumas ações do Macie podem ser aplicadas a vários recursos. Por exemplo, a ação `macie2:BatchGetCustomDataIdentifiers` pode recuperar os detalhes de vários

identificadores de dados personalizados. Nesses casos, a entidade principal deve ter permissões para acessar todos os recursos aos quais a ação se aplica. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas:

```
"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 uma lista dos tipos de recursos do Macie e a sintaxe dos ARNs para cada um, consulte Tipos de recursos definidos pelo Amazon Macie na Referência de autorização do serviço. Para saber quais ações você pode especificar com cada tipo de recurso, consulte Ações definidas pelo Amazon Macie na Referência de autorização do serviço. Para obter exemplos de políticas que especificam os recursos, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Chaves de condição de política para o Amazon Macie

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode utilizar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver

marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte AWSChaves de contexto de condição globais da no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Amazon Macie, consulte Chaves de condição do Amazon Macie na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pelo Amazon Macie. Para obter exemplos de políticas que usam chaves de condição, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Listas de controle de acesso (ACLs) no Amazon Macie

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

O Amazon Simple Storage Service (Amazon S3) é um exemplo de um AWS service (Serviço da AWS) que oferece suporte a ACLs. Para saber mais, consulte Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon Simple Storage Service.

O Macie não é compatível com ACLs. Ou seja, você não pode anexar um ACL a um recurso do Macie.

Controle de acesso por atributo (ABAC) com o Amazon Macie

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir

operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Você pode anexar tags aos recursos do Macie — listas de permissões, identificadores de dados personalizados, regras de filtro e regras de supressão, contas-membro e trabalhos de descoberta de dados confidenciais. Você também pode controlar o acesso a esses tipos de recursos fornecendo informações de tag no elemento `Condition` de uma política. Para obter informações sobre a marcação de recursos com tags no Macie, consulte Marcar recursos do Amazon Macie. Para obter um exemplo de uma política baseada em identidade que controla o acesso a um recurso com base em tags, consulte Exemplos de políticas baseadas em identidade para o Amazon Macie.

Usando credenciais temporárias com o Amazon Macie

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais

temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

O Macie oferece suporte ao uso de credenciais temporárias.

Sessões de acesso direto para o Amazon Macie

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

O Macie faz solicitações do FAS aos Serviços da AWS downstream quando você realiza as seguintes tarefas:

- Criar ou atualizar as configurações do Macie para uma lista de permissões armazenada em um bucket do S3.
- Verificar o status de uma lista de permissões armazenada em um bucket do S3.
- Recuperar amostras de dados confidenciais de um objeto afetado do S3 usando as credenciais de usuário do IAM.
- Criptografar amostras de dados confidenciais que são recuperadas usando credenciais de usuário do IAM ou um perfil do IAM.
- Permitir que o Macie se integre com o AWS Organizations.

- Designar a conta de administrador delegada do Macie para uma organização no AWS Organizations.

Para outras tarefas, o Macie usa um perfil vinculado a serviço para executar ações em seu nome. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço do Amazon Macie.

Perfis de serviço para o Amazon Macie

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

O Macie não assume nem usa perfis de serviço. Para executar ações em seu nome, o Macie usa basicamente um perfil vinculado a serviço. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço do Amazon Macie.

Perfis vinculados ao serviço para Amazon Macie

Oferece suporte a perfis vinculados ao serviço	Sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

O Macie usa um perfil vinculada ao serviço para executar ações em seu nome. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço do Amazon Macie.

Exemplos de políticas baseadas em identidade para o Amazon Macie

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Macie. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a AWS API. Para conceder aos usuários permissão para executar

ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Macie, incluindo o formato dos ARNs para cada tipo de recurso, consulte Ações, recursos e chaves de condição do Amazon Macie na Referência de autorização do serviço.

Ao criar uma política, solucione avisos de segurança, erros, avisos gerais e sugestões de AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) antes de salvar a política. O IAM Access Analyzer executa verificações de política para validar uma política em relação à gramática das políticas e às práticas recomendadas do IAM. Essas verificações geram descobertas e fornecem recomendações práticas que ajudam a criar políticas que sejam funcionais e estejam em conformidade com as práticas recomendadas de segurança. Para saber sobre a validação de políticas usando o IAM Access Analyzer, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM. Para rever uma lista de avisos, erros e sugestões que o IAM Access Analyzer pode retornar, consulte Referência de verificação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

Tópicos

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Macie em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Require multi-factor authentication (MFA) (Exigir autenticação multifator (MFA)): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usando o console do Amazon Macie

Para acessar o console do Amazon Macie, você deve ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e visualize detalhes sobre os recursos do Macie na sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que estão tentando executar.

Para garantir que usuários e funções possam usar o console do Amazon Macie, crie políticas do IAM que forneçam acesso ao console. Para ter mais informações, consulte Políticas e permissões no IAM, no Guia do usuário do IAM.

Se você criar uma política que permita que usuários ou funções usem o console do Amazon Macie, certifique-se de que a política permita a ação `macie2:GetMacieSession`. Caso contrário, esses usuários ou perfis não poderão acessar nenhum recurso ou dado do Macie no console.

Certifique-se também de que a política permita as ações `macie2:List` adequadas para os recursos que esses usuários ou perfis precisam acessar no console. Caso contrário, eles não conseguirão navegar ou exibir detalhes sobre esses recursos no console. Por exemplo, para rever os detalhes de um trabalho de descoberta de dados confidenciais usando o console, o usuário deve ter permissão para realizar a ação `macie2:DescribeClassificationJob` do trabalho e da ação `macie2:ListClassificationJobs`. Se um usuário não tiver permissão para realizar a ação `macie2:ListClassificationJobs`, ele não poderá exibir uma lista de trabalhos na página Trabalhos do console e, portanto, não poderá escolher um trabalho para exibir seus detalhes. Para que os detalhes incluam informações sobre um identificador de dados personalizado usado pelo trabalho, o usuário também deve ter permissão para realizar a ação `macie2:BatchGetCustomDataIdentifiers` do identificador de dados personalizado.

Exemplo: permita que os usuários revejam suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da 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": "*"
        }
    ]
}
```

Exemplo: permita que os usuários criem trabalhos de descoberta de dados confidenciais

Este exemplo mostra como você pode criar uma política que permita que um usuário crie trabalhos de descoberta de dados confidenciais.

No exemplo, a primeira instrução concede permissões `macie2:CreateClassificationJob` ao usuário. Essas permissões autorizam o usuário a criar trabalhos. A instrução também concede permissões `macie2:DescribeClassificationJob`. Essas permissões autorizam o usuário a acessar os detalhes dos trabalhos existentes. Embora essas permissões não sejam necessárias

para criar trabalhos, o acesso a esses detalhes pode ajudar o usuário a criar trabalhos com configurações exclusivas.

A segunda instrução no exemplo permite que o usuário crie, configure e revise trabalhos usando o console do Amazon Macie. As permissões `macie2:ListClassificationJobs` autorizam o usuário a exibir trabalhos existentes na página Trabalhos do console. Todas as outras permissões na instrução permitem que o usuário configure e crie um trabalho usando as páginas Criar trabalho no console.

```
{
    "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": "*"
        }
    ]
}
```

Exemplo: permita que os usuários gerenciem um trabalho de descoberta de dados confidenciais

Este exemplo mostra como criar uma política que permite que um usuário acesse os detalhes de um determinado trabalho de descoberta de dados confidenciais, o trabalho cujo ID é

`3ce05dbb7ec5505def334104bexample`. O exemplo também permite que o usuário altere o status do trabalho conforme necessário.

A primeira instrução do exemplo concede permissões `macie2:DescribeClassificationJob` e `macie2:UpdateClassificationJob` ao usuário. Essas permissões autorizam o usuário a recuperar os detalhes do trabalho e alterar o status do trabalho, respectivamente. A segunda instrução concede permissões `macie2:ListClassificationJobs` ao usuário, autorizando o usuário a acessar o trabalho usando a página Trabalhos no console do 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": "*"
 }
   ]
}
```

Você também pode permitir que o usuário acesse dados de registro (eventos de log) que o Macie publica no Amazon CloudWatch Logs para o trabalho. Para fazer isso, você pode adicionar instruções que concedem permissões para realizar ações no CloudWatch Logs (`logs`) no grupo de logs e no stream do trabalho. Por exemplo:

```
"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 obter informações sobre o gerenciamento de acesso ao CloudWatch Logs, consulte Visão geral do gerenciamento de permissões de acesso aos recursos do CloudWatch Logs no Guia do usuário do Amazon CloudWatch Logs.

Exemplo: permita que os usuários revisem as descobertas

Este exemplo mostra como criar uma política que permite que um usuário acesse os dados da descoberta.

Neste exemplo, as permissões `macie2:GetFindings` e `macie2:GetFindingStatistics` autorizam o usuário a recuperar os dados usando a API do Amazon Macie ou o console do Amazon Macie. As permissões `macie2:ListFindings` autorizam o usuário a recuperar e revisar os dados usando o painel de Resumo e as páginas de Descobertas no console do Amazon Macie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Você também pode permitir que o usuário crie e gerencie regras de filtro e regras de supressão para descobertas. Para fazer isso, você pode incluir uma instrução que conceda as seguintes permissões: `macie2:CreateFindingsFilter`, `macie2:GetFindingsFilter`, `macie2:UpdateFindingsFilter` e `macie2:DeleteFindingsFilter`. Para permitir que o usuário gerencie as regras usando o console do Amazon Macie, inclua também as permissões `macie2:ListFindingsFilters` na política. Por exemplo:

```
{
    "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": "*"
        }
    ]
```

```
}
```

Exemplo: permita que os usuários revisem identificadores de dados personalizados com base em tags

Nas política baseadas em identidade, você pode usar condições para controlar o acesso aos recursos do Amazon Macie com base em tags. Este exemplo mostra como você pode criar uma política que permite que um usuário revise os identificadores de dados personalizados usando o console do Amazon Macie ou a API do Amazon Macie. No entanto, a permissão é concedida somente se o valor da tag `Owner` for o nome de usuário do usuário.

```
{
    "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}"}
            }
        }
    ]
}
```

Neste exemplo, se um usuário com o nome de usuário `richard-roe` tentar revisar os detalhes de um identificador de dados personalizado, o identificador de dados personalizado deverá ser marcado com uma tag como `Owner=richard-roe` ou `owner=richard-roe`. Caso contrário, o usuário terá o acesso negado. A chave da tag de condição `Owner` corresponde a `Owner` e a `owner` porque os nomes de chaves de condição não fazem distinção entre maiúsculas e minúsculas. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

Funções vinculadas ao serviço do Amazon Macie

O Amazon Macie usa uma função vinculada ao serviço AWS Identity and Access Management (IAM) chamada. `AWSServiceRoleForAmazonMacie` A função vinculada ao serviço é uma função única do IAM vinculada diretamente ao Macie. É predefinido pelo Macie e inclui todas as permissões que o Macie exige para ligar para outras pessoas Serviços da AWS e monitorar AWS recursos em seu nome. O Macie usa essa função vinculada ao serviço em todos os Regiões da AWS em que o Macie está disponível.

Uma função vinculada ao serviço facilita a configuração do Macie, já que não é preciso adicionar as permissões necessárias manualmente. O Macie define as permissões dessa função vinculada ao serviço e, a menos que definido em contrário, só o Macie pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM. Você só pode excluir uma função vinculada a serviços após excluir seus recursos relacionados. Isso protege seus recursos porque você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas a serviços. Escolha um Sim com um link para analisar a documentação da função vinculada a esse serviço.

Tópicos

Permissões de função vinculada ao serviço para o Amazon Macie.

O Amazon Macie usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonMacie`. Essa função vinculada ao serviço confia no serviço `macie.amazonaws.com` para assumir a função.

A política de permissões para a função, denominada`AmazonMacieServiceRolePolicy`, permite que o Macie execute tarefas como as seguintes nos recursos especificados:

- Use as ações do Amazon S3 para recuperar informações sobre buckets e objetos do S3.
- Use as ações do Amazon S3 para recuperar objetos do S3.
- Use AWS Organizations ações para recuperar informações sobre contas associadas.
- Use as ações do Amazon CloudWatch Logs para registrar eventos para trabalhos confidenciais de descoberta de dados.

A função é configurada com a política de permissões abaixo.

```
{
  "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 obter detalhes sobre atualizações da `AmazonMacieServiceRolePolicy`política, consulte Atualizações do Amazon Macie para políticas gerenciadas AWS. Para receber alertas automáticos sobre mudanças nessa política, assine o feed RSS na página de histórico de documentos do Macie.

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário ou uma função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para o Amazon Macie

Você não precisa criar manualmente as `AWSServiceRoleForAmazonMacie` funções vinculadas ao serviço para o Amazon Macie. Quando você ativa o Macie para você Conta da AWS, o Macie cria automaticamente a função vinculada ao serviço para você.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Quando você habilita o Macie novamente, o Macie cria a função vinculada ao serviço para você novamente.

Editar uma função vinculada ao serviço para o Amazon Macie.

O Amazon Macie não permite que você edite a função vinculada ao serviço `AWSServiceRoleForAmazonMacie`. Após a criação da função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir a função vinculada ao serviço do Amazon Macie

Se você não precisa mais usar o Amazon Macie, recomendamos que exclua a função vinculada ao serviço `AWSServiceRoleForAmazonMacie`. Quando você desabilita o Macie, ele não exclui a função para você.

Antes de excluir a função, você deve desativar o Macie em cada Região da AWS local em que você a habilitou. Você também deve limpar manualmente os recursos da função. Para excluir a função, você pode usar o console do IAM AWS CLI, o ou a AWS API. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

> **Note**
>
> Se o Macie estiver usando a `AWSServiceRoleForAmazonMacie` função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Se excluir a função `AWSServiceRoleForAmazonMacie` vinculada ao serviço e precisar criá-la novamente, você poderá criá-la novamente ativando o Macie para sua conta. Quando você habilita o Macie novamente, o Macie cria a função vinculada ao serviço para você novamente.

Compatível com Regiões da AWS a função vinculada ao serviço Amazon Macie

O Amazon Macie oferece suporte ao uso da função `AWSServiceRoleForAmazonMacie` vinculada ao serviço em todos os Regiões da AWS lugares em que o Macie está disponível. Para obter uma lista de todas as regiões onde o Macie está disponível no momento, consulte endpoints do Amazon Macie e cotas no Referência geral da AWS.

AWS políticas gerenciadas para o Amazon Macie

Uma política gerenciada AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

O Amazon Macie fornece várias políticas AWS gerenciadas: a política `AmazonMacieFullAccess`, a política `AmazonMacieReadOnlyAccess`, e a política `AmazonMacieServiceRolePolicy`.

Tópicos

- Política gerenciada AWS: AmazonMacieFullAccess
- Política gerenciada AWS: AmazonMacieReadOnlyAccess
- Política gerenciada AWS: AmazonMacieServiceRolePolicy
- Atualizações do Amazon Macie para políticas gerenciadas AWS

Política gerenciada AWS: AmazonMacieFullAccess

Você pode anexar a política `AmazonMacieFullAccess` às suas entidades do IAM.

Essa política concede permissões administrativas completas que permitem que uma identidade do IAM (entidade principal) crie a função vinculada ao serviço Amazon Macie e execute todas as ações de leitura e gravação para o Amazon Macie. As permissões incluem alterações nas funções, como criar, atualizar e excluir funções. Se essa política for anexada a uma entidade principal, a entidade

principal poderá criar, recuperar e acessar todos os recursos, dados e configurações do Macie de sua conta.

Essa política deve ser anexada a uma entidade principal antes que a entidade principal possa habilitar o Macie para sua conta — uma entidade principal deve ter permissão para criar a função vinculada ao serviço do Macie para habilitar o Macie para sua conta.

Detalhes da permissão

Esta política inclui as seguintes permissões:

- `macie2`: permite que as entidades principais realizem todas as ações de leitura e gravação do Amazon Macie.
- `iam`: permite que as entidades principais criem funções vinculadas a serviços. O elemento `Resource` especifica a função vinculada ao serviço do Macie. O elemento `Condition` usa a chave de `iam:AWSServiceName` condição e o operador de `StringLike` condição para restringir as permissões à função vinculada ao serviço para Macie.
- `pricing`: permite que as entidades principais recuperem dados de preços para seu Conta da AWS de AWS Billing and Cost Management. O Macie usa esses dados para calcular e exibir os custos estimados quando as entidades principais criam e configuram trabalhos confidenciais de descoberta de dados.

```
{
   "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 gerenciada AWS: AmazonMacieReadOnlyAccess

Você pode anexar a política do `AmazonMacieReadOnlyAccess` às suas entidades do IAM.

Essa política concede permissões somente de leitura que permitem que uma identidade do IAM (entidade principal) execute todas as ações de leitura para o Amazon Macie. As permissões não incluem alterações nas funções, como criar, atualizar e excluir funções. Se essa política for anexada a uma entidade principal, a entidade principal poderá criar, recuperar e acessar todos os recursos, dados e configurações do Macie de sua conta.

Detalhes da permissão

Esta política inclui as seguintes permissões:

`macie2`: permite que as entidades principais realizem todas as ações de leitura do Amazon Macie.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
```

```
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

Política gerenciada AWS: AmazonMacieServiceRolePolicy

Não é possível anexar a política `AmazonMacieServiceRolePolicy` às suas entidades do IAM. Essa política está anexada a uma função vinculada ao serviço que permite que o Macie execute ações em seu nome. Para obter mais informações, consulte Funções vinculadas ao serviço do Amazon Macie.

Atualizações do Amazon Macie para políticas gerenciadas AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o Amazon Macie desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na página doHistórico de documentos do Macie.

Alteração	Descrição	Data
AmazonMacieReadOnlyAccess - Adicionou uma nova política	Macie adicionou uma nova política: a política `AmazonMacieReadOnlyAccess` . Essa política concede permissões somente de leitura que permitem que as entidades principais recuperem todos os recursos, dados e configurações do Macie de suas contas.	15 de junho de 2023
AmazonMacieFullAccess - Atualizou uma política existente	Na `AmazonMacieFullAccess` política, o Macie atualizou o nome do recurso	30 de junho de 2022

Alteração	Descrição	Data
	da Amazon (ARN) da função vinculada ao serviço do Macie (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	
AmazonMacieServiceRolePolicy - Atualizou uma política existente	Macie removeu ações e recursos do Amazon Macie Classic da política `AmazonMacieServiceRolePolicy` . O Amazon Macie Classic foi descontinuado e não está mais disponível. Mais especificamente, Macie removeu todas as ações AWS CloudTrail. Macie também removeu todas as ações do Amazon S3 para os seguintes recursos: `arn:aws:s3:::awsmacie-*` , `arn:aws:s3:::awsmacietrail-*` e `arn:aws:s3:::*-awsmacietrail-*` .	20 de maio de 2022

Alteração	Descrição	Data
AmazonMacieFullAccess - Atualizou uma política existente	Macie adicionou uma ação AWS Billing and Cost Management (`pricing`) à `AmazonMacieFullAccess` política. Essa ação permite que as entidades principais recuperem dados de preços para sua conta. O Macie usa esses dados para calcular e exibir os custos estimados quando as entidades principais criam e configuram trabalhos confidenciais de descoberta de dados. Macie também removeu ações e recursos do Amazon Macie Classic (`macie`) da política `AmazonMacieFullAccess` .	7 de março de 2022
AmazonMacieServiceRolePolicy - Atualizou uma política existente	Macie adicionou ações do Amazon CloudWatch Logs à política `AmazonMacieServiceRolePolicy` . Essas ações permitem que o Macie publique eventos de log no CloudWatch Logs para trabalhos confidenciais de descoberta de dados.	13 de abril de 2021
O Macie começou a rastrear alterações	O Macie passou a rastrear as alterações para suas políticas gerenciadas AWS.	13 de abril de 2021

Solução de problemas de identidade e acesso do Amazon Macie

As seguintes informações podem ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o e o Amazon Macie e o AWS Identity and Access Management (IAM).

Tópicos

Não estou autorizado a executar uma ação no Amazon Macie

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso *`my-example-widget`* fictício, mas não tem as permissões `macie2:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `macie2:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu a você suas credenciais de login.

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Amazon Macie

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte o seguinte:

- Para saber se o Macie oferece suporte a esses recursos, consulte Como o Amazon Macie trabalha com AWS Identity and Access Management.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Registrar em log e monitorar no Amazon Macie

O Amazon Macie é integrado ao AWS CloudTrail, um serviço que fornece um registro de ações que foram executadas no Macie por um usuário, uma função ou outro AWS service (Serviço da AWS). Isso inclui ações do console do Amazon Macie e chamadas programáticas às operações de API do Amazon Macie. Ao usar as informações coletadas pelo CloudTrail, é possível determinar quais solicitações foram feitas ao Macie. Para cada solicitação é possível identificar quando ela foi realizada, o endereço IP do qual foi feita, quem fez a solicitação e detalhes adicionais. Para obter mais informações, consulte Registre chamadas de API do Amazon Macie usando o AWS CloudTrail.

Validação de conformidade para o Amazon Macie

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports inAWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos

regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse estudo técnico descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

> **Note**
>
> Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar atributos com regras no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no Amazon Macie

A infraestrutura global da AWS é criada com base em Regiões da AWS e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global da AWS.

Segurança da infraestrutura no Amazon Macie

Como um serviço gerenciado, o Amazon Macie é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Macie por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Amazon Macie e endpoint da VPC de interface (AWS PrivateLink)

Se você usar a Amazon Virtual Private Cloud (Amazon VPC) para hospedar os recursos da AWS, poderá estabelecer uma conexão privada entre a VPC e o Amazon Macie. A Amazon VPC é um

AWS service (Serviço da AWS) que pode ser utilizado para iniciar os recursos da AWS em uma rede virtual definida por você. Com a VPC, você tem controle sobre as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede.

Para conectar sua VPC ao Macie, basta criar um endpoint da VPC de interface para o Macie. Os endpoints de interface são habilitados por AWS PrivateLink, uma tecnologia que permite acessar de forma privada as APIs do Amazon Macie sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com as APIs do Amazon Macie. O tráfego entre sua VPC e o Macie não deixa a rede da Amazon.

Cada endpoint de interface é representado por uma ou mais interfaces de rede elástica nas sub-redes. Para obter mais informações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint da VPC de interface, no Guia do usuário do Amazon VPC.

Tópicos

- Considerações sobre endpoints da VPC do Amazon ECS
- Criar um endpoint da VPC de interface para a API do Amazon Macie

Considerações sobre endpoints da VPC do Amazon ECS

O Amazon Macie é compatível com os endpoints da VPC em todas as Regiões da AWS em que está atualmente disponível, salvo nas regiões Asia Pacific (Osaka) e Israel (Tel Aviv). Para obter uma lista de todas as regiões onde o está disponível no momento, consulte os endpoints e quotas do Amazon Macie no Referência geral da AWS. Além disso, o Macie oferece suporte a chamadas para todas as ações de API de uma VPC.

Se você criar uma endpoint da VPC de interface para o Macie, considere fazer o mesmo com outros Serviços da AWS que forneçam suporte à VPC e se integrem ao Macie, como o Amazon EventBridge e AWS Security Hub. O Macie e esses serviços podem, então, usar os endpoints da VPC para a integração. Por exemplo, se você criar um endpoint da VPC para o Macie e um endpoint da VPC para o Security Hub, o Macie poderá usar seu endpoint da VPC ao publicar descobertas no Security Hub e o Security Hub poderá usar seu endpoint da VPC ao receber as descobertas. Para obter informações sobre serviços que oferecem suporte a endpoints da VPC, consulte Serviços da AWSessa integração com AWS PrivateLink no Guia do usuário do Amazon VPC.

Para outras considerações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint da VPC de interface, no Guia do usuário do Amazon VPC.

Observe que as políticas do endpoint da VPC não são compatíveis com o Macie. Por padrão, o acesso total ao Macie é permitido pelo endpoint. Para obter mais informações, consulte Gerenciamento de identidade e acesso para endpoints da VPC e serviços do endpoint da VPC no Guia do usuário do Amazon VPC.

Criar um endpoint da VPC de interface para a API do Amazon Macie

É possível criar um endpoint da VPC de interface para o serviço Amazon Macie usando o console do Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Crie um endpoint da VPC no Guia do usuário do Amazon VPC.

Ao criar um endpoint da VPC para o Macie, use o seguinte nome de serviço:

- com.amazonaws.*region*.macie2

Onde *região* é o código da Região para o Região da AWS pertinente.

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o Macie usando seu nome DNS padrão para a Região, por exemplo, `macie2.us-east-1.amazonaws.com` para a Região Leste dos EUA (Norte da Virgínia).

Para obter mais informações, consulte Acessar um AWS service (Serviço da AWS) usando um endpoint da VPC de interface , no Guia do usuário do Amazon VPC.

Registre chamadas de API do Amazon Macie usando o AWS CloudTrail

O Amazon Macie é integrado ao AWS CloudTrail, um serviço que fornece um registro de ações que foram executadas no Macie por um usuário, uma função ou outro AWS service (Serviço da AWS). O CloudTrail captura as chamadas de API do Macie como eventos. As chamadas capturadas incluem as chamadas do console do Amazon Macie e as chamadas programáticas para operações da API do Amazon Macie.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para o Macie. Se não configurar uma trilha, você ainda poderá analisar os eventos mais recentes no Histórico de eventos do console do AWS CloudTrail. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Macie, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Tópicos

- Informações sobre o Amazon Macie em AWS CloudTrail
- Noções básicas sobre entradas de arquivos de log do Amazon Macie

Informações sobre o Amazon Macie em AWS CloudTrail

AWS CloudTrail é habilitado em sua Conta da AWS quando você cria a conta. Quando ocorre uma atividade no Amazon Macie, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS no Histórico de eventos. Você pode analisar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Trabalhar com histórico de eventos do CloudTrail no Guia do usuário do AWS CloudTrail.

Para obter um registro contínuo de eventos em sua Conta da AWS, inclusive eventos do Macie, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon Simple Storage Service (Amazon S3). Por padrão, quando você cria uma trilha no console AWS CloudTrail, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log ao bucket do S3 que você especificar. Além disso,

você pode configurar outros Serviços da AWS para analisar melhor e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail:

- Criar uma trilha para a sua Conta da AWS
- Serviços e integrações compatíveis com o CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões
- Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Macie são registradas pelo CloudTrail e documentadas na Referência de API do Amazon Macie. Por exemplo, chamadas para as ações `CreateClassificationJob`, `DescribeBuckets` e `ListFindings` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail no Guia do usuário do AWS CloudTrail.

Noções básicas sobre entradas de arquivos de log do Amazon Macie

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon Simple Storage Service (Amazon S3) que você especifica. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e hora da ação, parâmetros de solicitação etc. Os arquivos de log do AWS CloudTrail contêm uma ou mais entradas de log para eventos. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto não são exibidos em uma ordem específica.

Os exemplos a seguir mostram entradas de log do CloudTrail que demonstram eventos para ações do Amazon Macie. Para obter detalhes sobre as informações que uma entrada de log pode conter, consulte Referência de evento de logs do CloudTrail no Guia do usuário do AWS CloudTrail.

Exemplo: listagem de descobertas

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra um evento para a ação ListFindings do Macie. Neste exemplo, um usuário do AWS Identity and Access Management (IAM) (`Mary_Major`) usou o console do Amazon Macie para recuperar um subconjunto de informações sobre as descobertas atuais da política para sua conta.


```
{
    "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"
}
```

Exemplo: como recuperar amostras de dados confidenciais para uma descoberta

Este exemplo mostra entradas de log do CloudTrail que demonstram eventos para recuperar e revelar amostras de dados confidenciais que o Macie relatou em uma descoberta. Neste exemplo, um usuário do IAM (`JohnDoe`) usou o console do Amazon Macie para recuperar e revelar amostras de dados confidenciais. A conta do Macie do usuário está configurada para assumir um perfil do IAM (`MacieReveal`) para recuperar e revelar amostras de dados confidenciais.

O evento de log a seguir mostra detalhes sobre a solicitação do usuário para recuperar e revelar amostras de dados confidenciais executando a ação GetSensitiveDataOccurrences do 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"
}
```


O próximo evento de logs mostra detalhes sobre o Macie assumindo o perfil do IAM especificado (`MacieReveal`) executando a ação AssumeRole do AWS Security Token Service (AWS STS).


```
{
    "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"
}
```

Marcar recursos do Amazon Macie

Uma tag é um rótulo opcional que você pode definir e atribuir a recursos da AWS, incluindo certos tipos de recursos do Amazon Macie. As tags podem ajudar você a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Por exemplo, você pode usar tags para aplicar políticas, alocar custos, distinguir entre versionamentos de recursos ou identificar recursos que suportam determinados requisitos ou fluxos de trabalho.

Você pode atribuir tags aos seguintes tipos de recursos do Macie: listas de permissões, identificadores de dados personalizados, regras de filtro e regras de supressão para descobertas e trabalhos de descoberta de dados confidenciais. Se você for o administrador do Macie de uma organização, também poderá atribuir tags às contas dos membros na sua organização.

Tópicos

Fundamentos da marcação com tags

Um recurso pode ter até 50 tags. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional, ambos definidos por você. Uma chave de tag é um rótulo geral que atua como uma categoria para um valore de tag mais específico. Um valor de tag atua como um descritor de uma chave de tag.

Por exemplo, se você criar identificadores de dados personalizados e trabalhos de descoberta de dados para analisar dados em diferentes pontos de um fluxo de trabalho (um conjunto para dados em estágios e outro para dados de produção), você pode atribuir uma chave de tag `Stack` a esses recursos. O valor da tag dessa chave de tag pode ser `Staging` para identificadores de dados personalizados e trabalhos projetados para analisar dados em estágios e `Production` para os outros.

Ao definir e atribuir tags aos recursos, lembre-se do seguinte:

- Cada recurso pode ter um máximo de 50 etiquetas.
- Em cada recurso, cada chave de tag deve ser única e pode ter apenas um valor de tag.
- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Como melhor prática, recomendamos definir uma estratégia para letras maiúsculas em etiquetas e implementá-las de forma consistente em todos os tipos de recursos.
- Uma chave de tag pode ter no máximo 128 caracteres UTF-8. Um valor de tag pode ter no máximo 256 caracteres UTF-8. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @
- O prefixo `aws:` é reservado para uso da AWS. Você não pode usá-lo em nenhuma chave ou valor de tag que você definir. Além disso, você não pode editar ou remover chaves de tag ou valores que usam esse prefixo. As tags que usam esse prefixo não contam com a cota de 50 tags por recurso.
- Todas as tags que você atribuir estão disponíveis somente para a sua Conta da AWS e somente na Região da AWS em que você as atribui.
- Se você excluir um recurso, todas as tags associadas ao recurso também serão excluídas.

Para obter mais restrições, dicas e melhores práticas, consulte o Guia do usuário dos recursos de tags da AWS.

> **Important**
>
> Não armazene dados confidenciais ou outros tipos de dados sensíveis em tags. As tags são acessíveis a partir de muitos Serviços da AWS, incluindo AWS Billing and Cost Management. As tags não devem ser usadas para dados confidenciais.

Para adicionar e gerenciar tags para recursos do Macie, você pode usar o console do Amazon Macie, a API do Amazon Macie, o editor de tags no console AWS Resource Groups ou a API de tags AWS Resource Groups. Com o Macie você pode adicionar tags aos recursos ao criá-los. Você também pode adicionar e gerenciar tags para recursos individuais existentes. Com o Resource Groups, você pode adicionar e gerenciar tags em massa para vários recursos existentes, abrangendo vários Serviços da AWS, incluindo o Macie. Para obter mais informações, consulte o Guia do usuário de recursos da AWS para tags.

Usando tags nas políticas do IAM

Depois de começar a marcar recursos, você pode definir permissões baseadas em tags no nível de recurso nas políticas do (IAM) AWS Identity and Access Management. Usando as tags dessa forma, é possível implementar um controle granular de quais usuários e funções na sua conta Conta da AWS têm permissão para criar e marcar recursos com tags, e quais grupos e usuários têm permissão para adicionar, editar e remover tags de maneira geral. Para controlar o acesso com base em tags, você pode usar as chaves de condição relacionadas tags no Elemento de condição das políticas do IAM.

Por exemplo, é possível criar uma política para permitir que um usuário tenha acesso completo a todos os recursos do Amazon Macie se a tag `Owner` para o recurso especificar seus nomes de usuário:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Se você definir permissões em nível de recurso e baseadas em tag, as permissões entrarão em vigor imediatamente. Isso significa que seus recursos ficam mais seguros assim que são criados, e você pode começar a aplicar rapidamente o uso de tags para novos recursos. Você também pode usar permissões em nível de recurso para controlar quais valores e chaves de tag podem ser associados a recursos novos e existentes. Para obter mais informações, consulte Controlar o acesso aos recursos da AWS usando tags no Guia do usuário do IAM.

Adicionar tags aos recursos do Amazon Macie

Para adicionar tags a um recurso individual do Amazon Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Para adicionar tags a vários recursos do Macie ao mesmo tempo, use o Editor de tags no console AWS Resource Groups ou as operações de tags da API de tags AWS Resource Groups.

> **Important**
>
> A adição de tags a um recurso pode afetar o acesso ao recurso. Antes de adicionar uma tag a um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar tags para controlar o acesso aos recursos.

Console

Quando você cria uma lista de permissões, um identificador de dados personalizados, ou um trabalho de descoberta de dados confidenciais, o console do Amazon Macie fornece opções para adicionar tags ao recurso. Siga as instruções no console para adicionar tags a esses tipos de recursos ao criar os recursos. Para adicionar tags a uma regra de filtro ou supressão, ou a uma conta de membro em uma organização, você precisa criar o recurso antes de adicionar tags a ele.

Para adicionar uma ou mais tags a um recurso existente usando o console do Amazon Macie, siga estas etapas.

Adiciona uma tag a um recurso

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Dependendo do tipo de recurso ao qual você quer adicionar uma tag, realize uma das seguintes ações:

   - Para uma lista de permissões, selecione Listas de permissões no painel de navegação.

     Em seguida, marque a caixa de seleção para essa lista na tabela. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para um identificador de dados personalizado, selecione Identificadores de dados personalizados no painel de navegação.

Em seguida, na tabela, marque a caixa de seleção do identificador de dados personalizados. Em seguida, selecione Gerenciar tags no menu Ações.

- Para uma regra de filtro ou supressão, selecione Descobertas no painel de navegação.

  Em seguida, na lista de Regras salvas, selecione o ícone de edição (✎) ao lado da regra. Em seguida, selecione Gerenciar tags.

- Para uma conta de membro em sua organização, selecione Contas no painel de navegação.

  Em seguida, na tabela, marque a caixa de seleção para essa conta. Em seguida, selecione Gerenciar tags no menu Ações.

- Para um trabalho de descoberta de dados confidenciais, selecione Trabalhos no painel de navegação.

  Em seguida, marque a caixa de seleção para essa trabalho na tabela. Em seguida, selecione Gerenciar tags no menu Ações.

A janela Gerenciar tags lista todas as tags atualmente atribuídas ao recurso.

3. Na janela Gerenciar tags, selecione Editar tags.
4. Escolha Adicionar tag.
5. Na caixa Chave, insira a chave da tag a ser adicionada ao recurso. Em seguida, na caixa Valor, você tem a opção de inserir o valor da tag.

   Uma chave de tag pode ter até 128 caracteres. Um valor de tag pode conter até 256 caracteres. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @
6. (Opcional) Para adicionar outra tag ao recurso, selecione Adicionar tag e repita a etapa anterior. É possível atribuir até 50 tags a um recurso.
7. Quando terminar de adicionar tags, selecione Salvar.

API

Para criar um recurso e adicionar a ele uma ou mais tags programaticamente, use a operação `Create` apropriada para o tipo de recurso que você deseja criar:

- Lista de permissões – Use a operação CreateAllowList ou, se estiver usando a AWS Command Line Interface (AWS CLI), execute o comando create-allow-list.
- Identificador de dados personalizados – Use a operação CreateCustomDataIdentifier ou, se estiver usando o AWS CLI, execute o comando create-custom-data-identifier.
- Regra de filtro ou supressão – Use a operação CreateFindingsFilter ou, se estiver usando a AWS CLI, execute o comando create-findings-filter.
- Conta de membro – Use a operação CreateMember ou, se estiver usando a AWS CLI, execute o comando create-member.
- Trabalho de descoberta de dados confidenciais – use a operação CreateClassificationJob ou, se estiver usando a AWS CLI, execute o comando create-classification-job.

Em sua solicitação, use o parâmetro `tags` para especificar a chave da tag (`key`) e o valor opcional da tag (`value`) para cada tag a ser adicionada ao recurso. O parâmetro `tags` especifica um mapa de string a string das chaves de tag e de seus valores de tag associados.

Para adicionar uma ou mais tags a um recurso existente, use a operação TagResource da API Amazon Macie ou, se você estiver usando AWS CLI, execute o comando tag-resource. Na sua solicitação, especifique o nome do recurso da Amazon (ARN) do recurso ao qual deseja adicionar uma tag. Use o parâmetro `tags` para especificar a chave da tag (`key`) e o valor opcional da tag (`value`) para cada tag a ser adicionada ao recurso. Como no caso de operações e comandos `Create`, o `tags` parâmetro especifica um mapa string a string das chaves de tag e seus valores de tag associados.

Por exemplo, o seguinte comando AWS CLI adiciona uma chave de tag `Stack` com um valor de tag `Production` ao trabalho especificado: Este exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

Onde:

- `resource-arn` especifica o ARN do trabalho ao qual adicionar uma tag.
- *`Stack`* é a chave da tag a ser adicionada ao trabalho.
- *`Production`* é o valor da tag especificada para a chave da tag especificada (*`Stack`*).

No exemplo a seguir, o comando adiciona várias tags ao trabalho:

```
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 tag em um mapa `tags`, os argumentos `key` e `value` são obrigatórios. No entanto, o valor do argumento `value` pode ser uma string vazia. Se você não quiser associar um valor de tag a uma chave de tag, não especifique um valor para o argumento `value`. Por exemplo, o comando AWS CLI a seguir adiciona uma chave de tag `Owner` sem valor de tag associado:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

Se a operação for bem sucedida, o Macie retornará uma resposta HTTP 204 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500, que indica o motivo de a operação ter falhado.

Revisão de tags para recursos do Amazon Macie

Você pode revisar as tags (tanto as chaves quanto os valores das tags) de um recurso do Amazon Macie usando o console do Amazon Macie ou a API do Amazon Macie. Se preferir fazer isso para vários recursos do Macie ao mesmo tempo, você pode usar o Editor de tags no console AWS Resource Groups ou as operações de tags da API de tags AWS Resource Groups.

Console

Siga estas etapas para revisar as tags de um recurso usando o console do Amazon Macie.

Para revisar as tags de um recurso

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Dependendo do tipo de recurso cujas tags você quer revisar, realize uma das seguintes ações:

   - Para uma lista de permissões, selecione Listas de permissões no painel de navegação.

Em seguida, marque a caixa de seleção para essa lista na tabela. Em seguida, selecione Gerenciar tags no menu Ações.

- Para um identificador de dados personalizadoa, selecione Identificadores de dados personalizados no painel de navegação.

  Em seguida, na tabela, marque a caixa de seleção do identificador de dados personalizados. Em seguida, selecione Gerenciar tags no menu Ações.

- Para uma regra de filtro ou supressão, selecione Descobertas no painel de navegação.

  Em seguida, na lista de Regras salvas, selecione o ícone de edição ( ) ao lado da regra. Em seguida, selecione Gerenciar tags.

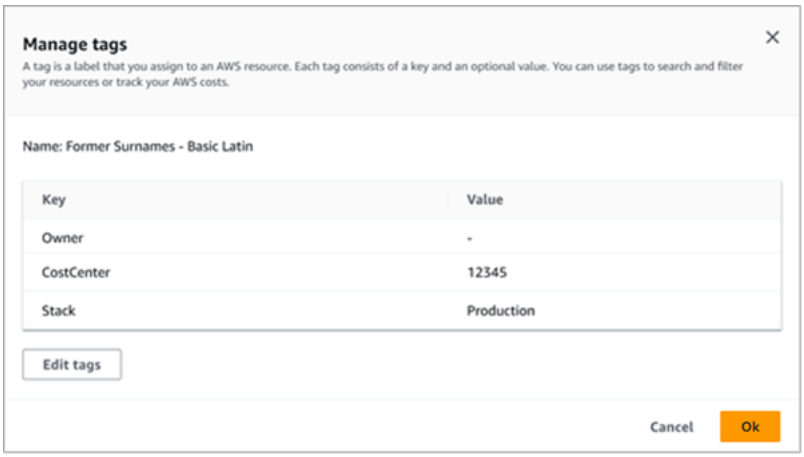
- Para uma conta de membro em sua organização, selecione Contas no painel de navegação.

  Em seguida, na tabela, marque a caixa de seleção para essa conta. Em seguida, selecione Gerenciar tags no menu Ações.

- Para um trabalho de descoberta de dados confidenciais, selecione Trabalhos no painel de navegação.

  Em seguida, marque a caixa de seleção para esse trabalho na tabela. Em seguida, selecione Gerenciar tags no menu Ações.

A janela Gerenciar tags lista todas as tags atualmente atribuídas ao recurso. Por exemplo, a imagem a seguir mostra as tags atribuídas a um identificador de dados personalizados.



Neste exemplo, três tags são atribuídas ao identificador de dados personalizados: a chave da tag Proprietário sem valor de tag associado; a chave da tag CostCenter com 12345 como valor de tag associado; e a chave da tag Pilha com Produção como valor de tag associado.

3. Ao terminar de revisar as tags, selecione Cancelar para fechar a janela.

API

Para recuperar e revisar programaticamente as tags de um recurso existente, você pode usar a operação `Get` ou `Describe` apropriada para o tipo de recurso para o qual deseja revisar as tags. Por exemplo, se você usar a operação GetCustomDataIdentifier ou executar o comando get-custom-data-identifier a partir do AWS Command Line Interface (AWS CLI), a resposta incluirá um objeto `tags`. O objeto lista todas as tags (tanto chaves e quanto valores de tag) que estão atualmente atribuídas ao recurso.

Também é possível usar a operação ListTagsForResource da API do Amazon Macie. Na sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) para esse recurso. Se você estiver usando o AWS CLI, execute o comando list-tags-for-resource e use o parâmetro `resource-arn` para especificar o ARN do recurso. Por exemplo:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

No exemplo anterior, *arn:aws:macie2:us-east- 1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample* é o ARN de um trabalho existente de descoberta de dados confidenciais.

Se a operação for bem-sucedida, o Macie retornará um objeto `tags` que lista todas as tags (chaves e valores de tag) atualmente atribuídas ao recurso. Por exemplo:

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

Onde `Stack`, `CostCenter` e `Owner` são as chaves de tag atribuídas ao recurso. `Production` é o valor da tag associado à chave da tag `Stack`. `12345` é o valor da tag associado à chave da tag `CostCenter`. A chave da tag `Owner` não tem um valor de tag associado.

Para exibir uma lista de todos os recursos do Macie que possuem tags, e todas as tags que estão associadas a cada um desses recursos, use a operação GetResources da API de tags do AWS Resource Groups. Na sua solicitação, defina o valor do parâmetro `ResourceTypeFilters` como `macie2`. Para fazer isso usando o AWS CLI, execute o comando get-resources e defina o valor do parâmetro `resource-type-filters` como `macie2`. Por exemplo:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Se a operação for bem-sucedida, o Resource Groups retornará uma matriz `ResourceTagMappingList` com os ARNs de todos os recursos do Macie que possuem tags e as chaves e valores de tag atribuídos a cada um desses recursos.

Edição de tags para recursos do Amazon Macie

Você pode revisar as tags (chaves ou valores das tags) de um recurso do Amazon Macie, você pode utilizar o console do Amazon Macie ou a API do Amazon Macie. Para fazer isso para vários recursos do Macie ao mesmo tempo, você pode usar o Editor de tags no console AWS Resource Groups ou as operações de tags da API de tags AWS Resource Groups.

> **Important**
>
> A edição de tags para um recurso pode afetar o acesso ao recurso. Antes de editar a chave ou o valor da tag para um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Console

Siga estas etapas para editar as tags de um recurso usando o console do Amazon Macie.

Para editar as tags de um recurso

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. Dependendo do tipo de recurso cujas tags você quer editar, realize uma das seguintes ações:

   - Para uma lista de permissões, selecione Listas de permissões no painel de navegação.

     Em seguida, marque a caixa de seleção para essa lista na tabela. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para um identificador de dados personalizados, selecione Identificadores de dados personalizados no painel de navegação.

     Em seguida, na tabela, marque a caixa de seleção do identificador de dados personalizados. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para uma regra de filtro ou supressão, selecione Descobertas no painel de navegação.

     Em seguida, na lista de Regras salvas, selecione o ícone de edição () ao lado da regra. Em seguida, selecione Gerenciar tags.
   - Para uma conta de membro em sua organização, selecione Contas no painel de navegação.

     Em seguida, na tabela, marque a caixa de seleção para essa conta. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para um trabalho de descoberta de dados confidenciais, selecione Trabalhos no painel de navegação.

     Em seguida, marque a caixa de seleção para esse trabalho na tabela. Em seguida, selecione Gerenciar tags no menu Ações.

   A janela Gerenciar tags lista todas as tags atualmente atribuídas ao recurso.
3. Na janela Gerenciar tags, selecione Editar tags.
4. Faça o seguinte:

   - Para adicionar um valor de tag a uma chave de tag, insira o valor na caixa Valor ao lado da chave de tag.
   - Para alterar uma chave de tag existente, selecione Remover ao lado da tag. Em seguida, selecione Adicionar tag. Na caixa Chave exibida, insira a nova chave de tag. Opcionalmente, insira um valor associado à tag na caixa Valor.

- Para alterar o valor de uma tag existente, selecione X na caixa Valor que contém o valor. Em seguida, digite o novo valor da tag na caixa Valor.
- Para remover o valor existente de uma tag, selecione X na caixa Valor que contém o valor.
- Para remover uma tag existente (a chave da tag e o valor da tag), selecione Remover ao lado da tag.

Um recurso pode ter até 50 tags. Uma chave de tag pode ter até 128 caracteres. Um valor de tag pode conter até 256 caracteres. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @

5. Depois de concluir a edição das tags, selecione Salvar.

API

Ao editar uma tag para um recurso programaticamente, você substitui a tag existente por novos valores. Portanto, a melhor maneira de editar uma tag depende se você deseja editar uma chave de tag, um valor de tag ou ambos. Para editar uma chave de tag, remova a tag atual e adicione uma nova tag.

Para editar ou remover somente o valor da tag associado a uma chave de tag, substitua o valor existente usando a operação TagResource da API Amazon Macie ou, se você estiver usando AWS Command Line Interface (AWS CLI), execute o comando tag-resource. Na sua solicitação, especifique o nome do recurso da Amazon (ARN) cujo valor da tag você deseja editar ou remover.

Para editar um valor de tag para uma chave de tag, use o parâmetro `tags` para especificar a chave de tag cujo valor você deseja alterar e especifique o novo valor de tag para a chave. Por exemplo, o comando a seguir altera o valor da tag de `Production` para `Staging` para a `Stack` chave de tag que é atribuída à regra de automação especificada: Este exemplo foi formatado para Microsoft Windows e usa o caractere de continuação de linha circunflexo (^) para melhorar a legibilidade.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

Onde:

- `resource-arn` especifica o ARN do trabalho.
- *`Stack`* é a chave de tag associada ao valor de tag a ser alterado.
- *`Staging`* é o novo valor da tag para a chave da tag especificada (*`Stack`*).

Para remover um valor de tag de uma chave de tag, não especifique um valor para o argumento `value` no parâmetro `tags`. Por exemplo:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

Se a operação for bem sucedida, o Macie retornará uma resposta HTTP 204 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500, que indica o motivo de a operação ter falhado.

Removendo tags dos recursos do Amazon Macie

Para remover tags de um recurso do Amazon Macie, você pode usar o console do Amazon Macie ou a API do Amazon Macie. Para fazer isso para vários recursos do Macie ao mesmo tempo, você pode usar o Editor de tags no console AWS Resource Groups ou as operações de tags da API de tags AWS Resource Groups.

> **Important**
>
> Remover tags de um recurso pode afetar o acesso ao recurso. Antes de remover uma tag, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Console

Siga estas etapas para remover uma ou mais tags de um recurso usando o console do Amazon Macie.

Remover uma tag de um recurso

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.

2. Dependendo do tipo de recurso ao qual você quer para remover uma tag, realize uma das seguintes ações:

   - Para uma lista de permissões, selecione Listas de permissões no painel de navegação.

     Em seguida, marque a caixa de seleção para essa lista na tabela. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para um identificador de dados personalizados, selecione Identificadores de dados personalizados no painel de navegação.

     Em seguida, na tabela, marque a caixa de seleção do identificador de dados personalizados. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para uma regra de filtro ou supressão, selecione Descobertas no painel de navegação.

     Em seguida, na lista de Regras salvas, selecione o ícone de edição () ao lado da regra. Em seguida, selecione Gerenciar tags.
   - Para uma conta de membro em sua organização, selecione Contas no painel de navegação.

     Em seguida, na tabela, marque a caixa de seleção para essa conta. Em seguida, selecione Gerenciar tags no menu Ações.
   - Para um trabalho de descoberta de dados confidenciais, selecione Trabalhos no painel de navegação.

     Em seguida, marque a caixa de seleção para esse trabalho na tabela. Em seguida, selecione Gerenciar tags no menu Ações.

   A janela Gerenciar tags lista todas as tags atualmente atribuídas ao recurso.
3. Na janela Gerenciar tags, selecione Editar tags.
4. Faça o seguinte:

   - Para remover somente o valor de tag de uma tag, selecione X na caixa Valor que contém o valor a ser removido.
   - Para remover a chave e também o valor de uma tag existente, selecione Remover ao lado da tag.

5. (Opcional) Para remover mais tags do recurso, repita a etapa anterior para cada tag adicional a ser removida.
6. Ao finalizar a remoção de tags, selecione Salvar.

API

Para remover uma ou mais tags de um recurso de forma programática, use a operação UntagResource da API do Amazon Macie. Na sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) do recurso do qual deseja remover uma tag. Use o parâmetro `tagKeys` para especificar a chave da tag a ser removida. Para remover somente um valor de tag específico (não uma chave de tag) de um recurso, edite a tag em vez de removê-la.

Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando untag-resource e use o parâmetro `resource-arn` para especificar o ARN do recurso do qual a tag deve ser removida. Use o parâmetro `tag-keys` para especificar a chave da tag a ser removida. Por exemplo, o comando a seguir remove a tag `Stack` (tanto a chave quanto o valor da tag) do trabalho de descoberta de dados confidenciais especificado:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

Onde `resource-arn` especifica o ARN da tarefa da qual remover uma tag e *`Stack`* é a chave da tag a ser removida.

Para remover várias tags de um recurso, acrescente cada chave adicional como argumento para o parâmetro `tag-keys`: Por exemplo:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

Onde `resource-arn` especifica o ARN do trabalho do qual remover as tags e *`Stack`* e *`Owner`* são as chaves das tags a serem removidas.

Se a operação for bem sucedida, o Macie retornará uma resposta HTTP 204 vazia. Caso contrário, o Macie retornará uma resposta HTTP 4xx ou 500, que indica o motivo de a operação ter falhado.

Como criar recursos do Amazon Macie com AWS CloudFormation

O Amazon Macie é integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS, para que você possa passar menos tempo criando e gerenciando seus recursos e sua infraestrutura. Você cria um modelo que descreve todos os recursos da AWS desejados (como identificadores de dados personalizados), e o AWS CloudFormation provisiona e configura esses recursos para você.

Quando você usa o AWS CloudFormation, é possível reutilizar seu modelo para configurar os seus recursos Macie repetidamente e de forma consistente. Descreva seus recursos uma vez e depois provisione os mesmos recursos repetidamente em várias regiões Contas da AWS e Regiões da AWS.

Tópicos

Amazon Macie e modelos do AWS CloudFormation

Para provisionar e configurar recursos para o Amazon Macie e serviços relacionados, é preciso entender os modelos do AWS CloudFormation. Modelos são arquivos de texto em formato JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation.

Se você não estiver familiarizado com JSON ou YAML, poderá usar o Designer AWS CloudFormation, uma ferramenta gráfica para criar e modificar modelos AWS CloudFormation. Com o Designer, você pode diagramar os recursos do modelo usando uma interface de arrastar e soltar e editar os seus detalhes usando o editor de JSON e YAML integrado. Para obter mais informações, consulte O que é o Designer? (O que é o AWS CloudFormation Designer) no Guia do usuário do AWS CloudFormation.

Você pode criar modelos AWS CloudFormation para os seguintes tipos de recursos do Macie:

- Listas de permissões
- Identificadores de dados personalizados

- Regras de filtro e regras de supressão para descobertas, também conhecidas como filtros de descobertas

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para esses recursos, consulte Referência de tipo de recurso do Amazon Macie no Guia do usuário do AWS CloudFormation.

Saiba mais sobre o AWS CloudFormation

Para saber mais sobre o AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Guia do usuário do AWS CloudFormation
- AWS CloudFormation Referência da API
- Guia do usuário da interface de linha de comando do AWS CloudFormation

Suspender ou desabilitar o Amazon Macie

Você pode suspender ou desabilitar o Amazon Macie de uma Região da AWS específica usando o console do Amazon Macie ou a API do Amazon Macie. O Macie então interrompe a execução de todas as atividades da sua conta naquela Região. Você não será cobrado pelo uso do Macie na Região enquanto ele estiver suspenso ou desabilitado.

Se você suspender ou desabilitar o Macie, poderá reabilitá-lo depois.

Tópicos

Suspender o Amazon Macie

Se você suspender o Amazon Macie, o Macie reterá o identificador da sessão, as configurações e os recursos da sua conta na Região da AWS aplicável. Por exemplo, suas descobertas existentes permanecem intactas e são retidas por até 90 dias. No entanto, quando você suspende o Macie, ele para de realizar todas as atividades da sua conta na Região aplicável. Isso inclui o monitoramento dos seus dados do Amazon Simple Storage Service (Amazon S3), realizar a descoberta automática de dados confidenciais e executar quaisquer trabalhos de descoberta de dados confidenciais que estejam atualmente em andamento. O Macie também cancela todos os seus trabalhos de descoberta de dados confidenciais na Região.

Depois de suspender o Macie, você poderá habilitá-lo novamente. Assim, você recuperará o acesso a todas as configurações e recursos na Região atual e o Macie retomará todas as atividades da sua conta nessa Região. Isso inclui atualizar o inventário de buckets do S3 da conta e monitorar esses buckets em relação à segurança e ao controle de acesso. Isso não inclui retomar ou reiniciar seus trabalhos de descoberta de dados confidenciais. Os trabalhos de descoberta de dados confidenciais não podem ser retomados ou reiniciados após serem cancelados.

Este tópico explica como suspender o Macie usando o console do Amazon Macie. Se preferir fazer isso de forma programática, você pode usar a operação UpdateMacieSession da API do Amazon Macie.

> **Note**
>
> Se você for o administrador do Macie, você deverá remover todas as contas-membro associadas à sua conta antes de suspender o Macie da sua conta. Para obter mais informações, consulte Gerenciar várias contas da .

Para suspender o Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja suspender o Macie.
3. No painel de navegação, selecione Settings (configurações).
4. Escolha Suspender Macie.
5. Quando a confirmação for solicitada, insira **`Suspend`** e escolha Suspender.

Para suspender o Macie em Regiões adicionais, repita as etapas anteriores para cada Região adicional.

Desabilitar o Amazon Macie

Quando você desabilita o Amazon Macie, o Macie deixa de realizar todas as atividades da sua conta na Região da AWS aplicável. Isso inclui o monitoramento dos seus dados do Amazon Simple Storage Service (Amazon S3), realizar a descoberta automática de dados confidenciais e executar quaisquer trabalhos de descoberta de dados confidenciais que estejam atualmente em andamento. O Macie também exclui todas as configurações e recursos existentes que ele armazena ou mantém para sua conta na Região aplicável, incluindo suas descobertas e trabalhos de descoberta de dados confidenciais. Os dados que você armazenou ou publicou para outras pessoas Serviços da AWS permanecem intactos e não são afetados — por exemplo, resultados de descoberta de dados confidenciais no Amazon S3 e localização de eventos no Amazon EventBridge.

> **Warning**
>
> Se você desativar o Macie, também excluirá permanentemente todas as suas descobertas existentes, trabalhos de descoberta de dados confidenciais, identificadores de dados personalizados e outros recursos que o Macie armazena ou mantém para sua conta na

Região aplicável. Não é possível recuperar esses recursos depois que forem excluídos. Para manter os recursos e apenas pausar o Macie, suspenda o Macie em vez de desativá-lo.

Este tópico explica como suspender o Macie usando o console do Amazon Macie. Se preferir fazer isso de forma programática, você pode usar a operação DisableMacie na API do Amazon Macie.

> **Note**
>
> Se a sua conta fizer parte de uma organização que gerencia centralmente várias contas do Macie, você deverá fazer o seguinte antes de desabilitar o Macie:
>
> - Se sua conta for uma conta de membro do Macie, trabalhe com o administrador do Macie para remover sua conta como conta de membro.
> - Se sua conta for uma conta de administrador do Macie, remova todas as contas de membros associadas à sua conta e exclua as associações entre sua conta e essas outras contas.
>
> O modo como você conclui as tarefas anteriores dependerá do fato de a sua conta Macie estar associada a outras contas por meio do AWS Organizations ou por convite. Para obter mais informações, consulte Gerenciar várias contas da .

Para desabilitar o Macie

1. Abra o console do Amazon Macie em https://console.aws.amazon.com/macie/.
2. Usando o seletor Região da AWS no canto superior direito da página, selecione a Região na qual você deseja suspender o Macie.
3. No painel de navegação, selecione Settings (configurações).
4. Selecione Desabilitar o Macie.
5. Quando a confirmação for solicitada, insira **`Disable`** e escolha Desabilitar.

Para suspender o Macie em Regiões adicionais, repita as etapas anteriores para cada Região adicional.

Cotas do Amazon Macie

Sua Conta da AWS tem certas cotas padrão, anteriormente chamadas de limites, para cada AWS service (Serviço da AWS). Essas quotas correspondem ao número máximo de recursos ou operações de serviço para sua conta. Este tópico lista as cotas que se aplicam aos recursos e às operações do Amazon Macie para sua conta. A menos que especificado de outra forma, cada cota se aplica à sua conta em cadaRegião da AWS.

Algumas cotas podem ser aumentadas, enquanto outras não. Para solicitar um aumento a uma cota, use o console do Service Quotas. Para saber como solicitar um aumento, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se uma cota não estiver disponível no console do Service Quotas, use o formulário de aumento do limite de serviço no AWS Support Center Console para solicitar um aumento na cota.

Contas

- Contas de membro por convite: 1.000
- Contas de membros até AWS Organizations: 10.000

Descobertas

- Regras de filtro e regras de supressão por conta: 1.000
- Descobertas por execução de um trabalho de descoberta de dados confidenciais: 100.000 + 5% de todas as descobertas restantes após o limite de 100.000 ser atingido

  Essa cota se aplica somente ao console do Amazon Macie e à API do Amazon Macie. Não há uma cota para o número de eventos de descoberta que o Macie publica no Amazon EventBridge ou para o número de resultados de descoberta de dados confidenciais que o Macie cria para cada execução de um trabalho.
- Locais de detecção por descoberta de dados confidenciais: 15
- Solicitações para recuperar e revelar amostras de dados confidenciais de um objeto do Amazon S3:100 por dia

  Essa cota é redefinida a cada 24 horas às 00:00:01 UTC+0.
- Tamanho de um objeto do Amazon S3 para recuperar e revelar amostras de dados confidenciais de:

- Arquivo de contêiner de objetos Apache Avro (.avro): 70 MB
- Arquivo Apache Parquet (.parquet): 100 MB
- Arquivo CSV (.csv): 255 MB
- Arquivo compactado GNU Zip (.gz ou .gzip): 90 MB
- Arquivo de linhas JSON ou JSON (.json ou .jsonl): 25 MB
- Arquivo da pasta de trabalho do Microsoft Excel (.xlsx): 20 MB
- Arquivo de texto não binário (text/plain): 100 MB
- Arquivo TSV (.tsv): 75 MB
- Arquivo compactado ZIP (.zip): 355 MB

Se uma descoberta for aplicável a um arquivo que gera vários arquivos .gz para os resultados da descoberta de dados confidenciais correspondentes, as amostras de dados confidenciais não poderão ser recuperadas e reveladas do arquivo.

Descoberta de dados confidenciais

- Análise mensal por conta por trabalhos confidenciais de descoberta de dados: 5 TB

  Essa cota se aplica somente aos trabalhos de descoberta de dados confidenciais. Para aumentar a cota para até 1.000 TB (1 PB), use o console Service Quotas. Para solicitar um aumento para mais de 1 PB, use o formulário de aumento do limite de serviço noAWS Support Center Console.
- Identificadores de dados personalizados por conta: 10.000
- Permitir listas por conta: 10, 1—5 listas de permissões que especificam texto predefinido e 1—5 listas de permissões que especificam expressões regulares

  As cotas adicionais se aplicam a uma lista de permissões que especifica um texto predefinido. A lista não pode conter mais de 100.000 entradas e o tamanho de armazenamento da lista não pode exceder 35 MB.
- Buckets de S3 a serem excluídos da descoberta automatizada de dados confidenciais: 1.000

  Se a conta for a conta do administrador do Macie de uma organização, essa cota se aplicará à organização em geral.
- Buckets de S3 por trabalho de descoberta de dados confidenciais: 1.000

  Essa cota não se aplica a trabalhos que usam critérios de bucket de runtime para determinar quais buckets analisar. Ela se aplica a um trabalho somente se você configurar o trabalho para analisar

buckets específicos selecionados. Se sua conta for a conta de administrador do Macie de uma organização, você poderá selecionar até 1.000 buckets abrangendo até 1.000 contas em sua organização.

- Identificadores de dados personalizados por trabalho de descoberta de dados confidenciais: 30
- Listas de permissões por trabalho de descoberta de dados confidenciais: 10, 1—5 listas de permissões que especificam texto predefinido e 1—5 listas de permissões que especificam expressões regulares
- Operação CreateClassificationJob: 0,1 solicitações por segundo
- Tempo para analisar um arquivo individual: 10 horas
- Tamanho de um arquivo individual a ser analisado:
  - Arquivo em formato de documento portátil da Adobe (.pdf): 1.024 MB
  - Arquivo de contêiner de objetos Apache Avro (.avro): 8 GB
  - Arquivo Apache Parquet (.parquet): 8 GB
  - Arquivo de mensagem de e-mail (.eml): 20 GB
  - Arquivo compactado GNU Zip (.gz ou .gzip): 8 GB
  - Arquivo da pasta de trabalho do Microsoft Excel (.xls ou .xlsx): 512 MB
  - Arquivo de documento do Microsoft Word (.doc ou .docx): 512 MB
  - Arquivo de texto não binário: 20 GB
  - Um arquivo TAR (.tar) de 20 GB
  - Arquivo compactado ZIP (.zip): 8 GB

  Se um arquivo for maior do que a cota aplicável, o Macie não analisará nenhum dado no arquivo.
- Extração e análise de dados em um arquivo compactado ou arquivado:
  - Tamanho de armazenamento (compactado): 8 GB para um arquivo compactado GNU Zip (.gz ou .gzip) ou arquivo compactado ZIP (.zip); 20 GB para um arquivo TAR (.tar)
  - Profundidade de arquivo aninhada: 10 níveis
  - Arquivos extraídos: 1.000.000
  - Bytes extraídos: 10 GB de dados não compactados em geral. 3 GB de dados não compactados para cada arquivo extraído que usa um tipo de arquivo ou formato de armazenamento compatível.

  Se os metadados de um arquivo compactado ou arquivado indicarem que o arquivo contém mais de 10 níveis aninhados ou excede a cota aplicável para tamanho de armazenamento ou bytes

extraídos, o Macie não extrai nem analisa nenhum dado no arquivo. Se o Macie começar a extrair e analisar dados em um arquivo compactado ou arquivado e, posteriormente, determinar que o arquivo contém mais de 1.000.000 de arquivos ou excede a cota de bytes extraídos, o Macie interrompe a análise dos dados no arquivo e cria descobertas de dados confidenciais e resultados de descoberta somente para os dados que foram processados.

- Análise de elementos aninhados em dados estruturados: 256 níveis por arquivo

  Essa cota se aplica somente aos arquivos JSON (.json) e JSON Lines (.jsonl). Se a profundidade aninhada de qualquer tipo de arquivo exceder essa cota, o Macie não analisará nenhum dado no arquivo.
- Locais de detecção por resultado de descoberta de dados confidenciais: 1.000 por tipo de detecção de dados confidenciais
- Detecção de nomes completos: 1.000 por arquivo, incluindo arquivos de arquivamento

  Depois que o Macie detecta as primeiras 1.000 ocorrências de nomes completos em um arquivo, o Macie para de incrementar a contagem e relatar os dados de localização dos nomes completos.
- Detecção de endereços de correspondência: 1.000 por arquivo, incluindo arquivos de arquivamento

  Depois que o Macie detecta as primeiras 1.000 ocorrências de endereços de correspondência em um arquivo, o Macie para de incrementar a contagem e relatar os dados de localização dos endereços de correspondência.

Histórico de documentos do Guia do usuário do Amazon Macie

A tabela a seguir descreve as alterações importantes na documentação desde a última versão do Amazon Macie. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Última atualização da documentação: 20 de fevereiro de 2024

Alteração	Descrição	Data
ova funcionalidade	AWS Security Hub agora fornece controles de segurança que verificam o status do Macie e a descobert a automatizada de dados confidenciais para contas. Se esses controles estiverem habilitados, o Security Hub executará periodicamente verificações de segurança para determinar se o Macie está habilitado para um Conta da AWS (controle Macie.1) e se a descoberta automática de dados confidenciais está habilitada para uma conta Macie (controle Macie.2).	20 de fevereiro de 2024
ova funcionalidade	Agora, o Macie pode analisar objetos do Amazon S3 que são criptografados usando criptografia de duas camadas do lado do servidor com (DSSE-KMS). AWS KMS keys Esses objetos agora são	17 de janeiro de 2024

	elegíveis para análise quando o Macie realiza a descobert a automática de dados confidenciais ou você executa trabalhos de descoberta de dados confidenciais. Além disso, os buckets e objetos do S3 que usam a criptogra fia DSSE-KMS agora estão incluídos nas estatísticas e nos metadados que o Macie fornece sobre seus dados do Amazon S3.	
Novo recurso	Agora você pode configura r o Macie para assumir uma função AWS Identity and Access Management (IAM) ao optar por recuperar e revelar amostras de dados confidenciais que o Macie relata nas descobertas. As amostras podem ajudar você a verificar a natureza dos dados confidenciais encontrados pelo Macie e a personalizar a sua investigação sobre um objeto e bucket afetados do Amazon S3.	16 de novembro de 2023

Nova funcionalidade	O Macie agora fornece identificadores de dados gerenciados projetados para detectar números de contas bancárias internacionais (IBANs) em mais 47 países e regiões. Agora você pode usar o Macie para detectar e relatar ocorrências de IBANs em mais de 50 países e regiões.	1.º de novembro de 2023
Nova funcionalidade	O Macie agora fornece identificadores de dados gerenciados projetados para detectar os seguintes tipos de dados confidenciais: chaves de API do Google Cloud, chaves da API Stripe e números de Aadhaar, números de contas permanentes (PANs) e números de identificação da carteira de motorista da Índia.	25 de setembro de 2023

Novas cotas	Para ajudar você a verificar a natureza dos dados confidenciais relatados pelas descobertas, aumentamos as cotas de tamanho para recuperar e revelar amostras de dados confidenciais de objetos do Amazon S3. Agora você pode recuperar e revelar amostras de objetos do S3 cujo tamanho de armazenamento excede 10 MB. Para obter uma lista das novas cotas, consulte Cotas do Amazon Macie.	7 de setembro de 2023
Disponibilidade regional	O Macie já está disponível na região de Israel (Tel Aviv). Para obter uma lista completa de Regiões da AWS onde o Macie está disponível atualmente, consulte Endpoints e cotas do Amazon Macie no arquivo Referência geral da AWS.	28 de agosto de 2023

Funcionalidade atualizada	Implementamos um novo conjunto dinâmico de identificadores de dados gerenciados padrão para a descoberta automatizada de dados confidenciais. O conjunto padrão inclui os identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados confidenciais. Ele foi projetado para detectar categorias e tipos comuns de dados confidenciais e, ao mesmo tempo, otimizar seus resultados automatizados de descoberta de dados confidenciais.	2 de agosto de 2023

Funcionalidade atualizada	Para ajudá-lo a localizar ocorrências de dados confidenciais que o Macie relata nas descobertas de dados confidenciais e nos resultados da descobert a de dados confidenciais, alteramos o limite de caractere s de 20 para 240 para os nomes dos elementos do caminho JSON nos objetos `Record`. Essa alteração afeta novas descobertas de dados confidenciais e resultados de descoberta para contêiner es de objetos Apache Avro, arquivos Apache Parquet, arquivos JSON e arquivos JSON Lines.	24 de julho de 2023
Funcionalidade atualizada	Se você for o administr ador delegado do Macie de uma organização em AWS Organizations, agora você pode gerenciar o Macie para até 10.000 contas em sua organização.	30 de junho de 2023

Novo recurso	Agora você pode criar e configurar trabalhos confidenciais de descoberta de dados para usar automaticamente o conjunto de identificadores de dados gerenciados que recomendamos para trabalhos. Esse conjunto recomendado de identificadores de dados gerenciados foi projetado para detectar categorias e tipos comuns de dados confidenciais e, ao mesmo tempo, otimizar os resultados do seu trabalho.	28 de junho de 2023
Nova política	Adicionamos uma nova política gerenciada pelaAWS, a política `AmazonMacieReadOnlyAccess`. Essa política concede permissões somente de leitura que permitem que uma identidade do IAM (principal) recupere todos os recursos, dados e configurações do Macie para sua conta.	15 de junho de 2023

Novo recurso	Para ajudá-lo a avaliar e monitorar a cobertura automatizada de descoberta de dados confidenciais de seus dados do Amazon S3, o console do Macie agora inclui uma página de cobertura de recursos. A página fornece uma visão unificada das estatísticas e dos dados de cobertura de todos os seus buckets do S3, incluindo um conjunto de problemas de análise (se houver) que ocorreram recentemente em cada bucket. Se ocorrerem problemas, a página também fornece orientações para remediação.	15 de maio de 2023

Novo recurso	O Macie se integra com Notificações de Usuários da AWS, que é um novo local AWS service (Serviço da AWS) que atua como um local central para suas AWS notificações no. AWS Management ConsoleCom Notificações de Usuários, você pode configurar regras personalizadas e canais de entrega para gerar e enviar notificações sobre EventBridge eventos da Amazon que o Macie publica para descobertas de políticas e dados confidenciais.	5 de maio de 2023

Conteúdo atualizado	Descrições atualizadas das estatísticas e metadados que o Macie fornece sobre as configurações de criptografia padrão para buckets do S3. Também atualizou a descrição da descoberta da política da Policy:IAMUser/S3BucketEncryptionDisabled. O Amazon S3 agora aplica automaticamente a criptografia no lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) como nível básico de criptografia para objetos adicionados a buckets novos e existentes. Para obter informações sobre essa mudança no Amazon S3, consulte Definindo o comportamento padrão de criptografia do lado do servidor para buckets do S3 no Guia do usuário do Amazon Simple Storage Service.	27 de fevereiro de 2023

Nova funcionalidade	O Macie agora pode gerar um tipo adicional de descoberta de política para um bucket do S3: `Policy:IAMUser/S3BucketSharedWithCloudFront` . Esse tipo de descoberta indica que a política de um bucket foi alterada para permitir que o bucket seja compartilhado com uma identidade de acesso de CloudFront origem da Amazon (OAI), um controle de acesso de CloudFront origem (OAC) ou ambos. Além disso, os buckets que são compartilhados com CloudFront OAIs ou OACs agora são considerados compartilhados externamente nas estatísticas e metadados que o Macie fornece sobre seus dados do Amazon S3.	24 de fevereiro de 2023

Nova funcionalidade	O Macie agora oferece suporte à classe de armazenamento Amazon S3 Glacier Instant Retrieval para descoberta de dados confidenciais. Os objetos do S3 que usam essa classe de armazenamento agora estão qualificados para análise quando o Macie realiza a descoberta automatizada de dados confidenciais ou você executa trabalhos de descoberta de dados confidenciais. Eles também são considerados objetos classificáveis em estatísticas e metadados que o Macie fornece sobre seus dados do Amazon S3.	21 de dezembro de 2022

Novo recurso	Agora você pode configurar o Macie para realizar a descoberta automática de dados confidenciais para sua conta ou organização. Com a descoberta automatizada de dados confidenciais, o Macie avalia continuamente seus dados do Amazon S3 e usa técnicas de amostragem para identificar, selecionar e analisar objetos representativos em seus buckets do S3, inspecionando os objetos em busca de dados confidenciais. Você pode avaliar os resultados das análises em estatísticas, descobertas e outras informações que o Macie fornece sobre seus dados do Amazon S3.	28 de novembro de 2022

Novo recurso	Agora você pode criar e usar listas de permissões para especificar texto e padrões de texto que você deseja que o Macie ignore ao inspecionar objetos do Amazon S3 em busca de dados confidenciais. Ao usar listas de permissões, você pode definir exceções de dados confidenciais para seus cenários ou ambientes específicos, por exemplo, os nomes dos representantes públicos da sua organização, números de telefone específicos ou dados de amostra que sua organização usa para testes.	30 de agosto de 2022
Novo recurso	Para verificar a natureza dos dados confidenciais que o Macie encontra nos objetos do S3, agora você pode configurar e usar o Macie para recuperar amostras de dados confidenciais relatados pelas descobertas.	26 de julho de 2022

Funcionalidade atualizada	Na política da AmazonMacieFullAccess, atualizamos o nome do recurso da Amazon (ARN) da função vinculada ao serviço do Macie (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	30 de junho de 2022
Funcionalidade atualizada	Atualizamos a política da AmazonMacieServiceRolePolicy, que é a política anexada à função vinculada ao serviço do Macie (`AWSServiceRoleForAmazonMacie`). A política não especifica mais ações e recursos para o Amazon Macie Classic. O Amazon Macie Classic foi descontinuado e não está mais disponível.	20 de maio de 2022
Nova funcionalidade	A Macie agora inclui o `OriginType` campo nas descobertas de dados confidenciais nas quais publica. AWS Security Hub O campo `OriginType` especifica como Macie encontrou os dados confidenciais que produziram uma descoberta.	11 de maio de 2022

Conteúdo atualizado	Esclareceu como as configurações de palavra-chave e distância máxima de correspondência funcionam para identificadores de dados personalizados.	22 de abril de 2022
Nova funcionalidade	O Macie agora fornece identificadores de dados gerenciados projetados para detectar cabeçalhos de Autorização Básica HTTP, cookies HTTP e Tokens Web JSON.	21 de abril de 2022
Novo conteúdo	Foram adicionadas descrições e definições dos principais conceitos e termos para o Macie.	16 de março de 2022
Nova funcionalidade	Para calcular e exibir os custos estimados ao criar e configurar trabalhos confidenciais de descoberta de dados, o Macie agora recupera os dados de preços do seu Conta da AWS formulário. AWS Billing and Cost Managemen tPara oferecer suporte a essa funcionalidade, adicionamos uma ação Gerenciamento de faturamento e custos à política AmazonMacieFullAccess.	7 de março de 2022

Nova funcionalidade	Macie agora inclui o `Sample` campo nas descobertas para as quais publica. AWS Security Hub O campo `Sample` especifica se uma descoberta é uma amostra de descoberta.	24 de fevereiro de 2022
Novo conteúdo	Foram adicionadas informaçõ es sobre o uso do Amazon Virtual Private Cloud para estabelecer uma conexão privada entre a VPC e o Macie.	19 de janeiro de 2022
Nova funcionalidade	Agora você pode usar o console do Amazon Macie para atribuir e gerenciar tags para identificadores de dados personalizados, regras de filtro e supressão para descobert as, trabalhos de descobert a de dados confidenciais e, se você for o administrador do Macie de uma organizaç ão, contas de membros em sua organização. Tag é um rótulo que você define e atribui opcionalmente a determinados tipos de recursos AWS .	12 de janeiro de 2022
Novo conteúdo	Foram adicionadas informaçõ es sobre o uso do AWS Identity and Access Management para gerenciar o acesso ao Macie.	20 de dezembro de 2021

Novo recurso	Ao criar um identificador de dados personalizado, agora você pode definir configurações de severidade para as descobertas de dados confidenciais que ele produz. Com essas configurações, você pode especificar qual severidade atribuir a uma descoberta com base no número de ocorrências de texto que correspondem aos critérios de detecção do identificador de dados personalizado.	4 de novembro de 2021
Nova funcionalidade	Para saber mais sobre os diferentes tipos de descobertas que o Macie fornece, você pode gerar amostras de descobertas. As amostras de descobertas usam dados de exemplo e valores de espaço reservado para demonstrar os tipos de informações que o Macie pode incluir em cada tipo de descoberta.	28 de outubro de 2021
Nova funcionalidade	Macie agora inclui o `OwnerAccountId` campo nas descobertas para as quais publica. AWS Security Hub Esse campo especifica o ID da conta do proprietário do Conta da AWS bucket do S3 afetado.	27 de outubro de 2021

Novo conteúdo	Foram adicionadas informaçõ es sobre o gerenciamento centralizado de várias contas do Macie. Você pode fazer isso de duas maneiras: integrando o Macie AWS Organizations ou enviando convites de associação do Macie.	13 de outubro de 2021
Nova funcionalidade	Seu inventário do bucket do S3 agora indica se as configurações de permissões de um bucket impedem que o Macie recupere informações sobre o bucket ou os objetos do bucket e avalie e monitore a segurança e a privacida de dos dados do bucket. Além disso, atualizamos as referências AWS KMS keys e as chaves gerenciadas pelo cliente para refletir a terminolo gia atual.	5 de outubro de 2021

Nova funcionalidade	O Macie agora armazena descobertas de políticas e dados confidenciais por 90 dias em vez de 30 dias. Se o Macie criou ou atualizou uma descoberta em ou após 31 de agosto de 2021, você poderá acessar a descobert a por até 90 dias usando o console do Macie ou a API do Macie. Com certeza Regiões da AWS, Macie começou a reter as descobertas por 90 dias já em 27 de setembro de 2021.	1.º de outubro de 2021
Novo recurso	Ao criar um trabalho de descoberta de dados confidenciais, agora você pode especificar quais identific adores de dados gerenciad os você deseja que o trabalho use ao analisar objetos do S3. Com esse recurso, você pode personalizar a análise de um trabalho para se concentra r em determinados tipos de dados confidenciais.	17 de setembro de 2021
Nova funcionalidade	As descobertas de dados confidenciais agora fornecem informações adicionais para ajudá-lo a localizar dados confidenciais em arquivos JSON e JSON Lines.	6 de julho de 2021

Funcionalidade atualizada	O Macie agora usa o tipo de `AwsS3Bucket` recurso nas descobertas nas quais publica. AWS Security Hub (Macie definiu esse valor anteriormente como `AWS::S3::Bucket`.) `AwsS3Bucket` é o valor do tipo de recurso usado para buckets do S3 no AWS Security Finding Format (ASFF).	28 de junho de 2021
Novo recurso	Ao criar um trabalho de descoberta de dados confidenciais, agora você pode definir critérios de runtime que determinam quais buckets do S3 o trabalho analisa. Com esse recurso, o escopo da análise de um trabalho pode se adaptar dinamicamente às mudanças em seu inventário de baldes.	15 de maio de 2021

Nova funcionalidade	Seu inventário de bucket do S3 e o painel de resumo agora fornecem metadados e estatísticas de criptografia indicando se as políticas de bucket exigem criptografia do lado do servidor de novos objetos. Além disso, agora você pode realizar atualizações sob demanda de metadados de objetos para buckets individuais em seu inventário de buckets.	30 de abril de 2021
Novo recurso	Agora você pode usar o Amazon CloudWatch Logs para monitorar e analisar eventos que ocorrem quando você executa trabalhos confidenciais de descoberta de dados. Para oferecer suporte a esse recurso, adicionamos ações de CloudWatch registros à política AWS gerenciada da função vinculada ao serviço do Macie.	14 de abril de 2021
Disponibilidade regional	Macie agora está disponível na região AWS Ásia-Pacífico (Osaka).	5 de abril de 2021
Novo recurso	Agora você pode configurar o Macie para publicar descobertas de dados confidenciais no AWS Security Hub.	22 de março de 2021

Novo conteúdo	Foram adicionadas informações sobre monitoramento e previsão de custos do Macie e participação no teste gratuito.	26 de fevereiro de 2021
Conteúdo atualizado	Substituímos o termo conta principal pelo termo conta de administrador. Uma conta de administrador é usada para gerenciar centralmente várias contas.	12 de fevereiro de 2021
Nova funcionalidade	Agora você pode refinar o escopo de trabalhos confidenciais de descoberta de dados usando prefixos de objetos do S3 em critérios personalizados de inclusão e exclusão.	2 de fevereiro de 2021
Conteúdo atualizado	O Macie agora adere à taxonomia do tipo de descoberta do AWS Security Finding Format (ASFF) quando publica descobertas de políticas em. AWS Security Hub	28 de janeiro de 2021
Novo conteúdo	Foram adicionadas informações sobre o monitoramento de dados do Amazon S3 e a avaliação da segurança e privacidade desses dados.	8 de janeiro de 2021

Disponibilidade regional	Macie agora está disponível na região da AWS África (Cidade do Cabo), na região da AWS Europa (Milão) e na região do Oriente AWS Médio (Bahrein).	21 de dezembro de 2020
Nova funcionalidade	Se sua conta for uma conta de administrador do Macie, agora você pode criar e executar trabalhos confidenciais de descoberta de dados que analisam dados de até 1.000 buckets abrangendo até 1.000 contas em sua organização.	25 de novembro de 2020
Nova funcionalidade	Seu inventário de bucket do S3 agora indica se você configurou algum trabalho de descoberta de dados confidenciais único ou periódico para analisar dados em um bucket. Se você tiver, ele também fornece detalhes sobre o trabalho executado mais recentemente.	23 de novembro de 2020
Novo conteúdo	Foram adicionadas informações sobre a filtragem de descobertas.	12 de novembro de 2020

Nova funcionalidade	As descobertas de dados confidenciais agora fornecem informações adicionais para ajudá-lo a localizar dados confidenciais em contêiner es de objetos Apache Avro, arquivos Apache Parquet e pastas de trabalho do Microsoft Excel.	9 de novembro de 2020
Novo recurso	Agora você pode usar descobertas de dados confidenciais para localizar ocorrências individuais de dados confidenciais em objetos do S3.	22 de outubro de 2020
Novo recurso	Agora você pode pausar e retomar trabalhos confidenc iais de descoberta de dados.	16 de outubro de 2020
Novo conteúdo	Foram adicionados detalhes sobre o sistema de pontuação de severidade para descobert as de políticas e descobertas de dados confidenciais.	6 de outubro de 2020

Novos atributos	Agora você pode visualizar estatísticas que indicam a quantidade de dados que o Macie pode analisar em buckets individuais do S3 quando você executa um trabalho confidencial de descoberta de dados. Além disso, agora você pode visualizar o custo estimado de um trabalho ao criar um trabalho.	3 de setembro de 2020
Novo conteúdo	Foram adicionadas informações sobre como configurar, executar e gerenciar trabalhos confidenciais de descoberta de dados.	31 de agosto de 2020
Nova funcionalidade	Os identificadores de dados gerenciados agora podem detectar certos tipos de informações de identificação pessoal no Brasil.	31 de julho de 2020
Conteúdo atualizado	Foram adicionadas informações sobre a sintaxe compatível com expressões regulares em identificadores de dados personalizados.	30 de julho de 2020

Conteúdo atualizado	Foram adicionados requisitos de palavras-chave para identificadores de dados gerenciados e aumentou a cota para o número de descobertas que cada trabalho confidencial de descoberta de dados pode produzir.	17 de julho de 2020
Novo conteúdo	Foram adicionadas informações sobre o uso da Amazon EventBridge e AWS Security Hub para monitorar e processar descobertas. Isso inclui o esquema de EventBridge eventos para descobertas e exemplos de eventos para descobertas de políticas e dados confidenciais.	22 de junho de 2020
Novo conteúdo	Foram adicionadas informações sobre análise e supressão de descobertas.	17 de junho de 2020
Novo conteúdo	Foram adicionadas instruções para configurar o Macie para armazenar resultados de descoberta detalhados em um bucket S3.	2 de junho de 2020
Novo conteúdo	Foram adicionadas informações sobre os tipos de dados confidenciais que o Macie pode detectar e os requisitos de criptografia para detectar dados confidenciais em objetos do Amazon S3.	28 de maio de 2020

Disponibilidade geral	Esse é o lançamento inicial público do Guia de usuário do Amazon Macie.	13 de maio de 2020

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.