aws

用户指南

Amazon Macie

Amazon Macie: 用户指南

Table of Contents

什么是 Amazon Macie？

Amazon Macie 是一项数据安全服务，该服务使用机器学习和模式匹配来发现敏感数据，提供对数据安全风险的可见性，并实现针对这些风险的自动防护。

为了帮助您管理组织的 Amazon Simple Storage Service (Amazon S3) 数据资产的安全状况，Macie 为您提供 S3 存储桶的清单，并自动评测和监控这些存储桶以实现安全性和访问控制。如果 Macie 检测到潜在的数据安全性或隐私问题（例如桶变为可供公共访问），Macie 会生成调查发现，供您查看并在必要时进行补救。

Macie 还能自动发现和报告敏感数据，以便您更好地了解您的组织在 Amazon S3 中存储的数据。要检测敏感数据，您可以使用 Macie 提供的内置标准和技术、您定义的自定义标准或两者的组合。如果 Macie 在 S3 对象中检测到敏感数据，Macie 会生成调查发现来通知您 Macie 发现的敏感数据。

除了调查发现之外，Macie 还提供统计数据和其他数据，让您深入了解 Amazon S3 数据的安全状况以及敏感数据可能在数据资产中的位置。统计数据和数据可以指导您做出决策，以便对特定的 S3 存储桶和对象进行更深入的调查。您可以使用 Amazon Macie 控制台或 Amazon Macie API 查看和分析调查发现、统计数据和其他数据。您还可以利用 Macie 与 Amazon EventBridge 和 AWS Security Hub 的集成，并使用其他服务、应用程序和系统来监控、处理和修复调查发现。

主题

Amazon Macie 的功能

以下是 Amazon Macie 可以帮助您发现、监控和保护您在 Amazon S3 中的敏感数据的一些主要方法。

自动敏感数据发现

借助 Macie，您可以通过两种方式自动发现和报告敏感数据：配置 Macie 以执行敏感数据自动发现，以及创建和运行敏感数据发现作业。如果 Macie 在 S3 对象中检测到敏感数据，它会为您创建敏感数据调查发现。调查发现会提供关于 Macie 找到的敏感数据的详细报告。

通过自动敏感数据发现，可以广泛了解敏感数据可能存放在您的 Amazon S3 数据资产中的位置。使用此选项，Macie 可以持续评测您的 S3 存储桶清单，并使用采样技术从您的存储桶中识别和选择具有代表性的 S3 对象。然后，Macie 检索并分析所选对象，检查它们是否有敏感数据。

敏感数据发现作业可提供更深入、更有针对性的分析。使用此选项，您可以定义分析的广度和深度，即要分析的 S3 存储桶、采样深度以及源自 S3 对象属性的自定义标准。您也可以将作业配置为仅运行一次以进行按需分析和评测，或者定期运行以进行定期分析、评测和监控。

这两个选项都可以帮助您构建和维护组织在 Amazon S3 中存储的数据以及这些数据的任何安全或合规风险的全面视图。

发现各种敏感数据类型

要使用 Macie 发现敏感数据，您可以使用内置标准和技术（例如机器学习和模式匹配）来分析 S3 存储桶中的对象。这些标准和技术被称为托管数据标识符，可以检测到许多国家和地区的大量且不断增长的敏感数据类型，包括多种类型的个人身份信息（PII）、财务信息和凭证数据。

您也可以使用自定义数据标识符。自定义数据标识符是您定义的一组检测敏感数据的标准，即定义要匹配的文本模式的正则表达式 (regex) 和可选的字符序列，以及优化结果的邻近规则。使用此类标识符，您可以检测反映特定场景、知识产权或专有数据的敏感数据。您可以补充 Macie 提供的托管数据标识符。

要微调分析，也可以使用允许列表。允许列表定义您希望 Macie 在 S3 对象中忽略的特定文本和文本模式。这些通常是针对您的特定场景或环境的敏感数据例外情况，例如，您组织的公共代表姓名、组织的公共电话号码或您的组织用于测试的示例数据。

评测和监控数据以确保安全和访问控制

启用 Macie 后，Macie 会自动生成并开始维护您的 S3 存储桶的完整清单。Macie 还开始评测和监控这些存储桶以确保安全性和进行访问控制。如果 Macie 检测到存储桶的安全性或隐私存在潜在问题，它会为您创建策略调查发现。

除了具体的调查发现外，控制面板还为您提供 Amazon S3 数据的汇总统计数据的快照。这包括关键指标的统计数据，例如您的存储桶中有多少可公开访问或与其他 AWS 账户 共享。您可以深入研究每个统计数据以查看支持数据。

Macie 还提供清单中各个 S3 存储桶的详细信息和统计数据。这些数据包括存储桶的公共访问和加密设置的明细，以及 Macie 可以分析以检测存储桶中敏感数据的对象的大小和数量。您可以浏览库存，也可以按特定字段对库存进行排序和筛选。当您选择存储桶时，面板会显示该存储桶的详细信息。

审查和分析调查发现

在 Macie 中，调查发现是对 Macie 在 S3 对象中检测到的敏感数据或 S3 存储桶安全性或隐私的潜在问题的详细报告。每项调查发现都提供了严重性评级、有关受影响资源的信息以及其他详细信息，例如 Macie 何时以及如何发现问题。

要查看、分析和管理调查发现，您可以使用 Amazon Macie 控制台上的调查发现页面。这些页面列出了您的调查发现，并提供了个别调查发现的详细信息。它们还提供了多个选项，用于对调查发现进行分组、筛选、排序和屏蔽。您还可以使用 Amazon Macie API 查询、检索和屏蔽调查发现。如果您使用 API，则可以将数据传递给其他应用程序、服务或系统，以进行更深入的分析、长期存储或报告。

使用其他服务和系统监控和处理调查发现

为了支持与其他服务和系统的集成，Macie 将调查发现作为查找事件发布到 Amazon EventBridge EventBridge 是一项无服务器事件总线服务，它可以将调查发现数据路由到目标，例如AWS Lambda函数和 Amazon Simple Notification Service (Amazon SNS)主题。借助 EventBridge，您可以近乎实时地监控和处理调查发现，这是现有安全和合规工作流程的一部分。

您可以将 Macie 配置为也将调查发现发布到 AWS Security Hub。Security Hub 是一项服务，可提供整个 AWS 环境中安全状况的全面视图，可帮助您检查您的环境是否符合安全行业标准和最佳实践。借助 Security Hub，您可以更轻松地监控和处理调查发现，以此作为对 AWS 中组织安全状况进行更广泛分析的一部分。您还可以聚合来自多个 AWS 区域 的调查发现，随后监控和处理来自单个区域的聚合调查发现数据。

集中管理多个 Macie 账户

如果您的 AWS 环境有多个账户，则可以集中管理环境中账户的 Macie。你可以通过两种方式做到这一点：将 Macie 与 AWS Organizations 集成，或者在 Macie 中发送和接受会员邀请。

在多账户配置中，指定的 Macie 管理员可以执行某些任务，也可以访问属于同一组织的账户的某些 Macie 设置、数据和资源。任务包括查看有关成员账户拥有的 S3 存储桶的信息、查看这些存储桶的策略调查发现以及检查存储桶中是否有敏感数据。如果账户是通过 AWS Organizations 关联的，Macie 管理员还可以为组织中的成员账户启用 Macie。

以编程方式开发和管理资源

除了 Amazon Macie 主机外，您还可以使用 Amazon Macie API 与 Macie 互动。Amazon Macie API 让您可以通过编程方式全面访问您的 Macie 账户设置、数据和资源。

要以编程方式与 Macie 进行交互，您可以直接向 Macie 发送 HTTPS 请求，也可以使用当前版本的 AWS 命令行工具或 AWS SDK。AWS 提供的工具和 SDK 由适用于各种语言和平台（例如 PowerShell、Java、Go、Python、C++ 和.NET）的库和示例代码组成。

访问 Amazon Macie

Amazon Macie 在大多数 AWS 区域 中都可用。有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。有关为您的 AWS 账户 管理 AWS 区域 的信息，请参阅 AWS Account Management 参考指南中的指定您的账户可以使用的 AWS 区域。

在每个区域中，您可以通过以下任意方式使用 Macie。

AWS Management Console

AWS Management Console 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。作为该主机的一部分，Amazon Macie 控制台提供对您的 Macie 账户、数据和资源的访问权限。您可以使用 Macie 控制台执行任何 Macie 任务，包括查看有关 S3 存储桶的统计数据和其他信息、创建和运行敏感数据发现任务、查看和分析调查发现等。

AWS 命令行工具

使用 AWS 命令行工具，您可在系统的命令行中发出命令以执行 Macie 任务和 AWS 任务。与使用控制台相比，使用命令行更快、更方便。如果要构建执行 任务的脚本，命令行工具也会十分有用。

AWS 提供两组命令行工具：AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell。有关安装和使用 AWS CLI 的更多信息，请参阅 AWS Command Line Interface 用户指南。有关安装和使用 Tools for PowerShell 的信息，请参阅 AWS Tools for PowerShell 用户指南。

AWS SDK

AWS 提供由各种编程语言和平台（例如 Java、Go、Python、C++ 和 .NET）的库和示例代码组成的 SDK。SDK 提供对 Macie 和其他 AWS 服务 的便捷、编程访问。它们还处理多个任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求。有关安装和使用 AWS SDK 的信息，请参阅在 AWS 上构建的工具。

Amazon Macie REST API

Amazon Macie REST API 允许您以编程方式全面访问你的 Macie 账户、数据和资源。使用此 API，您可以直接向 Macie 发送 HTTPS 请求。但是，与AWS命令行工具和 SDK 不同，使用此 API 需要您的应用程序处理低级别的详细信息，例如生成哈希值以签署请求。有关此 API 的信息，请参阅 Amazon Macie API 参考。

Amazon Macie 的定价

与其它 AWS 产品一样，在使用 Amazon Macie 时，您无需签订合同或承诺最低使用量。

Macie 的定价基于多个维度：评测和监控 S3 存储桶以实现安全性和访问控制，监控 S3 对象以自动敏感数据发现，以及分析 S3 对象以发现和报告对象中的敏感数据。有关更多信息，请参阅 Amazon Macie 定价。

为了帮助您了解和预测使用 Macie 的费用，Macie 为您的账户提供了估计的使用费用。你可以在 Amazon Macie 主机上查看这些估算值，然后使用 Amazon Macie API 进行访问。根据您使用服务的方式，将其他 AWS 服务 功能与某些 Macie 功能结合使用可能会产生额外费用，例如从 Amazon S3 检索存储桶数据以及使用客户管理的 AWS KMS keys 解密对象以进行分析。

当您首次启用 Macie 时，您的 AWS 账户 账户会自动注册 30 天的 Macie 免费试用。这包括作为 AWS Organizations 中组织的一部分启用的个人账户。在免费试用期间，在适用 AWS 区域 中使用 Macie 来评测和监控 S3 存储桶的安全性和访问控制不收取任何费用。根据您的账户设置，免费试用还可能包括对您的 Amazon S3 数据执行自动敏感数据发现。免费试用不包括运行敏感数据发现作业来发现和报告 S3 对象中的敏感数据。

为了帮助您了解和预测免费试用期结束后使用 Macie 的费用，Macie 会根据您在试用期间使用 Macie 的情况向您提供估算的使用成本。您的使用数据还会显示免费试用期结束之前的剩余时间。您可以在 Amazon Macie 主机上查看这些数据，然后使用 Amazon Macie API 进行访问。

相关服务

为了进一步保护您在 AWS 中的数据、工作负载和应用程序，请考虑将以下 AWS 服务 各项与 Amazon Macie 结合使用。

AWS Security Hub

AWS Security Hub 让您全面了解 AWS 资源的安全状态，并帮助您根据安全行业标准和最佳实践检查您的 AWS 环境。它部分是通过使用、汇总、整理和优先考虑来自多个 AWS 服务（包括 Macie）和支持的 AWS 合作伙伴网络 (APN) 产品的安全调查发现来实现的。Security Hub 可以帮助您分析安全趋势，并识别整个 AWS 环境中最高优先级的安全问题。

要了解有关 Security Hub 的更多信息，请参阅 AWS Security Hub 用户指南。要了解如何同时使用 Macie 和 Security Hub，请参阅 Amazon Macie 与 AWS Security Hub 集成。

Amazon GuardDuty

Amazon GuardDuty 是一项安全监控服务，用于分析和处理特定类型的 AWS 日志，例如 Amazon S3 的 AWS CloudTrail 数据事件日志和 CloudTrail 管理事件日志。它使用威胁情报源（例如，恶意 IP 地址和域的列表）和机器学习来标识您 AWS 环境中意外和未经授权的恶意活动。

有关 GuardDuty 更多信息，请参阅 Amazon GuardDuty 用户指南。

要了解其他 AWS 安全服务，请参阅 AWS 上的安全、身份和合规性。

Amazon Macie 入门

本教程介绍了 Amazon Macie。您将了解如何为您的 AWS 账户 启用 Macie。您还将学习如何评测您的 Amazon Simple Storage Service (Amazon S3) 安全态势，以及如何配置 Macie 的关键设置，以发现和报告 S3 存储桶中的敏感数据。

任务

开始前的准备工作

当您注册 Amazon Web Services 时 (AWS)，您的账户会自动注册所有 AWS 服务，包括 Amazon Macie。但是，要启用和使用 Macie，首先必须设置允许您访问 Amazon Macie 控制台和 API 操作的权限。为此，您或您的 AWS 管理员可以使用 AWS Identity and Access Management (IAM) 将名为 `AmazonMacieFullAccess` 的 AWS 托管策略附加到您的 IAM 身份。要了解更多信息，请参阅 适用于 Amazon Macie 的 AWS 托管式策略。

步骤 1：启用 Amazon Macie

设置所需权限后，您可以为您的 AWS 账户 启用 Amazon Macie。按照以下步骤为您的账户启用 Macie。

启用 Macie

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要启用并使用 Macie 的区域。
3. 在 Amazon Macie 页上，选择 开始。
4. （可选）启用 Macie 时，Macie 自动创建一个服务相关角色，让 Macie 拥有代表您调用其他 AWS 服务 和监控 AWS 资源所需的权限。要查看此角色的权限策略，请在控制台上选择查看角色权限。要了解有关此角色的更多信息，请参阅 Amazon Macie 的服务相关角色。

5. 选择 Enable Macie (启用 Macie)。

几分钟之内，Macie 就会自动生成并开始维护当前区域中 S3 存储桶的完整清单。Macie 还开始评测和监控这些存储桶以确保安全性和进行访问控制。要了解更多信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。

根据您的账户设置，Macie 还会开始对您的 S3 存储桶执行自动敏感数据发现。Macie 开始不断识别、选择和分析存储桶中具有代表性的 S3 对象，检查这些对象中是否有敏感数据。随着分析的进行，Macie 会提供统计数据和其他结果供您查看，通常是在为您的账户启用 Macie 后的 48 小时内。您可以通过为账户配置自动敏感数据发现设置来定制分析。要了解更多信息，请参阅 自动敏感数据发现的工作原理。

要查看聚合统计数据，请在控制台的导航窗格中选择概要。要查看清单中各个 S3 存储桶的详细信息，请在导航窗格中选择 S3 存储桶。要随后显示存储桶的详细信息，请选择存储桶。详细信息面板显示统计数据和其他信息，可让您深入了解存储桶数据的安全性、隐私性和敏感性。要了解有关这些细节的更多信息，请参阅 查看 S3 存储桶清单。

步骤 2：配置存储库以获取敏感数据发现结果

借助 Amazon Macie，您可以通过两种方式发现 S3 存储桶中的敏感数据：将 Macie 配置为自动敏感数据发现，以及运行敏感数据发现作业。敏感数据发现作业是您创建的作业，用于分析 S3 存储桶中的对象以确定这些对象是否包含敏感数据。

当您运行敏感数据发现作业或执行自动敏感数据发现时，Macie 为其分析的每个 S3 对象创建一条记录。这些记录称为敏感数据发现结果，记录有关单个对象分析的详细信息。Macie 还会为由于错误或问题而无法分析的对象创建敏感数据发现结果。敏感数据发现结果为您提供分析记录，这些记录可能有助于数据隐私和保护审计或调查。

Macie 仅将您的敏感数据发现结果存储 90 天。要访问结果并对其进行长期存储和保留，请将 Macie 配置为将结果存储在 S3 存储桶中。您应该在启用 Macie 后的 30 天内完成此操作。完成此操作后，存储桶可以作为所有敏感数据发现结果的权威长期存储库。

要了解如何配置此存储库，请参阅存储和保留敏感数据发现结果。

步骤 3：探索调查发现样本

在 Amazon Macie 中，调查发现是 Macie 检测到的 S3 存储桶或 Macie 在 S3 对象中检测到的敏感数据的潜在策略违规的详细报告。Macie 提供了两类调查发现，即政策调查发现和敏感数据调查发现。当存储桶的策略或设置发生更改而降低了存储桶及其对象的安全性或隐私性时，Macie 会创建一个策略调

查发现。当 Macie 在 S3 对象中检测到敏感数据时，Macie 会创建敏感数据调查发现。在每个类别中，都有多种类型的调查发现。

要探索和了解 Macie 提供的不同类别和类型的调查发现，可以选择创建和查看样本调查发现。样本调查发现使用示例数据和占位符值来演示 Macie 可能包含在每类调查发现中的信息类型。

按照以下步骤创建和查看样本调查发现。

创建和查看样本调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Settings (设置)。
3. 在 Sample findings 下，选择 Generate sample findings。Macie 会为 Macie 支持的每种调查发现生成一个样本调查发现。
4. 在导航窗格中，选择 Findings (结果)。调查发现页面显示当前 AWS 区域 中您的账户的调查发现。这包括您在前面步骤中创建的样本调查发现。
5. 在 调查发现页面上，找到类型以 [样本]开头的调查发现。
6. 要查看特定样本调查发现的详细信息，请选择该调查发现。详细信息面板显示了调查发现的详细信息。

要了解有关每种类型的调查发现的更多信息，请参阅 调查发现的类型。要了解有关创建和查看样本调查发现的更多信息，请参阅 处理样本调查发现。

步骤 4：创建发现敏感数据的作业

要发现和报告 S3 存储桶中的敏感数据，您可以运行敏感数据发现作业。敏感数据发现作业是您创建的作业，用于分析 S3 存储桶中的对象以确定这些对象是否包含敏感数据。与自动敏感数据发现不同，您可以定义分析的广度和深度。您还可以指定运行作业的频率，即按计划运行一次或定期运行。

按照以下步骤创建一个作业，该作业将在您创建后立即运行一次，并使用默认设置。要了解如何创建定期运行或使用自定义设置的作业，请参阅创建敏感数据发现作业。

创建敏感数据发现作业

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 请选择 Create job (创建任务)。

4. 在 选择 S3 存储桶步骤中，选择选择特定存储桶。然后，在表中选中要作业分析的每个 S3 存储桶对应的复选框。

   该表提供了当前 AWS 区域 中您的 S3 存储桶的完整清单。要更轻松地查找特定存储桶，请在表格上方的筛选框中输入筛选标准。还可以选择表中的列标题对表进行排序。
5. 选择完存储桶后，选择下一步。
6. 在 查看 S3 存储桶步骤中，查看并验证您的存储桶选择，然后选择 下一步。
7. 在 缩小范围步骤中，选择 一次性作业，然后选择下一步。
8. 在 选择托管数据标识符步骤中，选择 推荐。（可选）查看我们为作业推荐的托管数据标识符表，然后选择 下一步。

   托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如信用卡号、AWS 秘密访问密钥或特定国家或地区的护照号码。要了解更多信息，请参阅 使用托管数据标识符。
9. 在 选择自定义数据标识符步骤中，选择 下一步。

   自定义数据标识符是您定义的一组检测敏感数据的标准，即定义要匹配的文本模式的正则表达式（regex）和可选的字符序列，以及优化结果的邻近规则。要了解更多信息，请参阅 构建自定义数据标识符。
10. 在 选择允许列表步骤中，选择 下一步。

    在 Macie 中，允许列表指定了您希望 Macie 在检查 S3 对象是否存在敏感数据时忽略的文本或文本模式。这些通常是特定场景或环境的敏感数据异常。要了解更多信息，请参阅 使用允许列表定义敏感数据例外。
11. 在 输入常规设置步骤中，输入作业的名称和描述（可选）。然后选择下一步。
12. 对于 检查和创建步骤，检查作业的配置设置并验证它们是否正确。

    您还可以查看运行作业的总估计成本（以美元计）。该估算值可以帮助您在保存作业之前确定是否要调整作业的设置。要了解更多信息，请参阅 预测敏感数据发现作业的成本。
13. 完成查看和验证作业设置后，选择提交。

Macie 立即开始运行这项作业。要了解如何监控作业，请参阅检查敏感数据发现作业的状态。

步骤 5：查看调查发现

Amazon Macie 自动监控您的 S3 存储桶以实现安全性和访问控制，并且创建策略调查发现来报告存储桶安全或隐私方面的潜在问题。如果您创建并运行敏感数据发现作业，或者将 Macie 配置为执行自动

敏感数据发现，Macie 还会创建敏感数据调查发现以报告其在 S3 对象中检测到的敏感数据。要了解有关调查发现的更多信息，请参阅 分析调查发现。

请按照以下步骤查看您的调查发现。

查看调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。调查发现页面显示当前 AWS 区域 中您的账户的调查发现。
3. （可选）要按特定条件筛选调查发现，请在表格上方的筛选框中输入标准。
4. 要查看特定调查发现的详细信息，请选择该调查发现。详细信息面板显示了调查发现的详细信息。

要了解更多信息，包括如何对调查发现进行分组和筛选，请参阅查看调查发现。

Amazon Macie 概念和术语

在 Amazon Macie 中，我们在 的基础上建立通用 AWS 概念和术语，并使用这些附加术语。

account

一个包含您AWS的资源和可以访问这些资源的身份的标准AWS 账户。

要使用 Macie，您需要使用自己的AWS 账户凭证登录AWS，选择要在其中使用 Macie 的AWS 区域，然后在该地区为您的 AWS 账户 启用 Macie。有关更多信息，请参阅Amazon Macie 入门。

Macie 中有三种类型的账户：

- 管理员账户 - 这种类型的账户管理组织的 Macie 账户。组织是一组 Macie 账户，它们相互关联，并作为特定 AWS 区域 中的一组相关账户进行集中管理。
- 成员账户 - 此类账户与组织的 Macie 管理员账户关联并由其管理。
- 独立账户 – 这种类型的账户既不是管理员账户，也不是成员账户。它不是组织的一部分。

您可以通过两种方式将 Macie 账户添加到组织：将 Macie 与 AWS Organizations 集成，或者发送和接受 Macie 会员邀请。有关更多信息，请参阅管理多个 账户。

管理员账户

在 Macie 中，一种管理组织的 Macie 账户的账户。组织是一组 Macie 账户，它们相互关联，并作为特定 AWS 区域 中的一组相关账户进行集中管理。

Macie 管理员账户的用户可以访问其组织中所有账户的 Amazon Simple Storage Service (Amazon S3) 库存数据、策略调查发现以及某些 Macie 设置和资源。他们还可以执行自动敏感数据发现，并运行敏感数据发现作业来检测账户拥有的 S3 存储桶中的敏感数据。根据账户被指定为管理员账户的方式，他们可能还能够为组织中的其他账户执行其他任务。

有关更多信息，请参阅管理多个 账户。

允许列表

在 Macie 中，允许列表指定了您希望 Macie 在检查 S3 对象是否存在敏感数据时忽略的文本或文本模式。

您可以在 Macie 中创建两种类型的允许列表：列出要忽略的特定单词和其他类型的字符序列的纯文本文件，或者定义要忽略的文本模式的正则表达式（regex）。如果对象包含与允许列表中的条目或模式匹配的文本，Macie 不会在敏感数据调查发现、统计数据和其他类型的结果中报告该文本，即使该文本与托管数据标识符或自定义数据标识符的标准匹配。

有关更多信息，请参阅使用允许列表定义敏感数据例外。

自动敏感数据发现

Macie 持续执行的一系列自动分析活动，用于从 S3 存储桶中识别和选择具有代表性的对象，并检查所选对象中是否有敏感数据。

随着分析的进行，Macie 会生成其调查发现的敏感数据（敏感数据调查发现）及其执行的分析（敏感数据发现结果）的记录。Macie 还会更新其提供的有关 Amazon S3 数据的统计数据和其他信息。

有关更多信息，请参阅执行自动敏感数据发现。

AWS安全调查发现格式 (ASFF)

一种标准化 JSON 格式，用于显示发布给 AWS Security Hub 或由其生成的调查发现的内容。ASFF 包括有关安全问题根源、受影响资源以及调查发现当前状态的详细信息。

有关 ASFF 的更多信息，请参阅 《AWS Security Hub 用户指南》中的 AWS 安全调查发现格式 (ASFF)。有关将 Macie 调查发现发布到 Security Hub 的信息，请参阅 Amazon Macie 与 AWS Security Hub 集成。

可分类的字节或大小

在 Macie 提供的 S3 存储桶统计数据中，S3 存储桶中所有可分类对象的总存储大小。

如果对存储桶启用了版本控制，则该值基于存储桶中每个可分类对象的最新版本的存储大小。如果对象是压缩文件，则该值并不反映文件解压后文件内容的实际大小。

有关更多信息，请参阅 查看 S3 存储桶清单 和 评测您的 Amazon S3 安全状况。

可分类对象

Macie 可以分析以检测敏感数据的 S3 对象。

在计算 S3 存储桶统计数据时，Macie 会根据对象的存储类别和文件扩展名确定该对象是否可分类。如果对象使用支持的 Amazon S3 存储类并且具有支持的文件或存储格式的文件扩展名，则该对象可分类。

有关更多信息，请参阅 查看 S3 存储桶清单 和 评测您的 Amazon S3 安全状况：

为了发现敏感数据，Macie 会根据对象的存储类别、文件扩展名和内容来确定该对象是否可分类。如果满足以下条件，则对象可分类：它使用受支持的 Amazon S3 存储类，它具有受支持的文件或存储格式的文件扩展名，并且 Macie 验证它可以从对象中提取和分析数据。

有关更多信息，请参阅 发现敏感数据 和 预测和监控成本：

自定义数据标识符

您定义的一组用于检测敏感数据的标准。

标准由定义要匹配的文本模式的正则表达式（regex）和可选的字符序列以及优化结果的邻近规则组成。字符序列可以是：

- 关键字，即必须靠近匹配正则表达式的文本的字词或短语，或者
- 忽略字词，即要从结果中排除的字词或短语。

除了检测标准外，您还可以为自定义数据标识符生成的敏感数据调查发现定义自定义严重性设置。

有关更多信息，请参阅构建自定义数据标识符。

筛选规则

您创建并保存的一组基于属性的筛选标准，用于在 Amazon Macie 控制台上分析调查发现。筛选规则可以帮助您对具有特定特征的调查发现进行一致的分析，例如所有报告特定类型敏感数据的高严重性调查发现。

有关更多信息，请参阅创建和管理调查发现筛选规则。

调查发现

Macie 在 S3 对象中发现的敏感数据或 S3 存储桶安全或隐私方面的潜在问题的详细报告。每个调查发现都提供了详细信息，例如严重性评级、有关受影响资源的信息以及 Macie 发现数据或问题的时间。

Macie 生成两类调查发现：敏感数据调查发现（针对 Macie 在 S3 对象中检测到的敏感数据）和策略调查发现（针对 Macie 在 S3 存储桶的安全和访问控制设置中检测到的潜在问题）。每个类别中都有特定类型的调查发现。

有关更多信息，请参阅Amazon Macie 调查发现的类型。

调查发现事件

一个 Amazon EventBridge 事件，其中包含敏感数据调查发现或策略调查发现的详细信息。

Macie 会自动将敏感数据调查发现和策略调查发现作为事件发布到 Amazon EventBridge。事件都是一个符合 AWS 事件 EventBridge 架构的 JSON 对象。您可以通过使用其他应用程序、服务和系统，使用这些事件来监视、处理调查发现并根据调查发现采取行动。

有关更多信息，请参阅 Amazon Macie与 Amazon EventBridge 集成 和 用于 Amazon Macie 调查发现的 Amazon EventBridge 事件架构：

作业

参见敏感数据发现作业。

托管数据标识符

一组内置标准和技术，旨在检测特定类型的敏感数据。敏感数据的示例包括信用卡号、AWS秘密访问密钥或者特定国家或地区的护照号码。这些标识符可以检测许多国家和地区的大量且不断增长的敏感数据类型。

有关更多信息，请参阅使用托管数据标识符。

成员账户

由组织指定的 Macie 管理员账户管理的 Macie 账户。组织是一组 Macie 账户，它们相互关联，并作为特定 AWS 区域 中的一组相关账户进行集中管理。

账户可以通过两种方式成为成员账户：将 Macie 与 AWS Organizations 中账户组织集成，或者接受 Macie 会员资格邀请。

如果您拥有成员账户，则您的 Macie 管理员可以访问您的账户的 Amazon S3 清单数据、政策调查发现以及某些 Macie 设置和资源。您的管理员还可以执行自动敏感数据发现并运行敏感数据发现作业，

以检测您的 S3 存储桶中的敏感数据。他们可能还能为您的账户执行其他任务，具体取决于您的账户如何成为成员账户。

有关更多信息，请参阅管理多个 账户。

organization

一组 Macie 账户，它们相互关联，并作为特定 AWS 区域 中的一组相关账户进行集中管理。

每个组织都由一个指定的 Macie 管理员账户和一个或多个关联的成员账户组成。管理员账户可以访问成员账户的某些 Macie 设置、数据和资源。您可以通过两种方式创建组织：将 Macie 与 AWS Organizations 集成，或者在 Macie 中发送和接受会员邀请。

有关更多信息，请参阅管理多个 账户。

策略调查发现

关于 S3 存储桶的潜在策略违反情况或其安全和访问控制设置存在问题的详细报告。详细信息包括严重性评级、有关受影响资源的信息以及 Macie 发现问题的时间。

当 S3 存储桶的策略或设置更改导致存储桶及其对象的安全性或隐私性降低时，Macie 会生成策略调查发现。Macie 生成这些调查发现，作为其对您的 Amazon S3 数据的持续监控活动的一部分。Macie 可以生成多种类型的策略调查发现。

有关更多信息，请参阅 Amazon Macie 调查发现的类型 和 监控数据安全和隐私：

示例调查发现

使用示例数据和占位符值来演示调查发现可能包含的信息类型的调查发现。

有关更多信息，请参阅处理样本调查发现。

敏感数据调查发现

这是 Macie 在 S3 对象中发现的敏感数据的详细报告。详细信息包括：严重性等级、有关受影响资源的信息、Macie 发现的敏感数据的类型和出现次数，以及 Macie 发现敏感数据的时间。

如果 Macie 在您运行敏感数据发现作业时分析的 S3 对象中检测到敏感数据，或者在其执行自动敏感数据发现时检测到敏感数据，会生成敏感数据调查发现。Macie 可以生成几种类型的敏感数据调查发现。

有关更多信息，请参阅 Amazon Macie 调查发现的类型 和 发现敏感数据：

敏感数据发现作业

也称为作业，是 Macie 执行的一系列自动处理和分析任务，用于检测和报告 S3 对象中的敏感数据。创建作业时，您需要指定希望作业运行的频率，并定义作业分析的范围和性质。

在运行作业时，Macie 会生成其发现的敏感数据（敏感数据调查发现）及其执行的分析（敏感数据发现结果）的记录。Macie 还会将日志数据发布到 Amazon CloudWatch Logs。

有关更多信息，请参阅运行敏感数据发现作业。

敏感数据发现结果

记录有关 Macie 为确定该对象是否包含敏感数据而对 S3 对象执行的分析的详细信息的记录。Macie 生成这些记录并将其写入 JSON Lines (.jsonl) 文件，然后对其进行加密并存储在您指定的 S3 存储桶中。记录遵循标准化架构。

当您运行敏感数据发现作业 或 Macie 执行自动敏感数据发现时，Macie 会为分析范围中包含的每个对象创建敏感数据发现结果。这包括：

- Macie 在其中检测到敏感数据的对象，因此也会生成敏感数据调查发现。
- Macie 没有在其中检测到敏感数据的对象，因此不会生成敏感数据调查发现。
- Macie 由于错误或问题（例如权限设置或使用不受支持的文件或存储格式）而无法分析的对象。

有关更多信息，请参阅存储和保留敏感数据发现结果。

单独账户

在组织中既不是管理员也不是成员账户的 Macie 账户。它不是组织的一部分。

抑制的调查发现

根据抑制规则自动存档的调查发现。也就是说，Macie 自动将调查发现的状态更改为已存档，因为在 Macie 生成调查发现时，该发现符合抑制规则的标准。

有关更多信息，请参阅取消发现结果。

抑制规则

一组基于属性的筛选标准，您可以创建并保存这些标准以自动存档（抑制）调查发现。如果您已经查看了一类调查发现并且不想再次收到有关这些发现的通知，则抑制规则会很有用。

如果您使用抑制规则抑制调查发现，Macie 会继续生成符合该规则标准的调查发现。但是，Macie 会自动将调查发现的状态更改为已存档。这意味着默认情况下，这些调查发现不会出现在 Amazon Macie 控制台上，Macie 也不会将其发布给其他 AWS 服务。

有关更多信息，请参阅取消发现结果。

不可分类的字节或大小

在 Macie 提供的 S3 存储桶统计数据中，S3 存储桶中所有不可分类的对象的总存储大小。

如果对存储桶启用了版本控制，则该值基于存储桶中每个不可分类的对象的最新版本的存储大小。如果对象是压缩文件，则该值并不反映文件解压后文件内容的实际大小。

有关更多信息，请参阅 查看 S3 存储桶清单 和 评测您的 Amazon S3 安全状况：

不可分类的对象

Macie 无法通过分析以检测其中的敏感数据的 S3 对象。

在计算 S3 存储桶统计数据时，Macie 会根据对象的存储类别和文件扩展名确定该对象是否不可分类。如果一个对象不使用支持的 Amazon S3 存储类或者没有支持的文件或存储格式的文件扩展名，则该对象不可分类。

有关更多信息，请参阅 查看 S3 存储桶清单 和 评测您的 Amazon S3 安全状况：

为了发现敏感数据，Macie 会根据对象的存储类别、文件扩展名和内容来确定该对象是否不可分类。如果出现以下情况，则对象不可分类：它不使用支持的 Amazon S3 存储类、没有支持的文件或存储格式的文件扩展名，或者 Macie 无法从对象中提取和分析数据。例如，该对象是一个格式错误的文件。

有关更多信息，请参阅 发现敏感数据 和 预测和监控成本：

使用 Amazon Macie 监控数据安全和隐私

当您为您的 AWS 账户 启用 Amazon Macie 时，Macie 会自动生成并开始维护当前 AWS 区域 中的 Amazon Simple Storage Service (Amazon S3) 存储桶的完整清单。Macie 还开始评测和监控这些存储桶以确保安全性和进行访问控制。如果 Macie 检测到降低 S3 存储桶安全性或隐私的事件，Macie 会创建一个策略调查发现供您查看并在必要时进行补救。

要同时评测和监控 S3 存储桶中是否存在敏感数据，您可以创建和运行敏感数据发现任务。敏感数据发现任务可以每天、每周或每月对存储桶对象执行增量分析。根据您的账户设置，您还可以将 Macie 配置为对存储桶执行自动敏感数据发现。自动敏感数据发现使用采样技术持续识别、选择和分析存储桶中的代表性对象。如果 Macie 在 S3 对象中检测到敏感数据，Macie 会创建一个敏感数据调查发现来通知您 Macie 找到敏感数据。有关更多信息，请参阅 发现敏感数据。

除了调查发现外，Macie 还能持续监控您的 Amazon S3 数据的安全性和隐私。要评测您的数据的安全状况并确定在何处采取行动，您可以使用控制台上的摘要仪表板。控制面板提供您的 Amazon S3 数据的汇总统计数据的快照。统计数据包括关键安全指标的数据，例如可公开访问或与其他 AWS 账户 共享的存储桶的数量。控制面板还会显示您账户的汇总调查发现数据组，例如，在过去 7 天内发现次数最多的 1-5 个存储桶的名称。您可以深入研究每个统计数据以查看其支持数据。如果您更倾向于以编程方式查询统计数据，请使用 Amazon Macie API 的 GetBucketStatistics 操作。

为了进行更深入的分析和评测，Macie 还提供了清单中各个 S3 存储桶的详细信息和统计数据。这包括每个存储桶的公共访问和加密设置的明细，以及 Macie 可以分析以检测存储桶中敏感数据的对象的大小和数量。清单还会显示您是否配置了任何敏感数据发现任务来分析存储桶中的对象，如果是，则显示其中一个任务最近运行的时间。您可以使用 Amazon Macie 控制台或 Amazon Macie API 的 DescribeBuckets 操作来浏览、排序和筛选库存。

如果您是组织的 Macie 管理员，则可以访问有关您的成员账户拥有的 S3 存储桶的统计数据和其他数据。您还可以访问 Macie 为存储桶创建的策略调查发现，并检查存储桶中是否有敏感数据。作为 Macie 管理员，您可以使用 Macie 来评测和监控贵组织的 Amazon S3 数据资产的整体安全状况。有关更多信息，请参阅 管理多个 账户。

主题

Amazon Macie 如何监控 Amazon S3 数据安全性

当您为 AWS 账户 启用 Amazon Macie 时，Macie 会为您在当前 AWS 区域 中的账户创建一个 AWS Identity and Access Management (IAM) 服务相关角色。此角色的权限策略允许 Macie 代表您调用其他 AWS 服务并监控 AWS 资源。通过使用此角色，Macie 生成并维护区域中 Amazon Simple Storage Service (Amazon S3) 存储桶的完整清单，并且 Macie 监控和评测存储桶的安全性和访问控制。

如果您是组织的 Macie 管理员，则清单包含有关您的账户和组织中的成员账户拥有的 S3 存储桶的统计信息和其他数据。利用这些数据，您可以使用 Macie 来监控和评测您的组织在 Amazon S3 环境中的安全状况。有关更多信息，请参阅管理多个 账户。

主题

关键组件

Amazon Macie 结合使用功能和技术来提供和维护 S3 存储桶的数据，并监控和评测存储桶以实现安全性和访问控制。

收集元数据和计算统计信息

为了生成和维护您的存储桶清单的元数据和统计信息，Macie 会直接从 Amazon S3 检索存储桶和对象元数据。对于每个存储桶，元数据包括：

- 有关存储桶的一般信息，例如存储桶的名称、Amazon 资源名称（ARN）、创建日期、加密设置、标签以及拥有该存储桶的 AWS 账户 的账户 ID。
- 适用于存储桶的账户级别权限设置，例如账户的阻止公有访问设置。
- 存储桶的存储桶级别权限设置，例如存储桶的阻止公有访问设置以及源自存储桶策略或访问控制列表（ACL）的设置。
- 存储桶的共享访问和复制设置，包括存储桶数据是复制到不属于组织的 AWS 账户还是与之共享。
- 存储桶中对象的对象计数和设置，例如存储桶中对象的数量以及按加密类型、文件类型和存储类划分的对象计数明细。

Macie 直接向您提供这些信息。Macie 还使用这些信息来计算统计信息，并对您的整个存储桶清单以及清单中各个存储桶的安全性和隐私性进行评测。例如，您可以找到清单中的总存储大小和存储

桶数量、这些存储桶中的总存储大小和对象数量，以及 Macie 可以分析以检测存储桶中的敏感数据的总存储大小和对象数量。

默认情况下，元数据和统计信息包括由于分段上传不完整而存在的任何对象分段的数据。如果您手动刷新特定存储桶的对象元数据，Macie 会重新计算该存储桶和您的存储桶清单的总体统计信息，并从重新计算的值中排除对象分段的数据。下次 Macie 在每日刷新周期中从 Amazon S3 检索存储桶和对象元数据时，Macie 会更新您的清单数据并再次包含对象分段的数据。有关 Macie 何时检索存储桶和对象元数据的信息，请参阅数据刷新。

请注意，Macie 无法通过分析对象分段检测敏感数据。Amazon S3 必须先将分段重组成一个或多个对象，让 Macie 进行分析。有关分段上传和对象分段的信息，包括如何根据生命周期规则自动删除分段，请参阅 Amazon Simple Storage Service 用户指南中的使用分段上传来上传和复制对象。要识别包含对象分段的存储桶，您可以参考 Amazon S3 Storage Lens 存储统计管理工具中的未完成分段上传。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的评测您的存储活动和使用情况。

监控存储桶的安全性和隐私性

为了帮助确保清单中存储桶级数据的准确性，Macie 会监控和分析 Amazon S3 数据可能发生的某些 AWS CloudTrail 事件。如果发生相关事件，Macie 会更新相应的清单数据。

例如，如果您为存储桶启用阻止公有访问设置，Macie 会更新有关该存储桶公有访问设置的所有数据。同样，如果您为存储桶添加或更新存储桶策略，Macie 会分析该策略并更新清单中的相关数据。

Macie 监控和分析以下 CloudTrail 事件的数据：

- 账户级事件 – DeletePublicAccessBlock 和 PutPublicAccessBlock
- 存储桶级事件 – CreateBucket、DeleteAccountPublicAccessBlock、DeleteBucket、DeleteBucketEncryption、DeleteBu 和 PutBucketVersioning

您无法为其他 CloudTrail 事件启用监控，也无法禁用对上述任何事件的监控。有关上述事件的相应操作的详细信息，请参阅 Amazon Simple Storage Service API 参考。

> **Tip**
>
> 要监控对象级事件，我们建议您使用 Amazon GuardDuty 的 Amazon S3 保护功能。此功能监控对象级的 Amazon S3 数据事件，并分析它们是否存在恶意和可疑活动。有关更多信

息，请参阅《Amazon GuardDuty 用户指南》中的 Amazon GuardDuty 中的 Amazon S3 保护。

评测存储桶的安全性和访问控制

为了评测存储桶级别的安全性和访问控制，Macie 使用基于逻辑的自动推理来分析适用于存储桶的基于资源的策略。Macie 还会分析适用于存储桶的账户和存储桶级别的权限设置。此分析考虑了存储桶策略、存储桶级别 ACL 以及账户和存储桶的阻止公有访问设置。

对于基于资源的策略，Macie 使用 Zelkova。Zelkova 是一种自动推理引擎，可将AWS Identity and Access Management (IAM) policy 转换为逻辑语句，并针对决策问题运行一套通用和专用逻辑求解器（可满足模理论）。Macie 将 Zelkova 重复应用于具有越来越具体查询的策略，以表征该策略允许的行为类别。要详细了解 Zelkova 使用的求解器的性质，请参阅可满足模理论。

Important

要为存储桶执行上述任务，必须允许 Macie 访问该存储桶。如果存储桶的权限设置阻止 Macie 检索该存储桶或存储桶对象的元数据，Macie 只能提供有关该存储桶的信息子集，例如存储桶的名称和创建日期。Macie 无法为存储桶执行任何其他任务。有关更多信息，请参阅允许 Macie 访问 S3 存储桶和对象。

数据刷新

在为您的 AWS 账户启用 Amazon Macie 时，Macie 会直接从 Amazon S3 检索您的 S3 存储桶和对象的元数据。此后，作为每日刷新周期的一部分，Macie 每天自动直接从 Amazon S3 检索存储桶和对象元数据。

在出现以下任一情况时，Macie 还会直接从 Amazon S3 检索桶元数据：

- 您可以通过在 Amazon Macie 控制台上选择刷新 () 来刷新您的清单数据。您可以每五分钟刷新一次数据。
- 您以编程方式向 Amazon Macie API 提交 DescribeBuckets 请求，但在过去的五分钟内您尚未提交 DescribeBuckets 请求。
- Macie 检测到相关 AWS CloudTrail 事件。

如果您选择手动刷新特定存储桶的最新对象元数据，Macie 还可以检索该数据。如果您最近创建了存储桶或在过去 24 小时内对存储桶的对象进行了重大更改，这会很有帮助。要手动刷新存储桶的对象元数据，请在控制台的 S3 存储桶页面的存储桶详细信息面板的对象统计信息部分中选择刷新（ ）。此功能适用于所包含对象数量小于等于 30,000 的存储桶。

每次 Macie 检索存储桶或对象元数据时，Macie 都会自动更新清单中的所有相关数据。如果 Macie 检测到影响存储桶安全性或隐私性的差异，则 Macie 会立即开始评测和分析这些更改。分析完成后，Macie 会更新您的清单中的相关数据。如果任何差异降低了存储桶的安全性或隐私性，则 Macie 还会创建适当的策略调查发现供您在必要时进行查看和补救。

要确定 Macie 最近检索您账户的存储桶或对象元数据的时间，您可以参考控制台上的上次更新时间字段。此字段显示在摘要控制面板和 S3 存储桶页面上，以及 S3 存储桶页面上的存储桶详细信息面板中。（如果您使用 Amazon Macie API 查询清单数据，则该 `lastUpdated` 字段会提供此信息。）如果您是某个组织的 Macie 管理员，则上次更新时间字段会指示 Macie 检索组织中账户数据的最早日期和时间。

在极少数情况下，在某些条件下，延迟和其他问题可能会阻止 Macie 检索存储桶和对象元数据。它们还可能延迟 Macie 收到的有关您的存储桶清单变更或各个存储桶的权限设置和策略的通知。例如，CloudTrail 事件的交付问题可能会导致延迟。如果发生此情况，Macie 会在下次执行每日刷新时（24 小时内）分析新数据和更新后的数据。

其它注意事项

在使用 Amazon Macie 监控和评测 Amazon S3 数据的安全状况时，请记住以下几点：

- 清单数据仅适用于当前 AWS 区域中的 S3 存储桶。要访问其他区域的数据，请在每个其他区域中启用 Macie 并使用它。
- 如果您是组织的 Macie 管理员，则只有在当前区域为成员账户启用了 Macie 后，您才能访问该账户的清单数据。
- 如果存储桶的权限设置阻止 Macie 检索有关该存储桶或存储桶对象的信息，则 Macie 无法评测和监控该存储桶数据的安全性和隐私性，也无法提供有关该存储桶的详细信息。

  为了帮助您识别属于这种情况的存储桶，Macie 会执行以下操作：

  - 在您的存储桶清单中，Macie 会显示该存储桶的警告图标（ ）。对于存储桶的详细信息，Macie 仅显示字段和数据的子集：拥有该存储桶的 AWS 账户的账户 ID；存储桶的名称、Amazon 资源名称（ARN）、创建日期和区域；作为每日刷新周期的一部

分，Macie 最近检索存储桶和存储桶的对象元数据的日期和时间。如果您使用 Amazon Macie API 查询清单数据，Macie 会为存储桶提供错误代码和消息，并且存储桶的大部分属性的值为空。

- 在摘要控制面板上，公有访问、加密和共享统计信息的存储桶的值为未知。（如果您使用 Amazon Macie API 查询统计信息，则这些统计信息的存储桶的值为unknown。）此外，Macie 在计算存储和对象统计信息的数据时会排除存储桶。

要调查该问题，请在 Amazon S3 中查看存储桶的策略和权限设置。例如，存储桶可能具有限制性的存储桶策略。有关更多信息，请参阅允许 Macie 访问 S3 存储桶和对象。

- 有关访问和权限的数据仅限于账户和存储桶级别的设置。它不反映确定对存储桶中特定对象的访问的对象级别设置。例如，如果为存储桶中的特定对象启用了公有访问权限，则 Macie 不会报告该存储桶或该存储桶的对象可公开访问。

  要监控对象级操作并识别潜在的安全风险，我们建议您使用 Amazon GuardDuty 的 Amazon S3 保护功能。此功能监控对象级的 Amazon S3 数据事件，并分析它们是否存在恶意和可疑活动。有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的 Amazon GuardDuty 中的 Amazon S3 保护。
- 如果您手动刷新特定存储桶的对象元数据，Macie 会暂时将适用于对象的加密统计信息报告为未知。下次 Macie 执行每日数据刷新时（24 小时内），Macie 会重新评测对象的加密元数据，并再次报告统计信息的定量数据。
- 如果您手动刷新特定存储桶的对象元数据，由于分段上传不完整，Macie 会暂时排除该存储桶包含的任何对象分段的数据。下次 Macie 执行每日数据刷新时（24 小时内），Macie 会重新计算存储桶对象的数量值和存储大小值，并在这些计算中包括各部分的数据。
- 在极少数情况下，Macie 可能无法确定存储桶是可公开访问还是共享，或者需要对新对象进行服务器端加密。例如，临时问题可能会阻止 Macie 检索和分析必需的数据。或者 Macie 可能无法完全确定一个或多个策略语句是否授予对外部实体的访问权限。在这些情况下，Macie 会将清单中的相关统计信息和字段报告为未知。要调查这些情况，请检查 Amazon S3 中存储桶的策略和权限设置。

另请注意，只有在您为账户启用 Macie 后，存储桶的安全性或隐私性降低时，Macie 才会生成策略调查发现。例如，如果您在启用 Macie 后禁用存储桶的阻止公有访问设置，则 Macie 会为该存储桶生成策略：IAMUser/S3BlockPublicAccessDisabled 调查发现。但是，如果您在启用 Macie 时禁用了 S3 存储桶的阻止公共访问设置，并且这些设置继续处于禁用状态，则 Macie 不会为该存储桶生成 Policy:IAMUser/S3BlockPublicAccessDisabled 调查发现。

此外，当 Macie 评测存储桶的安全性和隐私性时，它不会检查访问日志，也不会分析账户的用户、角色和其他相关配置。相反，Macie 会分析和报告指明潜在安全风险的关键设置数据。例如，如果一个策略调查发现指明存储桶可公开访问，则不一定意味着外部实体访问了该存储桶。同样，如果策略调查发

现表明存储桶与组织外部的 AWS 账户共享，则 Macie 不会尝试确定此访问是否为预期行为且安全。相反，这些调查发现指明外部实体可能会访问存储桶的数据，这可能会带来意想不到的安全风险。

使用 Amazon Macie 评测您的 Amazon S3 安全状况

要评测您的 Amazon Simple Storage Service (Amazon S3) 数据的整体安全状况并确定在何处采取行动，您可以使用 Amazon Macie 控制台上的摘要控制面板。

摘要控制面板在当前 AWS 区域中提供您的 Amazon S3 数据的汇总统计信息的快照。统计数据包括关键安全指标的数据，例如可公开访问或与其他 AWS 账户 共享的存储桶的数量。该控制面板还会显示关于您账户的几组调查发现汇总数据 — 例如，过去七天内出现次数最多的调查发现类型。如果您是组织的 Macie 管理员，则控制面板会提供组织中所有账户的汇总统计结果和数据。您可选择按账户筛选数据。

要进行更深入的分析，可以在控制面板上深入挖掘并查看各个项目的支持数据。您还可以使用 Amazon Macie 控制台查看和分析您的 S3 存储桶清单，或者使用 Amazon Macie API 的DescribeBuckets操作以编程方式查询和分析库存数据。

主题

- 显示“摘要”控制面板
- 了解“摘要”控制面板的组件
- 了解“摘要”控制面板上的数据安全统计信息

显示“摘要”控制面板

在 Amazon Macie 控制台上，摘要控制面板在当前 AWS 区域中针对您的 Amazon S3 数据提供汇总统计信息和调查发现数据的快照。如果您更喜欢以编程方式查询统计数据，则可以使用 Amazon Macie API 的GetBucketStatistics操作。

要显示“摘要”控制面板

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择摘要。Macie 会显示摘要控制面板。
3. 要确定 Macie 最近何时从 Amazon S3 为您的账户检索存储桶或对象元数据，请参阅控制面板顶部的上次更新时间字段。有关更多信息，请参阅 数据刷新。
4. 要在控制面板上深入查看某一项的支持数据，请选择该项。

如果您是组织的 Macie 管理员，则控制面板会显示组织中您的账户和成员账户的汇总统计结果和数据。要对控制面板应用筛选条件，以仅显示特定账户的数据，请在控制面板上方的账户框中输入账户 ID。

了解“摘要”控制面板的组件

在摘要控制面板上，统计信息和数据分为几个部分。在控制面板的顶部，您将找到汇总的统计信息，这些统计信息指明您在 Amazon S3 中存储了多少数据，以及 Amazon Macie 可以分析多少这类数据以检测敏感数据。您还可以参考上次更新时间字段来确定 Macie 最近从 Amazon S3 为您的账户检索存储桶或对象元数据的时间。其他部分提供了统计信息和最新调查发现数据，它们可帮助您评测当前 AWS 区域中您的 Amazon S3 数据的安全性、隐私性和敏感性。

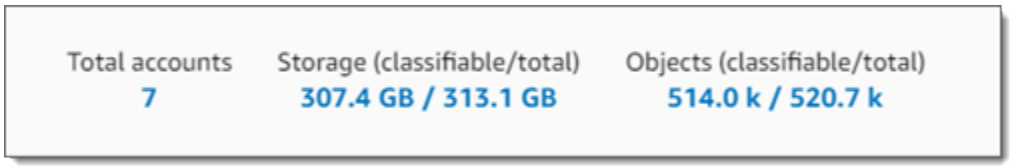
统计信息和数据分为以下几个部分：

存储和敏感数据发现 | 自动发现和覆盖率问题 | 数据安全性 | 最常见的 S3 存储桶 | 最常见的调查发现类型 | 策略调查发现

在查看每个部分时，可以选择一个项目进行深入研究并查看支持数据。

存储和敏感数据发现

控制面板顶部的统计信息会指明您在 Amazon S3 中存储了多少数据，以及 Macie 可以分析多少这类数据来检测敏感数据。例如：



本节内容：

- 账户总数 – 如果您是组织的 Macie 管理员或拥有独立的 Macie 账户，则会显示此字段。它会指明您的 S3 存储桶清单中拥有存储桶的 AWS 账户的总数。如果您是 Macie 管理员，这是您为组织管理的 Macie 账户总数。如果您有一个独立的 Macie 账户，则该值为 1。

  S3 存储桶总数 – 如果您的 Macie 账户是组织的成员，则会显示此字段。它表示您的清单中的存储桶总数，包括不包含任何对象的存储桶。
- 存储 – 这些指标提供有关存储桶清单中对象的存储大小的信息：
  - 可分类 – Macie 可在存储桶中分析的所有对象的总存储大小。
  - 总计 – 存储桶中所有对象的总存储大小，包括 Macie 无法分析的对象。

如果任何对象为压缩文件，则这些值不反映这些文件解压缩后的实际大小。如果对任何存储桶启用了版本控制，则这些值基于这些存储桶中每个对象最新版本的存储大小。

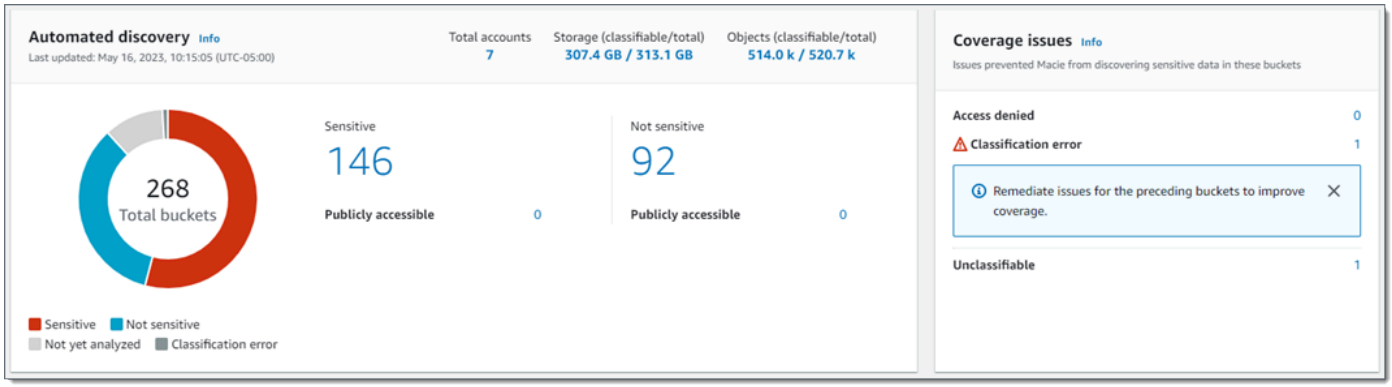
- 对象 – 这些指标提供有关存储桶清单中对象数量的信息：
  - 可分类 – Macie 可在存储桶中分析的对象的总数。
  - 总计 – 存储桶中所有对象的总数，包括 Macie 无法分析的对象。

在上述统计数据中，如果数据和对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式，则数据和对象属于可分类。您可以通过使用 Macie 检测对象中的敏感数据。有关更多信息，请参阅 支持的存储类别和格式。

请注意，存储和对象统计信息不包括 Macie 不允许 Macie 访问的、存储桶内对象的相关数据。例如，具有限制性存储桶策略的存储桶中的对象。要确定存在这种情况的存储桶，您可以通过使用 S3 存储桶表查看存储桶清单。如果存储桶名称旁边出现警告图标 (⚠)，则表示不允许 Macie 访问该存储桶。

自动发现和覆盖率问题

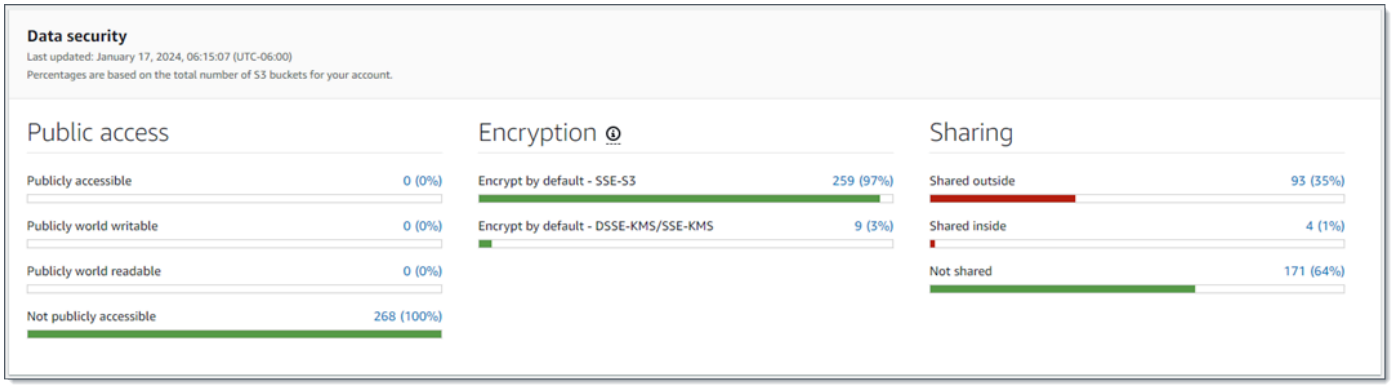
如果为您的账户启用了自动敏感数据发现，则这些部分将显示在控制面板上。这些部分中的统计信息捕获 Macie 迄今为止对您的 Amazon S3 数据执行的自动敏感数据发现活动的状态和结果。例如：



有关这些统计信息的详细信息，请参阅在摘要控制面板上查看数据灵敏度汇总统计数据。

数据安全性

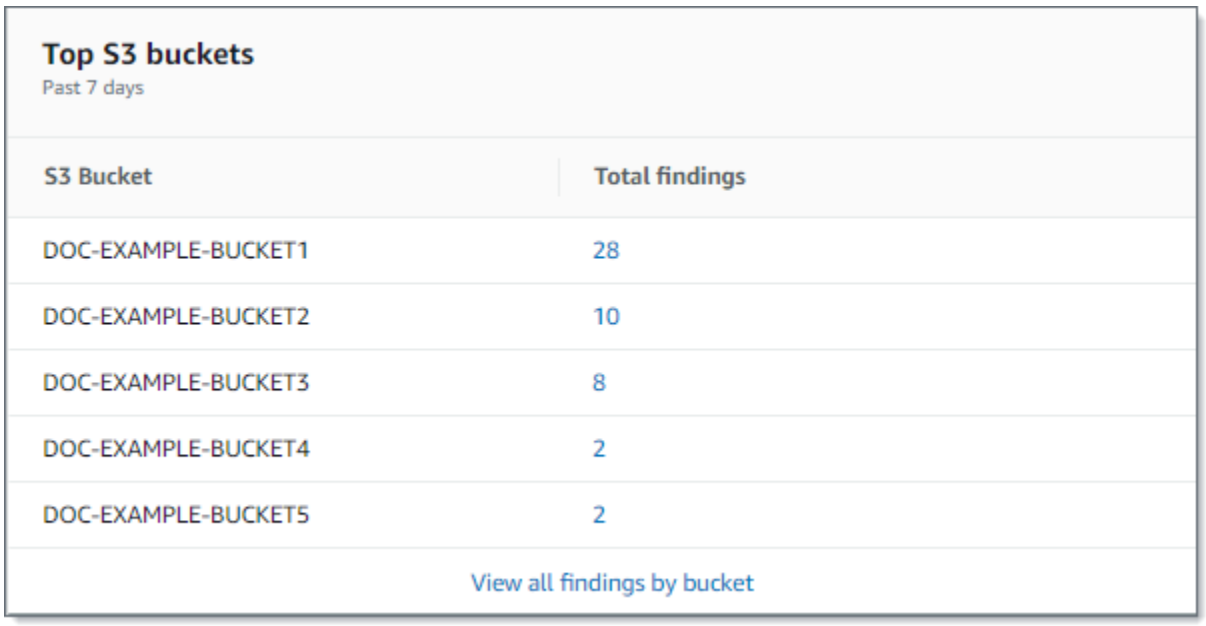
本部分提供的统计信息表明您的 Amazon S3 数据存在潜在的安全性和隐私性风险。例如：



有关这些统计信息的详细信息，请参阅了解“摘要”控制面板上的数据安全统计信息。

最常见的 S3 存储桶

本部分列出过去七天内生成了最多任意类型调查发现的 S3 存储桶，有多达五个存储桶。它还会指明 Macie 为每个存储桶创建的调查发现次数。例如：

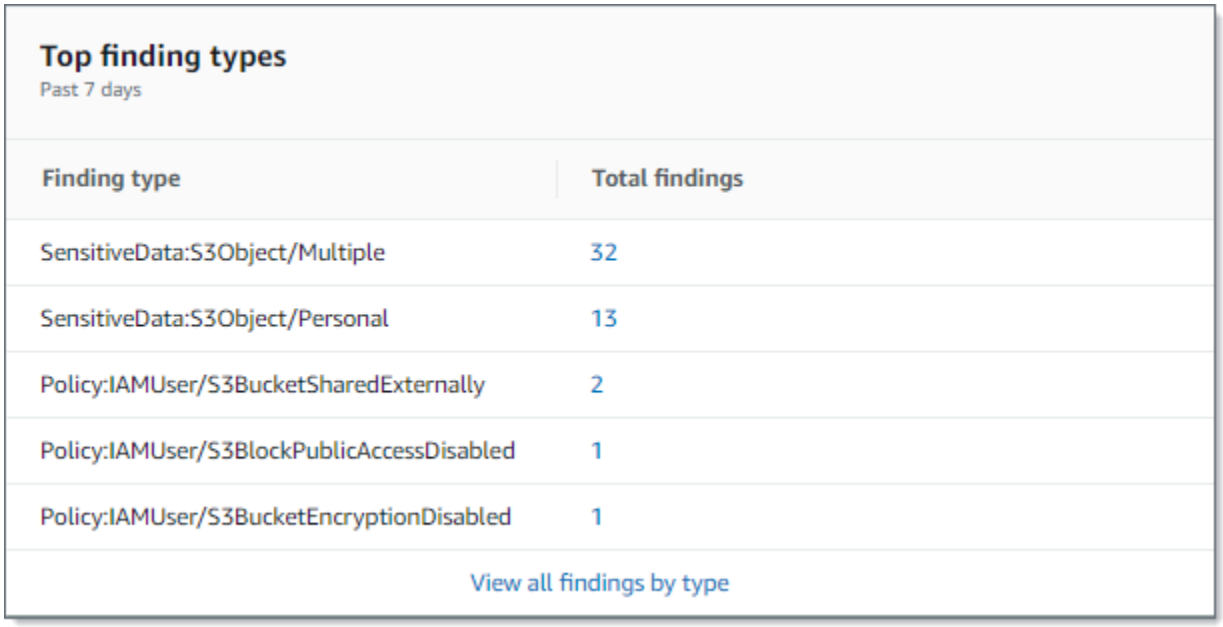


要显示并选择深入了解过去七天内某个存储桶的所有调查发现，请在调查发现总数字段中选择该值。要显示所有存储桶的所有当前调查发现（按存储桶分组），请选择按存储桶查看所有调查发现。

如果 Macie 在过去七天内未创建任何调查发现，则此部分为空。或者在过去七天内创建的所有调查发现均受抑制规则抑制。

最常见的调查发现类型

本部分列出过去七天内出现次数最多的调查发现类型，有多达五种类型的调查发现。它还会指明 Macie 为每种类型创建的调查发现次数。例如：



要显示并选择深入了解过去七天内特定类型的所有调查发现，请在调查发现总数字段中选择该值。要显示按调查发现类型分组的所有当前调查发现，请选择按类型查看所有调查发现。

如果 Macie 在过去七天内未创建任何调查发现，则此部分为空。或者在过去七天内创建的所有调查发现均受抑制规则抑制。

策略调查发现

本部分列出 Macie 最近创建或更新的策略调查发现，有多达十项调查发现。例如：

要显示特定调查发现的详细信息，请选择该调查发现。

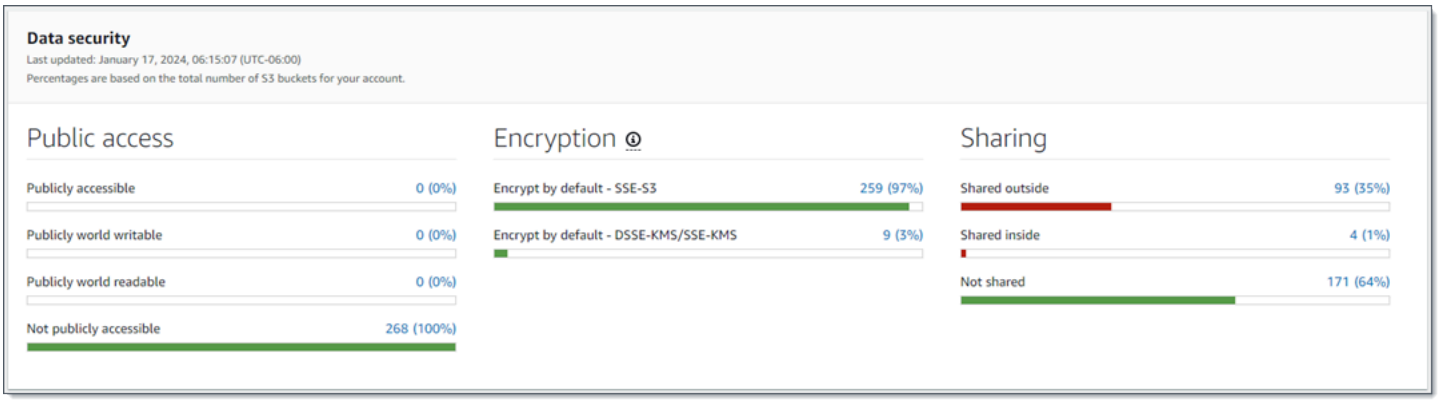
如果 Macie 在过去七天内未创建或更新任何策略调查发现，则此部分为空。或者在过去七天内创建或更新的所有策略调查发现均受抑制规则抑制。

了解“摘要”控制面板上的数据安全统计信息

摘要控制面板的数据安全性部分提供的统计信息可帮助您识别和调查您在当前 AWS 区域中的 Amazon S3 数据的潜在安全性和隐私性风险。例如，您可以使用这些数据来识别可公开访问或与其他 AWS 账户共享的 S3 存储桶。

如果您的 Macie 账户是组织的成员，则本部分顶部的存储和敏感数据发现统计信息会指明您在 Amazon S3 中存储了多少数据，以及 Macie 可以分析多少这类数据来检测敏感数据。

对于任何类型的 Macie 账户，其他统计信息分为三个区域，如下图中所示。



每个区域中的单独统计信息如下。

公有访问权限

这些统计信息指明有多少个 S3 存储桶可公开访问或不可公开访问：

- 可公开访问 - 允许公众对存储桶进行读或写访问的存储桶的数量和百分比。
- 公开可写 - 允许公众对存储桶进行写访问的存储桶的数量和百分比。
- 公开可读 – 允许公众对存储桶进行读访问的存储桶的数量和百分比。
- 不可公开访问 - 允许公众对存储桶进行读或写访问的存储桶的数量和百分比。

要计算每个百分比，Macie 会将适用存储桶的数量除以存储桶清单中的存储桶总数。

为了确定此部分中的值，Macie 分析每个存储桶的账户级别和存储桶级别设置的组合：账户的阻止公有访问设置；存储桶的阻止公有访问设置；存储桶的存储桶策略；以及存储桶的访问控制列表（ACL）。有关这些设置的信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的身份和访问管理和阻止对您的 Amazon S3 存储的公有访问。

在某些情况下，公有访问部分还会显示未知的值。如果出现这些值，则 Macie 无法评测指定数量和百分比的存储桶的公有访问设置。例如，由于临时问题或存储桶的权限设置，Macie 无法检索必要的数据。或者 Macie 无法完全确定一个或多个策略语句是否允许外部实体访问存储桶。

加密

这些统计信息会指明有多少 S3 存储桶被配置为对添加到存储桶的对象应用某些类型的服务器端加密：

- 默认加密 – SSE-S3 – 默认加密设置被配置为使用 Amazon S3 托管式密钥加密新对象的存储桶的数量和百分比。对于这些存储桶，将自动使用 SSE-S3 加密对新对象进行加密。
- 默认加密 — DSSE-KMS/SSE-KMS — 默认加密设置配置为使用客户托管密钥或客户托管密钥加密新对象的存储桶的数量和百分比。AWS KMS key AWS 托管式密钥对于这些存储桶，将使用 DSSE-KMS 或 SSE-KMS 加密自动加密新对象。

要计算每个百分比，Macie 会将适用存储桶的数量除以存储桶清单中的存储桶总数。

为了确定本部分中的值，Macie 会分析每个存储桶的默认加密设置。从 2023 年 1 月 5 日开始，Amazon S3 自动应用服务器端加密，并使用 Amazon S3 托管式密钥 (SSE-S3) 作为添加到存储桶的对象的基本加密级别。您可以选择配置存储桶的默认加密设置，改为使用带密钥的服务器端加密 (SSE-KMS) 或使用AWS KMS密钥的双层服务器端加密 (DSSE-KM AWS KMS S)。有关默认加密设置和选项的信息，请参阅 Amazon Simple Storage Service 用户指南中的为 S3 存储桶设置默认服务器端加密行为。

在某些情况下，加密部分还会显示未知的值。如果出现这些值，则 Macie 无法评测指定数量和百分比的存储桶的默认加密设置。例如，由于临时问题或存储桶的权限设置，Macie 无法检索必要的数据。

共享

这些统计数据表明有多少 S3 存储桶与其他AWS 账户、Amazon CloudFront 原始访问身份 (OAI) 或源站访问控制 (OAC) 共享，或 CloudFront 未共享：

- 外部共享 — 与以下一个或多个机构或任意组合共享存储桶的数量和百分比： CloudFront OAI、CloudFront OAC 或不在同一组织中的账户。
- 内部共享 – 与同一组织中的一个或多个账户共享的存储桶的数量和百分比。这些存储桶不与 CloudFront OAI 或 OAC 共享。
- 未共享-未与其他账户、OAI 或 CloudFront CloudFront OAC 共享的存储分区的数量和百分比。

要计算每个百分比，Macie 会将适用存储桶的数量除以存储桶清单中的存储桶总数。

为了确定存储桶是否与其他 AWS 账户存储桶共享，Macie 会分析每个存储桶的存储桶策略和 ACL。此外，组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。有关共享存储桶的 Amazon S3 选项的信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的标识和访问权限管理。

> **Note**
>
> 在某些情况下，Macie 可能会错误地报告存储桶与不在同一个组织中的 AWS 账户共享。如果 Macie 无法完全评测存储桶策略中的 `Principal` 元素与该策略 `Condition` 元素中的某些 AWS 全局条件上下文密钥或 Amazon S3 条件密钥之间的关系，则可能会发生这种情况。适用的条件密钥为：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:Princip` 和 `s3:DataAccessPointArn`。
>
> 要确定各个存储桶是否属于这种情况，请在控制面板上选择外部共享统计信息。在显示的表中，记下每个存储桶的名称。然后使用 Amazon S3 查看每个存储桶的策略，并确定共享访问设置是否符合预期且安全。

为了确定是与 CloudFront OAI 还是 OAC 共享存储桶，Macie 会分析每个存储分区的存储桶策略。CloudFront OAI 或 OAC 允许用户通过一个或多个指定的 CloudFront 分配访问存储桶的对象。有关 CloudFront OAI 和 OAC 的信息，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amazon S3 来源的访问。

在某些情况下，共享部分还会显示未知的值。如果出现这些值，则 Macie 无法确定指定数量和百分比的存储桶是否与其他账户、 CloudFront OAI 或 OAC 共享。 CloudFront 例如，由于临时问题或存储桶的权限设置，Macie 无法检索必要的数据。或者 Macie 无法全面评测存储桶的策略或 ACL。

使用 Amazon Macie 分析您的 Amazon S3 安全状况

为了帮助您对 Amazon Simple Storage Service (Amazon S3) 数据进行深入分析和评测其安全态势，Amazon Macie 会在您使用 Macie 的 AWS 区域 维护您的 S3 存储桶完整清单。要了解 Macie 如何为您维护此清单，请参阅 Macie 如何监控 Amazon S3 数据安全性。如果您是组织的 Macie 管理员，则此清单包括您的成员账户拥有的 S3 存储桶。

通过使用此清单，您可以查看您的 Amazon S3 数据资产，并检查适用于单个 S3 存储桶的关键安全设置和指标的详细信息和统计数据。例如，您可以访问每个存储桶分区的公共访问和加密设置明细，以及 Macie 可以分析用于检测每个存储桶中敏感数据的对象大小和数量。您还可以确定是否配置了任何敏感数据发现作业来分析存储桶中的对象，如果是，则确定其中一个作业最近运行的时间。如果您的账户启用了自动敏感数据发现，您还可以使用清单来查看 Macie 迄今为您的账户或组织执行的自动敏感数据发现活动的结果。有关更多信息，请参阅发现敏感数据。

您可以使用 Amazon Macie 控制台上的 S3 存储桶页面浏览和筛选清单数据。您也可以使用 Amazon Macie API 的 DescribeBuckets 操作以编程方式访问这些清单数据。

主题

通过 Amazon Macie 查看 S3 存储桶清单

在 Amazon Macie 控制台，S3 存储桶页面详细介绍了当前AWS 区域中 Amazon Simple Storage Service (Amazon S3) 数据的安全和隐私。借此页面，您可以查看和分析当前区域内 S3 存储桶的完整清单，并查看各个存储桶的详细信息和统计数据。如果您是组织的 Macie 管理员，则清单将包含组织中成员账户的 S3 桶的详细信息与统计数据。

S3 存储桶页面还会显示 Macie 最近一次从 Amazon S3 检索账户存储桶或对象元数据的时间。您可以在页面顶部的 上次更新时间字段中找到此信息。如果您是组织的 Macie 管理员，则此字段会显示 Macie 为您组织内账户检索数据的最早日期和时间。有关更多信息，请参阅 数据刷新。

请注意，大多数清单数据仅限允许 Macie 通过您的账户访问的存储桶。如果存储桶的权限设置阻止 Macie 检索有关该存储桶或存储桶对象的信息，则 Macie 只能提供有关此存储桶的部分信息。如果特定存储桶出现这种情况，Macie 将您的存储桶清单中显示该存储桶的警告图标 (⚠) 和消息。有关存储桶的详细信息，Macie 仅显示字段和数据子集：拥有该存储桶的 AWS 账户 的账户 ID；存储桶的名称、Amazon 资源名称（ARN）、创建日期和区域；以及 Macie 最近一次在每日刷新周期中检索存储桶和对象元数据的时间。要调查该问题，请在 Amazon S3 中查看存储桶的策略和权限设置。例如，存储桶可能具有限制性的存储桶策略。有关更多信息，请参阅 允许 Macie 访问 S3 存储桶和对象。

如果您更喜欢以编程方式访问和查询库存数据，则可以使用 Amazon Macie API 的DescribeBuckets操作。

主题

查看 S3 存储桶清单

Amazon Macie 控制台上的 S3 存储桶页面提供关于当前AWS 区域中 S3 存储桶的信息。此页面表格显示了清单中每个存储桶的摘要信息。要自定义视图，您可以对表格进行排序和筛选。如果您在表中选择

一个存储桶，则详细信息面板显示有关此存储桶的其他信息。这包括设置详情和统计数据，以及洞察存储桶数据安全和隐私的指标。您可以选择将数据从表中导出至逗号分隔值 (CSV) 文件。

如果您的账户启用了自动敏感数据发现，您还可通过交互式热图查看清单。该地图直观显示了整个 Amazon S3 数据资产的数据敏感度。它采集 Macie 为您的账户或组织执行的、自动敏感数据发现活动的结果。要详细了解相关内容，请参阅使用 S3 存储桶地图观察数据灵敏度。

要查看 S3 存储桶清单

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。S3 存储桶页面显示您的存储桶清单。

   如果页面显示您的存储桶清单的交互式地图，请选择页面顶部的表格
   ()。
   然后，Macie 会显示您的清单中的存储桶数量和存储桶表。
3. 在页面顶部，可以选择刷新
   ()，
   从 Amazon S3 检索最新的存储桶元数据。

   如果信息图标
   ()
   出现在任何存储桶名称旁边，我们建议您这样操作。此图标表明存储桶是在过去 24 小时内创建的，可能是 Macie 在每日刷新周期中最后一次从 Amazon S3 检索存储桶和对象元数据之后创建的。
4. 在 S3 存储桶页面，使用该表查看有关清单内每个存储桶的信息子集：

   - 灵敏度 – 存储桶的当前灵敏度分数。仅当您的账户启用了自动敏感数据发现功能时，才会显示此列。有关 Macie 定义的灵敏度分数范围的信息，请参阅 S3 存储桶的敏感度评分。
   - 存储桶 – 存储桶名称。
   - 账户 – 拥有存储桶的 AWS 账户 账户 ID。
   - 可分类对象 – Macie 可在存储桶中分析以检测敏感数据的对象总数。
   - 可分类大小 – Macie 可在存储桶中分析以检测敏感数据的所有对象的总存储大小。

     注意，此值不反映任何压缩对象在解压缩后的实际大小。此外，如果为存储桶启用了版本控制，则此值将基于存储桶中每个最新版本对象的存储大小。
   - 按作业监控 – 是否将任何敏感数据发现作业配置为：每天、每周或每月定期分析存储桶中的对象。

如果此字段的值为是，则表示该存储桶已显式包含在定期作业中，或者该存储桶在过去 24 小时内符合定期作业的条件。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。

- 最新运行的作业 – 如果将任何一次性或定期的敏感数据发现作业配置为分析存储桶中的对象，则此字段值表示其中一个作业开始运行的最新日期和时间。否则，将该字段留空。

在上述数据中，如果对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式，则对象属于可分类。您可以通过使用 Macie 检测对象中的敏感数据。有关更多信息，请参阅 支持的存储类别和格式。

5. 要使用表格分析清单，请执行以下操作之一：

   - 要按特定字段对表格进行排序，请点击该字段的列标题。若要更改排序顺序，请再次点击列标题。
   - 要筛选表格并仅显示含特定字段值的存储桶，请将光标置于筛选框内，然后为该字段添加筛选条件。若要进一步优化结果，请为其他字段添加筛选条件。有关更多信息，请参阅 筛选您的 S3 存储桶清单。

6. 要查看特定存储桶的详细信息和统计数据，请选择表中的存储桶名称，然后转到详细信息面板。

   > **Tip**
   >
   > 您可以使用存储桶详细信息面板来深入探究很多字段。要显示某个字段中具有相同值的存储桶，请在该字段中选择 。要显示其他字段值的存储桶，请在字段中选择 。

7. 要以 CSV 格式文件导出表内数据，请选择您想导出的每行的复选框，或选中选择列标题中的复选框以选择所有行。然后在页面顶部选择导出到 CSV。您最多可从表格中导出 50,000 行。

查看 S3 存储桶的详细信息

您可在 Amazon Macie 控制台上，使用S3 存储桶页面的详细信息面板查看关于存储桶清单内的单独 S3 存储桶的统计数据和其他信息。这包括设置和指标详细信息和统计数据，这些详细信息和统计数据提供了存储桶数据安全和隐私的洞察。

例如，您可以查看 S3 存储桶的公共访问设置明细，并确定存储桶的配置目的是重复对象还是与其他 AWS 账户分享。您还可以确定是否配置任何敏感数据发现作业，以检查存储桶内是否有敏感数据。如有，则可以访问有关最近运行作业的详细信息，也可以选择显示该作业产生的任何调查发现。

如果您的账户启用了自动敏感数据发现，您还可以使用详细信息面板查看有关单独 S3 存储桶的敏感数据发现统计数据和其他信息。此面板采集 Macie 迄今为止为存储桶执行的、自动敏感数据发现活动的结果。要了解更多详细信息，请参阅 查看各个 S3 存储桶的数据灵敏度详细信息。

要查看 S3 存储桶的详细信息

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。S3 存储桶页面显示您的存储桶清单。
3. 在页面顶部，可以选择刷新 ( )，从 Amazon S3 检索最新的存储桶元数据。
4. 在 S3 存储桶 表或地图中，选择要查看其详细信息的存储桶。此详细信息面板显示有关存储桶的统计数据和其他信息。

详细信息面板中的存储桶统计数据和信息分为以下主要部分：

概述 | 对象统计 | 服务器端加密 | 敏感数据发现 | 公共访问 | 复制 | 标签

在查看每个部分的信息时，您可以选择对某些字段进行转置和向下钻取。要显示某个字段中具有相同值的存储桶，请在该字段中选择 。要显示其他字段值的存储桶，请在字段中选择 。

概述

本部分提供有关存储桶的一般信息，例如存储桶名称、存储桶创建时间以及拥有该存储桶的 AWS 账户的账户 ID。特别值得注意的是，上次更新时间字段指示 Macie 最近从 Amazon S3 中检索存储桶或存储桶对象元数据的时间。

共享访问权限字段表示该存储桶是与其他人共享AWS 账户、Amazon CloudFront 源访问身份 (OAI) 还是 CloudFront 原始访问控制 (OAC)：

- 外部 — 存储桶与以下一个或多个或任意组合共享： CloudFront OAI、CloudFront OAC 或组织外部（不属于）的账户。
- 内部 – 存储桶与组织内部（一部分）的一个或多个账户共享。它不会与 CloudFront OAI 或 OAC 共享。
- 未共享-存储桶未与其他账户、 CloudFront OAI 或 OAC 共享。 CloudFront
- 未知 – Macie 无法评测存储桶的共享访问权限设置。

为了确定存储桶是否与其他AWS 账户共享，Macie 会分析存储桶的存储桶策略和访问控制列表（ACL）。分析仅限于存储桶级设置。它不反映用于共享存储桶内特定对象的任何对象级设置。此外，组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。要了解分享存储桶的 Amazon S3 选项，请参阅 Amazon Simple Storage Service 用户指南 中的 Amazon S3 中的身份和访问管理。

> **Note**
>
> 在某些情况下，Macie 可能会发生错误，指示存储桶与组织外部（非组织内）的AWS 账户共享。如果 Macie 无法完全评测存储桶策略中的 `Principal` 元素与该策略 `Condition` 元素中的某些 AWS 全局条件上下文密钥或 Amazon S3 条件密钥之间的关系，则可能会发生这种情况。适用的条件密钥为：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:PrincipalO` 和 `s3:DataAccessPointArn`。我们建议您检查存储桶的策略，以确定此访问是否为预期行为且是安全的。

为了确定存储桶是与 CloudFront OAI 还是 OAC 共享，Macie 会分析该存储桶的存储桶策略。CloudFront OAI 或 OAC 允许用户通过一个或多个指定的 CloudFront 分配访问存储桶的对象。要了解 CloudFront OAI 和 OAC，请参阅亚马逊 CloudFront 开发者指南中的限制对 Amazon S3 来源的访问。

面板的 概述部分还包括 最近的自动发现运行时间 字段。如果您的账户启用了自动敏感数据发现，则此字段会显示 Macie 最近一次“分析存储桶内对象，同时对账户执行自动发现”的时间。如果您的账户禁用了自动敏感数据发现，则此字段显示短划线 (–)。

对象统计数据

本部分提供关于存储桶对象的信息，首先介绍存储桶内的对象总数（总数）、所有对象的总存储大小（总存储大小），以及所有压缩文件 (.gz、.gzip 或 .zip) 对象的总存储大小（总压缩大小）。本节中的其他统计数据可帮您评测 Macie 可分析的数据量，以检测存储桶内的敏感数据。

如果您最近创建了存储桶，或在过去 24 小时内对存储桶对象进行了重大更改，则可以选择选择刷新
()
以检索存储桶对象的最新元数据。Macie 显示信息图标
()，
以帮助您确定是否可能出现这种情况。如果存储桶包含的对象数量小于等于 30,000 个，则可以使用刷新选项。

查看本节统计数据时，请牢记以下几点：

- 如果为存储桶启用了版本控制，则大小值将基于存储桶中每个最新版本对象的存储大小。
- 如果存储桶内包含压缩对象，则大小值不反映这些对象在解压缩后的实际大小。
- 如果您刷新存储桶的对象元数据，Macie 会临时报告 未知，以获取适用于该对象的加密统计信息。当在 24 小时内对存储桶和对象元数据执行下一次日常刷新，Macie 将重新评测和更新这些统计数据。
- 默认情况下，对象计数和大小值包括：存储桶内包含的、作为不完全分段上传结果的、任何对象部分数据。如果您刷新存储桶对象元数据，Macie 会从重新计算的值中排除对象部分数据。当 Macie 对存储桶和对象元数据执行下一次日常刷新（24 小时内）时，Macie 会重新计算和更新这些统计数据的值，并将对象部分的数据再次纳入值中。

  请注意，Macie 无法通过分析对象部分检测敏感数据。Amazon S3 必须先将分段重组成一个或多个对象，让 Macie 进行分析。有关分段上传和对象分段的信息，包括如何根据生命周期规则自动删除分段，请参阅 Amazon Simple Storage Service 用户指南中的使用分段上传来上传和复制对象。要识别包含对象分段的存储桶，您可以参考 Amazon S3 Storage Lens 存储统计管理工具中的未完成分段上传。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的评测您的存储活动和使用情况。

对象统计信息组织方式如下。

可分类对象

此部分所示为 Macie 可分析的对象总数，用于检测这些对象的敏感数据和总存储大小。这些对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式。您可以通过使用 Macie 检测对象中的敏感数据。有关更多信息，请参阅 支持的存储类别和格式。

不可分类的对象

此部分所示为 Macie 无法分析的对象总数，用于检测这些对象的敏感数据和总存储大小。这些对象不使用所支持的 Amazon S3 存储类别，并且其文件扩展名未表示支持的文件或存储格式。

不可分类的对象：存储分类

本节详细介绍了 Macie 无法分析对象的数量和存储大小，无法分析的原因是这些对象不使用支持的 Amazon S3 存储类别。

不可分类的对象：文件类型

本节详细介绍了 Macie 无法分析对象的数量和存储大小，无法分析的原因是这些对象未使用支持的文件扩展名或存储格式。

按加密类型统计的对象

本节详细介绍了使用 Amazon S3 支持的每种加密类型的对象数量：

- 客户提供-使用客户提供的密钥加密的对象数量。这些对象使用 SSE-C 加密。
- AWS KMS托管 — 使用客户托管密钥AWS 托管式密钥或客户托管密钥加密的对象数量。AWS KMS key这些对象使用 DSSE-KMS 或 SSE-KMS 加密。
- Amazon S3 托管 — 使用 Amazon S3 托管密钥加密的对象数量。这些对象使用 SSE-S3 加密。
- 不加密 – 未加密或未使用客户端加密的对象数量。（如果对象通过客户端加密，Macie 无法访问和报告对象加密数据。）
- 未知 – Macie 没有其当前加密元数据的对象数量。如果您最近选择手动刷新存储桶对象元数据，则通常会发生这种情况。当在 24 小时内对存储桶和对象元数据执行下一次日常刷新，Macie 将加密统计数据。

有关每种支持的加密类型的信息，请参阅《Amazon 简单存储服务用户指南》中的使用加密保护数据。

服务器端加密

本节深入介绍存储桶服务器端加密设置。

按存储桶策略要求加密字段指明在向存储桶添加对象时，存储桶】的策略是否要求对对象进行服务器端加密：

- 否 – 存储桶没有存储桶策略，或者存储桶的策略不要求对新对象进行服务器端加密。如果存在存储桶策略，则它不需要PutObject请求中包含有效的服务器端加密标头。
- 是 – 存储桶策略要求对新对象进行服务器端加密。存储桶的 PutObject 请求必须包含有效的服务器端加密标题。否则，Amazon S3 拒绝该请求。
- 未知 – Macie 无法评测存储桶的策略以确定它是否需要对新对象进行服务器端加密。

在此评测中，有效的服务器端加密标题为：`x-amz-server-side-encryption` 值为`AES256`或 `aws:kms`，`x-amz-server-side-encryption-customer-algorithm`值为`AES256`。有关使用存储桶策略要求对新对象进行服务器端加密的信息，请参阅《A mazon 简单存储服务用户指南》中的使用服务器端加密保护数据。

默认加密字段表示存储桶配置为默认应用于添加到存储桶中的对象的服务器端加密算法：

- AES256 – 存储桶的默认加密设置配置为：通过 Amazon S3 托管密钥加密新对象。新对象通过 SSE-S3 加密法自动加密。
- aws:kms – 存储桶的默认加密设置配置为：通过 AWS KMS key，AWS 托管式密钥 或客户托管密钥加密新对象。新对象使用 SSE-KMS 加密法自动加密。该AWS KMS key字段显示所用密钥的 Amazon 资源名称 (ARN) 或唯一标识符（密钥 ID）。
- aws: kms: dsse — 存储桶的默认加密设置配置为使用客户托管密钥或客户托管密钥加密新对象。AWS KMS key AWS 托管式密钥新对象使用 DSSE-KMS 加密自动加密。该AWS KMS key字段显示所用密钥的 ARN 或密钥 ID。
- 无 – 存储桶的默认加密设置不为新对象指定服务器端加密行为。

从 2023 年 1 月 5 日开始，Amazon S3 自动应用服务器端加密，并使用 Amazon S3 托管式密钥 (SSE-S3) 作为添加到存储桶的对象的基本加密级别。您可以选择配置存储桶的默认加密设置，改为使用带密钥的服务器端加密 (SSE-KMS) 或使用AWS KMS密钥的双层服务器端加密 (DSSE-KM AWS KMS S)。有关默认加密设置和选项的信息，请参阅 Amazon Simple Storage Service 用户指南中的为 S3 存储桶设置默认服务器端加密行为。

敏感数据发现

本节详细介绍了是否将任何敏感数据发现作业配置为：每天、每周或每月定期分析存储桶中的对象。如果由作业主动监控字段的值为是，则该存储桶将明确包含在定期作业中，或者该存储桶在过去 24 小时曾匹配定期作业条件。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。

如果将任何类型的敏感数据发现作业（定期作业或一次性作业）配置为检查存储桶，则最新作业字段将提供最近开始运行任务的唯一标识符。最近作业运行时间字段指示该作业开始运行的时间。

> **Tip**
>
> 要显示作业生成的所有敏感数据调查发现，请选择最近的作业字段中的链接。在出现的作业详细信息面板中，选择面板顶部的显示结果，然后选择显示调查发现。

公有访问权限

本节还指示存储桶是否可公开访问。它还详细介绍决定这种情况的各类账户和存储桶级设置。有效权限字段指示这些设置的累积结果：

- 非公开访问 – 存储桶不可公开访问。
- 公开访问 – 存储桶可公开访问。
- 未知 – Macie 无法评测存储桶的所有公有访问设置。

请注意，此数据仅限账户和存储桶级设置。它不反映允许公有访问特定存储桶对象的对象级设置。

要了解管理存储桶和存储桶数据公开访问的 Amazon S3 设置，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的身份和访问管理和 阻止对 Amazon S3 存储的公共访问。

复制

在本节中，Replicated 字段指示存储桶是否配置为将对象复制到其他存储桶。如果此字段的值为 是，则表示已为此存储桶配置并启用一条或多条复制规则。本部分还列出了拥有目标存储桶的、每个AWS 账户的账户 ID。

外部复制 字段指明存储桶是否配置为：复制AWS 账户的、组织以外的存储桶对象。组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。如果此字段的值为 是，则为该存储桶配置并启用了复制规则，并将该规则配置为：将对象复制到由外部 AWS 账户拥有的存储桶。

> **Note**
>
> 在某些条件下，Macie 可能不正确地指示存储桶配置为将对象复制到外部 AWS 账户 拥有的存储桶。如果目标存储桶是在过去 24 小时内，也就是 Macie 在每日刷新周期中从 Amazon S3 检索存储桶和对象元数据之后在不同的 AWS 区域 中创建，则可能会发生这种情况。
> 要使用 Macie 调查问题，请选择刷新
> ()
> 从 Amazon S3 检索最新的存储桶元数据。然后查看本节的账户 ID 列表。若要进行更深入的调查，请使用 Amazon S3 查看存储桶的复制规则。

要了解复制存储桶对象的 Amazon S3 选项和设置，请参阅 Amazon Simple Storage Service 用户指南中的复制对象。

标签

如果标签与存储桶相关联，则此部分将在面板中显示，并列出这些标签。标签是您可以定义并分配给某些类型的 AWS 资源（包括 S3 存储桶）的标签。每个标签都包含一个必需的标签键和一个可选的标签值。

要了解标签存储桶，请参阅 Amazon Simple Storage Service 用户指南中的使用成本分配 S3 存储桶标签。

使用 Amazon Macie 筛选您的 S3 存储桶清单

要识别并关注具有特定特征的存储桶，您可以在 Amazon Macie 控制台和使用 Amazon Macie API 以编程方式提交的查询中筛选您的 S3 存储桶清单。创建筛选条件时，您可以使用特定的存储桶属性来定义在视图或查询结果中包含或排除存储桶的标准。存储桶属性是存储存储桶特定元数据的字段。

Macie 中的筛选条件包含一个或多个条件。每个条件，也称为标准，由三个部分组成：

- 基于属性的字段，例如存储桶名称、标签键或在作业中定义。
- 一个运算符，例如等于或不等于。
- 一个或多个值。值的类型和数量取决于您选择的字段和运算符。

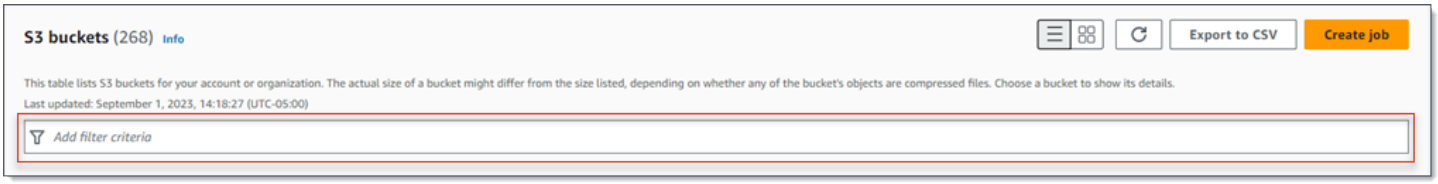
如何定义和应用筛选条件取决于您使用的是 Amazon Macie 主机还是 Amazon Macie API。

主题

- 在 Amazon Macie 主机上筛选您的库存
- 使用 Amazon Macie API 以编程方式筛选您的库存

在 Amazon Macie 主机上筛选您的库存

如果您使用 Amazon Macie 控制台筛选 S3 存储桶清单，Macie 会提供一些选项来帮助您为各个条件选择字段、运算符和值。您可以使用 S3 存储桶页面上的筛选框访问这些选项，如下图中所示。

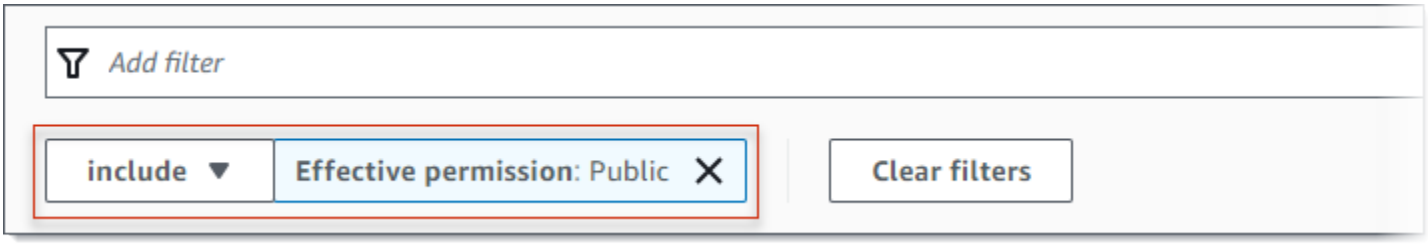


当您将光标置于筛选条件框中时，Macie 会显示可在筛选条件中使用的字段列表。这些字段按逻辑类别组织。例如，常用字段类别包括存储有关 S3 存储桶的一般信息的字段。公共访问类别包括存储有关可应用于存储桶的各种类型的公共访问权限设置数据的字段。这些字段在每个类别中按字母顺序排序。

要添加条件，请先从列表中选择一个字段。要查找字段，请浏览完整列表，或输入部分字段名称以缩小字段列表范围。

根据您选择的字段，Macie 显示不同的选项。这些选项反映了您选择的字段的类型和性质。例如，如果您选择共享访问权限字段，Macie 会显示一个值列表供您选择。如果您选择存储桶名称字段，Macie 会显示一个文本框，您可以在其中输入 S3 存储桶的名称。无论您选择哪个字段，Macie 都会指导您完成添加包含该字段所需设置的条件的步骤。

添加条件后，Macie 会为该条件应用标准，并在筛选框下方的筛选条件令牌中显示该条件，如下图所示。



在此示例中，条件配置为包括所有可公开访问的存储桶，并排除所有其他存储桶。它返回有效权限字段的值等于 Public 的存储桶。

当您添加更多条件时，Macie 会应用其标准并将其显示在筛选框下方。如果您添加多个条件，Macie 会使用 AND 逻辑来连接条件并评测筛选标准。这意味着，只有当 S3 存储桶与筛选条件中的所有条件都匹配时，它才会匹配筛选标准。您可以随时参考筛选框下方的区域，以确定您应用了哪些标准。

使用控制台筛选清单

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。S3 存储桶页面显示您的存储桶清单。
3. 在页面顶部，可以选择刷新
   ()，
   从 Amazon S3 检索最新的存储桶元数据。
4. 将光标置于筛选框中，然后选择要用于条件的字段。
5. 请记住以下提示，为该字段选择或输入适当的值类型。

日期、时间和时间范围

对于日期和时间，使用从和到框定义包含的时间范围：

- 要定义固定的时间范围，请使用从和到框分别指定该范围内的第一个日期和时间以及最后一个日期和时间。
- 要定义从特定日期和时间开始并在当前时间结束的相对时间范围，请在从框中输入开始日期和时间，然后删除到框中的任何文本。
- 要定义在特定日期和时间结束的相对时间范围，请在到框中输入结束日期和时间，然后删除从框中的任何文本。

请注意，时间值使用 24 小时表示法。如果您使用日期选择器选择日期，则可以通过直接在从和到框中输入文本来细化值。

数字和数值范围

对于数值，使用从和到框输入定义包含数值范围的整数：

- 要定义固定的数值范围，请使用从和到框分别指定该范围内的最小和最高数字。
- 要定义仅限于一个特定值的固定数值范围，请在从和到框中输入该值。例如，要仅包含恰好包含 15 个对象的 S3 存储桶，请在从和到框中输入 **15**。
- 要定义从某个数字开始的相对数值范围，请在从框中输入数字，不要在到框中输入任何文本。
- 要定义以特定数字结尾的相对数值范围，请在到框中输入数字，不要在从框中输入任何文本。

文本（字符串）值

对于此类值，请为该字段输入一个完整、有效的值。值区分大小写。

请注意，您不能在此类型的值中使用部分值或通配符。唯一的例外是存储桶名称字段。对于该字段，您可以指定前缀而不是完整的存储桶名称。例如，要查找名称以 my-S3 开头的所有 S3 存储桶，请输入 **my-S3** 作为存储桶名称字段的筛选值。如果您输入任何其他值，例如 **My-s3** 或 **my***，Macie 将不会返回存储桶。

6. 为该字段添加完值后，选择 应用。Macie 应用筛选标准并在筛选条件框下方的筛选器令牌中显示条件。
7. 对于要添加的每个附加条件，重复步骤 4 到 6。
8. 要删除条件，请在筛选条件令牌中为该条件选择 X。

9. 要更改条件，请通过在条件的筛选条件令牌中选择 X 来移除该条件。然后重复步骤 4 到 6，添加设置正确的条件。

使用 Amazon Macie API 以编程方式筛选您的库存

要以编程方式筛选 S3 存储桶库存，请在使用 Amazon Macie API 的 DescribeBuckets 操作提交的查询中指定筛选标准。此操作返回对象数组。每个对象都包含与筛选标准相匹配的存储桶的统计数据和其他信息。

要在查询中指定筛选标准，请在请求中加入筛选条件地图。为每个条件指定一个字段、一个运算符以及该字段的一个或多个值。值的类型和数量取决于您选择的字段和运算符。有关可在条件中使用的字段、运算符和值类型的信息，请参阅 Amazon Macie API 参考中的 Amazon S3 数据来源。

以下示例向您展示了如何在使用 AWS Command Line Interface(AWS CLI) 提交的查询中指定筛选标准。您也可以使用其他 AWS 命令行工具或 AWS SDK 的当前版本，或者直接向 Macie 发送 HTTPS 请求来执行此操作。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

示例

- 示例 1：按存储桶名称查找存储桶
- 示例 2：查找可公开访问的存储桶
- 示例 3：查找包含未加密对象的存储桶
- 示例 4：查找未受任务监控的存储桶
- 示例 5：查找将数据复制到外部账户的存储桶
- 示例 6：根据多个条件查找存储桶

这些示例使用 describe-buckets 命令。如果示例成功运行，Macie 将返回一个 `buckets` 数组。该数组包含当前 AWS 区域 中且符合筛选条件的每个存储桶的一个对象。有关此输出的示例，请展开以下部分。

`buckets` 数组示例

在此示例中，`buckets` 数组提供了与查询中指定的筛选条件相匹配的两个存储桶的详细信息。

```
{
    "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
        }
    ]
```

```
}
```

如果没有符合筛选标准的存储桶，Macie 将返回一个空的 buckets 数组。

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

示例 1：按存储桶名称查找存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中名称以 my-S3 开头的所有存储桶的元数据。

对于 Linux、macOS 或 Unix：

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

对于 Microsoft Windows：

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

其中：

- *bucketName* 指定存储桶名称字段的 JSON 名称。
- *prefix* 指定前缀运算符。
- *my-S3* 是存储桶名称字段的值。

示例 2：查找可公开访问的存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中的存储桶的元数据，这些存储桶基于一系列权限设置可公开访问。

对于 Linux、macOS 或 Unix：

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

对于 Microsoft Windows：

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

其中：

- *publicAccess.effectivePermission* 指定有效权限字段的 JSON 名称。
- *eq* 指定等于运算符。
- *PUBLIC* 是有效权限字段的枚举值。

示例 3：查找包含未加密对象的存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中包含未加密对象的存储桶的元数据。

对于 Linux、macOS 或 Unix：

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

对于 Microsoft Windows：

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

其中：

- *objectCountByEncryptionType.unencrypted* 指定不加密字段的 JSON 名称。
- *gte* 指定大于或等于运算符。
- *1* 是不加密字段在包含性相对数值范围内的最低值。

示例 4：查找未受任务监控的存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中存储桶的元数据，这些存储桶与任何定期敏感数据发现任务无关。

对于 Linux、macOS 或 Unix：

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

对于 Microsoft Windows：

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

其中：

- *jobDetails.isMonitoredByJob* 指定受任务主动监控字段的 JSON 名称。
- *eq* 指定等于运算符。
- *FALSE* 是受任务主动监控字段的枚举值。

示例 5：查找将数据复制到外部账户的存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中的存储桶的元数据，这些存储桶已配置为将对象复制到不属于您的组织的 AWS 账户。

对于 Linux、macOS 或 Unix：

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

对于 Microsoft Windows：

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

其中：

- *replicationDetails.replicatedExternally* 指定外部复制字段的 JSON 名称。
- *eq* 指定等于运算符。
- *true* 为外部复制字段指定布尔值。

示例 6：根据多个条件查找存储桶

此示例使用 describe-buckets 命令查询当前 AWS 区域 中存储桶的元数据，这些存储桶符合以下条件：可根据权限设置组合公开访问；包含未加密的对象；不与任何定期的敏感数据发现任务关联。

对于 Linux、macOS 或 Unix，使用反斜杠 (\) 行继续符来提高可读性：

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

对于 Microsoft Windows，使用脱字符 (^) 行继续符来提高可读性：

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

其中：

- *publicAccess.effectivePermission* 指定有效权限字段的 JSON 名称，并且：
  - *eq* 指定等于运算符。
  - *PUBLIC* 是有效权限字段的枚举值。
- *objectCountByEncryptionType.unencrypted* 指定无加密字段的 JSON 名称，并且：
  - *gte* 指定大于或等于运算符。
  - *1* 是不加密字段在包含性相对数值范围内的最低值。
- *jobDetails.ismonitoredByJob* 指定受任务主动监控字段的 JSON 名称，并且：
  - *eq* 指定等于运算符。
  - *FALSE* 是受任务主动监控字段的枚举值。

允许 Amazon Macie 访问 S3 存储桶和对象

当您为您的 AWS 账户 启用 Amazon Macie 时，Macie 会创建一个服务相关角色，该角色授予 Macie 代表您调用 Amazon Simple Storage Service (Amazon S3) 和其他 AWS 服务 所需的权限。服务相关角色简化了设置 AWS 服务 的过程，因为您不必手动添加服务代表您完成操作所需的权限。要了解有关此类角色的更多信息，请参阅 AWS Identity and Access Management 用户指南中的使用服务相关角色。

Macie 服务相关角色 (AWSServiceRoleForAmazonMacie) 的权限策略允许 Macie 执行操作，包括检索有关您的 S3 存储桶和对象的信息，以及从您的存储桶中检索对象。如果您是组织的 Macie 管理员，则此策略还允许 Macie 代表您组织中的成员账户执行以下作业。

Macie 使用这些权限执行以下作业：

- 生成并维护 S3 存储桶的清单
- 提供有关存储桶和存储桶中对象的统计数据和其他数据
- 监控和评测存储桶的安全性和访问控制
- 分析存储桶中的对象以检测敏感数据

在大多数情况下，Macie 拥有执行这些作业所需的权限。但是，如果 S3 存储桶具有限制性存储桶策略，则该策略可能会阻止 Macie 执行部分或全部作业。

存储桶策略是一种基于资源的 AWS Identity and Access Management (IAM) policy ，它指定主体（用户、账户、服务或其他实体）可以对 S3 存储桶执行哪些操作，以及主体可以在哪些条件下执行这些操作。这些操作和条件可能适用于存储桶级别的操作（例如检索有关存储桶的信息）和对象级操作（例如从存储桶中检索对象）。

存储桶策略通常使用显式 `Allow` 或 `Deny` 语句和条件来授予或限制访问权限。例如，存储桶策略可能包含拒绝访问存储桶的 `Allow` 或 `Deny` 语句，除非使用特定源 IP 地址、Amazon Virtual Private Cloud (Amazon VPC) 端点或 VPC 来访问存储桶。有关使用存储桶策略授予或限制对存储桶的访问权限的信息，请参阅 Amazon Simple Storage Service 用户指南中的存储桶策略和用户策略以及 Amazon S3 如何授权请求。

如果存储桶策略使用显式 `Allow` 语句，该策略不会阻止 Macie 检索有关存储桶和存储桶对象的信息，或从存储桶中检索对象。这是因为 Macie 服务相关角色的权限策略中的 `Allow` 语句授予了这些权限。

但是，如果存储桶策略使用带有一个或多个条件的显式 `Deny` 语句，则可能不允许 Macie 检索有关存储桶或存储桶对象的信息，也不允许检索存储桶的对象。例如，如果存储桶策略明确拒绝来自除特定 IP 地址之外的所有来源的访问，则在您运行敏感数据发现作业时，将不允许 Macie 分析存储桶的对象。这是因为限制性存储桶策略优先于 Macie 服务相关角色的权限策略中的 `Allow` 语句。

要允许 Macie 访问具有限制性存储桶策略的 S3 存储桶，您可以在存储桶策略中添加 Macie 服务相关角色的条件 (`AWSServiceRoleForAmazonMacie`)。该条件可以将 Macie 服务相关角色排除在与策略 `Deny` 限制的匹配范围之外。它可以通过使用 `aws:PrincipalArn` 全局条件上下文密钥和 Macie 服务相关角色的 Amazon 资源名称（ARN）来完成此操作。

下面的程序将指导您完成这一过程，并提供了一个示例。

将 Macie 服务相关角色添加到存储桶策略中

1. 登录到 AWS Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在导航窗格中，选择桶。
3. 请选择要允许 Macie 访问的 S3 存储桶。
4. 在 Permissions（权限）标签页中，在 Bucket policy（桶策略）下，请选择 Edit（编辑）。
5. 在 存储桶策略编辑器中，标识限制访问权限并阻止 Macie 访问存储桶或存储桶对象的每条 Deny 语句。
6. 在每条 Deny 语句中，添加一个使用 `aws:PrincipalArn` 全局条件上下文密钥的条件，并为您的 AWS 账户 指定 Macie 服务相关角色的 ARN。

   条件密钥的值应为 `arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`，其中 *123456789012* 是您的 AWS 账户 的账户 ID。

将其添加到存储桶策略的位置取决于该策略当前包含的结构、元素和条件。要了解支持的结构和元素，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的策略和权限。

以下是存储桶策略的示例，该策略使用显式 Deny 语句来限制对名为 DOC-EXAMPLE-BUCKET 的 S3 存储桶的访问。根据当前策略，只能从 ID 为 `vpce-1a2b3c4d` 的 VPC 端点访问存储桶。所有其他 VPC 端点的访问均被拒绝，包括来自 AWS Management Console 和 Macie 的访问。

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

```
}
```

要更改此策略并允许 Macie 访问 S3 存储桶和存储桶的对象，我们可以添加一个使用StringNotLike条件运算符和aws:PrincipalArn全局条件上下文密钥的条件。此附加条件将 Macie 服务相关角色排除在与 Deny 限制的匹配范围之外。

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

在前面的示例中，StringNotLike 条件运算符使用 aws:PrincipalArn 条件上下文密钥指定 Macie 服务相关角色的 ARN，其中：

- 123456789012 是允许 AWS 账户 使用 Macie 检索有关存储桶和存储桶对象的信息以及从存储桶中检索对象的账户 ID。
- macie.amazonaws.com 是 Macie 服务主体的标识符。
- AWSServiceRoleForAmazonMacie 是 Macie 服务相关角色的名称。

我们之所以使用 `StringNotLike` 运算符，是因为策略已经使用了 `StringNotEquals` 运算符。一个策略只能使用 `StringNotEquals` 运算符一次。

有关管理对 Amazon S3 资源的访问的其他策略示例和详细信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的身份和访问管理。

使用 Amazon Macie 发现敏感数据

借助 Amazon Macie，您可以自动发现、记录和报告 Amazon Simple Storage Service (Amazon S3) 数据资产中的敏感数据。您可以通过两种方式执行此操作：通过配置 Macie 以为您的账户或组织执行自动敏感数据发现，以及通过为您的账户或组织创建并运行敏感数据发现作业。

自动敏感数据发现

通过自动敏感数据发现，可以广泛了解敏感数据可能存放在您的 Amazon S3 数据资产中的位置。使用此选项，Macie 可以每天评测您的 S3 存储桶清单，并使用采样技术从您的存储桶中识别和选择具有代表性的 S3 对象。然后，Macie 检索并分析所选对象，检查它们是否有敏感数据。有关更多信息，请参阅执行自动敏感数据发现。

敏感数据发现作业

敏感数据发现作业可提供更深入、更有针对性的分析。使用此选项，您可以定义分析的广度和深度 — 您选择的特定 S3 存储桶或符合特定条件的存储桶。您还可以通过选择选项（例如源自 S3 对象属性的自定义标准）来细化分析范围。此外，您可以将作业配置为仅运行一次以进行按需分析和评测，或者定期运行以进行定期分析、评测和监控。有关更多信息，请参阅运行敏感数据发现作业。

无论是通过自动敏感数据发现选项还是敏感数据发现作业选项，您都可以使用 Macie 提供的托管数据标识符、您定义的自定义数据标识符或两者的组合来分析 S3 对象。您也可以通过使用允许列表来微调分析。

托管数据标识符

托管数据标识符是内置标准和技术，旨在检测特定类型的敏感数据，例如信用卡号码、AWS 秘密访问密钥或特定国家或地区的护照号码。它们可以检测许多国家和地区的大量且不断增长的敏感数据类型列表，包括多种类型的凭证数据、财务信息和个人身份信息（PII）。有关更多信息，请参阅使用托管数据标识符。

自定义数据标识符

自定义数据标识符定义检测敏感数据的自定义标准。每个自定义数据标识符指定一个正则表达式 (regex)，该正则表达式定义要匹配的文本模式，以及（可选）字符序列和优化结果的邻近规则。您可以使用它们来检测反映您的特定场景、知识产权或专有数据的敏感数据，例如员工 ID、客户账号或内部数据分类。有关更多信息，请参阅构建自定义数据标识符。

允许列表

在 Macie 中，允许列表指定在 S3 对象中要忽略的文本和文本模式，通常是特定场景或环境的敏感数据异常，例如，组织的公开名称或电话号码，或者组织用于测试的示例数据。如果 Macie 发现与允许列表中的条目或模式匹配的文本，Macie 不会报告该文本的出现，即使该文本与托管数据标识符或自定义数据标识符的条件匹配。有关更多信息，请参阅使用允许列表定义敏感数据例外。

当 Macie 分析 S3 对象时，Macie 会从 Amazon S3 中检索该对象的最新版本，然后检查该对象的内容中是否有敏感数据。如果以下条件成立，则 Macie 可以分析对象：

- 该对象使用支持的文件或存储格式，并使用支持的存储类直接存储在 Amazon S3 中。有关更多信息，请参阅支持的存储类别和格式。
- 如果对象已加密，则会使用 Macie 可以访问并允许使用的密钥进行加密。有关更多信息，请参阅分析加密 S3 对象。
- 如果对象存储在具有限制性存储桶策略的存储桶中，则该策略允许 Macie 访问存储桶中的对象。有关更多信息，请参阅允许 Macie 访问 S3 存储桶和对象。

为了帮助您满足和保持对数据安全性和隐私性要求的合规性，Macie 会生成其发现的敏感数据及其所执行分析（敏感数据调查发现和敏感数据发现结果）的记录。敏感数据调查发现是 Macie 在 S3 对象中发现的敏感数据的详细报告。敏感数据发现结果是关于对象分析的详细信息的记录。每种类型的记录都遵循标准化架构，该架构可以帮助您根据需要使用其他应用程序、服务和系统来对它们进行查询、监控和处理。

> **Tip**
>
> 尽管 Macie 针对 Amazon S3 进行了优化，但您可以使用它来发现当前存储在其他位置的资源中的敏感数据。为此，您可以暂时或永久地将数据移动到 Amazon S3。例如，将 Amazon Relational Database Service 或 Amazon Aurora 快照以 Apache Parquet 格式导出到 Amazon S3。或者将 Amazon DynamoDB 表导出到 Amazon S3。然后，您可以创建作业来分析 Amazon S3 中的数据。

主题

- 在 Amazon Macie 中使用托管数据标识符
- 在 Amazon Macie 中构建自定义数据标识符
- 使用 Amazon Macie 允许列表定义敏感数据例外

- 使用 Amazon Macie 执行自动敏感数据发现
- 在 Amazon Macie 中运行敏感数据发现作业
- 使用 Amazon Macie 分析加密的 Amazon S3 对象
- 使用 Amazon Macie 存储和保留敏感数据发现结果
- Amazon Macie 支持的存储类别和格式

在 Amazon Macie 中使用托管数据标识符

Amazon Macie 将包括机器学习和模式匹配在内的标准和技术结合使用来检测 Amazon Simple Storage Service (Amazon S3) 中的敏感数据。这些标准和技巧统称为托管数据标识符，可以检测到许多国家和地区的大量敏感数据类型，而且这些类型还在不断增长中，包括多种类型的凭证数据、财务信息、个人健康信息（PHI）和个人身份信息（PII）。每个托管数据标识符都设计用于检测特定类型的敏感数据，例如AWS 秘密访问密钥、信用卡号或者特定国家或地区的护照号码。

Macie 可以使用托管数据标识符检测以下类别的敏感数据：

- 凭证，例如私有密钥或 AWS 秘密访问密钥之类的凭证数据。
- 财务信息，用于信用卡号和银行账户号等财务数据。
- 个人健康信息，如健康保险和医疗识别号码；个人信息，如驾驶证号码和护照号码。

在每个类别中，Macie 可以检测多种类型的敏感数据。本节中的主题列出并描述了各种类型以及对其进行检测的相关要求。对于每种类型，它们还说明了托管数据标识符的唯一标识符 (ID)，此标识符设计用于检测数据。在创建敏感数据发现作业或配置自动敏感数据发现果设置时，您可以使用这些 ID 来指定希望 Macie 在分析 S3 对象时使用哪些托管数据标识符。

有关我们推荐用于作业的托管数据标识符列表，请参阅 推荐用于敏感数据发现作业的托管数据标识符。有关我们推荐并默认用于自动敏感数据发现的托管数据标识符列表，请参阅 自动敏感数据发现的默认设置。

主题

- Amazon Macie 托管数据标识符的关键字需求
- 快速参考：Amazon Macie 托管数据标识符
- 详细参考：Amazon Macie 托管数据标识符

Amazon Macie 托管数据标识符的关键字需求

为了使用托管数据标识号检测某些类型的敏感数据，Amazon Macie 要求关键字的位置必须靠近数据。如果特定类型的数据属于这种情况，此部分中的后续主题将说明该数据的特定关键字要求。

如果关键字必须靠近特定类型的数据，则该关键字通常必须在 30 个字符以内（含）数据。其他邻近要求因 Amazon Simple Storage Service (Amazon S3) 对象的文件类型或存储格式而异。

结构化柱状数据

对于列式数据，关键字必须是相同值的一部分或在存储值的列或字段的名称中。这适用于 Microsoft Excel 工作簿、CSV 文件和 TSV 文件。

例如，如果某个字段的值同时包含 SSN 和使用美国社会安全号码 (SSN) 语法的九位数字，则 Macie 可以在该字段中检测到 SSN。同样，如果列名包含 SSN，Macie 可以检测该列中的每个 SSN。Macie 将该列中的值视为与关键字 SSN 接近。

基于记录的结构化数据

对于基于记录的数据，关键字必须是相同值的一部分，或者是在存储值的字段或数组路径中元素的名称中。这适用于 Apache Avro 对象容器、Apache Parquet 文件、JSON 文件和 JSON Lines 文件。

例如，如果字段的值同时包含凭证和使用 AWS 秘密访问密钥语法的字符序列，则 Macie 可以检测该字段中的密钥。同样，如果字段的路径是 `$.credentials.aws.key`，则 Macie 可以在该字段中检测到 AWS 秘密访问密钥。Macie 将该字段中的值视为与关键字凭证相近。

非结构化数据

除了 CSV、JSON、JSON Lines 和 TSV 文件之外，Adobe 便携式文档格式文件、Microsoft Word 文档、电子邮件和非二进制文本文件没有任何额外的邻近要求。关键字通常必须在数据的 30（含）个字符以内。这包括这些类型的文件中的任何结构化数据，例如表。

关键字不区分大小写。此外，如果关键字包含空格，Macie 会自动匹配不包含空格的变体，或包含下划线 (_) 或连字符 (-) 而不是空格的关键字变体。在某些情况下，Macie 还会扩展或缩写关键字以应对该关键字的常见变体。

要演示关键字如何提供上下文并帮助 Macie 检测特定类型的敏感数据，请观看以下视频：Amazon Macie 如何使用关键字发现敏感数据。

快速参考：Amazon Macie 托管数据标识符

在 Amazon Macie 中，托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如信用卡号、 AWS 私有访问密钥或特定国家或地区的护照号码。这些标识符可以检测许多国家和地区的大量且不断增长的敏感数据类型列表，包括多种类型的凭证数据、财务信息、个人健康信息 (PHI) 和个人身份信息（PII）。

下表列出了 Macie 当前提供的所有托管数据标识符，按敏感数据类型排列。对于每种类型，它提供以下信息：

- 敏感数据类别-指定敏感数据的一般类别，包括以下类型：凭证，用于凭证数据，例如私钥；财务信息，用于财务数据，例如信用卡号和银行账户；个人信息：PHI 个人健康信息，例如健康保险和医疗身份证号；个人信息：PII 个人身份信息，例如驾驶执照识别号和护照号码。
- 托管数据标识符 ID – 指定用于检测数据的一个或多个托管数据标识符的唯一标识符 (ID)。创建敏感数据发现作业或配置自动敏感数据发现设置时，您可以使用这些 ID 指定希望 Macie 在分析数据时使用的托管数据标识符。有关我们推荐用于作业的托管数据标识符列表，请参阅 推荐用于敏感数据发现作业的托管数据标识符。有关我们推荐用于自动敏感数据发现的托管数据标识符列表，请参阅 自动敏感数据发现的默认设置。
- 必填关键字 - 指定检测是否要求关键字靠近数据。有关 Macie 在分析数据时如何使用关键字的信息，请参阅 关键字要求。
- 国家和地区 – 指示适用的托管数据标识符是针对哪些国家或地区设计的。如果托管数据标识符不是为特定国家或地区设计的，则此值为任何。

要查看有关特定类型敏感数据的托管数据标识符的其他详细信息，请选择该类型。

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
AWS秘密访问密钥	凭证	AWS_CREDENTIALS	支持	任何
银行账户	财务信息	BANK_ACCOUNT_NUMBER（适用于加拿大和美国）	支持	加拿大、美国
基本银行账户 (BBAN)	财务信息	视国家或地区而定： FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOU	支持	法国、德国、意大利

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		NT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER		、西班牙、英国
出生日期	个人信息：PII	DATE_OF_BIRTH	支持	任何
信用卡到期日期	财务信息	CREDIT_CARD_EXPIRATION	支持	任何
信用卡磁条数据	财务信息	CREDIT_CARD_MAGNETIC_STRIPE	支持	任何
信用卡号	财务信息	CREDIT_CARD_NUMBER（适用于关键字附近的信用卡号），CREDIT_CARD_NUMBER_(NO_KEYWORD)（适用于不在关键字附近的信用卡号）	变化	任何
信用卡验证码	财务信息	CREDIT_CARD_SECURITY_CODE	支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
驾驶执照识别号	个人信息：PII	视国家或地区而定： 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	支持	澳大利亚、奥地利、比利时、保加利亚、加拿大、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、印度、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、英国、美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
毒品管理局 (DEA) 注册号	个人信息：PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	支持	美国
选民名册编号	个人信息：PII	UK_ELECTORAL_ROLL_NUMBER	支持	英国
全名	个人信息：PII	NAME	不支持	如果名称使用拉丁字符集，则为“任何”
全球定位系统 (GPS) 坐标	个人信息：PII	LATITUDE_LONGITUDE	支持	如果坐标靠近英语关键字，则为“任何”
Google Cloud API 密钥	凭证	GCP_API_KEY	支持	任何
健康保险索赔编号 (HICN)	个人信息：PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	支持	美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
健康保险或医疗识别号	个人信息：PHI	视国家或地区而定： CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	支持	加拿大、欧盟、芬兰、法国、英国、美国
医疗保健通用程序编码系统 (HCPCS) 代码	个人信息：PHI	USA_HEALTHCARE_PROCEDURE_CODE	支持	美国
HTTP 基本授权标头	凭证	HTTP_BASIC_AUTH_HEADER	不支持	任何
HTTP cookie	个人信息：PII	HTTP_COOKIE	不支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
国际银行账户 (IBAN)	财务信息	视国家或地区而定： 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,	不支持	阿尔巴尼亚、安道尔、波斯尼亚-黑塞哥维那、巴西、保加利亚、哥斯达黎加、克罗地亚、塞浦路斯、捷克共和国、丹麦、多米尼加共和国、埃及、爱沙尼亚、法罗群岛、芬兰、法国、格鲁吉亚、德国、希腊、格陵兰、匈牙利、冰岛、爱尔兰、意大利、约旦、科索沃、列支敦士登、立陶宛、马耳他、毛里塔尼亚、毛里求斯、摩纳哥、黑山、荷兰、北马其顿、

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		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_EMIRAT		波兰、葡萄牙、圣马力诺、塞内加尔、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、瑞士、东帝汶、突尼斯、土耳其、英国、乌克兰、阿拉伯联合酋长国、维尔京群岛(英属)

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER（适用于英属维尔京群岛）		
JSON Web 令牌 (JWT)	凭证	JSON_WEB_TOKEN	不支持	任何
邮寄地址	个人信息：PII	ADDRESS，BRAZIL_CEP_CODE（适用于巴西的《邮政编码法》）	变化	澳大利亚、巴西、加拿大、法国、德国、意大利、西班牙、英国、美国
国家药品编码 (NDC)	个人信息：PHI	USA_NATIONAL_DRUG_CODE	支持	美国
身份证号码	个人信息：PII	视国家或地区而定： BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	支持	巴西、法国、德国、印度、意大利、西班牙
国民保险号码 (NINO)	个人信息：PII	UK_NATIONAL_INSURANCE_NUMBER	支持	英国
国家提供商识别码 (NPI)	个人信息：PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	支持	美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
OpenSSH 私有密钥	凭证	OPENSSH_PRIVATE_KEY	不支持	任何
护照编号	个人信息：PII	视国家或地区而定： CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	支持	加拿大、法国、德国、意大利、西班牙、英国、美国
永久居留号码	个人信息：PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	支持	加拿大
PGP 私有密钥	凭证	PGP_PRIVATE_KEY	不支持	任何
电话号码	个人信息：PII	视国家或地区而定： 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	变化	巴西、加拿大、法国、德国、意大利、西班牙、英国、美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	凭证	PKCS	不支持	任何
PuTTY 私有密钥	凭证	PUTTY_PRIVATE_KEY	不支持	任何
社会保险号码 (SIN)	个人信息：PII	CANADA_SOCIAL_INSURANCE_NUMBER	支持	加拿大
社会保障号码（SSN）	个人信息：PII	视国家或地区而定：SPAIN_SOCIAL_SECURITY_NUMBER，USA_SOCIAL_SECURITY_NUMBER	支持	西班牙、美国
the section called “Stripe API 密钥”	凭证	STRIPE_CREDENTIALS	不支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
纳税人识别号或参考号	个人信息：PII	视国家或地区而定： 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	支持	澳大利亚、巴西、法国、德国、印度、意大利、西班牙、英国、美国
唯一设备标识符 (UDI)	个人信息：PHI	MEDICAL_DEVICE_UDI	支持	美国
车辆识别号码 (VIN)	个人信息：PII	VEHICLE_IDENTIFICATION_NUMBER	支持	如果 VIN 与以下语言之一的关键字相邻，则为任意国家和地区：英语、法语、德语、立陶宛语、波兰语、葡萄牙语、罗马尼亚语或西班牙语。

详细参考：Amazon Macie 托管数据标识符

在 Amazon Macie 中，托管数据标识符是内置条件和技术，旨在检测特定类型的敏感数据。它们可以检测许多国家和地区的大量且不断增长的敏感数据类型列表，包括多种类型的凭证数据、财务信息和个人信息。每个托管数据标识符都设计用于检测特定类型的敏感数据，例如 AWS 秘密访问密钥、信用卡号或者特定国家或地区的护照号码。

Macie 可以使用托管数据标识符检测几种类别的敏感数据。在每个类别中，Macie 可以检测多种类型的敏感数据。本节中的主题列出并描述了各种类型以及对数据进行检测的相关要求。有关特定类型敏感数据的托管数据标识符的详细信息，您可以按类别浏览主题：

- 凭证-用于凭证数据，例如私钥和 AWS 秘密访问密钥。
- 财务信息 – 指信用卡号和银行账户号等财务数据。
- 个人信息：PHI – 指个人健康信息 (PHI)，例如健康保险和医疗识别号。
- 个人信息：PII – 指个人身份信息（PII），例如驾照识别号和护照号码。

或者，您可以从下表中选择特定类型的敏感数据。表格列出了 Macie 当前提供的所有托管数据标识符，按敏感数据类型排列。该表还汇总了检测每种类型的相关要求。

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
AWS秘密访问密钥	凭证	AWS_CREDENTIALS	支持	任何
银行账户	财务信息	BANK_ACCOUNT_NUMBER（适用于加拿大和美国）	支持	加拿大、美国
基本银行账户 (BBAN)	财务信息	视国家或地区而定： FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	支持	法国、德国、意大利、西班牙、英国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
出生日期	个人信息：PII	DATE_OF_BIRTH	支持	任何
信用卡到期日期	财务信息	CREDIT_CARD_EXPIRATION	支持	任何
信用卡磁条数据	财务信息	CREDIT_CARD_MAGNETIC_STRIPE	支持	任何
信用卡号	财务信息	CREDIT_CARD_NUMBER（适用于关键字附近的信用卡号），CREDIT_CARD_NUMBER_(NO_KEYWORD)（适用于不在关键字附近的信用卡号）	变化	任何
信用卡验证码	财务信息	CREDIT_CARD_SECURITY_CODE	支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
驾驶执照识别号	个人信息：PII	视国家或地区而定： 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	支持	澳大利亚、奥地利、比利时、保加利亚、加拿大、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、印度、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、英国、美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
毒品管理局 (DEA) 注册号	个人信息：PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	支持	美国
选民名册编号	个人信息：PII	UK_ELECTORAL_ROLL_NUMBER	支持	英国
全名	个人信息：PII	NAME	不支持	如果名称使用拉丁字符集，则为“任何”
全球定位系统 (GPS) 坐标	个人信息：PII	LATITUDE_LONGITUDE	支持	如果坐标靠近英语关键字，则为“任何”
Google Cloud API 密钥	凭证	GCP_API_KEY	支持	任何
健康保险索赔编号 (HICN)	个人信息：PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	支持	美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
健康保险或医疗识别号	个人信息：PHI	视国家或地区而定： CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	支持	加拿大、欧盟、芬兰、法国、英国、美国
医疗保健通用程序编码系统 (HCPCS) 代码	个人信息：PHI	USA_HEALTHCARE_PROCEDURE_CODE	支持	美国
HTTP 基本授权标头	凭证	HTTP_BASIC_AUTH_HEADER	不支持	任何
HTTP cookie	个人信息：PII	HTTP_COOKIE	不支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
国际银行账户 (IBAN)	财务信息	视国家或地区而定： 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,	不支持	阿尔巴尼亚、安道尔、波斯尼亚-黑塞哥维那、巴西、保加利亚、哥斯达黎加、克罗地亚、塞浦路斯、捷克共和国、丹麦、多米尼加共和国、埃及、爱沙尼亚、法罗群岛、芬兰、法国、格鲁吉亚、德国、希腊、格陵兰、匈牙利、冰岛、爱尔兰、意大利、约旦、科索沃、列支敦士登、立陶宛、马耳他、毛里塔尼亚、毛里求斯、摩纳哥、黑山、荷兰、北马其顿、

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		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_EMIRAT		波兰、葡萄牙、圣马力诺、塞内加尔、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、瑞士、东帝汶、突尼斯、土耳其、英国、乌克兰、阿拉伯联合酋长国、维尔京群岛(英属)

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER（适用于英属维尔京群岛）		
JSON Web 令牌 (JWT)	凭证	JSON_WEB_TOKEN	不支持	任何
邮寄地址	个人信息：PII	ADDRESS，BRAZIL_CEP_CODE（适用于巴西的《邮政编码法》）	变化	澳大利亚、巴西、加拿大、法国、德国、意大利、西班牙、英国、美国
国家药品编码 (NDC)	个人信息：PHI	USA_NATIONAL_DRUG_CODE	支持	美国
身份证号码	个人信息：PII	视国家或地区而定： BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	支持	巴西、法国、德国、印度、意大利、西班牙
国民保险号码 (NINO)	个人信息：PII	UK_NATIONAL_INSURANCE_NUMBER	支持	英国
国家提供商识别码 (NPI)	个人信息：PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	支持	美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
OpenSSH 私有密钥	凭证	OPENSSH_PRIVATE_KEY	不支持	任何
护照编号	个人信息：PII	视国家或地区而定： CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	支持	加拿大、法国、德国、意大利、西班牙、英国、美国
永久居留号码	个人信息：PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	支持	加拿大
PGP 私有密钥	凭证	PGP_PRIVATE_KEY	不支持	任何
电话号码	个人信息：PII	视国家或地区而定： 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	变化	巴西、加拿大、法国、德国、意大利、西班牙、英国、美国

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	凭证	PKCS	不支持	任何
PuTTY 私有密钥	凭证	PUTTY_PRIVATE_KEY	不支持	任何
社会保险号码 (SIN)	个人信息：PII	CANADA_SOCIAL_INSURANCE_NUMBER	支持	加拿大
社会保障号码（SSN）	个人信息：PII	视国家或地区而定：SPAIN_SOCIAL_SECURITY_NUMBER，USA_SOCIAL_SECURITY_NUMBER	支持	西班牙、美国
the section called “Stripe API 密钥”	凭证	STRIPE_CREDENTIALS	不支持	任何

敏感数据类型	敏感数据类别	托管数据标识符 ID	所需关键字	国家和地区
纳税人识别号或参考号	个人信息：PII	视国家或地区而定： 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	支持	澳大利亚、巴西、法国、德国、印度、意大利、西班牙、英国、美国
唯一设备标识符 (UDI)	个人信息：PHI	MEDICAL_DEVICE_UDI	支持	美国
车辆识别号码 (VIN)	个人信息：PII	VEHICLE_IDENTIFICATION_NUMBER	支持	如果 VIN 与以下语言之一的关键字相邻，则为任意国家和地区：英语、法语、德语、立陶宛语、波兰语、葡萄牙语、罗马尼亚语或西班牙语。

凭证数据的托管数据标识符

Amazon Macie 可通过使用托管数据标识符检测多种类型的敏感凭证数据。此页面上的主题指定了每种类型，并提供了有关旨在检测数据的托管数据标识符的相关信息。每个主题都提供以下信息：

- 托管数据标识符 ID - 指定用于检测数据的托管数据标识符的唯一标识符 (ID)。在创建敏感数据发现作业或配置自动敏感数据发现设置时，您可以使用此 ID 来指定是否希望 Macie 在分析数据时使用托管数据标识符。
- 支持的国家和地区 - 指明适用的托管数据标识符是为哪些国家或地区设计的。如果托管数据标识符不是为特定国家或地区设计的，则此值为任何。
- 必填关键字 - 指定检测是否要求关键字靠近数据。如果关键字是必需的，该主题还提供了必填关键字的示例。有关 Macie 在分析数据时如何使用关键字的信息，请参阅 关键字要求。
- 注释 – 提供可能影响您选择托管数据标识符或调查报告的敏感数据发生次数的任何相关详细信息。详细信息包括支持的标准、语法要求和例外情况等信息。

这些主题按敏感数据类型的字母顺序列出。

敏感数据类型

- AWS秘密访问密钥
- Google Cloud API 密钥
- HTTP 基本授权标头
- JSON Web 令牌 (JWT)
- OpenSSH 私有密钥
- PGP 私有密钥
- 公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥
- PuTTY 私有密钥
- Stripe API 密钥

AWS秘密访问密钥

托管数据标识符 ID： AWS_CREDENTIALS

支持的国家和地区：任何

必填关键字：是。关键字包括：aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

注释：Macie 不会报告以下角色序列的出现，这些序列通常用作虚构的示例：`je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` 和 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`。

Google Cloud API 密钥

托管数据标识符 ID： GCP_API_KEY

支持的国家和地区：任何

必填关键字：是。关键字包括：G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

注释：Macie 只能检测 Google Cloud API 密钥的字符串 (`keyString`) 组件。支持不包括检测 Google Cloud API 密钥的 ID 或显示名称组件。

HTTP 基本授权标头

托管数据标识符 ID： HTTP_BASIC_AUTH_HEADER

支持的国家和地区： 任何

必填关键字：否

注释：检测需要完整的标头，包括字段名称和身份验证方案指令，如 RFC 7617 所述。例如：`Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` 和 `Proxy-Authorization: Basic dGVzdDoxMjPCow==`。

JSON Web 令牌 (JWT)

托管数据标识符 ID： JSON_WEB_TOKEN

支持的国家和地区： 任何

必填关键字：否

注释：Macie 可以检测符合 RFC 7519 对 JSON Web 签名 (JWS) 结构规定的要求的 JSON 网络令牌 (JWT)。令牌可以是签名的，也可以是未签名的。

OpenSSH 私有密钥

托管数据标识符 ID： OPENSSH_PRIVATE_KEY

支持的国家和地区： 任何

必填关键字：否

注释：无

PGP 私有密钥

托管数据标识符 ID： PGP_PRIVATE_KEY

支持的国家和地区： 任何

必填关键字：否

注释：无

公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥

托管数据标识符 ID： PKCS

支持的国家和地区： 任何

必填关键字：否

注释：无

PuTTY 私有密钥

托管数据标识符 ID： PUTTY_PRIVATE_KEY

支持的国家和地区： 任何

必填关键字：否

评论：Macie 可以检测使用以下标准标头和标题序列的 Putty 私钥`PuTTY-User-Key-File：Encryption`、、`Comment`、`Public-LinesPrivate-Lines`、和。`Private-MAC`标头值可以包含字母数字字符、连字符 (-) 和换行符 (或)。`\n \r Public-LinesPrivate-Lines`值也可以包含正斜杠 (/)、加号 (+) 和等号 (=)。 `Private-MAC`值也可以包含加号 (+)。Support 不包括检测标头值包含其他字符（例如空格或下划线 (_)）的私钥。Support 也不包括对包含自定义标头的私钥的检测。

Stripe API 密钥

托管数据标识符 ID： STRIPE_CREDENTIALS

支持的国家和地区： 任何

必填关键字：否

注释：Macie 不会报告以下角色序列的出现，这些序列通常用作条带代码示例：`sk_test_4eC39HqLyjWDarjtT1zdp7dc` 和 `pk_test_TYooMQauvdEDq54NiTphI7jx`。

财务信息的托管数据标识符

Amazon Macie 可通过使用托管数据标识符检测多种类型的敏感财务信息。本页上的主题列出了每种类型，并提供有关旨在检测数据的托管数据标识符的信息。每个主题都提供以下信息：

- 托管数据标识符 ID – 指定用于检测数据的一个或多个托管数据标识符的唯一标识符 (ID)。创建敏感数据发现作业或配置自动敏感数据发现设置时，您可以使用这些 ID 指定希望 Macie 在分析数据时使用的托管数据标识符。
- 支持的国家和地区 – 指示适用的托管数据标识符是针对哪些国家或地区设计的。如果托管数据标识符不是为特定国家或地区设计的，则此值为任何。
- 必填关键字 - 指定检测是否要求关键字靠近数据。如果关键字是必需的，该主题还提供了必填关键字的示例。有关 Macie 在分析数据时如何使用关键字的信息，请参阅 关键字要求。
- 注释 – 提供可能影响您选择托管数据标识符或调查报告的敏感数据发生次数的任何相关详细信息。详细信息包括支持的标准、语法要求和例外情况等信息。

这些主题按敏感数据类型的字母顺序列出。

敏感数据类型

- 银行账户
- 基本银行账户 (BBAN)
- 信用卡到期日期
- 信用卡磁条数据
- 信用卡号
- 信用卡验证码
- 国际银行账户 (IBAN)

银行账户

Macie 可以检测由 9-17 位数字序列组成且不包含任何空格的加拿大和美国银行账户。

托管数据标识符 ID： BANK_ACCOUNT_NUMBER

支持的国家和地区：加拿大、美国

必填关键字：是。关键字包括：bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

注释：此托管数据标识符明确专为检测加拿大和美国的银行账户而设计。这些国家/地区不使用 ISO 13616 规定的 ISO 国际标准定义的基本银行账户 (BBAN) 或国际银行账户 (IBAN) 格式对银行账户进行编号。要检测其他国家和地区的银行账户，请使用专为这些格式设计的托管数据标识符。有关更多信息，请参阅 基本银行账户 (BBAN) 和 国际银行账户 (IBAN)。

基本银行账户 (BBAN)

Macie 可以检测基本银行账户 (BBAN)，这些账户符合 ISO 13616 规定的银行账户编号 ISO 国际标准所定义的 BBAN 结构。这包括不包含空格、不使用空格或连字符分隔符的 BBAN，例如，`NWBK60161331926819`、`NWBK 6016 1331 9268 19` 和 `NWBK-6016-1331-9268-19`。

托管数据标识符 ID：视国家或地区而定，FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

支持的国家和地区：法国、德国、意大利、西班牙、英国

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

国家或地区	关键字
法国	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
德国	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzah l, iban, kartennummer, kontonummer, kreditkar tennummer, sepa

国家或地区	关键字
意大利	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
西班牙	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
英国	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

注释：这些托管数据标识符还可以检测符合 ISO 13616 标准的国际银行账户 (IBAN)。有关更多信息，请参阅 国际银行账户 (IBAN)。英国的托管数据标识符 (UK_BANK_ACCOUNT_NUMBER) 还可以检测英国的国内银行账户，例如，`60-16-13 31926819`。

信用卡到期日期

托管数据标识符 ID： CREDIT_CARD_EXPIRATION

支持的国家和地区： 任何

必填关键字：是。关键字包括：exp d, exp m, exp y, expiration, expiry

注释： 支持包括大多数日期格式，例如所有数字以及数字和月份名称的组合。日期组件可以用斜杠(/)、连字符(-)或适用的关键字分隔。例如，Macie 可以检测诸如 `02/26`、`02/2026`、`Feb 2026`、`26-Feb` 和 `expY=2026, expM=02` 之类的日期。

信用卡磁条数据

托管数据标识符 ID： CREDIT_CARD_MAGNETIC_STRIPE

支持的国家和地区： 任何

必填关键字：是。关键字包括：card data, iso7813, mag, magstripe, stripe, swipe

注释：支持包括轨道 1 和 2。

信用卡号

托管数据标识符 ID：CREDIT_CARD_NUMBER 用于与关键字邻近的信用卡号、CREDIT_CARD_NUMBER_(NO_KEYWORD) 用于不与关键字邻近的信用卡号

支持的国家和地区： 任何

必填关键字：各不相同。CREDIT_CARD_NUMBER托管数据标识符需要关键字。关键字包括：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。CREDIT_CARD_NUMBER_(NO_KEYWORD)托管数据标识符不需要关键字。

评论：检测要求数据为13-19位数的序列，该序列符合卢恩支票公式，并对以下任何类型的信用卡使用标准卡号前缀：美国运通、丹科特、大莱卡、Discover、Electron、日本信用卡局（JCB）、万事达卡和Visa。 UnionPay

Macie 不会报告以下序列的出现情况，信用卡发卡机构已保留这些序列供公开测试：122000000000003、2222405343248877、2222990905257051、2223007648726984、2223577
4111111111111111、4222222222222、4444333322221111、4462030000000000、4484070000000
5204740009900014、5420923878724339、5454545454545454、5455330760000018、5506900490
和 76009244561。

信用卡验证码

托管数据标识符 ID： CREDIT_CARD_SECURITY_CODE

支持的国家和地区： 任何

必填关键字：是。关键字包括：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

注释：无

国际银行账户 (IBAN)

Macie 可以检测最多由 34 个字母数字字符组成的国际银行账户(IBAN)，包括国家/地区代码等元素。更具体地说，Macie 可以检测符合 ISO 13616 规定的 ISO 国际银行账户编号标准的 IBAN。这包括不包含空格、不使用空格或连字符分隔符的 IBAN，例如，`GB29NWBK60161331926819`、`GB29 NWBK 6016 1331 9268 19` 和 `GB29-NWBK-6016-1331-9268-19`。检测包括基于模数 97 方案的验证检查。

托管数据标识符 ID：视国家或地区而定，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（适用于英属维尔京群岛）

支持的国家和地区：阿尔巴尼亚、安道尔、波黑、巴西、保加利亚、哥斯达黎加、克罗地亚、塞浦路斯、捷克共和国、丹麦、多米尼加共和国、埃及、爱沙尼亚、法罗群岛、芬兰、法国、格鲁吉亚、德国、希腊、格陵兰岛、匈牙利、冰岛、爱尔兰、意大利、约旦、科索沃、列支敦士登、立陶宛、马耳他、毛里塔尼亚、毛里求斯、摩纳哥、黑山、荷兰、北马其顿、波兰、葡萄牙、圣马力诺、塞内加尔、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、瑞士、东帝汶、突尼斯、土耳其、英国、乌克兰、阿拉伯联合酋长国阿联酋航空，维尔京群岛（英国）

必填关键字：否

注释：如果字符序列邻近关键字，则法国、德国、意大利、西班牙和英国的托管数据标识符还可以检测符合 ISO 13616 标准定义的 BBAN 结构的基本银行账户 (BBAN)。有关更多信息，请参阅 基本银行账户 (BBAN)。

个人健康信息(PHI)托管数据标识符

Amazon Macie 可通过使用托管数据标识符检测多种类型的敏感个人健康信息(PHI)。此页面上的主题指定了每种类型，并提供了有关旨在检测数据的托管数据标识符的相关信息。每个主题都提供以下信息：

- 托管数据标识符 ID - 指定用于检测数据的托管数据标识符的唯一标识符 (ID)。在创建敏感数据发现作业或配置自动敏感数据发现设置时，您可以使用此 ID 来指定是否希望 Macie 在分析数据时使用托管数据标识符。
- 支持的国家和地区 - 指明适用的托管数据标识符是为哪些国家或地区设计的。如果托管数据标识符不是为特定国家或地区设计的，则此值为任何。
- 必填关键字 - 指定检测是否要求关键字靠近数据。如果关键字是必需的，该主题还提供了必填关键字的示例。有关 Macie 在分析数据时如何使用关键字的信息，请参阅 关键字要求。
- 注释 – 提供可能影响您选择托管数据标识符或调查报告的敏感数据发生次数的任何相关详细信息。详细信息包括支持的标准、语法要求和例外情况等信息。

这些主题按敏感数据类型的字母顺序列出。

敏感数据类型

- 毒品管理局 (DEA) 注册号
- 健康保险索赔编号 (HICN)
- 健康保险或医疗识别号
- 医疗保健通用程序编码系统 (HCPCS) 代码

- 国家药品编码 (NDC)
- 国家提供商识别码 (NPI)
- 唯一设备标识符 (UDI)

毒品管理局 (DEA) 注册号

托管数据标识符 ID：US_DRUG_ENFORCEMENT_AGENCY_NUMBER

支持的国家和地区：US

必填关键字：是。关键字包括：dea number, dea registration

注释：无

健康保险索赔编号 (HICN)

托管数据标识符 ID： USA_HEALTH_INSURANCE_CLAIM_NUMBER

支持的国家和地区：US

必填关键字：是。关键字包括：health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

注释：无

健康保险或医疗识别号

支持包括欧盟和芬兰的欧洲健康保险卡号、法国的健康保险号码、美国的医疗保险受益人标识符、英国的 NHS 号码和加拿大的个人健康号码。

托管数据标识符 ID：视国家或地区而定，CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

支持的国家和地区：加拿大、欧盟、芬兰、法国、英国、美国

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

Country or region（国家或地区）	Keywords
加拿大	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
EU	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d’assurance maladie, numéro de carte d’assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
芬兰	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

Country or region（国家或地区）	Keywords
法国	carte d'assuré social, carte vitale, insurance card
UK	national health service, NHS
US	mbi, medicare beneficiary

注释：无

医疗保健通用程序编码系统 (HCPCS) 代码

托管数据标识符 ID： USA_HEALTHCARE_PROCEDURE_CODE

支持的国家和地区：US

必填关键字：是。关键字包括：current procedural terminology, hcpcs, healthcare common procedure coding system

注释：无

国家药品编码 (NDC)

托管数据标识符 ID： USA_NATIONAL_DRUG_CODE

支持的国家和地区：US

必填关键字：是。关键字包括：national drug code, ndc

注释：无

国家提供商识别码 (NPI)

托管数据标识符 ID： USA_NATIONAL_PROVIDER_IDENTIFIER

支持的国家和地区：US

必填关键字：是。关键字包括：hipaa, n.p.i, national provider, npi

注释：无

唯一设备标识符 (UDI)

托管数据标识符 ID： MEDICAL_DEVICE_UDI

支持的国家和地区：US

必填关键字：是。关键字包括：blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

注释：Macie 可以检测符合美国食品药品监督管理局批准格式的唯一设备标识符 (UDI)。这包括 GS1、HIBCC 和 ICCBBA 定义的标准格式。ICCBA 支持适用于 ISBT 标准。

个人身份信息（PII）的数据标识符 ARN

Amazon Macie 可以使用托管数据标识符检测多种类型的敏感个人身份信息（PII）。本页上的主题列出了每种类型，并提供有关旨在检测数据的托管数据标识符的信息。每个主题都提供以下信息：

- 托管数据标识符 ID – 指定用于检测数据的一个或多个托管数据标识符的唯一标识符 (ID)。创建敏感数据发现作业或配置自动敏感数据发现设置时，您可以使用这些 ID 指定希望 Macie 在分析数据时使用的托管数据标识符。
- 支持的国家和地区 – 指示适用的托管数据标识符是针对哪些国家或地区设计的。如果托管数据标识符不是为特定国家或地区设计的，则此值为任何。
- 必填关键字 - 指定检测是否要求关键字靠近数据。如果关键字是必需的，该主题还提供了必填关键字的示例。有关 Macie 在分析数据时如何使用关键字的信息，请参阅 关键字要求。
- 注释 – 提供可能影响您选择托管数据标识符或调查报告的敏感数据发生次数的任何相关详细信息。详细信息包括支持的标准、语法要求和例外情况等信息。

这些主题按敏感数据类型的字母顺序列出。

敏感数据类型

- 出生日期
- 驾驶执照识别号
- 选民名册编号
- 全名
- 全球定位系统 (GPS) 坐标
- HTTP cookie
- 邮寄地址

- 身份证号码
- 国民保险号码 (NINO)
- 护照编号
- 永久居留号码
- 电话号码
- 社会保险号码 (SIN)
- 社会保障号码（SSN）
- 纳税人识别号或参考号
- 车辆识别号码 (VIN)

出生日期

托管数据标识符 ID： DATE_OF_BIRTH

支持的国家和地区： 任何

必填关键字：是。关键字包括：bday, b-day, birth date, birthday, date of birth, dob

注释： 支持包括大多数日期格式，例如所有数字以及数字和月份名称的组合。日期组件可以用空格、斜杠（/）或连字符（-）分隔。

驾驶执照识别号

托管数据标识符 ID：视国家或地区而定，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

支持的国家和地区：澳大利亚、奥地利、比利时、保加利亚、加拿大、克罗地亚、塞浦路斯、捷克、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、印度、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、 荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、英国、美国

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

国家或地区	关键词
澳大利亚	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
奥地利	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
比利时	fuehrerschein, fuehrerschein- nr, fuehrerschheinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrerschheinnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
保加利亚	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
加拿大	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,

国家或地区	关键词
	drivers permit number, driving licence, driving license, driving permit, permis de conduire
克罗地亚	vozačka dozvola
塞浦路斯	άδεια οδήγησης
捷克共和国	číslo licence, číslo licence řidiče, číslo řidičského průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
丹麦	kørekort, kørekortnummer
爱沙尼亚	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
芬兰	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
法国	permis de conduire
德国	fuehrerschein, fuehrerschein- nr, fuehrerscheinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrerscheinnummer, führerscheinnummer
希腊	δεια οδήγησης, adeia odigisis
匈牙利	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély

国家或地区	关键词
印度	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
爱尔兰	ceadúnas tiomána
意大利	patente di guida, patente di guida numero, patente guida, patente guida numero
拉脱维亚	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
立陶宛	vairuotojo pažymėjimas
卢森堡	fahrerlaubnis, führerschäin
马耳他	liċenzja tas-sewqan
荷兰	permis de conduire, rijbewijs, rijbewijsnummer
波兰	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
葡萄牙	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
罗马尼亚	numărul permisului de conducere, permis de conducere

国家或地区	关键词
斯洛伐克	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
斯洛文尼亚	vozniško dovoljenje
西班牙	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
瑞典	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
UK	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

国家或地区	关键词
美国	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

注释：无

选民名册编号

托管数据标识符 ID： UK_ELECTORAL_ROLL_NUMBER

支持的国家和地区：英国

必填关键字：是。关键字包括：electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

注释：无

全名

托管数据标识符 ID： NAME

支持的国家和地区： 任何

必填关键字：否

注释：Macie 只能检测全名。只支持拉丁字符集。

全球定位系统 (GPS) 坐标

托管数据标识符 ID： LATITUDE_LONGITUDE

支持的国家和地区：任何（如果坐标靠近英语关键字）。

必填关键字：是。关键字包括：coordinate, coordinates, lat long, latitude longitude, position

注释：如果纬度和经度坐标成对存储并且采用十进制度 (DD) 格式，Macie 可以检测 GPS 坐标，例如 41.948614,-87.655311。支持不包括以下格式的坐标检测：十进制分 （DDM） 格式，例如 41°56.9168'N 87°39.3187'W；或度、分、秒 (DMS) 格式，例如 41°56'55.0104"N 87°39'19.1196"W。

HTTP cookie

托管数据标识符 ID： HTTP_COOKIE

支持的国家和地区： 任何

必填关键字：否

注释：检测需要完整的 Cookie 或 Set-Cookie 标头。标头可以包含一个或多个名称/值对，例如：Set-Cookie: id=TWlrZQ 和 Cookie: session=3948; lang=en。

邮寄地址

托管数据标识符 ID：ADDRESS（适用于澳大利亚、加拿大、法国、德国、意大利、西班牙、英国和美国）、BRAZIL_CEP_CODE（适用于巴西邮政编码）

支持的国家和地区：澳大利亚、巴西、加拿大、法国、德国、意大利、西班牙、英国、美国

必填关键字：各不相同。ADDRESS托管数据标识符不需要关键字。BRAZIL_CEP_CODE托管数据标识符需要关键字。关键字包括：cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

评论：尽管ADDRESS托管数据标识符不需要关键字，但检测要求地址中包含城市或地点的名称以及受支持的国家或地区的相应邮政编码或邮政编码。BRAZIL_CEP_CODE托管数据标识符只能检测地址的邮政编码 (CEP) 部分。

身份证号码

支持包括印度的 Aadhaar 号码、意大利的 Codice Fiscale 号码、西班牙的 Documento Nacional de Identidad (DNI) 标识符、法国国家统计和经济研究所 (INSEE) 代码、德国国民身份证号码和巴西的 Registro Geral (RG) 号码。

托管数据标识符 ID：视国家或地区而定，BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

支持的国家和地区：巴西、法国、德国、印度、意大利、西班牙

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

国家或地区	关键词
巴西	registro geral, rg
法国	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#
德国	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
印度	aadhaar, aadhar, adhaar, uidai
意大利	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
西班牙	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#

注释：无

国民保险号码 (NINO)

托管数据标识符 ID： UK_NATIONAL_INSURANCE_NUMBER

支持的国家和地区：英国

必填关键字：是。关键字包括：insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

注释：无

护照编号

托管数据标识符 ID：视国家或地区而定，CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

支持的国家和地区：加拿大、法国、德国、意大利、西班牙、英国、美国

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

国家或地区	关键词
加拿大	passeport, passeport#, passport, passport#, passportno, passportno#
法国	numéro de passeport, passeport, passeport #, passeport n °, passeport non
德国	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
意大利	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
西班牙	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport

国家或地区	关键词
UK	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
美国	passport, travel document

注释：无

永久居留号码

托管数据标识符 ID： CANADA_NATIONAL_IDENTIFICATION_NUMBER

支持的国家和地区：加拿大

必填关键字：是。关键字包括：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

注释：无

电话号码

托管数据标识符 ID：视国家或地区而定，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

支持的国家和地区：巴西、加拿大、法国、德国、意大利、西班牙、英国、美国

必填关键字：各不相同。如果关键字靠近数据，则数字不必包含国家/地区代码。关键字包括：cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number。对于巴西，关键字还包括：cel, celular, fone, móvel, número residencial, numero residencial, telefone。如果关键字并不靠近数据，则数字必须包含国家/地区代码。

注释：对于美国，支持包括免费电话号码。

社会保险号码 (SIN)

托管数据标识符 ID： CANADA_SOCIAL_INSURANCE_NUMBER

支持的国家和地区：加拿大

必填关键字：是。关键字包括：canadian id, numéro d'assurance sociale, sin, social insurance number

注释：无

社会保障号码（SSN）

托管数据标识符 ID：视国家或地区而定，SPAIN_SOCIAL_SECURITY_NUMBER，USA_SOCIAL_SECURITY_NUMBER

支持的国家和地区：西班牙、美国

必填关键字：是。对于西班牙，关键字包括：número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#。对于美国，关键字包括：social security, ss#, ssn。

注释：无

纳税人识别号或参考号

支持包括：西班牙的 CIF、NIE 和 NIF 号码；巴西的 CNPJ 和 CPF 号码；意大利的 Codice Fiscale 号码；美国的 ITIN；印度的 PAN；德国的 Steueridentifikationsnummer 号码；澳大利亚的 TFN；法国的 TIN；以及英国的 TRN 和 UTR 号码。

托管数据标识符 ID：视国家或地区而定，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

支持的国家和地区：澳大利亚、巴西、法国、德国、印度、意大利、西班牙、英国、美国

必填关键字：是。下表列出了 Macie 识别的特定国家和地区的关键字。

国家或地区	关键词
澳大利亚	tax file number, tfn
巴西	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa

国家或地区	关键词
	jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
法国	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
德国	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
印度	e-pan, pan card, pan number, permanent account number
意大利	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
西班牙	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#
UK	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
美国	i.t.i.n.，个人纳税人识别号，itin

注释：无

车辆识别号码 (VIN)

托管数据标识符 ID： VEHICLE_IDENTIFICATION_NUMBER

支持的国家和地区：如果 VIN 与以下语言之一的关键字相邻，则为任意国家和地区：英语、法语、德语、立陶宛语、波兰语、葡萄牙语、罗马尼亚语或西班牙语。

必填关键字：是。关键字包括：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

注释：Macie 可以检测由 17 个字符序列组成并符合 ISO 3779 和 3780 标准的 VIN。这些标准旨在供全球使用。

在 Amazon Macie 中构建自定义数据标识符

自定义数据标识符是您定义的一组标准，用于检测 Amazon Simple Storage Service (Amazon S3) 对象中的敏感数据。标准由定义要匹配的文本模式的正则表达式（regex）和可选的字符序列以及优化结果的邻近规则组成。

使用自定义数据标识符，您可以定义反映组织特定场景、知识产权或专有数据（例如，员工 ID、客户账号或内部数据分类）的检测标准。如果将敏感数据发现作业或自动敏感数据发现配置为使用这些标识符，则可以用增添 Amazon Macie 提供的托管数据标识符的方式分析 S3 对象。

除了检测标准外，您还可以为自定义数据标识符生成的敏感数据调查发现定义自定义严重性设置。默认情况下，Macie 会为自定义数据标识符生成的所有调查发现分配中严重性，严重性不会根据与自定义数据标识符的检测标准匹配的文本出现次数而变化。通过定义自定义严重性设置，您可以根据匹配标准的文本的出现次数指定要分配的严重性。

主题

- 为自定义数据标识符定义检测标准
- 为自定义数据标识符定义调查发现严重性设置
- 创建自定义数据标识符
- 自定义数据标识符中支持正则表达式

为自定义数据标识符定义检测标准

在创建自定义数据标识符时，指定一个正则表达式 (regex) 来定义要在 S3 对象中匹配的文本模式。Macie 支持 Perl 兼容正则表达式 (PCRE) 库提供的正则表达式模式语法子集。有关更多信息，请参阅此部分后面的正则表达式支持。

您还可以指定字符序列，例如字词和短语，以及一个邻近规则来优化结果。

关键字

这些是特定的字符序列，必须靠近匹配正则表达式模式的文本。接近要求会随 S3 对象的存储格式或文件类型而变化：

- 对于结构化的列数据，如果文本匹配 regex 模式，并且关键字位于存储文本的字段或列的名称中，或者文本前面有相同字段或单元格值中关键字的最大匹配距离并在其范围内，则 Macie 将包括结果。这适用于 Microsoft Excel 工作簿、CSV 文件和 TSV 文件。
- 对于结构化的、基于记录的数据，如果文本匹配 regex 模式并且文本在关键字的最大匹配距离范围内，则 Macie 将包括结果。关键字可以是存储文本的字段或数组路径中某个元素的名称，也可以位于存储文本的字段或数组中的相同值之前并成为该值的一部分。这适用于 Apache Avro 对象容器、Apache Parquet 文件、JSON 文件和 JSON Lines 文件。
- 对于非结构化数据，如果文本匹配 regex 模式并且文本前面有关键字的最大匹配距离并在其范围内，则 Macie 将包括结果。对于 Adobe 便携式文档格式文件、Microsoft Word 文档、电子邮件消息和非二进制文本文件（CSV、JSON、JSON Lines 和 TSV 文件除外）都是如此。这包括这些类型的文件中的任何结构化数据，例如表。

您最多可以指定 50 个关键字。每个关键字可以包含 3–90 个 UTF-8 字符。关键字不区分大小写。

最大匹配距离

这是基于字符的关键字邻近规则。Macie 使用此设置来确定关键字是否位于与正则表达式模式匹配的文本之前。该设置定义了完整关键字的结尾与匹配正则表达式模式的文本结尾之间可以存在的最大字符数。如果文本与正则表达式模式匹配，出现在至少一个完整的关键字之后，并且出现在关键字的指定距离范围内，则 Macie 会将其包括在结果中。否则，Macie 会将其排除在结果之外。

您可以指定 1–300 个字符的距离。默认距离为 50 个字符。为了获得最佳结果，此距离应大于正则表达式设计用于检测的最小文本字符数。如果只有部分文本在关键字的最大匹配距离之内，则 Macie 不会将其包括在结果中。

忽略字词

这些是要从结果中排除的特定字符序列。如果文本与正则表达式模式匹配，但它包含忽略字词，则 Macie 不会将其包括在结果中。

您最多可以指定 10 个忽略字词。每个忽略字词可以包含 4–90 个 UTF-8 字符。忽略字词区分大小写。

例如，许多公司对员工 ID 都有特定的语法。其中一种语法可能是：一个大写字母，表示员工是全职 (F) 还是兼职 (P) 员工，后跟一个连字符 (-)，然后是一个用于识别员工的八位数序列。示例：F-12345678（表示全职员工）和 P-87654321（表示兼职员工）。

如果您创建自定义数据标识符来检测使用此语法的员工 ID，则可以使用以下正则表达式：`[A-Z]-\d{8}`。为了完善分析并避免误报，您还可以配置自定义数据标识符以使用关键字员工和员工 ID，最大匹配距离为 20 个字符。根据这些标准，只有当文本出现在关键字员工或员工 ID 之后并且所有文本都出现在其中一个关键字的 20 个字符范围内时，结果才会包括与正则表达式匹配的文本。

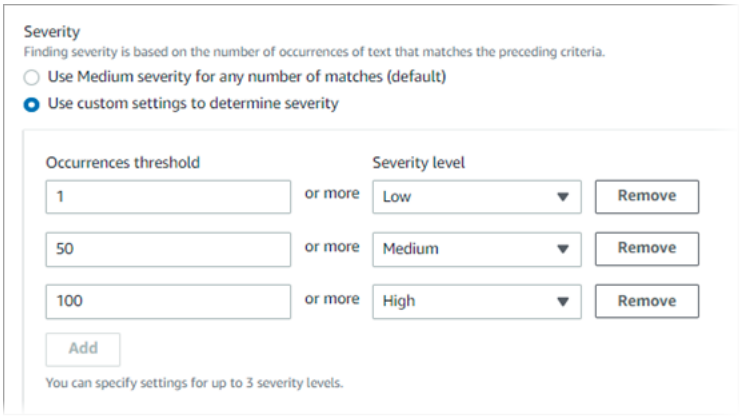
要演示关键字如何帮助您查找敏感数据并避免误报，请观看以下视频：Amazon Macie 如何使用关键字发现敏感数据。

为自定义数据标识符定义调查发现严重性设置

在创建自定义数据标识符时，您还可以为标识符生成的敏感数据调查发现定义自定义严重性设置。默认情况下，Macie 会为自定义数据标识符生成的所有调查发现分配中严重性，如果 S3 对象包含至少一次与自定义数据标识符的检测标准相匹配的文本，则 Macie 会自动为产生的调查发现分配中严重性。

使用自定义严重性设置，您可以根据与自定义数据标识符的检测标准匹配的文本的出现次数指定要分配的严重性。为此，您可以为多达三个严重性级别定义出现次数阈值：低（最不严重）、中和高（最严重）。出现次数阈值是 S3 对象中必须存在的最小匹配数，以生成具有具有指定严重性的调查发现。如果指定多个阈值，则这些阈值必须按严重性从低到高升序排列。

例如，下图显示了自定义数据标识符的严重性设置，该标识符指定了三个出现次数阈值，Macie 支持的每个严重性级别对应一个阈值。



下表显示了自定义数据标识符生成的调查发现的严重性。

出现次数阈值	严重性级别	结果
1	低	如果 S3 对象包含 1-49 次符合检测标准的文本，则产生的调查发现的严重性为低。

出现次数阈值	严重性级别	结果
50	中	如果 S3 对象包含 50-99 次符合检测标准的文本，则产生的调查发现的严重性为中。
100	高	如果 S3 对象包含 100 次或更多次符合检测标准的文本，则产生的调查发现的严重性为高。

您也可以使用严重性设置来指定是否要创建调查发现。如果 S3 对象包含的出现次数少于最低出现次数阈值，则 Macie 不会创建调查发现。

创建自定义数据标识符

按照以下步骤，通过使用 Amazon Macie 控制台创建自定义数据标识符。要以编程方式创建自定义数据标识符，请使用 Amazon Macie API 的 CreateCustomDataIdentifier 操作。

创建自定义数据标识符

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中的设置下方，选择自定义数据标识符。
3. 选择 Create（创建）。
4. 对于名称，输入自定义数据标识符的名称。名称可以包含多达 128 个字符。

   避免在名称中包含任何敏感数据。您账户的其他用户也许能够看到该名称，这取决于他们在 Macie 中允许执行的操作。
5. （可选）对于描述，输入自定义数据标识符的简要描述。描述可包含多达 512 个字符。

   避免在描述中包含任何敏感数据。您账户的其他用户也许能够看到该描述，这取决于他们在Macie 中允许执行的操作。
6. 对于正则表达式，输入定义要匹配的文本模式的正则表达式 (regex)。正则表达式可以包含多达 512 个字符。要了解支持的语法和约束条件，请参阅此部分后面的正则表达式支持。
7. （可选）对于关键字，输入多达 50 个字符序列（用逗号分隔）以定义特定文本，该文本必须贴近与正则表达式模式匹配的文本。每个关键字可以包含 3–90 个 UTF-8 字符。关键字不区分大小写。

只有当文本与正则表达式模式匹配并且文本位于其中一个关键字的最大匹配距离范围内时，Macie 才会在结果中包括一次出现，如前面的主题所述。

8. （可选）对于忽略字词，输入多达 10 个字符序列（用逗号分隔），用于定义要从结果中排除的特定文本。每个忽略字词可以包含 4–90 个 UTF-8 字符。忽略字词区分大小写。

   如果文本与正则表达式模式匹配，但它包含其中一个忽略字词，则 Macie 会从结果中排除一次出现。

9. （可选）对于最大匹配距离，输入关键字结尾与匹配正则表达式的文本结尾之间的最大字符数。距离可以为 1–300 个字符。默认距离为 50 个字符。

   只有当文本与正则表达式模式匹配并且文本在完整关键字的这个距离范围内时，Macie 才会在结果中包括一次出现，如前面的主题所述。

10. 对于严重性，选择您希望 Macie 如何为自定义数据标识符生成的敏感数据调查发现分配严重性：

    - 要自动为所有调查发现分配中严重性，请选择为任意数量的匹配项使用“中”严重性（默认）。使用此选项，如果受影响的 S3 对象包含一次或多次符合检测标准的文本，则 Macie 会自动为调查发现分配中严重性。
    - 要根据您指定的出现次数阈值来分配严重性，请选择使用自定义设置来确定严重性。然后使用出现次数阈值和严重性级别选项来指定 S3 对象中必须存在的最小匹配数，以生成具有所选严重性的调查发现。

      例如，要为报告符合检测标准的文本的 100 次或更多次出现的调查发现分配高严重性，请在出现次数阈值框中输入 **`100`**，然后从严重性级别列表中选择高。

      您最多可以指定三个出现次数阈值，Macie 支持的每个严重性级别对应一个阈值：低（表示最不严重）、中或高（表示最严重）。如果指定多个阈值，则阈值必须按严重性从低到高升序排列。如果 S3 对象包含的出现次数少于指定的最低阈值，则 Macie 不会创建调查发现。

11. （可选）对于标签，请选择添加标签，然后最多输入 50 个要分配给自定义数据标识符的标签。

    标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

12. （可选）对于评测，在样本数据框中输入最多 1,000 个字符，然后选择测试以测试检测标准。Macie 评测样本数据，并报告与检测标准匹配的文本出现次数。您可根据需要多次重复此步骤，以完善和优化标准。

> **Note**
>
> 我们强烈建议您在保存自定义数据标识符之前测试并完善检测标准。由于敏感数据发现作业使用自定义数据标识符，因此您无法在保存自定义数据标识符后对其进行编辑。这有助于确保您拥有敏感数据调查发现和发现结果的不可变历史记录，以便您执行数据隐私和保护的审计或调查。

13. 完成后，选择 Submit（提交）。

Macie 测试设置并验证它是否可以编译正则表达式。如果任何设置或正则表达式出现问题，则会发生错误并指明问题的性质。解决任何问题后，您可以保存自定义数据标识符。

自定义数据标识符中支持正则表达式

Macie 支持 Perl 兼容正则表达式 (PCRE) 库提供的正则表达式模式语法子集。在 PCRE 库提供的构造中，Macie 不支持以下模式元素：

- 反向引用
- 捕获组
- 条件模式
- 嵌入式代码
- 全局模式标志，如`/i`、`/m` 和 `/x`
- 递归模式
- 正向和负向后视和前视零宽度断言，如`?=`、`?!`、`?<=` 和 `?<!`

要为自定义数据标识符创建有效的正则表达式模式，还请注意以下提示和建议：

- 锚点 – 仅当您希望模式出现在文件的开头或结尾而不是行的开头或结尾时，才使用锚点（`^` 或 `$`）。
- 有界重复 – 出于性能考虑，Macie 限制了有界重复组的大小。例如，`\d{100,1000}` 无法在 Macie 中进行编译。为了近似于此功能，您可以使用开放式重复，如 `\d{100,}`。
- 不区分大小写 – 要使模式的某些部分不区分大小写，可以使用 `(?i)` 构造代替 `/i` 标志。
- 性能 – 无需手动优化前缀或者替代项。例如，将 `/hello|hi|hey/` 更改为 `/h(?:ello|i|ey)/` 不会提高性能。

- 通配符 – 出于性能考虑，Macie 限制了重复通配符的数量。例如，a*b*a* 无法在 Macie 中进行编译。

为了防范格式错误或长时间运行的表达式，Macie 会自动根据示例文本集合测试正则表达式模式。

使用 Amazon Macie 允许列表定义敏感数据例外

使用 Amazon Macie 中的允许列表，您可以定义 Macie 检查 Amazon Simple Storage Service (Amazon S3)对象中是否存在敏感数据时要忽略的特定文本和文本模式。对于您的特定场景或环境，这些通常是敏感数据异常。如果数据与允许列表中的文本或文本模式匹配，则即使该数据与托管数据标识符或自定义数据标识符的条件匹配，Macie 也不会报告该数据。通过使用允许列表，您可以完善对 Amazon S3 数据的分析并减少噪音。

您可以在 Macie 中创建和使用两种类型的允许列表：

- 预定义文本 – 对于此类列表，您可以指定要忽略的某些字符序列，例如，您所在组织的公众代表姓名、特定电话号码或您的组织用于测试的特定示例数据。如果您使用此类列表，Macie 会忽略与列表中的条目完全匹配的文本。

  如果您想要指定不敏感、不太可能更改且不一定遵循通用模式的单词、短语和其他类型的字符序列，则这种类型的允许列表非常有用。
- 正则表达式 – 对于此类列表，您可以指定一个正则表达式 (regex)，该正则表达式定义了要忽略的文本模式，例如，组织的公共电话号码、组织域的电子邮件地址或组织用于测试的模式化示例数据。如果您使用此类列表，Macie 会忽略与列表定义的模式完全匹配的文本。

  如果您想指定不敏感但有所变化或可能发生变化的文本，同时遵循通用模式，则这种类型的允许列表非常有用。

创建允许列表后，您可以创建和配置敏感数据发现任务以使用该列表，或者将其添加到自动敏感数据发现设置中。然后，Macie 在分析数据时使用该列表。如果 Macie 在允许列表中找到与条目或模式匹配的文本，则 Macie 不会在敏感数据发现、统计数据和其他类型的结果中报告该文本的出现情况。

您可以在除亚太地区（大阪）区域以外 Macie 当前可用的所有 AWS 区域 中创建和使用允许列表。

主题

- 允许在 Amazon Macie 中列出选项和要求
- 在 Amazon Macie 中创建和管理允许列表

允许在 Amazon Macie 中列出选项和要求

在 Amazon Macie 中，您可通过允许列表，指定想要 Macie 在检查 Amazon Simple Storage Service (Amazon S3) 对象敏感数据时会忽略的文本或文本模式。Macie 提供两类允许列表选项，即预定义文本和正则表达式。

如果您想让 Macie 忽略您认为不敏感的特定单词、短语和其他类型字符序列，则预定义文本列表非常有用。例如，您的组织公共代表的姓名、具体的电话号码或您的组织用于测试的具体样本数据。如果 Macie 发现符合托管数据标识符或自定义数据标识符的文本，并且该文本也与允许列表中的条目匹配，则 Macie 不会报告敏感数据发现、统计数据和其他类型的结果中出现的文本。

如果您希望 Macie 在遵循通用模式的情况下忽略已有变化或可能发生变化的文本，则适用正则表达式 (regex)。正则表达式指定要忽略的文本模式。示例包括贵组织的公共电话号码、组织域的电子邮件地址，或组织用于测试的模式化示例数据。如果 Macie 发现匹配托管数据标识符或自定义数据标识符的文本，并且该文本也与允许列表中的正则表达式模式匹配，则 Macie 不会报告敏感数据发现、统计数据和其他类型的结果中出现的文本。

您可以在除亚太地区（大阪）区域以外 Macie 当前可用的所有 AWS 区域 中创建和使用两种类型的允许列表。创建和管理允许列表时，切记以下选项和要求。另请注意，不支持邮件地址的允许列表条目及正则表达式模式。

主题

预定义文本列表的选项与要求

对于这种类型的允许列表，您可以提供以行分隔的纯文本文件，其中列出了要忽略的特定字符序列。列表条目通常包含特定的单词、短语和其他类型的字符序列，这些字符序列不敏感，不太可能改变，也不一定遵循特定模式。如果您使用这种类型的列表，Amazon Macie 不会报告出现与列表中的条目完全匹配的文本。Macie 将列表中的每个条目都视为字符串文本值。

若要使用这种类型的允许列表，首先要在文本编辑器中创建列表，并将其另存为纯文本文件。然后将列表上传至 S3 存储桶，并确保存储桶和对象的存储和加密设置允许 Macie 检索和解密该列表。然后在 Macie 中为列表创建和配置设置。

在 Macie 中配置设置后，我们建议您使用一组适用于您的账户或组织的、少量具有代表性的数据测试允许列表。若要测试列表，除了通常用于分析数据的托管数据标识符和自定义数据标识符之外，您还可以创建一次性作业并将该作业配置为使用该列表。然后您可查看作业结果，包括敏感数据调查发现、敏感数据发现结果或两者兼而有之。如果作业的结果与您的预期不同，则可更改和测试列表，直至结果达到预期。

配置和测试完允许列表后，您可创建和配置其他待使用作业，或将其添加至您的自动敏感数据发现设置。当每项作业开始运行或下一个自动发现分析周期开始时，Macie 会从 Amazon S3 中检索最新版本列表，并将其存储至临时内存。然后，Macie 在检查 S3 对象中是否有敏感数据时，使用此临时列表副本。当作业完成运行或分析周期完成后，Macie 会从内存中永久删除其列表副本。Macie 中的列表不存在。Macie 中仅保留列表设置。

> **Important**
>
> 由于 Macie 中不保留预定义文本列表，因此务必定期检查允许列表状态。如果 Macie 无法检索或解析您所配置的作业或使用的自动发现列表，Macie 不使用列表。这可能会导致异常结果，例如您在列表中指定的文本敏感数据调查发现。

主题

- 语法要求
- 存储需求
- 加密/解密要求
- 设计注意事项和建议

语法要求

创建此类允许列表时，请注意以下列表文件要求：

- 该列表必须存储为纯文本 (`text/plain`) 文件，例如.txt、.text 或 .plain 文件。
- 列表必须使用换行符分隔各个条目。例如：

```
Akua Mansa
```

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

Macie 将每行视为列表中的单独条目。该文件还可以包含空行，以提高可读性。Macie 在解析文件时会跳过空行。

- 每个关键字可以包含 1 到 90 个 UTF–8 字符。
- 每个条目必须完整、完全匹配，才能忽略文本。Macie 不支持在条目中使用通配符或者部分值。Macie 将每个条目都视为字符串文本值。匹配项不区分大小写。
- 该文件可以包含 1–100,000 个条目。
- 附加文件的存储总大小不能超过35 MB。

存储需求

在 Amazon S3 中添加和管理允许列表时，请注意以下存储要求与建议：

- 区域支持 – 允许列表必须存储在与您的 Macie 账户相同的 AWS 区域S3 存储桶内。如果运行列表存储在其他区域，Macie 将无法访问该列表。
- 存储桶所有权 – 允许列表必须存储在您AWS 账户拥有的、S3 存储桶内。如果您希望其他账户使用同样的允许列表，可以考虑创建 Amazon S3 复制规则，将该列表复制到这些账户拥有的存储桶。有关复制 S3 对象的信息，请参阅 Amazon Simple Storage Service 用户指南中的复制对象。

  此外，您的 AWS Identity and Access Management (IAM) 身份必须具有对存储列表的 S3 存储桶以及对象的读取权限。否则，您将无法使用 Macie 创建或更新列表的设置或者检查列表状态。
- 存储桶策略 – 如果您将允许列表存储在具有限制性存储桶策略的 S3 存储桶内，请确保该策略允许 Macie 检索该列表。为此，您可以将 Macie 服务关联角色条件添加至存储桶策略。有关更多信息，请参阅 允许 Macie 访问 S3 存储桶和对象。

  此外，请确保该策略允许您的 IAM 身份可读取存储桶。否则，您将无法使用 Macie 创建或更新列表的设置或者检查列表状态。
- 对象路径 – 如果您在 Amazon S3 中存储了多个允许列表，则每个列表的对象路径必须是唯一的。换言之，每个允许列表必须作为自己的 S3 对象单独存储。
- 存储类 – 允许列表必须使用以下存储类型之一直接存储至 Amazon S3 中：去冗余 (RRS)、S3 Glacier Instant Retrieval、S3 One Zone-IA、S3 Standard 或 S3 Standard-IA。

- 版本控制 – 向 S3 存储桶添加允许列表时，我们建议您同时为此存储桶启用版本控制。然后，您可以使用日期和时间值，将列表的版本与使用该列表的敏感数据发现任务和自动敏感数据发现周期结果相关联。这可以帮助您保护数据隐私、审计或调查行为。
- 对象锁定 – 为了防止允许列表在一定时间内或无限期地被删除或覆盖，您可以为存储该列表的 S3 存储桶启用对象锁定。启用此设置并不会阻止 Macie 访问此列表。有关此设置的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 S3 对象锁定。

加密/解密要求

如果您在 Amazon S3 中加密允许列表，则 Macie 服务相关角色 的权限策略通常会授予 Macie 解密该列表所需的权限。但是，这取决于所用的加密类型：

- 如果使用服务器端加密和 Amazon S3 托管密钥 (SSE-S3) 对列表进行加密，则 Macie 可以解密该列表。您的 Macie 账户的服务关联角色会向 Macie 授予其所需权限。
- 如果使用服务器端加密和AWS托管AWS KMS key（DSSE-KMS 或 SSE-KMS）对列表进行加密，Macie 可以解密该列表。您的 Macie 账户的服务关联角色会向 Macie 授予其所需权限。
- 如果列表使用服务器端加密并由客户管理AWS KMS key（DSSE-KMS 或 SSE-KMS）进行加密，则只有在您允许 Macie 使用密钥的情况下，Macie 才能解密该列表。要了解如何执行此操作，请参阅允许 Amazon Macie 使用客户自主管理型 AWS KMS key。

> **Note**
>
> 您可以使用外部密钥存储中的客户托管AWS KMS key解密列表。但是，与完全在 AWS KMS 中管理的密钥相比，密钥可能更慢且更不可靠。如果延迟或可用性问题使 Macie 无法解密列表，则 Macie 在分析 S3 对象时无法使用该列表。这可能会导致异常结果，例如您在列表中指定的文本敏感数据调查发现。为了降低这种风险，可以考虑将列表存储在“将密钥用作 S3 存储桶密钥”的 S3 存储桶内。
>
> 有关在外部密钥存储中使用 KMS 密钥的信息，请参阅 AWS Key Management Service 开发者指南中的外部密钥存储。有关使用 S3 存储桶密钥的信息，请参阅 Amazon Simple Storage Service 用户指南中的通过 Amazon S3 存储桶密钥降低 SSE-KMS 成本。

- 如果列表采用服务器端加密方法、通过客户提供的密钥 (SSE-C) 或客户端加密，则 Macie 无法解密此列表。可以考虑改用 SSE-S3、DSSE-KMS 或 SSE-KMS 加密。

如果列表通过 AWS 托管 KMS 密钥或客户托管 KMS 密钥加密，则您的 AWS Identity and Access Management (IAM) 身份必须获得此密钥使用许可。否则，您将无法使用 Macie 创建或更新列表的设

置或者检查列表状态。若要了解如何检查或更改 KMS 密钥的权限，请参阅AWS Key Management Service 开发者指南中的AWS KMS中的密钥策略。

有关 Amazon S3 数据加密选项的详细信息，请参阅《亚马逊简单存储服务用户指南》中的使用加密保护数据。

设计注意事项和建议

Macie 通常将允许列表中的每个条目都视为字符串文本值。也就是说，Macie 会忽略每次出现的、与允许列表中完整条目完全匹配的文本。匹配项不区分大小写。

但是，Macie 将这些条目用于更大的数据提取与分析框架。该框架包括机器学习和模式匹配函数，这些函数可以考虑语法和句法变体等维度，在多种情况下还包括关键字接近度。该框架还考虑了 S3 对象文件类型或存储格式。因此，在添加和管理允许列表中的条目时，切记以下注意事项和建议。

为不同的文件类型与存储格式做好准备

对于非结构化数据，例如 Adobe 可移植文档文件 (.pdf) 格式文本，Macie 会忽略与允许列表中完整条目完全匹配的文本，包括跨多行或多页的文本。

对于结构化数据（如 CSV 文件中的列式数据或 JSON 文件中基于记录的数据），如果所有文本都存储在单个字段、单元格或数组中，则 Macie 会忽略与允许列表中完整条目完全匹配的文本。此要求不适用于存储在其他非结构化文件 (例如 .pdf 文件中的表) 中的结构化数据。

例如，考虑 CSV 文件内的以下内容：

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

如果 `Akua Mansa` 和 `John Doe` 是允许列表中的条目，则 Macie 会忽略 CSV 文件中的这些名称。每个列表条目的完整文本存储至单个 `Name` 字段。

相反，请考虑包含以下列和字段的 CSV 文件：

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

如果 `Akua Mansa` 和 `John Doe` 是允许列表中的条目，则 Macie 不会忽略 CSV 文件中的这些名称。CSV 文件中的所有字段均不包含允许列表内条目的完整文本。

包含常见变体

为数字数据、专有名词、术语和字母数字字符序列等常见变体添加条目。例如，如果您要添加的名称或短语在单词之间仅包含一个空格，则还要添加单词之间含两个空格的变体。同样，添加包含/不包含特殊字符的单词和短语，并考虑纳入常见的句法和语义变体。

例如，对于美国电话号码425-555-0100，您可以将以下条目添加至允许列表中：

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

在跨国背景下，对于 2022 年 2 月 1 日 的日期，您可以添加包含英语和法语常见句法变体的条目，包括包含特殊字符/不包含特殊字符的变体：

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

对于人物姓名，请纳入您认为不敏感的、不同形式的名字条目。例如，包括：名字后跟姓氏；姓氏后跟名字，名字和姓氏由一个空格分隔；名字和姓氏由两个空格分隔；以及昵称。

例如，对于Martha Rivera这个姓名，您可以添加：

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

如果要忽略包含许多分段的特定名称变体，请创建一个使用正则表达式的允许列表。例如，对于名字Dr. Martha Lyda Rivera, PhD，您可以使用以下正则表达式：`^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`。

允许列表中正则表达式的选项和要求

对于这种类型的允许列表，您可以指定一个正则表达式 (regex)，该正则表达式定义了要忽略的文本模式，例如，组织的公共电话号码、组织域的电子邮件地址，或组织用于测试的模式化示例数据。正则表达式为您视为非敏感的指定种类数据定义了通用模式。如果您使用这种类型的允许列表，Amazon Macie 不会报告出现与特定模式完全匹配的文本。与要忽略的指定预定义文本的允许列表不同，您可以创建正则表达式和所有其他列表设置并将其存储在 Macie 中。

创建或更新此类允许列表时，可以在保存列表之前通过示例数据测试列表的正则表达式。建议您使用多组样本数据执行此操作。如果你创建的正则表达式过于笼统，Macie 可能会忽略您视为敏感的文本。如果正则表达式过于具体，Macie 可能会忽略您未视为敏感的文本。为了防范格式不正确或长时间运行表达式，Macie 还会根据一组示例文本自动编译和测试正则表达式，并通知您需要解决的问题。

为进行其他测试，我们建议您使用账户或组织的一小部分具有代表性的数据测试列表的正则表达式。为此，除了通常用于数据分析的托管数据标识符和自定义数据标识符之外，您还可以创建一次性作业，并将该作业配置为使用该列表。然后您可查看作业结果，包括敏感数据调查发现、敏感数据发现结果或两者兼而有之。如果作业的结果与预期不同，则可以更改和测试正则表达式，直到结果达到预期为止。

配置和测试允许列表后，您可以创建和配置其他作业，以使用该列表，或者将其添加至您账户的自动敏感数据发现设置中。当这些作业运行，或 Macie 对您的账户执行自动发现，Macie 使用最新版的列表正则表达式分析数据。

主题

语法支持和建议

允许列表可以指定包含最多 512 个字符的正则表达式 (regex)。Macie 支持 Perl 兼容正则表达式 (PCRE) 库提供的正则表达式模式语法子集。在 PCRE 库提供的构造中，Macie 不支持以下模式元素：

- 反向引用
- 捕获组
- 条件模式
- 嵌入式代码
- 全局模式标志，如 `/i`、`/m` 和 `/x`
- 递归模式

- 正向和负向后视和前视零宽度断言，如?=、?!、?<=和 ?<!

要为允许列表创建有效的正则表达式模式，还需注意以下提示和建议：

- 锚点 – 仅当您希望模式出现在文件的开头或结尾而不是行的开头或结尾时，才使用锚点（^或$）。
- 有界重复 – 出于性能考虑，Macie 限制了有界重复组的大小。例如，\d{100,1000} 无法在 Macie 中进行编译。为了近似于此功能，您可以使用开放式重复，如 \d{100,}。
- 不区分大小写 – 要使模式的某些部分不区分大小写，可以使用 (?i) 构造代替 /i 标志。
- 性能 – 无需手动优化前缀或者替代项。例如，将 /hello|hi|hey/ 更改为 /h(?:ello|i|ey)/ 不会提高性能。
- 通配符 – 出于性能考虑，Macie 限制了重复通配符的数量。例如，a*b*a* 无法在 Macie 中进行编译。
- 交替 – 要在单个允许列表中指定多个模式，可以使用交替运算符 (|) 连接这些模式。如果您这样操作，Macie 会使用 OR 逻辑组合模式并形成新模式。例如，如果您指定 (apple|orange)，Macie 会将苹果和橙色都识别为匹配项，并忽略两个单词的出现次数。如果要串联模式，请务必将串联表达式的总长度限制为 512 个或更少字符。

最后，在开发正则表达式时，请对其进行设计，以适应不同的文件类型和存储格式。在更大的数据提取和分析框架中，Macie 使用正则表达式。该框架考虑了 S3 对象的文件类型或者存储格式。对于结构化数据（例如 CSV 文件中的列式数据或 JSON 文件中基于记录的数据），只有当所有文本都存储在单个字段、单元格或数组中时，Macie 才会忽略与模式完全匹配的文本。此要求不适用于存储在其他非结构化文件（例如 Adobe 可移植文档文件 (.pdf) 中的表格）中的结构化数据。对于非结构化数据（例如 .pdf 文件中的文本），Macie 会忽略与模式完全匹配的文本，包括跨多行或多页的文本。

示例

以下示例演示了部分常见场景的有效正则表达式模式。

电子邮件地址

如果您使用自定义数据标识符检测电子邮件地址，则可以忽略您视为不敏感的电子邮件地址，例如您组织的电子邮件地址。

要忽略特定的二级和顶级域名电子邮件地址，可以使用以下模式：

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

其中*##*是二级域的名称，*com* 是顶级域。在这种情况下，Macie 会匹配和忽略johndoe@example.com 和 john.doe@example.com等地址。

要忽略任何通用顶级域名 (gTLD) (例如 .com 或 .gov) 中特定域名的电子邮件地址，可以使用以下模式：

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

其中*##* 是域的名称。在这种情况下，Macie 会匹配和忽略johndoe@example.com、john.doe@example.gov和 johndoe@example.edu等地址。

要忽略任何一个国家/地区代码顶级域名 (ccTLD) 中特定域名的电子邮件地址，例如加拿大的 .ca或澳大利亚的.au，您可使用此模式：

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

其中 *##* 是域名，*ca* 和 *au* 是要忽略的特定 ccTLD。在这种情况下，Macie 会匹配和忽略johndoe@example.ca 个 john.doe@example.au 等地址。

若要忽略用于特定域和 gTLD、且纳入第三级和第四级域的电子邮件地址，您可使用此模式：

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

其中*##*是域名，*com* 是 gTLD。在这种情况下，Macie 会匹配和忽略johndoe@www.example.com 和 john.doe@www.team.example.com等地址。

电话号码

Macie 提供托管数据标识符，可检测多个国家和地区的电话号码。要忽略某些电话号码（例如贵组织的免费电话号码或公用电话号码），您可以使用以下模式。

要忽略使用 800区号、且格式为(800) ###-####的免费电话号码：

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

要忽略使用 888区号、且格式为(888) ###-####的免费电话号码：

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

要忽略包含33个国家/地区代码、且格式为 +33 ## ## ## ## ## 的 10 位数法语电话号码：

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

要忽略使用特定区号和交换码的美国和加拿大电话号码，请不要包含国家/地区代码，且格式为 (###) ###-#### ：

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

其中 *123* 是区号，*555* 为交换码。

要忽略使用特定地区和交换代码的美国和加拿大电话号码，请包含国家/地区代码，且格式为+1 (###) ###-#### ：

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

其中 *123* 是区号，*555* 为交换码。

在 Amazon Macie 中创建和管理允许列表

在 Amazon Macie 中，允许列表定义了 Macie 在检查 Amazon Simple Storage Service (Amazon S3) 对象时是否存在敏感数据时要忽略的特定文本或文本模式。如果文本与允许列表中的输入或模式相匹配，则即使文本匹配托管数据标识符和自定义数据标识符的标准，Macie 也不会报告敏感数据调查发现中的文本。

您可通过 Macie 创建和管理以下类型的允许列表。

预定义的文本

使用这种类型的列表来指定单词、短语和其他类型的字符序列，它们不敏感，不太可能改变，也不一定遵循通用模式。例如，您的组织公共代表的姓名、具体的电话号码以及您的组织用于测试的具体样本数据。如果您使用此类列表，Macie 会忽略与列表中的条目完全匹配的文本。

对于这种类型的列表，您可以创建一个以行分隔的纯文本文件，其中列出了要忽略的指定文本。然后，将文件存储在一个 S3 存储桶并配置 Macie 的设置以访问桶中的列表。然后创建和配置敏感数据发现作业，以使用列表，或将列表添加至账户中的自动敏感数据发现设置。当每项作业开始运行或下一个自动发现分析周期开始时，Macie 会从 Amazon S3 中检索最新版本列表。然后，Macie 在检查 S3 对象中是否有敏感数据时，使用该版本列表。如果 Macie 发现与列表中的条目完全匹配的文本，Macie 不会将所示文本报告为敏感数据。

正则表达式

使用这种类型的列表（正则表达式），指定一个正则表达式来定义要忽略的文本模式。示例包括贵组织的公共电话号码、组织域的电子邮件地址，以及组织用于测试的模式化示例数据。如果您使用这种类型的列表，Macie 会忽略与列表定义的正则表达式完全匹配的文本。

对于此类列表，您可以创建正则表达式，该正则表达式定义不敏感、但有所变化或可能发生变化的文本。与包含预定义文本的列表不同，您可以创建并将正则表达式和所有其他列表设置存储在 Macie 中。然后创建和配置敏感数据发现作业，以使用列表，或将列表添加至账户中的自动敏感数据发现设置。当运行此作业或 Macie 对您的账户执行自动发现时，Macie 会使用最新版本的列表正则表达式分析数据。如果 Macie 发现与列表定义模式完全匹配的文本，Macie 不会将所示文本报告为敏感数据。

有关每种列表类型的详细要求、建议和示例，请参阅 允许列出选项和要求。在每个支持的AWS 区域账户中可创建最多 10 条允许列表、最多五条指定预定义文本的允许列表、最多五条指定正则表达式的允许列表。您可以在除亚太地区（大阪）区域以外 Macie 当前可用的所有 AWS 区域 中创建和使用允许列表。

若要创建和管理允许列表，您可使用 Amazon Macie 控制台或Amazon Macie API。以下主题说明如何使用。对于 API，主题包括如何使用 AWS Command Line Interface(AWS CLI) 执行这些任务的示例。您也可以使用当前版本的其他 AWS 命令行工具或 AWS SDK，或者直接向 Macie 发送 HTTPS 请求。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

主题

- 创建允许列表
- 检查允许列表状态
- 更改允许列表
- 删除允许列表

创建允许列表

在 Amazon Macie 中创建允许列表的方式，取决于您要创建的列表类型。允许列表可以是列出要忽略预定义文本的文件，也可以是定义要忽略的文本模式的正则表达式 (regex)。选择您想要创建的列表类型部分。

预定义的文本

在 Macie 中创建此类允许列表前，请执行以下步骤：

1. 使用文本编辑器创建以行分隔的纯文本文件，其中列出了要忽略的特定文本，例如 .txt、.text 或 .plain 文件。有关更多信息，请参阅预定义文本列表语法要求。
2. 将文件上传至 S3 存储桶并记下存储桶和对象的名称。在 Macie 中配置设置时，需要输入此名称。

3. 确保 S3 存储桶和对象的设置允许您和 Macie 从存储桶检索列表。有关更多信息，请参阅预定义文本列表存储要求。
4. 如果对 S3 对象进行了加密，还要确保使用允许您和 Macie 使用的密钥对其进行加密。有关更多信息，请参阅预定义文本列表加密/解密要求。

完成上述步骤后，就可以在 Macie 中配置列表设置了。您可通过 Amazon Macie 控制台或 Amazon Macie API 配置设置。

Console

按照以下步骤，使用 Amazon Macie 控制台配置允许列表设置。

若要在 Macie 中配置允许列表设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的 设置 下，选择 允许列表。
3. 在允许列表页面，选择 创建。
4. 在 选择列表类型 下，选择 预定义文本。
5. 在 列表设置 下，使用以下选项，输入允许列表的其他设置：

   - 对于 名称，输入列表名称。名称可以包含多达 128 个字符。
   - 对于 描述，选择性地输入列表的简要描述。描述可包含多达 512 个字符。
   - 在 S3 存储桶名称中，输入存储列表的存储桶的全名。

     在 Amazon S3 中，您可在存储桶属性的名称字段中找到此值。此值区分大小写。此外，输入名称时不要使用通配符或部分值。
   - 在 S3 对象名称中，输入存储列表的 S3 对象的全名。

     在 Amazon S3 中，您可在对象属性的密钥字段中找到此值。如果名称包含路径，请确保在输入名称时包含完整路径，例如**`allowlists/macie/mylist.txt`**。此值区分大小写。此外，输入名称时不要使用通配符或部分值。
6. （可选）在 标签下，选择 添加标记，然后最多可输入 50 个可分配至允许列表的标签。

   标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。
7. 完成后，选择 Create（创建）。

Macie 正在测试列表设置。Macie 还会验证它是否可从 Amazon S3 中检索列表和解析列表内容。如果出现了错误，Macie 则显示一条说明错误的消息。有关错误故障排除的详细信息，请参阅 预定义文本列表的选项与要求。解决任何错误后，您可以保存列表设置。

API

要以编程方式配置允许列表设置，请使用 Amazon Macie API 的 CreateAllowList 操作，并为所需参数指定相应值。

对于 `criteria` 参数，使用 `s3WordsList` 对象指定 S3 存储桶 (`bucketName`) 的名称和存储列表的 S3 对象 (`objectKey`) 的名称。若要确定存储桶名称，请参阅 Amazon S3 中的 `Name` 字段。若要确定对象名称，请参阅 Amazon S3 中的 `Key` 字段。注意，这些值区分大小写。此外，指定这些名称时不要使用通配符或部分值。

若要使用AWS CLI配置设置，请运行create-allow-list命令，并为所需参数指定相应的值。以下示例介绍了如何为存储于 S3 存储桶内的、名为 *DOC-EXAMPLE-BUCKET* 的允许列表配置设置。存储列表的 S3 对象名称是 *allowlists/macie/mylist.txt*。

此示例针对 Linux、macOS 或 Unix 进行格式化，并使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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."
```

此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
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."
```

当您提交请求时，Macie 会测试列表设置。Macie 还会验证它是否可从 Amazon S3 中检索列表和解析列表内容。如果发生错误，您的请求将会失败，Macie 会返回一条描述错误的消息。有关错误故障排除的详细信息，请参阅 预定义文本列表的选项与要求。

如果 Macie 能够检索并解析列表，则您的请求成功，并且您将收到与以下类似的输入内容。

```
{
```

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

arn 是所创建允许列表的 Amazon 资源名称（ARN），id是此列表的唯一标识符。

保存列表设置后，您可创建和配置敏感数据发现作业以使用列表，或将列表添加至账户中的自动敏感数据发现设置。当作业开始运行或自动发现分析周期开始时，Macie 会从 Amazon S3 中检索最新版本列表。然后，Macie 在分析数据时使用该版本列表。

正则表达式

当您创建指定正则表达式 (regex) 的允许列表时，可以直接在 Macie 中定义正则表达式和所有其他列表设置。Macie 支持 Perl 兼容正则表达式 (PCRE) 库提供的正则表达式模式语法子集。有关更多信息，请参阅语法支持和建议。

您可以使用 Amazon Macie 控制台或 Amazon Macie API 创建此类列表。

Console

按照以下步骤，使用 Amazon Macie 控制台创建允许列表。

若要创建允许列表

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的 设置 下，选择 允许列表。
3. 在允许列表页面，选择 创建。
4. 在 选择列表类型 下，选择 正则表达式。
5. 在 列表设置 下，使用以下选项，输入允许列表的其他设置：
   - 对于 名称，输入列表名称。名称可以包含多达 128 个字符。
   - 对于 描述，选择性地输入列表的简要描述。描述可包含多达 512 个字符。
   - 用于 正则表达式，输入定义要忽略的文本模式的正则表达式。正则表达式可以包含多达 512 个字符。
6. （可选）对于 评测，在 样本数据框中输入最多 1,000 个字符，然后选择 测试以测试正则表达式。Macie 评测样本数据，并报告与正则表达式匹配的文本出现次数。您可根据需要多次重复此步骤，以完善和优化正则表达式。

> **Note**
>
> 我们建议您通过多组样本数据测试和完善正则表达式。如果你创建的正则表达式过于笼统，Macie 可能会忽略您视为敏感的文本。如果正则表达式过于具体，Macie 可能会忽略您未视为敏感的文本。

7. （可选）在 标签下，选择 添加标记，然后最多可输入 50 个可分配至允许列表的标签。

   标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

8. 完成后，选择 Create（创建）。

Macie 正在测试列表设置。Macie 还会测试正则表达式，以验证它是否可以编译表达式。如果出现了错误，Macie 则显示一条说明错误的消息。有关错误故障排除的详细信息，请参阅 允许列表中正则表达式的选项和要求。解决任何错误后，您可以保存允许列表设置。

API

在 Macie 中创建此类允许列表前，我们建议您使用多组示例数据测试和完善正则表达式。如果你创建的正则表达式过于笼统，Macie 可能会忽略您视为敏感的文本。如果正则表达式过于具体，Macie 可能会忽略您未视为敏感的文本。

若要测试 Macie 测试表达式，您可使用 Amazon Macie API 的TestCustomDataIdentifier操作；或对于AWS CLI，运行test-custom-data-identifier命令。Macie 使用相同的基础代码编译允许列表和自定义数据标识符的表达式。如果以这种方式测试表达式，请确保仅为 `regex` 和 `sampleText` 参数指定值。否则，您将无法收到准确结果。

当您准备好创建此类允许列表时，请使用 Amazon Macie API 的 CreateAllowList 操作，并为所需参数指定相应的值。对于 `criteria` 参数，使用`regex`字段，以指定送一待忽略文本模式的正则表达式。表达式可包含多达 512 个字符。

若要使用 AWS CLI创建此类列表，请运行 create-allow-list 命令，并为所需参数指定相应的值。以下示例创建了名为*`my_allow_list`*的允许列表。正则表达式旨在忽略自定义数据标识符能够检测到的、`example.com` 域的所有电子邮件地址。

此示例针对 Linux、macOS 或 Unix 进行格式化，并使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws macie2 create-allow-list \
```

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

此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

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

当您提交请求时，Macie 会测试列表设置。Macie 还会测试正则表达式，以验证它是否可以编译表达式。如果发生错误，请求将会失败，Macie 会返回一条描述错误的消息。有关错误故障排除的详细信息，请参阅 允许列表中正则表达式的选项和要求。

如果 Macie 可编译表达式，则请求成功并且您将收到类似于以下内容的输出：

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

`arn` 是所创建允许列表的 Amazon 资源名称（ARN），`id`是此列表的唯一标识符。

保存列表后，您可创建和配置敏感数据发现作业以使用列表，或将列表添加至账户中的自动敏感数据发现设置。当运行此作业或 Macie 对您的账户执行自动发现时，Macie 会使用最新版本的列表正则表达式分析数据。

检查允许列表状态

务必定期检查允许列表状态。否则，错误可能会导致 Amazon Macie 生成异常分析结果，例如您在允许列表中指定的文本敏感数据调查发现。

如果您将敏感数据发现作业配置为使用允许列表，但是 Macie 在作业开始运行时无法访问或使用该列表，则该作业将继续运行。但是，Macie 在分析 S3 对象时不使用此列表。同样，如果分析周期开始自动敏感数据发现，而 Macie 无法访问或使用指定的允许列表，则分析将继续进行，但 Macie 不使用此列表。

指定正则表达式 (regex) 的允许列表发生错误的概率较低。部分原因是当您创建或者更新列表设置时，Macie 会自动测试正则表达式。此外，您还可以将正则表达式和所有其他列表设置存储至 Macie 。

但是，指定预定义文本的允许列表可能会出错，部分原因是您将列表存储在 Amazon S3 中，而非 Macie 中。错误的常见原因包括：

- S3 存储桶或对象已被删除。
- S3 存储桶或对象已被重命名，Macie 中的列表设置未指定新名称。
- S3 存储桶的权限设置已更改，Macie 将失去对存储桶和对象的访问权限。
- S3 存储桶的加密设置已更改，Macie 无法解密存储列表对象。
- 加密密钥策略已更改，Macie 将无法访问此密钥。Macie 无法解密存储列表的 S3 对象。

> **Important**
>
> 由于这些错误会影响您的分析结果，因此我们建议您定期检查允许列表状态。如果您更改了存储允许列表的 S3 存储桶的权限或加密设置，或者更改了用于加密列表的 AWS Key Management Service (AWS KMS) 密钥策略，我们建议您也执行此操作。

您可以使用 Amazon Macie 控制台或 Amazon Macie API 检查允许列表状态。有关帮助您进行错误故障排除的详细信息，请参见 预定义文本列表的选项与要求。

Console

按照以下步骤，使用 Amazon Macie 控制台检查允许列表状态。

检查允许列表状态

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的 设置 下，选择 允许列表。
3. 在允许列表页面，选择刷新 ()。Ma
   会测试所有允许列表设置，并更新 状态 字段以指示每个列表的当前状态。

   如果列表指定了正则表达式，则其状态通常为 确定。这意味着 Macie 可以编译表达式。如果列表指定了预定义文本，则可能包含以下状态之一。

确定

Macie 可以检索和解析列表的内容。

访问被拒绝

不允许 Macie 访问存储列表的 S3 对象。Amazon S3 拒绝了检索对象的请求。如果通过 Macie 不允许使用的客户托管AWS KMS key加密对象，则列表也可以具有此状态。

要解决此错误，检查桶策略以及桶和对象的其他权限设置。确保允许 Macie 访问和检索对象。如果使用客户托管 AWS KMS 密钥加密对象，还要查看密钥政策并确保允许 Macie 使用密钥。

Error

Macie 尝试检索或解析列表内容时发生暂时性或内部错误。如果使用 Amazon S3 和 Macie 无法访问或使用的加密密钥对列表进行加密，则允许列表也可以具有此状态。

若要修正此错误，请等待几分钟，然后再次选择刷新
()。
如果状态继续为 错误，请检查 S3 对象的加密设置。确保使用 Amazon S3 和 Macie 可以访问和使用的密钥加密对象。

对象为空

Macie 可以检索 Amazon S3 列表，但列表不包含任何内容。

若要修正此错误，请从 Amazon S3 下载数据元并确保其中包含正确的条目。如果条目正确，请在 Macie 中查看列表设置。确保指定的存储桶和对象名称正确。

未找到对象

该列表在 Amazon S3 中不存在。

若要修正错误，请在 Macie 中查看列表设置。确保指定的存储桶和对象名称正确。

超出配额

Macie 可以在 Amazon S3 中访问列表。但是，列表中的条目数或列表的存储大小超过了允许列表配额。

若要修正此错误，请将列表分成多个文件。确保每个文件包含的条目数量少于 100,000 个。还要确保每个文件的大小都小于 35MB。将文件上传到 Amazon S3 然后，在 Macie 中为每个文件配置列表设置。每个支持的AWS 区域最多有五个自定义文本列表。

受限

Amazon S3 限制了检索列表的请求。

若要修正此错误，请等待几分钟，然后再次选择刷新 ()。

用户访问被拒绝

Amazon S3 拒绝了检索对象的请求。如果指定的对象存在，则不允许您访问该对象，或者使用不允许使用的 AWS KMS 密钥对其进行加密。

要解决此错误，与您的 AWS 管理员合作，确保列表的设置指定正确的桶和对象名称，并且您具有对桶和对象的读取权限。如果对象已加密，还要确保使用允许您使用的密钥对其进行加密。

4. 若要检查特定列表的设置和状态，请选择列表的名称。

API

若要以编程的方式检查允许列表状态，请使用Amazon Macie API 中的GetAllowList操作；或对于 AWS CLI，运行get-allow-list命令

对于 `id` 参数，指定待检查状态允许列表的唯一标识符。要获取此标识符，可以使用ListAllowLists操作。ListAllowLists 操作会检索有关您账户的所有允许列表的信息。如果您 使用的是AWS CLI，则可以运行list-allow-lists命令检索此信息。

当您提交 GetAllowList 请求时，Macie 会测试允许列表的所有设置。如果设置指定了正则表达式 (regex)，Macie 会验证它是否可以编译此表达式。如果设置指定了预定义文本列表，Macie 会验证它是否可以检索和解析此列表。

然后 Macie 返回提供允许列表详细信息的`GetAllowListResponse`对象。在 `GetAllowListResponse` 对象中，`status` 对象表示列表的当前状态：状态码 (`code`)；以及列表状态的简要描述 (`description`)，视状态代码而定。

如果允许列表指定了正则表达式，则状态码通常为`OK`，并且没有相关的描述。这意味着 Macie 成功编译了此表达式。

如果允许列表指定了预定义文本，则状态代码会视测试结果而异：

- 如果 Macie 成功检索并解析了列表，则状态码为0K，并且没有相关的描述。
- 如果错误阻止 Macie 检索或解析列表，则状态代码和描述将表明错误性质。

有关可能的状态代码列表和每个状态码的描述，请参阅Amazon Macie API 引用中的AllowListStatus。

更改允许列表

创建允许列表后，您可以在 Amazon Macie 中更改该大部分列表设置。例如，您可以更改列表的名称和描述，也可添加和编辑列表标签。仅列表类型设置无法更改。例如，如果现有的允许列表指定了正则表达式，则无法将其类型更改为预定义文本。

如果允许列表指定了预定义文本，您也可以更改列表中的条目。据此，请更新包含条目的文件，然后将该文件的新版本上传至 Amazon S3。下次 Macie 准备使用此列表时，Macie 会从 Amazon S3 中检索该文件的最新版本。当您上传新文件时，请确保将其存储在同一 S3 存储桶和对象中。或者，如果您更改了存储桶或对象的名称，请确保在 Macie 中更新列表设置。

您可以使用 Amazon Macie 控制台或 Amazon Macie API 更改允许列表状态。

Console

按照以下步骤，使用 Amazon Macie 控制台更改允许列表设置。

若要更改允许列表

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的 设置 下，选择 允许列表。
3. 在 允许列表页面，选择要更改的允许列表的名称。允许列表页面打开并显示此列表当前设置。
4. 若要为允许列表分配或编辑标签，请在标签部分中选择管理标签。然后根据需要更改标签。完成后，选择 Save (保存)。
5. 要更改允许列表的其他设置，请在 列表设置部分中选择 编辑。然后，更改您希望对其进行更改的设置。

    - 名称 - 输入列表的新名称。名称可以包含多达 128 个字符。
    - 描述 - 输入列表的新描述。描述可包含多达 512 个字符。
    - 如果允许列表指定了预定义文本：

- S3 存储桶名称 - 输入存储列表的存储桶的全名。

  在 Amazon S3 中，您可在存储桶属性的名称字段中找到此值。此值区分大小写。此外，输入名称时不要使用通配符或部分值。

- S3 对象名称 - 输入存储列表的 S3 对象的全名。

  在 Amazon S3 中，您可在对象属性的密钥字段中找到此值。如果名称包含路径，请确保在输入名称时包含完整路径，例如**allowlists/macie/mylist.txt**。此值区分大小写。此外，输入名称时不要使用通配符或部分值。

- 如果允许列表指定了正则表达式 (regex)，请在正则表达式框内输入新的正则表达式。正则表达式可以包含多达 512 个字符。

  输入新的正则表达式后，可选择对其进行测试。为此，请在示例数据框中输入最多包含 1,000 个字符的文本，然后选择测试。Macie 评测样本数据，并报告与正则表达式匹配的文本出现次数。保存更改前，您可根据需要多次重复此步骤，以完善和优化正则表达式。

更改完设置后，选择 保存。

Macie 正在测试列表设置。对于预定义文本列表，Macie 还会验证它是否可从 Amazon S3 中检索列表和解析列表内容。对于正则表达式，Macie 还会验证它是否可以编译表达式。如果出现了错误，Macie 则显示一条说明错误的消息。有关错误故障排除的详细信息，请参阅 允许列出选项和要求。修正错误后，您可保存更改。

API

若要以编程的方式更改允许列表，请使用 Amazon Macie API 中的 UpdateAllowList 操作；或对于 AWS CLI，运行update-allow-list命令。根据您的请求，使用支持的参数，为所有待更改设置指定新值。注意，`criteria`、`id` 和 `name` 参数是必需的。如果您不想更改必填参数值，请指定昂钱参数值。

例如，以下命令可更改现有允许列表的名称和描述。此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
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"
```

其中：

- *km2d4y22hp6rv05example*是列表的唯一标识符。
- *my_allow_list-email* 是列表的新名称。
- *[a-z]@example.com* 是列表的标准，一个正则表达式。
- *## example.com ##########* 是该列表的新描述。

当您提交请求时，Macie 会测试列表设置。如果列表指定了预定义文本，Macie 还会验证它是否可从 Amazon S3 中检索列表和解析列表内容。如果列表指定了正则表达式，则包括验证 Macie 是否可编译表达式。

如果 Macie 测试设置时发生错误，请求将会失败，Macie 会返回一条描述错误的消息。有关错误故障排除的详细信息，请参阅 允许列出选项和要求。如果请求由于其他原因失败，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

如果请求成功，Macie 会更新列表设置，并且您将收到与以下类似的输入内容。

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

`arn` 是所更新允许列表的 Amazon 资源名称（ARN），`id`是此列表的唯一标识符。

删除允许列表

当您在 Amazon Macie 中删除允许列表时，即永久删除此列表的所有设置。这些设置在删除后将无法恢复。如果设置指定了您存储在 Amazon S3 中的预定义文本列表，则 Macie 不删除存储该列表的 S3 对象。仅删除 Macie 中的设置。

如果您将敏感数据发现任务配置为使用允许列表，然后删除此列表，则这些作业将按计划运行。但是，您的作业结果（包括敏感数据调查发现和敏感数据发现结果）可能会报告您之前在允许列表中指定的文本。同样，如果您将自动敏感数据发现配置为使用列表，然后删除此列表，则每日分析周期将继续运行。但是，敏感数据调查发现、统计数据或其他类型的结果可能会报告您之前在允许列表中指定的文本。

在删除允许列表之前，我们建议您 查看任务清单，以确定使用该列表并计划在将来运行的作业。在清单中，详细信息面板会显示作业是否配置为使用任何允许列表。如果是，则显示指定的允许列表。此外，检查您的自动敏感数据发现设置。您可能认为，列表更改优于删除。

作为附加保护措施，当您尝试删除允许列表时，Macie 会检查所有作业设置。如果您将作业配置为使用此列表，并且其中任何一个作业的状态不是 完成 或已取消，则如果您不提供其他确认信息，Macie 不会删除该列表。

您可以使用 Amazon Macie 控制台或 Amazon Macie API 删除允许列表。

Console

按照以下步骤，使用 Amazon Macie 控制台删除允许列表。

若要删除允许列表

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的 设置 下，选择 允许列表。
3. 在 允许列表页面，选择您希望删除的允许列表的复选框。
4. 在 Actions 菜单上，选择 Delete。
5. 提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

API

要以编程方式删除允许名单，请使用 Amazon Macie API 中的 DeleteAllowList 操作。对于 `id` 参数，指定待删除允许列表的唯一标识符。要获取此标识符，可以使用 ListAllowLists 操作。ListAllowLists 操作会检索有关您账户的所有允许列表的信息。如果您 使用的是AWS CLI，则可以运行list-allow-lists命令检索此信息。

对于 `ignoreJobChecks` 参数，指定是否强制删除列表，即使敏感数据发现任务配置为使用该列表也不例外：

- 如果您指定 `false`，Macie 会检查所有状态非 `COMPLETE` 或 `CANCELLED` 的作业设置。如果这些作业均未配置为使用此列表，则 Macie 将永久删除此列表。如果其中任何一项作业配置为使用此列表，Macie 会拒绝您的请求并返回 HTTP 400 (`ValidationException`) 错误。错误消息指出了最多 200 项作业的适用任务数。
- 如果您指定 `true`，Macie 将永久删除此列表，而不检查任何作业设置。

若要使用AWS CLI删除允许列表，请运行 delete-allow-list 命令。例如：

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

其中 *nkr81bmtu2542yyexample* 是唯一一个允许删除列表的标识符。

如果请求成功，Macie 将返回空的 HTTP 200 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

如果允许列表指定了预定义文本，则可以选择删除存储此列表的 S3 对象。但是，保留此对象有助于确保您拥有敏感数据的调查发现、数据隐私及保护审计或调查的发现结果的不可变历史记录。

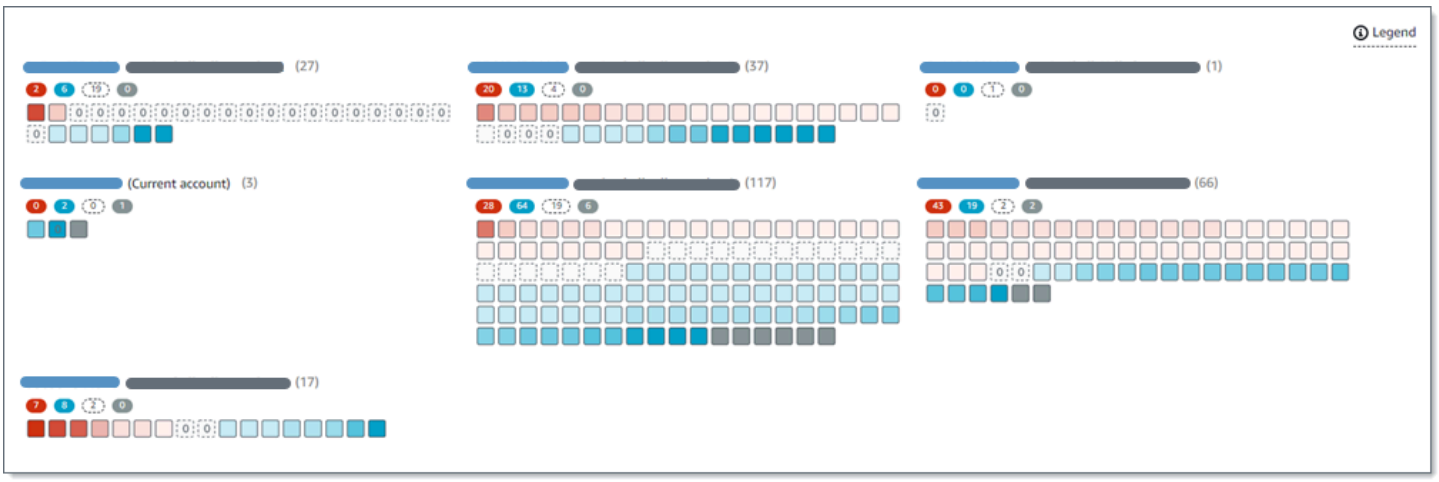
使用 Amazon Macie 执行自动敏感数据发现

要广泛了解敏感数据可能存放在您的 Amazon Simple Storage Service (Amazon S3) 数据资产中的位置，请将 Amazon Macie 配置为对您的账户或组织执行自动敏感数据发现。通过自动敏感数据发现，Macie 可以持续评测您的 S3 存储桶清单，并使用采样技术识别和选择存储桶中具有代表性的 S3 对象。然后，Macie 检索并分析所选对象，检查它们是否有敏感数据。

默认情况下，Macie 使用我们为自动化敏感数据发现推荐的一组托管数据标识符来分析 S3 对象。您可以通过将 Macie 配置为在为您的账户或组织执行自动敏感数据发现时使用特定的托管数据标识符、自定义数据标识符和允许列表来定制分析。此外，Macie 还会自动从您的所有 S3 存储桶中选择和分析对象。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶中的对象。您可以通过排除特定存储桶（例如，通常存储AWS日志数据的 S3 存储桶）来调整分析范围。

随着分析的每天进行，Macie 会生成其发现的敏感数据及其执行的分析的记录：敏感数据调查发现，用于报告 Macie 在单个 S3 对象中发现的敏感数据，以及敏感数据发现结果，用于记录有关单个 S3 对象分析的详细信息。Macie 还会更新统计数据、库存数据以及它提供的有关您的 Amazon S3 数据的其他信息。

例如，控制台上的交互式热图可直观地呈现整个数据资产的数据敏感度：



这些功能旨在帮助您评测整个 Amazon S3 数据资产的数据敏感度，并深入调查和评测个人账户、存储桶和对象。它们还可以通过运行敏感数据发现作业，帮助您确定在哪里进行更深入、更直接的分析。结合 Macie 提供的有关您的 Amazon S3 数据安全和隐私的信息，您还可以使用这些功能来识别可能需要立即进行补救的情况，例如，Macie 在其中发现敏感数据的可公开访问存储桶。

要配置和使用自动化敏感数据发现，您的账户必须是独立的 Macie 账户或组织的 Macie 管理员账户。

主题

自动敏感数据发现的工作原理

当您为 AWS 账户 启用 Amazon Macie 时，Macie 会为您在当前 AWS 区域 中的账户创建一个 AWS Identity and Access Management (IAM) 服务相关角色。此角色的权限策略允许 Macie 代表您调用其他 AWS 服务 并监控 AWS 资源。通过使用此角色，Macie 生成并维护该区域中 Amazon Simple Storage Service (Amazon S3) 存储桶的完整清单。清单包括有关每个 S3 存储桶和存储桶中对象的信息。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶信息。有关更多信息，请参阅管理多个 账户。

如果您的 Macie 账户启用了自动敏感数据发现，Macie 将每天评测清单数据，以识别符合自动发现条件的 S3 对象。作为评测的一部分，Macie 还会选择代表性对象的样本进行分析。然后，Macie 从 Amazon S3 中检索并分析每个选定对象的最新版本，检查每个对象中是否有敏感数据。

随着分析的进行，Macie 会更新统计数据、清单数据及其提供的有关您 Amazon S3 数据的其他信息。Macie 还会记录其发现的敏感数据及其执行的分析。生成的数据可以深入了解 Macie 在您的 Amazon S3 数据资产中发现敏感数据的位置，涵盖了 Macie 为您的账户监控和分析的所有 S3 存储桶。这些数据可以帮助您评测敏感数据的安全性和隐私，确定在哪里进行更深入的调查，并确定需要采取补救措施的案例。

有关自动化敏感数据发现如何工作的简短演示，请观看以下视频：Amazon Macie 自动数据发现概述。

要配置和使用自动化敏感数据发现，您的账户必须是独立的 Macie 账户或组织的 Macie 管理员账户。

主题

关键组件

Amazon Macie 使用多种功能和技术来自动发现您的 Amazon S3 数据的敏感数据。这些功能和技术与 Macie 用来帮助您监控 Amazon S3 数据以实现安全和访问控制的功能和技术相结合。

选择要分析的 S3 对象

Macie 每天都会评测您的 Amazon S3 清单数据，以识别符合自动敏感数据发现分析条件的 S3 对象。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶清单数据。

作为评测的一部分，Macie 使用采样技术选择代表性对象进行分析。这些技术定义了具有相似元数据且可能具有相似内容的对象组。这些组基于存储桶名称、前缀、存储类别、文件扩展名和上次修改日期等维度。然后，Macie 从每个组中选择一组具有代表性的样本，从 Amazon S3 中检索每个选定对象的最新版本，并分析每个选定对象以确定该对象是否包含敏感数据。分析完成后，Macie 会丢弃其对象副本。

采样策略优先考虑分布式分析。通常，它对您的 Amazon S3 数据资产使用广度优先的方法。每天，根据您的 Amazon S3 数据资产中所有可分类对象的总存储大小，从尽可能多的存储桶中选择一组具有代表性的 S3 对象。例如，如果 Macie 已经分析并在一个 S3 存储桶中的对象中发现了敏

感数据，但尚未分析另一个存储桶中的对象，则后一个存储桶的分析优先级更高。通过这种方法，您可以更快地深入了解 Amazon S3 数据的敏感度。根据您的数据资产的大小，分析结果可在为您的账户启用自动敏感数据发现后 48 小时内开始显示。

采样策略还优先分析不同类型的 S3 对象和最近创建或更改的对象。不能保证任何单个对象样本都是结论性的。因此，分析各种各样的对象可以更好地了解 S3 存储桶可能包含的敏感数据类型和数量。此外，对新的或最近更改的对象进行优先级排序有助于分析适应存储桶清单的变化。例如，如果对象是在先前的分析之后创建或更改的，则这些对象在后续分析中的优先级更高。相反，如果之前分析过某个对象，并且自那次分析以来没有发生变化，那么 Macie 就不会再次分析该对象。此方法可帮助您为单个 S3 存储桶建立敏感度基准。然后，随着对您的账户进行持续的增量分析，您对各个存储桶的敏感度评测可以以可预测的速度变得越来越深入和详细。

定义分析范围

默认情况下，Macie 在评测您的清单数据并选择要分析的 S3 对象时会包含针对您的账户监控和分析的所有 S3 存储桶。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的存储桶。

您可以将特定的 S3 存储桶排除在分析之外。例如，您或许想排除通常存储 AWS 日志数据的存储桶，例如 AWS CloudTrail 事件日志。要排除存储桶，您可以更改账户或存储桶的自动敏感数据发现设置。如果您这样做，当下一个每日评测和分析周期开始时，Macie 就会开始排除存储桶。您可以从分析中排除多达 1,000 个存储桶。

如果您排除了某个存储桶，可以随后再次将其包括在内。要排除存储桶，您可以再次更改账户或存储桶的自动敏感数据发现设置。然后当下一个每日评测和分析周期开始时，Macie 就会开始将此存储桶包括在内。

确定要检测和报告哪些类型的敏感数据

默认情况下，Macie 使用我们为自动敏感数据发现推荐的一组托管数据标识符来检查 S3 对象。有关这些托管数据标识符的列表，请参阅 自动敏感数据发现的默认设置。

您可以定制分析，将重点放在特定类型的敏感数据上。为此，您可以选择以下任一方式更改账户的自动敏感数据发现设置。

- 添加或删除特定托管数据标识符 – 托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如特定国家或地区的信用卡号码、AWS 秘密访问密钥或护照号码。有关更多信息，请参阅使用托管数据标识符。
- 添加或随后删除自定义数据标识符 – 自定义数据标识符是您定义来检测敏感数据的一组标准。使用自定义数据标识符，您可以检测反映组织特定场景、知识产权或专有数据（例如员工 ID、客户账号或内部数据分类）的敏感数据。有关更多信息，请参阅构建自定义数据标识符。

- 添加或随后删除允许列表 – 在 Macie，允许列表指定您希望 Macie 忽略的 S3 对象中的文本或文本模式，通常是您的特定场景或环境的敏感数据异常，例如，您组织的公开名称或电话号码，或者您的组织用于测试的示例数据。有关更多信息，请参阅使用允许列表定义敏感数据例外。

如果您更改设置，Macie 会在下一个每日分析周期开始时应用您的更改。

您还可以调整存储桶级的设置，以确定存储桶敏感度评测中是否包含特定类型的敏感数据。要了解如何操作，请参阅管理单个 S3 存储桶的自动敏感数据发现。

计算敏感度分数

默认情况下，Macie 对为您的账户监控和分析的每个 S3 存储桶自动计算敏感度分数。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的存储桶。

在 Macie 中，敏感度分数是衡量两个主要维度交叉点的定量指标：Macie 在存储桶中发现的敏感数据量和 Macie 在存储桶中分析的数据量。存储桶的敏感度分数决定了 Macie 为存储桶分配哪个敏感度标签。敏感度标签是存储桶敏感度分数的定性表示，例如敏感、不敏感和尚未分析。有关 Macie 定义的灵敏度分数范围和标签的详细信息，请参阅 S3 存储桶的敏感度评分。

> **Important**
>
> S3 存储桶的敏感度分数和标签并不暗示或以其他方式表明该存储桶或存储桶的对象可能对您的组织具有的严重程度或重要性。相反，它们旨在提供参考点，帮助您识别和监控潜在的安全风险。

当您最初为账户启用自动敏感数据发现时，Macie 会自动为每个 S3 存储桶分配 50 的敏感度分数和尚未分析标签。唯一的例外是空桶。空存储桶是指不包含任何对象或存储桶的所有对象都包含零 (0) 字节数据的存储桶。如果存储桶是这种情况，Macie 会为该存储桶分配 1 分，然后为该存储桶分配不敏感标签。

随着账户自动发现的进展，Macie 会更新敏感度分数和标签以反映分析结果。例如：

- 如果 Macie 在对象中找不到敏感数据，Macie 会降低存储桶的敏感度分数，并在必要时更新存储桶敏感度标签。
- 如果 Macie 在对象中找到敏感数据，Macie 会增加存储桶的敏感度分数，并在必要时更新存储桶敏感度标签。
- 如果 Macie 在随后更改的对象中发现敏感数据，Macie 会从存储桶的敏感度分数中删除该对象的敏感数据检测，并根据需要更新存储桶的敏感度标签。

- 如果 Macie 在随后删除的对象中发现敏感数据，Macie 会从存储桶的敏感度分数中删除该对象的敏感数据检测，并根据需要更新存储桶的敏感度标签。

您可以通过在存储桶的分数中包含或排除特定类型的敏感数据来调整单个 S3 存储桶的敏感度评分设置。您还可以通过手动为存储桶分配最高分数 (100) 来覆盖该存储桶的计算得分。如果您分配了最高分数，则该存储桶将被标记为敏感。有关更多信息，请参阅管理单个 S3 存储桶的自动发现。

生成元数据、统计数据和结果

为您的账户启用自动敏感数据发现后，Macie 会自动生成和保留有关其监控和分析的、关于您账户的 S3 存储桶的其他清单数据、统计数据和其他信息。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的存储桶。

此额外信息会采集 Macie 迄今为止为您的账户进行的自动敏感数据发现活动的结果。它还会补充 Macie 提供的、有关您的 Amazon S3 数据的其他信息，例如各个存储桶的公开访问和共享访问设置。其他信息包括：

- 整合的数据敏感度统计数据，例如 Macie 在其中发现敏感数据的存储桶总数，以及其中可公开访问的存储桶数量。
- 交互式直观显示了整个 Amazon S3 数据资产的数据敏感度。
- 存储桶级别的详细信息，用于指示分析的当前状态，例如 Macie 在存储桶中分析的对象的列表、Macie 在存储桶中发现的敏感数据的类型以及 Macie 发现的每种敏感数据的出现次数。

有关更多信息，请参阅查看自动敏感数据发现统计数据和结果。

其他信息还包括统计数据和详细信息，可帮助您评测和监控 Amazon S3 数据的覆盖范围。您可以查看整个数据资产以及存储桶清单中各个 S3 存储桶的分析状态。您还可以找出阻碍 Macie 分析特定存储桶中对象的问题。如果您修复了这些问题，则可以在后续分析周期中扩大 Amazon S3 数据的覆盖范围。有关更多信息，请参阅评测自动敏感数据发现覆盖率。

Macie 会自动重新计算和更新这些信息，同时自动发现账户敏感数据。例如，如果 Macie 在随后更改或删除的对象中发现敏感数据，Macie 会更新相应存储桶的元数据：从分析对象列表中删除该对象；移除 Macie 在对象中发现的敏感数据出现次数；如果分数是自动计算的，则重新计算敏感度分数；并根据需要更新敏感度标签以反映新的分数。

除了元数据和统计数据外，Macie 会提供有关其发现的敏感数据及其执行的分析的详细报告：敏感数据调查发现，用于报告 Macie 在单个 S3 对象中发现的敏感数据，以及敏感数据发现结果（记录有关单个 S3 对象分析的详细信息）。

注意事项

在使用 Amazon Macie 对您的 Amazon S3 数据执行自动敏感数据发现时，请记住以下几点：

- 您的自动发现设置仅适用于当前 AWS 区域 设置。因此，生成的分析和数据仅适用于当前区域中的 S3 存储桶和对象。要在其他区域执行自动发现并访问生成的数据，请在每个其他区域启用和配置自动发现。
- 如果您是某个组织的 Macie 管理员：
  - 只有在当前区域为成员账户启用 Macie 后，您才能为该账户执行自动发现。成员账户无法为自己的账户执行自动发现。
  - 成员账户无法访问适用于其 S3 存储桶的自动发现设置。只有 Macie 管理员可以访问这些设置。
  - 成员账户无法访问 Macie 直接为其 S3 存储桶提供的敏感数据发现统计数据和其他结果。例如，成员账户无法使用 Amazon Macie 控制台查看其 S3 存储桶的敏感度分数。只有 Macie 管理员可以访问这些数据。
- 如果 S3 存储桶的权限设置阻止 Macie 检索有关该存储桶或存储桶对象的信息或访问该存储桶或存储桶的对象，则 Macie 无法对该存储桶执行自动发现。Macie 只能提供有关存储桶的部分信息，例如拥有该存储桶的 AWS 账户 账户 ID、存储桶的名称，以及 Macie 最近在每日刷新周期中检索存储桶和对象元数据的时间。在您的存储桶清单中，这些存储桶的敏感度分数为 50，其敏感度标签为尚未分析。

  要快速识别出现这种情况的 S3 存储桶，请参阅您的自动发现覆盖数据。有关更多信息，请参阅评测自动敏感数据发现覆盖率。要调查特定存储桶的问题，请查看 Amazon S3 中该存储桶的策略和权限设置。例如，存储桶可能具有限制性的存储桶策略。有关更多信息，请参阅允许 Macie 访问 S3 存储桶和对象。
- 要获得选择和分析资格，S3 对象必须是可分类的。可分类对象使用支持的 Amazon S3 存储类，并且具有支持的文件或存储格式的文件扩展名。有关更多信息，请参阅支持的存储类别和格式。
- 如果 S3 对象已加密，则仅当使用 Macie 可以访问并允许使用的密钥对其进行加密时，Macie 才能对其进行分析。有关更多信息，请参阅分析加密 S3 对象。要确定加密设置阻止 Macie 分析存储桶中一个或多个对象的情况，请参阅您的自动发现覆盖数据。有关更多信息，请参阅评测自动敏感数据发现覆盖率。

为您的账户配置自动化敏感数据发现

通过自动化敏感数据发现，Amazon Macie 可以持续从您的 Amazon Simple Storage Service (Amazon S3) 存储桶中选择示例对象，并分析这些对象以确定它们是否包含敏感数据。如果您是组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶中的对象。随着分析的进行，Macie 会更新统计数

据、清单数据及其提供的有关您的 Amazon S3 数据的其他信息。Macie 还会记录其发现的敏感数据及其执行的分析。

要配置和使用自动化敏感数据发现，您的账户必须是独立的 Macie 账户或组织的 Macie 管理员账户。如果您拥有成员账户并希望对您的 S3 存储桶执行自动化发现，请联系您组织的 Macie 管理员。有关更多信息，请参阅 管理多个 账户。

主题

当您为账户启用、配置或禁用自动化敏感数据发现时，您的更改仅适用于当前 AWS 区域。要在其他区域进行相同的更改，请在每个其他区域中重复适用的步骤。

开始前的准备工作

在为账户配置自动化敏感数据发现之前，请确认您拥有所需的权限。此外，请确认您已为敏感数据发现结果配置了存储库。

要验证权限，请使用 AWS Identity and Access Management (IAM) 查看附加到您的 IAM 身份的 IAM policy。然后将这些策略中的信息与以下必须允许您执行的操作列表进行比较：

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`

第一个操作允许您访问您的 Amazon Macie 账户。第二个操作允许您更改您账户的自动化敏感数据发现配置设置。这包括启用和禁用配置。（可选）验证您是否也被允许执行 `macie2:GetAutomatedDiscoveryConfiguration` 操作。此操作允许您检索当前的配置设置和配置的当前状态。

除了验证您的权限外，还要验证您是否已配置存储库来存储敏感数据发现结果。敏感数据发现结果是记录有关 Macie 对 S3 对象执行的分析的详细信息的记录。在执行自动化敏感数据发现时，Macie 会为其分析的每个 S3 对象创建敏感数据发现结果。这包括 Macie 没有发现敏感数据、因而不会产生敏感数据调查发现的对象，以及 Macie 因错误或权限设置等问题而无法分析的对象。如果 Macie 确实在对象中找到了敏感数据，则敏感数据发现结果将包括来自相应调查发现的数据。它还包含其他信息。这些结果可为您提供分析记录，有助于数据隐私和保护审计或调查。

Macie 仅将您的敏感数据发现结果存储 90 天。要访问结果并对其进行长期存储和保留，请将 Macie 配置为将结果存储在 S3 存储桶中。存储桶可以用作所有敏感数据发现结果的最终长期存储库。

要验证您是否已为账户配置了此存储库，请在 Amazon Macie 控制台的导航窗格中选择发现结果。如果您更喜欢以编程方式执行此操作，请使用 Amazon Macie API 的 getClassorationExportConfiguration 操作。要了解如何配置此存储库，请参阅存储和保留敏感数据发现结果。

如果您已配置存储库，则当您的账户首次启用自动化敏感数据发现时，Macie 会在存储库中创建一个名为 automated-sensitive-data-discovery 的文件夹。此文件夹存储 Macie 在为您的账户执行自动化发现时创建的敏感数据发现结果。

为您的账户启用自动化敏感数据发现

当您为账户启用自动化敏感数据发现后，Amazon Macie 会开始评测您的 Amazon S3 清单，并在当前的 AWS 区域 中为您的账户执行其他自动化发现活动。根据您的 Amazon S3 数据资产的大小，敏感数据发现统计数据和其他结果可在为您的账户启用自动化发现后 48 小时内开始显示。

按照以下步骤使用 Amazon Macie 控制台为您的账户启用自动化敏感数据发现。要以编程方式启用自动化发现，请使用 Amazon Macie API 的 updateAutomatedDiscoveryConfiguration 操作。

启用账户的自动化敏感数据发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要启用敏感数据自动化发现的区域。
3. 在导航窗格的设置下，选择自动化发现。
4. 在状态部分，选择启用。
5. 当系统提示进行确认时，选择启用 。

启用自动化敏感数据发现后，请查看和配置您的设置，以完善 Macie 随后执行的分析。

为您的账户配置自动化敏感数据发现设置

如果您的账户启用了自动化敏感数据发现，则可以调整您账户的自动化发现设置，以完善 Amazon Macie 执行的分析。这些设置指定了要在分析中包含的哪些 S3 存储桶。它们还指定了您希望 Macie 检测和报告的敏感数据的类型和产生，包括托管数据标识符、自定义数据标识符以及分析 S3 对象时使用的允许列表。

默认情况下，Macie 对您的账户会为其监控和分析的所有 S3 存储桶执行自动化感数据发现敏。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。您可以将特定的存储桶排除在分析之外。例如，您可以排除通常存储 AWS 日志数据的存储桶，例如 AWS CloudTrail 事件日志。如果您排除了某个存储桶，可以随后再次将其包括在内。

此外，Macie 仅使用我们推荐用于自动化敏感数据发现的一组托管数据标识符来分析 S3 对象。Macie 不使用您定义的自定义数据标识符或允许列表。要自定义分析，您可以将 Macie 配置为使用特定的允许列表、自定义数据标识符和托管数据标识符。

以下各部分提供了有关每种设置类型的更多信息，并介绍了如何使用 Amazon Macie 控制台更改设置。选择一个部分以了解更多信息。要以编程方式查看或更改设置，您可以使用 Amazon Macie API 的以下操作：updateClassificationScope（指定要从分析中排除哪些 S3 存储桶）和 updateSensitivityInsectionTemplate（指定要使用的允许列表、自定义数据标识符和托管数据标识符）。

如果您更改了设置，Macie 会在下一个评测和分析周期开始时应用您的更改，以便自动化敏感数据发现，通常在 24 小时内。

在分析中排除或包含 S3 存储桶

默认情况下，Macie 对您的账户会为其监控和分析的所有 S3 存储桶执行自动化感数据发现敏。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。要缩小范围，您可以从分析中排除多达 1,000 个存储桶。

如果您排除了 S3 存储桶，则 Macie 会在对您的账户执行自动化敏感数据发现时停止分析该存储桶中的对象。存储桶的现有敏感数据发现统计数据和详细信息将保留——例如，存储桶的当前灵敏度评分保持不变。排除某个存储桶后，您可以随后再次将其包括在内。

排除或包含特定的 S3 存储桶

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要在自动化发现分析中排除或包含特定 S3 存储桶的区域。
3. 在导航窗格的设置下，选择自动化发现。将出现自动化敏感数据发现页面，并显示您的当前设置。在该页面上，S3 存储桶部分列出了当前被排除的 S3 存储桶，或者显示当前包含的所有存储桶。
4. 在 S3 存储桶部分中，选择 编辑。
5. 请执行下列操作之一：

- 要排除一个或多个 S3 存储桶，请选择 将存储桶添加到排除列表。然后，在 S3 存储桶表中，选中要排除的每个存储桶对应的复选框。下表列出了您的账户在当前区域中的所有 S3 存储桶。
- 要包含您之前排除的一个或多个 S3 存储桶，请选择 从排除列表中删除存储桶。然后，在 S3 存储桶表中，选中要包含的每个存储桶对应的复选框。该表列出了当前被排除在自动化敏感数据发现之外的所有存储桶。

要更轻松地查找特定存储桶，请在表格上方的搜索框中输入搜索条件。您还可以按存储桶名称对表进行排序。

6. 选择完存储桶后，根据您在上一步中选择的选项，选择添加或 移除。

在分析中添加或删除托管数据标识符

托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如信用卡号、AWS 秘密访问密钥或特定国家或地区的护照号码。默认情况下，Macie 使用我们为自动化敏感数据发现推荐的一组托管数据标识符来分析 S3 对象。要查看此集合中包含的标识符列表，请参阅 自动敏感数据发现的默认设置。

您可以定制分析以关注特定类型的敏感数据：为希望 Macie 检测和报告的敏感数据类型添加托管数据标识符，为不希望 Macie 检测和报告的敏感数据类型删除托管数据标识符。如果您删除某个托管数据标识符，则您的更改不会影响 S3 存储桶的现有敏感数据发现统计数据和详细信息。例如，如果您删除了用于检测AWS秘密访问密钥的托管数据标识符，而 Macie 之前在存储桶中检测到该类型的敏感数据，则 Macie 会继续报告该存储桶的这些检测结果。

> **Tip**
>
> 您可以从特定存储桶的灵敏度评分中排除该类型的检测，而不是从所有 S3 存储桶的后续分析中删除托管数据标识符。有关更多信息，请参阅 管理单个 S3 存储桶的自动敏感数据发现。

要添加或删除托管数据标识符

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要从自动化发现分析中添加或删除受管数据标识符的区域。
3. 在导航窗格的设置下，选择自动化发现。在自动化敏感数据发现页面上，托管数据标识符部分显示您当前的设置，分为两个选项卡：

- 已添加到默认设置 – 此选项卡列出了您明确添加的托管数据标识符。除了默认设置中的且您尚未明确删除的标识符外，Macie 还使用这些托管数据标识符。
- 已从默认设置中删除 – 此选项卡列出了您明确删除的托管数据标识符。Macie 不使用这些托管数据标识符。

4. 在托管数据标识符部分中，选择 编辑。
5. 执行以下任一操作：

   - 要添加一个或多个托管数据标识符，请选择已添加到默认设置选项卡。然后，在表中选中要添加的每个托管数据标识符对应的复选框。如果已选中某个复选框，则表示已添加该标识符。
   - 要删除一个或多个托管数据标识符，请选择从默认设置中移除选项卡。然后，在表中选中要删除的每个托管数据标识符对应的复选框。如果已选中某个复选框，则表示已删除该标识符。

   在每个选项卡上，该表显示了 Macie 当前提供的所有托管数据标识符的列表。在该表中，每个托管数据标识符的 ID 描述了该标识符旨在检测的敏感数据的类型——例如，用于检测美国护照号码的 USA_PASSPORT_NUMBER。要更轻松地查找特定的托管数据标识符，请在表格上方的搜索框中输入搜索条件。您还可以通过选择列标题对表格进行排序。有关每个标识符的详细信息，请参阅 使用托管数据标识符。
6. 完成后，选择 Save (保存)。

在分析中添加或删除自定义数据标识符

自定义数据标识符是您为检测敏感数据定义的一组标准。标准由定义要匹配的文本模式的正则表达式（regex）和可选的字符序列以及优化结果的邻近规则组成。要了解更多信息，请参阅 构建自定义数据标识符。

默认情况下，Amazon Macie 在执行自动化敏感数据发现时不使用自定义数据标识符。如果您希望 Macie 使用特定的自定义数据标识符，可以将其添加到分析中。然后，除了您配置 Macie 使用的任何托管数据标识符之外，Macie 还使用自定义数据标识符。

如果您在分析中添加了自定义数据标识符，则可以随后将其删除。您的更改不会影响 S3 存储桶的现有敏感数据发现统计数据和详细信息。例如，如果您删除了之前为某个存储桶生成检测结果的自定义数据标识符，Macie 将继续报告该存储桶的这些检测结果。但是，请考虑将该类型的检测从特定存储桶的灵敏度评分中排除，而不是从随后对所有存储桶的分析中删除该标识符。有关更多信息，请参阅 管理单个 S3 存储桶的自动敏感数据发现。

要添加或删除自定义数据标识符

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要从自动化发现分析中添加或删除自定义数据标识符的区域。
3. 在导航窗格的设置下，选择自动化发现。将出现自动化敏感数据发现页面，并显示您的当前设置。在该页面上，自定义数据标识符部分列出了您添加的自定义数据标识符，或者显示您尚未选择任何自定义数据标识符用于自动化发现。
4. 在 自定义数据标识符部分中，选择 编辑。
5. 执行以下任一操作：

   - 要添加一个或多个自定义数据标识符，请选中要添加的每个自定义数据标识符对应的复选框。如果已选中某个复选框，则表示已添加该标识符。
   - 要删除一个或多个自定义数据标识符，请清除要删除的每个自定义数据标识符对应的复选框。如果已清除某个复选框，则 Macie 当前在执行自动化发现时不使用该标识符。

   > **Tip**
   >
   > 要在添加或删除自定义数据标识符之前查看或测试其设置，请选择该标识符名称旁边的链接图标
   > ( )。Macie
   > 会打开一个显示标识符设置的页面。
   > 您还可以使用此页面通过示例数据测试标识符。为此，请在示例数据框中输入最多包含 1,000 个字符的文本，然后选择测试。Macie 使用标识符评测示例数据，然后报告匹配项的数量。

6. 完成后，选择 Save (保存)。

在分析中添加或删除允许列表

在 Amazon Macie 中，允许列表定义了您希望 Macie 在检查 S3 对象中是否存在敏感数据时忽略的特定文本或文本模式。如果文本与允许列表中的条目或模式相匹配，则即使该文本与托管数据标识符或自定义数据标识符的条件匹配，Macie 也不会报告该文本。要了解更多信息，请参阅 使用允许列表定义敏感数据例外。

默认情况下，Macie 在执行自动化敏感数据发现时不使用允许列表。如果您希望 Macie 使用特定的允许列表，可以将其添加到分析中。如果您在分析中添加允许列表，则可以随后将其删除。

要添加或删除允许列表

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要从自动化发现分析中添加或删除允许列表的区域。
3. 在导航窗格的设置下，选择自动化发现。将出现自动化敏感数据发现页面，并显示您的当前设置。在该页面上，允许列表部分会显示您添加了哪些允许列表，或者显示您尚未选择任何允许列表用于自动化发现。
4. 在允许列表部分中选择 编辑。
5. 执行以下任一操作：

   - 要添加一个或多个允许列表，请选中要添加的每个允许列表对应的复选框。如果已选中某个复选框，则表示已添加该列表。
   - 要删除一个或多个允许列表，请清除要删除的每个允许列表对应的复选框。如果某个复选框已被清除，则 Macie 当前在执行自动化发现时不会使用该列表。

   > **Tip**
   >
   > 要在添加或删除允许列表之前查看其设置，请选择列表名称旁边的链接图标 ( )。Macie 会打开一个显示列表设置的页面。

6. 完成后，选择 Save (保存)。

禁用账户的自动化敏感数据发现

您可以随时禁用账户的自动化敏感数据发现。如果您禁用自动化敏感数据发现，Macie 将在下一个评测和分析周期开始之前（通常在 24 小时内）停止为您的账户执行所有自动化发现活动。此外，您无法访问 Macie 在执行这些活动时生成和直接提供的所有统计数据、清单数据和其他信息。例如，您的 S3 存储桶清单不再包含灵敏度评分和可视化，也不再分析单个 S3 存储桶的统计数据和详细信息。

您可以继续访问 Macie 在为您的账户执行自动化发现时生成的敏感数据调查发现。Macie 会将您的调查发现存储 90 天。此外，您存储或发布给其他 AWS 服务 的数据保持不变且不受影响，例如 Amazon S3 中的敏感数据发现结果和 Amazon EventBridge 中的调查发现事件。

如果您禁用账户的自动化敏感数据发现，则可以再次启用它。然后 Macie 会恢复您账户的所有自动化发现活动。如果您在 30 天内重新启用，则可以重新访问 Macie 之前在执行这些活动时生成并直接提供的所有统计数据、清单数据和其他信息。如果您未在 30 天内重新启用，Macie 会永久删除之前生成并直接提供的统计数据和其他信息。

按照以下步骤使用 Amazon Macie 控制台，为您的账户禁用自动化敏感数据发现。要以编程方式禁用自动化发现，请使用 Amazon Macie API的 updateAutomatedDiscoveryConfiguration 操作。

要禁用账户的自动化敏感数据发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要禁用自动化敏感数据发现的区域。
3. 在导航窗格的设置下，选择自动化发现。
4. 在 状态部分中选择 禁用。
5. 当系统提示确认时，选择 Disable（禁用）。

管理单个 S3 存储桶的自动敏感数据发现

在查看和评测自动敏感数据发现的统计数据和结果时，您可以调整各个 Amazon Simple Storage Service (Amazon S3) 存储桶的敏感度评分和其他设置。通过调整这些设置，您可以微调对整个 Amazon S3 数据资产及其中的特定存储桶的敏感度评测。您还可以捕获对特定存储桶执行的调查的结果。

您可以通过以下方式调整 S3 存储桶的自动敏感数据发现设置。

分配灵敏度分数

默认情况下，Amazon Macie 会自动计算存储桶的敏感度分数。该分数主要基于 Macie 在存储桶中发现的敏感数据量，以及 Macie 在存储桶中分析的数据量。有关更多信息，请参阅S3 存储桶的敏感度评分。

您可以覆盖存储桶的计算分数并手动分配最高分数 (100)，这也会将敏感标签应用于该存储桶。如果您这样做，Macie 将继续对存储桶执行自动发现。但是，随后的分析不会影响存储桶的分数。要再次自动计算分数，请再次更改设置。

在敏感度分数中排除或包括特定的敏感数据类型

如果自动计算，则存储桶的敏感度分数将部分基于 Macie 在存储桶中发现的敏感数据量。这主要源于 Macie 在存储桶中发现的敏感数据类型的性质和数量以及每种类型的出现次数。默认情况下，Macie 在计算存储桶的敏感度分数时会包含所有类型的敏感数据的出现次数。

您可以通过在存储桶的分数中排除或包含特定类型的敏感数据来调整计算方式。例如，如果 Macie 在存储桶中检测到邮寄地址，而您认为这是可以接受的，则可以将所有出现的邮件地址从存储桶的分数中排除。如果您排除某个敏感数据类型，Macie 将继续检查存储桶中是否有该类型的数据，并报告发现的事件。但是，这些事件不会影响存储桶的计算分数。要再次在计算存储中包含敏感数据类型，请再次更改设置。

在后续分析中排除或包含该存储桶

默认情况下，Macie 会自动发现针对您的账户监控和分析的所有 S3 存储桶。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。您可以将特定的存储桶排除在分析之外。例如，您可以排除通常存储 AWS 日志数据的存储桶，例如 AWS CloudTrail 事件日志。

如果您排除某个存储桶，则该存储桶的现有敏感数据发现统计数据和详细信息将保持不变，例如，该存储桶的当前敏感度分数保持不变。但是，当 Macie 对您的账户执行自动发现时，它会停止分析存储桶中的对象。排除某个存储桶后，您可以随后再次将其包括在内。

如果您更改了影响 S3 存储桶敏感度分数的设置，Macie 会立即开始重新计算和更新相关的敏感数据发现统计数据以及它提供的有关您的 Amazon S3 数据的其他信息。例如，如果您为存储桶分配最高分数，Macie 会增加账户汇总统计数据中敏感存储桶的数量。

按照以下步骤使用 Amazon Macie 控制台更改设置。要以编程方式更改设置，您可以使用 Amazon Macie API 的以下操作：UpdateResourceProfile，为存储桶分配敏感度分数；UpdateResourceProfileDetections，在存储桶的分数中排除或随后包含敏感数据类型；UpdateClassificationScope 用于在后续分析中排除或包含存储桶。

更改 S3 存储桶的自动敏感数据发现设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 S3 存储桶。
3. 在 S3 存储桶页面上，选择要更改其设置的 S3 存储桶。您可以使用表格视图
   ()
   或交互式地图
   ()
   来选择存储桶。
4. 在详细信息面板中，执行以下任一操作：

- 要覆盖计算得出的分数并手动将敏感度分数分配给存储桶，请打开 分配最高分数( )。
  这会将存储桶的分数更改为 100，并将 敏感标签应用于该存储桶。

  要指定 Macie 自动计算的分数，请关闭 分配最高分数( )。
- 要将存储桶排除在后续分析之外，请开启从自动发现中排除( )。

  如果您之前将存储桶排除在分析之外，请关闭从自动发现中排除( )以再次将其包括在内。
- 要在存储桶的敏感度分数中排除或包括出现的特定类型的敏感数据，请选择 敏感度选项卡。在检测表中，选中要排除或包含的敏感数据类型的复选框。然后，在 操作菜单上，选择 从分数中排除以排除该类型，或者选择 包含在分数中 以包含该类型。

  在表中，敏感数据类型字段指定了检测到数据的托管数据标识符的唯一标识符 (ID)，或检测到数据的自定义数据标识符的名称。托管数据标识符的 ID 描述了该标识符旨在检测的敏感数据类型，例如，用于检测美国护照号码的 USA_PASSPORT_NUMBER。有关每个托管数据标识符的详细信息，请参阅 使用托管数据标识符。

如果您更改了影响 S3 存储桶敏感度分数的设置，Macie 会立即开始重新计算和更新相关的敏感数据发现统计数据以及有关 S3 存储桶的其他信息。

评测自动敏感数据发现覆盖率

随着自动发现您账户敏感数据的进展，Amazon Macie 会提供统计数据和详细信息，以帮助您评测和监控其对 Amazon Simple Storage Service (Amazon S3) 数据资产的覆盖率。利用这些数据，您可以检查您的整个数据资产以及存储桶清单中各个 S3 存储桶的自动敏感数据发现状态。您还可以找出阻碍 Macie 分析特定存储桶中对象的问题。如果您修复了这些问题，则可以在后续分析周期中扩大 Amazon S3 数据的覆盖范围。

覆盖率数据提供了对当前 AWS 区域 中 S3 存储桶中自动敏感数据发现的当前状态的快照。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。对于每个存储桶，数据表明 Macie 尝试分析存储桶中的对象时是否出现问题。如果出现问题，则数据会显示每个问题的性质，在某些情况下，还会显示出现的次数。数据会随着您账户每天自动敏感数据发现的进展而更新。如果 Macie 在

每日分析周期内分析或尝试分析存储桶中的一个或多个对象，Macie 会更新覆盖率和其他数据以反映结果。

对于某些类型的问题，您可以查看所有 S3 存储桶的汇总数据，也可以选择深入了解有关每个存储桶的更多详细信息。例如，覆盖率数据可以帮助您快速识别 Macie 不允许您账户访问的所有存储桶。覆盖率数据还会报告发生的对象级问题。这些问题被称为分类错误，使 Macie 无法分析存储桶中的特定对象。例如，您可以确定 Macie 无法在存储桶中分析多少对象，因为这些对象是使用不再可用的 AWS Key Management Service (AWS KMS) 密钥加密的。

如果您使用 Amazon Macie 控制台查看覆盖率数据，则您的数据视图包括修复每类问题的指南。本节的后续主题还为每种类型提供了补救指导。

主题

查看自动敏感数据发现覆盖率数据

要查看和评测您账户的自动敏感数据发现覆盖率，您可以使用 Amazon Macie 控制台或 Amazon Macie API。控制台和 API 都提供了数据，这些数据可显示在当前 AWS 区域 中对您的 Amazon Simple Storage Service (Amazon S3) 存储桶进行的分析的当前状态。这些数据包括有关在分析中造成差距的问题的信息：

- 不允许 Macie 访问的 S3 存储桶。Macie 无法分析这些存储桶中的任何对象，因为存储桶的权限设置会阻止 Macie 访问存储桶和存储桶的对象。
- 不存储任何可分类对象的 S3 存储桶。Macie 无法分析这些存储桶中的任何对象，因为所有对象都使用了 Macie 不支持的 Amazon S3 存储类别，或者它们有 Macie 不支持的文件或存储格式的文件扩展名。
- 由于对象级分类错误，Macie 尚未能够分析的 S3 存储桶。Macie 试图分析这些存储桶中的一个或多个对象。但是，由于对象级权限设置、对象内容或配额存在问题，Macie 无法分析对象。

覆盖率数据会随着您账户每天自动敏感数据发现的进展而更新。如果您是一个组织的 Macie 管理员，则这些数据将包含您的成员账户拥有的 S3 存储桶的信息。

> **Note**
>
> 覆盖率数据并未明确包含您创建和运行的敏感数据发现任务的结果。但是，修复影响自动敏感数据发现结果的覆盖范围问题也可能增加您随后运行的敏感数据发现任务的覆盖率。要评测某项工作的覆盖率，请查看该职位的统计数据和结果。如果作业的日志事件或其他结果表明存在覆盖率问题，则本节后面的补救指南可以帮助您解决其中一些问题。

查看自动敏感数据发现覆盖率数据

您可以使用 Amazon Macie 控制台或 Amazon Macie API 来查看您的账户或组织的覆盖率数据。在控制台上，单个页面提供了所有 S3 存储桶的覆盖率数据的统一视图，包括每个存储桶最近发生的问题的汇总。该页面还提供了按问题类型查看数据组的选项。要跟踪您对特定存储桶问题的调查，您可以将页面中的数据导出到逗号分隔值 (CSV) 文件中。

Console

按照以下步骤使用 Amazon Macie 控制台查看自动敏感数据发现覆盖率数据。

查看覆盖率数据

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择资源覆盖率。
3. 在资源覆盖率页面上，选择要查看的覆盖率数据类型的选项卡：

   - 全部 – 列出 Macie 监控和分析您账户的全部 S3 存储桶。

     对于每个存储桶，问题字段会显示是否存在问题阻止 Macie 分析存储桶中的对象。如果此字段的值为无，则表示 Macie 已经分析了存储桶的至少一个对象，或者 Macie 尚未尝试分析该存储桶的任何对象。如果存在问题，则此字段会显示问题的性质以及如何修复问题。对于对象级分类错误，它还可以（在括号中）显示错误的出现次数。
   - 访问被拒绝-列出不允许 Macie 访问的 S3 存储桶。这些存储桶的权限设置会阻止 Macie 访问存储桶和存储桶的对象。因此，Macie 无法分析这些存储桶中的任何对象。
   - 分类错误 – 列出 Macie 由于对象级分类错误（对象级权限设置、对象内容或配额存在问题）而尚未分析的 S3 存储桶。

对于每个存储桶，问题字段会显示所发生的每种类型的错误的性质，这些错误阻止 Macie 分析存储桶中的对象。它还显示如何修复每种类型的错误。根据错误的不同，它还可以（在括号中）显示错误的出现次数。

- 不可分类 - 列出 Macie 无法分析的 S3 存储桶，因为它们不存储任何可分类的对象。这些存储桶中的所有对象都使用不支持的 Amazon S3 存储类别，或者对不支持的文件或存储格式具有文件扩展名。因此，Macie 无法分析这些存储桶中的任何对象。

4. 要深入查看某个 S3 存储桶的支持数据，请选择该存储桶的名称。然后，请参阅存储桶详细信息面板，了解有关该存储桶的统计数据和其他信息。
5. 要将表格导出为 CSV 文件，请选择页面顶部的导出到 CSV。生成的 CSV 文件包含表中每个 S3 存储桶的元数据子集，最多 50,000 个存储桶。该文件包含覆盖率问题字段。此字段的值表明问题是否阻止 Macie 分析存储桶中的对象，如果是，则指示问题的性质。

API

要以编程方式查看覆盖率数据，请在使用 Amazon Macie API 的 DescribeBuckets 操作提交的查询中指定筛选条件。此操作返回对象数组。每个对象都包含与筛选条件相匹配的 S3 存储桶的统计数据和其他信息。

在筛选条件中，包括要查看的覆盖率数据类型的条件：

- 要识别由于存储桶的权限设置而不允许 Macie 访问的存储桶，请包括 `errorCode` 字段值等于 `ACCESS_DENIED` 的条件。
- 要识别允许 Macie 访问但尚未分析的存储桶，请包括 `sensitivityScore` 字段值等于 `50` 且 `errorCode` 字段值不等于 `ACCESS_DENIED` 的条件。
- 要识别因所有存储分区对象都使用不支持的存储类或格式而导致 Macie 无法分析的存储桶，请包括 `classifiableSizeInBytes` 字段值等于 `0` 且 `sizeInBytes` 字段值大于 `0` 的条件。
- 要识别 Macie 已经分析了至少一个对象的存储桶，请包括 `sensitivityScore` 字段值在 1—99 范围内但不等于 `50` 的条件。要同时包括您手动分配最高分数的存储桶，范围应为 1—100。
- 要识别 Macie 由于对象级分类错误而尚未分析的存储桶，请包括 `sensitivityScore` 字段值等于 `-1` 的条件。然后，要查看特定存储桶发生的错误类型和数量的明细，请使用 GetResourceProfile 操作。

如果您使用的是 AWS Command Line Interface(AWS CLI)，请通过运行 describe-buckets 命令在您提交的查询中指定筛选条件。要查看特定 S3 存储桶发生的错误类型和数量的明细（如果有），请运行 get-resource-profile 命令。

例如，以下 AWS CLI 命令使用筛选条件来检索 Macie 由于存储桶的权限设置而无法访问的所有 S3 存储桶的详细信息。

此示例的格式适用于 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

此示例的格式适用于 Microsoft Windows：

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

如果请求成功，Macie 将返回一个 `buckets` 数组。该数组包含每个 S3 存储桶的对象，该对象位于当前 AWS 区域 中，并且符合筛选条件。

如果没有符合筛选条件的 S3 存储桶，Macie 将返回一个空 `buckets` 数组。

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

有关在查询中指定筛选条件的更多信息（包括常用条件的示例），请参阅 筛选您的 S3 存储桶清单。

修复自动敏感数据发现的覆盖率问题

Amazon Macie 报告了几种类型的问题，这些问题降低了 Amazon Simple Storage Service (Amazon S3) 数据的自动敏感数据发现的覆盖率。以下信息可帮助您调查和修复这些问题。

问题类型和详情

- 访问被拒绝
- 分类错误：内容无效
- 分类错误：加密无效
- 分类错误：KMS 密钥无效
- 分类错误：权限被拒绝
- 不可分类

> **Tip**
>
> 要调查 S3 存储桶的对象级分类错误，请先查看该存储桶的对象样本列表。此列表显示 Macie 在存储桶中分析或尝试分析哪些对象，最多可包含 100 个对象。
> 要查看 Amazon Macie 控制台上的列表，请在 S3 存储桶页面上选择存储桶，然后在存储桶详细信息面板中选择对象示例选项卡。要以编程方式查看清单，请使用 Amazon Macie API 的 listResourceProfileArtiFacts 操作。如果某个对象的分析状态为已跳过 (SKIPPED)，则可能是该对象导致了错误。

访问被拒绝

此问题表明 S3 存储桶的权限设置阻止 Macie 访问该存储桶和存储桶的对象。Macie 无法检索和分析存储桶内的任何对象。

详细信息

此类问题的最常见原因是限制性存储桶策略。存储桶策略是一种基于资源的 AWS Identity and Access Management (IAM) policy ，它指定主体（用户、账户、服务或其他实体）可以对 S3 存储桶执行哪些操作，以及主体可以在哪些条件下执行这些操作。限制性存储桶策略使用明确的 `Allow` 或 `Deny` 声明，根据特定条件授予或限制对存储桶数据的访问权限。例如，存储桶策略可能包含拒绝访问存储桶的 `Allow` 或 `Deny` 语句，除非使用特定的源 IP 地址访问存储桶。

如果 S3 存储桶的存储桶策略包含带有一个或多个条件的明确 `Deny` 声明，则可能不允许 Macie 检索和分析存储桶的对象以检测敏感数据。Macie 只能提供有关存储桶的部分信息，例如存储桶的名称和创建日期。

补救指南

要修复此问题，请更新 S3 存储桶的存储桶策略。确保该策略允许 Macie 访问存储桶和存储桶的对象。要允许此访问权限，请在策略中添加 Macie 服务相关角色 (`AWSServiceRoleForAmazonMacie`) 的条件。该条件应将 Macie 服务相关角色排除在与策略 `Deny` 限制的匹配范围之外。它可以通过使用 `aws:PrincipalArn` 全局条件上下文密钥和您账户的 Macie 服务相关角色的 Amazon 资源名称（ARN）实现这一点。

如果您更新存储桶策略且 Macie 获得了对 S3 存储桶的访问权限，Macie 将检测到更改。发生这种情况时，Macie 将更新统计数据、库存数据以及它提供的有关您的 Amazon S3 数据的其他信息。此外，在随后的分析周期中，存储桶的对象将具有更高的优先级进行分析。

其他参考资料

有关更新 S3 存储桶策略以允许 Macie 访问存储桶的更多信息，请参阅允许 Amazon Macie 访问 S3 存储桶和对象。有关使用存储桶策略控制存储桶访问权限的信息，请参阅 Amazon Simple Storage Service 用户指南中的存储桶策略和用户策略以及 Amazon S3 如何授权请求。

分类错误：内容无效

如果 Macie 尝试分析 S3 存储桶中的对象，但该对象格式不正确，或者该对象包含的内容超过敏感数据发现配额，则会发生此类分类错误。Macie 无法分析该对象。

详细信息

出现此错误的原因通常是因为 S3 对象是格式错误或损坏的文件。因此，Macie 无法解析和分析文件中的所有数据。

如果对 S3 对象的分析超过单个文件的敏感数据发现配额，也会发生此错误。例如，对象的存储大小超过了该类型文件的大小配额。

无论哪种情况，Macie 都无法完成对 S3 对象的分析，并且该对象的分析状态为已跳过 (SKIPPED)。

补救指南

要调查此错误，请下载 S3 对象并检查文件的格式和内容。此外，还要根据 Macie 配额评测文件内容，以发现敏感数据。

如果您不修复此错误，Macie 将尝试分析 S3 存储桶中的其他对象。如果 Macie 成功分析了另一个对象，Macie 将更新覆盖率数据以及它提供的有关该存储桶的其他信息。

其他参考资料

有关敏感数据发现配额的列表，包括某些类型的文件的配额，请参阅 Amazon Macie 限额。有关 Macie 如何更新敏感度分数以及它提供的有关 S3 存储桶的其他信息的信息，请参阅 自动敏感数据发现的工作原理。

分类错误：加密无效

如果 Macie 尝试分析 S3 存储桶中的对象，并且该对象使用客户提供的密钥进行加密，则会发生此类分类错误。该对象使用 SSE-C 加密，这意味着 Macie 无法检索和分析该对象。

详细信息

Amazon S3 支持多种 S3 对象的加密选项。对于其中的大多数选项，Macie 都可以使用您账户的 Macie 服务关联角色来解密对象。但是，这取决于其使用的加密类型。

要让 Macie 解密 S3 对象，必须使用 Macie 可以访问并允许使用的密钥对该对象进行加密。如果使用客户提供的密钥对对象进行加密，则 Macie 无法提供从 Amazon S3 检索该对象所需的密钥材料。因此，Macie 无法分析该对象，并且该对象的分析状态为已跳过 (SKIPPED)。

补救指南

要纠正此错误，请使用 Amazon S3 托管密钥或 AWS Key Management Service (AWS KMS) 密钥加密 S3 对象。如果您更喜欢使用 AWS KMS 密钥，则密钥可以是 AWS 托管 KMS 密钥或允许 Macie 使用的客户托管 KMS 密钥。

要使用 Macie 可以访问和使用的密钥加密现有 S3 对象，您可以更改对象的加密设置。要使用 Macie 可以访问和使用的密钥加密新对象，请更改 S3 存储桶的默认加密设置。还要确保存储桶的策略不要求使用客户提供的密钥对新对象进行加密。

如果您不修复此错误，Macie 将尝试分析 S3 存储桶中的其他对象。如果 Macie 成功分析了另一个对象，Macie 将更新覆盖率数据以及它提供的有关该存储桶的其他信息。

其他参考资料

有关使用 Macie 分析加密的 S3 对象的要求和选项的信息，请参阅使用 Amazon Macie 分析加密的 Amazon S3 对象。有关 S3 存储桶的加密选项和设置的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用加密保护数据和为 S3 存储桶设置默认服务器端加密行为。

分类错误：KMS 密钥无效

如果 Macie 尝试分析 S3 存储桶中的对象，并且该对象使用不再可用的 AWS Key Management Service (AWS KMS) 密钥加密，则会发生此类分类错误。Macie 无法检索和分析该对象。

详细信息

AWS KMS 提供了禁用和删除客户管理的 AWS KMS keys 的选项。如果 S3 对象使用已禁用、计划删除或已被删除的 KMS 密钥加密，Macie 将无法检索和解密该对象。因此，Macie 无法分析该对象，并且该对象的分析状态为已跳过 (SKIPPED)。为使 Macie 分析加密对象，必须使用 Macie 可以访问和使用的密钥对该对象进行加密。

补救指南

要纠正此错误，请根据密钥的当前状态重新启用或取消相应 AWS KMS key 的删除计划。如果适用的密钥已被删除，则无法纠正此错误。

要确定哪个 AWS KMS key 用于加密 S3 对象，您可以先使用 Macie 查看 S3 存储桶的服务器端加密设置。如果将存储桶的默认加密设置配置为使用 KMS 密钥，则存储桶的详细信息将表明使用的是哪个密钥。然后，您可以查看该密钥的状态。或者，您可以使用 Amazon S3 查看存储桶和存储桶中各个对象的加密设置。

如果您不修复此错误，Macie 将尝试分析 S3 存储桶中的其他对象。如果 Macie 成功分析了另一个对象，Macie 将更新覆盖率数据以及它提供的有关该存储桶的其他信息。

其他参考资料

有关使用 Macie 查看 S3 存储桶的服务器端加密设置的信息，请参阅 查看 S3 存储桶的详细信息。有关重新启用或取消按计划删除的信息AWS KMS key，请参阅 AWS Key Management Service 开发者指南中的启用和禁用密钥以及计划和取消密钥删除。

分类错误：权限被拒绝

如果 Macie 尝试分析 S3 存储桶中的对象，而 Macie 由于该对象的权限设置或用于加密该对象的密钥的权限设置而无法检索或解密该对象，则会发生此类分类错误。Macie 无法检索和分析该对象。

详细信息

之所以出现此错误，通常是因为 S3 对象使用不允许 Macie 使用的客户托管 AWS Key Management Service (AWS KMS) 密钥进行加密。如果使用客户管理的 AWS KMS key 加密对象，则密钥的策略必须允许 Macie 使用该密钥解密数据。

如果 Amazon S3 权限设置阻止 Macie 检索 S3 对象，也会发生此错误。S3 存储桶的存储桶策略可能会限制对特定存储桶对象的访问权限，或者仅允许某些主体（用户、账户、服务或其他实体）访问这些对象。或者，对象的访问控制列表（ACL）可能会限制对该对象的访问。因此，可能不允许 Macie 访问该对象。

对于上述任何情况，Macie 都无法检索和分析对象，并且该对象的分析状态为已跳过 (SKIPPED)。

补救指南

要纠正此错误，请确定 S3 对象是否使用客户托管的 AWS KMS key 进行加密。如果是，请确保密钥的策略允许 Macie 服务相关角色 (AWSServiceRoleForAmazonMacie) 使用密钥解密数据。您

如何允许此访问取决于拥有 AWS KMS key 的账户是否还拥有存储该对象的 S3 存储桶。如果同一个账户拥有 KMS 密钥和存储桶，则该账户的用户必须更新密钥策略。如果一个账户拥有 KMS 密钥而另一个账户拥有存储桶，则拥有密钥账户的用户必须允许跨账户存取密钥。

> **Tip**
>
> 您可以自动生成一份关于 Macie 需要访问的所有客户托管AWS KMS keys的列表，以分析您账户的 S3 存储桶中的对象。为此，请运行 AWS KMS 权限分析器脚本，该脚本可从 GitHub 的 Amazon Macie Scripts 存储库获取。该脚本还可以生成关于 AWS Command Line Interface (AWS CLI) 命令的附加脚本。您可以选择运行这些命令来更新指定 KMS 密钥的必要配置设置和策略。

如果已允许 Macie 使用适用的 AWS KMS key，或者 S3 对象未使用客户托管的 KMS 密钥加密，请确保存储桶的策略允许 Macie 访问该对象。还要验证对象的 ACL 是否允许 Macie 读取对象的数据和元数据。

对于存储桶策略，您可以通过向策略中添加 Macie 服务相关角色的条件来允许此访问权限。该条件应将 Macie 服务相关角色排除在与策略 `Deny` 限制的匹配范围之外。它可以通过使用 `aws:PrincipalArn` 全局条件上下文密钥和您账户的 Macie 服务相关角色的 Amazon 资源名称（ARN）实现这一点。

对于对象 ACL，您可以通过与对象所有者合作将您的 AWS 账户 添加为拥有对象 `READ` 权限的被授权者来允许此访问。然后 Macie 可以使用您账户的服务相关角色检索和分析该对象。还可以考虑更改存储桶的对象所有权设置。您可以使用这些设置为存储桶中的所有对象禁用 ACL，并向拥有该存储桶的账户授予所有权权限。

如果您不修复此错误，Macie 将尝试分析 S3 存储桶中的其他对象。如果 Macie 成功分析了另一个对象，Macie 将更新覆盖率数据以及它提供的有关该存储桶的其他信息。

其他参考资料

有关允许 Macie 在客户管理的 AWS KMS key 的情况下解密数据的更多信息，请参阅 允许 Amazon Macie 使用客户托管 AWS KMS key。有关更新 S3 存储桶策略以允许 Macie 访问存储桶的信息，请参阅 允许 Amazon Macie 访问 S3 存储桶和对象。

有关更新密钥政策的信息，请参阅 AWS Key Management Service 开发者指南中的更改密钥政策。有关使用客户托管 AWS KMS keys 加密 S3 对象的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用带有 AWS KMS 密钥的服务器端加密。

有关使用 S3 存储桶策略控制存储桶访问权限的信息，请参阅 Amazon Simple Storage Service 用户指南中的存储桶策略和用户策略以及 Amazon S3 如何授权请求。有关使用 ACL 或对象所有权设置来控制对 S3 对象的访问的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 ACL 管理访问权限和控制对象所有权以及为存储桶禁用 ACL。

不可分类

此问题表明 S3 存储桶中的所有对象均使用不支持的 Amazon S3 存储类或不支持的文件或存储格式进行存储。Macie 无法分析存储桶内的任何对象。

详细信息

要获得选择和分析资格，S3 对象必须使用 Macie 支持的 Amazon S3 存储类。该对象还必须具有 Macie 支持的文件或存储格式的文件扩展名。如果对象不符合这些标准，则该对象将被视为不可分类的对象。Macie 不会尝试检索或分析不可分类的对象中的数据。

如果 S3 存储桶中的所有对象都是不可分类的对象，则整个存储桶是不可分类的存储桶。Macie 无法对存储桶执行自动敏感数据发现。

补救指南

要解决此问题，请查看生命周期配置规则和其他设置，以确定哪些存储类用于在 S3 存储桶中存储对象。考虑调整这些设置以使用 Macie 支持的存储类别。您也可以更改存储桶中现有对象的存储类别。

还要评测 S3 存储桶中现有对象的文件和存储格式。要分析对象，可以考虑将数据临时或永久移植到使用支持格式的新对象。

如果将对象添加到 S3 存储桶中，并且它们使用支持的存储类和格式，则 Macie 将在下次评测您的存储桶清单时检测到这些对象。发生这种情况时，Macie 将停止报告该存储桶在统计数据、覆盖率数据以及它提供的有关您的 Amazon S3 数据的其他信息中不可分类的情况。此外，在随后的分析周期中，新对象将具有更高的分析优先级。

其他参考资料

有关 Amazon S3 存储类别以及 Macie 支持的文件和存储格式的信息，请参阅 Amazon Macie 支持的存储类别和格式。有关生命周期配置规则和 Amazon S3 提供的存储类选项的信息，请参阅 Amazon Simple Storage Service 用户指南中的管理存储生命周期和使用 Amazon S3 存储类别。

查看自动敏感数据发现统计数据和结果

为您的账户启用自动敏感数据调查发现后，Amazon Macie 会自动生成和保留有关其监控和分析的、关于您账户的 Amazon Simple Storage Service (Amazon S3) 存储桶的其他库存数据、统计数据和其他信息。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。

此额外信息会采集 Macie 迄今为止为您的账户进行的自动敏感数据发现活动的结果。它还会补充 Macie 提供的、有关您的 Amazon S3 数据的其他信息，例如各个 S3 存储桶的公开访问和加密设置。除了元数据和统计数据外，Macie 还会记录其发现的敏感数据及其执行的分析 — 敏感数据调查发现和敏感数据发现结果。

在自动敏感数据发现分析您账户的进度时，以下功能和数据可以帮助您查看和评测结果：

- 摘要控制面板 – 提供关于 Amazon S3 数据资产的汇总统计数据。统计数据包括关键指标数据，例如 Macie 在其中发现敏感数据的存储桶总数，以及其中可公开访问的存储桶数量。它们还包括有关影响数据资产覆盖范围问题的数据。
- S3 存储桶热图 – 提供跨数据资产（按 AWS 账户分组）数据敏感性的交互式可视化表示。每个账户的地图都包含汇总的灵敏度统计数据，并使用颜色来表示该账户拥有的每个存储桶的当前灵敏度分数。地图还使用符号帮助您识别可公开访问的存储桶、Macie 无法分析的存储桶等。
- S3 存储桶表 – 提供清单中每个 S3 存储桶的摘要信息。对于每个存储桶，该表都包含以下数据：存储桶名称和当前灵敏度得分；Macie 可分析的存储桶内对象数量；您是否已配置任何敏感数据发现作业，以定期分析存储桶对象。您可以选择将数据从表中导出至逗号分隔值 (CSV) 文件。
- 详细信息面板 – 为您在热图或表格中选择的 S3 存储桶提供详细信息和统计数据。详细信息包括 Macie 在存储桶中分析的对象列表，以及 Macie 在存储桶中发现的敏感数据的类型和出现次数的明细。您还可以使用该面板管理各个存储分区的自动发现设置。
- 敏感数据调查发现 - 提供 Macie 在单个 S3 对象中发现的敏感数据的详细报告。详细信息包括：Macie 发现敏感数据的时间；以及 Macie 发现的敏感数据类型和出现次数。详细信息还包括有关受影响的 S3 存储桶和对象的信息，其中包括存储桶的公共访问设置以及对象最近更改时间。
- 敏感数据发现结果-提供 Macie 对单个 S3 对象执行的分析记录。这包括 Macie 在 中没有发现敏感数据，因而不会产生敏感数据调查发现以及 Macie 因问题和错误而无法分析的对象。

您可通过这些数据，评测整个 Amazon S3 数据资产的数据灵敏度，并深入评测和调查各个 S3 存储桶和对象。将 Macie 提供的、关于 Amazon S3 数据的安全和隐私信息相结合，您还可识别可能需要立即修复的情况，例如，Macie 在其中发现敏感数据的可公开访问存储桶。

其他数据可帮助您评测和监控 Amazon S3 数据资产的覆盖范围。通过覆盖范围数据，您可以查看整个数据资产以及存储桶清单中各个 S3 存储桶的分析状态。您还可以找出阻碍 Macie 分析特定存储桶中对

象的问题。如果您修复了这些问题，则可以在后续分析周期中扩大 Amazon S3 数据的覆盖范围。有关更多信息，请参阅 评测自动敏感数据发现覆盖率。

主题

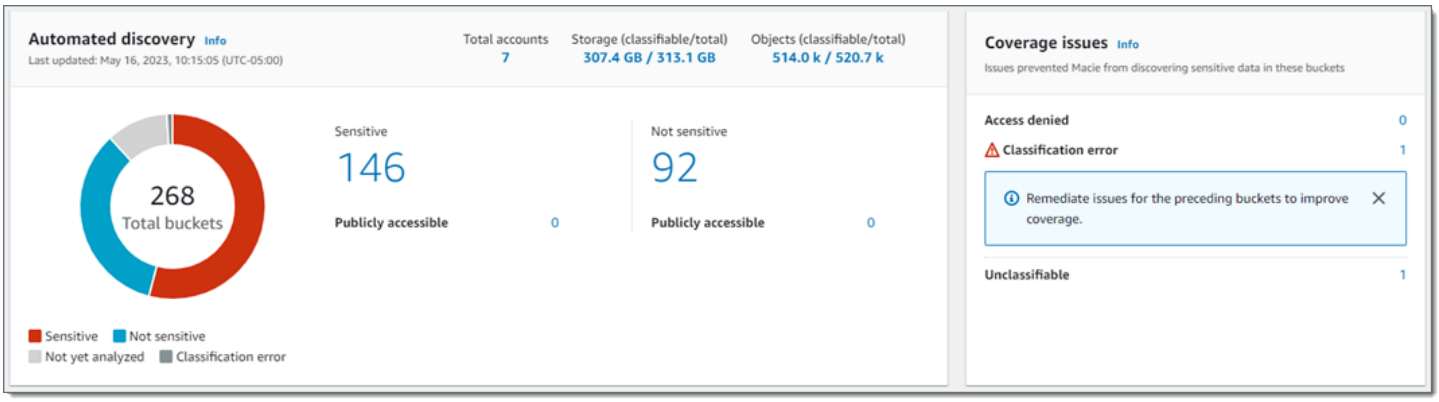
- 在摘要控制面板上查看数据灵敏度汇总统计数据
- 使用 S3 存储桶地图观察数据灵敏度
- 使用 S3 存储桶表评测数据灵敏度
- 查看各个 S3 存储桶的数据灵敏度详细信息
- 分析自动发现产生的敏感数据调查发现
- 访问自动发现产生的敏感数据调查发现

在摘要控制面板上查看数据灵敏度汇总统计数据

在 Amazon Macie 控制台，摘要控制面板提供了当前 AWS 区域的 Amazon Simple Storage Service (Amazon S3) 的统计数据和调查发现数据汇总快照。它旨在帮助评测 Amazon S3 数据的整体安全状况。

控制面板统计数据包括关键安全指标数据，例如可公开访问或与其他 AWS 账户共享的 S3 存储桶的数量。控制面板还会显示您账户的调查发现数据组汇总，例如，在过去七天内生成最多结果的 S3 存储桶。如果您是组织的 Macie 管理员，则控制面板会提供组织中所有账户的汇总统计结果和数据。您可选择按账户筛选数据。

如果您的账户启用了自动敏感数据发现，则 摘要 控制面板将包含自动敏感数据发现的统计信息。此数据采集 Macie 迄今为止为 Amazon S3 数据执行的、自动敏感数据发现活动的状态和结果。例如：



自动发现部分中的统计信息提供了自动敏感数据发现活动的当前状态和结果的快照。这些数据不包括您创建和运行的敏感数据发现任务的结果。

覆盖范围问题部分的统计信息表示阻止 Macie 分析单独 S3 存储桶对象的问题。这些统计数据并未明确包含您创建和运行的敏感数据发现任务的数据。但是，修复影响自动发现敏感数据结果的覆盖范围问题也可能增加您随后运行的作业的覆盖范围。

主题

显示“摘要”控制面板

按照以下步骤在 Amazon Macie 控制台上显示摘要 控制面板。如果您更喜欢以编程方式查询统计数据，则可以使用 Amazon Macie API 的GetBucketStatistics操作。

要显示“摘要”控制面板

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择摘要。Macie 会显示摘要控制面板。
3. 要在控制面板上深入查看某一项的支持数据，请选择该项。

如果您是组织的 Macie 管理员，则控制面板会显示组织中您的账户和成员账户的汇总统计结果和数据。要对控制面板应用筛选条件，以仅显示特定账户的数据，请在控制面板上方的账户框中输入账户 ID。

在摘要控制面板上了解自动敏感数据发现统计信息

Amazon Macie 控制台上的摘要控制面板包含统计信息汇总，可帮助您监控 Amazon S3 数据的自动敏感数据发现操作。例如，您可以使用控制面板统计信息快速确定 Amazon Macie 在其中发现敏感数据的 S3 存储桶数量，以及其中可公开访问的存储桶数量。控制面板提供您当前 AWS 区域的 Amazon S3 数据的状态和分析结果快照。

您还可以使用控制面板统计信息评测您的 Amazon S3 数据的覆盖范围，并找出阻碍 Macie 分析单个 S3 存储桶中对象的问题。例如，您可以确定账户中不允许 Macie 访问的存储桶数量。

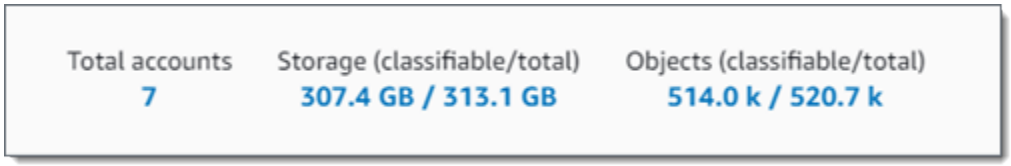
在控制面板上，自动敏感数据发现统计信息主要分为以下几个部分：

- 覆盖范围问题

每个部分的单独统计数据如下。有关 摘要控制面板其他部分中统计数据的信息，请参阅了解“摘要”控制面板的组件。

存储和敏感数据发现

在 自动发现部分的顶部，您将找到统计数据，这些统计数据表明您在 Amazon S3 中存储的数据数量，以及 Macie 可分析检测敏感数据的数据量。例如：



本节内容：

- 账户总数-您的 S3 存储桶清单中拥有的存储桶的总数。 AWS 账户 如果您是某组织的委托 Macie 管理员，这是您管理的您组织中 的 Macie 账户的总数。如果您有一个独立的 Macie 账户，则该值为 1。
- 存储
  - 可分类 – Macie 可在存储桶中分析的所有对象的总存储大小。
  - 总计 – 存储桶中所有对象的总存储大小，包括 Macie 无法分析的对象。

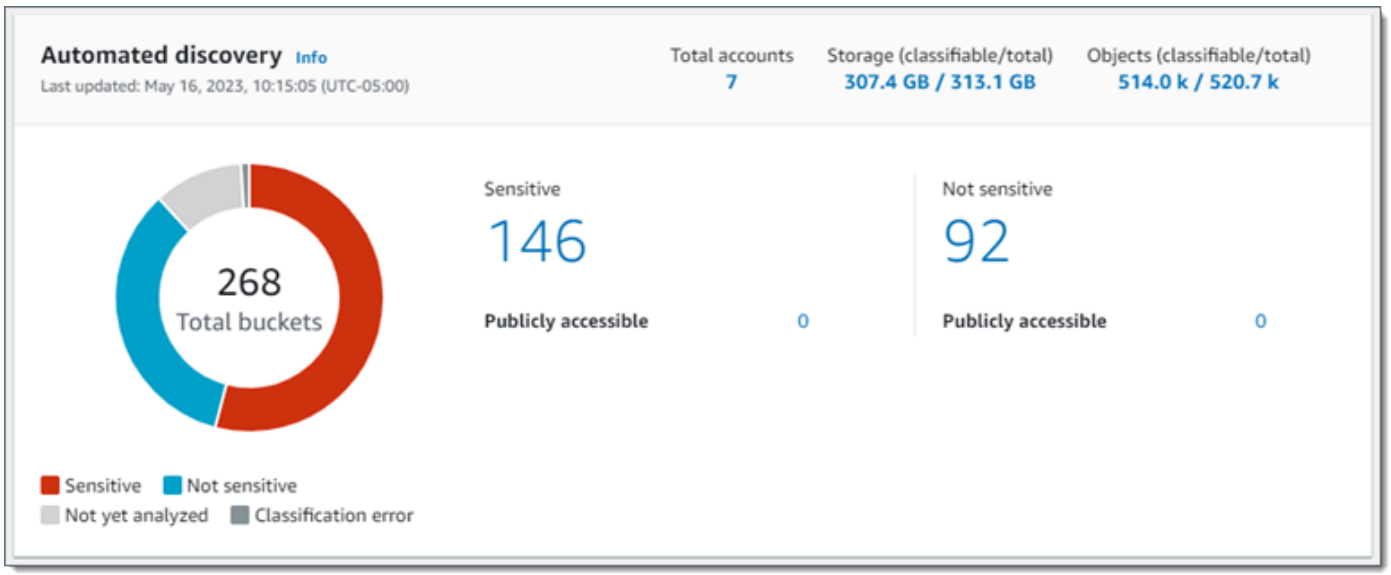
  如果任何对象为压缩文件，则这些值不反映这些文件解压缩后的实际大小。如果对任何存储桶启用了版本控制，则这些值基于这些存储桶中每个对象最新版本的存储大小。
- Objects
  - 可分类 – Macie 可在存储桶中分析的对象的总数。
  - 总计 – 存储桶中所有对象的总数，包括 Macie 无法分析的对象。

在上述统计数据中，如果数据和对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式，则数据和对象属于可分类。有关更多信息，请参阅 支持的存储类别和格式。

请注意，存储和对象统计信息不包括 Macie 不允许 Macie 访问的、存储桶内对象的相关数据。要确定出现这种情况的存储桶，请在控制面板的 覆盖范围问题部分中选择 访问被拒绝 统计数据。

自动发现

这些统计数据主要采集 Macie 迄今为止为您的 Amazon S3 数据执行的、自动敏感数据调查发现活动的状态和结果。例如：



本部分的单独统计数据如下。

存储桶总数

环形图显示您的 S3 存储桶清单中的存储桶总数。该图表根据每个存储桶的当前灵敏度分数将存储分组为：

- 敏感（红色）- 灵敏度分数介于 51 至 100 之间的存储桶总数。
- 不敏感（蓝色）-灵敏度分数介于 1 至 49 之间的存储桶总数。
- 尚未分析（浅灰色）- 灵敏度分数为 50 的存储桶的总数。
- 分类错误（深灰色）- 灵敏度分数为 -1 的存储桶总数。

有关 Macie 定义的灵敏度分数范围和标签的详细信息，请参阅 S3 存储桶的敏感度评分。

要查看某个群组的其他统计信息，请将鼠标悬停在该群组上：

- 存储桶 – 存储桶的总数。
- 可公开访问 - 允许公众进行读取或写入的存储桶总数。
- 可分类字节 – Macie 可在存储桶中分析的所有对象的总存储大小。这些对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式。有关更多信息，请参阅 支持的存储类别和格式。
- 字节总数 - 所有存储桶的总存储大小。

在前述统计信息中，存储大小值基于存储桶中每个最新版本对象的存储大小。如果任何对象为压缩文件，则这些值不反映这些文件解压缩后的实际大小。

敏感

此区域表示当前灵敏度分数介于 51 至 100 之间的 S3 存储桶的总数。在此组中，可公开访问表示允许公众进行读取或写入的存储桶总数。

不敏感

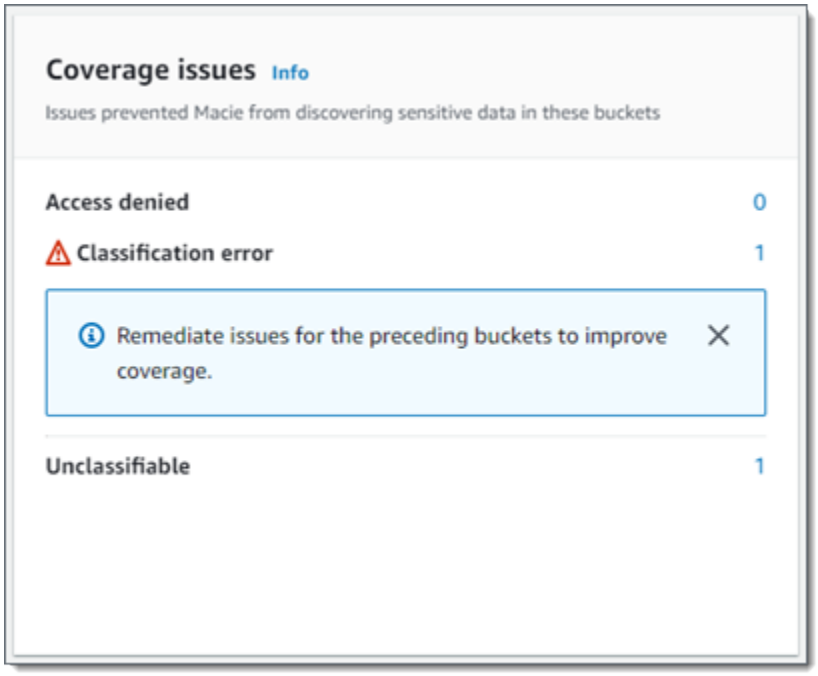
此区域表示当前灵敏度分数介于 1 至 49 之间的 S3 存储桶的总数。在此组中，可公开访问表示允许公众进行读取或写入的存储桶总数。

为了确定和计算可公开访问的统计数据值，Macie 会分析每个存储桶的账户和存储桶级别设置组合，例如账户和存储分区的阻止公共访问设置，以及存储桶的存储桶策略。有关更多信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。

请注意，自动发现部分中的统计信息不包括您创建和运行的敏感数据发现任务的结果。

覆盖范围问题

此部分统计信息表示阻止 Macie 分析单独 S3 存储桶对象的问题。例如：



本节内容：

- 访问被拒绝 - 不允许 Macie 访问的存储桶总数。Macie 无法分析这些存储桶内的任何对象。存储桶的权限设置会阻止 Macie 访问存储桶和存储桶对象。
- 分类错误 – 由于对象级分类错误而导致的、Macie 未分析的存储桶总数。Macie 试图分析这些存储桶中的一个或多个对象。但是，由于对象级权限设置、对象内容或配额存在问题，Macie 无法分析对象。

- 不可分类 - 不存储任何可分类对象的存储桶总数。Macie 无法分析这些存储桶内的任何对象。所有对象使用 Macie 不支持的 Amazon S3 存储类别，并且其文件扩展名表示 Macie 不支持的文件或存储格式。

选择统计信息值，可显示其他详细信息，并显示补救措施指南（如适用）。如果您修复了访问问题和分类错误，则可以在后续分析周期中扩大 Amazon S3 数据的覆盖范围。有关更多信息，请参阅评测自动敏感数据发现覆盖率。

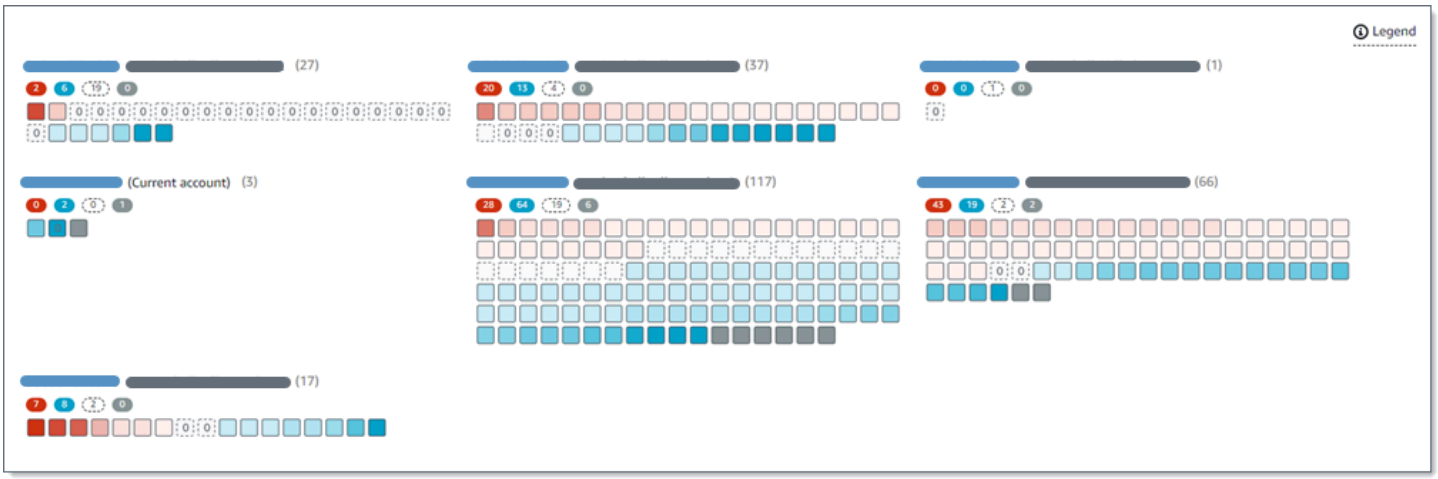
请注意，覆盖率问题部分中的统计数据并未明确包含您创建和运行的敏感数据发现任务的数据。但是，修复影响自动发现敏感数据结果的覆盖范围问题也可能增加您随后运行的作业的覆盖范围。

有关摘要 控制面板其他部分的信息，请参阅 了解“摘要”控制面板的组件。

使用 S3 存储桶地图观察数据灵敏度

在 Amazon Macie 控制台，S3 存储桶热图提供了当前 AWS 区域 Amazon Simple Storage Service (Amazon S3) 数据资产中数据灵敏度的交互式可视化表示。它采集 Macie 迄今为止为您的账户执行的、自动敏感数据发现活动的结果。

如果您是组织的 Macie 管理员，则该地图将包含您的成员账户拥有的 S3 存储桶的结果，按账户 ID 进行分组 AWS 账户 和排序。例如：



地图的每一页最多可显示 99 个账户或 1,000 个存储桶的数据，具体取决于您的组织或 Amazon S3 数据资产大小。

要展示地图，在控制台的导航窗格中选择 S3 存储桶。然后在页面顶部选择地图
()。

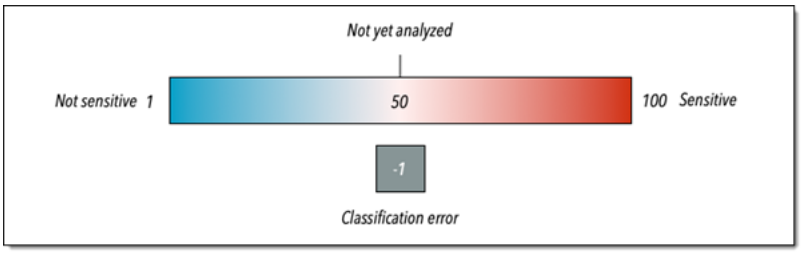
仅当您的账户启用了自动敏感数据发现功能时，才会显示此地图。它不包括您创建和运行的敏感数据调查发现作业结果。

主题

- 解读 S3 存储桶地图中的数据
- 与 S3 存储桶地图交互

解读 S3 存储桶地图中的数据

在 S3 存储桶地图中，每个方块都代表存储桶清单中的一个 S3 存储桶。正方形的颜色代表存储桶的当前灵敏度分数，它衡量两个主要维度的交集：即 Macie 在存储桶中发现的敏感数据量和 Macie 在存储桶内分析的数据量。颜色色调的强度表示一系列数据灵敏度值中桶分数下降位置，如下图所示。



通常，您可以按如下方式解读颜色和色调强度：

- 蓝色 – 如果存储桶的当前灵敏度分数介于 1 至 49 之间，则该桶的正方形为蓝色，存储桶的灵敏度标签为 不敏感。蓝色色调的强度反映了 Macie 在存储桶中分析的唯一对象的数量与存储桶中唯一对象总数的比率。色调越深，表示灵敏度分数越低。
- 无颜色 – 如果存储桶的当前灵敏度分数为 50，则该桶的正方形未着色，并且桶的灵敏度标签为未分析。此外，正方形还有虚线边框。
- 红色 – 如果存储桶的当前灵敏度分数介于 51 至 100 之间，则该桶的正方形为红色，存储桶的灵敏度标签为 敏感。红色调的强度反映了 Macie 在存储桶内发现的敏感数据量。色调越深表示灵敏度分数越高。
- 灰色 – 如果存储桶的当前灵敏度分数为 -1，则该存储桶的正方形为深灰色，存储桶的灵敏度标签显示分类错误。色相强度无变化。

有关 Macie 定义的灵敏度分数范围和标签的详细信息，请参阅 S3 存储桶的敏感度评分。

地图中的 S3 存储桶的正方形也可能包含一个符号。该符号表示可能影响您对存储桶灵敏度评测的错误、问题或其他类型注意事项。符号也可以表示存储桶的安全性存在潜在问题，例如存储桶可公开访问。下表列出了 Macie 用于通知您这些情况的符号。

符号	定义	描述
	访问被拒绝	不允许 Macie 访问存储桶或存储桶对象。因此，Macie 无法分析这些存储桶内的任何对象。 此问题的原因通常是存储桶具有限制性存储桶策略。有关如何解决此问题的信息，请参阅允许 Macie 访问 S3 存储桶和对象。
	公开访问	公众对存储桶拥有读写权限。 为了做出此决策，Macie 会分析每个存储桶的账户和存储桶级别设置组合，例如账户和存储桶的阻止公共访问设置，以及存储桶的存储桶策略。有关更多信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。
	不可分类	Macie 无法分析存储桶内的任何对象。所有存储桶对象都使用 Macie 不支持的 Amazon S3 存储类别，或者有 Macie 不支持的文件扩展名或存储格式。 Macie 要分析某个对象，该对象必须使用所支持的存储类别，并且其文件扩展名表示支持的文件或存储格式。有关更多信息，请参阅 支持的存储类别和格式。

符号	定义	描述
0	零字节	此存储桶不包含任何要由 Macie 分析的对象。存储桶为空，或存储桶中的所有对象都包含零 (0) 字节的数据。

与 S3 存储桶地图交互

在查看 S3 存储桶 地图时，您可以通过不同的方式与其交互，以揭示和评测个人账户和存储桶的其他数据和详细信息。按以下步骤在 Amazon Macie 控制台上显示地图，并与地图提供的各种功能交互。

与 S3 存储桶地图进行交互

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。S3 存储桶页面显示您的存储桶清单地图。如果页面以表格格式显示您的存储桶清单，请选择页面顶部的地图 ( )。
3. 在页面顶部，可以选择刷新 ( )，从 Amazon S3 检索最新的存储桶元数据。
4. 在 S3 存储桶地图中，执行以下任一操作：

   - 要确定有多少桶有特定的敏感度标签，请参阅 ID 正下方的彩色徽章。 AWS 账户 此徽章显示按灵敏度标签细分的汇总存储桶计数。

     例如，红色徽章会报告该账户拥有、且带有灵敏度标签的存储桶的总数。这些存储桶的灵敏度分数介于 51 到 100 之间。蓝色徽章报告该账户拥有且带有 不敏感 标签的存储桶总数。这些存储桶的灵敏度分数介于 1 到 49 之间。
   - 要查看有关存储桶的信息子集，请将鼠标悬停在存储桶的正方形上。弹出框显示存储桶的名称和当前的灵敏度分数。

     弹出框还会显示 Macie 可以在存储桶中分析的对象总数，以及这些对象的最新版本的总存储大小。这些对象为 可分类。它们使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式。有关更多信息，请参阅 支持的存储类别和格式。

- 要筛选地图并仅显示含特定字段值的存储桶，请将光标置于筛选框内，然后为该字段添加筛选条件。Macie 应用条件并在筛选框下方显示该条件。若要进一步优化结果，请为其他字段添加筛选条件。有关更多信息，请参阅 筛选您的 S3 存储桶清单。
- 要深入查看并仅显示特定账户拥有的存储桶，请选择该账户 ID。Macie 会打开新选项卡，该选项卡仅筛选和显示该账户数据。

5. 要查看 Macie 提供的、有关特定存储桶的所有敏感数据调查发现统计数据和其他信息，请选择该存储桶的方块，然后参阅详细信息面板。有关更多信息，请参阅 查看各个 S3 存储桶的数据灵敏度详细信息。

> **Tip**
>
> 在面板的存储桶详细信息选项卡，您可以对许多字段进行转置和向下钻取。要显示某个字段中具有相同值的存储桶，请在该字段中选择 。要显示其他字段值的存储桶，请在字段中选择 。

使用 S3 存储桶表评测数据灵敏度

在 Amazon Macie 控制台，S3 存储桶表显示当前 AWS 区域 Amazon Simple Storage Service (Amazon S3) 存储桶的摘要信息。如果您是组织的 Macie 管理员，则这包括关于您的成员账户拥有的 S3 存储桶的信息。如果您更喜欢以编程方式访问数据，则可以使用 Amazon Macie API 的DescribeBuckets操作。

要自定义视图，您可以在控制台上对表格进行排序和筛选。您也可以选择将数据从表中导出至逗号分隔值 (CSV) 文件。如果您在表中选择一个 S3 存储桶，则详细信息面板显示有关此存储桶的其他信息。这包括详细信息和统计数据，这些详细信息和统计数据采集 Macie 迄今为止为存储桶执行的、自动敏感数据发现活动的结果。这还包括设置和指标数据，这些设置和指标数据提供了存储桶数据安全和隐私的洞察。除了查看存储桶的详细信息外，您还可以使用详细信息面板调整存储桶的自动敏感数据调查发现设置。要了解如何操作，请参阅 管理单个 S3 存储桶的自动敏感数据发现。

若要使用 S3 存储桶表评测数据灵敏度

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。

3. 在 S3 存储桶页面，选择页面顶部的表
()。Ma
会显示您的清单中的存储桶数量和存储桶表。
4. 在页面顶部，可以选择刷新
()，
从 Amazon S3 检索最新的存储桶元数据。

   如果信息图标
()
出现在任何存储桶名称旁边，我们建议您这样操作。此图标表明存储桶是在过去 24 小时内创建的，可能是 Macie 在每日刷新周期中最后一次从 Amazon S3 检索存储桶和对象元数据之后创建的。
5. 在 S3 存储桶表中查看有关清单内每个存储桶的摘要信息：

   - 灵敏度 – 存储桶的当前灵敏度分数。有关 Macie 定义的灵敏度分数范围的信息，请参阅 S3 存储桶的敏感度评分。
   - 存储桶 – 存储桶名称。
   - 账户-拥有存储桶的 AWS 账户 的账户 ID。
   - 可分类对象 – Macie 可在存储桶中分析以检测敏感数据的对象总数。
   - 可分类大小 – Macie 可在存储桶中分析以检测敏感数据的所有对象的总存储大小。

     此值不反映任何压缩对象在解压缩后的实际大小。此外，如果为存储桶启用了版本控制，则此值将基于存储桶中每个最新版本对象的存储大小。
   - 按作业监控 - 指定是否将任何敏感数据发现作业配置为：每天、每周或每月定期分析存储桶中的对象。

     如果此字段的值为是，则表示该存储桶已显式包含在定期作业中，或者该存储桶在过去 24 小时内符合定期作业的条件。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。
   - 最新运行的作业 – 如果将任何一次性或定期的敏感数据发现作业配置为分析存储桶中的对象，则此字段值表示其中一个作业开始运行的最新日期和时间。否则，将该字段留空。

   在上述数据中，如果对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式，则对象属于可分类。您可以通过使用 Macie 检测对象中的敏感数据。有关更多信息，请参阅 支持的存储类别和格式。

6. 要使用表格分析清单，请执行以下操作之一：

   - 要按特定字段对表格进行排序，请点击该字段的列标题。若要更改排序顺序，请再次点击列标题。
   - 要筛选表格并仅显示含特定字段值的存储桶，请将光标置于筛选框内，然后为该字段添加筛选条件。Macie 应用条件并在筛选框下方显示该条件。若要进一步优化结果，请为其他字段添加筛选条件。有关更多信息，请参阅 筛选您的 S3 存储桶清单。
   - 要查看特定存储桶的详细信息和统计数据，请选择表中的存储桶名称，然后转到详细信息面板。有关更多信息，请参阅 查看 S3 存储桶的详细信息。

   > **Tip**
   >
   > 在面板的存储桶详细信息选项卡，您可以对许多字段进行转置和向下钻取。要显示某个字段中具有相同值的存储桶，请在该字段中选择 。要显示其他字段值的存储桶，请在字段中选择 。

7. 要以 CSV 格式文件导出表内数据，请选择您想导出的每行的复选框，或选中选择列标题中的复选框以选择所有行。然后在页面顶部选择导出到 CSV。您最多可从表格中导出 50,000 行。
8. 要对一个或多个存储桶中的对象进行更深入、更直接的分析，请选中每个存储桶对应的复选框，然后选择创建作业。有关更多信息，请参阅 创建敏感数据发现作业。

查看各个 S3 存储桶的数据灵敏度详细信息

在 Amazon Macie 控制台，您可以使用 S3 存储桶页面上的详细信息面板查看 Macie 监控和分析账户的、单独 Amazon Simple Storage Service (Amazon S3) 存储桶的统计信息和其他信息。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。

此统计数据和信息包括详细信息，这些详细信息提供了 S3 存储桶数据安全和隐私的洞察。如果您的账户启用了自动敏感数据发现，它们还会捕获 Macie 迄今为止为存储桶执行的、自动敏感数据发现活动结果。例如，您可发现 Macie 在存储桶中分析的对象列表，以及 Macie 在存储桶中发现的敏感数据的类型和出现次数的明细。注意：此数据不包括您创建和运行的敏感数据调查发现作业结果。

Macie 会自动重新计算和更新这些统计信息和详细信息，同时自动发现账户敏感数据。例如：

- 如果 Macie 在 S3 对象中找不到敏感数据，Macie 会降低存储桶的灵敏度分数，并在必要时更新存储桶灵敏度标签。Macie 还会将该对象添加至其分析的存储桶对象列表。

- 如果 Macie 在 S3 对象中发现敏感数据，Macie 会将这些事件添加至 Macie 在存储桶中发现的、灵敏度数据类型的细分中。Macie 还将提高存储桶的灵敏度分数，并在必要时更新存储桶的灵敏度标签。此外，Macie 还会将该对象添加至其分析的存储桶对象列表。除了为对象创建敏感数据调查发现之外，还包含此任务。
- 如果 Macie 在随后更改或删除的 S3 对象中发现敏感数据，Macie 会从存储桶的敏感数据类型细分中删除此对象的敏感数据。Macie 还将降低存储桶的灵敏度分数，并在必要时更新存储桶的灵敏度标签。此外，Macie 还会将该对象从其分析的存储桶对象列表中移除。
- 如果 Macie 尝试分析 S3 对象，但是因问题或错误而无法执行，则 Macie 会将该对象添加至存储桶中分析的对象列表中，并表示无法分析该对象。

除了查看统计信息和详细信息外，您还可以使用面板调整 S3 存储桶的自动敏感数据调查发现设置。例如，您可将特定类型的敏感数据纳入存储桶分数，或将其移除。有关更多信息，请参阅 管理单个 S3 存储桶的自动发现。

查看 S3 存储桶数据灵敏度详细信息

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 S3 存储桶。S3 存储桶页面显示您的存储桶清单的交互地图。也可选择页面顶部表格
   ()，
   以显示您的表格格式清单。
3. 在 S3 存储桶 地图或表中，选择要查看其详细信息的 S3 存储桶。此详细信息面板显示有关存储桶的统计数据和其他信息。

面板顶部显示有关存储桶的一般信息：存储桶的名称和拥有 AWS 账户 该存储桶的账户 ID。它还为此存储桶提供了更改特定自动敏感数据发现设置选项。有关存储桶的其他设置和信息，请按以下选项卡进行组织：

- 灵敏度
- 存储桶详细信息
- 对象示例
- 敏感数据发现

每个选项卡上的单独设置和信息如下所示。

灵敏度

此选项卡显示存储桶的当前灵敏度分数，范围从 -1 至 100。有关 Macie 定义的灵敏度分数范围的信息，请参阅 S3 存储桶的敏感度评分。

该选项卡还详细列出了 Macie 在存储桶对象中发现的敏感数据类型，以及每种类型出现的次数：

- 敏感数据类型 - 检测数据的托管数据标识符的唯一标识符 (ID)，或检测数据的自定义数据标识符名称。

  托管数据标识符的 ID 描述了该标识符旨在检测的敏感数据类型，例如，用于检测美国护照号码的 USA_PASSPORT_NUMBER。有关每个托管数据标识符的详细信息，请参阅 使用托管数据标识符。
- 计数 - 托管或自定义数据标识符检测到的数据出现的总次数。
- 评分状态 - 指定是将数据出现次数包括在存储桶的灵敏度分数中还是排除在外。

  如果您将 Macie 配置为自动计算存储桶分数，则可以通过在存储分区的分数中纳入或排除特定类型的敏感数据调整计算方式：选中要纳入或排除的数据标识符对应的复选框，然后在 操作菜单上选择所需的选项。有关更多信息，请参阅 管理单个 S3 存储桶的自动发现。

如果 Macie 未在存储桶当前存储的对象中找到敏感数据，则此部分将显示 未找到检测结果 消息。

请注意，灵敏度 选项卡不包含由 Macie 分析、且随后被更改或删除的对象数据。如果在 Macie 分析对象后更改或从存储桶中删除对象，Macie 会自动重新计算和更新相应的统计信息和数据，以排除这些对象。

存储桶详细信息

此选项卡提供关于存储桶设置的详细信息，包括数据安全和隐私设置。例如，您可以查看存储桶的公共访问设置明细，并确定存储桶重复对象还是与其他 AWS 账户分享。

特别值得注意的是，上次更新时间字段指示 Macie 最近从 Amazon S3 中检索存储桶或存储桶对象元数据的时间。最近的自动发现运行时间字段指示 Macie 最近在执行自动发现时分析存储桶对象的时间。

该选项卡还提供对象级统计信息，可帮助评测 Macie 可在存储桶中分析的数据量。它还指示是否将任何敏感数据发现任务配置为分析存储桶中的对象。如有，则可以访问有关最近运行作业的详细信息，然后也可以选择显示该作业产生的任何调查发现。

有关此选项卡的更多详情，请参阅 查看 S3 存储桶的详细信息。

对象示例

此选项卡列出了 Macie 在执行自动敏感数据发现时分析的存储桶对象列表。选择对象名称，以打开 Amazon S3 并显示对象属性。

该列表包含最多 100 个对象的数据。此列表基于对象灵敏度字段值填充：敏感后跟不敏感，后跟 Macie 无法分析的对象。

在列表中，对象灵敏度 字段指示 Macie 是否在对象中找到了敏感数据：

- 敏感 – Macie 发现对象中至少出现过一次敏感数据。
- 不敏感 – Macie 未在对象中找到敏感数据。
- —（短划线）– 因问题或错误，Macie 无法完成对对象的分析。

分类结果 字段指示 Macie 是否能够分析对象：

- 完成 – Macie 完成了对象分析。
- 部分 – 由于问题或错误，Macie 仅分析部分对象数据。例如，该对象是一个存档文件，其中包含不支持的格式的文件。
- 已跳过 – 因问题或错误，Macie 无法分析对象中的任何数据。例如，使用不允许 Macie 使用的密钥加密对象。

请注意，该列表不包括 Macie 分析或尝试分析后更改或删除的对象。如果某个对象随后被更改或删除，Macie 会自动从列表中移除此对象。

敏感数据发现

此选项卡为存储桶提供聚合、自动敏感数据发现统计信息：

- 已分析字节数 – Macie 在存储桶中分析的数据总量（以字节为单位）。
- 可分类字节 – Macie 可在存储桶中分析的所有对象的总存储大小（以字节计）。这些对象使用所支持的 Amazon S3 存储类别，并且其文件扩展名表示支持的文件或存储格式。有关更多信息，请参阅 支持的存储类别和格式。
- 检测总数 - Macie 在存储桶中发现的敏感数据的总出现次数。这包括当前被存储桶的灵敏度评分设置隐藏的事件。

已分析对象图表显示 Macie 在存储桶中分析的对象总数。它呈现了 Macie 在其中找到/未找到敏感数据的对象数量。图表下方的图例介绍了这些结果的细分：

- 敏感对象（红色）- Macie 在其中发现至少一次敏感数据的对象总数。
- 非敏感对象（蓝色）- Macie 未在其中找到敏感数据的对象总数。

- 跳过的对象（深灰色）- Macie 因问题或错误而无法分析的对象总数。

图表图例下方的区域详细列出了 Macie 因出现某些类型的权限问题或加密错误而无法分析对象的情况：

- 已跳过：加密无效-使用客户提供的密钥加密的对象总数。Macie 无法访问这些密钥。
- 已跳过：KMS 无效 — 使用 AWS Key Management Service (AWS KMS) 密钥加密但不再可用的对象总数。这些对象使用 AWS KMS keys 已禁用、计划删除或已删除的对象进行加密。Macie 无法使用这些按键。
- 已跳过：权限被拒绝 — 由于对象的权限设置或用于加密对象的密钥的权限设置，Macie 无法访问的对象总数。

有关这些问题以及可能发生的其他类型的问题和错误的详细信息，请参阅修复自动敏感数据发现的覆盖率问题。如果您修复了问题和错误，则可以在随后的分析周期中增加存储桶数据的覆盖范围。

敏感数据发现 选项卡上的统计信息中，不包括 Macie 分析或尝试分析后更改或删除的对象数据。如果 Macie 分析或尝试分析后从存储桶更改或删除对象，则 Macie 会自动计算这些统计数据以排除这些对象。

分析自动发现产生的敏感数据调查发现

在自动敏感数据发现时，Amazon Macie 会为在其中发现敏感数据的每个 Amazon Simple Storage Service (Amazon S3)对象创建敏感数据调查发现。敏感数据调查发现是 Macie 在 S3 对象中发现的敏感数据的详细报告。每项敏感数据调查发现都会提供严重性评级和详细信息，如：

- Macie 发现敏感数据的日期与时间。
- Macie 发现敏感数据的类别和类型。
- Macie 发现的每种敏感数据的出现次数。
- Macie 是如何找到敏感数据、自动敏感数据发现或敏感数据发现任务作业。
- 受影响的 S3 存储桶和对象的名称、公开访问设置、加密类型和其他信息。

根据受影响 S3 对象的文件类型或存储格式，详细信息还可能包括 Macie 发现的、多达 15 处敏感数据的位置。敏感数据调查发现不包括 Macie 发现的敏感数据。相反，它提供了用于进一步调查和必要补救的信息。

Macie 会将发现的敏感数据存储 90 天。您可以使用 Amazon Macie 控制台或 Amazon Macie API 访问它们。您还可以使用其他应用程序、服务和系统，监控和处理调查发现。有关更多信息，请参阅 分析调查发现。

分析自动敏感数据发现所得出的结果

若要识别和分析 Macie 创建的敏感数据调查发现，同时为您的账户执行自动化敏感数据发现，您可筛选调查发现。您可通过筛选条件，指定调查发现属性，以构建自定义视图和调查发现查询。您可以使用 Amazon Macie 控制台筛选结果，也可以使用Amazon Macie API 以编程方式提交查询。

Console

按照以下步骤，使用 Amazon Macie 控制台识别和分析调查发现。

要分析自动发现所得出的调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 **调查发现**。
3. （可选）要显示被抑制规则隐藏的调查发现，请使用调查发现状态设置。选择**全部**可同时显示隐藏和未隐藏的调查发现，或者选择**已存档**以仅显示隐藏的调查发现。然后要再次隐藏被抑制的调查发现，请选择**当前**。
4. 将光标置于筛选标准框。在出现的字段列表中，选择 **原始类型**。

   此字段指定 Macie 是如何找到敏感数据（生成调查发现）、自动敏感数据发现或敏感数据发现任务作业。要在筛选字段列表中查找此字段，您可以浏览完整列表，或者输入部分字段名称以缩小字段列表范围。
5. 选择 AUTOMATED_SENSITIVE_DATA_DISCOVERY 作为该字段的值，然后选择**应用**。Macie 应用筛选标准并将该条件添加到筛选标准框中的筛选条件令牌中。
6. （可选）若要细化结果，请为其他字段添加筛选条件，例如：**创建时间**表示调查发现创建的时间；**S3 存储桶名称** 表示受影响存储桶的名称；或 **敏感数据检测类型** 表示检测和产生调查发现的敏感类型。有关更多信息，请参阅 筛选调查发现。

如果您想在随后再次使用这组条件，可以将其另存为筛选规则。为此，请在筛选标准框中选择**保存规则**。输入规则的名称和描述（可选）。完成后，选择**保存**。

API

要以编程方式识别和分析调查结果，请在使用 Amazon Macie API 的ListFindings或GetFindingStatistics操作提交的查询中指定筛选条件。该 ListFindings 操作返回一个由调查发现 ID 组成的数组，每个符合筛选条件的调查发现对应一个 ID。然后，您可以使用这些 ID 检索每个调查发现的详细信息。GetFindingStatistics 操作会返回与筛选条件匹配的所有调查发现的汇总统计数据，这些数据按您在请求中指定的字段分组。有关以编程方式筛选调查发现的更多信息，请参阅 筛选调查发现

在筛选条件中，纳入 originType 字段条件。此字段指定 Macie 是如何找到敏感数据（生成调查发现）、自动敏感数据发现或敏感数据发现任务作业。如果调查发现产生的同时执行自动发现，则此字段值为AUTOMATED_SENSITIVE_DATA_DISCOVERY。

要使用 AWS Command Line Interface (AWS CLI) 识别和分析调查结果，请运行 list- findings 或get-finding-statistics命令。以下示例使用 list-findings 命令检索当前 AWS 区域由自动敏感数据调查发现生成的、所有高严重性调查发现的 ID。

对于 Linux、macOS 或 Unix，使用反斜杠 (\) 行继续符来提高可读性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

对于 Microsoft Windows，使用脱字符 (^) 行继续符来提高可读性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

其中：

- classificationDetails.originType 指定 原始类型 字段的 JSON 名称，以及：
  - eq 指定 等于 运算符。
  - AUTOMATED_SENSITIVE_DATA_DISCOVERY 是该字段的枚举值。
- *severity.description* 指定 严重性 字段的 JSON 名称，以及：
  - *eq* 指定 等于 运算符。
  - *High* 是该字段的枚举值。

如果命令成功运行，Macie 将返回一个 findingIds 数组。该数组列出了符合筛选标准的每个调查发现的唯一标识符，如以下示例所示。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
```

```
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

如果没有符合筛选条件的调查发现，Macie 将返回空`findingIds`数组。

```
{
    "findingIds": []
}
```

访问自动发现产生的敏感数据调查发现

Amazon Macie 对其选择进行分析的每个 Amazon Simple Storage Service (Amazon S3) 创建分析记录，同时为账户或组织执行敏感分析发现。这些记录称为敏感数据发现，记录有关 Macie 对单个 S3 对象执行的分析详细信息。这包括 Macie 在 中没有发现敏感数据因而不会产生调查发现的对象，以及 Macie 因错误或权限设置等问题而无法分析的对象。

如果 Macie 在 S3 对象中找到了敏感数据，则敏感数据发现结果将包括来自相应调查发现的数据。它还提供了其他信息，例如 Macie 在对象中发现的每种敏感数据出现多达 1000 次的位置。例如：

- Microsoft Excel 工作簿、CSV 文件或 TSV 文件中单元格或字段的列号和行号
- JSON 或 JSON Lines 文件中的字段或数组路径
- 除 CSV、JSON、JSON Lines 或 TSV 文件之外的非二进制文本文件中的行号，例如 HTML、TXT 或 XML 文件
- Adobe 可移植文档格式 (PDF) 文件中页面的页码
- Apache Avro 对象容器或 Apache Parquet 文件中记录的字段的记录索引和路径

如果受影响的 S3 对象是存档文件（如 .tar 或 .zip 文件），则敏感数据发现结果还会提供 Macie 从存档中提取的单个文件中敏感数据出现的详细位置数据。Macie 不会在存档文件的敏感数据调查发现中包含此信息。为了报告位置数据，敏感数据发现结果使用标准化 JSON 架构。

敏感数据发现结果不包括 Macie 发现的敏感数据。相反，它为您提供分析记录，有助于数据隐私和保护审计或调查。

Macie 会将您的敏感数据发现结果存储 90 天。您无法直接在 Amazon Macie 控制台或使用 Amazon Macie API 访问它们。相反，您可以配置 Macie 将其加密并存储至 S3 存储桶内。存储桶可以用作所有敏感数据发现结果的最终长期存储库。然后，您可以选择访问和查询该存储库中的结果。

要确定是否已为您的账户配置了此存储库，请在 Amazon Macie 控制台的导航窗格中选择发现结果。要以编程方式执行此GetClassificationExportConfiguration操作，请使用亚马逊 Macie API 的操作。如果您尚未为账户配置此存储库，请参阅 存储和保留敏感数据发现结果 以了解具体操作方法。

将 Macie 配置为将敏感数据发现存储在 S3 存储桶中后，Macie 会将结果写入 JSON Lines (.jsonl) 文件，然后加密这些文件并将其作为 GNU Zip (.gz) 文件添加至存储桶。为了自动发现敏感数据，Macie 会将文件添加到存储桶automated-sensitive-data-discovery中名为的文件夹中。

与敏感数据调查发现一样的是，敏感数据发现遵循标准化架构。这可以帮助您选择性地使用其他应用程序、服务和系统进行查询、监控和处理。

> **Tip**
>
> 有关如何查询和使用敏感数据发现结果来分析和报告潜在的数据安全风险的详细教学示例，请参阅安全博客上的 “如何使用 Amazon Athena 和 A QuickSight mazon 查询和可视化 Macie 敏感数据发现结果” 博客文章。AWS
> 有关可用于分析敏感数据发现结果的 Athena 查询示例，请访问上的 Amazon Macie 结果分析存储库。 GitHub此存储库还提供了有关配置 Athena 以检索和解密结果的说明，以及用于为结果创建表的脚本。

S3 存储桶的敏感度评分

如果您的账户启用了自动敏感数据发现功能，Amazon Macie 会自动计算敏感度分数，并将其分配给它为您的账户监控和分析的每个 Amazon Simple Storage Service (Amazon S3) 存储桶。敏感度分数是 S3 存储桶可能包含的敏感数据量的定量表示。根据该分数，Macie 还会为每个存储桶分配一个敏感度标签。敏感度标签是存储桶敏感度分数的定性表示。这些值可以作为参考点，用于确定敏感数据可能存放在您的 Amazon S3 数据资产中的位置，以及识别和监控这些数据的潜在安全风险。

默认情况下，S3 存储桶的敏感度分数和标签反映了 Macie 迄今为止为该存储桶执行的自动敏感数据发现活动的结果。它们不反映您创建和运行的敏感数据发现作业的结果。此外，分数和标签均不暗示或以其他方式表明存储桶或存储桶对象可能对您的组织具有的关键性或重要性。但是，您可以通过手动为存储桶分配最高分数 (100) 来覆盖存储桶的计算得分，这也会为存储桶分配敏感标签。

主题

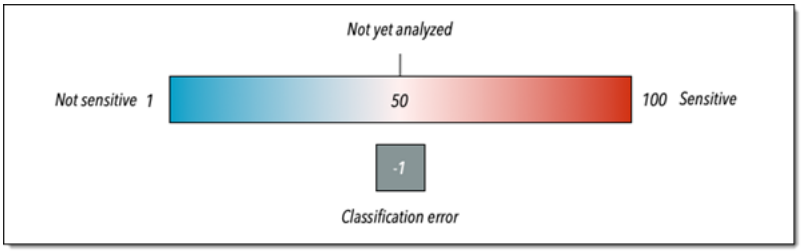
- 敏感度评分维度和范围
- 监控敏感度分数

敏感度评分维度和范围

如果由 Amazon Macie 计算，则 S3 存储桶的敏感度分数是两个主要维度交叉点的定量衡量标准：

- Macie 在存储桶中找到的敏感数据量。这主要源于 Macie 在存储桶中发现的敏感数据类型的性质和数量以及每种类型的出现次数。
- Macie 在存储桶内分析的数据量。这主要源于 Macie 在存储桶中分析的唯一对象的数量相对于存储桶中唯一对象的总数。

S3 存储桶的敏感度分数决定了 Macie 为存储桶分配哪个敏感度标签。敏感度标签是分数的定性表示形式，例如敏感或不敏感。在 Amazon Macie 控制台上，存储桶的敏感度分数还决定了 Macie 在数据可视化中使用哪种颜色来表示存储桶，如下图所示。



敏感度分数介于 -1 到 100 之间，如下表所述。要评测对 S3 存储桶分数的输入，您可以参考 Macie 提供的有关该存储桶的敏感数据发现统计数据和其他详细信息。

敏感度评分	敏感度标签	其他信息
–1	分类错误	由于对象级分类错误（对象级权限设置、对象内容或配额存在问题），Macie 尚未分析存储桶的任何对象。 当 Macie 尝试分析存储桶中的一个或多个对象时，出现了错误。例如，对象是格式错误的文件，或者对象是使用 Macie 无法访问或不允许使用的密钥加密的。存储桶的覆盖数据可以帮助您调查和修复错误。有关更多信息，请参阅评测自动敏感数据发现覆盖率。

敏感度评分	敏感度标签	其他信息
		Macie 将继续尝试分析存储桶中的对象。如果 Macie 成功分析了对象，Macie 将更新存储桶的敏感度分数和标签以反映分析结果。
1-49	不敏感	在此范围内，较高的分数（例如 49）表明 Macie 已经分析了存储桶中相对较少的对象。较低的分数（例如 1）表示 Macie 已经分析了存储桶中的许多对象（相对于存储桶中对象的总数），并且在这些对象中检测到的敏感数据的类型和出现次数相对较少。 分数为 1 也表示存储桶不包含任何对象，或者存储桶中的所有对象都包含零 (0) 字节的数据。存储桶详细信息中的对象统计信息可以帮助您确定是否是这种情况。有关更多信息，请参阅查看 S3 存储桶的详细信息。

敏感度评分	敏感度标签	其他信息
50	尚未分析	Macie 尚未尝试分析或分析存储桶中的任何对象。当您最初为账户启用自动发现功能时，Macie 会自动将此分数分配给存储桶，或者存储桶已添加到您的存储桶清单中。 分数为 50 也表示存储桶的权限设置阻止 Macie 访问存储桶或存储桶的对象。这通常是由限制性存储桶策略造成的。存储桶的详细信息可以帮助您确定是否是这种情况，因为 Macie 只能提供有关存储桶的部分信息。有关如何解决此问题的信息，请参阅 允许 Macie 访问 S3 存储桶和对象。
51-99	敏感	在这个范围内，分数越高，例如 99，表明 Macie 分析了存储桶中的许多对象（相对于存储桶中对象的总数），并且在这些对象中检测到许多类型和出现多次的敏感数据。较低的分数，例如 51，表明 Macie 分析了存储桶中中等数量的对象（相对于存储桶中对象的总数），并且在这些对象中检测到至少几种类型和出现几次的敏感数据。
100	敏感	分数是手动分配给桶的，覆盖了计算得出的分数。Macie 不会将此分数分配给存储桶。

监控敏感度分数

当您最初为账户启用自动敏感数据发现时，Amazon Macie 会自动为每个 S3 存储桶分配 50 的敏感度分数。当存储桶添加到您的存储桶清单时，Macie 还会将该分数分配给该存储桶。根据该分数，每个存储桶的敏感度标签为尚未分析。空存储桶是例外，它是不包含任何对象或存储桶中所有对象包含零 (0) 字节数据的存储桶。如果存储桶是这种情况，Macie 给存储桶分配 1 分，存储桶的灵敏度标签为不敏感。

随着每天对您的账户进行自动敏感数据发现，Macie 会更新 S3 存储桶的敏感性分数和标签，以反映分析结果。例如：

- 如果 Macie 在对象中找不到敏感数据，Macie 会降低存储桶的敏感度分数，并在必要时更新存储桶敏感度标签。
- 如果 Macie 在对象中找到敏感数据，Macie 会增加存储桶的敏感度分数，并在必要时更新存储桶敏感度标签。
- 如果 Macie 在随后更改的对象中发现敏感数据，Macie 会从存储桶的敏感度分数中删除该对象的敏感数据检测，并根据需要更新存储桶的敏感度标签。
- 如果 Macie 在随后删除的对象中发现敏感数据，Macie 会从存储桶的敏感度分数中删除该对象的敏感数据检测，并根据需要更新存储桶的敏感度标签。
- 如果一个对象被添加到一个先前为空的存储桶中，并且 Macie 在该对象中发现了敏感数据，Macie 会增加存储桶的敏感度评分，并根据需要更新存储桶的敏感度标签。
- 如果存储桶的权限设置阻止 Macie 检索有关该存储桶或存储桶对象的信息或访问该存储桶或存储桶的对象，Macie 会将该存储桶的敏感度分数更改为 50，并将该存储桶的敏感度标签更改为尚未分析。

根据您在 Amazon S3 中存储的数据量，分析结果可以在为您的账户启用自动敏感数据发现后的 48 小时内开始出现。

您可以调整账户的敏感度评分设置，这会更改所有 S3 存储桶的后续分析设置。您也可以调整单个 S3 存储桶的设置。对于账户级别的设置，您可以开始在分析中包括或排除特定的允许列表、自定义数据标识符或托管数据标识符。您也可以将特定的存储桶排除在分析之外。有关更多信息，请参阅为您的账户配置自动化发现设置。

要调整特定存储桶的评分设置，您可以在该存储桶的分数中包含或排除特定类型的敏感数据。此外，您还可以指定是否为存储桶分配自动计算出的分数。有关更多信息，请参阅管理单个 S3 存储桶的自动发现。

自动敏感数据发现的默认设置

如果您的账户启用了自动敏感数据发现功能，Amazon Macie 会自动从其监控和分析您的账户的所有 Amazon Simple Storage Service (Amazon S3) 存储桶中选择和分析样本对象。如果您是某个组织的 Macie 管理员，则这包括您的成员账户拥有的 S3 存储桶。要细化分析范围，您可以将特定的存储桶排除在自动敏感数据发现之外。您可以通过两种方式执行此操作：更改账户的自动敏感数据发现设置，以及更改各个存储桶的自动敏感数据发现设置。

默认情况下，Macie 仅使用我们推荐用于自动敏感数据发现的一组托管数据标识符来分析 S3 对象。Macie 不使用您定义的任何自定义数据标识符或允许列表。要自定义分析，您可以将 Macie 配置为使用特定的托管数据标识符、自定义数据标识符和允许列表。您可以通过更改账户的自动敏感数据发现设置来实现此目的。

主题

- 敏感数据自动发现的默认托管数据标识符
- 更新了自动敏感数据发现的默认设置

敏感数据自动发现的默认托管数据标识符

默认情况下，Amazon Macie 仅使用我们推荐用于自动敏感数据发现的一组托管数据标识符来分析 S3 对象。这组默认的托管数据标识符旨在检测敏感数据的常见类别和类型。根据我们的研究，它可以检测一般类别和类型的敏感数据，同时还可以通过降低噪音来优化您的自动发现结果。

默认设置为动态。在我们发布新的托管数据标识符时，如果它们有可能进一步优化您的自动敏感数据发现结果，我们会将其添加到默认标识符集中。随着时间的推移，我们还可能在集合中添加或删除现有的托管数据标识符。移除托管数据标识符不会影响 S3 存储桶的现有敏感数据发现统计数据和详细信息。例如，如果我们移除 Macie 之前在存储桶中检测到的某类敏感数据的托管数据标识符，Macie 将继续报告该存储桶的这些检测结果。如果我们在默认集中添加或删除托管数据标识符，我们会更新此页面以表明更改的性质和时间。有关这些更改的自动警报，您可以订阅 Macie 文档历史记录页面上的 RSS 源。

以下主题列出了当前位于默认集中的托管数据标识符，这些标识符按敏感数据类别和类型组织。它们为集合中的每个托管数据标识符指定唯一标识符 (ID)。此 ID 描述了托管数据标识符旨在检测的敏感数据类型，例如：PGP_PRIVATE_KEY 表示 PGP 私钥，USA_PASSPORT_NUMBER 表示美国护照号码。如果您更改账户的自动敏感数据发现设置，则可以使用此 ID 将托管数据标识符明确排除在后续分析之外。

主题

- 凭证
- 财务信息
- 个人身份信息（PII）

有关特定托管数据标识符的详细信息或 Macie 当前提供的所有托管数据标识符的完整列表，请参阅使用托管数据标识符。

凭证

为了检测 S3 对象中出现的凭证数据，Macie 默认使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
AWS秘密访问密钥	AWS_CREDENTIALS
HTTP 基本授权标头	HTTP_BASIC_AUTH_HEADER
OpenSSH 私有密钥	OPENSSH_PRIVATE_KEY
PGP 私有密钥	PGP_PRIVATE_KEY
公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	PKCS
PuTTY 私有密钥	PUTTY_PRIVATE_KEY

财务信息

为了检测 S3 对象中出现的财务信息，Macie 默认使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
信用卡磁条数据	CREDIT_CARD_MAGNETIC_STRIPE
信用卡号	CREDIT_CARD_NUMBER （适用于关键字附近的信用卡号）

个人身份信息（PII）

为了检测 S3 对象中出现的个人身份信息（PII），Macie 默认使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
驾驶执照识别号	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE （对于美国）， UK_DRIVERS_LICENSE
选民名册编号	UK_ELECTORAL_ROLL_NUMBER
身份证号码	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保险号码 (NINO, National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER
护照编号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社会保险号码 (SIN, Social Insurance Number)	CANADA_SOCIAL_INSURANCE_NUMBER
社会保障号码 (SSN, Social Security number)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
纳税人识别号或参考号	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX

敏感数据类型	托管数据标识符 ID
	_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

更新了自动敏感数据发现的默认设置

下表描述了 Amazon Macie 默认用于自动敏感数据发现的设置的更改。有关这些更改的自动警报，可以订阅 Macie 文档历史记录页面上的 RSS 源。

更改	说明	日期
实现了一组新的动态默认托管数据标识符	新的自动敏感数据发现配置现在基于一组动态的默认托管数据标识符。如果您在此日期或之后首次启用自动敏感数据发现，则您的配置将基于动态集。 如果您在此日期之前首次启用自动敏感数据发现，则您的配置将基于另一组托管数据标识符。有关更多信息，请参阅此表后面的注释。	2023 年 8 月 2 日
通用版	自动敏感数据发现的初始版本。	2022 年 11 月 28 日

如果您最初在 2023 年 8 月 2 日之前为账户启用自动敏感数据发现，则您的配置不是基于默认托管数据标识符的动态集合。相反，您的配置基于一组静态的托管数据标识符，这些标识符是我们在自动敏感数据发现的初始版本中定义的，如下表所示。

要确定您最初何时为账户启用自动敏感数据发现，请在 Amazon Macie 控制台的导航窗格中选择自动发现，然后参阅 状态部分中的启用日期。要以编程方式执行此操作，请使用 Amazon Macie API 的 GetAutomatedDiscoveryConfiguration 操作并参考 `firstEnabledAt` 字段的值。如果日期早于 2023 年 8 月 2 日，并且您想开始使用默认托管数据标识符的动态集，请联系 AWS Support 寻求帮助。

下表列出了静态集中的所有托管数据标识符。该表首先按敏感数据类别排序，然后按敏感数据类型排序。有关特定托管数据标识符的详细信息，请参阅使用托管数据标识符。

敏感数据类别	敏感数据类型	托管数据标识符 ID
凭证	AWS秘密访问密钥	AWS_CREDENTIALS
凭证	HTTP 基本授权标头	HTTP_BASIC_AUTH_HEADER
凭证	OpenSSH 私有密钥	OPENSSH_PRIVATE_KEY
凭证	PGP 私有密钥	PGP_PRIVATE_KEY
凭证	公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	PKCS
凭证	PuTTY 私有密钥	PUTTY_PRIVATE_KEY
财务信息	银行账号	BANK_ACCOUNT_NUMBER （适用于加拿大和美国银行账号），FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
财务信息	信用卡到期日期	CREDIT_CARD_EXPIRATION
财务信息	信用卡磁条数据	CREDIT_CARD_MAGNETIC_STRIPE

敏感数据类别	敏感数据类型	托管数据标识符 ID
财务信息	信用卡号	CREDIT_CARD_NUMBER （适用于关键字附近的信用卡号）
财务信息	信用卡验证码	CREDIT_CARD_SECURITY_CODE
个人信息：个人健康信息（PHI）	毒品管理局(DEA, Drug Enforcement Agency)注册号	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
个人信息：PHI	健康保险索赔编号 (HICN, Health Insurance Claim Number)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
个人信息：PHI	健康保险或医疗识别号	CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
个人信息：PHI	医疗保健通用程序编码系统 (HCPCS, Healthcare Common Procedure Coding System) 代码	USA_HEALTHCARE_PROCEDURE_CODE
个人信息：PHI	国家药品编码 (NDC, National Drug Code)	USA_NATIONAL_DRUG_CODE
个人信息：PHI	国家提供商识别码 (NPI, National Provider Identifier)	USA_NATIONAL_PROVIDER_IDENTIFIER

敏感数据类别	敏感数据类型	托管数据标识符 ID
个人信息：PHI	唯一设备标识符(UDI)	MEDICAL_DEVICE_UDI
个人信息：个人身份信息（PII）	出生日期	DATE_OF_BIRTH

敏感数据类别	敏感数据类型	托管数据标识符 ID
个人信息：PII	驾驶执照识别号	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 （对于美国），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, NETHERLAN

敏感数据类别	敏感数据类型	托管数据标识符 ID
		DS_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
个人信息：PII	选民名册编号	UK_ELECTORAL_ROLL_NUMBER
个人信息：PII	全名	NAME
个人信息：PII	全球定位系统(GPS, Global Positioning System)坐标	LATITUDE_LONGITUDE
个人信息：PII	邮寄地址	ADDRESS, BRAZIL_CEP_CODE
个人信息：PII	身份证号码	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

敏感数据类别	敏感数据类型	托管数据标识符 ID
个人信息：PII	国民保险号码 (NINO, National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER
个人信息：PII	护照编号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
个人信息：PII	永久居留号码	CANADA_NATIONAL_IDENTIFICATION_NUMBER
个人信息：PII	电话号码	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER （适用于加拿大和美国），SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
个人信息：PII	社会保险号码 (SIN, Social Insurance Number)	CANADA_SOCIAL_INSURANCE_NUMBER
个人信息：PII	社会保障号码 (SSN, Social Security number)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

敏感数据类别	敏感数据类型	托管数据标识符 ID
个人信息：PII	纳税人识别号或参考号	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
个人信息：PII	车辆识别号码 (VIN, Vehicle Identification Number)	VEHICLE_IDENTIFICATION_NUMBER

在 Amazon Macie 中运行敏感数据发现作业

借助 Amazon Macie，您可以创建和运行敏感数据发现作业，以自动发现、记录和报告 Amazon Simple Storage Service (Amazon S3) 存储桶中的敏感数据。敏感数据发现作业是 Macie 执行的一系列自动处理和分析任务，用于检测和报告 Amazon S3 对象中的敏感数据。每项作业都提供有关 Macie 发现的敏感数据以及 Macie 执行的分析的详细报告。通过创建和运行作业，您可以构建和维护组织存储在 Amazon S3 中的数据以及这些数据的任何安全性或合规性风险的全面视图。

为了帮助您满足并保持对数据安全和隐私要求的合规性，Macie 提供了多种用于安排和定义作业范围的选项。您可以将作业配置为仅运行一次以进行按需分析和评测，或定期运行一次以进行定期分析、评测和监控。您还可以定义作业分析的广度和深度 - 您选择的特定 S3 存储桶或符合特定条件的存储桶。您可以选择通过选择其他选项来细化该分析的范围。这些选项包括派生自 S3 对象属性的自定义包含和排除条件，例如标签、前缀以及对象上次修改时间。

对于每项作业，您还可以指定希望 Macie 检测和报告的敏感数据类型。您可以将作业配置为使用 Macie 提供的托管数据标识符、您定义的自定义数据标识符或两者的组合。通过为作业选择特定的托管和自定义数据标识符，您可以定制分析，将重点放在特定类型的敏感数据上。要微调分析，您还可以将作业配置为使用您定义的允许列表。允许列表指定了您希望 Macie 忽略的文本和文本模式，通常是组织特定场景或环境的敏感数据异常。

每项作业都会生成 Macie 发现的敏感数据以及 Macie 执行的分析的记录—敏感数据调查发现和敏感数据发现结果。敏感数据调查发现是 Macie 在 S3 对象中发现的敏感数据的详细报告。敏感数据发现结果是关于 S3 对象分析的详细信息的记录。Macie 会为您配置作业进行分析的每个对象创建敏感数据发现结果。这包括 Macie 找不到敏感数据的对象，因此不会生成敏感数据调查发现，以及 Macie 由于错误或问题而无法分析的对象。每种类型的记录都遵循标准化架构，该架构可以帮助您查询、监控和处理记录，以满足您的安全性和合规性要求。

主题

敏感数据发现作业的范围选项

使用敏感数据发现作业，您可以定义 Amazon Simple Storage Service (Amazon S3) 数据的范围，Amazon Macie 会分析这些数据以检测和报告敏感数据。为了帮助您执行此操作，Macie 提供了几个特定于作业的选项，您可以在创建和配置作业时选择这些选项。

范围选项

S3 存储桶

在创建敏感数据发现作业时，您可以指定哪些 S3 存储桶包含您希望 Macie 在任务运行时分析的对象。您可以通过以下两种方式中的任何一种来执行此操作：从存储桶清单中选择特定的 S3 存储桶，或指定派生自 S3 存储桶属性的自定义条件。

选择特定存储桶

使用此选项，您可以显式选择希望作业分析的每个 S3 存储桶。然后，当作业运行时，它仅分析您所选存储桶中的对象。如果您将作业配置为每天、每周或每月定期运行，则该作业每次运行时都会分析这些相同存储桶中的对象。

如果您更喜欢对一组特定数据进行有针对性的分析，则此配置非常有用。它使您可以精确、可预测地控制作业分析哪些存储桶。

指定存储桶标准

使用此选项，您可以定义运行时标准，以确定作业分析哪些 S3 存储桶。该条件由一个或多个派生自存储桶属性的条件组成，如公共访问设置和标签。当任务运行时，它会识别符合条件的存储桶，然后分析这些存储桶中的对象。如果您将作业配置为定期运行，则该作业每次运行时都会执行此操作。因此，作业每次运行时可能会分析不同存储桶中的对象，具体取决于存储桶清单的变化和您定义的条件。

如果您希望作业的分析范围能动态适应存储桶清单的变化，则此配置非常有用。如果您将作业配置为使用存储桶条件并定期运行，则该作业会自动识别符合条件的新存储桶，并检查这些存储桶中是否存在敏感数据。

本节中的主题提供了有关每个选项的更多详细信息。

主题

选择特定 S3 存储桶

如果您选择显式选择要进行作业分析的每个 S3 存储桶，Macie 会为您提供当前 AWS 区域 中存储桶的完整清单。然后，您可以查看您的清单并选择所需的存储桶。要了解 Macie 如何为您生成和维护此清单，请参阅 Macie 如何监控 Amazon S3 数据安全性。

如果您是某个组织的 Macie 管理员，则清单中会包含组织中成员账户所拥有的存储桶。您可以选择多达 1000 个存储桶，涵盖多达 1000 个账户。

为了帮助您选择存储桶，该清单提供了每个存储桶的详细信息和统计数据。这包括作业可以在每个存储桶中分析的数据量 - 可分类对象是指使用支持的 Amazon S3 存储类且具有支持的文件或存储格式文件扩展名的对象。清单还会显示是否已将任何现有作业配置为分析存储桶中的对象。这些详细信息可以帮助您估算作业的范围，并优化您的存储桶选择。

在清单表中：

- 敏感度 - 如果您的账户启用了自动敏感数据发现，则显示存储桶当前敏感度分数。
- 可分类对象 - 指定作业可在一个存储桶中分析的对象总数。
- 可分类大小 - 指定作业可在一个存储桶中分析的所有对象的总存储大小。

  如果存储桶包含压缩对象，则该值并不反映这些对象解压后的实际大小。如果为存储桶启用了版本控制，则此值基于存储桶中每个对象的最新版本的存储大小。
- 由作业监控 – 指示是否将任何现有作业配置为每天、每周或每月定期分析存储桶中的对象。

  如果此字段的值为是，则表示该存储桶已显式包含在定期作业中，或者该存储桶在过去 24 小时内符合定期作业的条件。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。
- 最近作业运行时间– 如果将现有定期或一次性作业配置为分析存储桶中的对象，则此字段表示其中一个作业开始运行的最新日期和时间。否则，将该字段留空。

如果表中任何存储桶名称旁边显示信息图标
()，
我们建议您从 Amazon S3 中检索最新的存储桶元数据。为此，请选择表上方的刷新
()。
该信息图标表示存储桶是在过去 24 小时内创建的，可能是在 Macie 上次作为每日刷新周期的一部分从 Amazon S3 检索存储桶和对象元数据之后创建的。有关更多信息，请参阅 数据刷新。

如果表中存储桶名称旁边显示警告图标
()，
则不允许 Macie 访问该存储桶或存储桶的对象。Macie 只能提供有关存储桶的信息子集，如存储桶的名称。这意味着作业将无法分析存储桶中的对象。要调查该问题，请在 Amazon S3 中查看存储桶的策略和权限设置。例如，存储桶可能具有限制性的存储桶策略。有关更多信息，请参阅 允许 Macie 访问 S3 存储桶和对象。

要自定义清单视图并更轻松地查找特定存储桶，您可以通过在筛选框中输入筛选条件来筛选表。下表提供了一些示例。

要显示所有存储桶……	应用此筛选条件……
归特定账户所有	账户 ID = *### 12 ### ID*
可公开访问	有效权限 = 公共
不包含在任何定期作业中	由作业主动监控 = False
不包括在任何定期或一次性作业中	在作业中定义 = False
有一个特定标签键*	Tag key = *###*
有一个特定标签值*	Tag value = *###*
包含未加密对象（或使用客户端加密）	加密对象计数为未加密和从 = 1

* 标签键和值区分大小写。此外，您必须在筛选条件中为这些字段指定一个完整的有效值。您不能指定部分值或使用通配符。

要显示存储桶的详细信息，请选择存储桶名称并参阅详细信息面板。您还可以在此页面上：

- 通过为字段选择一个放大镜来透视和深入查看某些字段。选择
  
  显示具有相同值的存储桶，或者选择
  
  显示具有其他值的存储桶。
- 检索存储桶中对象的最新元数据。如果您最近创建了一个存储桶或在过去 24 小时内对存储桶的对象进行了重大更改，这可能会很有帮助。要检索数据，请在面板的对象统计信息部分中选择刷新
  ()。
  此选项适用于所包含对象数量不超过 30,000 的存储桶。

指定 S3 存储桶条件

如果您选择为作业指定存储桶条件，Macie 会提供用于定义和测试条件的选项。这些是运行时标准，用于确定哪些 S3 存储桶包含供作业分析的对象。每次运行作业时，它都会识别符合条件的存储桶，然后

分析相应存储桶中的对象。如果您是某个组织的 Macie 管理员，则这包括组织中成员账户所拥有的存储桶。

定义存储桶条件

存储桶条件由一个或多个派生自 S3 存储桶属性的条件组成。每个条件，也称为标准，由以下部分组成：

- 基于属性的字段，例如账户 ID或有效权限。
- 运算符，等于 (eq) 或不等于 (neq)。
- 一个或多个值。
- 包含或排除语句，用于指示您是希望进行作业分析（包含）还是跳过（排除）符合条件的存储桶。

如果您为一个字段指定多个值，Macie 会使用 OR 逻辑来联接这些值。如果您为某个标准指定多个条件，Macie 会使用 AND 逻辑来联接这些条件。此外，排除条件优先于包含条件。例如，如果包含可公开访问的存储桶并排除具有特定标签的存储桶，则该作业会分析任何可公开访问的存储桶中的对象，除非该存储桶具有指定标签之一。

您可以为 S3 存储桶定义从以下任何基于属性的字段中派生的条件。

账户 ID

拥有存储桶的 AWS 账户 的唯一标识符(ID)。若要为此字段指定多个值，请输入每个账户的 ID，并用逗号分隔每个条目。

请注意，Macie 不支持在此字段中使用通配符或部分值。

Bucket name（桶名称）

存储桶的名称。此字段与 Amazon S3 中的名称字段相关联，而不是 Amazon 资源名称（ARN）字段。若要为此字段指定多个值，请输入每个存储桶的名称，并用逗号分隔每个条目。

注意，值区分大小写。此外，Macie 不支持在此字段中使用通配符或部分值。

有效的权限

指定存储桶是否可公开访问。您可以为此字段选择以下一个或多个值：

- 非公开 – 公众对存储桶没有读写权限。
- 公开 – 公众对存储桶拥有读写权限。
- 未知 – Macie 无法评测存储桶的公共访问设置。

为了确定存储桶的此值，Macie 分析了存储桶的账户级和存储桶级设置的组合：账户的阻止公共访问设置；存储桶的阻止公共访问设置；存储桶的存储桶策略；以及存储桶的访问控制列表(ACL)。

共享访问

指定存储桶是否与其他 AWS 账户、Amazon CloudFront 来源访问身份(OAI) 或 CloudFront 来源访问控制 (OAC) 共享。您可以为此字段选择以下一个或多个值：

- 外部 – 该存储桶与以下一个或多个或以下任意组合共享：CloudFront OAI、CloudFront OAC 或组织外部(不属于组织)的账户。
- 内部 – 存储桶与组织内部（一部分）的一个或多个账户共享。它不与 CloudFront OAI 或 OAC 共享。
- 未共享 – 存储桶不会与其他账户、CloudFront OAI 或 CloudFront OAC 共享。
- 未知 – Macie 无法评测存储桶的共享访问权限设置。

为了确定某个存储桶是否与其他 AWS 账户 共享，Macie 会分析该存储桶的存储桶策略和 ACL。此外，组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。有关共享存储桶的 Amazon S3 选项的信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的标识和访问权限管理。

为了确定存储桶的共享对象是 CloudFront OAI 还是 OAC 共享，Macie 会分析该存储桶的策略。CloudFront OAI 或 OAC 允许用户通过一个或多个指定的 CloudFront 分配访问存储桶的对象。有关 CloudFront OAI 和 OAC 的信息，请参阅 Amazon CloudFront 开发者指南中的限制对 Amazon S3 源的访问。

标签

与存储桶关联的标签。标签是您可以定义并分配给某些类型的 AWS 资源（包括 S3 存储桶）的标签。每个标签都包含一个必需的标签键和一个可选的标签值。有关标记 S3 存储桶的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用成本分配 S3 存储桶标签。

对于敏感数据发现作业，您可以使用此类条件来包含或排除具有特定标签键、特定标签值或特定标签键和标签值（成对）的存储桶。例如：

- 如果您指定 **`Project`** 为标签键，但未为条件指定任何标签值，那么任何具有 Project 标签键的存储桶都符合条件的标准，而不考虑与该标签键相关联的标签值。
- 如果您指定 **`Development`** 和 **`Test`** 为标签值，并且没有为条件指定任何标签键，则任何具有 **`Development`** 或 **`Test`** 标签值的存储桶都符合条件的标准，而不考虑与这些标签值关联的标签键。

若要在一个条件中指定多个标签键，请在键字段中输入每个标签键，并用逗号分隔每个条目。若要在一个条件中指定多个标签值，请在值字段中输入每个标签值，并用逗号分隔每个条目。

请注意，标签键和值区分大小写。此外，Macie 不支持在标签条件中使用通配符或部分值。

测试存储桶条件

在定义存储桶条件时，您可以通过预览结果来测试和完善该条件。为此，请展开控制台上条件下方显示的预览条件结果部分。此部分显示当前符合标准的所有存储桶的表。

该表还提供了作业可在每个存储桶中分析的数据量的详细信息 - 可分类对象是指使用支持的 Amazon S3 存储类且具有支持的文件或存储格式文件扩展名的对象。该表还会显示是否已将任何现有作业配置为定期分析存储桶中的对象。

在此表格中：

- 敏感度 - 如果您的账户启用了自动敏感数据发现，则显示存储桶当前敏感度分数。
- 可分类对象 - 指定作业可在一个存储桶中分析的对象总数。
- 可分类大小 - 指定作业可在一个存储桶中分析的所有对象的总存储大小。

  如果存储桶包含压缩对象，则该值并不反映这些对象解压后的实际大小。如果为存储桶启用了版本控制，则此值基于存储桶中每个对象的最新版本的存储大小。
- 由作业监控 – 指示是否将任何现有作业配置为每天、每周或每月定期分析存储桶中的对象。

  如果此字段的值为是，则表示该存储桶已显式包含在定期作业中，或者该存储桶在过去 24 小时内符合定期作业的条件。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。

如果存储桶名称旁边显示警告图标
(⚠)，
则不允许 Macie 访问该存储桶或存储桶的对象。Macie 只能提供有关存储桶的信息子集，如存储桶的名称。这意味着作业将无法分析存储桶中的对象。要调查该问题，请在 Amazon S3 中查看存储桶的策略和权限设置。例如，存储桶可能具有限制性的存储桶策略。有关更多信息，请参阅 允许 Macie 访问 S3 存储桶和对象。

要细化作业的存储桶条件，请使用筛选条件选项在条件中添加、更改或删除条件。然后，Macie 会更新表格以反映您的更改。

包括现有 S3 对象

您可以使用敏感数据发现作业对 S3 存储桶中的对象执行持续的增量分析。如果您将作业配置为定期运行，Macie 会自动为您执行此操作 - 每次运行将仅分析在上一次运行后创建或更改过的对象。使用包括现有对象选项，您可以选择第一个增量的起点：

- 要在完成创建作业后立即分析所有现有对象，请选中此选项的复选框。
- 若要等待并仅分析那些在创建作业后和首次运行前创建或更改的对象，请清除此选项的复选框。

  如果您已经分析了数据并希望继续定期对其进行分析，则清除此复选框会很有帮助。例如，如果您以前使用其他服务或应用程序对数据进行分类，而最近又开始使用 Macie，则可以使用此选项来确保持续发现和分类数据，而不会产生不必要的成本或重复分类数据。

定期作业的每次后续运行将仅自动分析在上一次运行之后创建或更改过的对象。

对于定期作业和一次性作业，您还可以将作业配置为仅分析在特定时间之前或之后或特定时间范围内创建或更改的对象。为此，请添加使用对象上次修改日期的对象条件。

采样深度

使用此选项，您可以指定在运行敏感数据发现作业时希望 Macie 分析的符合条件的 S3 对象的百分比。符合条件的对象包括：使用支持的 Amazon S3 存储类、具有支持的文件或存储格式的文件扩展名以及符合您为作业指定的其他条件的对象。

如果此值小于 100%，Macie 会随机选择要分析的合格对象，最多可达指定的百分比，并分析这些对象中的所有数据。例如，如果您将某个作业配置为分析 10,000 个对象，并将采样深度指定为 20%，则该作业将分析约 2,000 个随机选择的符合条件的对象。

减少作业的采样深度可降低成本并缩短作业的持续时间。如果对象中的数据高度一致，并且您希望确定 S3 存储桶（而不是每个对象）是否包含敏感数据，这将非常有用。

请注意，此选项控制的是所分析对象的百分比，而不是所分析的字节百分比。如果您输入的采样深度小于 100%，Macie 会分析每个选定对象中的所有数据，而不是每个选定对象中数据的百分比。

S3 对象条件

要微调敏感数据发现作业的范围，您还可以定义自定义条件，以确定 Macie 在作业分析中包含或排除哪些 S3 对象。这些条件由一个或多个派生自 S3 对象的条件组成。这些条件适用于作业配置为分析的所有 S3 存储桶中的对象。如果一个存储桶中包含对象的多个版本，则条件适用于该对象的最新版本。

如果您将多个条件定义为对象条件，则 Macie 会使用 AND 逻辑来联接条件。此外，排除条件优先于包含条件。例如，如果包含文件扩展名为 .pdf 的对象并排除大于 5 MB 的对象，则作业会分析任何文件扩展名为 .pdf 的对象，除非该对象大于 5 MB。

您可以定义从 S3 对象的以下任何属性派生的条件。

文件扩展名

这与 S3 对象的文件扩展名相关。您可以使用此类条件根据文件类型来包含或排除对象。若要对多种类型的文件执行此操作，请输入每种类型的文件扩展名，并用逗号分隔每个条目，例如：**docx,pdf,xlsx**。如果您输入多个文件扩展名作为条件的值，则 Macie 会使用 OR 逻辑来联接这些值。

注意，值区分大小写。此外，Macie 不支持在此类条件下使用部分值或通配符。

有关 Macie 可分析的文件类型的信息，请参阅 支持的文件和存储格式。

上次修改时间

这与 Amazon S3 中的上次修改时间字段相关。在 Amazon S3 中，此字段存储创建或上次更改 S3 对象的日期和时间，以最新日期为准。

对于敏感数据发现作业，此条件可以是特定日期、特定日期和时间或独占时间范围：

- 若要分析在特定日期或日期和时间之后最后一次修改的对象，请在从字段中输入值。
- 若要分析在特定日期或日期和时间之前最后一次修改的对象，请在至字段中输入值。
- 若要分析在特定时间范围内最后一次修改的对象，请使用从字段输入时间范围内的第一个日期或日期和时间的值。使用至字段输入时间范围内的最后日期或日期和时间的值。
- 若要分析某一天中最后一次修改的对象，请在从日期字段中输入日期。在至日期字段中输入第二天的日期。然后确认两个时间字段均为空。(Macie 将空白时间字段视为 `00:00:00`。) 例如，要分析在 2022 年 8 月 9 日更改的对象，请在从日期字段中输入 **2022/08/09**，在至日期字段中输入 **2022/08/10**，请勿在任一时间字段中输入值。

以世界协调时间(UTC)输入任意时间值，并使用 24 小时制表示法。

前缀

这与 Amazon S3 中的键字段相关。在 Amazon S3 中，此字段存储 S3 对象的名称，包括该对象的前缀。前缀类似于存储桶中的目录路径。它使您能够将相似的对象分组在一个存储桶中，就像您可以将相似的文件一起存储在文件系统上的一个文件夹中一样。有关 Amazon S3 中对象前缀和文件夹的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用文件夹在 Amazon S3 控制台中组织对象。

您可以使用此类条件来包含或排除其键（名称）以特定值开头的对象。例如，要排除其键以AWSLogs开头的所有对象，请输入 **AWSLogs** 作为前缀条件的值，然后选择排除。

如果您输入多个前缀作为条件的值，则 Macie 会使用 OR 逻辑来联接这些值。例如，如果您输入 **AWSLogs1** 和 **AWSLogs2** 作为条件的值，则其键以 AWSLogs1 或 AWSLogs2 开头的任何对象都符合该条件的标准。

在为前缀条件输入值时，请注意以下几点：

- 值区分大小写。
- Macie 不支持在这些值中使用通配符。
- 在 Amazon S3 中，对象的键不包括包含该对象的存储桶的名称。因此，请勿在这些值中指定存储桶名称。
- 如果前缀包含分隔符，则在该值中包含分隔符。例如，输入 **AWSLogs/eventlogs** 可为其键以 AWSLogs/eventlogs 开头的所有对象定义条件。Macie 支持默认的 Amazon S3 分隔符（即斜杠 (/)）和自定义分隔符。

另请注意，仅当对象的键与您输入的值（从对象键中的第一个字符开始）完全匹配时，该对象才符合条件的标准。此外，Macie 会对对象的完整键值应用一个条件，包括该对象的文件名。

例如，如果对象的键为 AWSLogs/eventlogs/testlog.csv，并且您为条件输入了以下任意值，则该对象符合条件的标准：

- **AWSLogs**
- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

但是，如果您输入 **eventlogs**，则该对象不符合条件，条件的值不包括键的第一部分（AWSLogs/）。同样，如果您输入 **awslogs**，由于大小写差异，该对象也不符合条件。

存储大小

这与 Amazon S3 中的大小字段相关。在 Amazon S3 中，此字段指示 S3 对象的总存储大小。如果对象是压缩文件，则此值不反映文件解压后的实际大小。

您可以使用此类条件来包含或排除小于特定大小、大于特定大小或位于特定大小范围内的对象。Macie 将此类条件应用于所有类型的对象，包括压缩或存档文件及其包含的文件。有关每种支持格式基于大小的限制信息，请参阅 Amazon Macie 限额。

标签

与 S3 对象关联的标签。标签是您可以定义并分配给某些类型的 AWS 资源（包括 S3 对象）的标签。每个标签都包含一个必需的标签键和一个可选的标签值。有关标记 S3 对象的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用标签对存储进行分类。

对于敏感数据发现作业，您可以使用此类条件来包含或排除具有特定标签的对象。这可以是特定的标签键，也可以是特定的标签键和标签值（成对）。如果您指定多个标签作为条件的值，则 Macie 会使用 OR 逻辑来联接这些值。例如，如果您指定 **`Project1`** 和 **`Project2`** 作为条件的标签键，则任何具有Project1或Project2标签键的对象都将符合该条件的标准。

请注意，标签键和值区分大小写。此外，Macie 不支持在此类条件下使用部分值或通配符。

创建敏感数据发现作业

借助 Amazon Macie，您可以创建和运行敏感数据发现作业，以自动发现、记录和报告 Amazon Simple Storage Service (Amazon S3) 存储桶中的敏感数据。敏感数据发现作业是 Macie 执行的一系列自动处理和分析任务，用于检测和报告 Amazon S3 对象中的敏感数据。随着分析的进行，Macie 会提供有关其发现的敏感数据及其执行的分析的详细报告：敏感数据调查发现，用于报告 Macie 在单个 S3 对象中发现的敏感数据，以及敏感数据发现结果（记录有关单个 S3 对象分析的详细信息）。有关更多信息，请参阅 查看作业统计数据和结果。

创建作业时，首先要指定哪些 S3 存储桶包含您希望 Macie 在作业运行时分析的对象，即您选择的特定存储桶或符合特定标准的存储桶。然后，您可以指定运行作业的频率，即每天、每周或每月运行一次，或者定期运行一次。您也可以选择选项来优化作业的分析范围。这些选项包括派生自 S3 对象属性的自定义标准，例如标签、前缀以及对象上次修改时间。

定义作业的时间表和范围后，您可以指定希望作业使用的托管数据标识符和自定义数据标识符：

- 托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如信用卡号、AWS 秘密访问密钥或特定国家或地区的护照号码。这些标识符可以检测许多国家和地区的大量且不断增长的敏感数据类型列表，包括多种类型的凭证数据、财务信息和个人身份信息（PII）。有关更多信息，请参阅 使用托管数据标识符。
- 自定义数据标识符是您为检测敏感数据定义的一组标准。使用自定义数据标识符，您可以检测反映组织特定场景、知识产权或专有数据（例如员工 ID、客户账号或内部数据分类）的敏感数据。您可以补充 Macie 提供的托管数据标识符。有关更多信息，请参阅 构建自定义数据标识符。

然后，您可以选择希望作业使用的允许列表。允许列表指定您希望 Macie 忽略的文本或文本模式，通常是您的特定场景或环境的敏感数据异常，例如，您组织的公开名称或电话号码，或者您的组织用于测试的示例数据。有关更多信息，请参阅 使用允许列表定义敏感数据例外。

选择完这些选项后，就可以输入作业的常规设置了，例如作业的名称和说明。然后，您可以查看并保存作业。

任务

- 开始前的准备工作
- 第 1 步：选择 S3 存储桶
- 第 2 步：检查您的 S3 存储桶选择或标准
- 第 3 步：定义时间表并优化范围
- 第 4 步：选择托管数据标识符
- 第 5 步：选择自定义数据标识符
- 第 6 步：选择允许列表
- 第 7 步：输入常规设置
- 第 8 步：审核并创建

开始前的准备工作

创建作业之前，最好执行以下步骤：

- 请检查您是否将 Macie 配置为将敏感数据发现结果存储在 S3 存储桶中。为此，请在 Amazon Macie 控制台的导航窗格中选择发现结果。然后验证您输入了设置。要了解这些设置，请参阅 存储和保留敏感数据发现结果。
- 创建希望作业使用的任何自定义数据标识符。要了解如何操作，请参阅 构建自定义数据标识符。
- 创建您希望作业使用的任何允许列表。要了解如何操作，请参阅 创建和管理允许列表。
- 如果要分析加密的 S3 对象，请确保 Macie 可以访问和使用相应的加密密钥。有关更多信息，请参阅 分析加密 S3 对象。
- 如果您要分析具有限制性存储桶策略的 S3 存储桶中的对象，请确保允许 Macie 访问这些对象。有关更多信息，请参阅 允许 Macie 访问 S3 存储桶和对象。

如果您在创建作业之前执行这些操作，则可以简化作业的创建并有助于确保作业可以分析所需的数据。

第 1 步：选择 S3 存储桶

创建作业的第一步是指定哪些 S3 存储桶包含您希望 Macie 在作业运行时分析的对象。您有两个选项来执行此步骤：

- 选择特定存储桶 – 使用此选项，您可以显式选择希望作业分析的每个 S3 存储桶。然后，当作业运行时，它仅分析您所选存储桶中的对象。
- 指定存储桶标准 – 使用此选项，您可以定义运行时标准来确定作业分析哪些 S3 存储桶。标准由一个或多个派生自 S3 存储桶属性的条件组成。当作业运行时，它会识别符合标准的存储桶，然后分析这些存储桶中的对象。

有关这些选项的详细信息，请参阅 作业的范围选项。

以下各节提供了选择和配置每个选项的说明。选择所需选项的部分。

选择特定存储桶

如果您选择显式选择要进行作业分析的每个 S3 存储桶，Macie 会为您提供当前 AWS 区域 中存储桶的完整清单。然后，您可以使用此清单为作业选择一个或多个存储桶进行分析。要了解此清单，请参阅选择特定 S3 存储桶。

如果您是某个组织的 Macie 管理员，则清单中会包含组织中成员账户所拥有的存储桶。您可以将作业配置为分析多达 1,000 个此类存储桶中的对象，跨越多达 1,000 个账户。

为作业选择特定的存储桶

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 请选择 Create job (创建作业)。
4. 在选择 S3 存储桶页面上，选择选择特定存储桶。Macie 会显示您账户在当前区域中的所有存储桶的表格。
5. 在选择 S3 存储桶部分，可以选择刷新
   ()，
   从 Amazon S3 检索最新的存储桶元数据。

   如果信息图标
   ()
   出现在任何存储桶名称旁边，我们建议您这样操作。此图标表明存储桶是在过去 24 小时内创建

的，可能是 Macie 在每日刷新周期中最后一次从 Amazon S3 检索存储桶和对象元数据之后创建的。

6. 在表中，选中希望作业分析的每个存储桶对应的复选框。

> **Tip**
>
> - 要更轻松地查找特定存储桶，请在表格上方的筛选框中输入筛选标准。您还可以通过选择列标题对表格进行排序。
> - 要确定您是否已将作业配置为定期分析存储桶中的对象，请参阅按作业监控字段。如果此字段显示是，存储桶已显式包含在定期作业中，或者该存储桶在过去 24 小时内符合定期作业的标准。此外，其中至少有一个作业的状态非已取消。Macie 每天都会更新这些数据。
> - 要确定现有定期或一次性作业最近一次分析存储桶中的对象的时间，请参阅最新作业运行字段。有关该作业的更多信息，请参阅存储桶的详细信息。
> - 要显示存储桶的详细信息，请选择存储桶的名称。除了与作业相关的信息外，详细信息面板还提供有关存储桶的统计数据和其他信息，例如存储桶的公共访问设置。要详细了解此数据，请参阅 查看 S3 存储桶清单。

7. 选择完存储桶后，选择下一步。

在下一步中，您将检查并验证您的选择。

指定存储桶标准

如果您选择指定运行时标准来确定作业分析哪些 S3 存储桶，Macie 会提供一些选项来帮助您为标准中的各个条件选择字段、运算符和值。要了解有关这些选项的更多信息，请参阅 指定 S3 存储桶条件。

为作业指定存储桶标准

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 请选择 Create job (创建作业)。
4. 在选择 S3 存储桶页面上，选择指定存储桶标准。
5. 在指定存储桶标准下，执行以下操作以向标准添加条件：

   a. 将光标置于筛选框中，然后选择要用于条件的存储桶属性。

b. 在第一个框中，为条件选择一个运算符等于或不等于。

c. 在下一个框中，为该属性输入一个或多个值。

根据存储桶属性的类型和性质，Macie 会显示不同的值输入选项。例如，如果您选择有效权限属性，Macie 会显示一个值列表供您选择。如果您选择账户 ID 属性，Macie 会显示一个文本框，您可以在其中输入一个或多个 AWS 账户 ID。要在文本框中输入多个值，请输入每个值并用逗号分隔每个条目。

d. 选择 Apply（应用）。Macie 添加条件并将其显示在筛选框下方。

默认情况下，Macie 使用包含语句添加条件。这意味着作业配置为分析（包含）存储桶中符合条件的对象。要跳过（排除）符合条件的存储桶，请为条件选择包含，然后选择排除。

e. 对要添加到标准的每个其他条件重复上述步骤。

6. 要测试您的标准，请展开预览标准结果部分。此部分显示当前符合标准的所有存储桶的表。

7. 要优化标准，请执行以下任一操作：

- 要移除条件，请选择条件的 X。
- 要更改条件，请通过为条件选择 X 来移除该条件。然后添加具有正确设置的条件。
- 要移除所有条件，请选择清除筛选条件。

Macie 会更新标准结果表以反映您的更改。

8. 指定完存储桶标准后，选择下一步。

在下一步中，您将检查并验证您的标准。

第 2 步：检查您的 S3 存储桶选择或标准

在此步骤中，请验证您在上一步中选择的设置是否正确：

- 查看您的存储桶选择 - 如果您为作业选择了特定的 S3 存储桶，请查看存储桶表并根据需要更改存储桶选择。该表提供了对作业分析的预计范围和成本的深入了解。数据基于当前存储在存储桶中的对象的大小和类型。

  在表中，估计成本字段表示分析 S3 存储桶中对象的估计成本总额（以美元计）。每个估计值都反映了作业将在存储桶中分析的预计未压缩数据量。如果有任何对象是压缩文件或存档文件，则该估计假设这些文件使用 3:1 的压缩比，并且作业可以分析所有提取的文件。有关更多信息，请参阅 预测和监控作业成本。

- 查看您的存储桶标准 - 如果您为作业指定了存储桶标准，请查看条件中的每个条件。要更改标准，请选择上一步，然后使用上一步中的筛选选项输入正确的标准。完成后，选择 Next (下一步)。

完成对设置的查看和验证后，选择下一步。

第 3 步：定义时间表并优化范围

在此步骤中，您可以指定运行作业的频率，即每天、每周或每月运行一次，或者定期运行一次。您也可以选择各种选项来优化作业的分析范围。要了解有关这些选项的信息，请参阅 作业的范围选项。

定义时间表并优化作业范围

1. 在优化范围页面上，指定您希望作业运行的频率：

   - 要仅运行一次作业，请在完成创建作业后立即选择一次性作业。
   - 要定期运行作业，请选择计划作业。对于更新频率，选择是每天、每周还是每月运行作业。然后使用包含现有对象选项来定义作业首次运行的范围：
     - 选中此复选框可在创建作业后立即分析现有的对象。每次后续运行将仅分析在上一次运行之后创建或更改过的对象。
     - 清除此复选框可跳过对现有对象的分析。此作业的第一次运行仅分析在完成作业创建之后和第一次运行开始之前创建或更改的对象。每次后续运行将仅分析在上一次运行之后创建或更改过的对象。

       如果您已经分析了数据并希望继续定期对其进行分析，则清除此复选框会很有帮助。例如，如果您以前使用其他服务或应用程序对数据进行分类，而最近又开始使用 Macie，则可以使用此选项来确保持续发现和分类数据，而不会产生不必要的成本或重复分类数据。
2. （可选）要指定您希望作业分析的对象的百分比，请在采样深度框中输入该百分比。

   如果此值小于 100%，Macie 会随机选择要分析的对象，最多可达指定的百分比，并分析这些对象中的所有数据。默认值为 100%。
3. （可选）要添加确定作业分析中包含或排除哪些 S3 对象的特定标准，请展开其他设置部分，然后输入标准。这些标准由派生自 S3 对象属性的单个条件组成：

   - 要分析（包括）满足特定条件的对象，请输入条件类型和值，然后选择包括。
   - 要分析（排除）满足特定条件的对象，请输入条件类型和值，然后选择排除。

   对所需的每个包括或排除条件重复此步骤。

如果您输入多个条件，则任何排除条件优先于包括条件。例如，如果包括文件扩展名为 .pdf 的对象并排除大于 5 MB 的对象，则作业会分析任何文件扩展名为 .pdf 的对象，除非该对象大于 5 MB。

4. 完成后，选择 Next (下一步)。

第 4 步：选择托管数据标识符

在此步骤中，请指定希望作业在分析 S3 对象时使用的托管数据标识符。您有两种选择：

- 使用推荐的设置 - 使用此选项，作业将使用我们为作业推荐的一组托管数据标识符来分析 S3 对象。该组用于检测常见的敏感数据类别和类型。要查看该组中当前的托管数据标识符列表，请参阅 推荐用于作业的托管数据标识符。每次在组中添加或移除托管数据标识符时，我们都会更新该列表。
- 使用推荐的设置 - 使用此选项，作业将使用您选择的托管数据标识符来分析 S3 对象。这可以是当前可用的全部托管数据标识符，也可以仅为部分托管数据标识符。您也可以将作业配置为不使用任何托管数据标识符。相反，该作业只能使用您在下一步中选择的自定义数据标识符。要查看当前可用的托管数据标识符列表，请参阅 快速参考：Amazon Macie 托管数据标识符。每次发布新的托管数据标识符时，我们都会更新该列表。

选择任一选项时，Macie 都会显示托管数据标识符表。在表中，敏感数据类型字段指定了托管数据标识符的唯一标识符 (ID)。此 ID 描述了托管数据标识符旨在检测的敏感数据类型，例如：美国护照号码的 USA_PASSPORT_NUMBER、信用卡号的 CREDIT_CARD_NUMBER 和 PGP 私钥的 PGP_PRIVATE_KEY。要更快地找到特定的标识符，您可以按敏感数据类别或类型对表格进行排序和筛选。

为作业选择托管数据标识符

1. 在选择托管数据标识符页面的托管数据标识符选项下，执行以下操作之一：

   - 要使用我们为作业推荐的一组托管数据标识符，请选择推荐。

     如果您选择此选项并将作业配置为多次运行，则每次运行都会自动使用运行开始时推荐组中的所有托管数据标识符。这包括我们发布并添加到组中的新的托管数据标识符。它不包括我们从组中移除的托管数据标识符，不再推荐用于作业。

   - 要仅使用您选择的特定托管数据标识符，请选择自定义，然后选择使用特定的托管数据标识符。然后，在表中选中选择希望作业使用的每个托管数据标识符的复选框。

如果您选择此选项并将作业配置为多次运行，则每次运行仅使用您选择的托管数据标识符。换句话说，作业每次运行时都使用这些相同的托管数据标识符。

- 使用 Macie 当前提供的所有托管数据标识符，请选择自定义，然后选择使用特定的托管数据标识符。然后，在表格中，选中选择列标题中的复选框以选择所有行。

  如果您选择此选项并将作业配置为多次运行，则每次运行仅使用您选择的托管数据标识符。换句话说，作业每次运行时都使用这些相同的托管数据标识符。

- 要不使用任何托管数据标识符而仅使用自定义数据标识符，请选择自定义，然后选择不使用任何托管数据标识符。然后，在下一步中，选择要使用的自定义数据标识符。

2. 完成后，选择 Next (下一步)。

第 5 步：选择自定义数据标识符

在此步骤中，选择您希望作业在分析 S3 对象时使用的任何自定义数据标识符。除了配置作业要使用的任何托管数据标识符外，作业还将使用选定的标识符。要了解有关自定义数据标识符的更多信息，请参阅 构建自定义数据标识符。

为作业选择自定义数据标识符

1. 在选择自定义数据标识符页面上，选中希望作业使用的每个自定义数据标识符的复选框。您可以选择多达 30 个自定义数据标识符。

   > **Tip**
   >
   > 要在选择自定义数据标识符之前查看或测试其设置，请选择该标识符名称旁边的链接图标 ( )。Macie 会打开一个显示标识符设置的页面。
   > 您还可以使用此页面通过示例数据测试标识符。为此，请在示例数据框中输入最多包含 1,000 个字符的文本，然后选择测试。Macie 使用标识符评测示例数据，然后报告匹配项的数量。

2. 选择完自定义数据标识符后，选择下一步。

第 6 步：选择允许列表

在此步骤中，选择您希望作业在分析 S3 对象时使用的任何允许列表。要了解有关允许列表的更多信息，请参阅 使用允许列表定义敏感数据例外。

为作业选择允许列表

1. 在选择允许列表页面上，选择您希望作业使用的每个允许列表的复选框。您可以选择多达 10 个列表。

   > **Tip**
   >
   > 要在选择允许列表之前查看其设置，请选择列表名称旁边的链接图标 ( )。Macie 会打开一个显示列表设置的页面。
   >
   > 如果列表指定了正则表达式 (regex)，您也可以使用此页使用示例数据测试正则表达式。为此，请在示例数据框中输入最多包含 1,000 个字符的文本，然后选择测试。Macie 使用正则表达式评测示例数据，然后报告匹配项的数量。

2. 选择完允许列表后，选择下一步。

第 7 步：输入常规设置

在此步骤中，请指定作业的名称和（可选）的作业说明。

您也可以为作业分配标签。标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

输入作业的常规设置

1. 在输入常规设置页面上，在作业名称框中输入作业的名称。名称最多可以包含 500 个字符。
2. （可选）对于作业说明，输入作业的简短说明。说明最多可以包含 200 个字符。
3. （可选）在标签下，选择添加标记，然后最多可输入 50 个标签来分配给作业。
4. 完成后，选择 Next (下一步)。

第 8 步：审核并创建

在最后一步中，检查作业的配置设置并验证设置是否正确。这是非常重要的一步。创建作业后，您无法更改任何设置。这有助于确保您拥有敏感数据调查发现和发现结果的不可变历史记录，以便您执行数据隐私和保护的审计或调查。

根据作业的设置，您还可以查看一次运行作业的总估计成本（以美元计）。如果您为作业选择了特定的 S3 存储桶，则估计值将基于所选存储桶中对象的大小和类型，以及该作业可以分析的数据量。如果您为作业指定了存储桶标准，则估计值将基于多达 500 个存储桶中当前符合标准的对象的大小和类型，以及该作业可以分析的数据量。要了解此估计值，请参阅 预测和监控作业成本。

审核和创建作业

1. 在查看并创建页面上，查看每项设置并验证其是否正确。要更改设置，选择包含该设置的部分中的编辑，然后输入正确的设置。您也可以使用导航选项卡转到包含设置的页面。
2. 验证完设置后，选择提交以创建并保存作业。Macie 会检查设置并通知您任何需要解决的问题。

> **Note**
>
> 如果您尚未为敏感数据发现结果配置存储库，Macie 会显示警告，并且不会保存作业。要解决此问题，请在敏感数据发现结果的存储库部分中选择配置。然后输入存储库的配置设置。要了解如何操作，请参阅 存储和保留敏感数据发现结果。输入设置后，返回到查看并创建页面，然后在该页面的敏感数据发现结果的存储库部分中选择刷新（ ）。
>
> 虽然我们不建议这样做，但您可以暂时覆盖存储库要求并保存作业。如果您这样做，您就有可能丢失作业中的发现结果 — Macie 只会将结果保留 90 天。要暂时覆盖该要求，请选中改写选项对应的复选框。

3. 如果 Macie 通知您要解决的问题，请解决这些问题，然后再次选择提交以创建并保存作业。

如果您将作业配置为运行一次、每天运行或者在每周或每月的当前日期运行，Macie 将会在您保存之后，立即开始运行该作业。否则，Macie 会准备在每周或每月中的指定日期运行作业。要监控作业，您可以检查作业的状态。

查看敏感数据发现作业的统计数据和结果

当您运行敏感数据发现作业时，Amazon Macie 会自动计算并报告该作业的某些统计数据。例如，Macie 会报告作业运行的次数以及该作业在当前运行期间尚未处理的 Amazon Simple Storage Service (Amazon S3) 对象的大致数量。Macie 还会为该作业生成多种类型的结果：日志事件、敏感数据调查发现和敏感数据发现结果。

主题

- 敏感数据发现作业的结果类型

- 查看敏感数据发现作业的统计数据和结果

敏感数据发现作业的结果类型

随着敏感数据发现作业的进行，Amazon Macie 会为该作业生成以下类型的结果。

日志事件

这是作业运行时发生的事件的记录。Macie 会自动将某些事件的数据记录并发布到 Amazon CloudWatch Logs。这些日志中的数据提供了作业进度或状态变化的记录，例如作业开始或停止运行的确切日期和时间。这些数据还提供了有关作业运行时发生的任何账户或存储桶级错误的详细信息。

日志事件可以帮助您监控作业，并解决任何阻碍该作业分析所需数据的问题。如果作业使用运行时标准来确定要分析哪些 S3 存储桶，则日志事件还可以帮助您确定作业运行时是否符合标准以及哪些 S3 存储桶符合标准。

您可以使用 Amazon CloudWatch 控制台或 Amazon CloudWatch Logs API 访问日志事件。为了帮助您导航到作业的日志事件，Amazon Macie 控制台提供了指向这些事件的链接。有关更多信息，请参阅 监控作业。

敏感数据调查发现

这是 Macie 在 S3 对象中发现的敏感数据的报告。每项调查发现都会提供严重性评级和详细信息，如：

- Macie 发现敏感数据的日期与时间。
- Macie 发现敏感数据的类别和类型。
- Macie 发现的每种敏感数据的出现次数。
- 生成调查发现的作业的唯一标识符。
- 受影响的 S3 存储桶和对象的名称、公开访问设置、加密类型和其他信息。

根据受影响 S3 对象的文件类型或存储格式，详细信息还可能包括 Macie 发现的、多达 15 处敏感数据的位置。为了报告位置数据，敏感数据调查发现使用标准化的 JSON 架构。

敏感数据调查发现不包括 Macie 发现的敏感数据。相反，它提供了用于进一步调查和必要补救的信息。

Macie 会将敏感数据调查发现存储 90 天。您可以使用 Amazon Macie 控制台或 Amazon Macie API 访问它们。您还可以使用其他应用程序、服务和系统，监控和处理它们。有关更多信息，请参阅 分析调查发现。

敏感数据发现结果

这是记录有关 S3 对象分析详细信息的记录。Macie 会自动为您配置作业进行分析的每个对象创建敏感数据发现结果。这包括 Macie 在其中没有发现敏感数据、因而不会产生敏感数据调查发现的对象，以及 Macie 因错误或问题（例如，权限设置或使用不受支持的文件或存储格式）而无法分析的对象。

如果 Macie 在 S3 对象中发现敏感数据，则敏感数据发现结果将包含来自相应敏感数据调查发现的数据。它还提供了其他信息，例如 Macie 在对象中发现的每种敏感数据出现多达 1000 次的位置。例如：

- Microsoft Excel 工作簿、CSV 文件或 TSV 文件中单元格或字段的列号和行号
- JSON 或 JSON Lines 文件中的字段或数组路径
- 除 CSV、JSON、JSON Lines 或 TSV 文件之外的非二进制文本文件中的行号，例如 HTML、TXT 或 XML 文件。
- Adobe 可移植文档格式 (PDF) 文件中页面的页码
- Apache Avro 对象容器或 Apache Parquet 文件中记录的字段的记录索引和路径

如果受影响的 S3 对象是存档文件（如 .tar 或 .zip 文件），则敏感数据发现结果还会提供 Macie 从存档中提取的单个文件中敏感数据出现的详细位置数据。Macie 不会在存档文件的敏感数据调查发现中包含此信息。为了报告位置数据，敏感数据发现结果使用标准化 JSON 架构。

敏感数据发现结果不包括 Macie 发现的敏感数据。相反，它为您提供分析记录，有助于数据隐私和保护审计或调查。

Macie 会将您的敏感数据发现结果存储 90 天。您无法直接在 Amazon Macie 控制台或使用 Amazon Macie API 访问它们。相反，您可以配置 Macie 将其加密并存储至 S3 存储桶内。存储桶可以用作所有敏感数据发现结果的最终长期存储库。然后，您可以选择访问和查询该存储库中的结果。要了解如何配置这些设置，请参阅 存储和保留敏感数据发现结果。

配置好这些设置之后，Macie 会将敏感数据发现结果写入 JSON Lines (.jsonl) 文件，然后它加密这些文件并将其作为 GNU Zip (.gz) 文件添加至 S3 存储桶。为了帮助您导航到结果，Amazon Macie 控制台提供了指向这些结果的链接。

敏感数据调查发现和敏感数据发现结果都遵循标准化架构。这可以帮助您选择性地使用其他应用程序、服务和系统进行查询、监控和处理。

> **Tip**
>
> 有关如何查询和使用敏感数据发现结果来分析和报告潜在数据安全风险的详细说明性示例，请参阅 AWS 安全博客上的如何使用 Amazon Athena 和 Amazon QuickSight 查询和可视化 Macie 敏感数据发现结果博客文章。
> 有关可用于分析敏感数据发现结果的 Amazon Athena 查询示例，请访问 GitHub 上的 Amazon Macie Results Analytics 存储库。此存储库还提供了有关配置 Athena 以检索和解密结果的说明，以及用于为结果创建表的脚本。

查看敏感数据发现作业的统计数据和结果

要查看单个敏感数据发现作业的处理统计数据和结果，您可以使用 Amazon Macie 控制台或 Amazon Macie API。按照以下步骤，使用控制台查看作业的统计数据和结果。

要以编程方式访问作业的处理统计数据，请使用 Amazon Macie API 的 DescribeClassificationJob 操作。要以编程方式访问作业产生的调查发现，请使用 Amazon Macie API 的 ListFindings 操作，并在 `classificationDetails.jobId` 字段的筛选条件中指定该作业的唯一标识符。要了解如何操作，请参阅 创建筛选条件并将其应用于调查发现。然后，您可以使用 GetFindings 操作来检索调查发现的详细信息。

查看作业的统计数据和结果

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 在作业页面上，选择要查看其统计数据和结果的作业的名称。此详细信息面板显示有关作业的统计数据、设置和其他信息。
4. 在详细信息面板中，执行以下任一操作：

   - 要查看作业的处理统计数据，请参阅面板的统计数据部分。此部分显示统计数据，例如作业运行的次数以及该作业在当前运行期间尚未处理的大致对象数。
   - 要查看作业的日志事件，请选择面板顶部的显示结果，然后选择显示 CloudWatch 日志。Macie 打开 Amazon CloudWatch 控制台并显示 Macie 为该作业发布的日志事件表。
   - 要查看作业生成的所有敏感数据调查发现，请选择面板顶部的显示结果，然后选择显示调查发现。Macie 会打开调查发现页面，并显示作业中的所有调查发现。然后，要查看特定调查发现的详细信息，请选择该调查发现，然后参考详细信息面板。

> **Tip**
>
> 在调查发现详细信息面板中，您可以使用详细结果位置字段中的链接导航到 Amazon S3 中相应的敏感数据发现结果：
>
> - 如果调查发现适用于大型存档或压缩文件，则该链接将显示包含该文件发现结果的文件夹。如果存档文件或压缩文件生成的发现结果超过 100 个，则该文件大。
> - 如果调查发现适用于小存档或压缩文件，则该链接将显示包含该文件发现结果的文件。如果存档文件或压缩文件生成的发现结果不超过 100 个，则该文件小。
> - 如果调查发现适用于其他类型的文件，则该链接将显示包含该文件发现结果的文件。

- 要查看作业生成的所有敏感数据发现结果，请选择面板顶部的显示结果，然后选择显示分类。Macie 打开 Amazon S3 控制台并显示包含作业所有发现结果的文件夹。只有在将 Macie 配置为将敏感数据发现结果存储在 S3 存储桶后，此选项才可用。

使用 Amazon CloudWatch Logs 监控敏感数据发现作业

除了监控敏感数据发现作业的整体状态外，您还可以监控和分析作业进行过程中发生的特定事件。您可以通过使用 Amazon Macie 自动发布到 Amazon CloudWatch Logs 的近乎实时的日志数据来做到这一点。这些日志中的数据提供了作业进度或状态变化的记录，例如作业开始或停止运行的确切日期和时间。

日志数据还提供了有关作业运行时发生的任何账户或存储桶级错误的详细信息。例如，如果 S3 存储桶的权限设置阻止作业分析存储桶中的对象，则 Macie 会记录一个事件。该事件指示错误发生的时间，它可以识别受影响的存储桶和拥有该存储桶的账户。这些类型事件的数据可以帮助您识别、调查和解决阻碍 Macie 分析所需数据的错误。

借助 Amazon CloudWatch Logs，您可以监控、存储和访问多个系统、应用程序和和AWS 服务（包括 Macie）的日志文件。您还可以查询和分析日志数据，将 CloudWatch Logs 配置为在某些事件发生或达到阈值时通知您。CloudWatch Logs 还提供用于存档日志数据和将数据导出到 Amazon S3 的功能。有关 CloudWatch Logs 的更多信息，请参阅 Amazon CloudWatch Logs 用户指南。

主题

- 敏感数据发现作业的日志工作原理
- 查看敏感数据发现作业的日志
- 敏感数据发现作业的日志事件架构
- 敏感数据发现作业的日志事件类型

敏感数据发现作业的日志工作原理

当您开始运行敏感数据发现作业时，Macie 会自动在 Amazon CloudWatch Logs 中创建和配置相应的资源，以记录当前 AWS 区域 中所有作业的事件。然后，当您的作业运行时，Macie 会自动将事件数据发布到这些资源。您的账户的 Macie 服务相关角色的权限策略允许 Macie 代表您执行这些任务。您无需采取任何步骤即可在 CloudWatch Logs 中创建或配置资源，也无需为作业记录事件数据。

在 CloudWatch Logs 中，日志按日志组进行组织。每个日志组都包含日志流。每个日志流包含日志事件。这些资源的一般用途如下：

- 日志组是具有相同保留、监控和访问控制设置的日志流的集合，例如，所有敏感数据发现作业的日志集。
- 日志流是共享同一个源的一系列日志事件，例如单个敏感数据发现作业。
- 日志事件是应用程序或资源记录的活动记录，例如，Macie 为特定的敏感数据发现作业记录和发布的单个事件。

Macie 将所有敏感数据发现作业的事件发布到一个日志组，每个作业在该日志组中有唯一的日志流。该日志组具有以下前缀和名称：

```
/aws/macie/classificationjobs
```

如果此日志组已经存在，Macie 将使用它来存储作业的日志事件。如果您的组织使用自动化配置（例如AWS CloudFormation），为作业事件创建具有预定义日志保留期、加密设置、标记、指标筛选条件等的日志组，这可能会很有用。

如果此日志组不存在，Macie 会使用 CloudWatch Logs 用于新日志组的默认设置来创建该日志组。这些设置包括永不过期的日志保留期，这意味着 CloudWatch Logs 会无限期地存储日志。要更改日志组保留期，请使用 Amazon CloudWatch 控制台或 Amazon CloudWatch Logs API。有关更多信息，请参阅《Amazon CloudWatch Logs 用户指南》中的使用日志组和日志流。

在此日志组中，Macie 会为您运行的每项首次运行的作业创建唯一的日志流。日志流的名称是作业的唯一标识符，例如`85a55dc0fa6ed0be5939d0408example`，采用以下格式。

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

每个日志流都包含 Macie 为相应作业记录和发布的所有日志事件。对于定期作业，这包括所有作业运行的事件。如果您删除定期作业的日志流，Macie 会在该作业下次运行时再次创建该日志流。如果您删除一次性作业的日志流，则无法将其恢复。

请注意，默认情况下，已为所有作业启用日志记录。您无法将其禁用或以其他方式阻止 Macie 将作业事件发布到 CloudWatch Logs。如果您不想存储日志，则可以将日志组的保留期缩短至一天。在保留期结束时，CloudWatch Logs 会自动从日志组中删除过期的事件数据。

查看敏感数据发现作业的日志

您可以使用Amazon CloudWatch 控制台或 Amazon CloudWatch Logs API 查看敏感数据发现作业的日志。控制台和 API 都提供旨在帮助您查看和分析日志数据的功能。您可以使用这些功能来处理作业的日志流和事件，就像在 CloudWatch Logs 中处理任何其他类型的日志数据一样。

例如，您可以搜索和筛选聚合数据，以识别在特定时间范围内所有作业发生的特定类型的事件。或者，您可以对特定作业发生的所有事件进行有针对性的审查。CloudWatch Logs 还提供了用于监控日志数据、定义指标筛选条件和创建自定义警报的选项。

> **Tip**
>
> 要使用 Amazon Macie 控制台导航到特定作业的日志事件，请执行以下操作：在作业页面上，选择作业名称。在详细信息面板的顶部，选择显示结果，然后选择显示 CloudWatch 日志。Macie 打开 Amazon CloudWatch 控制台并显示该作业的日志事件表。

查看作业日志（Amazon CloudWatch 控制台）

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 使用页面右上角的 AWS 区域 选择器，选择要查看其日志的作业在其中运行的区域。
3. 在导航窗格中，选择 Logs（日志），然后选择 Log groups（日志组）。
4. 在日志组页面上，选择 /aws/macie/classificationjobs 日志组。CloudWatch Logs 会显示您已运行的作业的日志流表。每项作业都有一个唯一的流。每个流的名称都与作业的唯一标识符相关。
5. 在日志流 下，执行以下操作之一：
   - 要查看特定作业的日志事件，请选择该作业的日志流。要更轻松地找到流，请在表格上方的筛选框中输入作业的唯一标识符。在您选择日志流后，CloudWatch Logs 会显示该作业的日志事件表。
   - 要查看所有作业的日志事件，请选择搜索所有日志流。CloudWatch Logs 会显示您的所有作业的日志事件表。
6. （可选）在表格上方的筛选框中，输入用于指定要查看的特定事件特征的术语、短语或值。有关更多信息，请参阅《Amazon CloudWatch Logs 用户指南》中的使用筛选模式搜索日志数据。

7. 要查看特定日志事件的详细信息，请选择该事件所在行的右箭头
   ()。Clo
   Logs 以 JSON 格式显示事件的详细信息。

熟悉日志事件中的数据后，您还可以执行一些任务，例如创建指标筛选条件，将日志数据转换为数字 CloudWatch 指标，以及创建自定义警报，以便您更轻松地识别和响应特定的日志事件。有关更多信息，请参阅 Amazon CloudWatch Logs 用户指南。

敏感数据发现作业的日志事件架构

敏感数据发现作业的每个日志事件都是一个 JSON 对象，该对象符合 Amazon CloudWatch Logs 事件架构并包含一组标准字段。某些类型的事件还有其他字段，这些字段提供的信息对此类事件特别有用。例如，账户级错误事件包括受影响的 AWS 账户 的账户 ID。存储桶级错误事件包括受影响的 S3 存储桶的名称。有关 Macie 发布到 CloudWatch Logs 的作业事件的详细列表，请参阅 作业的日志事件类型。

以下示例显示敏感数据发现作业的日志事件架构。在此示例中，事件报告说，由于 Amazon S3 拒绝访问存储桶，Macie 无法分析该存储桶中的任何对象。

```
{
    "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"
    }
}
```

在前面的示例中，Macie 尝试使用 Amazon S3 API 的 ListObjectsV2 操作列出存储桶中的对象。当 Macie 向 Amazon S3 发送请求时， Amazon S3 拒绝访问该存储桶。

以下字段是敏感数据发现作业的所有日志事件的通用字段：

- `adminAccountId` – 创建作业的 AWS 账户 的唯一标识符。

- `jobId` – 作业的唯一标识符。
- `eventType` – 发生的事件类型。有关可能值的完整列表和每个值的说明，请参见 作业的日志事件类型。
- `occurredAt` – 事件发生时的日期和时间，采用协调世界时 (UTC) 和扩展 ISO 8601 格式。
- `description` – 事件的简要说明。
- `jobName` – 作业的自定义名称。

根据事件的类型和性质，日志事件还可以包含以下字段：

- `affectedAccount` – 拥有受影响资源的 AWS 账户 的唯一标识符。
- `affectedResource` – 提供有关受影响资源的详细信息的对象。在对象中，`type` 字段指定一个用于存储有关资源的元数据的字段。`value` 字段指定字段 (`type`) 的值。
- `operation` – Macie 尝试执行并导致错误的操作。
- `runDate` – 适用作业或作业运行开始时的日期和时间，采用协调世界时 (UTC) 和扩展 ISO 8601 格式。

敏感数据发现作业的日志事件类型

Macie 发布三类事件的日志事件：

- 作业状态事件，用于记录作业或作业运行的状态或进度的变化。
- 账户级错误事件，用于记录阻止 Macie 分析特定 AWS 账户 的 Amazon S3 数据的错误。
- 存储桶级错误事件，用于记录阻止 Macie 分析特定 S3 存储桶的数据的错误。

本节中的主题列出并描述了 Macie 为每个类别发布的事件类型。

主题

- 作业状态事件
- 账户级错误事件
- 存储桶级错误事件

作业状态事件

作业状态事件，用于记录作业或作业运行的状态或进度的变化。对于定期作业，Macie 会记录并发布整个作业和单个作业运行的这些事件。有关确定作业总体状态的信息，请参阅 检查敏感数据发现作业的状态。

以下示例使用示例数据来显示作业状态事件中字段的结构和性质。在此示例中，SCHEDULED_RUN_COMPLETED事件表示定期作业的计划运行已完成运行。如 runDate 字段所示，运行于世界标准时间 2021 年 4 月 14 日 17:09:30 开始。如 occurredAt 字段所示，运行于世界标准时间 2021 年 4 月 14 日 17:16:30 结束。

```
{
    "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"
}
```

下表列出并描述了 Macie 记录并发布到 CloudWatch Logs 的作业状态事件的类型。事件类型列表示每个事件在事件eventType字段中显示的名称。说明列提供事件显示在事件description字段中的简要说明。其他信息提供有关该事件适用的作业类型的信息。该表首先按事件可能发生的大致时间顺序排序，然后按事件类型按字母升序排序。

事件类型	说明	其他信息
JOB_CREATED	已创建作业。	适用于一次性和定期作业。
ONE_TIME_JOB_STARTED	作业开始运行。	仅适用于一次性作业。
SCHEDULED_RUN_STARTED	计划作业开始运行。	仅适用于定期作业。为了记录一次性作业的开始，Macie 发布一个 ONE_TIME_JOB_STARTED 事件，而不是此类事件。

事件类型	说明	其他信息
BUCKET_MATCHED_THE_CRITER	受影响的存储桶符合为作业指定的存储桶标准。	适用于使用运行时存储桶标准来确定要分析哪些 S3 存储桶的一次性和定期作业。 `affectedResource` 对象指定符合标准并包含在作业分析中的存储桶的名称。
NO_BUCKETS_MATCHED_THE_CRITERIA	作业已开始运行，但当前没有与为该作业指定的存储桶标准相匹配的存储桶。该作业没有分析任何数据。	适用于使用运行时存储桶标准来确定要分析哪些 S3 存储桶的一次性和定期作业。
SCHEDULED_RUN_COMPLETED	计划作业结束运行。	仅适用于定期作业。为了记录一次性作业的完成，Macie 发布一个 JOB_COMPLETED 事件，而不是此类事件。
JOB_PAUSED_BY_USER	作业已被用户暂停。	适用于您暂时停止（已暂停）的一次性和定期作业。
JOB_RESUMED_BY_USER	作业已由用户恢复。	适用于您暂时停止（已暂停）并且之后又恢复了的一次性和定期作业。

事件类型	说明	其他信息
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	作业已被 Macie 暂停。作业的完成将超过受影响账户的每月配额。	适用于 Macie 暂时停止（已暂停）的一次性和定期作业。 当作业或作业运行的额外处理超过该作业为其分析数据的一个或多个账户的每月敏感数据发现配额时，Macie 会自动暂停该作业。为避免出现此问题，请考虑增加受影响账户的配额。
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	作业已由 Macie 恢复。受影响账户的每月服务配额已取消。	适用于 Macie 暂时停止（已暂停）并且之后又恢复了的一次性和定期作业。 如果 Macie 自动暂停一次性作业，Macie 将在下一个月开始时或所有受影响账户的每月敏感数据发现配额增加时（以先发生者为准）自动恢复该作业。如果 Macie 自动暂停定期作业，Macie 将在计划下一次运行开始或下一个月开始时（以先发生者为准）自动恢复该作业。

事件类型	说明	其他信息
JOB_CANCELLED	作业已取消。	适用于您永久停止（取消）的一次性和定期作业，或者对于一次性作业，已暂停但未在 30 天内恢复。 如果您挂起或禁用 Macie，则此类事件也适用于在您挂起或禁用 Macie 时处于活动状态或暂停状态的作业。如果您挂起或禁用在 AWS 区域 区域中的 Macie，Macie 会自动取消您在该区域中的作业。
JOB_COMPLETED	作业已完成运行。	仅适用于一次性作业。为了记录定期作业的作业运行的完成，Macie 发布一个 SCHEDULED_RUN_COMPLETED 事件，而不是此类事件。

账户级错误事件

账户级错误事件记录导致 Macie 无法分析由特定 AWS 账户 拥有的 S3 存储桶中的对象的错误。每个事件中的 `affectedAccount` 字段都指定该账户的账户 ID。

以下示例使用示例数据来显示账户级错误事件中字段的结构和性质。在此示例中，`ACCOUNT_ACCESS_DENIED` 事件表明 Macie 无法分析账户 `444455556666` 拥有的任何 S3 存储桶中的对象。

```
{
    "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"
}
```

下表列出并描述了 Macie 记录并发布到 CloudWatch Logs 的账户级错误事件的类型。事件类型列表示每个事件在事件`eventType`字段中显示的名称。说明列提供事件显示在事件`description`字段中的简要说明。其他信息列提供调查或解决所发生错误的所有适用提示。该表按事件类型字母顺序升序排序。

事件类型	说明	其他信息
ACCOUNT_ACCESS_DENIED	Macie 无权访问受影响账户的 S3 存储桶数据。	之所以发生这种情况，通常是因为账户拥有的存储桶具有限制性的存储桶策略。有关如何解决此问题的信息，请参阅 允许 Macie 访问 S3 存储桶和对象。 事件中 `operation` 字段的值可以帮助您确定哪些权限设置阻止 Macie 访问该账户的 S3 数据。此字段表示错误发生时 Macie 尝试执行的 Amazon S3 操作。
ACCOUNT_DISABLED	作业跳过了受影响账户拥有的资源。Macie 已对账户禁用。	要解决此问题，在同一 AWS 区域 中为该账户重新启用 Macie。
ACCOUNT_DISASSOCIATED	作业跳过了受影响账户拥有的资源。该账户不再作为成员账户与您的 Macie 管理员账户关联。	如果您作为组织的 Macie 管理员，将作业配置为分析关联成员账户的数据，而该成员账户随后从您的组织中被移除，则会发生这种情况。

事件类型	说明	其他信息
		要解决此问题，请将受影响的账户与您的 Macie 管理员账户重新关联为成员账户。有关更多信息，请参阅 管理多个 账户。
ACCOUNT_ISOLATED	作业跳过了受影响账户拥有的资源。AWS 账户 被隔离。	–
ACCOUNT_REGION_DISABLED	作业跳过了受影响账户拥有的资源。当前 AWS 区域中，AWS 账户 不处于活动状态。	–
ACCOUNT_SUSPENDED	作业被取消或跳过了受影响账户拥有的资源。Macie 已对账户挂起	如果指定的账户是您自己的账户，那么当您在同一地区挂起 Macie 时，Macie 会自动取消作业。要解决此问题，请在该地区重新启用 Macie。 如果指定的账户是成员账户，请在同一地区为该账户重新启用 Macie。
ACCOUNT_TERMINATED	作业跳过了受影响账户拥有的资源。AWS 账户 已终止。	–

存储桶级错误事件

存储桶级错误事件记录导致 Macie 无法分析特定 S3 存储桶中的对象的错误。每个事件中的 `affectedAccount` 字段都指定拥有存储桶的 AWS 账户 的账户 ID。每个事件中的 `affectedResource` 对象都指定了存储桶名称。

以下示例使用示例数据来显示存储桶级错误事件中字段的结构和性质。在此示例中，BUCKET_ACCESS_DENIED 事件表明 Macie 无法分析名为 DOC-EXAMPLE-BUCKET 的 S3 存储桶中的任何对象。Macie 尝试使用 Amazon S3 API 的 ListObjectsV2 操作列出存储桶中的对象时，Amazon S3 拒绝访问存储桶。

```
{
    "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"
    }
}
```

下表列出并描述了 Macie 记录并发布到 CloudWatch Logs 的存储桶级错误事件的类型。事件类型列表示每个事件在事件eventType字段中显示的名称。说明列提供事件显示在事件description字段中的简要说明。其他信息列提供调查或解决所发生错误的所有适用提示。该表按事件类型字母顺序升序排序。

事件类型	说明	其他信息
BUCKET_ACCESS_DENIED	Macie 无权访问受影响的 S3 存储桶。	此问题的原因通常是存储桶具有限制性存储桶策略。有关如何解决此问题的信息，请参阅允许 Macie 访问 S3 存储桶和对象。 事件中 operation 字段的值可以帮助您确定哪些权限设置阻止 Macie 访问存储桶。此字段表示错误发生时 Macie 尝试执行的 Amazon S3 操作。

事件类型	说明	其他信息
BUCKET_DETAILS_UNAVAILABLE	由于临时问题，Macie 无法检索有关存储桶和存储桶对象的详细信息。	如果暂时性问题阻止 Macie 检索分析存储桶对象所需的存储桶和对象元数据，则会发生这种情况。例如，当 Macie 尝试验证是否允许其访问存储桶时，就会出现 Amazon S3 异常。 要解决一次性作业的该问题，可以考虑创建并运行一个新的一次性作业来分析存储桶中的对象。对于计划作业，Macie 将在下一次作业运行期间再次尝试检索元数据。
BUCKET_DOES_NOT_EXIST	受影响的 S3 存储桶已不存在。	发生这种情况通常是因为存储桶已被删除。
BUCKET_IN_DIFFERENT_REGION	受影响的 S3 存储桶已移至其他 AWS 区域。	–
BUCKET_OWNER_CHANGED	受影响的 S3 存储桶的所有者已更改。Macie 不再有权限访问存储桶。	如果存储桶的所有权已转移给不属于您的组织的 AWS 账户，则通常会发生这种情况。事件中的`affectedAccount` 字段表示先前拥有该存储桶的账户的账户 ID。

管理敏感数据发现作业

为了帮助您管理敏感数据发现作业，Amazon Macie 提供了每个 AWS 区域 中的完整作业清单。使用此清单，您可以将作业作为单个集合进行管理，并访问各个作业的配置设置、状态和处理统计信息。您还可以访问每个作业产生的敏感数据发现和其他结果。

除了这些任务外，您还可以创建各个作业的自定义变体：拷贝现有作业，调整副本的设置，然后将副本另存为新作业。如果您想以相同的方式分析不同的数据集，或者以不同的方式分析同一组数据，这可能会很有帮助。或者，您想调整现有作业的配置设置 — 取消现有作业，将其复制，然后调整副本并将其另存为新作业。

主题

查看您的敏感数据发现作业清单

Amazon Macie 控制台上的作业页面提供有关您账户在当前 AWS 区域 的所有敏感数据发现作业的信息。对于每个作业，该表显示的摘要信息包括：作业的当前状态；作业是否按计划定期运行；以及该作业是分析特定数量的 S3 存储桶还是分析符合运行时系统标准的 S3 存储桶。如果您在表中选择一项作业，则详细信息面板将显示有关该作业的配置设置和其他信息。

要查看您的作业清单

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。作业页面将打开并显示清单中的作业数量以及这些作业的表格。
3. 要更快地找到特定作业，请执行以下任一操作：

    - 要按特定字段对表格进行排序，请点击该字段的列标题。若要更改排序顺序，请再次点击列标题。
    - 要仅显示那些具有特定字段值的作业，请将光标置于筛选框中。在出现的菜单中，选择要用于筛选条件的字段，然后输入筛选条件的值。然后选择 Apply（应用）。
    - 要隐藏那些具有特定字段值的作业，请将光标置于筛选框中。在出现的菜单中，选择要用于筛选条件的字段，然后输入筛选条件的值。

然后选择 Apply（应用）。在筛选框中，为筛选条件选择等于图标
(●)。
这会将筛选条件的运算符从等于更改为不等于
(⦸)。

- 要移除筛选条件，请选择要移除的筛选条件的“移除筛选条件图标”(⊗)。

4. 要查看特定作业的配置设置和其他详细信息，请在表中选择作业的名称，然后转到详细信息面板。

查看敏感数据发现作业的配置设置

在 Amazon Macie 控制台上，您可以使用作业页面上的详细信息面板来查看配置设置以及有关各个敏感数据发现作业的其他信息。例如，您可以查看作业配置为分析的 S3 存储桶列表，以及作业使用哪些托管数据标识符来分析这些存储桶中的对象。

> **Note**
>
> 您无法更改现有作业的任何配置设置。这有助于确保您拥有敏感数据调查发现和发现结果的不可变历史记录，以便您执行数据隐私和保护的审计或调查。如果要更改现有作业，请取消该作业。然后复制作业，将副本配置为使用所需的设置，然后将副本另存为新作业。
> 如果这样操作，您还应该采取措施确保新作业不会再次以同样的方式分析现有数据。为此，请记下您取消现有作业的日期和时间。然后将新作业的范围配置为仅包含在您取消原始作业之后创建或更改过的对象。例如，使用对象条件添加上次修改的排除条件，该条件指定您取消原始作业的日期和时间。

查看作业的配置设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 在作业页面上，选择要查看其设置的作业名称。详细信息面板将显示有关该作业的配置设置和其他信息。根据作业的设置，该面板包含以下部分。

一般信息

本节提供有关作业的一般信息，例如，作业的 Amazon 资源名称（ARN）、作业最近开始运行的时间以及作业的当前状态。如果您暂停了作业，则此部分还会指出您何时暂停了该作业，以及作业或最新运行的作业何时过期，或者如果您不恢复则将何时过期。

统计数据

此部分显示改作业统计信息的处理，例如作业运行的次数以及该作业在当前运行期间尚未处理的大致对象数。

范围

本节说明作业的运行频率。它还会显示用于细化作业范围的设置，例如，采样深度以及任何在作业分析中包含或排除 S3 对象的对象条件。

S3 存储桶

如果将作业配置为分析您在创建作业时明确选择的存储桶，则此部分将显示在面板中。它表示作业所配置以分析数据的 AWS 账户 的数量。它还表示作业配置为分析的存储桶数量以及这些存储桶的名称（按账户分组）。

要以 JSON 格式显示账户和存储桶的完整列表，请在存储桶总数字段中选择数字。

S3 存储桶条件

如果作业使用运行时系统条件来确定要分析哪些存储桶，则此部分将显示在面板中。它列出了配置作业要使用的条件。

要以 JSON 格式显示条件，请选择详细信息，然后在出现的窗口中选择条件选项卡。

要查看当前符合条件的存储桶表，请选择详细信息，然后在出现的窗口中选择匹配存储桶选项卡。（可选）选择刷新（ ）以检索最新数据。

> **Tip**
>
> 如果作业已经运行，您还可以确定是否有任何存储桶符合作业运行时的条件，如果是，则确定这些存储桶的名称。为此，查看作业的日志事件，请选择面板顶部的显示结果，然后选择显示 CloudWatch 日志。Macie 打开 Amazon CloudWatch 控制台并显

示该作业的日志事件表。这些事件包括符合条件并包含在作业分析中的每个存储桶的 BUCKET_MATCHED_THE_CRITERIA 事件。有关更多信息，请参阅监控作业。

自定义数据标识符

如果将作业配置为使用一个或多个自定义数据标识符，则此部分将显示在面板中。它指定了这些自定义数据标识符的名称。

允许列表

如果将作业配置为使用一个或多个允许列表，则此部分将显示在面板中。它指定了这些列表的名称。若要查看列表的设置和状态，请选择列表名称旁边的链接图标 ( )。

托管数据标识符

本节指出了配置作业要使用哪些托管数据标识符。这由作业的托管数据标识符选择类型决定：

- 推荐-作业运行时使用推荐集中的托管数据标识符。
- 包括选定项-仅使用选择部分中列出的托管数据标识符。
- 全部包含-使用作业运行时可用的所有托管数据标识符。
- 排除选定项-使用作业运行时可用的所有托管数据标识符，但选择部分中列出的标识符除外。
- 全部排除-不要使用任何托管数据标识符。仅使用指定的自定义数据标识符。

要以 JSON 格式查看这些设置，请选择详细信息。

标签

如果标签与作业相关联，则此部分将在面板中显示。它列出了这些标签。

标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

4. 要查看作业设置并将其保存为 JSON 格式，请在面板顶部选择作业的唯一标识符（作业 ID），然后选择下载。

检查敏感数据发现作业的状态

创建敏感数据发现作业时，其初始状态为活动（正在运行）或活动（空闲），具体取决于作业的类型和计划。然后，作业会经过其他状态，您可以随着作业的进展对其进行监控。

> **Tip**
>
> 除了监控作业的整体状态外，您还可以监控作业进行过程中发生的特定事件。您可以通过使用 Macie 自动发布到 Amazon CloudWatch Logs 的日志数据来做到这一点。这些日志中的数据提供了作业状态更改的记录，以及作业运行时发生的任何账户或存储桶级错误的详细信息。有关更多信息，请参阅监控作业。

检查作业状态

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 在作业页面上，找到要检查其状态的作业。状态字段显示作业的当前状态。

活动（空闲）

对于定期作业，上一次运行已完成，下一次计划运行处于待处理状态。此值不适用于一次性作业。

活跃（正在运行）

对于一次性作业，该作业当前正在进行中。对于定期作业，计划运行正在进行中。

已取消

对于任何类型的作业，该作业均永久停止（已取消）。

如果您明确取消了作业，或者如果这是一次性作业，该作业已暂停但未在 30 天内恢复，则该作业将处于此状态。如果您之前在当前 AWS 区域 中暂停了 Macie，则作业也可能处于此状态。

完成

对于一次性作业，该作业已成功运行，现已完成。此值不适用于定期作业。相反，当每次运行成功完成时，定期作业的状态会更改为活动（空闲）。

已暂停（由 Macie）

对于任何类型的作业，Macie 暂时停止（暂停）该作业。

如果作业或作业运行的完成将超过您账户的每月敏感数据发现配额，则该任务将处于此状态。发生这种情况时，Macie 会自动暂停作业。当下一个日历月开始（并且您的账户的每月配额已重置），或者您增加账户的配额，则 Macie 会自动恢复该作业。

如果您是组织的 Macie 管理员，并且将作业配置为分析成员账户的数据，那么如果作业或作业运行的完成超过成员账户的每月敏感数据发现配额，则该作业也可能处于此状态。

如果作业正在运行，并且对符合条件的对象的分析达到成员账户的此配额，该作业将停止分析该账户拥有的对象。当该作业完成对所有其他未达到配额账户对象的分析后，Macie 会自动暂停作业。如果这是一次性作业，Macie 将在下一个日历月开始时或所有受影响账户的配额增加时（以先发生者为准）自动恢复该作业。如果是定期作业，Macie 将在计划下一次运行开始或下一个日历月开始时（以先发生者为准）自动恢复该作业。如果计划运行在下一个日历月开始之前开始，或者受影响账户的配额增加，该作业不会分析该账户拥有的对象。

已暂停（由用户）

对于任何类型的作业，您暂时停止（暂停）该作业。

如果您暂停了一次性作业，但未在 30 天内恢复该作业，则该作业将过期，Macie 会将其取消。如果您在定期作业处于活动运行状态时暂停该作业，但在 30 天内没有恢复该作业，则该作业的运行将过期，Macie 将取消该运行。要查看已暂停的作业或作业运行的到期日期，请在表中选择该作业的名称，然后参考详细信息面板状态详细信息部分中的过期字段。

如果作业被取消或暂停，则可以参考该作业的详细信息来确定该作业是否已开始运行，或者对于定期作业，在取消或暂停之前至少运行过一次。要执行此操作，请在表中选择作业的名称，然后转到详细信息面板。在面板中，运行次数字段表示作业已运行的次数。上次运行时间字段会显示作业开始运行的最近日期和时间。

根据作业的当前状态，您可以选择暂停、恢复或取消作业。

暂停、恢复或取消敏感数据发现作业

创建敏感数据发现作业后，您可以暂时将其暂停或永久取消。当您暂停正在运行的作业时，Macie 会立即开始暂停该作业的所有处理任务。当您暂停正在运行的作业时，Macie 会立即开始停止该作业的所有处理任务。作业取消后无法恢复或重新启动。

如果您暂停了一次性作业，则可以在 30 天内恢复该作业。当您恢复作业时，Macie 会立即从您暂停作业的位置开始恢复处理——Macie 不会从头重新启动作业。如果您暂停了一次性作业，但未在 30 天内恢复该作业，则该作业将过期，Macie 会将其取消。

如果您暂停定期作业，您可以随时恢复作业。如果您恢复定期作业，但暂停作业时该作业处于空闲状态，则 Macie 会根据您在创建该作业时选择的计划和其他配置设置恢复该作业。如果您恢复定期作业，并且暂停作业时该作业正在运行中，那么 Macie 如何恢复该作业取决于您何时恢复该作业：

- 如果在暂停作业后的 30 天内恢复作业，Macie 会立即从暂停作业的位置恢复最近一次计划的运行—Macie 不会从头开始重新启动运行。
- 如果您在暂停作业后的 30 天内没有恢复该作业，则最新的计划运行将过期，Macie 将取消该运行的所有剩余处理任务。当您随后恢复作业时，Macie 会根据您在创建作业时选择的计划和其他配置设置恢复作业。

为了帮助您确定暂停的作业或作业运行何时过期，Macie 在作业暂停时在作业的详细信息中添加了到期日期。要查看此日期，请在作业页面的表中选择作业的名称，然后在详细信息面板的状态详细信息部分中查看过期字段。此外，我们会在作业或作业运行到期前大约七天通知您。当作业或作业运行到期并被取消时，我们会再次通知您。为了通知您，我们会将电子邮件发送到与您的 AWS 账户 关联的地址。我们还会为您的账户创建 AWS Health 活动和 Amazon CloudWatch Events。

暂停、恢复或取消作业

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。
3. 在作业页面上，选中要暂停、恢复或取消的作业的复选框，然后在操作菜单上执行以下操作之一：
   - 要暂时暂停作业，请选择暂停。仅当作业的当前状态为活动（空闲）、活动（正在运行）或已暂停（由 Macie）时，此选项才可用。
   - 要恢复作业，请选择恢复。仅当作业的当前状态为已暂停（由用户）时，此选项才可用。
   - 要永久取消作业，请选择取消。选择此选项后，您随后将无法恢复或重新启动作业。

复制敏感数据发现作业

要快速创建与现有作业类似的新敏感数据发现作业，您可以创建该作业的副本，编辑副本的设置，然后将该副本另存为新作业。这对于您想要创建现有作业的自定义变体的情况很有帮助。或者，您想调整现有作业的配置设置 — 取消作业，然后将其复制、更改和保存为新作业。

复制作业

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择作业。

3. 选中要复制的作业的复选框。
4. 在操作菜单中，选择复制到新项目。
5. 完成控制台上的步骤以查看和调整作业副本的设置。对于调整范围步骤，请考虑选择一些选项，以防止作业再次以相同的方式分析现有数据：

   - 对于一次性作业，使用对象条件仅包括在一定时间后创建或更改的对象。例如，如果您要创建已取消的作业的副本，请添加上次修改时间条件，以指定您取消现有作业的日期和时间。
   - 对于定期作业，请清除包括现有对象复选框。如果您执行此操作，第一次运行作业将仅分析在作业创建完成之后以及第一次运行作业前创建或更改过的对象。您也可以使用对象条件来排除在特定日期和时间之前最后一次修改的对象。

   有关此步骤和其他步骤的更多详细信息，请参阅 创建敏感数据发现作业。
6. 完成后，选择提交将副本另存为新作业。

预测和监控敏感数据发现作业的成本

Amazon Macie 的定价部分取决于您通过运行敏感数据发现作业所分析的数据量。要预测和监控运行敏感数据发现作业的估计成本，您可以查看 Macie 在创建作业时和开始运行作业之后提供的成本估算。

要查看和监控您的实际成本，您可以使用 AWS Billing and Cost Management。AWS Billing and Cost Management 提供的功能旨在帮助您跟踪和分析 AWS 服务 的成本，并管理您的账户或组织的预算。它还提供可帮助您根据历史数据预测使用成本的功能。要了解有关更多信息，请参阅 AWS Billing 用户指南。

有关 Macie 定价的详细信息，请参阅 Amazon Macie 定价。

主题

预测敏感数据发现作业的成本

当您创建敏感数据发现作业时，Amazon Macie 可以计算并显示作业创建过程中的两个关键步骤中的估计成本：查看为作业选择的 S3 存储桶表（步骤 2）和查看作业的所有设置时（步骤 8）。这些估计值可以帮助您在保存作业之前确定是否要调整作业的设置。估算值的可用性和性质取决于您为作业选择的设置。

查看各个存储桶的估计成本（步骤 2）

如果您明确选择单个存储桶供作业分析，则可以查看分析每个存储桶中对象的估计成本。当您查看您的存储桶选择时，Macie 会在创建作业过程的第 2 步中显示这些估算值。在此步骤的表中，估计成本字段指示运行作业一次以分析存储桶中的对象的估计成本总额（以美元计）。

根据当前存储在存储桶中的对象的大小和类型，每个估计值都反映了作业将在存储桶中分析的预计未压缩数据量。该估计值还反映了对当前 AWS 区域 的 Macie 定价。

存储桶的成本估算中仅包括可分类的对象。可分类对象是使用支持的 Amazon S3 存储类的 S3 对象，其文件扩展名表示支持的文件或存储格式。如果任何可分类的对象是压缩文件或存档文件，则该估算假设这些文件使用 3:1 的压缩比，并且作业可以分析所有提取的文件。

查看作业的总估计成本（步骤 8）

如果您创建了一次性作业，或者创建并配置了包含现有 S3 对象的定期作业，则 Macie 会在作业创建过程的最后一步计算并显示该作业的总估计成本。在查看和验证为该作业选择的所有设置时，您可以查看此估算值。

该估算值表示在当前区域中运行作业一次的预计成本总额（以美元计）。该估算值反映了作业将要分析的未压缩数据的预计量。它基于当前存储在您为作业明确选择的存储桶中的对象的大小和类型，或者当前存储在符合您为作业指定的存储桶标准的最多 500 个存储桶中的对象的大小和类型，具体取决于作业的设置。

请注意，此估算值并未反映您为优化和缩小作业范围而选择的任何选项，例如，较低的采样深度或将某些 S3 对象排除在作业之外的标准。它也无法反映您每月的敏感数据发现配额，这可能会限制作业分析的范围和成本，也无法反映可能适用于您的账户的任何折扣。

除了作业的总估计成本外，该估算还提供了汇总数据，可以深入了解作业的预计范围和成本：

- 大小值表示作业可以分析和不能分析的对象的总存储大小。
- 对象计数值表示作业可以分析和不能分析的对象总数。

在这些值中，可分类对象是使用支持的 Amazon S3 存储类的 S3 对象，其文件扩展名表示支持的文件或存储格式。成本估算中仅包括可分类的对象。不可分类对象是指不使用支持的存储类或者没有支持的文件或存储格式的文件扩展名的对象。这些对象不包括在成本估算中。

该估算值为压缩文件或存档文件的 S3 对象提供了额外的聚合数据。压缩值表示使用支持的 Amazon S3 存储类且具有支持的压缩或存档文件类型的文件扩展名的对象的总存储大小。未压缩值根据指定的压缩比指示这些对象解压缩后的大致大小。这些数据之所以相关，是因为 Macie 分析压缩文件和存档文件的方式。

当 Macie 分析压缩文件或存档文件时，它会同时检查完整文件和文件内容。为了检查文件的内容，Macie 会解压缩该文件，然后检查使用受支持格式的每个提取文件。因此，作业分析的实际数据量取决于：

- 文件是否使用压缩，如果是，它使用的压缩比。
- 提取的文件的数量、大小和格式。

默认情况下，Macie 在计算作业的成本估算值时会假设以下条件：

- 所有压缩文件和存档文件都使用 3:1 的压缩比。
- 所有提取的文件都使用支持的文件或存储格式。

这些假设可能会导致对作业将要分析的数据范围进行更大的估计，从而使作业的成本估算值更高。

您可以根据不同的压缩率重新计算作业的总估计成本。为此，请从 估计成本部分的 选择估计压缩比列表中选择比率。然后，Macie 会更新估算值以匹配您的选择。

有关 Macie 如何计算估计成本的更多信息，请参阅了解如何计算估计使用成本。

监控敏感数据发现作业的估计成本

如果您已经在运行敏感数据发现作业，Amazon Macie 控制台上的 使用情况页面可以帮助您监控这些作业的估计成本。该页面显示您在当前日历月在 AWS 区域 中使用 Macie 的估计成本（以美元计）。有关 Macie 如何计算这些估算值的信息，请参阅了解如何计算估计使用成本。

查看运行作业的估计成本

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要查看估计成本的区域。
3. 在导航窗格中，选择使用情况。
4. 在 使用情况页面上，请参阅您账户的估计成本明细。敏感数据发现作业项会报告您在当月迄今为止在当前区域运行的作业的总估计成本。

   如果您是某个组织的 Macie 管理员，估计成本部分会显示您所在组织当前月份在当前区域的总估计成本。要显示为特定账户运行的作业的总估计成本，请在表中选择该账户。然后，估计成本部分显示了该账户的估计成本明细，包括已运行作业的估计成本。要显示不同账户的此数据，请在表中选择该账户。要清除账户选择，请选择账户 ID 旁边的 X。

要查看和监控您的实际成本，请使用 AWS Billing and Cost Management。

推荐用于敏感数据发现作业的托管数据标识符

要优化敏感数据发现作业的结果，您可以将单个作业配置为自动使用我们为作业推荐的托管数据标识符集。托管数据标识符是一组内置标准和技术，旨在检测特定类型的敏感数据，例如 AWS 秘密访问密钥、信用卡号或特定国家或地区的护照号码。

推荐的托管数据标识符集旨在检测常见的敏感数据类别和类型。根据我们的研究，它可以检测一般类别和类型的敏感数据，同时还可以通过减少噪音来优化您的作业结果。在我们发布新的托管数据标识符时，如果它们有可能进一步优化您的作业结果，我们会将其添加到此集合中。随着时间的推移，我们还可能在集合中添加或删除现有的托管数据标识符。如果我们在推荐的集合中添加或移除托管数据标识符，我们会更新此页面以说明更改的性质和时间。有关这些更改的自动警报，您可以订阅 Macie 文档历史记录页面上的 RSS 源。

创建敏感数据发现作业时，您可以指定您希望该作业使用哪些托管数据标识符来分析 Amazon Simple Storage Service (Amazon S3) 存储桶中的对象。要将作业配置为使用推荐的托管数据标识符集，请在创建作业时选择推荐选项。然后，当作业开始运行时，该作业将自动使用推荐集中的所有托管数据标识符。如果将作业配置为多次运行，则每次运行将自动使用运行开始时推荐集中的所有托管数据标识符。

以下主题列出了当前位于推荐集中的托管数据标识符，这些标识符按敏感数据类别和类型组织。它们为集合中的每个托管数据标识符指定唯一标识符 (ID)。此 ID 描述了托管数据标识符旨在检测的敏感数据类型，例如：`PGP_PRIVATE_KEY` 表示 PGP 私钥，`USA_PASSPORT_NUMBER` 表示美国护照号码。

主题

有关特定托管数据标识符的详细信息或 Macie 当前提供的所有托管数据标识符的完整列表，请参阅使用托管数据标识符。

凭证

为了检测 S3 对象中出现的凭证数据，推荐集使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
AWS秘密访问密钥	`AWS_CREDENTIALS`

敏感数据类型	托管数据标识符 ID
HTTP 基本授权标头	HTTP_BASIC_AUTH_HEADER
OpenSSH 私有密钥	OPENSSH_PRIVATE_KEY
PGP 私有密钥	PGP_PRIVATE_KEY
公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	PKCS
PuTTY 私有密钥	PUTTY_PRIVATE_KEY

财务信息

为了检测 S3 对象中出现的财务信息，推荐集使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
信用卡磁条数据	CREDIT_CARD_MAGNETIC_STRIPE
信用卡号	CREDIT_CARD_NUMBER （适用于关键字附近的信用卡号）

个人身份信息（PII）

为了检测 S3 对象中出现的个人身份信息（PII），推荐集使用以下托管数据标识符。

敏感数据类型	托管数据标识符 ID
驾驶执照识别号	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE （对于美国），UK_DRIVERS_LICENSE
选民名册编号	UK_ELECTORAL_ROLL_NUMBER
身份证号码	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_I

敏感数据类型	托管数据标识符 ID
	DENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保险号码 (NINO, National Insurance Number)	UK_NATIONAL_INSURANCE_NUMBER
护照编号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社会保险号码 (SIN, Social Insurance Number)	CANADA_SOCIAL_INSURANCE_NUMBER
社会保障号码 (SSN, Social Security number)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
纳税人识别号或参考号	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

推荐集的更新

下表描述了我们为敏感数据发现作业推荐的托管数据标识符集的更改。有关这些更改的自动警报，可以订阅 Macie 文档历史记录页面上的 RSS 源。

更改	说明	日期
通用版	推荐集首次发布。	2023 年 6 月 27 日

使用 Amazon Macie 分析加密的 Amazon S3 对象

当您为您的 AWS 账户 启用 Amazon Macie 时，Macie 会创建一个服务相关角色，该角色授予 Macie 代表您调用 Amazon Simple Storage Service (Amazon S3) 和其他 AWS 服务 所需的权限。服务相关角色简化了设置 AWS 服务 的过程，因为您不必手动添加服务代表您完成操作所需的权限。要了解有关此类角色的更多信息，请参阅 AWS Identity and Access Management 用户指南中的使用服务相关角色。

Macie 服务相关角色的权限策略 (`AWSServiceRoleForAmazonMacie`) 允许 Macie 执行操作，包括检索有关 S3 存储桶和对象的信息，以及检索和分析 S3 存储桶内的对象。如果您的账户是组织的 Macie 管理员账户，则该策略还允许 Macie 代表您对组织中的成员账户执行此操作。

如果 S3 对象已加密，则 Macie 服务相关角色的权限策略通常会向 Macie 授权解密该对象。但是，这取决于其使用的加密类型。还可能取决于是否允许 Macie 使用适当的加密密钥。

主题

- Amazon S3 对象的加密选项
- 允许 Amazon Macie 使用客户托管 AWS KMS key

Amazon S3 对象的加密选项

Amazon S3 支持多种 S3 对象的加密选项。对于其中的大多数选项，Amazon Macie 都可以使用账户的 Macie 服务关联角色解密对象。但是，这取决于用于对象的加密类型。

具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）

> 如果使用服务器端加密和 Amazon S3 托管密钥 (SSE-S3) 对对象进行加密，则 Macie 可以解密该对象。
>
> 若要了解此类加密，请参阅Amazon Simple Storage Service 用户指南中的使用具有 Amazon S3 托管密钥的服务器端加密。

使用AWS KMS keys（DSSE-KMS 和 SSE-KMS）进行服务器端加密

如果使用双层服务器端加密或使用AWS托管AWS KMS key（DSSE-KMS 或 SSE-KMS）进行服务器端加密，Macie 可以解密该对象。

如果使用双层服务器端加密或由客户管理的服务器端加密AWS KMS key（DSSE-KMS 或 SSE-KMS）对对象进行加密，则只有在您允许 Macie 使用密钥的情况下，Macie 才能解密该对象。这种对象的加密方式为：AWS KMS中完全托管的 KMS 密钥；以及外部密钥存储中的 KMS 密钥。如果不允许 Macie 使用适当的 KMS 密钥，则 Macie 只能存储和报告此对象的元数据。

要了解这些类型的加密，请参阅《A mazon 简单存储服务用户指南》中的 “使用双层服务器端加密 AWS KMS keys” AWS KMS keys 和 “使用服务器端加密”。

> **Tip**
>
> 您可以自动生成一份关于 Macie 需要访问的所有客户托管AWS KMS keys的列表，以分析您账户的 S3 存储桶中的对象。为此，请运行AWS KMS权限分析器脚本，该脚本可从上的 Amazon Macie 脚本存储库中获得。 GitHub该脚本还可以生成关于 AWS Command Line Interface (AWS CLI) 命令的附加脚本。您可以选择运行这些命令来更新指定 KMS 密钥的必要配置设置和策略。

使用客户提供的密钥进行服务器端加密 (SSE-C)

如果使用服务器端加密和客户提供的密钥 (SSE-C) 对对象进行加密，则 Macie 无法解密该对象。Macie 只能存储和报告对象元数据。

要了解此类加密，请参阅Amazon Simple Storage Service 用户指南的使用客户提供密钥的服务器端加密。

客户端加密

如果对象的加密方式为客户端加密，则 Macie 无法解密此对象。Macie 只能存储和报告对象元数据。例如，Macie 可以报告对象的大小，以及与该对象关联的标签。

要在 Amazon S3 环境中了解此类加密，请参阅Amazon Simple Storage Service 用户指南中的使用客户端加密保护数据。

您可以在 Macie 中 筛选存储桶清单，以确定哪些 S3 存储桶存储了使用特定加密类型的对象。您还可通过存储新对象时的默认设置，确定哪些存储桶使用特定类型的服务器端加密。下表提供了筛选条件示例，您可以将这些筛选条件应用于存储桶清单以查找此信息。

若要显示存储桶……	应用此筛选条件……
存储了使用 SSE-C 加密的对象	加密后的对象计数由客户提供，发件人 = 1
存储使用 DSSE-KMS 或 SSE-KMS 加密的对象	通过加密AWS KMS管理对象计数，并且 F ro m = 1
存储了使用 SSE-S3 加密的对象	加密后的对象计数由 A mazon S3 托管，发件人 = 1
存储了使用客户端加密（或未加密）的对象	加密对象计数为未加密和从 = 1
默认情况下使用 DSSE-KMS 加密对新对象进行加密	默认加密 = aw s: kms: dsse
默认情况下使用 SSE-KMS 加密新对象	默认加密 = aws:kms
默认情况下使用 SSE-S3 加密新对象	默认加密 = AES256

如果将存储桶配置为默认使用 DSSE-KMS 或 SSE-KMS 加密来加密新对象，则您还可以确定使用哪个。AWS KMS key为此，请在 S3 存储桶页面上选择存储桶。在存储桶详细信息面板的 “服务器端加密” 下，请参阅AWS KMS key字段。此字段显示密钥的 Amazon 资源名称（ARN）或唯一标识符（密钥 ID）。

允许 Amazon Macie 使用客户托管 AWS KMS key

如果 Amazon S3 对象使用双层服务器端加密或由客户托管AWS KMS key（DSSE-KMS 或 SSE-KMS）进行服务器端加密，则只有在允许其使用密钥的情况下，Amazon Macie 才能解密该对象。此访问权限的提供方式，取决于拥有密钥的账户是否还拥有存储对象的 S3 存储桶：

- 如果该 AWS KMS key和该存储桶由同一账户拥有，则必须该账户的用户必须更新该密钥的策略。
- 如果该 AWS KMS key由一个账户拥有，而该存储桶由另一个账户拥有，则拥有密钥的账户的用户必须允许对该密钥进行跨账户存取。

本主题介绍如何执行这些任务，并提供了两种场景示例。要详细了解如何允许访问客户托管AWS KMS keys，请参阅《AWS Key Management Service开发人员指南》AWS KMS中的身份验证和访问控制。

允许同一个账户访问客户托管密钥

如果该 AWS KMS key和该 S3 存储桶由同一账户拥有，则该账户的用户必须在密钥的策略中添加一条语句。该附加语句必须允许该 Macie 服务相关角色使用该密钥来解密数据。有关更新密钥政策的详细信息，请参阅 AWS Key Management Service 开发者指南 中的更改密钥政策。

在以下语句中：

- `Principal` 元素必须为拥有 AWS KMS key和 S3 存储桶的账户指定 Macie 服务相关角色的 Amazon 资源名称（ARN）。

  如果账户位于选择加入型 AWS 区域中，则 ARN 还必须包含该区域的相应区域代码。例如，如果账户位于中东（巴林）地区，其区域代码为 me-south-1，`Principal` 元素必须指定`arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`，其中 *`123456789012`* 是该账户的账户 ID。有关当前已开放 Macie 服务的所有区域的列表，请参阅《AWS 一般参考》中的 Amazon Macie 端点和限额。
- 数 `Action` 数组必须指定 `kms:Decrypt` 操作。这是解密使用该密钥进行加密的 S3 对象时必须允许 Macie 执行的唯一 AWS KMS 操作。

以下为添加到 AWS KMS key策略的语句示例。

```
{
    "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": "*"
}
```

在上述示例中：

- `Principal` 元素的 `AWS` 字段指定账户的 Macie 服务相关角色 (`AWSServiceRoleForAmazonMacie`) 的 ARN。它允许 Macie 服务相关角色执行策略语句中指定

的操作。*123456789012* 是示例账户 ID。请将该值替换拥有该 KMS 密钥和 S3 存储桶的账户的 ID。

- `Action` 数组指定了允许该 Macie 服务相关角色使用该 KMS 密钥执行的操作，即解密使用该密钥加密的加密文字。

将此语句添加到密钥政策的位置，取决于该策略当前包含的结构和元素。当添加语句时，请确保语法有效。JSON 格式的密钥策略。这意味着您还必须在语句前后添加逗号，具体取决于您在策略中添加语句的位置。

允许跨账户存取客户托管密钥

如果 AWS KMS key由一个账户拥有（密钥所有者），而 S3 存储桶由另一个账户拥有（存储桶所有者），则密钥所有者必须向存储桶所有者提供对该 KMS 密钥的跨账户存取权限。为此，密钥拥有者首先要确保密钥策略允许存储桶拥有者使用密钥，并为密钥创建授权。然后，存储桶拥有者为此密钥创建授权。授权是一种策略分析工具，如果由授权指定的条件得到满足，则允许 AWS 主体将 KMS 密钥用于加密操作中。在此例中，该授权将相关权限委派给存储桶所有者账户的 Macie 服务相关角色。

有关更新密钥政策的详细信息，请参阅 AWS Key Management Service 开发者指南 中的更改密钥政策。要了解有关授权的信息，请参阅AWS Key Management Service 开发者指南中的AWS KMS授权。

第 1 步：更新密钥政策

在密钥政策中，密钥所有者应确保该策略包含两个语句：

- 第一条语句允许存储桶拥有者使用密钥解密数据。
- 第二条语句允许存储桶所有者为其账户的 Macie 服务相关角色创建授权。

在第一条语句中，`Principal` 元素必须指定存储桶拥有者账户的 ARN。数 `Action` 数组必须指定 `kms:Decrypt` 操作。这是解密使用该密钥进行加密的对象时必须允许 Macie 执行的唯一 AWS KMS 操作。以下为在 AWS KMS key策略中使用此语句的示例。

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
```

```
    ],
    "Resource": "*"
}
```

在上述示例中：

- Principal 元素中的 AWS 字段指定存储桶拥有者账户 (*111122223333*) 的 ARN。它允许存储桶拥有者执行策略语句中指定的操作。*111122223333* 是示例账户 ID。请将该值替换存储桶所有者账户的账户 ID。
- Action 数组指定了允许该存储桶所有者使用该 KMS 密钥执行的操作，即解密使用该密钥加密的加密文字。

密钥政策中的第二条语句，允许存储桶拥有者为其账户的 Macie 服务相关角色创建授权。在此语句中，Principal 元素必须指定存储桶拥有者账户的 ARN。数 Action 数组必须指定 kms:CreateGrant 操作。Condition 元素可以筛选对语句中指定 kms:CreateGrant 操作的访问权限。以下为在 AWS KMS key策略中使用此语句的示例。

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

在上述示例中：

- Principal 元素中的 AWS 字段指定存储桶拥有者账户 (*111122223333*) 的 ARN。它允许存储桶拥有者执行策略语句中指定的操作。*111122223333* 是示例账户 ID。请将该值替换存储桶所有者账户的账户 ID。

- 该 Action 数组指定存储桶拥有者可对 KMS 密钥执行的操作 — 创建密钥授权。
- Condition 元素使用 StringEquals 条件运算符和 kms:GranteePrincipal 条件密钥来筛选策略语句所指定操作的访问权限。在此例中，存储桶所有者只能为指定 GranteePrincipal（即其账户的 Macie 服务相关角色的 ARN）创建授权。在 ARN 中，*111122223333* 是示例账户 ID。请将该值替换存储桶所有者账户的账户 ID。

  如果存储桶所有者的账户位于选择加入型 AWS 区域中，则还需要在 Macie 服务相关角色的 ARN 中包含相应的区域代码。例如，如果账户位于中东（巴林）地区，且该地区代码为 me-south-1，则将 ARN 中的macie.amazonaws.com替换为macie.me-south-1.amazonaws.com。有关当前已开放 Macie 服务的所有区域的列表，请参阅《AWS 一般参考》中的 Amazon Macie 端点和限额。

密钥拥有者将这些语句添加到密钥政策的位置，取决于策略当前包含的结构和元素。当密钥所有者添加语句时，应确保语法有效。密钥策略使用 JSON 格式。这意味着密钥所有者还必须在语句之前或之后添加逗号，具体取决于在策略中添加语句的位置。

第 2 步：创建授权

在密钥拥有者根据需要更新密钥政策后，存储桶拥有者必须为密钥创建授权。该授权将存储桶拥有者账户的相关权限委托至 Macie 服务相关角色。在存储桶拥有者创建授权前，他们应验证是否允许为自己的账户执行kms:CreateGrant操作。此操作使其能够向现有的客户自主管理型 AWS KMS key添加授权。

要创建授权，存储桶拥有者可以使用 AWS Key Management Service API 的CreateGrant操作。存储桶拥有者创建授权时，应为所需参数指定以下值：

- KeyId – KMS 密钥的 ARN。对于跨账户存取 KMS 密钥，该值必须是 ARN。它不能是密钥 ID。
- GranteePrincipal – 其账户的 Macie 服务相关角色（AWSServiceRoleForAmazonMacie）的 ARN。此值应为 arn:aws:iam::*111122223333*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie，其中 *111122223333* 是存储桶拥有者账户的账户 ID。

  如果账户位于选择加入型区域中，则 ARN 还必须包相应的区域代码。例如，假设其账户位于中东（巴林）区域，其区域代码为 me-south-1，则 ARN 应为 arn:aws:iam::*111122223333*:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie，其中 *111122223333* 是存储桶所有者账户的账户 ID。
- Operations – AWS KMS 解密操作（Decrypt）。这是解密使用该 KMS 密钥进行加密的对象时必须允许 Macie 执行的唯一 AWS KMS 操作。

要使用 AWS Command Line Interface（AWS CLI）为客户自主管理型的 KMS 密钥创建授权，请运行 create-grant 命令。下面的示例演示如何操作。此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
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"
```

其中：

- `key-id` 指定要应用授权的 KMS 密钥的 ARN。
- `grantee-principal` 指定了允许执行该授权所指定操作的账户的 Macie 服务相关角色 ARN。该值应与密钥政策中第二个语句的 `kms:GranteePrincipal` 条件指定的 ARN 一致。
- `operations` 指定了授权允许指定主体执行的操作，即解密使用该 KMS 密钥加密的加密文字。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

其中 `GrantToken`，代表已创建授权的唯一、非秘密的、长度可变的 base64 编码字符串，`GrantId` 也是唯一授权标识符。

使用 Amazon Macie 存储和保留敏感数据发现结果

当您运行敏感数据发现任务或 Amazon Macie 执行自动敏感数据发现时，Macie 会为分析范围中包含的每个 Amazon Simple Storage Service (Amazon S3) 对象创建分析记录。这些记录被称为敏感数据发现结果，记录了有关 Macie 对单个 S3 对象执行的分析的详细信息。这包括 Macie 无法检测到敏感数据的对象，因此不会生成调查发现，以及 Macie 由于错误或问题而无法分析的对象。如果 Macie 在物体中检测到敏感数据，则记录将包括来自相应发现的数据以及其他信息。敏感数据发现结果为您提供分析记录，这些记录可能有助于数据隐私和保护审计或调查。

Macie 仅将您的敏感数据发现结果存储 90 天。要访问您的结果并启用它们的长期存储和保留，请将 Macie 配置为使用 AWS Key Management Service (AWS KMS) 密钥加密结果并将其存储在 S3 存储桶

中。存储桶可以用作所有敏感数据发现结果的最终长期存储库。然后，您可以选择访问和查询该存储库中的结果。

本主题将指导您完成使用 AWS Management Console 为敏感数据发现结果配置存储库的过程。该配置是加密结果的 AWS KMS key 、存储结果的 S3 存储桶以及指示要使用的密钥和存储桶的 Macie 设置的组合。如果您更喜欢以编程方式配置 Macie 设置，则可以使用 Amazon Macie API 的PutClassificationExportConfiguration操作。

在 Macie 中配置设置时，您的选择仅适用于当前的 AWS 区域。如果您是组织的 Macie 管理员，则您的选择仅适用于您的账户。它们不适用于任何关联的成员账户。

如果您在多个区域中使用 Macie AWS 区域，请为使用 Macie 的每个区域配置存储库设置。您可以选择将多个区域的敏感数据发现结果存储在同一个 S3 存储桶中。不过，请注意以下要求：

- 要存储默认 AWS 启用的区域（例如美国东部（弗吉尼亚北部）地区的结果，您必须在默认情况下启用的区域中选择一个存储桶。 AWS 账户结果不能存储在选择加入型区域（默认情况下被禁用的区域）的存储桶中。
- 对于选择加入型区域，例如如中东（巴林）区域，要存储该区域的结果，您必须在同一区域或默认启用的区域中选择存储桶。结果不能存储在另一个选择加入型区域的存储桶中。

要确定某个区域是否已默认启用，请参阅《AWS Identity and Access Management 用户指南》中的 区域和端点。除了上述要求外，还要考虑是否要检索 Macie 在个别调查结果中报告的敏感数据样本。要从受影响的 S3 对象检索敏感数据样本，必须将以下所有资源和数据存储在同一个区域中：受影响的对象、适用的发现结果和相应的敏感数据发现结果。

任务

概述

当您运行敏感数据发现作业或为您的账户或组织执行自动敏感数据发现时，Amazon Macie 会自动为其分析或尝试分析的每个 Amazon S3 对象创建敏感数据发现结果。这包括：

- Macie 在其中检测敏感数据的对象，因此也会生成敏感数据调查发现。

- Macie 不会检测到敏感数据的对象，因此不会生成敏感数据调查发现。
- Macie 由于错误或问题（例如权限设置或使用不受支持的文件或存储格式）而无法分析的对象。

如果 Macie 在 S3 对象中检测到敏感数据，则敏感数据调查发现将包含来自相应敏感数据查找的数据。它还提供了其他信息，例如 Macie 在对象中发现的每种敏感数据出现多达 1000 次的位置。例如：

- Microsoft Excel 工作簿、CSV 文件或 TSV 文件中单元格或字段的列号和行号
- JSON 或 JSON Lines 文件中的字段或数组路径
- 除 CSV、JSON、JSON Lines 或 TSV 文件之外的非二进制文本文件中的行号，例如 HTML、TXT 或 XML 文件
- Adobe 可移植文档格式 (PDF) 文件中页面的页码
- Apache Avro 对象容器或 Apache Parquet 文件中记录的字段的记录索引和路径

如果受影响的 S3 对象是存档文件（如 .tar 或 .zip 文件），则敏感数据发现结果还会提供 Macie 从存档中提取的单个文件中敏感数据出现的详细位置数据。Macie 不会在存档文件的敏感数据调查发现中包含此信息。为了报告位置数据，敏感数据发现结果使用标准化 JSON 架构。

敏感数据发现结果不包括 Macie 发现的敏感数据。相反，它为您提供了有助于审计或调查的分析记录。

Macie 会将您的敏感数据发现结果存储 90 天。您无法直接在 Amazon Macie 控制台或使用 Amazon Macie API 访问它们。相反，请按照本主题中的步骤将 Macie 配置为使用您指定的加密结果，并将结果存储在您也指定的 S3 存储桶中。 AWS KMS key 然后，Macie 会将结果写入 JSON Lines（.jsonl）文件，将这些文件作为 GNU Zip（.gz）文件添加到存储桶中，然后使用 SSE-KMS 加密对数据进行加密。从 2023 年 11 月 8 日起，Macie 还会使用 HMAC 散列消息认证码 AWS KMS key对生成的 S3 对象进行签名。

将 Macie 配置为将您的敏感数据发现结果存储在某个 S3 存储桶中后，该存储桶可以作为这些结果的权威长期存储库。然后，您可以选择访问和查询该存储库中的结果。

> **Tip**
>
> 有关如何查询和使用敏感数据发现结果来分析和报告潜在的数据安全风险的详细教学示例，请参阅安全博客上的 “如何使用 Amazon Athena 和 A QuickSight mazon 查询和可视化 Macie 敏感数据发现结果” 博客文章。AWS

有关可用于分析敏感数据发现结果的 Amazon Athena 查询示例，请访问上的 Amazon Macie 结果分析存储库。 GitHub此存储库还提供了有关配置 Athena 以检索和解密结果的说明，以及用于为结果创建表的脚本。

第 1 步：验证权限

在为敏感数据发现结果配置存储库之前，请确认您具有加密和存储结果所需的权限。要验证您的权限，请使用 AWS Identity and Access Management (IAM) 查看附加到您的 IAM 身份的 IAM 策略。然后，将这些策略中的信息与以下操作列表进行比较，您必须允许这些操作来配置存储库。

Amazon Macie

对于 Macie，请验证是否允许您执行以下操作：

`macie2:PutClassificationExportConfiguration`

此操作允许您在 Macie 中添加或更改存储库设置。

Amazon S3

对于 Amazon S3，请验证您是否被允许执行以下操作：

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

通过这些操作，您可以访问和配置可用作存储库的 S3 存储桶。

AWS KMS

要使用 Amazon Macie 控制台添加或更改存储库设置，还要验证您是否被允许执行以下 AWS KMS 操作：

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

通过这些操作，您可以检索和显示有关账户的 AWS KMS keys 的信息。然后，您可以选择其中一个密钥来加密敏感数据发现结果。

如果您计划创建新的 AWS KMS key 来加密数据，则还需要允许您执行以下操作：`kms:CreateKey`、`kms:GetKeyPolicy`和`kms:PutKeyPolicy`。

如果不允许你执行必要的操作，请在继续下一步之前向 AWS 管理员寻求帮助。

步骤 2：配置 AWS KMS key

验证权限后，确定 AWS KMS key 您希望 Macie 使用哪个来加密您的敏感数据发现结果。该密钥必须是客户托管的对称加密 KMS 密钥，该密钥与您要存储结果的 S3 存储桶 AWS 区域 相同。

密钥可以是您自己账户 AWS KMS key 中的现有密钥，也可以是其他账户拥有 AWS KMS key 的现有密钥。如果要使用新的 KMS 密钥，请在继续之前创建密钥。如果要使用其他账户拥有的现有密钥，请获取该密钥的 Amazon 资源名称（ARN）。在 Macie 中配置存储库设置时，您需要输入此 ARN。有关创建和查看 KMS 密钥设置的信息，请参阅 AWS Key Management Service 开发者指南中的管理密钥。

> **Note**
>
> 密钥可以 AWS KMS key 位于外部密钥存储库中。但是，与完全在 AWS KMS中管理的密钥相比，密钥可能更慢且更不可靠。您可以通过将敏感数据发现结果存储在配置为将密钥用作 S3 Bucket 密钥的 S3 存储桶中来降低此风险。这样做可以减少加密敏感数据发现结果所必须发出的 AWS KMS 请求数。
>
> 有关在外部密钥存储中使用 KMS 密钥的信息，请参阅 AWS Key Management Service 开发者指南中的外部密钥存储。有关使用 S3 存储桶密钥的信息，请参阅 Amazon Simple Storage Service 用户指南中的通过 Amazon S3 存储桶密钥降低 SSE-KMS 成本。

确定您希望 Macie 使用哪个 KMS 密钥后，授予 Macie 使用该密钥的权限。否则，Macie 将无法在存储库中加密或存储您的结果。若要授予 Macie 使用密钥的权限，请更新密钥的密钥政策。有关密钥政策和管理对 KMS 密钥的访问的详细信息，请参阅 AWS Key Management Service 开发者指南中的AWS KMS中的密钥政策。

更新密钥策略

1. 打开 AWS KMS 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。

3. 选择您希望 Macie 用于加密敏感数据发现结果的密钥。
4. 在密钥政策选项卡上，选择编辑。
5. 将以下语句复制到剪贴板，然后将其添加到策略中：

```
{
    "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/*"
             ]
         }
    }
}
```

添加语句时，请确保语法有效。策略使用 JSON 格式。这意味着您还需要在语句之前或之后添加逗号，具体取决于将语句添加到策略的位置。如果将该语句添加为最后一个语句，请在前一个语句的右大括号后添加逗号。如果将其添加为第一个语句或两个现有语句之间，请在语句的右大括号后添加逗号。

6. 使用适合您的环境的正确值更新语句：

- 在 Condition 字段中，替换占位符值，其中：
  - *111122223333* 是 AWS 账户的账户 ID。
  - *##*是你使用 Macie 并且你想允许 Macie 使用密钥的区域。 AWS 区域

    如果您在多个区域中使用 Macie，并希望允许 Macie 在其他区域中使用密钥，请为每个附加区域添加 aws:SourceArn 个条件。例如：

```
"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/*"
]
```

或者，您可以允许 Macie 在所有区域中使用密钥。为此，请将占位符值替换为通配符 (*)。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- 如果您在选择加入型区域中使用 Macie，请将相应的区域代码添加到 `Service` 字段的值中。例如，如果您在中东（巴林）区域中使用 Macie，其区域代码为 me-south-1，请将 `macie.amazonaws.com` 替换为 `macie.me-south-1.amazonaws.com`。有关 Macie 当前可用区域的列表以及每个区域的区域代码，请参阅 AWS 一般参考 中的 Amazon Macie 端点和限额。

请注意，`Condition` 字段使用两个 IAM 全局条件密钥：

- a@@ ws: SourceAccount — 此条件仅允许 Macie 对您的账户执行指定操作。更具体地说，它确定哪个账户可以对 `aws:SourceArn` 条件指定的资源和操作执行指定的操作。

  若要允许 Macie 对其他账户执行指定操作，请将每个其他账户的账户 ID 添加到此条件中。例如：

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

- a@@ w SourceArn s: — 此条件会 AWS 服务 阻止其他人执行指定的操作。它还可以防止 Macie 在为您的账户执行其他操作时使用该密钥。换言之，仅当 S3 对象是敏感数据发现结果，并且仅当这些结果属于自动敏感数据发现的结果或指定账户在指定区域创建的敏感数据发现作业时，才允许 Macie 使用该密钥来加密这些对象。

  要允许 Macie 对其他账户执行指定的操作，请将每个其他账户的 ARN 添加到此条件。例如：

  ```
  "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/*"
]
```

`aws:SourceAccount` 和 `aws:SourceArn` 条件指定的账户应匹配。

这些条件有助于防止Macie在与之进行交易时被用作困惑不解的 AWS KMS副手。尽管我们不建议这样做，但您可以从语句中删除这些条件。

7. 添加和更新完语句后，选择 保存更改。

步骤 3：选择 S3 存储桶

在验证权限并配置之后 AWS KMS key，您就可以指定要使用哪个 S3 存储桶作为敏感数据发现结果的存储库了。您有两种选择：

- 使用 Macie 创建的新 S3 存储桶 — 如果您选择此选项，Macie 会自动在当前版本中 AWS 区域 为您的发现结果创建一个新的 S3 存储桶。Macie 还会将存储桶策略应用于存储桶。该策略允许 Macie 向存储桶添加对象。此外还要求使用您指定的 AWS KMS key 和 SSE-KMS 加密方法加密这些对象。要检查策略，请在指定存储桶的名称和要使用的 KMS 密钥后，在 Amazon Macie 控制台上选择查看策略。
- 使用您创建的现有 S3 存储桶 – 如果您希望将发现结果存储在您创建的特定 S3 存储桶中，请先创建该存储桶，然后再继续。然后检查存储桶的设置并更新存储桶的策略，以确保 Macie 可以向存储桶添加对象。本主题介绍要检查的设置以及如何更新策略。它还提供了要添加到策略中的语句的示例。

以下部分提供了每个选项的说明。选择所需选项的部分。

使用 Macie 创建的新 S3 存储桶

如果您希望使用 Macie 为您创建的新 S3 存储桶，则该过程的最后一步是在 Macie 中配置存储库设置。

在 Macie 中配置存储库设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的设置下，选择发现结果。

3. 在敏感数据发现结果存储库下，选择创建存储桶。
4. 在创建存储桶对话框中，输入存储桶的名称。

   该名称在所有 S3 存储桶中必须是唯一的。此外，名称只能由小写字母、数字、句点 (.) 和连字符 (-) 组成。有关其他命名要求，请参阅 Amazon Simple Storage Service 用户指南中的存储桶命名规则。
5. 展开 Advanced (高级) 部分。
6. （可选）要指定要在存储桶中某个位置的路径中使用的前缀，请在数据发现结果前缀框中输入前缀。

   当您输入值时，Macie 会更新框下方的示例，以显示存储发现结果的存储桶位置的路径。
7. 对于 阻止所有公有访问，选择 是 以启用存储桶的所有阻止公有访问设置。

   有关这些设置的信息，请参阅 Amazon Simple Storage Service 用户指南中的阻止对 Amazon S3 存储的公有访问。
8. 在加密设置下，指定您希望 Macie 用于加密结果的 AWS KMS key ：

   - 要使用您自己账户中的密钥，请选择 从您的账户中选择密钥。然后，在AWS KMS key列表中，选择要使用的密钥。该列表显示您账户的客户托管的对称加密 KMS 密钥。
   - 要使用其他账户拥有的密钥，请选择输入来自另一个账户的密钥的 ARN。然后，在 AWS KMS key ARN 框内，输入要使用的密钥的 Amazon 资源名称（ARN），例如 **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**。
9. 输入完设置后，选择保存。

   Macie 会测试设置以验证它们是否正确。如果任何设置不正确，Macie 会显示一条错误消息，以帮助您解决问题。

保存存储库设置后，Macie 会将前 90 天的现有发现结果添加到存储库中。Macie 还开始向存储库添加新的发现结果。

使用您创建的现有 S3 存储桶

如果您希望将敏感数据发现结果存储在您创建的特定 S3 存储桶中，请先创建并配置该存储桶，然后再在 Macie 中配置存储库设置。创建存储桶时，请注意以下要求：

- 如果为存储桶启用对象锁定，则必须禁用该功能的默认保留设置。否则，Macie 将无法将您的发现结果添加到存储桶中。有关此设置的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 S3 对象锁定。

- 要存储默认启用的区域（例如美国东部（弗吉尼亚北部）地区的发现结果，存储桶必须位于默认启用的区域中。 AWS 账户结果不能存储在选择加入型区域（默认情况下被禁用的区域）的存储桶中。
- 对于选择加入型区域，例如如中东（巴林）区域，要存储该区域的发现结果，该存储桶必须位于同一区域或默认启用的区域。结果不能存储在另一个选择加入型区域的存储桶中。

要确定某个区域是否已默认启用，请参阅《AWS Identity and Access Management 用户指南》中的区域和端点。

创建存储桶后，更新存储桶的策略以允许 Macie 检索有关存储桶的信息并将对象添加到存储桶。然后，您可以在 Macie 中配置存储库设置。

更新存储桶的存储桶策略

1. 打开 Amazon S3 控制台，网址为：https://console.aws.amazon.com/s3/。
2. 选择要在其中存储发现结果的存储桶。
3. 选择 Permissions（权限）选项卡。
4. 在存储桶策略部分中，选择编辑。
5. 将以下示例策略复制到剪贴板：

```
{
    "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. 将示例策略粘贴到 Amazon S3 控制台上的存储桶策略编辑器中。
7. 使用适合您环境的正确值更新示例策略：

   - 在拒绝不正确的加密标头的可选语句中：
     - *myBucketName*替换为存储桶的名称。
     - StringNotEquals在这种情况下，将 *arn: aws: kms: region: 111122223333: key/KMS ################## (AR KeyId* N)。 AWS KMS key
   - 在所有其他语句中，替换占位符值，其中：
     - *myBucketName*是存储桶的名称。
     - *111122223333* 是 AWS 账户的账户 ID。
     - *Region* 是您在其中使用 Macie 并希望允许 Macie 将发现结果添加到存储桶的 AWS 区域 。

     如果您在多个区域中使用 Macie，并希望允许 Macie 将结果添加到其他区域的存储桶中，请为每个其他区域添加 aws:SourceArn 条件。例如：

     ```
     "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/*"
]
```

或者，您可以允许 Macie 将结果添加到您使用 Macie 的所有区域的存储桶中。为此，请将占位符值替换为通配符 (*)。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- 如果您在选择加入型区域中使用 Macie，请在每个指定 Macie 服务主体的语句中将相应的区域代码添加到 `Service` 字段的值中。例如，如果您在中东（巴林）区域使用 Macie，其区域代码为 me-south-1，请在每个适用的语句中将 `macie.amazonaws.com` 替换为 `macie.me-south-1.amazonaws.com`。有关 Macie 当前可用区域的列表以及每个区域的区域代码，请参阅 AWS 一般参考 中的 Amazon Macie 端点和限额。

请注意，示例策略包含允许 Macie 确定存储桶所在的区域（`GetBucketLocation`）以及向存储桶添加对象（`PutObject`）的语句。这些语句定义使用两个 IAM 全局条件密钥的条件：

- a@@ ws: SourceAccount — 此条件仅允许 Macie 将您的账户的敏感数据发现结果添加到存储桶中。它可以防止 Macie 将其他账户的发现结果添加到存储桶中。更具体地说，该条件指定哪个账户可以将存储桶用于 `aws:SourceArn` 条件指定的资源和操作。

  要在存储桶中存储其他账户的结果，请将每个其他账户的账户 ID 添加到此条件中。例如：

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

- a@@ ws: SourceArn — 此条件根据要添加到存储桶中的对象的来源限制对存储桶的访问权限。它可以 AWS 服务 防止其他人向存储桶添加对象。它还可以防止 Macie 在为您的账户执行其他操作时向存储桶添加对象。更具体地说，仅当相关对象是敏感数据发现结果，并且仅当这些结果属于自动敏感数据发现的结果或指定账户在指定区域创建的敏感数据发现作业时，才允许 Macie 将这些对象添加到该存储桶

  要允许 Macie 对其他账户执行指定的操作，请将每个其他账户的 ARN 添加到此条件。例如：

```
"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/*"
]
```

`aws:SourceAccount` 和 `aws:SourceArn` 条件指定的账户应匹配。

这两种情况都有助于防止 Macie 在与 Amazon S3 的交易中被用作混乱的代理。尽管我们不建议这样做，但您可以从存储桶策略中删除这些条件。

8. 完成存储桶策略更新后，选择保存更改。

您现在可以在 Macie 中配置存储库设置。

在 Macie 中配置存储库设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中的设置下，选择发现结果。
3. 在 敏感数据发现结果存储库 下，选择 现有存储桶。
4. 对于选择存储桶，选择要在其中存储发现结果的存储桶。
5. （可选）要指定要在存储桶中某个位置的路径中使用的前缀，请展开高级部分。然后，对于数据发现结果前缀，输入要使用的前缀。

   当您输入值时，Macie 会更新框下方的示例，以显示存储发现结果的存储桶位置的路径。
6. 在加密设置下，指定您希望 Macie 用于加密结果的 AWS KMS key ：

   - 要使用您自己账户中的密钥，请选择 从您的账户中选择密钥。然后，在AWS KMS key列表中，选择要使用的密钥。该列表显示您账户的客户托管的对称加密 KMS 密钥。
   - 要使用其他账户拥有的密钥，请选择输入来自另一个账户的密钥的 ARN。然后，在 AWS KMS key ARN 框中，输入要使用的密钥的 ARN，例如 **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**。
7. 输入完设置后，选择保存。

   Macie 会测试设置以验证它们是否正确。如果任何设置不正确，Macie 会显示一条错误消息，以帮助您解决问题。

保存存储库设置后，Macie 会将前 90 天的现有发现结果添加到存储库中。Macie 还开始向存储库添加新的发现结果。

> **Note**
>
> 如果您随后更改了数据发现结果前缀设置，请同时更新 Amazon S3 中的存储桶策略。指定先前路径的策略语句必须指定新路径。否则，Macie 将无法将您的发现结果添加到该存储桶。

> **Tip**
>
> 要降低服务器端加密成本，还要将 S3 存储桶配置为使用 S3 存储桶密钥，并指定您为加密敏感数据发现结果而配置的。 AWS KMS key 使用 S3 存储桶密钥可以减少对的调用次数 AWS KMS，从而降低 AWS KMS 请求成本。如果 KMS 密钥位于外部密钥存储中，则使用 S3 Bucket 密钥还可以最大程度地减少使用密钥对性能的影响。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

Amazon Macie 支持的存储类别和格式

为了帮助您发现 Amazon Simple Storage Service (Amazon S3) 数据资产中的敏感数据，Amazon Macie 支持大多数 Amazon S3 存储类以及各种文件和存储格式。此支持适用于使用 托管数据标识符 和 自定义数据标识符 来分析 S3 对象的场景。

要使 Macie 分析 S3 对象，必须使用支持的存储类将对象存储在 Amazon S3 通用型存储桶中。该对象还必须使用受支持的文件或存储格式。本节中的主题列出了 Macie 当前支持的存储类别以及文件和存储格式。

> **Tip**
>
> 尽管 Macie 针对 Amazon S3 进行了优化，但您可以使用它来发现当前存储在其他位置的资源中的敏感数据。为此，您可以暂时或永久地将数据移动到 Amazon S3。例如，将 Amazon Relational Database Service 或 Amazon Aurora 快照以 Apache Parquet 格式导出到 Amazon S3。或者将 Amazon DynamoDB 表导出到 Amazon S3。然后，您可以创建敏感数据发现任务来分析 Amazon S3 中的数据。

主题

支持的 Amazon S3 存储类别

对于敏感数据发现，Amazon Macie 支持以下 Amazon S3 存储类别：

- 去冗余 (RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 单区 – 不频繁访问（S3 单区 – IA）
- S3 标准
- S3 标准 - 不频繁访问（S3 标准 - IA）

Macie 不会分析使用其他 Amazon S3 存储类别（如 S3 Glacier Deep Archive 或 S3 Express One Zone）的 S3 对象。此外，Macie 不会分析存储在 Amazon S3 目录存储桶中的对象。

如果您将敏感数据发现任务配置为分析不使用受支持的 Amazon S3 存储类的 S3 对象，则 Macie 会在任务运行时跳过这些对象。Macie 不会尝试检索或分析对象中的数据，这些对象被视为不可分类的对象。不可分类的对象是指不使用受支持的存储类或受支持的文件或存储格式的对象。Macie 仅分析那些使用受支持的存储类和支持的文件或存储格式的对象。

同样，如果将 Macie 配置为执行自动敏感数据发现，则不可分类的对象不符合选择和分析条件。Macie 仅选择使用受支持的 Amazon S3 存储类别以及受支持的文件或存储格式的对象。

要识别包含不可分类的对象的 S3 存储桶，您可以筛选 S3 存储桶清单。对于清单中的每个存储桶，都有字段报告存储桶中不可分类的对象的数量和总存储大小。

有关 Amazon S3 提供的存储类的详细信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 存储类别。

支持的文件和存储格式

当 Amazon Macie 分析 S3 对象时，Macie 会从 Amazon S3 中检索该对象的最新版本，然后对对象的内容执行深入检查。此检查会考虑数据的文件或存储格式。Macie 可以分析许多不同格式的数据，包括常用的压缩和存档格式。

当 Macie 分析压缩文件或存档文件中的数据时，Macie 会检查完整文件和文件内容。为了检查文件的内容，Macie 会解压缩该文件，然后检查使用受支持格式的每个提取文件。Macie 可以对多达 1,000,000 个文件和高达 10 个级别的嵌套深度执行此操作。有关适用于敏感数据发现的其他配额的信息，请参阅 Amazon Macie 限额。

下表列出并描述了 Macie 可以分析以检测敏感数据的文件类型和存储格式。对于每种受支持的类型，该表还列出了适用的文件扩展名。

文件或存储类型	描述	文件扩展名
大数据	Apache Avro 对象容器和 Apache Parquet 文件	.avro、.parquet
压缩或存档	GNU Zip 压缩存档、TAR 存档和 ZIP 压缩存档	.GZ， .gzip， .tar， .zip
文档	Adobe 可移植文档格式文件、Microsoft Excel 工作簿和 Microsoft Word 文档	.doc、.docx、.pdf、.xls、.xlsx
电子邮件消息	其内容符合 IETF RFC 为电子邮件指定的要求（如 RFC 2822）的电子邮件文件	.eml
文本	非二进制文本文件，例如逗号分隔值 (CSV) 文件、超文本标记语言 (HTML) 文件、JavaScript 对象表示法 (JSON) 文件、JSON Lines 文件、纯文本文档、制表符分隔值 (TSV) 文件和可扩展标记语言 (XML) 文件	.csv、.htm、.html、.json、.jsonl、.tsv、.txt、.xml 等（取决于非二进制文本文件的类型）

Macie 不会分析图像、音频、视频和其他类型的多媒体内容中的数据。

如果您将敏感数据发现作业配置为分析不使用受支持的文件或存储格式的 S3 对象，则 Macie 会在作业运行时跳过这些对象。Macie 不会尝试检索或分析对象中的数据，这些对象被视为不可分类的对象。不

可分类的对象是指不使用受支持的 Amazon S3 存储类或受支持的文件或存储格式的对象。Macie 仅分析那些使用受支持的存储类和支持的文件或存储格式的对象。

同样，如果将 Macie 配置为执行自动敏感数据发现，则不可分类的对象不符合选择和分析条件。Macie 仅选择使用受支持的 Amazon S3 存储类别以及受支持的文件或存储格式的对象。

要识别包含不可分类的对象的 S3 存储桶，您可以筛选 S3 存储桶清单。对于清单中的每个存储桶，都有字段报告存储桶中不可分类的对象的数量和总存储大小。

分析 Amazon Macie 调查发现

当 Amazon Macie 检测到潜在的违反策略或 Amazon Simple Storage Service (Amazon S3) 存储桶的安全或隐私问题，或者检测到 S3 对象中的敏感数据时，它会生成调查发现。调查发现是 Macie 发现的潜在问题或敏感数据的详细报告。每个调查发现都提供了严重性评级、有关受影响资源的信息以及其他详细信息，例如 Macie 何时以及如何发现问题或数据。Macie 会将您的策略和敏感数据调查发现存储 90 天。

您可以通过以下方法查看、分析和管理调查发现。

Amazon Macie 控制台

Amazon Macie 控制台上的调查发现页面列出了您的调查发现，并提供了各个调查发现的详细信息。这些页面还提供用于对调查发现进行分组、筛选和排序以及创建和管理禁止规则的选项。禁止规则可以帮助您简化对调查发现的分析。

Amazon Macie API

借助 Amazon Macie API，您可以使用 AWS 命令行工具或 AWS SDK，或者直接向 Macie 发送 HTTPS 请求来查询和检索调查发现数据。要查询数据，您需要向 Amazon Macie API 提交请求，然后使用支持的参数来指定要检索哪些调查发现。提交请求后，Macie 将以 JSON 响应的形式返回结果。然后，您可以将结果传递给另一个服务或应用程序，以进行更深入的分析、长期存储或报告。有关更多信息，请参阅Amazon Macie API 参考资料。

Amazon EventBridge

为了进一步支持与其他服务和系统（例如监控或事件管理系统）集成，Macie 会将调查发现以事件形式发布至 Amazon EventBridge。EventBridge（前身为 Amazon CloudWatch Events）是一项无服务器事件总线服务，可以从您自己的应用程序、软件即服务（SaaS）应用程序和 Macie 等 AWS 服务 应用程序传输实时数据流。它可以将这些数据路由到 AWS Lambda 函数、Amazon Simple Notification Service 主题和 Amazon Kinesis 流等目标，以进行额外的自动处理。使用 EventBridge 还有助于确保长期保留调查发现数据。要了解有关 EventBridge 的更多信息，请参阅 Amazon EventBridge 用户指南。

Macie 会自动将事件发布到 EventBridge 以获取新调查发现。它还为现有策略调查发现的后续事件自动发布事件。由于调查发现数据是以 EventBridge 事件为结构的，因此您可以使用其他服务和工具更轻松地监控、分析调查发现，并根据这些调查发现采取行动。例如，您可以使用 EventBridge 将特定类型的新调查发现自动发送到 AWS Lambda 函数，该函数反过来会处理数据并将其发送到您的安全事件和事件管理 (SIEM) 系统。如果您将 AWS 用户通知服务与 Macie 集成，则还可以使

用事件通过您指定的交付渠道自动收到有关调查发现的通知。要了解如何使用 EventBridge 事件来监控和处理调查发现，请参阅 Amazon Macie与 Amazon EventBridge 集成。

AWS Security Hub

要对组织的安全态势进行更多、更广泛的分析，您也可以将调查发现发布到 AWS Security Hub。Security Hub 是一项从 AWS 服务 和支持的 AWS Partner Network 安全解决方案中收集安全数据的服务，可为您提供整个 AWS 环境中安全状态的全面视图。Security Hub 还可以帮助您根据安全行业标准和最佳实践检查环境。要了解有关 Security Hub 的更多信息，请参阅 AWS Security Hub 用户指南。要了解如何使用 Security Hub 来监控和处理调查发现，请参阅 Amazon Macie 与 AWS Security Hub 集成。

除了调查发现外，Macie 还会为 S3 对象创建敏感数据调查发现，并对其进行分析以发现敏感数据。敏感数据发现结果是关于对象分析的详细信息的记录。这包括 Macie 无法发现到敏感数据的对象，因此不会生成调查发现，以及 Macie 由于错误或问题而无法分析的对象。敏感数据发现结果为您提供分析记录，这些记录可能有助于数据隐私和保护审计或调查。您无法直接在 Amazon Macie 控制台或使用 Amazon Macie API 访问敏感数据发现结果。相反，您可以配置 Macie 将结果存储至 S3 存储桶内。然后，您可以选择访问和查询该存储桶中的结果。要了解如何配置 Macie 以存储结果，请参阅 存储和保留敏感数据发现结果。

主题

Amazon Macie 调查发现的类型

Amazon Macie 会生成两类调查发现：策略调查发现和敏感数据调查发现。策略调查发现是有关 Amazon Simple Storage Service (Amazon S3) 存储桶的潜在策略违规或安全或隐私问题的详细报告。Macie 会生成策略调查发现，作为其持续活动的一部分，以评测和监控您的 S3 存储桶的安全性和访问控制。敏感数据调查发现是 Macie 在 S3 对象中检测到的敏感数据的详细报告。当您运行敏感数据

发现作业或为您的账户执行自动化敏感数据发现时，Macie 会生成敏感数据调查发现，作为其执行的活动的一部分。

在每个类别中，都有特定的类型。调查发现的类型有助于深入了解 Macie 发现的问题或敏感数据的性质。调查发现的详细信息提供了严重性评级、受影响资源的信息以及其他信息，例如 Macie 何时以及如何发现问题或敏感数据。每个调查发现的严重性和细节因其类型和性质而异。

主题

> **Tip**
>
> 要探索和了解 Macie 可以生成的不同类别和类型的调查发现，请创建示例调查发现。样本调查发现使用示例数据和占位符值来演示每种类型的调查发现可能包含的信息类型。

策略调查发现的类型

当 S3 存储桶的策略或设置更改导致存储桶及其对象的安全性或隐私性降低时，Amazon Macie 会生成策略调查发现。有关 Macie 如何检测这些更改的信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。

只有您在为您的 AWS 账户 启用 Macie 之后发生更改时，Macie 才会生成策略调查发现。例如，如果在启用 Macie 后禁用了 S3 存储桶的封禁公开访问设置，则 Macie 会为该存储桶生成一个策略：iam BlockPublicAccessDisabled user/S3 查找结果。但是，如果您在启用 Macie 时禁用了存储桶的封禁公共访问设置，但这些设置继续处于禁用状态，则 Macie 不会为该存储桶生成策略:iamU BlockPublicAccessDisabled ser/S3 查找结果。

如果 Macie 检测到现有策略调查发现后续出现，Macie 会通过添加有关后续事件的详细信息并增加发生次数来更新现有调查发现。Macie 将策略调查发现存储 90 天。

Macie 可以为 S3 存储桶生成以下类型的策略调查发现。

Policy:IAMUser/S3BlockPublicAccessDisabled

该存储桶的所有存储桶级阻止公共访问设置均已禁用。对存储桶的访问由账户的阻止公共访问设置、访问控制列表（ACL）以及存储桶的存储桶策略控制。

要了解 S3 存储桶的阻止公共访问设置，请参阅 《Amazon Simple Storage Service 用户指南》中的阻止对 Amazon S3 存储的公共访问。

Policy:IAMUser/S3BucketEncryptionDisabled

存储桶的默认加密设置已重置为默认 Amazon S3 加密行为，即使用 Amazon S3 托管密钥自动加密新对象。

从 2023 年 1 月 5 日开始，Amazon S3 自动应用服务器端加密，并使用 Amazon S3 托管式密钥 (SSE-S3) 作为添加到存储桶的对象的基本加密级别。您可以选择配置存储桶的默认加密设置，改为使用带密钥的服务器端加密 (SSE-KMS) 或使用AWS KMS密钥的双层服务器端加密 (DSSE-KM AWS KMS S)。要了解 S3 存储桶的默认加密设置和选项，请参阅 《Amazon Simple Storage Service 用户指南》中的设置 S3 存储桶的默认服务器端加密行为。

如果 Macie 在 2023 年 1 月 5 日之前生成了此类调查发现，则该调查发现表明受影响的存储桶已禁用默认加密设置。这意味着存储桶的设置没有为新对象指定默认的服务器端加密行为。Amazon S3 不再支持禁用存储桶默认加密设置的功能。

Policy:IAMUser/S3BucketPublic

存储桶的 ACL 或存储桶策略已更改为允许匿名用户或所有经过身份验证的 AWS Identity and Access Management (IAM) 身份访问。

要了解 S3 存储桶的 ACL 和存储桶策略，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的身份和访问管理。

Policy:IAMUser/S3BucketReplicatedExternally

复制已启用并配置为将对象从存储桶复制到组织外部（不是组织的一部分）的 AWS 账户 中。组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。

在某些条件下，Macie 可能会为未配置为将对象复制到外部 AWS 账户 存储桶的存储桶生成此类调查发现。如果目标存储桶是在过去 24 小时内，也就是 Macie 在每日刷新周期中从 Amazon S3 检索存储桶和对象元数据之后在不同的 AWS 区域 中创建，则可能会发生这种情况。要调查发现结果，请先刷新您的清单数据。然后查看存储桶的详细信息。详细信息会显示存储桶是否配置为将对象复制到其他存储桶。如果存储桶配置为执行此操作，则详细信息将包括拥有目标存储桶的每个账户的账户 ID。

要了解 S3 存储桶的复制设置，请参阅 《Amazon Simple Storage Service 用户指南》中的复制对象。

Policy:IAMUser/S3BucketSharedExternally

存储桶的 ACL 或存储桶策略已更改，以允许与组织外部的 AWS 账户（不是组织的一部分）共享存储桶。组织被定义为一组 Macie 账户，这些账户通过 AWS Organizations 或受 Macie 邀请作为一组相关账户进行集中管理。

在某些情况下，Macie 可能会为未与外部 Amazon Web Services account 共享的存储桶生成此类调查发现。如果 Macie 无法完全评测存储桶策略中的 `Principal` 元素与该策略 `Condition` 元素中的某些 AWS 全局条件上下文密钥或 Amazon S3 条件密钥之间的关系，则可能会发生这种情况。适用的条件密钥为：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:PrincipalOr` 和 `s3:DataAccessPointArn`。我们建议您检查存储桶的策略，以确定此访问是否为预期行为且是安全的。

要了解 S3 存储桶的 ACL 和存储桶策略，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 中的身份和访问管理。

Policy:IAMUser/S3BucketSharedWithCloudFront

存储桶的存储桶策略已更改，允许与 Amazon CloudFront 原始访问身份 (OAI)、源站访问控制 (OAC) 或 OAI 和 OA CloudFront I 和 OAC 共享存储桶。 CloudFront CloudFront CloudFront OAI 或 OAC 允许用户通过一个或多个指定的 CloudFront分配访问存储桶的对象。

要了解 CloudFront OAI 和 OAC，请参阅亚马逊 CloudFront开发者指南中的限制对 Amazon S3 来源的访问。

> **Note**
>
> 在某些情况下，Macie 会为存储桶生成策略:iamuser/S3 BucketSharedExternally 查找结果，而不是策略:iamUser/S3 查找结果。BucketSharedWithCloudFront这些情况包括：
>
> - 除了 CloudFront OAI 或 OAC 之外，AWS 账户该存储桶还与组织外部的用户共享。
> - 存储桶的策略指定 OAI 的规范用户 ID，而不是亚马逊资源名称 (ARN)。 CloudFront
>
> 这会为存储桶生成更高严重性的策略调查发现。

敏感数据调查发现的类型

Macie 在 S3 对象中检测到敏感数据时，会生成敏感数据调查发现，并对其进行分析以发现敏感数据。这包括 Macie 在您运行敏感数据发现作业和自动化敏感数据发现时执行的分析。

例如，如果您创建并运行敏感数据发现任务，而 Macie 在 S3 对象中检测到银行账号，则 Macie 会为该对象生成 A: s3Ob SensitiveData ject/Financial 查找结果。同样，如果 Macie 在自动敏感数据发现周期中检测到其分析的 S3 对象中的银行账号，则 Macie 会为该对象生成 A: s3Ob SensitiveData ject/Financial 查找结果。

如果 Macie 在随后的作业运行或自动化敏感数据发现周期中检测到同一 S3 对象中的敏感数据，则 Macie 会为该对象生成新的敏感数据调查发现。与策略调查发现不同，所有敏感数据调查发现都被视为新的（唯一的）。Macie 会将敏感数据调查发现存储 90 天。

Macie 可以为 S3 对象生成以下类型的敏感数据调查发现。

SensitiveData:S3Object/Credentials

该对象包含敏感的凭证数据，例如私有访问 AWS 秘密访问密钥或私有密钥。

SensitiveData:S3Object/CustomIdentifier

该对象包含与一个或多个自定义数据标识符的检测标准相匹配的文本。该对象可能包含多种类型的敏感数据。

SensitiveData:S3Object/Financial

该对象包含敏感的财务信息，例如银行账号或信用卡号。

SensitiveData:S3Object/Multiple

该对象包含多个类别的敏感数据，即符合一个或多个自定义数据标识符检测标准的凭证数据、财务信息、个人信息或文本的任意组合。

SensitiveData:S3Object/Personal

该对象包含敏感的个人信息——个人身份信息（PII），例如护照号码或驾照识别号，个人健康信息(PHI)，例如健康保险或医疗识别号，或者个人身份信息和 PHI 的组合。

有关 Macie 可以使用内置标准和技术检测到的敏感数据的类型的信息，请参阅 使用托管数据标识符。有关 Macie 可以分析的 S3 对象类型的信息，请参阅 支持的存储类别和格式。

在 Amazon Macie 中处理样本调查发现

要探索和了解 Amazon Macie 可以生成的不同类型的调查发现，您可以创建样本调查发现。样本调查发现使用示例数据和占位符值来演示每种类型的调查发现可能包含的信息类型。

例如，Policy:IAMUser/S3BucketPublic 样本调查发现包含有关虚构的Amazon Simple Storage Service (Amazon S3) 存储桶的详细信息。调查发现的详细信息包括有关操作者的示例数据和操作，这些操作更改了存储桶的访问控制列表（ACL），并使存储桶可公开访问。同样，SensitiveData:S3Object/Multiple 样本调查发现包含有关虚构的微软 Excel 工作簿的详细信息。调查发现的详细信息包括有关工作簿中敏感数据的类型和位置的示例数据。

除了熟悉不同类型的发现结果可能包含的信息外，您还可以使用样本调查发现来测试与其他应用程序、服务和系统的集成。根据您账户的抑制规则，Macie 可以将样本调查发现作为事件发布到 Amazon EventBridge。通过使用样本调查发现中的示例数据，您可以开发和测试用于监控和处理这些事件的自动化解决方案。根据您账户的发布设置，Macie 还可以将样本调查发现发布到 AWS Security Hub。这意味着您还可以使用样本调查发现来开发和测试解决方案，以便在 Security Hub 中监控和处理 Macie 调查发现。有关将调查发现发布到这些服务的信息，请参阅监控和处理结果。

主题

生成样本调查发现

您可以使用 Amazon Macie 控制台或 Amazon Macie API 创建样本调查发现。如果您使用控制台，Macie 会自动为 Macie 支持的每种调查发现生成一个样本调查发现。如果您使用 API，则可以为每种类型创建样本，也可以仅为指定的某些类型创建样本。

Console

按照以下步骤使用 Amazon Macie 控制台创建样本调查发现。

创建样本调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Settings (设置)。

3. 在 Sample findings 下，选择 Generate sample findings。

API

要以编程方式创建样本调查发现，请使用 Amazon Macie API 的 CreateSampleFindings 操作。提交请求时，可以选择使用 `findingTypes` 参数仅指定要创建的某些类型的样本调查发现。要自动创建所有类型的样本，请不要在请求中包含此参数。

要使用 AWS Command Line Interface(AWS CLI) 创建样本调查发现，请运行 create-sample-findings 命令。要自动创建所有类型调查发现的样本，请不要包含 `finding-types` 参数。要仅创建某些类型调查发现的样本，请包含此参数并指定要创建的样本调查发现的类型。例如：

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

其中 *SensitiveData:S3Object/Multiple* 是一种要创建的敏感数据调查发现，而 *Policy:IAMUser/S3BucketPublic* 是一种要创建的策略调查发现。

如果该命令成功运行，Macie 将返回空响应。

查看样本调查发现

为了帮助您识别您创建的样本调查发现，Macie 将每个样本调查发现的样本字段的值设置为真。此外，所有样本调查发现的受影响的 S3 存储桶的名称都相同：macie-sample-finding-bucket。如果您使用 Amazon Macie 控制台上的调查发现页面查看样本调查发现，Macie 还会在每个样本调查发现的 调查发现类型字段中显示[样本]前缀。

Console

按照以下步骤使用 Amazon Macie 控制台查看样本调查发现。

查看样本调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。
3. 在 调查发现页面上，执行以下任何操作：

   - 在调查发现类型列中，找到类型以[样本]开头的调查发现，如下图所示。

Severity	Finding type	Resources affected
Low	[SAMPLE] Policy:IAMUser/S3BucketEncryptionDisabled	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/CustomIdentifier	macie-sample-finding-bucket/
Low	[SAMPLE] SensitiveData:S3Object/Personal	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketPublic	macie-sample-finding-bucket
Medium	[SAMPLE] Policy:IAMUser/S3BucketSharedWithCloudFront	macie-sample-finding-bucket
High	[SAMPLE] Policy:IAMUser/S3BucketSharedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Financial	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BucketReplicatedExternally	macie-sample-finding-bucket
High	[SAMPLE] SensitiveData:S3Object/Credentials	macie-sample-finding-bucket/
High	[SAMPLE] SensitiveData:S3Object/Multiple	macie-sample-finding-bucket/
High	[SAMPLE] Policy:IAMUser/S3BlockPublicAccessDisabled	macie-sample-finding-bucket

- 使用表格上方的 筛选标准框，筛选表格以仅显示样本调查发现。为此，请将光标放在框中。在出现的字段列表中，选择 样本。然后选择真，再选择应用。这将在表格中添加以下筛选条件：

4. 要查看特定样本调查发现的详细信息，请选择该调查发现。详细信息面板会显示调查发现的信息。

您也可以下载一个或多个样本调查发现的详细信息并将其保存为 JSON 文件。为此，选中要下载并保存的每个样本调查发现的复选框。然后在调查发现页面顶部的操作菜单上选择导出 (JSON)。在出现的窗口中，选择 下载。有关调查发现可能包含的 JSON 字段的详细描述，请参阅 Amazon Macie API 参考中的调查发现。

API

要以编程方式查看样本调查发现，请先使用 Amazon Macie API 的 ListFindings 操作来检索您创建的每个样本调查发现的唯一标识符 (`findingId`)。然后使用 GetFindings 操作来检索这些调查发现的详细信息。

提交 ListFindings 请求时，您可以指定筛选标准，以便在结果中仅包含样本调查发现。为此，请添加一个筛选条件，其中 `sample` 字段的值为 `true`。如果您使用的是 AWS CLI，请运行 list-findings 命令并使用 `finding-criteria` 参数指定筛选条件。例如：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":[\"true\"]}}}
```

如果请求成功，Macie 将返回一个 `findingIds` 数组。该数组列出了当前 AWS 区域 中您的账户的每个样本调查发现的唯一标识符。

要随后检索样本调查发现的详细信息，请在 GetFindings 请求中指定这些唯一标识符，或者在运行 get-findings 命令时为 AWS CLI 指定这些唯一标识符。

抑制样本调查发现

与其他调查发现一样，Macie 会将样本调查发现存储 90 天。完成样本的查看和实验后，您可以选择通过创建抑制规则将其存档。如果执行此操作，则默认情况下，样本调查发现将停止显示在控制台上，其状态将更改为已存档。

要使用 Amazon Macie 控制台存档样本调查发现，请将规则配置为存档样本字段值为真的调查发现。要使用 Amazon Macie API 存档样本调查发现，请配置规则以存档 `sample` 字段的值为 `true` 的调查发现。

在 Amazon Macie 控制台上查看调查发现

Amazon Macie 会监控您的 AWS 环境，并在检测到 Amazon Simple Storage Service (Amazon S3) 存储桶的潜在策略违规或安全或隐私问题时生成策略调查发现。当 Macie 在 S3 对象中检测到敏感数据时，会生成敏感数据调查发现。Macie 会将您的策略和敏感数据调查发现存储 90 天。

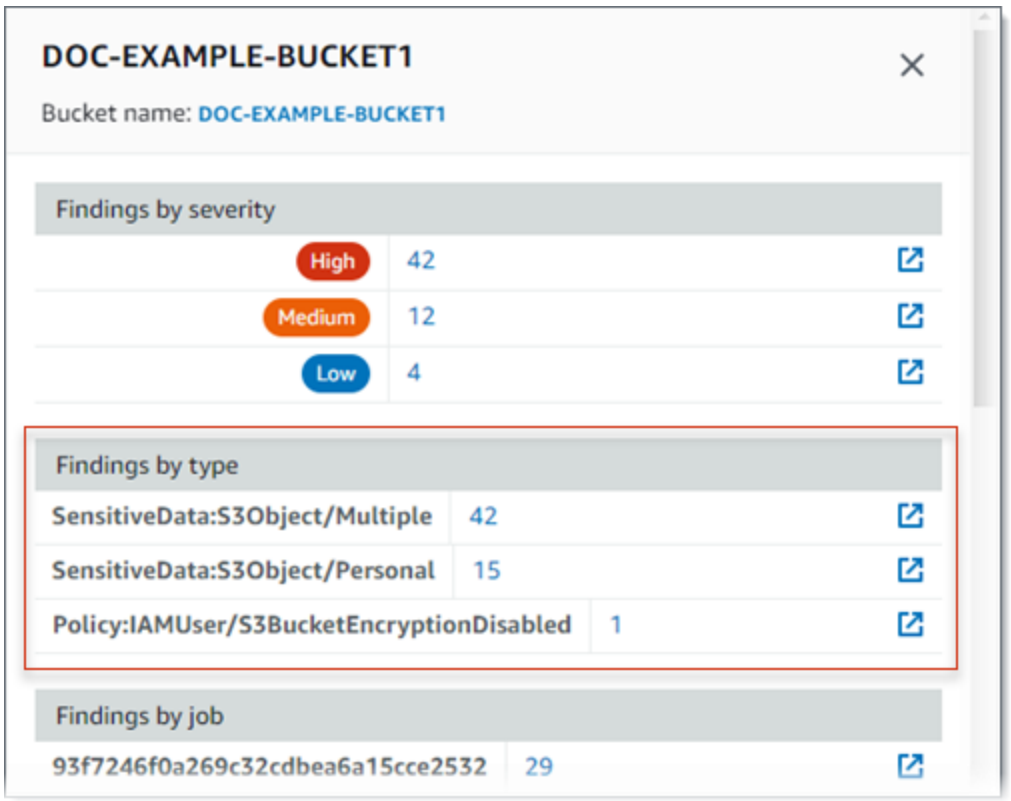
每项调查发现都指定了调查发现类型和严重性等级。其他详细信息包括受影响的资源信息，Macie 何时和如何发现问题，或调查发现报告的敏感数据信息。每个调查发现的严重性和细节因其类型和性质而异。

通过使用 Amazon Macie 控制台，您可以查看和分析调查发现，并访问个别调查发现的详细信息。您也可以将一项或多项调查发现导出到 JSON 文件。为了帮助您简化分析，控制台提供了多个用于构建自定义调查发现视图的选项。

使用预定义的分组

使用特定页面查看按条件分组的调查发现，例如受影响的 S3 存储桶、调查发现类型或敏感数据发现作业。通过这些页面，您可以查看每个组的汇总统计信息，例如按严重性划分的调查发现计数。您还可以深入查看组中各项调查发现的详细信息，并且可以应用筛选条件来完善您的分析。

例如，如果您按 S3 存储桶对所有调查发现进行分组，并注意到特定存储桶存在策略违规，则您可以快速确定该存储桶是否还存在敏感数据调查发现。为此，请在导航窗格（在调查发现下）中选择按存储桶，然后选择存储桶。在出现的详细信息面板中，按类型分类的调查发现部分列出了适用于存储桶的调查发现类型，如下图所示。

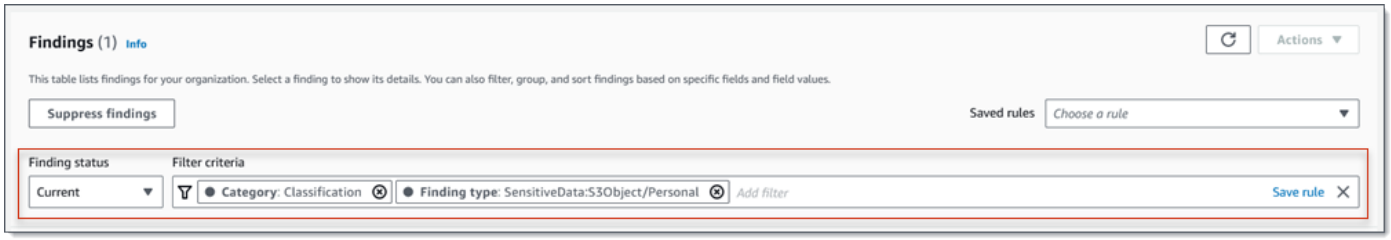


要调查特定类型，请选择该类型的编号。Macie 会显示一个表格，其中列出了与所选类型匹配并适用于存储桶的所有调查发现。要完善结果，请对表格进行筛选。

创建和应用筛选条件

使用特定的调查发现属性在调查发现表中包含或排除某些调查发现。调查发现属性是存储调查发现的特定数据字段，例如调查发现类型、严重性或受影响的 S3 存储桶的名称。如果筛选表格，则可以更轻松地识别出具有特定特征的调查发现。然后，您可以深入查看这些调查发现的细节。

例如，要查看所有敏感数据调查发现，请为 类别字段添加筛选条件。要优化结果并仅包括特定类型的敏感数据调查发现，请为调查发现类型字段添加筛选条件。例如：



然后，要查看特定调查发现的详细信息，请选择该调查发现。详细信息面板会显示调查发现的信息。

您也可以按照升序或降序，对调查发现进行排序。为此，请单击该字段的列标题。若要更改排序顺序，请再次点击列标题。

在控制台上查看调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Findings（调查发现）。调查发现页面显示 Macie 于过去 90 天内在当前的 AWS 区域 为您的账户创建或更新的调查发现。默认情况下，这不包括被抑制规则隐藏的调查发现。
3. 要按预定义的逻辑组透视和查看调查发现，请在导航窗格（在调查发现下）中选择按存储桶、按类型或按作业。然后在表格中选择一个项目。在详细信息面板中，为字段选择要转置的链接。
4. 要按特定标准筛选调查发现，请使用表格上方的筛选选项：

   - 要显示被抑制规则隐藏的搜索结果，请使用调查发现状态菜单。选择全部可同时显示隐藏和未隐藏的调查发现，或者选择已存档以仅显示隐藏的调查发现。然后要再次隐藏被抑制的调查发现，请选择当前。
   - 要仅显示那些具有特定属性的调查发现，请使用筛选标准框。将光标置于框中，然后为该属性添加筛选条件。要进一步优化结果，请为其他属性添加条件。要随后删除某个条件，请为要删除的条件选择删除条件图标（ ）。

   有关筛选调查发现的更多信息，请参阅 创建筛选条件并将其应用于调查发现。
5. 要按特定字段对调查发现进行排序，请单击该字段的列标题。若要更改排序顺序，请再次点击列标题。
6. 要查看特定调查发现的详细信息，请选择该调查发现。详细信息面板会显示调查发现的信息。

> **Tip**
>
> 您可以使用详细信息面板来查看特定字段的详情。要显示某个字段中具有相同值的调查发现，请选择该字段中的  。或者选择  ，以显示该字段具有其他值的调查发现。
>
> 对于敏感数据调查发现，您还可以使用详细信息面板来调查 Macie 在受影响的 S3 对象中发现的敏感数据：
>
> - 要查找特定类型的敏感数据的出现位置，请选择该类型数据字段中的数字链接。Macie 显示有关 Macie 在何处找到数据的信息（以 JSON 格式）。有关更多信息，请参阅 定位敏感数据。
> - 要检索 Macie 找到的敏感数据的示例，请在显示示例字段中选择查看。有关更多信息，请参阅 检索敏感数据样本。
> - 要导航到相应的敏感数据发现结果，请选择详细结果位置字段中的链接。Macie 打开 Amazon S3 控制台并显示包含发现结果的文件或文件夹。有关更多信息，请参阅 存储和保留敏感数据发现结果。

您也可以下载一个或多个调查发现的详细信息并将其保存为 JSON 文件。为此，请选中要下载并保存的每个调查发现对应的复选框。然后在 调查发现页面顶部的 操作菜单上选择 导出 (JSON)。在出现的窗口中，选择 下载。有关调查发现可能包含的 JSON 字段的详细描述，请参阅 Amazon Macie API 参考中的调查发现。

筛选 Amazon Macie 调查发现

为了执行有针对性的分析并更有效地分析结果，您可以筛选 Amazon Macie 调查发现。您可通过筛选条件，为调查发现构建自定义视图和查询，帮助您识别和关注有指定特点的调查发现。使用 Amazon Macie 控制台筛选调查发现，或者使用 Amazon Macie API 以编程方式提交查询。

创建筛选条件时，您可使用指定的调查发现属性，定义在视图或查询结果中包含或排除调查发现的标准。调查发现属性是一个存储调查发现的特定数据的字段，例如严重性、类型或调查发现所适用的 S3 存储桶的名称。

Macie 中的筛选条件包含一个或多个条件。每个条件，也称为标准，由三个部分组成：

- 基于属性的字段，例如严重性或调查发现类型。
- 一个运算符，例如等于或不等于。
- 一个或多个值。值的类型和数量取决于您选择的字段和运算符。

如果您创建了想再次使用的筛选条件，则可以将其另存为筛选规则。筛选规则是一组筛选标准，您可以创建并保存这些筛选标准，以便在您在 Amazon Macie 控制台上查看结果时重新应用。

您也可以将筛选条件另存为隐藏规则。抑制规则是您创建并保存的一组筛选条件，用于自动存档符合规则标准的调查发现。要了解有关抑制规则的信息，请参阅取消发现结果。

主题

筛选结果的基础知识

在创建筛选条件时，请记住以下功能和指南。另请注意，筛选结果仅限于前 90 天和当前 AWS 区域。Amazon Macie 在每个 AWS 区域 中将您的调查发现仅保存 90 天。

主题

在筛选条件中使用多个条件

筛选条件可能包含一个或多个条件。每个条件，也称为标准，由三个部分组成：

- 基于属性的字段，例如严重性或调查发现类型。有关可以使用的字段列表，请参阅 用于筛选调查发现的字段。
- 一个运算符，例如等于或不等于。有关可以使用的运算符列表，请参阅 在条件中使用运算符。

- 一个或多个值。值的类型和数量取决于您选择的字段和运算符。

如果一个筛选条件包含多个条件，Macie 会使用 AND 逻辑来连接条件并评测筛选标准。这意味着，只有当结果与筛选条件中的所有条件都匹配时，它才会匹配筛选条件。

例如，如果您添加一个条件以仅包含高严重性调查发现，而添加另一个条件以仅包含敏感数据调查发现，则 Macie 将返回所有高严重性的敏感数据调查发现。换句话说，Macie 会排除所有策略调查发现以及所有中等严重性和低严重性的敏感数据调查发现。

在筛选条件中只能使用一个字段一次。但是，您可以为多个字段指定多个值。

例如，如果某个条件使用严重性字段仅包含高严重性调查发现，则不能在其他条件中使用严重性字段来包含中等严重性或低严重性调查发现。相反，可以为现有条件指定多个值，或者对现有条件使用不同的运算符。例如，要包括所有中等严重性和高严重性结果，请添加严重性等于中、高条件或添加严重性不等于低条件。

为字段指定值

为字段指定值时，该值必须符合该字段的基础数据类型。根据字段的不同，您可以指定以下值类型之一。

文本数组（字符串）

为字段指定文本（字符串）值列表。每个字符串都与字段的预定义值或现有值相关联，例如，严重性字段为高，调查发现类型字段为 SensitiveData:S3Object/Financial 或 S3 存储桶名称字段为 S3 存储桶名称。

如果您使用数组，请注意以下几点：

- 值区分大小写。
- 您不能指定部分值或使用值中的通配符。您必须为字段指定一个完整的有效值。

例如，要筛选名为 my-s3-Bucket 的 S3 存储桶的调查发现，请在 S3 存储桶名称字段中输入 **`my-S3-bucket`** 作为值。如果您输入任何其他值，例如 **`my-s3-bucket`** 或 **`my-S3`**，Macie 将不会返回存储桶的调查发现。

有关每个字段的有效值的列表，请参阅 用于筛选调查发现的字段。

您最多可以在一个数组中指定 50 个值。如何指定这些值取决于您使用的是 Amazon Macie 控制台还是 Amazon Macie API，如 为字段指定多个值 中所述。

布尔值

为字段指定两个互斥值中的一个。

如果您使用 Amazon Macie 控制台来指定此类值，则控制台会提供一个值列表供您选择。如果您使用 Amazon Macie API，请为值指定 `true` 或 `false`。

日期/时间（及时间范围）

为字段指定绝对日期和时间。如果指定这种类型的值，则必须同时指定日期和时间。

在 Amazon Macie 控制台上，日期和时间值以您的当地时区为单位，并使用 24 小时表示法。在所有其他情况下，这些值均采用协调世界时 (UTC) 和扩展的 ISO 8601 格式，例如 `2020-09-01T14:31:13Z` 为世界标准时间 2020 年 9 月 1 日下午 2:31:13。

如果字段存储日期/时间值，则可以使用该字段来定义固定或相对时间范围。例如，您可以仅包括在两个特定日期和时间之间创建的调查发现，或者仅包含在特定日期和时间之前或之后创建的调查发现。如何定义时间范围取决于您是否使用 Amazon Macie 控制台或 Amazon Macie API:

- 在控制台上，使用日期选择器或直接在从和到框中输入文本。
- 在 API 上，通过添加一个用于指定该范围内的第一个日期和时间的条件来定义固定时间范围，然后添加另一个用于指定该范围内最后一个日期和时间的条件。如果这样做，Macie 会使用 AND 逻辑来加入条件。要定义相对时间范围，请添加一个条件来指定该范围内的第一个或最后一个日期和时间。将这些值指定为以毫秒为单位的 Unix 时间戳，例如，`1604616572653` 为世界标准时间 2020 年 11 月 5 日 22:49:32。

在控制台上，时间范围包含在内。在 API 上，时间范围可以是包容性的，也可以是排他性的，具体取决于您选择的运算符。

数字（和数值范围）

为字段指定长整数。

如果字段存储数值，则可以使用该字段定义固定或相对数值范围。例如，您只能包含那些在 S3 对象中报告 50-90 次出现的敏感数据的发现。如何定义数值范围取决于您是否使用 Amazon Macie 控制台或 Amazon Macie API:

- 在控制台上，使用从和到框分别输入该范围内的最小和最高数字。
- 使用API，通过添加一个指定范围内最低数字的条件来定义一个固定的数字范围，并添加另一个指定范围内最高数字的条件。如果这样做，Macie 会使用 AND 逻辑来加入条件。要定义相对数值范围，请添加一个条件来指定该范围内的最小或最高数字。

在控制台上，数值范围包含在内。使用 API，数值范围可以是包容性的，也可以是排他性的，具体取决于您选择的运算符。

文本（字符串）

为字段指定单个文本（字符串）值。该字符串与字段的预定义值或现有值相关联，例如严重性字段为高，S3 存储桶名称字段为 S3 存储桶的名称，或作业 ID字段为敏感数据发现作业的唯一标识符。

如果您指定一个文本字符串，请注意以下几点：

- 值区分大小写。
- 您不能使用部分值或使用值中的通配符。您必须为字段指定一个完整的有效值。

例如，要筛选名为 my-s3-Bucket 的 S3 存储桶的调查发现，请在 S3 存储桶名称字段中输入 **my-S3-bucket** 作为值。如果您输入任何其他值，例如 **my-s3-bucket** 或 **my-S3**，Macie 将不会返回存储桶的调查发现。

有关每个字段的有效值的列表，请参阅 用于筛选调查发现的字段。

为字段指定多个值

使用某些字段和运算符，您可以为一个字段指定多个值。如果您这样做，Macie 会使用 OR 逻辑来连接值并评测筛选条件。这意味着，如果某项查找结果具有为该字段指定的任何值，则该结果与该条件相匹配。

例如，如果您添加一个条件以包括调查发现类型字段的值等于 SensitiveData:S3Object/Financial, SensitiveData:S3Object/Personal 的结果，则 Macie 会返回仅包含财务信息的 S3 对象和仅包含个人信息的 S3 对象的敏感数据调查发现。换句话说，Macie 排除了所有策略调查发现。对于包含其他类型的敏感数据或多种类型的敏感数据的对象，Macie 还会排除所有敏感数据发现。

使用 eqExactMatch 运算符的条件除外。对于这个运算符，Macie 使用 AND 逻辑连接值并评测筛选条件。这意味着，只有当查找结果包含该字段的所有值并且仅包含该字段的那些值时，它才符合标准。要详细了解此运算符，请参阅 在条件中使用运算符。

如何为一个字段指定多个值取决于您是使用 Amazon Macie API 还是 Amazon Macie 控制台。使用 API，您可以使用列出值的数组。

在控制台上，您通常会从列表中选择值。但是，对于某些字段，您必须为每个值添加不同的条件。例如，要包括 Macie 使用某些自定义数据标识符检测到的数据的调查发现，请执行以下操作：

1. 将光标置于筛选标准框中，然后选择自定义数据标识符名称字段。输入自定义数据标识符的名称，然后选择应用。
2. 对要为筛选条件指定的每个其他自定义数据标识符重复上述步骤。

有关需要执行此操作的字段列表，请参阅 用于筛选调查发现的字段。

在条件中使用运算符

您可以在各个条件中使用以下类型的运算符。

等于号 (eq)

匹配 (=) 为该字段指定的任何值。可以对以下类型的值使用等号运算符：文本数组（字符串）、布尔值、日期/时间、数字和文本（字符串）。

对于许多字段，您可以使用此运算符为该字段指定多达 50 个值。如果这样做，Macie 将使用 OR 逻辑连接这些值。这意味着，如果某项查找结果具有为该字段指定的任何值，则该结果与该条件相匹配。

例如：

- 要包含报告财务信息、个人信息或财务和个人信息出现情况的结果，请添加使用敏感数据类别字段和此操作符的条件，并将财务信息和个人信息指定为该字段的值。
- 要包括报告信用卡号、邮寄地址或同时出现信用卡号和邮寄地址的调查发现，请为敏感数据检测类型字段添加条件，使用此运算符，然后指定 CREDIT_CARD_NUMBER 和 ADDRESS 作为该字段的值。

如果您使用 Amazon Macie API 定义使用此运算符和日期/时间值的条件，请将该值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

等于完全匹配 (eqExactMatch)

只匹配为该字段指定的所有值。您可以将等于完全匹配运算符与一组选定的字段一起使用。

如果您使用此运算符并为一个字段指定多个值，Macie 会使用 AND 逻辑来连接这些值。这意味着，只有当查找结果包含为该字段指定的所有值并且仅包含该字段的那些值时，它才符合条件。您最多可以指定 50 个值。

例如：

- 要包括报告信用卡号出现次数而不报告其他类型敏感数据的结果，请为敏感数据检测类型字段添加条件，使用此运算符，然后指定 CREDIT_CARD_NUMBER 为该字段的唯一值。

- 要包含报告出现信用卡号和邮寄地址(不包含其他类型的敏感数据)的结果，请为敏感数据检测类型字段添加一个条件，使用此操作符，并指定 CREDIT_CARD_NUMBER 和 ADDRESS 作为该字段的值。

由于 Macie 使用 AND 逻辑来连接字段的值，因此对于同一字段，您不能将此运算符与任何其他运算符组合使用。换句话说，如果您在一个条件中对字段使用等于完全匹配运算符，则必须在使用相同字段的所有其他条件中使用该运算符。

与其他运算符一样，可以在筛选条件中的多个条件使用等于完全匹配运算符。如果这样做，Macie 会使用 AND 逻辑来加入条件并评测筛选条件。这意味着查找结果只有在具有筛选条件中所有条件指定的所有值时才符合筛选条件。

例如，要包括在一定时间后创建的调查发现，报告信用卡号的出现次数，并且不报告任何其他类型的敏感数据，请执行以下操作：

1. 添加一个条件，该条件使用创建时间字段，使用大于运算符，并指定筛选条件的开始日期和时间。
2. 添加另一个条件，该条件使用敏感数据检测类型字段，使用等于完全匹配运算符，并指定 CREDIT_CARD_NUMBER 为该字段的唯一值。

您可以对以下字段使用等于完全匹配运算符:

- 自定义数据标识符 ID (`customDataIdentifiers.detections.arn`)
- 自定义数据标识符名称 (`customDataIdentifiers.detections.name`)
- S3 存储桶标签键 (`resourcesAffected.s3Bucket.tags.key`)
- S3 存储桶标签值 (`resourcesAffected.s3Bucket.tags.value`)
- S3 对象标签键 (`resourcesAffected.s3Object.tags.key`)
- S3 对象标签值 (`resourcesAffected.s3Object.tags.value`)
- 敏感数据检测类型 (`sensitiveData.detections.type`)
- 敏感数据类别 (`sensitiveData.category`)

在前面的列表中，括号中的名称使用点符号来表示搜索结果和 Amazon Macie API 的 JSON 表示形式中的字段名称。

大于 (gt)

大于 (>) 为该字段指定的值。您可以将大于运算符与数字和日期/时间值一起使用。

例如，要仅包括那些在 S3 对象中报告敏感数据出现次数超过 90 次的结果，请添加一个使用敏感数据总计数字段和此运算符的条件，并指定 90 作为该字段的值。要在 Amazon Macie 控制台上执行

此操作，请在从框中输入 **91**，不要在到框中输入值，然后选择应用。控制台上包含数字和基于时间的比较。

如果您使用 Amazon Macie API 定义使用此运算符的时间范围，则必须将日期/时间值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

大于或等于 (gte)

大于或等于 (>=) 为该字段指定的值。您可以将大于或等于运算符与数字和日期/时间值一起使用。

例如，要仅包含那些报告 S3 对象中敏感数据出现 90 次或以上的结果，可以添加一个条件，使用敏感数据总计数字段和此操作符，并指定 90 作为该字段的值。要在 Amazon Macie 控制台上执行此操作，请在从框中输入 **90**，不要在到框中输入值，然后选择应用。

如果您使用 Amazon Macie API 定义使用此运算符的时间范围，则必须将日期/时间值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

小于 (lt)

小于 (<) 为该字段指定的值。您可以将小于运算符与数字和日期/时间值一起使用。

例如，要只包含那些报告 S3 对象中敏感数据出现次数少于 90 次的结果，可以添加一个条件，使用敏感数据总计数字段和此操作符，并指定 90 作为该字段的值。要在 Amazon Macie 控制台上执行此操作，请在到框中输入 **89**，不要在从框中输入值，然后选择应用。控制台上包含数字和基于时间的比较。

如果您使用 Amazon Macie API 定义使用此运算符的时间范围，则必须将日期/时间值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

小于或等于 (lte)

小于或等于 (<=) 为该字段指定的值。您可以将小于或等于运算符与数字和日期/时间值一起使用。

例如，要仅包括那些在 S3 对象中报告敏感数据出现次数少于或等于 90 次的结果，请添加一个使用敏感数据总计数字段和此运算符的条件，并指定 90 作为该字段的值。要在 Amazon Macie 控制台上执行此操作，请在到框中输入 **90**，不要在从框中输入值，然后选择应用。

如果您使用 Amazon Macie API 定义使用此运算符的时间范围，则必须将日期/时间值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

不等于 (neq)

不匹配 (≠) 为该字段指定的任何值。可以对以下类型的值使用不等于运算符：文本数组（字符串）、布尔值、日期/时间、数字和文本（字符串）。

对于许多字段，您可以使用此运算符为该字段指定多达 50 个值。如果这样做，Macie 将使用 OR 逻辑连接这些值。这意味着，如果某项查找结果没有该字段的任何值，则该结果与该条件相匹配。

例如：

- 要排除报告财务信息、个人信息或财务和个人信息出现情况的调查发现，请添加一个使用敏感数据类别字段和此运算符的条件，并将财务信息和个人信息指定为该字段的值。
- 要排除报告出现信用卡号的结果，请为敏感数据检测类型字段添加一个条件，使用此运算符，并指定 CREDIT_CARD_NUMBER 为该字段的值。
- 要排除报告信用卡号、邮寄地址或同时出现信用卡号和邮寄地址的调查发现，请为敏感数据检测类型字段添加条件，使用此运算符，然后指定CREDIT_CARD_NUMBER和ADDRESS作为该字段的值。

如果您使用 Amazon Macie API 定义使用此运算符和日期/时间值的条件，请将该值指定为以毫秒为单位的 Unix 时间戳，例如，1604616572653 为世界标准时间 2020 年 11 月 5 日 22:49:32。

创建筛选条件并将其应用于调查发现

要识别并重点关注具有特定特征的调查发现，您可以在 Amazon Macie 控制台和使用 Amazon Macie API 以编程方式提交的查询中筛选调查发现。创建筛选条件时，您可使用指定的调查发现属性，定义在视图或查询结果中包含或排除调查发现的标准。调查发现属性是一个存储调查发现的特定数据的字段，例如严重性、类型或调查发现所适用的 S3 存储桶的名称。

Macie 中的筛选条件包含一个或多个条件。每个条件，也称为标准，由三个部分组成：

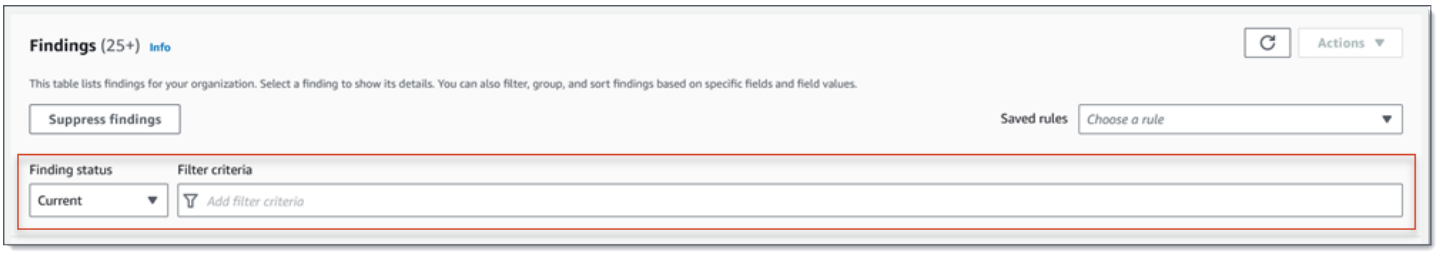
- 基于属性的字段，例如严重性或调查发现类型。
- 一个运算符，例如等于或不等于。
- 一个或多个值。值的类型和数量取决于您选择的字段和运算符。

如何定义和应用筛选条件取决于您使用的是 Amazon Macie 主机还是 Amazon Macie API。

主题

筛选 Amazon Macie 主机上的调查发现

如果您使用 Amazon Macie 控制台筛选调查发现，Macie 会提供一些选项来帮助您为各个条件选择字段、运算符和值。您可以使用 调查发现页面上的筛选条件设置访问这些选项，如下图中所示。



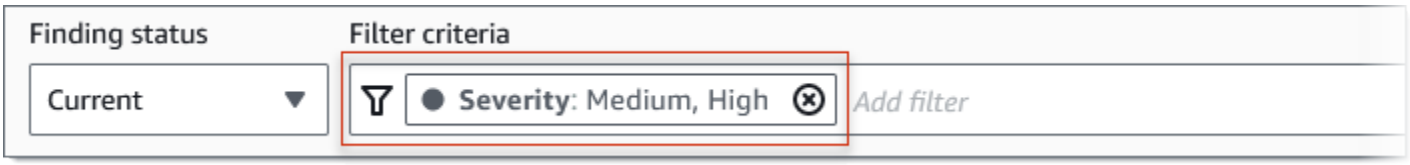
通过使用调查发现状态菜单，您可以指定是否包括被屏蔽规则屏蔽（自动存档）的调查发现。通过使用筛选标准框，您可以输入筛选条件。

当您将光标置于筛选标准框中时，Macie 会显示可在筛选条件中使用的字段列表。这些字段按逻辑类别组织。例如，常用字段类别包括适用于任何类型的调查发现的字段，而分类字段类别包括仅适用于敏感数据调查发现的字段。这些字段在每个类别中按字母顺序排序。

要添加条件，请先从列表中选择一个字段。要查找字段，请浏览完整列表，或输入部分字段名称以缩小字段列表范围。

根据您选择的字段，Macie 显示不同的选项。这些选项反映了您选择的字段的类型和性质。例如，如果您选择严重性字段，Macie 会显示一个值列表供您选择：低、中和高。如果您选择 S3 存储桶名称字段，Macie 会显示一个文本框，您可以在其中输入存储桶名称。无论您选择哪个字段，Macie 都会指导您完成添加包含该字段所需设置的条件的步骤。

添加条件后，Macie 会应用该条件的标准并将该条件添加到筛选标准框中的筛选条件令牌，如下图所示。



在此示例中，条件配置为包括所有中严重性和高严重性调查发现，并排除所有低严重性调查发现。它会返回严重性字段的值等于中或高的调查发现。

> **Tip**
>
> 对于许多字段，您可以通过在条件的筛选条件令牌中选择等号图标
> (●)

来将条件的运算符从等于更改为不等于。如果您这样做，Macie 会将运算符更改为不等于，并在令牌中显示不等于图标
()。
要再次切换到等于运算符，请选择不等于图标。

当您添加更多条件时，Macie 会应用其标准并将其添加到筛选标准框中的令牌中。您可以随时参考方框来确定您应用了哪些标准。要删除条件，请在条件的令牌中选择移除条件图标
()。

要使用控制台筛选结果

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Findings (结果)。
3. （可选）要首先根据预定义的逻辑组进行透视和查看调查发现，请在导航窗格（在调查发现下）中选择按存储桶、按类型或按作业。然后在表格中选择一个项目。在详细信息面板中，为字段选择要转置的链接。
4. （可选）要显示被屏蔽规则屏蔽的调查发现，请更改筛选状态设置。选择已存档 以仅显示屏蔽的调查发现，或选择全部以同时显示屏蔽和未屏蔽的调查发现。要隐藏屏蔽的调查发现，请选择当前。
5. 要添加筛选条件，请执行以下操作：

   a. 将光标置于筛选标准框中，然后选择要用于条件的字段。有关您可以使用的字段的信息，请参阅 用于筛选调查发现的字段。

   b. 输入字段的相应类型的值。有关不同类型值的详细信息，请参阅 为字段指定值。

      文本数组（字符串）

      对于这种类型的值，Macie 通常会提供一个值列表供您选择。如果是这种情况，请选择要在条件中使用的每个值。

      如果 Macie 未提供值列表，请为该字段输入一个完整、有效的值。要为该字段指定其他值，请选择应用，然后为每个附加值添加另一个条件。

      注意，值区分大小写。此外，不能在值中使用部分值或通配符。例如，要筛选名为 my-S3-Bucket 的 S3 存储桶的调查发现，请在 S3 存储桶名称字段中输入 **`my-S3-bucket`** 作为

值。如果您输入任何其他值，例如 **my-s3-bucket** 或 **my-S3**，Macie 将不会返回存储桶的调查发现。

Boolean

对于这种类型的值，Macie 提供了一个值列表供您选择。选择要在条件中使用的值。

日期/时间（时间范围）

对于这种类型的值，使用从和到框定义一个包含性时间范围：

- 要定义固定的时间范围，请使用从和到框分别指定该范围内的第一个日期和时间以及最后一个日期和时间。
- 要定义从特定日期和时间开始并在当前时间结束的相对时间范围，请在从框中输入开始日期和时间，然后删除到框中的任何文本。
- 要定义在特定日期和时间结束的相对时间范围，请在到框中输入结束日期和时间，然后删除从框中的任何文本。

请注意，时间值使用 24 小时表示法。如果您使用日期选择器选择日期，则可以通过直接在从和到框中输入文本来细化值。

数字（数值范围）

对于这种类型的值，使用从和到框输入一个或多个整数，这些整数定义了包含、固定或相对数值范围。

文本（字符串）值

对于此类值，请为该字段输入一个完整、有效的值。

注意，值区分大小写。此外，不能在值中使用部分值或通配符。例如，要筛选名为 my-s3-Bucket 的 S3 存储桶的调查发现，请在 S3 存储桶名称字段中输入 **my-S3-bucket** 作为值。如果您输入任何其他值，例如 **my-s3-bucket** 或 **my-S3**，Macie 将不会返回存储桶的调查发现。

c. 为该字段添加完值后，选择应用。Macie 应用筛选标准并将该条件添加到筛选标准框中的筛选条件令牌中。

6. 对于要添加的每个附加条件，请重复步骤 5。
7. 要删除条件，请在条件的筛选条件令牌中选择移除条件图标 (⊗)。

8. 要更改条件，请在条件的筛选条件令牌中选择移除条件图标 () 来移除该条件。然后重复步骤 5，添加设置正确的条件。

如果您想随后再次使用这组条件，可以将该条件集另存为筛选规则。为此，请在筛选标准框中选择保存规则。输入规则的名称和描述（可选）。完成后，选择保存。

使用 Amazon Macie API 以编程方式筛选调查发现

要以编程方式筛选调查发现，请在使用 Amazon Macie API 的 ListFindings 或 GetFindingStatistics 操作提交的查询中指定筛选标准。该 ListFindings 操作返回一个由调查发现 ID 组成的数组，每个符合筛选条件的调查发现对应一个 ID。GetFindingStatistics 操作会返回与筛选条件匹配的所有调查发现的汇总统计数据，这些数据按您在请求中指定的字段分组。

请注意，ListFindings 和 GetFindingStatistics 操作与用于屏蔽调查发现的操作不同。与还指定筛选标准的屏蔽操作不同，ListFindings 和 GetFindingStatistics 操作仅查询调查发现数据。它们不会对符合筛选条件的调查发现执行任何操作。要屏蔽调查发现，请使用 Amazon Macie API 的 CreateFindingsFilter 操作。

要在查询中指定筛选标准，请在请求中加入筛选条件地图。为每个条件指定一个字段、一个运算符以及该字段的一个或多个值。值的类型和数量取决于您选择的字段和运算符。有关可在条件中使用的字段、运算符和值类型的信息，请参阅用于筛选调查发现的字段、在条件中使用运算符和为字段指定值。

以下示例向您展示了如何在使用 AWS Command Line Interface(AWS CLI) 提交的查询中指定筛选标准。您也可以使用其他 AWS 命令行工具或 AWS SDK 的当前版本，或者直接向 Macie 发送 HTTPS 请求来执行此操作。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

示例

- 示例 1：基于严重性筛选调查发现
- 示例 2：基于敏感数据类别筛选调查发现
- 示例 3：根据固定时间范围筛选调查发现
- 示例 4：根据屏蔽状态筛选调查发现
- 示例 5：根据多个字段和值类型筛选调查发现

这些示例使用 list-findings 命令。如果示例成功运行，Macie 将返回一个 `findingIds` 数组。该数组列出了符合筛选标准的每个调查发现的唯一标识符，如以下示例所示。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

如果没有符合筛选条件的调查发现，Macie 将返回空`findingIds`数组。

```
{
    "findingIds": []
}
```

示例 1：基于严重性筛选调查发现

此示例使用 list-findings 命令检索当前 AWS 区域 中所有高严重性和中严重性调查发现的调查发现 ID。

对于 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

对于 Microsoft Windows：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

其中：

- *severity.description* 指定严重性字段的 JSON 名称。
- *eq* 指定等于运算符。
- *#*和*#*是严重性字段的枚举值数组。

示例 2：基于敏感数据类别筛选调查发现

此示例使用 list-findings 命令检索当前区域中所有敏感数据调查发现的调查发现 ID，并报告 S3 对象中出现的财务信息（没有其他类别的敏感数据）。

对于 Linux、macOS 或 Unix，使用反斜杠 (\) 行继续符来提高可读性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

对于 Microsoft Windows，使用脱字符 (^) 行继续符来提高可读性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

其中：

- *classificationDetails.result.sensitiveData.category* 指定敏感数据类别字段的 JSON 名称。
- *eqExactMatch* 指定等于精确匹配运算符。
- *FINANCIAL_INFORMATION* 是敏感数据类别字段的枚举值。

示例 3：根据固定时间范围筛选调查发现

此示例使用 list-findings 命令检索当前区域中所有调查发现的调查发现 ID，这些调查发现是在 2020 年 10 月 5 日 07:00 UTC 到 2020 年 11 月 5 日 07:00 UTC（包括这两个时间点）之间创建的。

对于 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

对于 Microsoft Windows：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

其中：

- *createdAt* 指定创建时间字段的 JSON 名称。
- *gte* 指定大于或等于运算符。

- *1601881200000* 是时间范围内的第一个日期和时间（作为以毫秒为单位的 Unix 时间戳）。
- *lte* 指定小于或等于运算符。
- *1604559600000* 是时间范围内的最后一个日期和时间（作为以毫秒为单位的 Unix 时间戳）。

示例 4：根据屏蔽状态筛选调查发现

此示例使用 list-findings 命令检索位于当前区域并被屏蔽规则屏蔽（自动存档）的所有调查发现的调查发现 ID。

对于 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

对于 Microsoft Windows：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

其中：

- *###*指定已存档字段的 JSON 名称。
- *eq* 指定等于运算符。
- *true* 是已存档字段的布尔值。

示例 5：根据多个字段和值类型筛选调查发现

此示例使用 list-findings 命令检索位于当前区域且符合以下标准的所有敏感数据调查发现的调查发现 ID：创建于 2020 年 10 月 5 日 07:00 UTC 至 2020 年 11 月 5 日 07:00 UTC 之间（不包括这两个时间点）；报告 S3 对象中出现的财务数据但没有其他类别的敏感数据；未被屏蔽规则屏蔽（自动存档）。

对于 Linux、macOS 或 Unix，使用反斜杠 (\) 行继续符来提高可读性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

对于 Microsoft Windows，使用脱字符 (^) 行继续符来提高可读性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

其中：

- *createdAt* 指定创建时间字段的 JSON 名称，并且：
  - *gt* 指定大于或等于运算符。
  - *1601881200000* 是时间范围内的第一个日期和时间（作为以毫秒为单位的 Unix 时间戳）。
  - *#*指定小于或等于运算符。
  - *1604559600000* 是时间范围内的最后一个日期和时间（作为以毫秒为单位的 Unix 时间戳）。
- *classificationDetails.result.sensitiveData.category* 指定敏感数据类别字段的 JSON 名称，并且：
  - *eqExactMatch* 指定等于精确匹配运算符。
  - *FINANCIAL_INFORMATION* 是该字段的枚举值。
- *archived*指定已存档字段的 JSON 名称，并且：
  - *eq* 指定等于运算符。
  - *false* 是该字段的布尔值。

创建和管理调查发现筛选规则

筛选规则 是您创建并保存的一组筛选条件，用于在 Amazon Macie 控制台上查看调查发现时再次使用。筛选规则可以帮助您对具有特定特征的调查发现执行一致分析。例如，您可创建一条筛选规则，以用于分析包含未解密对象的 S3 存储桶的所有高严重性策略调查发现；创建另一条规则，用于分析可报告指定类型敏感数据的、高严重性敏感数据调查发现。

请注意，筛选规则与隐藏规则不同。抑制规则是您创建并保存的一组筛选条件，用于自动存档符合规则标准的调查发现。尽管这两种类型的规则都存储和应用筛选条件，但筛选规则不会对符合规则条件的调查发现执行任何操作。相反，筛选规则只会决定应用规则后再控制台上显示的调查发现。有关接收规则的更多信息，请参阅取消发现结果。

要创建和管理筛选规则，您可使用 Amazon Macie 控制台或Amazon Macie API。以下主题说明如何使用。对于 API，主题包括如何使用 AWS Command Line Interface(AWS CLI) 执行这些任务的示例。您也可以使用当前版本的其他 AWS 命令行工具或 AWS SDK，或者直接向 Macie 发送 HTTPS 请求。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

主题

创建筛选规则

创建筛选规则时，需要指定筛选条件、名称以及规则描述（可选）。您可以使用 Amazon Macie 控制台或 Amazon Macie API 创建筛选规则。

Console

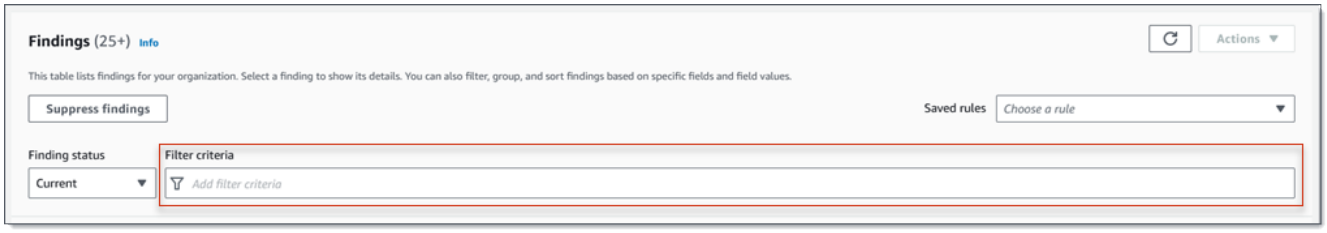
按照以下步骤，使用 Amazon Macie 控制台创建筛选规则。

创建筛选规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Findings (结果)。

> **Tip**
>
> 若要先使用现有筛选规则，请从已保存规则列表中选择此规则。
> 您还可以通过首先透视和深入研究预定义逻辑组的调查发现来简化规则的创建。如果您这样做，Macie 会自动创建并应用适当的筛选条件，这可能是创建规则的有用起点。据此，请在导航窗格选择按存储桶、按类型或 按作业（调查发现下），然后选择表内的项目。在详细信息面板中，为字段选择要转置的链接。

3. 在筛选标准框，添加定义规则筛选条件的条件。



要了解如何添加筛选条件，请参阅 创建筛选条件并将其应用于调查发现。

4. 定义完规则筛选条件后，在筛选标准框内选择保存规则。

5. 在 筛选规则下，输入规则的名称和描述（可选）。
6. 选择 Save（保存）。

API

要以编程方式创建筛选规则，请使用 Amazon Macie API 的 CreateFindingsFilter 操作，并为所需参数指定相应值：

- 对于 `action` 参数，指定 NOOP 以确保 Macie 不会隐藏（自动存档）符合规则标准的结果。
- 对于 `criterion` 参数，请指定定义规则筛选条件的条件映射。

  在映射中，每项条件都应为该字段指定一个字段、一个运算符以及一个或多个值。值的类型和数量取决于您选择的字段和运算符。有关可在条件中使用的字段、运算符和值类型的信息，请参阅用于筛选调查发现的字段、在条件中使用运算符和为字段指定值。

要使用 AWS CLI 创建规则，请运行 create-findings-filter命令，并为所需参数指定相应的值。以下示例创建了一个筛选规则，该规则可返回当前AWS 区域中的所有敏感数据，并报告 S3 对象中出现的个人信息（不包括其他类别的敏感数据）。

此示例针对 Linux、macOS 或 Unix 进行格式化，并使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
```

```
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

其中：

- *my_filter_rule*是自定义规则名称。
- criterion 是该规则的筛选条件映射：
  - *####.result.sensitiveData.Category ####### ### JSON ###*
  - *eqExactMatch* 指定 等于精确匹配 运算符。
  - *PERSONAL_INFORMATION* 是 敏感数据类别字段的枚举值。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

arn 是所创建筛选规则的 Amazon 资源名称（ARN），id是此规则的唯一标识符。

有关筛选标准的其他示例，请参阅 使用 Amazon Macie API 以编程方式筛选调查发现。

应用筛选规则

当您应用筛选规则时，Amazon Macie 会使用规则条件确定纳入工作台调查发现视图或从中移除的调查发现。Macie 还会显示条件，帮助您确定您的应用条件。

请注意，筛选规则专为与 Amazon Macie 控制台配合使用而设计。您不能在以编程方式提交的查询（通过 Amazon Macie API）中直接使用它们。但是，如果您使用 API 查询结果，则可以使用GetFindingsFilter操作检索规则筛选条件。然后，您可以将条件添加至查询。有关在查询中指定筛选条件的信息，请参见 创建筛选条件并将其应用于调查发现。

按以下步骤，通过应用筛选规则在控制台上筛选调查发现。

要应用筛选规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。

2. 在导航窗格中，选择 发现结果。
3. 在已保存规则列表中，选择要应用的规则。Macie 应用规则条件并在筛选标准 框内显示此条件。
4. （可选）若要细化条件，请使用筛选标准框添加或移除筛选条件。如果您这样操作，则您的更改不会影响规则设置。若非您明确将其另存为新规则，否则 Macie 不会保存您的任何更改。
5. 若要应用不同的筛选规则，请重复第 3 步。

应用筛选规则后，您可以通过在筛选标准框内选择X，以从您的视图中快速移除所有筛选条件。

更改筛选规则

您可以随时使用 Amazon Macie 控制台或 Amazon Macie API 更改筛选规则设置。您还可以为规则分配和管理标签。

标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

Console

按照以下步骤，使用 Amazon Macie 控制台更改现有筛选规则设置。

要更改筛选规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 发现结果。
3. 在已保存规则列表中，在要更改的筛选规则旁边选择编辑图标 ( )。
4. 执行以下任一操作：
   - 若要更改规则筛选条件，请使用筛选标准框输入所需条件。要了解如何操作，请参阅创建筛选条件并将其应用于调查发现。
   - 若要更改规则的名称，请在 筛选规则 下的 名称 框内输入新名称。
   - 要更改规则的描述，请在 筛选规则 下的 描述 框内输入新的描述。
   - 若要分配、查看或编辑规则标签，请在 筛选规则 下选择管理标签。然后根据需要查看并更改标签。一个规则可具有最多 50 个标签。
5. 完成更改后，选择 Save (保存)。

API

要以编程方式更改筛选规则，请使用 Amazon Macie API 的 updateFindingsFilter 操作。提交请求时，请使用支持的参数为要更改的每个设置指定一个新值。

对于 id 参数，请为待更改规则指定唯一标识符。您可以使用 ListFindingsFilter 操作获取此标识符，以检索账户的筛选和隐藏规则列表。如果您使用的是 AWS CLI，请运行 list-findings-filters 命令来检索此列表。

要使用AWS CLI更改筛选规则，请运行 update-findings-filter 命令并使用支持的参数指定待更改设置的新值。例如，以下命令可更改现有筛选规则的名称。

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

其中：

- *9b2b4508-aa2f-4940-b347-d1451example* 是该规则的唯一标识符。
- *personal_information_only*是该规则的新名称。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

其中 arn 是已更改规则的 Amazon 资源名称（ARN），id 是该规则的唯一标识符。

同样，以下示例通过将 action 参数值从 ARCHIVE 更改为NOOP，以将隐藏规则转换为筛选规则。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

其中：

- *8a1c3508-aa2f-4940-b347-d1451example* 是该规则的唯一标识符。
- *NOOP* 是 Macie 对符合规则条件的调查发现执行的新操作——不执行任何操作（不要隐藏调查发现）。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

其中 `arn` 是已更改规则的 Amazon 资源名称（ARN），`id` 是该规则的唯一标识符。

删除筛选规则

您可以随时使用 Amazon Macie 控制台或 Amazon Macie API 删除筛选规则。

Console

按照以下步骤，使用 Amazon Macie 控制台删除筛选规则。

要删除筛选规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Findings (结果)。
3. 在已保存规则列表中，在要删除的筛选规则旁边选择编辑图标 ()。
4. 在 筛选规则下，选择 删除。

API

要以编程方式删除规则，请使用 Amazon Macie API 中的 DeleteFindingsFilter 操作。对于 `id` 参数，请为待删除规则指定唯一标识符。您可以使用 ListFindingsFilter 操作获取此标识符，以检索账户的筛选和隐藏规则列表。如果您使用的是 AWS CLI，请运行 list-findings-filters 命令来检索此列表。

要使用AWS CLI删除筛选规则，请运行 delete-findings-filter 命令。例如：

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

9b2b4508-aa2f-4940-b347-d1451example 是待删除规则的唯一标识符。

如果命令运行成功，Macie 将返回一个空 HTTP 200 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

用于筛选调查发现的字段

为了帮助您更有效地分析调查发现，Amazon Macie 控制台和 Amazon Macie API 提供了对多组字段的访问权限，用于筛选调查发现：

- 常用字段 – 这些字段存储适用于任何类型的调查发现的数据。它们与调查发现的常见属性相关，例如严重性、调查发现类型和调查发现 ID。
- 受影响的资源字段-这些字段存储与调查发现适用的资源相关的数据，例如受影响的 S3 存储桶或对象的名称、标签和加密设置。
- 策略字段 – 这些字段存储特定于策略调查发现的数据，例如产生调查发现的操作以及执行操作的实体。
- 敏感数据分类字段 – 这些字段存储特定于敏感数据调查发现的数据，例如 Macie 在受影响的 S3 对象中发现的敏感数据的类别和类型。

筛选条件可以使用前面任意组中的字段组合。

本节中的主题列出并描述了您可用于筛选调查发现的各个字段。有关这些字段的更多详情，包括字段之间的任何关系，请参阅 Amazon Macie API 参考中的调查发现。

主题

公用字段

下表列出并描述了可用于根据常见调查发现属性筛选结果的字段。这些字段存储适用于任何类型的调查发现的数据。

在表中，字段列指明了 Amazon Macie 控制台上该字段的名称。JSON 字段列使用点符号在调查发现和 Amazon Macie API 的 JSON 表示形式中表示字段的名称。描述列简要描述了该字段存储的数据，并指出了对筛选值的任何要求。该表按字段的字母升序排序，然后按 JSON 字段排序。

字段	JSON 字段	描述
账户 ID*	`accountId`	调查发现适用的 AWS 账户 的唯一标识符。这通常是拥有受影响资源的账户。
—	`archived`	一个布尔值，它指定调查发现是否被屏蔽规则屏蔽（自动存档）。 要在控制台的筛选条件中使用此字段，请在调查发现状态菜单上选择一个选项：已存档（仅限屏蔽）、当前（仅限取消屏蔽）或全部（包括屏蔽和未屏蔽）。
类别	`category`	调查发现的类别。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。在 API 中，有效值为：`CLASSIFICATION` ，针对敏感数据调查发现；和 `POLICY`，针对策略调查发现。
—	`count`	调查发现的出现总数。对于敏感数据调查发现，此值始终为 1。所有敏感数据调查发现都被认为是唯一的。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义数值范围。
创建时间	`createdAt`	Macie 创建调查发现的日期和时间。

字段	JSON 字段	描述
		您可以使用此字段为筛选条件定义时间范围。
调查发现 ID*	`id`	调查发现的唯一标识符。这是 Macie 在创建调查发现时生成并分配给调查发现的随机字符串。
调查发现类型*	`type`	调查发现的类型，例如，`SensitiveData:S3Object/Personal` 或 `Policy:IAMUser/S3BucketPublic` 。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 中有效值的列表，请参阅FindingType《亚马逊 Macie API 参考》。
区域	`region`	Macie 在其中创建了调查发现的 AWS 区域，例如，`us-east-1` 或 `ca-central-1` 。
样本	`sample`	指定调查发现是否为样本调查发现的布尔值。样本调查发现是一种使用示例数据和占位符值来演示调查发现可能包含的内容的调查发现。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。

字段	JSON 字段	描述
严重性	`severity.description`	调查发现严重程度的定性表示。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。在 API 中，有效值为 `Low`、`Medium` 和 `High`。
更新时间	`updatedAt`	上次更新调查发现的日期和时间。对于敏感数据调查发现，此值与创建时间字段的值相同。所有敏感数据调查发现均被视为新发现（唯一的）。 您可以使用此字段为筛选条件定义时间范围。

* 要在控制台上为此字段指定多个值，请添加一个使用该字段的条件并为筛选条件指定一个不同的值，然后对每个其他值重复该步骤。要使用 API 执行此操作，请使用一个列出用于筛选条件的值的数组。

受影响的资源字段

以下主题列出并描述了可用于根据查找调查发现适用的资源筛选调查发现的字段。主题按资源类型组织。

主题

- S3 存储桶
- S3 对象

S3 存储桶

下表列出并描述了可用于根据调查发现所适用的 S3 存储桶特征筛选调查发现的字段。

在表中，字段列指明了 Amazon Macie 控制台上该字段的名称。JSON 字段列使用点符号在调查发现和 Amazon Macie API 的 JSON 表示形式中表示字段的名称。（较长的 JSON 字段名称使用换行符序

列 (\ n) 来提高可读性。 ） 描述列简要描述了该字段存储的数据，并指出了对筛选值的任何要求。该表按字段的字母升序排序，然后按 JSON 字段排序。

字段	JSON 字段	描述
—	`resourcesAffected.s3Bucket.createdAt`	受影响的存储桶的创建日期和时间，或者最近对受影响的存储桶进行更改（例如修改存储桶的策略）的日期和时间。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义时间范围。
S3 存储桶的默认加密	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	服务器端加密算法，默认情况下用于加密添加到受影响存储桶中的对象。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 的有效值列表，请参阅EncryptionType《亚马逊 Macie API 参考》。
S3 存储桶加密 KMS 密钥 ID*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	默认情况下用于加密添加到受影响存储桶的对象的 AWS KMS key 的 Amazon 资源名称（ARN）或唯一标识符（密钥 ID）。
存储桶策略必需的 S3 存储桶加密	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	指定在向存储桶添加对象时，受影响存储桶的存储桶策略是否要求对对象进行服务器端加密。

字段	JSON 字段	描述
		当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 的有效值列表，请参阅 Amazon Macie API 参考中的 S3Bucket。
S3 存储桶名称*	`resourcesAffected.s3Bucket.name`	受影响存储桶的全名。
S3 存储桶所有者显示名称*	`resourcesAffected.s3Bucket.owner.displayName`	拥有受影响存储桶的 AWS 用户的显示名称。
S3 存储桶公开访问权限	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	根据适用于存储桶的权限设置组合，指定受影响的存储桶是否可公开访问。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 的有效值列表，请参阅BucketPublicAccess《亚马逊 Macie API 参考》。

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		一个布尔值，指定 Amazon S3 是否屏蔽受影响存储桶和存储桶中的对象的公共访问权限控制列表（ACL）。这是存储桶的账户级屏蔽公共访问权限设置。
		
		此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.blockPublicPolicy	一个布尔值，指定 Amazon S3 是否屏蔽受影响存储桶的公共存储桶策略。这是存储桶的账户级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.ignorePublicAcls	一个布尔值，指定 Amazon S3 是否忽略受影响存储桶和存储桶中对象的公共 ACL。这是存储桶的账户级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets	一个布尔值，指定 Amazon S3 是否限制受影响存储桶的公共存储桶策略。这是存储桶的账户级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess	一个布尔值，用于指定受影响存储桶的存储桶级 ACL 是否向公众授予该存储桶的读取访问权限。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess	一个布尔值，用于指定受影响存储桶的存储桶级 ACL 是否向公众授予该存储桶的写入访问权限。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAcls	一个布尔值，指定 Amazon S3 是否屏蔽受影响的存储桶和存储桶中对象的公共 ACL。这是存储桶的存储桶级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy	一个布尔值，指定 Amazon S3 是否屏蔽受影响存储桶的公共存储桶策略。这是存储桶的存储桶级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls	一个布尔值，指定 Amazon S3 是否忽略受影响存储桶和存储桶中对象的公共 ACL。这是存储桶的存储桶级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets	一个布尔值，指定 Amazon S3 是否限制受影响存储桶的公共存储桶策略。这是存储桶的存储桶级屏蔽公共访问权限设置。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	一个布尔值，用于指定受影响的存储桶的策略是否允许公众拥有对该存储桶的读取权限。 此字段不能作为控制台上的筛选选项使用。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	一个布尔值，用于指定受影响的存储桶的策略是否允许公众拥有对存储桶的写入权限。 此字段不能作为控制台上的筛选选项使用。
S3 存储桶标签键*	`resourcesAffected.s3Bucket.tags.key`	与受影响的存储桶关联的标签键。
S3 存储桶标签值*	`resourcesAffected.s3Bucket.tags.value`	与受影响的存储桶关联的标签值。

* 要在控制台上为此字段指定多个值，请添加一个使用该字段的条件并为筛选条件指定一个不同的值，然后对每个其他值重复该步骤。要使用 API 执行此操作，请使用一个列出用于筛选条件的值的数组。

S3 对象

下表列出并描述了可用于根据调查发现所适用的 S3 对象的特征筛选调查发现的字段。

在表中，字段列指明了 Amazon Macie 控制台上该字段的名称。JSON 字段列使用点符号在调查发现和 Amazon Macie API 的 JSON 表示形式中表示字段的名称。描述列简要描述了该字段存储的数据，并指出了对筛选值的任何要求。该表按字段的字母升序排序，然后按 JSON 字段排序。

字段	JSON 字段	描述
S3 对象加密 KMS 密钥 ID*	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	用于加密受影响对象的AWS KMS key 的 Amazon 资源名称（ARN）或唯一标识符（密钥 ID）。
S3 对象加密类型	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	用于加密受影响对象的服务器端加密算法。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 的有效值列表，请参阅EncryptionType《亚马逊 Macie API 参考》。
—	`resourcesAffected.s3Object.extension`	受影响对象的文件扩展名。对于没有文件扩展名的对象，请指定 "" 为筛选条件的值。 此字段不能作为控制台上的筛选选项使用。
—	`resourcesAffected.s3Object.lastModified`	创建受影响对象或上次更改受影响对象的日期和时间，以最新日期为准。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义时间范围。

字段	JSON 字段	描述
S3 对象键*	`resourcesAffected.s3Object.key`	受影响对象的全名（键），包括对象的前缀（如果适用）。
—	`resourcesAffected.s3Object.path`	受影响对象的完整路径，包括受影响存储桶的名称和对象的名称（键）。 此字段不能作为控制台上的筛选选项使用。
S3 对象公共访问权限	`resourcesAffected.s3Object.publicAccess`	一个布尔值，它根据适用于该对象的权限设置组合来指定受影响对象是否可公开访问。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。
S3 对象标签键*	`resourcesAffected.s3Object.tags.key`	与受影响对象关联的标签键。
S3 对象标签值*	`resourcesAffected.s3Object.tags.value`	与受影响对象关联的标签值。

* 要在控制台上为此字段指定多个值，请添加一个使用该字段的条件并为筛选条件指定一个不同的值，然后对每个其他值重复该步骤。要使用 API 执行此操作，请使用一个列出用于筛选条件的值的数组。

策略字段

下表列出并描述了您可使用筛选策略调查发现的字段。这些字段存储特定于策略调查发现的数据。

在表中，字段列指明了 Amazon Macie 控制台上该字段的名称。JSON 字段列使用点符号在调查发现和 Amazon Macie API 的 JSON 表示形式中表示字段的名称。（较长的 JSON 字段名称使用换行符序

列 (\ n) 来提高可读性。 ） 描述列简要描述了该字段存储的数据，并指出了对筛选值的任何要求。该表按字段的字母升序排序，然后按 JSON 字段排序。

字段	JSON 字段	描述
操作类型	`policyDetails.action.actionType`	产生调查发现的操作的类型。该字段的唯一有效值是 `AWS_API_CALL` 。
API 调用名称*	`policyDetails.action.apiCallDetails.api`	最近调用并得出调查发现的操作的名称，例如。`PutBucketPublicAccessBlock`
API 服务名称*	`policyDetails.action.apiCallDetails.apiServiceName`	AWS 服务 的 URL 提供了被调用并产生调查发现的操作，例如，`s3.amazonaws.com` 。
—	`policyDetails.action.apiCallDetails.firstSeen`	调用任何操作并得出调查发现的第一个日期和时间。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义时间范围。
—	`policyDetails.action.apiCallDetails.lastSeen`	调用指定操作（API 调用名称或 `api`）并生成调查发现的最新日期和时间。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义时间范围。
—	`policyDetails.actor.domainDetails.domainName`	用于执行操作的设备的域名。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
知识产权城市*	`policyDetails.actor.ipAddressDetails.ipCity.name`	用于执行操作的设备的 IP 地址的起始城市名称。
IP 国家/地区*	`policyDetails.actor.ipAddressDetails.ipCountry.name`	用于执行操作的设备 IP 地址的来源国家/地区的名称，例如，`United States`。
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	自治系统的自治系统号（ASN），包括用于执行操作的设备的 IP 地址。 此字段不能作为控制台上的筛选选项使用。
IP 所有者 ASN 组织*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	与自治系统的 ASN 关联的组织标识符，其中包括用于执行操作的设备的 IP 地址。
IP 所有者 ISP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	拥有用于执行操作的设备的 IP 地址的互联网服务提供商（ISP）的名称。
IP V4 地址*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	用于执行操作的设备的互联网协议版本 4（IPv4）。
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	对于使用通过 AWS STS API 的 `AssumeRole` 操作获得的临时安全凭证执行的操作，请提供标识凭证的 AWS 访问密钥 ID。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
用户身份代入角色账户 id*	`policyDetails.actor.userIdentity.assumedRole.accountId`	对于使用通过 AWS STS API 的 `AssumeRole` 操作获得的临时安全凭证执行的操作，请提供拥有用于获取凭证的实体的 AWS 账户 的唯一标识符。
用户身份代入角色主体 id*	`policyDetails.actor.userIdentity.assumedRole.principalId`	对于使用通过 AWS STS API 的 `AssumeRole` 操作获得的临时安全凭证执行的操作，请提供用于获取凭证的实体的唯一标识符。
用户身份代入角色会话 ARN*	`policyDetails.actor.userIdentity.assumedRole.arn`	对于使用通过 AWS STS API 的 `AssumeRole` 操作获得的临时安全凭证执行的操作，请提供用于获取凭证的来源账户、IAM 用户或角色的 Amazon 资源名称（ARN）。

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		对于使用通过 AWS STS API 的 `AssumeRole` 操作获得的临时安全凭证执行的操作，请提供临时安全凭证的来源，例如 `Root`、`IAMUser`、或 `Role`。
		
		此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName	对于使用通过 AWS STS API 的 AssumeRole 操作获得的临时安全凭证执行的操作，请提供发布会话的用户或角色的名称或别名。请注意，如果凭证是从没有别名的根账户获得的，则此值为空。 此字段不能作为控制台上的筛选选项使用。
用户身份 AWS 账户账户 ID*	policyDetails.actor.userIdentity.awsAccount.accountId	对于使用另一个 AWS 账户 的凭证执行的操作，请提供该账户的唯一标识符。
用户身份 AWS 账户主体 ID*	policyDetails.actor.userIdentity.awsAccount.principalId	对于使用另一个 AWS 账户 的凭证执行的操作，请提供执行该操作的实体的唯一标识符。
调用的用户身份 AWS 服务	policyDetails.actor.userIdentity.awsService.invokedBy	对于属于 AWS 服务 的账户执行的操作，请提供服务的名称。
—	policyDetails.actor.userIdentity.federatedUser.accessKeyId	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供标识凭证的 AWS 访问密钥 ID。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
用户身份联合验证会话 ARN*	policyDetails.actor.userIdentity.federatedUser.arn	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供用于获取凭证的实体的 ARN。
用户身份联合验证用户账户 ID*	policyDetails.actor.userIdentity.federatedUser.accountId	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供拥有用于获取凭证的实体的 AWS 账户 的唯一标识符。
用户身份联合验证用户主体 ID*	policyDetails.actor.userIdentity.federatedUser.principalId	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供用于获取凭证的实体的唯一标识符。
—	policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.type	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供临时安全凭证的来源，例如 Root、IAMUser 或 Role。 此字段不能作为控制台上的筛选选项使用。

字段	JSON 字段	描述
—	policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName	对于使用通过 AWS STS API 的 GetFederationToken 操作获得的临时安全凭证执行的操作，请提供发布会话的用户或角色的名称或别名。请注意，如果凭证是从没有别名的根账户获得的，则此值为空。 此字段不能作为控制台上的筛选选项使用。
用户身份 IAM 账户 ID *	policyDetails.actor.userIdentity.iamUser.accountId	对于使用 IAM 用户的凭证执行的操作，请提供与执行该操作的 IAM 用户关联的 AWS 账户的唯一标识符。
用户身份 IAM 主体 ID*	policyDetails.actor.userIdentity.iamUser.principalId	对于使用 IAM 用户的凭证执行的操作，请提供执行该操作的 IAM 用户的唯一标识符。
用户身份 IAM 用户名*	policyDetails.actor.userIdentity.iamUser.userName	对于使用 IAM 用户的凭证执行的操作，请提供执行该操作的 IAM 用户的用户名。
用户身份根账户 ID*	policyDetails.actor.userIdentity.root.accountId	对于使用您的 AWS 账户 的凭证执行的操作，请提供账户的唯一标识符。
用户身份根主体 ID*	policyDetails.actor.userIdentity.root.principalId	对于使用您的 AWS 账户 的凭证执行的操作，请提供执行该操作的实体的唯一标识符。

字段	JSON 字段	描述
用户身份类型	`policyDetails.actor.userIdentity.type`	执行产生调查发现的操作的实体的类型。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关 API 的有效值列表，请参阅UserIdentityType《亚马逊 Macie API 参考》。

* 要在控制台上为此字段指定多个值，请添加一个使用该字段的条件并为筛选条件指定一个不同的值，然后对每个其他值重复该步骤。要使用 API 执行此操作，请使用一个列出用于筛选条件的值的数组。

敏感数据分类字段

下表列出并描述了您可用于筛选敏感数据调查发现的字段。这些字段存储特定于敏感数据调查发现的数据。

在表中，字段列指明了 Amazon Macie 控制台上该字段的名称。JSON 字段列使用点符号在调查发现和 Amazon Macie API 的 JSON 表示形式中表示字段的名称。描述列简要描述了该字段存储的数据，并指出了对筛选值的任何要求。该表按字段的字母升序排序，然后按 JSON 字段排序。

字段	JSON 字段	描述
自定义数据标识符 ID*	`classificationDetails.result.customDataIdentifiers.detections.arn`	检测数据并生成调查发现的自定义数据标识符的唯一标识符。
自定义数据标识符名称*	`classificationDetails.result.customDataIdentifiers.detections.name`	用于检测数据并生成调查发现的自定义数据标识符的名称。

字段	JSON 字段	描述
自定义数据标识符总数	classificationDetails.result.customDataIdentifiers.detections.count	由自定义数据标识符检测到并产生调查发现的数据总出现次数。 您可以使用此字段为筛选条件定义数值范围。
作业 ID*	classificationDetails.jobId	产生调查发现的敏感数据发现任务的唯一标识符。
来源类型	classificationDetails.originType	Macie 是如何找到产生这一调查发现的敏感数据的：AUTOMATED_SENSITIVE_DATA_DISCOVERY 或 SENSITIVE_DATA_DISCOVERY_JOB 。
—	classificationDetails.result.mimeType	调查发现适用的内容类型（以 MIME 类型表示），例如，用于 CSV 文件的 text/csv 或用于 Adobe 便携文档格式文件的 application/pdf 。 此字段不能作为控制台上的筛选选项使用。
—	classificationDetails.result.sizeClassified	调查发现适用的 S3 对象的总存储大小（以字节为单位）。 此字段不能作为控制台上的筛选选项使用。通过 API，您可以使用此字段为筛选条件定义数值范围。

字段	JSON 字段	描述
结果状态代码*	`classificationDetails.result.status.code`	调查发现的状态。有效值为： • COMPLETE – Macie 完成了对对象的分析。 • PARTIAL – Macie 仅分析对象中的数据子集。例如，该对象是一个存档文件，其中包含不支持的格式的文件。 • SKIPPED – Macie 无法分析对象。例如，该对象是一个格式错误的文件。
敏感数据类别	`classificationDetails.result.sensitiveData.category`	检测到并产生调查发现的敏感数据类别。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。在 API 中，有效值为 `CREDENTIALS` 、`FINANCIAL_INFORMATION` 和 `PERSONAL_INFORMATION` 。
敏感数据检测类型	`classificationDetails.result.sensitiveData.detections.type`	检测到并产生调查发现的敏感数据的类型。 当您将此字段添加到筛选条件时，控制台会提供一个值列表供您选择。有关控制台和 API 的有效值的列表，请参阅 敏感数据检测类型。

字段	JSON 字段	描述
敏感数据总数	`classificationDetails.result.sensitiveData.detections.count`	检测到并产生调查发现的敏感数据的总出现次数。 您可以使用此字段为筛选条件定义数值范围。

* 要在控制台上为此字段指定多个值，请添加一个使用该字段的条件并为筛选条件指定一个不同的值，然后对每个其他值重复该步骤。要使用 API 执行此操作，请使用一个列出用于筛选条件的值的数组。

敏感数据检测类型

以下主题列出了可以在筛筛选条件中为敏感数据检测类型字段指定的值。（此字段的 JSON 名称为 `classificationDetails.result.sensitiveData.detections.type`。）主题按 Macie 可以使用托管数据标识符检测的敏感数据类别组织。

类别

- 凭证
- 财务信息
- 个人信息：个人健康信息（PHI）
- 个人信息：个人身份信息（PII）

要了解有关特定类型敏感数据的托管数据标识符的更多信息，请参阅 详细参考：Amazon Macie 托管数据标识符。

凭证

您可以指定以下值来筛选报告 S3 对象中凭证数据出现情况的调查发现。

敏感数据类型	筛选值
AWS秘密访问密钥	`AWS_CREDENTIALS`
Google Cloud API 密钥	`GCP_API_KEY`
HTTP 基本授权标头	`HTTP_BASIC_AUTH_HEADER`

敏感数据类型	筛选值
JSON Web 令牌 (JWT)	JSON_WEB_TOKEN
OpenSSH 私有密钥	OPENSSH_PRIVATE_KEY
PGP 私有密钥	PGP_PRIVATE_KEY
公有密钥加密标准 (PKCS) 私有密钥	PKCS
PuTTY 私有密钥	PUTTY_PRIVATE_KEY
Stripe API 密钥	STRIPE_CREDENTIALS

财务信息

您可以指定以下值来筛选报告 S3 对象中财务信息出现情况的调查发现。

敏感数据类型	筛选值
银行账号	BANK_ACCOUNT_NUMBER （适用于加拿大和美国）
基本银行账号 (BBAN)	视国家或地区而定：FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
信用卡到期日期	CREDIT_CARD_EXPIRATION
信用卡磁条数据	CREDIT_CARD_MAGNETIC_STRIPE
信用卡号	CREDIT_CARD_NUMBER （适用于关键字附近的信用卡号），CREDIT_CARD_NUMBER_(NO_KEYWORD) （适用于不在关键字附近的信用卡号）

敏感数据类型	筛选值
信用卡验证码	CREDIT_CARD_SECURITY_CODE

敏感数据类型	筛选值
国际银行账号 (IBAN)	视国家或地区而定：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, MA

敏感数据类型	筛选值
	URITIUS_BANK_ACCOUNT_NUMBER , MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_N UMBER, NETHERLANDS_BANK_AC COUNT_NUMBER, NORTH_MACEDO NIA_BANK_ACCOUNT_NUMBER, P OLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER , SWITZERLAND_BANK_ACCOUNT_NU MBER, TIMOR_LESTE_BANK_ACC OUNT_NUMBER, TUNISIA_BANK_ ACCOUNT_NUMBER, TURKIYE_B ANK_ACCOUNT_NUMBER, UK_BAN K_ACCOUNT_NUMBER, UKRAINE_B ANK_ACCOUNT_NUMBER, UNITED _ARAB_EMIRATES_BANK_ACCOUNT _NUMBER, VIRGIN_ISLANDS_BA NK_ACCOUNT_NUMBER （适用于英属维尔京群岛）

个人信息：个人健康信息（PHI）

您可以指定以下值来筛选报告 S3 对象中个人健康信息 (PHI) 出现情况的调查发现。

敏感数据类型	筛选值
毒品管理局 (DEA) 注册号	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
健康保险索赔编号 (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
健康保险或医疗识别号	视国家或地区而定：CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
医疗保健通用程序编码系统 (HCPCS) 代码	USA_HEALTHCARE_PROCEDURE_CODE
国家药品编码 (NDC)	USA_NATIONAL_DRUG_CODE
国家提供商识别码 (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
设备唯一标识符 (UDI)	MEDICAL_DEVICE_UDI

个人信息：个人身份信息（PII）

您可以指定以下值来筛选报告 S3 对象中个人身份信息（PII）出现情况的调查发现。

敏感数据类型	筛选值
出生日期	DATE_OF_BIRTH
驾驶执照识别号	视国家或地区而定：AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE,

敏感数据类型	筛选值
	CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE （对于美国）, 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
选民名册编号	UK_ELECTORAL_ROLL_NUMBER
全名	NAME
全球定位系统 (GPS) 坐标	LATITUDE_LONGITUDE
HTTP cookie	HTTP_COOKIE
邮寄地址	ADDRESS, BRAZIL_CEP_CODE

敏感数据类型	筛选值
身份证号码	视国家或地区而定：BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保险号码 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
护照编号	视国家或地区而定：CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
永久居留号码	CANADA_NATIONAL_IDENTIFICATION_NUMBER
电话号码	视国家或地区而定：BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER （适用于加拿大和美国），SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
社会保险号码 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社会保障号码（SSN）	视国家或地区而定：SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

敏感数据类型	筛选值
纳税人识别号或参考号	视国家或地区而定：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
车辆识别号码 (VIN)	VEHICLE_IDENTIFICATION_NUMBER

使用 Amazon Macie 调查发现调查敏感数据

当您运行敏感数据发现任务或 Amazon Macie 执行自动敏感数据发现时，Macie 会捕获有关其在 Amazon Simple Storage Service (Amazon S3) 对象中发现的每次敏感数据出现位置的详细信息。这包括 Macie 使用托管数据标识符检测到的敏感数据，以及符合您配置任务或 Macie 要使用的自定义数据标识符标准的数据。

通过敏感数据调查发现，您可以查看 Macie 在单个 S3 对象中发现的多达 15 次敏感数据的详细信息。这些详细信息使您可以深入了解特定 S3 存储桶和对象可能包含的敏感数据的类别和类型的广度。它们可以帮助您定位对象中出现的单个敏感数据，并确定是否对特定的存储桶和对象进行更深入的调查。

为了获得更多见解，您可以选择配置和使用 Macie 来检索 Macie 在个别调查发现中报告的敏感数据样本。这些样本可以帮助您验证 Macie 发现的敏感数据的性质。此外还有助您对受影响的 Amazon S3 存储桶和对象进行定制的调查。如果您选择检索调查发现的敏感数据样本，Macie 会使用调查发现中的数据来定位该调查发现报告的每种敏感数据的 1-10 个匹配项。然后，Macie 从受影响的对象中提取出现的敏感数据，并显示这些数据供您查看。

如果 S3 对象包含多次出现的敏感数据，则调查发现还可以帮助您导航到相应的敏感数据发现结果。与敏感数据调查发现不同，敏感数据发现结果提供 Macie 在对象中发现的每种敏感数据类型的多达 1,000

次出现的详细位置数据。Macie 对敏感数据调查发现和敏感数据发现结果中的位置数据使用相同的架构。要了解有关敏感数据发现结果的更多信息，请参阅 存储和保留敏感数据发现结果。

本节中的主题说明了如何定位和有选择地检索敏感数据调查发现所报告的敏感数据的出现次数。他们还解释了 Macie 用来报告 Macie 发现的单个敏感数据出现位置的架构。

主题

使用 Amazon Macie 调查发现定位敏感数据

当您运行敏感数据发现作业或者 Amazon Macie 执行自动敏感数据发现时，Macie 会对其分析的每个 Amazon Simple Storage Service (Amazon S3) 对象的最新版本进行深入检查。对于每个作业运行或分析周期，Macie 还使用深度优先搜索算法，使用 Macie 在 S3 对象中发现的敏感数据出现特定次数的位置相关详细信息填充产生的调查发现。这些出现次数提供了对受影响的 S3 存储桶和对象可能包含的敏感数据的类别和类型的深入了解。这些详细信息可以帮助您定位对象中出现的单个敏感数据，并确定是否对特定的存储桶和对象进行更深入的调查。

通过敏感数据调查发现，您可以确定 Macie 在受影响的 S3 对象中发现的多达 15 次敏感数据的位置。这包括 Macie 使用托管数据标识符检测到的敏感数据，以及符合您配置作业或 Macie 要使用的自定义数据标识符标准的数据。

敏感数据调查发现可以提供详细信息，例如：

- Microsoft Excel 工作簿、CSV 文件或 TSV 文件中单元格或字段的列号和行号。
- JSON 或 JSON Lines 文件中的字段或数组路径。
- 除 CSV、JSON、JSON Lines 或 TSV 文件之外的非二进制文本文件中的行号，例如 HTML、TXT 或 XML 文件。
- Adobe 便携式文档格式 (PDF) 文件中页面的页码。
- Apache Avro 对象容器或 Apache Parquet 文件中记录的字段的记录索引和路径。

您可以通过使用 Amazon Macie 控制台或 Amazon Macie API 访问这些详细信息。您还可以在 Macie 发布到其他 AWS 服务（包括 Amazon EventBridge 和 AWS Security Hub）的调查发现中访问这些详细信息。要了解 Macie 用来报告这些详细信息的 JSON 结构，请参阅敏感数据位置的 JSON 架构。要了解如何访问 Macie 发布到其他 AWS 服务 的调查发现中的详细信息，请参阅监控和处理结果。

如果 S3 对象包含多次出现的敏感数据，则您还可以使用调查发现来导航到相应的敏感数据发现结果。与敏感数据调查发现不同，敏感数据发现结果为 Macie 在对象中发现的各种敏感数据多达 1,000 次的出现提供详细位置数据。如果 S3 对象是存档文件，例如 .tar 或 .zip 文件，则这包括 Macie 从存档中提取的各个文件中出现多次的敏感数据。（Macie 不会在敏感数据调查发现中包含此信息。）要了解有关敏感数据发现结果的更多信息，请参阅 存储和保留敏感数据发现结果。Macie 对敏感数据调查发现和敏感数据发现结果中的位置数据使用相同的架构。

查找敏感数据的出现位置

要查找敏感数据的出现位置，您可以使用Amazon Macie 控制台或 Amazon Macie API。以下步骤说明如何通过使用控制台定位敏感数据。

要以数据编程方式查找敏感数据，请使用 Amazon Macie API 的 GetFindings 操作。如果调查发现包含有关特定类型敏感数据一次或多次出现的位置的详细信息，则该调查发现中的`occurrences`对象将提供这些详细信息。有关更多信息，请参阅敏感数据位置的 JSON 架构。

定位敏感数据的出现位置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。

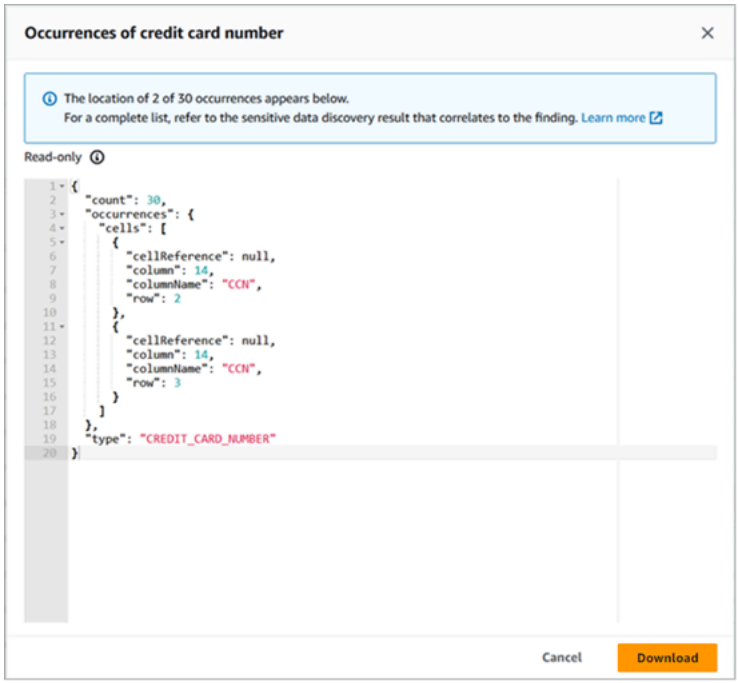
   > **Tip**
   >
   > 您可以使用作业页面来显示特定敏感数据发现作业中的所有调查发现。为此，在导航窗格中选择作业，然后选择该作业的名称。在详细信息面板的顶部，选择显示结果，然后选择显示调查发现。

3. 在调查发现页面上，选择要定位的敏感数据的调查发现。详细信息面板会显示调查发现的信息。
4. 在详细信息面板中，滚动至敏感数据部分。本部分提供有关 Macie 在受影响的 S3 对象中发现的敏感数据的类别和类型的信息。它还会显示 Macie 发现的各种敏感数据的出现次数。

   例如，下图显示了调查发现的一些详细信息，该调查发现报告了信用卡号出现 30 次、姓名出现 30 次和美国社会安全号码出现 30 次。

如果调查发现包含有关特定类型敏感数据一次或多次出现的位置的详细信息，则出现次数是一个链接。选择该链接以显示详细信息。Macie 会打开一个新窗口，并以 JSON 格式显示详细信息。

例如，下图显示了受影响的 S3 对象中信用卡号两次出现的位置。



要将详细信息另存为 JSON 文件，请选择下载，然后为该文件指定名称和位置。

5. （可选）要将所有调查发现的详细信息另存为 JSON 文件，请在详细信息面板顶部选择调查发现的标识符（调查发现 ID）。Macie 会打开一个新窗口，并以 JSON 格式显示所有详细信息。选择下载，然后为该文件指定名称和位置。

要访问有关受影响对象中各种敏感数据多达 1,000 次出现的位置的详细信息，请参阅调查发现的相应敏感数据发现结果。为此，请滚动至面板的详细信息部分的开头。然后在详细结果位置字段中选择链接。Macie 会打开 Amazon S3 控制台并显示包含相应发现结果的文件或文件夹。

使用 Amazon Macie 的调查发现检索敏感数据样本

要验证 Amazon Macie 在调查发现中报告的敏感数据的性质，您可以配置并使用 Amazon Macie 来检索和显示在单独的调查发现中报告的敏感数据样本。这包括 Macie 使用托管数据标识符检测到的敏感数据，以及符合自定义数据标识符标准的数据。这些样本有助您定制对受影响的 Amazon Simple Storage Service（Amazon S3）对象和存储桶的调查。

检索和显示调查发现的敏感数据样本时，Macie 会执行以下常规任务：

1. 验证调查发现是否指定了敏感数据单次出现的位置，以及相应的敏感数据发现位置。
2. 评估相应的敏感数据发现结果，检查受影响 S3 对象的元数据的有效性，以及受影响对象中敏感数据的出现位置数据的有效性。
3. 通过使用敏感数据发现结果的数据，可以定位调查发现报告的前 1-10 次出现的敏感数据，并从受影响的 S3 对象中提取每次出现的前 1-128 个字符。如果调查发现报告多种类型敏感数据，Macie 报告最多 100 种类型。
4. 它使用您指定的 AWS Key Management Service （AWS KMS）密钥加密已提取的数据。
5. 将加密的数据临时存储在缓存中，并显示数据以供您查看。传输中的数据和静态中的数据均可加密。
6. 解压缩和加密后不久，会永久删除缓存数据，临时需要额外保留以解决操作问题的情况除外。

如果您选择重新检索和显示某个调查发现的敏感数据样本，Macie 会重复这些任务来查找、提取、加密、存储和最终删除样本。

Macie 不会使用账户的服务相关角色来执行这些任务。而应使用您的 AWS Identity and Access Management（IAM）身份或允许 Macie 代入您账户中的 IAM 角色。如果您或该角色有权访问必要的资源和数据，以及执行必要的操作，则可以检索和显示调查发现的敏感数据样本。所有必需的操作都已登录AWS CloudTrail。

> **Important**
>
> 我们建议您使用自定义 IAM 策略 限制对此功能的访问。作为额外的访问控制，我们建议您创建专用 AWS KMS key，以加密检索到的敏感数据样本，并限制该密钥的使用，使密钥仅限于必须允许其检索和显示敏感数据样本的主体。
> 有关您想要控制访问此功能的策略建议和样本，请参见AWS 安全博客中的如何使用 Amazon Macie 预览 S3 存储桶中的敏感数据。

此部分中的主题介绍了：如何配置和使用 Macie 检索和显示敏感数据样本以获取调查发现。您可在 Macie 当前可用的所有 AWS 区域中执行该任务，亚太地区（大阪）和以色列（特拉维夫）地区除外。

主题

- 使用调查发现检索敏感数据样本的配置选项和要求
- 配置 Amazon Macie 来使用调查发现检索和显示敏感数据样本
- 使用调查发现检索和显示敏感数据样本

使用调查发现检索敏感数据样本的配置选项和要求

您可以配置并使用 Amazon Macie 来检索和显示 Macie 在单独的调查发现中报告的敏感数据样本。检索和显示某项调查发现的敏感数据样本时，Macie 会使用相应敏感数据调查发现结果中的数据来从受影响的 Amazon Simple Storage Service（Amazon S3）对象中查找敏感数据。然后，Macie 从受影响的对象中提取这些事件样本。Macie 使用您指定的 AWS Key Management Service (AWS KMS) 密钥对提取数据进行加密，将加密的数据临时存储至缓存，然后返回调查发现中的数据以进行查找。解压缩和加密后不久，Macie 会从缓存中永久删除数据，除非临时需要额外保留以解决操作问题。

Macie 不会使用您账户的 Macie 服务相关角色来查找、检索、加密或显示受影响 S3 对象中的敏感数据样本，而是使用您为账户配置的设置和资源。在 Macie 中配置这些设置时，需要指定访问受影响的 S3 对象的方式。您还可以指定用来加密样本的 AWS KMS key。您可在当前开放 Macie 服务的所有 AWS 区域配置这些设置，亚太地区（大阪）和以色列（特拉维夫）区域除外。

您可以通过两种方法来访问受影响的 S3 对象并从中检索敏感数据样本。您可以将 Macie 配置为使用 AWS Identity and Access Management（IAM）用户凭证或代入 IAM 角色：

- 使用 IAM 用户凭证 – 选择此选项后，您账户中的每个用户都将使用自己的 IAM 身份来查找、检索、加密和显示样本。这意味着，如果允许用户访问必要的资源和数据以及执行必要的操作，用户将可以检索和显示调查发现的敏感数据样本。
- 代入 IAM 角色 – 选择此选项后，您可以创建一个 IAM 角色来将访问权限委派给 Macie。您还需要确保该角色的信任和权限策略满足 Macie 代入该角色的所有要求。然后在您账户中的用户选择查找、检索、加密和显示某个调查发现的敏感数据样本时，Macie 将代入该角色。

这两种配置可以用于任何类型的 Macie 账户，例如组织的委派 Macie 管理员帐户、组织中的 Macie 成员账户或独立的 Macie 账户。

以下主题说明了有助于确定如何为账户配置设置和资源的相关选项、要求和注意事项。这包括要附加到 IAM 角色的信任和权限策略。有关可用于检索和显示敏感数据样本的更多建议和策略示例，请参阅《AWS 安全博客》中的 How to use Amazon Macie to preview sensitive data in S3 buckets。

主题

确定要使用的访问方法

在确定哪种配置最适合您的 AWS 环境时，一个关键的考量因素是您的环境是否包含作为组织进行集中管理的多个 Amazon Macie 账户。如果您是组织的委派 Macie 管理员，则建议将 Macie 配置为代入 IAM 角色，这样可以简化组织中账户从受影响的 S3 对象中检索敏感数据样本的流程。使用这种方法时，您需要在自己的管理员账户中创建一个 IAM 角色。您还需要在每个相关成员账户中创建一个 IAM 角色。管理员账户中的角色将访问权限委派给 Macie。成员账户中的角色会将跨账户存取权限委派给管理员账户中的角色。如果实施了角色链，则可以使用角色链来访问成员账户的受影响的 S3 对象。

此外还要考虑默认情况下谁可以直接访问具体的调查发现。要检索和显示调查发现的敏感数据样本，用户首先要有该调查发现的访问权限：

- 敏感数据发现作业 – 仅创建作业的账户才能访问该作业生成的调查发现。如果您拥有 Macie 管理员账户，则可以配置一个作业来分析组织中任何账户的 S3 存储桶中对象。因此，您的任务可能会生成成员账户所拥有存储桶中的对象的调查发现。如果您有成员账户或独立的 Macie 账户，则可以配置作业以仅分析您的账户所拥有存储桶中的对象。
- 自动敏感数据发现 – 只有 Macie 管理员账户才能访问自动发现功能为组织中的账户生成的调查发现。成员账户无法访问这些调查发现。如果您拥有独立的 Macie 账户，则只能访问自动发现功能为自己的账户生成的调查发现。

如果您计划使用 IAM 角色来访问受影响的 S3 对象，则还要考虑以下几点：

- 要查找对象中的敏感数据出现频次，必须将调查发现的相应敏感数据发现结果存储在 Macie 使用 HMAC 散列消息认证码 AWS KMS key 签名的 S3 对象中。Macie 必须要能够验证敏感数据发现结果的完整性和真实性。否则，Macie 不会代入该 IAM 角色来检索敏感数据样本。这是一项额外的防护机制，可限制对账户的 S3 对象中数据的访问权限。
- 要检索使用客户自主管理型 AWS KMS key 加密的对象中的敏感数据样本，必须要允许该 IAM 角色使用该密钥解密数据。更具体地说，该密钥的策略必须允许该角色执行 `kms:Decrypt` 操作。对于其他类型的服务器端加密，无需额外的权限或资源即可解密受影响的对象。有关更多信息，请参阅解密受影响的 S3 对象。
- 要检索其他账户的对象中的敏感数据样本，您当前必须是该账户在相应 AWS 区域中的委派 Macie 管理员。此外：
  - 当前必须在相应的区域为该成员账户启用 Macie。
  - 成员账户必须有一个 IAM 角色，用来向您的 Macie 管理员账户中的 IAM 角色委派跨账户存取权限。您的 Macie 管理员账户和该成员账户中的角色名称必须相同。
  - 在成员账户中，该 IAM 角色的信任策略必须包含一个正确指定您配置的外部 ID 的条件。此 ID 是一个唯一的字母数字字符串，由 Macie 在您为 Macie 管理员账户配置设置后自动生成。有关信任

策略中的外部 ID 的信息，请参阅《AWS Identity and Access Management IAM 用户》指南中的如何在向第三方授予对 AWS 资源的访问权时使用外部 ID。

- 如果成员账户中的 IAM 角色满足 Macie 的所有要求，则该成员账户无需配置和启用 Macie 设置，即可让您从其账户的对象中检索敏感数据样本。Macie 仅使用您的 Macie 管理员账户中的设置和 IAM 角色以及成员账户中的 IAM 角色。

> **Tip**
>
> 如果您的账户属于某个大型组织，则建议使用 AWS CloudFormation 模板和堆栈集来为组织中的成员账户预置和管理 IAM 角色。有关创建和使用模板及堆栈集的信息，请参阅 AWS CloudFormation 用户指南。
>
> 要查看并选择下载可以作为起点使用的 CloudFormation 模板，您可以使用 Amazon Macie 控制台。在控制台的导航窗格中，在设置下，选择显示样本。选择编辑，然后选择查看成员角色权限和 CloudFormation 模板。

本节的后续主题介绍了每种配置类型的更多详细信息和注意事项。对于 IAM 角色，这包括要附加到角色的信任和权限策略。如果您不确定哪种配置最适合您的环境，请向您的 AWS 管理员寻求帮助。

使用 IAM 用户凭证访问受影响的 S3 对象

如果您将 Amazon Macie 配置为使用 IAM 用户凭证来检索敏感数据样本，则您的 Macie 账户中的每个用户都将使用自己的 IAM 身份来查找、检索、加密和显示具体调查发现的样本。这意味着，如果允许用户的 IAM 身份访问必要的资源和数据以及执行必要的操作，用户将可以检索和显示调查发现的敏感数据样本。所有必需的操作都 已登录AWS CloudTrail。

要检索和显示特定调查发现的敏感数据样本，必须要允许用户访问下列数据和资源：发现结果、相应的敏感数据发现结果、受影响的 S3 存储桶以及受影响的 S3 对象。如果适用，还必须允许用户使用用于加密受影响对象的 AWS KMS key，以及您为 Macie 配置的用于加密敏感数据样本的 AWS KMS key。如果任何 IAM policy、资源策略或其他权限设置拒绝提供必要的访问权限，则该用户将无法检索和显示该调查发现的样本。

要设置此类配置，请完成以下常规任务：

1. 确认您已配置了用于存储敏感数据发现结果的存储库。
2. 配置用来加密敏感数据样本的 AWS KMS key。
3. 确认您拥有在 Macie 中配置这些设置的权限。
4. 在 Macie 中配置并启用这些设置。

有关执行这些任务的信息，请参阅 配置 Amazon Macie 来使用调查发现检索和显示敏感数据样本。

代入 IAM 角色来访问受影响的 S3 对象

要将 Amazon Macie 配置为通过代入 IAM 角色来检索敏感数据样本，首先需要创建一个向 Macie 委派访问权限的 IAM 角色。需要确保该角色的信任和权限策略满足 Macie 代入该角色的所有要求。当 Macie 账户中的用户随后选择检索和显示某项调查发现的敏感数据样本时，Macie 将代入该角色来检索受影响 S3 对象中的样本。仅当用户选择检索和显示某项调查发现的样本时，Macie 才会代入该角色。Macie 会使用 AssumeRole AWS Security Token Service（AWS STS）API操作来代入该角色。所有必需的操作都 已登录AWS CloudTrail。

要检索和显示特定调查发现的敏感数据样本，必须允许用户访问该调查发现、相应的敏感数据发现结果以及您为 Macie 配置的用于加密敏感数据样本的 AWS KMS key。该 IAM 角色必须允许 Macie 访问受影响的 S3 存储桶和受影响的 S3 对象。如果适用，还必须允许该角色使用用于加密受影响对象的 AWS KMS key。如果任何 IAM policy、资源策略或其他权限设置拒绝提供必要的访问权限，则该用户将无法检索和显示该调查发现的样本。

要设置此类配置，请完成以下常规任务。如果您拥有组织中的成员帐户，请联系您的 Macie 管理员以确定是否能够以及如何配置账户的设置和资源。

1. 定义以下内容：
   - 您希望 Macie 代入的 IAM 角色的名称。如果您的账户属于某个组织，则对于该组织的委派 Macie 管理员账户和每个相关成员账户，该名称必须相同。否则，Macie 管理员将无法访问相关成员账户的受影响的 S3 对象。
   - 要附加到该 IAM 角色的 IAM 权限策略的名称。如果您的账户属于某个组织，我们建议您为该组织中的每个相关成员账户使用相同的策略名称。这可以简化成员账户中的角色预置和管理过程。
2. 确认您已配置了用于存储敏感数据发现结果的存储库。
3. 配置用来加密敏感数据样本的 AWS KMS key。
4. 确认您拥有在 Macie 中创建 IAM 角色和配置这些设置的权限。
5. 如果您是组织的委派 Macie 管理员或拥有独立的 Macie 账户：
   a. 为您的账户创建并配置 IAM 角色。需要确保该角色的信任和权限策略满足 Macie 代入该角色的所有要求。有关这些要求的详细信息，请参阅 下一个主题。
   b. 在 Macie 中配置并启用这些设置。然后，Macie 会为该配置生成一个外部 ID。如果您是某个组织的 Macie 管理员，请记下此 ID。您必须在每个相关成员账户中为该 IAM 角色的信任策略指定此 ID。
6. 如果您拥有某个组织的成员账户：

a. 向您的 Macie 管理员索要将在您的账户中为该 IAM 角色的信任策略指定的外部 ID。此外还需要确认该 IAM 角色的名称以及要创建的权限策略。

b. 为您的账户创建并配置 IAM 角色。需要确保该角色的信任和权限策略满足 Macie 管理员代入该角色的所有要求。有关这些要求的详细信息，请参阅 下一个主题。

c. （可选）如果需要从自己账户中的受影响 S3 对象检索和显示敏感数据样本，请在 Macie 中配置并启用这些设置。如果您希望 Macie 通过代入某个 IAM 角色来检索样本，请首先在您的账户中额外创建和配置一个 IAM 角色。确保此额外角色的信任和权限策略满足 Macie 代入该角色的所有要求。然后在 Macie 中配置这些设置并指定此额外角色的名称。有关该角色的策略要求的详细信息，请参阅 下一个主题。

有关执行这些任务的信息，请参阅 配置 Amazon Macie 来使用调查发现检索和显示敏感数据样本。

配置 IAM 角色以访问受影响的 S3 对象

要使用 IAM 角色来访问受影响的 S3 对象，首先需要创建并配置一个向 Amazon Macie 委派访问权限的角色。需要确保该角色的信任和权限策略满足 Macie 代入该角色的所有要求。具体操作步骤取决于您拥有的 Macie 账户的类型。

以下部分详细介绍了对于每种类型的 Macie 账户，需要附加到 IAM 角色的信任和权限策略。选择与您所拥有账户的类型对应的部分。

> **Note**
>
> 如果您拥有某个组织的成员账户，则可能需要为您的账户创建和配置两个 IAM 角色：
>
> - 要允许您的 Macie 管理员从您账户中的受影响 S3 对象检索和显示敏感数据样本，请创建并配置管理员账户可以代入的角色。要了解这些详细信息，请选择 Macie 成员账户部分。
> - 要从您自己账户中的受影响 S3 对象检索和显示敏感数据样本，请创建并配置 Macie 可以代入的角色。要了解这些详细信息，请选择独立 Macie 账户部分。
>
> 在创建和配置任何一个 IAM 角色之前，请首先联系您的 Macie 管理员，以确定您账户的适当配置。

有关使用 IAM 创建角色的详细信息，请参阅《AWS Identity and Access Management 用户指南》中的使用自定义信任策略创建角色。

Macie 管理员账户

如果您是某个组织的委派 Macie 管理员，请首先使用 IAM policy 编辑器为该 IAM 角色创建权限策略。该策略应如下所示：

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

其中 *IAMRoleName* 是 Macie 从组织的账户中受影响的 S3 对象检索敏感数据样本时要代入的 IAM 角色的名称。将该值替换为您正在为您的账户创建，并且计划为组织中相关成员账户创建的角色的名称。对于 Macie 管理员账户与每个相关成员账户，该名称必须相同。

> **Note**
>
> 在前面的权限策略中，第一条语句中的 `Resource` 元素使用了通配符（`*`）。这将允许附加的 IAM 实体从组织拥有的所有 S3 存储桶中检索对象。要仅允许访问特定的存储桶，请将通配符替换为每个存储桶的 Amazon 资源名称（ARN）。例如，要仅允许访问名为 DOC-EXAMPLE-BUCKET 的存储桶中的对象，请将该元素更改为：
>
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`

> 您还可以将访问范围限定为个别账户的特定 S3 存储桶中的对象。要实现此目的，请在每个相关账户中在该 IAM 角色的权限策略的 `Resource` 元素中指定存储桶 ARN。有关更多信息和示例，请参阅《IAM 用户指南》AWS Identity and Access Management中的 IAM JSON 策略元素：Resource。

为该 IAM 角色创建权限策略后，创建并配置该角色。如果使用 IAM 控制台执行此操作，则对于该角色的可信实体类型，请选择自定义信任策略。对于为该角色定义可信实体的信任策略，请指定以下内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

其中，*accountID* 是您的 AWS 账户的账户 ID。请将该值替换为您的 12 位账户 ID。

在前面的信任策略中：

- `Principal` 元素指定了 Macie 在从受影响的 S3 对象 `reveal-samples.macie.amazonaws.com` 检索敏感数据样本时将使用的服务主体。
- `Action` 元素指定了允许该服务主体执行的操作，即 AssumeRole AWS Security Token Service（AWS STS）API 操作。
- `Condition` 元素定义了一个使用 aws:SourceAccount 全局条件上下文键的条件。该条件决定了可以执行指定操作的账户。在此例中，该条件只允许 Macie 为指定账户（*accountID*）代入该角色。该条件有助于防止 Macie 在与 AWS STS 进行事务处理时被用作 混淆代理。

为 IAM 角色定义信任策略后，请将权限策略附加到该角色。这应是您在开始创建角色之前就已经创建的权限策略。然后在 IAM 中完成剩余的步骤以完成角色的创建和配置。完成后，在 Macie 中配置并启用设置。

Macie 成员账户

如果您拥有 Macie 成员账户，并且希望允许您的 Macie 管理员从账户中的受影响 S3 对象检索和显示敏感数据样本，请首先要求您的 Macie 管理员提供以下信息：

- 要创建的 IAM 角色的名称。对于您的账户和组织的 Macie 管理员账户，该名称必须相同。
- 要附加到该角色的 IAM 权限策略的名称。
- 要在信任策略中为该角色指定的外部 ID。该 ID 必须是 Macie 为您的 Macie 管理员配置生成的外部 ID。

收到这些信息后，使用 IAM policy 编辑器为该角色创建权限策略。该策略应如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

前述权限策略将允许附加的 IAM 实体从您账户的所有 S3 存储桶中检索对象。这是因为，策略中的 `Resource` 元素使用了通配符（`*`）。要仅允许访问特定的存储桶，请将通配符替换为每个存储桶的 Amazon 资源名称（ARN）。例如，要仅允许访问名为 DOC-EXAMPLE-BUCKET2 的存储桶中的对象，请将该元素更改为：

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

有关更多信息和示例，请参阅《IAM 用户指南》AWS Identity and Access Management中的 IAM JSON 策略元素：Resource。

为该 IAM 角色创建权限策略后，请创建该角色。如果使用 IAM 控制台创建该角色，则对于该角色的可信实体类型，请选择自定义信任策略。对于为该角色定义可信实体的信任策略，请指定以下内容。

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

在前面的策略中，请将占位符值替换为适合您的 AWS 环境的值，其中：

- *administratorAccountID* 是 Macie 管理员账户的 12 位账户 ID。
- *IAMRoleName* 是该 IAM 角色在 Macie 管理员账户中的名称。这应是 Macie 管理员提供的名称。
- *externalID* 是 Macie 管理员提供的外部 ID。

通常，信任策略将允许您的 Macie 管理员代入该角色，从而从您账户的受影响 S3 对象中检索和显示敏感数据样本。`Principal` 元素指定了 Macie 管理员账户中的 IAM 角色的 ARN。这是 Macie 管理员用来检索和显示组织账户中的敏感数据样本的角色。`Condition` 块定义了两个条件，这些条件进一步确定了谁可以代入该角色：

- 第一个条件指定了组织的配置所独有的外部 ID。要了解有关外部 ID 的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的 如何在向第三方授予对 AWS 资源的访问权时使用外部 ID。
- 第二个条件使用 aws:PrincipalOrgID 全局条件上下文键。该键的值是一个动态变量，表示组织在 AWS Organizations（`${aws:ResourceOrgID}`）中的唯一标识符。该条件将访问范围限定仅允许

属于 AWS Organizations 中同一组织的账户访问。如果通过在 Macie 中接受邀请加入您的组织，则请从策略中移除此条件。

为 IAM 角色定义信任策略后，请将权限策略附加到该角色。这应是您在开始创建角色之前就已经创建的权限策略。然后在 IAM 中完成剩余的步骤以完成角色的创建和配置。请勿在 Macie 中配置和输入该角色的设置。

独立 Macie 账户

如果您拥有独立的 Macie 账户或 Macie 成员账户，并且想要从自己账户中的受影响 S3 对象中检索和显示的敏感数据样本，请首先使用 IAM policy 编辑器为该 IAM 角色创建权限策略。该策略应如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

在前面的权限策略中，`Resource` 元素使用了通配符（`*`）。这将允许附加的 IAM 实体您账户的所有 S3 存储桶中检索对象。要仅允许访问特定的存储桶，请将通配符替换为每个存储桶的 Amazon 资源名称（ARN）。例如，要仅允许访问名为 DOC-EXAMPLE-BUCKET3 的存储桶中的对象，请将该元素更改为：

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

有关更多信息和示例，请参阅《IAM 用户指南》AWS Identity and Access Management中的 IAM JSON 策略元素：Resource。

为该 IAM 角色创建权限策略后，请创建该角色。如果使用 IAM 控制台创建该角色，则对于该角色的可信实体类型，请选择自定义信任策略。对于为该角色定义可信实体的信任策略，请指定以下内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

其中，*accountID* 是您的 AWS 账户的账户 ID。请将该值替换为您的 12 位账户 ID。

在前面的信任策略中：

- `Principal` 元素指定了 Macie 在从受影响的 S3 对象 `reveal-samples.macie.amazonaws.com` 检索和显示敏感数据样本时将使用的服务主体。
- `Action` 元素指定了允许该服务主体执行的操作，即 AssumeRole AWS Security Token Service（AWS STS）API 操作。
- `Condition` 元素定义了一个使用 aws:SourceAccount 全局条件上下文键的条件。该条件决定了可以执行指定操作的账户。该条件只允许 Macie 为指定账户（*accountID*）代入该角色。该条件有助于防止 Macie 在与 AWS STS 进行事务处理时被用作 混淆代理。

为 IAM 角色定义信任策略后，请将权限策略附加到该角色。这应是您在开始创建角色之前就已经创建的权限策略。然后在 IAM 中完成剩余的步骤以完成角色的创建和配置。完成后，在 Macie 中配置并启用设置。

解密受影响的 S3 对象

Amazon S3 支持多种 S3 对象的加密选项。对于大多数选项，IAM 用户或角色无需额外的资源或权限即可解密和检索受影响对象中的敏感数据样本。使用 Amazon S3 托管式密钥或 AWS 托管式 AWS KMS key进行服务器端加密的对象就属于这种情况。

但是，如果 S3 对象是使用客户自主管理型的 AWS KMS key进行加密的，则需要额外的权限才能解密和检索该对象中的敏感数据样本。更具体地说，该 KMS 密钥的密钥政策必须允许该 IAM 用户或角色执行 `kms:Decrypt` 操作。否则会出现错误，并且 Macie 不会从对象中检索任何样本。要了解如何为 IAM 用户提供此访问权限，请参阅《AWS Key Management Service 开发人员指南》中的 Authentication and access control for AWS KMS。

为 IAM 角色提供此访问权限的方法取决于拥有 AWS KMS key的账户是否同时也拥有该角色：

- 如果该 KMS 密钥和该角色由同一账户拥有，则该账户的用户必须更新该密钥的策略。
- 如果该 KMS 密钥由一个账户拥有，而该角色由另一个账户拥有，则拥有密钥的账户的用户必须允许对该密钥进行跨账户存取。

本主题介绍了如何为您创建的 IAM 角色执行这些任务，以检索 S3 对象中的敏感数据样本。此外还提供了这两种场景的示例。有关在其他场景中允许访问客户自主管理型 AWS KMS keys的信息，请参阅《AWS Key Management Service 开发人员指南》AWS KMS中的 Authentication and access control for 。

允许同一个账户访问客户托管密钥

如果该 AWS KMS key和该 IAM 角色由同一账户拥有，则该账户的用户必须在该密钥的策略中添加一条语句。该附加语句必须允许该 IAM 角色使用该密钥来解密数据。有关更新密钥政策的详细信息，请参阅 AWS Key Management Service 开发者指南 中的更改密钥政策。

在以下语句中：

- `Principal` 元素必须指定该 IAM 角色的 Amazon 资源名称（ARN）。
- 数 `Action` 数组必须指定 `kms:Decrypt` 操作。这是解密使用该密钥进行加密的对象时必须允许该 IAM 角色执行的唯一 AWS KMS 操作。

以下是添加至 KMS 密钥策略的语句示例。

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
```

```
    ],
    "Resource": "*"
}
```

在上述示例中：

- `Principal` 元素中的 `AWS` 字段指定了账户的 IAM 角色的 ARN。这将允许该角色执行策略语句中指定的操作。*123456789012* 是示例账户 ID。请将该值替换拥有该角色和 KMS 密钥的账户的 ID。*IAMRoleName* 是一个示例名称。请将该值替换为账户中的 IAM 角色的名称。
- `Action` 数组指定了允许该 IAM 角色使用该 KMS 密钥执行的操作，即解密使用该密钥加密的加密文字。

将此语句添加到密钥政策的位置，取决于该策略当前包含的结构和元素。当添加语句时，请确保语法有效。JSON 格式的密钥策略。这意味着您还必须在语句前后添加逗号，具体取决于您在策略中添加语句的位置。

允许跨账户存取客户托管密钥

如果 AWS KMS key由一个账户拥有（密钥所有者），而 IAM 角色由另一个账户拥有（角色所有者），则密钥所有者必须向角色所有者提供对该密钥的跨账户存取权限。执行此操作的一种方法是使用授权。授权是一种策略分析工具，如果由授权指定的条件得到满足，则允许 AWS 主体将 KMS 密钥用于加密操作中。要了解有关授权的信息，请参阅AWS Key Management Service 开发者指南中的AWS KMS授权。

使用这种方法时，密钥所有者首先要确保该密钥的策略允许角色所有者为该密钥创建授权。然后，角色所有者需要为该密钥创建授权。该授权会将相关权限委派给其账户中的 IAM 角色。这将允许该角色解密使用该密钥加密的 S3 对象。

第 1 步：更新密钥政策

在密钥政策中，密钥所有者应确保策略中包含一条语句，从而允许角色所有者在角色所有者的账户中为 IAM 角色创建授权。在此语句中，`Principal` 元素必须指定角色所有者账户的 ARN。数 `Action` 数组必须指定 `kms:CreateGrant` 操作。`Condition` 块可以筛选对指定操作的访问权限。以下为 KMS 密钥策略语句示例。

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

在上述示例中：

- `Principal` 元素中的 `AWS` 字段指定了角色所有者账户的 ARN。这将允许该账户执行策略语句中指定的操作。*111122223333* 是示例账户 ID。请将该值替换为角色所有者账户的账户 ID。
- `Action` 数组指定了允许角色所有者对该 KMS 密钥执行的操作，即为该密钥创建授权。
- `Condition` 块使用了 条件运算符 和以下条件键，用来筛选角色所有者有权对 KMS 密钥执行的操作的访问权限：
  - kms:GranteePrincipal – 此条件允许角色所有者仅为指定的被授权主体（即其账户中 IAM 角色的 ARN）创建授权。在 ARN 中，*111122223333* 是示例账户 ID。请将该值替换为角色所有者账户的账户 ID。*IAMRoleName* 是一个示例名称。请将该值替换为角色所有者账户中的 IAM 角色的名称。
  - kms:GrantOperations – 此条件允许角色所有者创建仅委派执行 AWS KMS `Decrypt` 操作（解密使用该密钥加密的加密文字）的权限的授权。这可以防止角色所有者创建委派对 KMS 密钥执行其他操作的权限的授权。AWS KMS 操作是解密使用该密钥进行加密的对象时必须允许该 IAM 角色执行的唯一 `Decrypt` 操作。

密钥所有者将此语句添加到密钥政策的位置，取决于密钥政策当前包含的结构和元素。当密钥拥有者添加语句时，他们应确保语法有效。JSON 格式的密钥策略。这意味着密钥拥有者还必须在语句前后添加逗号，具体取决于他们在策略中添加语句的位置。有关更新密钥政策的详细信息，请参阅 AWS Key Management Service 开发者指南 中的更改密钥政策。

第 2 步：创建授权

在密钥所有者根据需要更新密钥政策后，角色所有者需要为该密钥创建授权。该授权会将相关权限委派给角色所有者账户中的 IAM 角色。角色所有者应首先确认自己是否有权执行 kms:CreateGrant 操作，然后才能创建授权。此操作使其能够向现有的客户自主管理型 AWS KMS key添加授权。

要创建授权，角色所有者可以使用 CreateGrant AWS Key Management Service API 操作。角色所有者创建授权时，应为所需参数指定以下值：

- KeyId – KMS 密钥的 ARN。对于跨账户存取 KMS 密钥，该值必须是 ARN。它不能是密钥 ID。
- GranteePrincipal – 其账户中 IAM 角色的 ARN。该值应为 arn:aws:iam::*111122223333*:role/*IAMRoleName*，其中 *111122223333* 是角色所有者账户的账户 ID，*IAMRoleName* 是角色的名称。
- Operations – AWS KMS 解密操作（Decrypt）。这是解密使用该 KMS 密钥进行加密的对象时必须允许该 IAM 角色执行的唯一 AWS KMS 操作。

如果角色所有者使用的是 AWS Command Line Interface（AWS CLI），则可以运行 create-grant 命令来创建授权。下面的示例演示如何操作。此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
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"
```

其中：

- key-id 指定要应用授权的 KMS 密钥的 ARN。
- grantee-principal 指定了允许执行该授权所指定操作的 IAM 角色的 ARN。该值应与密钥政策中 kms:GranteePrincipal 条件指定的 ARN 一致。
- operations 指定了授权允许指定主体执行的操作，即解密使用该密钥加密的加密文字。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

其中 GrantToken，代表已创建授权的唯一、非秘密的、长度可变的 base64 编码字符串，GrantId 也是唯一授权标识符。

配置 Amazon Macie 来使用调查发现检索和显示敏感数据样本

您可以选择配置和使用 Amazon Macie 来检索和显示 Macie 在个别敏感数据调查发现中报告的敏感数据样本。这些样本可以帮助您验证 Macie 发现的敏感数据的性质。他们还可以帮助您对受影响的 Amazon Simple Storage Service (Amazon S3) 对象和存储桶定制调查。您可在当前可用的 Macie 所有 AWS 区域 中检索和显示敏感数据样本，亚太地区（大阪）和以色列（特拉维夫）地区除外。

当您检索和显示调查发现的敏感数据样本时，Macie 会使用相应敏感数据调查发现中的数据来定位受影响的 S3 对象中的敏感数据。然后，Macie 从受影响的对象中提取这些事件样本。Macie 使用您指定的 AWS Key Management Service (AWS KMS) 密钥对提取数据进行加密，将加密的数据临时存储至缓存，然后返回调查发现中的数据以进行查找。解压缩和加密后不久，Macie 会从缓存中永久删除数据，除非临时需要额外保留以解决操作问题。

要检索和显示调查发现的敏感数据样本，首先需要配置并启用您的 Macie 账户设置。此外还需要为您的账户配置支持资源和权限。本节中的主题将指导您完成配置 Macie 以检索和显示敏感数据样本以及管理账户配置状态的过程。

主题

- 开始之前
- 配置和启用 Amazon Macie 设置
- 禁用 Amazon Macie 设置

> **Tip**
>
> 有关您想要控制访问此功能的策略建议和样本，请参见AWS 安全博客中的如何使用 Amazon Macie 预览 S3 存储桶中的敏感数据。

开始之前

请首先完成以下任务，以确保您拥有所需的资源和权限，然后再配置 Amazon Macie 来检索和显示调查发现的敏感数据样本。

任务

- 第 1 步：配置用于存储敏感数据发现结果的存储库

- 第 2 步：确定如何访问受影响的 S3 对象
- 步骤 3：配置 AWS KMS key
- 第 4 步：验证您的权限

如果您已配置了 Macie 来检索和显示敏感数据样本，只需要更改配置设置，则这些任务是可选的。

第 1 步：配置用于存储敏感数据发现结果的存储库

当您检索和显示调查发现的敏感数据样本时，Macie 会使用相应敏感数据调查发现中的数据来定位受影响的 S3 对象中的敏感数据。因此，请务必确认您已配置了用于存储敏感数据发现结果的存储库。否则，Macie 将无法找到您想要检索与显示的敏感数据样本。

要确定您的账户是否已经配置了此存储库，请在 Amazon Macie 控制台的导航窗格中选择发现结果（在设置下）。要以编程方式执行此操作，请使用 Amazon Macie API 的 getClassorationExportConfiguration 操作。要详细了解敏感数据发现结果以及如何配置此存储库，请参阅 存储和保留敏感数据发现结果。

第 2 步：确定如何访问受影响的 S3 对象

您可以通过两种方法来访问受影响的 S3 对象并从中检索敏感数据样本。您可以将 Macie 配置为使用您的 AWS Identity and Access Management（IAM）用户凭证。您也可以将 Macie 配置为代入一个向 Macie 委派访问权限的 IAM 角色。这两种配置可以用于任何类型的 Macie 账户，例如组织的委派 Macie 管理员帐户、组织中的 Macie 成员账户或独立的 Macie 账户。在 Macie 中配置设置之前，首先需要确定要使用哪种访问方法。有关每种访问方法的选项和要求的详细信息，请参阅 使用调查发现检索敏感数据样本的配置选项和要求。

如果您计划使用 IAM 角色，请首先创建并配置该角色，然后再在 Macie 中配置设置。此外还需要确保该角色的信任和权限策略满足 Macie 代入该角色的所有要求。如果您的账户属于集中管理多个 Macie 账户的组织，请首先联系您的 Macie 管理员，确定是否能够以及如何为您的账户配置该角色。

步骤 3：配置 AWS KMS key

检索和显示某项调查发现的敏感数据样本时，Macie 会使用您指定的 AWS Key Management Service（AWS KMS）密钥对样本进行加密。因此，您需要确定要用来加密样本的 AWS KMS key。密钥可以是您自己账户中的现有 KMS 密钥，也可以是其他账户当前拥有的 KMS 密钥。要使用其他账户拥有的密钥，请获取此密钥的 Amazon 资源名称（ARN）。在 Macie 中输入设置时，您需要指定此 ARN。

KMS 密钥必须是客户自主管理的对称加密密钥。它还必须是与您的 Macie 账户AWS 区域 相同的单区域密钥。KMS 密钥可以置于外部密钥存储。但是，与完全在 AWS KMS 中管理的密钥相比，密钥可能

更慢且更不可靠。您要检索和显示的敏感数据样本遇到延迟或可用性问题，使 Macie 无法加密，则会发生错误，并且 Macie 不会为该调查发现返回任何样本。

此外，密钥的密钥政策必须允许相应的主体 (IAM 角色、IAM 用户或AWS 账户）执行以下操作：

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> 作为额外的访问控制层，我们建议您创建专用 KMS 密钥，以加密检索到的敏感数据样本，并限制该密钥的使用，使其仅限需要检索和显示敏感数据样本的主体。如果不允许用户对密钥执行上述操作，Macie 会拒绝用户检索和显示敏感数据样本的请求。Macie 没有为该调查发现返回任何样本。

有关创建和配置 KMS 密钥的信息，请参阅《AWS Key Management Service 开发人员指南》中的 Managing keys。有关密钥政策和管理 KMS 密钥访问权限的信息，请参阅《AWS Key Management Service 开发人员指南》中的 Key policies in AWS KMS。

第 4 步：验证您的权限

在 Macie 中配置设置之前，还需要确认自己拥有所需的权限。要验证权限，请使用 AWS Identity and Access Management (IAM) 查看附加到您的 IAM 身份的 IAM policy。然后将这些策略中的信息与以下必须允许您执行的操作列表进行比较。

Amazon Macie

对于 Macie，请确认允许您执行以下操作：

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

第一个操作允许您访问您的 Macie 账户。第二个操作让您可以更改有关检索和显示敏感数据样本的配置设置。这包括启用和禁用您账户的配置。

（可选）验证您是否也被允许执行 `macie2:GetRevealConfiguration` 操作。此操作让您可以检索当前的配置设置以及您账户当前的配置状态。

AWS KMS

如果您计划使用 Amazon Macie 控制台来输入配置设置，则还需要确认您是否拥有执行以下 AWS Key Management Service（AWS KMS）操作的权限：

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

这些操作允许您检索关于账户 AWS KMS keys 的信息。然后，您可以在输入设置时选择其中一个密钥。

IAM

如果您计划将 Macie 配置为通过代入某个 IAM 角色来检索和显示敏感数据样本，则还需要确认是否您是否有执行以下 IAM 操作的权限：`iam:PassRole`。此操作让您能够将该角色传递给 Macie，从而让 Macie 能够代入该角色。当您输入账户的配置设置时，Macie 还可以验证您的账户中是否存在该角色以及配置是否正确。

如果不允许您执行必要操作，请向 AWS 管理员寻求帮助。

配置和启用 Amazon Macie 设置

确认自己拥有所需的资源和权限后，您可以在 Amazon Macie 中配置设置并为您的账户启用该配置。

如果您的账户属于集中管理多个 Macie 账户的组织，在配置或随后更改账户设置之前，应注意以下要求：

- 如果您有成员帐户，请联系您的 Macie 管理员以确定是否能够以及如何配置账户的设置。您的 Macie 管理员可以协助您确定账户的正确配置设置。
- 如果您拥有 Macie 管理员账户，并且更改了有关访问受影响的 S3 对象的设置，则您的更改可能会影响您组织的其他账户和资源。这取决于当前是否将 Macie 配置为代入 AWS Identity and Access Management（IAM）角色来检索敏感数据样本。如果属于这种情况，并且您将 Macie 重新配置为使用 IAM 用户凭证，则 Macie 会永久删除该 IAM 角色的现有设置，即您配置的角色名称和外部 ID。如果您的组织随后选择重新使用 IAM 角色，则需要在信任策略中为每个相关成员账户中的角色指定新的外部 ID。

要详细了解这两种账户的配置选项，请参阅 使用调查发现检索敏感数据样本的配置选项和要求。

要在 Macie 中配置设置并为您的账户启用该配置，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤，使用 Amazon Macie 控制台配置和启用设置。

配置和启用 Macie 设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择您希望配置 Macie 以检索和显示敏感数据样本并启用该配置的区域。
3. 在导航窗格中的 设置 下，选择 展示样本。
4. 在 Settings（设置）部分中，选择 Edit（编辑）。
5. 对于状态，选择已启用。
6. 在访问下，指定从受影响的 S3 对象检索敏感数据样本时要使用的访问方法和设置：
   - 要使用向 Macie 委派访问权限的 IAM 角色，请选择代入 IAM 角色。如果选择此选项，Macie 将使用您的 AWS 账户中创建和配置的 IAM 角色来检索样本。在角色名称对话框中，输入该角色的名称。
   - 要使用请求样本的 IAM 用户的凭证，请选择使用 IAM 用户凭证。如果选择此选项，则您账户中的每个用户都将使用自己的 IAM 身份来检索样本。
7. 在加密下，指定要用于加密检索到的敏感数据样本的 AWS KMS key：
   - 要使用您自己账户中的 KMS密钥，请选择从您的账户中选择一个密钥。然后，在AWS KMS key列表中选择要使用的密钥。该列表显示您账户中现有的对称加密 KMS 密钥。
   - 要使用其他账户拥有的 KMS 密钥，请选择输入另一个账户中密钥的 ARN。然后，在 AWS KMS key ARN 框内，输入要使用的密钥的 Amazon 资源名称（ARN），例如**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**。
8. 输入完设置后，选择保存。

Macie 会测试设置并验证设置是否正确。如果您将 Macie 配置为代入某个 IAM 角色，Macie 还会验证您的账户中是否存在该角色以及信任和权限策略的配置是否正确。如果存在问题，Macie 会显示一条描述相关问题的消息。

要解决有关 AWS KMS key 的问题，请参阅上一主题中的要求并指定一个符合要求的 KMS 密钥。要解决有关 IAM 角色的问题，请首先确认您输入的角色名称是否正确。如果名称正确，请确保该角色的策略满足 Macie 代入该角色的所有要求。有关详细信息，请参阅 配置 IAM 角色以访问受影响的 S3 对象。解决所有问题后，您可以保存并启用设置。

> **Note**
>
> 如果您是组织的 Macie 管理员，并且已将 Macie 配置为代入某个 IAM 角色，则在保存账户设置后，Macie 会生成并显示一个外部 ID。记下此 ID。您必须在每个相关成员账户中为该 IAM 角色的信任策略指定此 ID。否则，您将无法从这些账户拥有的 S3 对象中检索敏感数据样本。

API

要以编程方式配置并启用这些设置，请使用 UpdateRevealConfiguration Amazon Macie API 操作。在请求中，请为支持的参数指定恰当的值：

- 对于 `retrievalConfiguration` 参数，请指定从受影响的 S3 对象检索敏感数据样本时要使用的访问方法和设置：
  - 要代入向 Macie 委派访问权限的 IAM 角色，请为 `retrievalMode` 参数指定 `ASSUME_ROLE` 并为 `roleName` 参数指定该角色的名称。如果您指定了这些设置，Macie 将代入您的 AWS 账户中创建和配置的 IAM 角色来检索样本。
  - 要使用请求样本的 IAM 用户的凭证，请为 `retrievalMode` 参数指定 `CALLER_CREDENTIALS`。如果您指定了此设置，则您账户中的每个用户都将使用自己的 IAM 身份来检索样本。

  > **Important**
  >
  > 如果您没有指定这些参数的值，Macie 会将访问方法（`retrievalMode`）设置为 `CALLER_CREDENTIALS`。如果 Macie 当前配置为使用 IAM 角色来检索样本，则 Macie 还会永久删除您配置的当前角色名称和外部 ID。要保留现有配置的这些设置，请在请求中包含 `retrievalConfiguration` 参数并指定这些参数的当前设置。要检索当前设置，请使用 GetRevealConfiguration 操作；如果您使用的是 AWS Command Line Interface（AWS CLI），请运行 get-reveal-configuration 令。

- 对于 `kmsKeyId` 参数，请指定要用于加密检索到的敏感数据样本的 AWS KMS key：
  - 要使用其他账户的 KMS 密钥，请为密钥指定 Amazon 资源名称（ARN）、ID 或别名。如果指定别名，请包括`alias/`前缀，例如`alias/ExampleAlias`。
  - 要使用其他账户拥有的 KMS 密钥，请指定此密钥的 ARN，例如`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。或

者为密钥指定别名的 ARN，例如`arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`。

- 对于 `status` 参数，请指定 ENABLED 以为您的 Macie 账户启用配置。

在请求中，还务必要指定要在其中启用和使用该配置的 AWS 区域。

要使用 AWS CLI 配置并启用这些设置，请运行 update-reveal-configuration 命令，并为支持的参数指定恰当的值。例如，假设您在 Microsoft Windows 上使用 AWS CLI，则运行以下命令：

```
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\"}
```

其中：

- *us-east-1* 是要启用和使用该配置的区域。在本示例中，为美国东部（弗吉尼亚州北部）区域。
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias* 是要使用的 AWS KMS key 的别名 ARN。在此示例中，密钥由另一个账户拥有。
- ENABLED 为配置状态。
- *ASSUME_ROLE* 是要使用的访问方法。在此示例中将会代入指定的 IAM 角色。
- *MacieRevealRole* 是 Macie 在检索敏感数据样本时要代入的 IAM 角色的名称。

上述示例使用脱字号（^）续行字符来提高可读性。

当您提交请求时，Macie 会测试设置。如果您将 Macie 配置为代入某个 IAM 角色，Macie 还会验证您的账户中是否存在该角色以及信任和权限策略的配置是否正确。如果出现问题，您的请求将会失败，并且 Macie 会返回一条描述该问题的消息。要解决有关 AWS KMS key 的问题，请参阅上一主题中的要求并指定一个符合要求的 KMS 密钥。要解决有关 IAM 角色的问题，请首先确认您指定的角色名称是否正确。如果名称正确，请确保该角色的策略满足 Macie 代入该角色的所有要求。有关详细信息，请参阅 配置 IAM 角色以访问受影响的 S3 对象。解决该问题后，请重新提交请求。

如果您的请求成功，Macie 会在指定区域为您的账户启用配置，您会收到与以下内容类似的输入。

```
{
```

```
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

其中，`kmsKeyId` 指定用于加密检索到的敏感数据样本的 AWS KMS key，`status` 是 Macie 账户的配置状态。`retrievalConfiguration` 值指定检索样本时要使用的访问方法和设置。

> **Note**
>
> 如果您是组织的 Macie 管理员，并且已将 Macie 配置为代入 IAM 角色，请记下响应中的外部 ID（`externalId`）。您必须在每个相关成员账户中为该 IAM 角色的信任策略指定此 ID。否则，您将无法从这些账户拥有的受影响 S3 对象中检索敏感数据样本。

若要在随后检查账户配置的设置和状态，请对AWS CLI使用 GetRevealConfiguration 运算符，运行 get-reveal-configuration 命令。

禁用 Amazon Macie 设置

您可以随时禁用 Amazon Macie 账户的配置设置。如果您禁用该配置，Macie 会保留指定用来加密检索到的敏感数据样本的 AWS KMS key 的设置。Macie 会永久删除该配置的 Amazon S3 访问设置。

> **Warning**
>
> 禁用 Macie 账户的配置设置时，也将永久删除指定如何访问受影响的 S3 对象的当前设置。如果当前将 Macie 配置为通过代入 AWS Identity and Access Management（IAM）角色来访问受影响的对象，则这将包括：角色名称以及 Macie 为该配置生成的外部 ID。这些设置在删除后将无法恢复。

要为您的 Macie 账户禁用配置设置，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤，使用 Amazon Macie 控制台为您的账户禁用配置设置。

禁用 Macie 设置

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中为您的 Macie 账户禁用配置设置的区域。
3. 在导航窗格中的 设置 下，选择 展示样本。
4. 在 Settings（设置）部分中，选择 Edit（编辑）。
5. 对于状态，请选择禁用。
6. 选择 Save（保存）。

API

要以编程方式禁用配置设置，请使用 UpdateRevealConfiguration Amazon Macie API 操作。在请求中，务必要指定要在其中禁用该配置的 AWS 区域。对于 `status` 参数，请指定 `DISABLED`：

要使用 AWS Command Line Interface（AWS CLI）禁用配置设置，请运行 update-reveal-configuration 命令。使用 `region` 参数指定要在其中禁用该配置的区域。对于 `status` 参数，请指定 `DISABLED`：例如，假设您在 Microsoft Windows 上使用 AWS CLI，则运行以下命令：

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

其中：

- *`us-east-1`* 是要禁用该配置的区域。在本示例中，为美国东部（弗吉尼亚州北部）区域。
- `DISABLED` 是配置的新状态。

如果您的请求成功，Macie 会在指定区域为您的账户禁用该配置，并且您会收到与以下类似的输出。

```
{
    "configuration": {
        "status": "DISABLED"
    }
```

```
}
```

其中 `status` 是 Macie 账户的新配置状态。

如果之前将 Macie 配置为代入 IAM 角色来检索敏感数据样本，则也可以选择删除该角色和该角色的权限策略。禁用账户的配置设置时，Macie 不会删除这些资源。此外，Macie 不会使用这些资源为您的账户执行任何其他任务。要删除该角色及其权限策略，您可以使用 IAM 控制台或 IAM API。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的 删除角色。

使用调查发现检索和显示敏感数据样本

使用 Amazon Macie，您可以检索并显示 Macie 在单独的敏感数据调查发现中报告的敏感数据样本。这包括 Macie 使用托管数据标识符检测到的敏感数据，以及符合自定义数据标识符标准的数据。这些样本可以帮助您验证 Macie 发现的敏感数据的性质。他们还可以帮助您对受影响的 Amazon Simple Storage Service (Amazon S3) 对象和存储桶定制调查。除亚太地区（大阪）和以色列（特拉维夫）地区外，您可以检索和显示当前所有 Macie 可用区域的敏感数据样本。 AWS 区域

如果您检索并显示某项发现的敏感数据样本，Macie 会使用相应敏感数据发现结果中的数据来定位该发现报告的前 1-10 次出现的敏感数据。然后，Macie 从受影响的 S3 对象中提取每次出现的前 1-128 个字符。如果一项调查发现报告了多种类型的敏感数据，则 Macie 会对调查发现报告的多达 100 种敏感数据执行此操作。

当 Macie 从受影响的 S3 对象中提取敏感数据时，Macie 会使用您指定的 AWS Key Management Service (AWS KMS) 密钥对数据进行加密，将加密的数据临时存储在缓存中，然后返回结果中的数据以进行查找。解压缩和加密后不久，Macie 会从缓存中永久删除数据，除非临时需要额外保留以解决操作问题。

如果您选择重新检索和显示有关某个调查发现的敏感数据样本，Macie 会重复查找、提取、加密、存储和最终删除样本的过程。

要演示如何使用 Amazon Macie 控制台检索和显示敏感数据样本，请观看以下视频：使用 Amazon Macie 检索和显示敏感数据样本。

主题

开始前的准备工作

您首先需要 为您的 Amazon Macie 账户配置并启用设置，然后才能检索和显示调查发现的敏感数据样本。您还需要与 AWS 管理员合作，验证自己是否拥有所需的权限和资源。

当您检索和显示某项调查发现的敏感数据样本时，Macie 会执行一系列任务来查找、检索、加密和显示样本。Macie 不会使用账户的 服务相关角色来执行这些任务。相反，您可以使用您的 AWS Identity and Access Management (IAM) 身份或允许 Macie 在您的账户中担任 IAM 角色。

要检索和显示某项发现的敏感数据样本，您必须有权访问调查结果、相应的敏感数据发现结果以及您配置 Macie 以用于加密敏感数据样本的结果。 AWS KMS key 此外，您或该 IAM 角色必须有权访问受影响的 S3 存储桶和受影响的 S3 对象。还必须允许您或该角色使用用于加密受影响对象的（如果适用）。 AWS KMS key 如果任何 IAM policy、资源策略或其他权限设置拒绝必要的访问权限，则会发生错误，并且 Macie 不会返回调查发现的任何样本。

还必须允许您执行以下 Macie 操作：

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

前三个操作允许您访问您的 Macie 账户并检索调查发现的详细信息。最后一个操作允许您检索和显示调查发现的敏感数据样本。

要使用 Amazon Macie 控制台检索和显示敏感数据样本，还必须允许您执行以下操作：`macie2:GetSensitiveDataOccurrencesAvailability`。此操作允许您确定是否有针对个别调查发现的样本。您无需权限即可执行此操作以编程方式检索和显示样本。但是，拥有此权限可以简化样本检索流程。

如果您是某个组织的委派 Macie 管理员，并且您将 Macie 配置为通过代入 IAM 角色来检索敏感数据样本，则还必须允许您执行以下操作：`macie2:GetMember`。此操作将允许您检索有关您的账户与受影响账户之间关联的信息。这让 Macie 能够验证您当前是否是受影响账户的 Macie 管理员。

如果不允许您执行必要的操作或访问必需的数据和资源，请向 AWS 管理员寻求帮助。

确定调查发现是否有敏感数据样本可用

要检索和显示某项调查发现的敏感数据样本，该调查发现需要满足某些标准。它必须包括特定出现的敏感数据的位置数据。此外，它还必须指定有效的、相应的敏感数据发现结果的位置。敏感数据发现结果

必须与发现 AWS 区域 结果存储在同一位置。如果您通过担任 AWS Identity and Access Management (IAM) 角色将 Amazon Macie 配置为访问受影响的 S3 对象，则敏感数据发现结果还必须存储在 Macie 使用基于哈希的消息身份验证码 (HMAC) 签名的 S3 对象中。 AWS KMS key

受影响的 S3 对象还需要满足某些标准。对象的 MIME 类型必须是以下类型之一：

- application/avro，用于 Apache Avro 对象容器 (.avro) 文件
- application/gzip，用于 GNU Zip 压缩存档（ .gz 或 .gzip ）文件
- application/json，用于 JSON 或 JSON Lines（ .json 或.jsonl ）文件
- application/parquet，用于 Apache Parquet (.parquet) 文件
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet，用于 Microsoft Excel 工作簿（ .xlsx ）文件
- application/zip，用于 ZIP 压缩存档 (.zip) 文件
- text/csv，用于 CSV (.csv) 文件
- text/plain，用于 CSV、JSON、JSON Lines 或 TSV 文件以外的非二进制文本文件
- text/tab-separated-values，用于 TSV (.tsv) 文件

此外，该 S3 对象的内容必须与创建调查发现时的内容相同。Macie 会检查对象的实体标签 (ETag)，以确定它是否与调查发现指定的 ETag 相匹配。此外，对象的存储大小不能超过检索和显示敏感数据样本的适用大小配额。有关适用配额的列表，请参阅Amazon Macie 限额。

如果调查发现和受影响的 S3 对象符合上述标准，则该调查发现就有敏感数据样本可用。在尝试检索和显示某项调查发现的样本之前，您可以选择确定某项调查发现是否属于这种情况。

若要确定是否有敏感数据样本可用于调查发现

您可以使用 Amazon Macie 控制台或 Amazon Macie API 来确定是否有敏感数据样本可用于调查发现。

Console

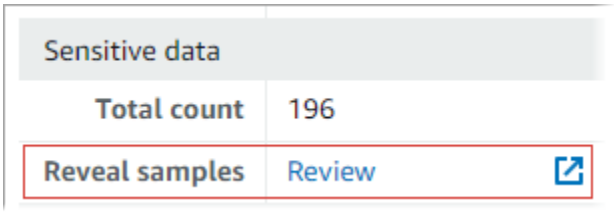
在 Amazon Macie 控制台上执行以下步骤，确定是否有敏感数据样本可用于调查发现。

确定是否有样本可用于调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 调查发现。

3. 在 调查发现页面上，选择该调查发现。详细信息面板会显示调查发现的信息。
4. 在详细信息面板中，滚动至敏感数据部分。然后参阅 显示样本字段。

   如果调查发现有敏感数据样本可用，则字段中会出现 查看链接，如下图所示。



   如果调查发现没有敏感数据样本可用，则 显示样本字段会显示文本，说明原因：

   - 账户不属于组织 – 您无权使用 Macie 访问受影响的 S3 对象。受影响的账户不属于您的组织。或者该账户属于您的组织，但当前未在当前 AWS 区域中为该账户启用 Macie。
   - 分类结果无效 – 该调查发现没有相应的敏感数据发现结果。或者相应的敏感数据发现结果在当前 AWS 区域中不可用、格式错误或已损坏，或者使用了不支持的存储格式。Macie 无法验证要检索的敏感数据的位置。
   - 结果签名无效 – 相应的敏感数据发现结果存储在未经 Macie 签名的 S3 对象中。Macie 无法验证敏感数据发现结果的完整性和真实性。因此，Macie 无法验证要检索的敏感数据的位置。
   - 成员角色权限过于宽松 – 受影响成员账户中 IAM 角色的信任或权限策略不符合 Macie 有关限制该角色访问权限的要求。或者，该角色的信任策略没有为您的组织指定正确的外部 ID。Macie 无法代入该角色来检索敏感数据。
   - 缺少 GetMember 权限-不允许您检索有关您的账户与受影响账户之间关联的信息。Macie 无法确定您是否有权以受影响账户的委派 Macie 管理员身份访问受影响的 S3 对象。
   - 对象超出大小限额 – 受影响 S3 对象的存储大小超过了从该类型文件中检索和显示敏感数据样本的大小限额。
   - 对象不可用 – 受影响的 S3 对象不可用。在 Macie 创建调查发现后，该对象已被重命名、移动或删除，或其内容发生了变化。或者，用于加密该对象的 AWS KMS key 当前被禁用。
   - 结果未签名 – 相应的敏感数据发现结果存储在未签名的 S3 对象中。Macie 无法验证敏感数据发现结果的完整性和真实性。因此，Macie 无法验证要检索的敏感数据的位置。
   - 角色权限过于宽松 – 您的账户配置为通过使用 IAM 角色来检索敏感数据的出现频次，但该角色的信任或权限策略不符合 Macie 限制该角色访问权限的要求。Macie 无法代入该角色来检索敏感数据。
   - 不支持的对象类型 – 受影响的 S3 对象使用了 Macie 不支持用来检索和显示敏感数据样本的文件或存储格式。受影响 S3 对象的 MIME 类型不是 前述列表 的值之一。

如果调查发现的敏感数据发现结果存在问题，则该调查发现的详细结果位置字段中的信息有助于您调查问题。此字段指定了发现结果在 Amazon S3 中的原始路径。要调查有关 IAM 角色的问题，请确保该角色的策略符合 Macie 代入该角色的所有要求。有关详细信息，请参阅 配置 IAM 角色以访问受影响的 S3 对象。

API

要以编程方式确定敏感数据样本是否可用于查找，请使用 Amazon Macie API 的GetSensitiveDataOccurrencesAvailability操作。提交请求时，使用 `findingId` 参数指定调查发现的唯一标识符。要获取此标识符，您可以使用ListFindings操作。

如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行 get-sensitive-data-occurrences-availabil ity 命令并使用`finding-id`参数指定查找结果的唯一标识符。要获取此标识符，可以运行 list-findings 命令。

如果您的请求成功并且有样本可用于调查发现，则您将收到类似于以下内容的输出：

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

如果您的请求成功并且没有样本可用于调查发现，则该 `code` 字段的值为 `UNAVAILABLE`，`reasons` 数组会指定原因。例如：

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

如果调查发现的敏感数据发现结果存在问题，则该调查发现的 `classificationDetails.detailedResultsLocation` 字段中的信息有助于您调查问题。此字段指定了发现结果在 Amazon S3 中的原始路径。要调查有关 IAM 角色的问题，请确保该角色的策略符合 Macie 代入该角色的所有要求。有关详细信息，请参阅 配置 IAM 角色以访问受影响的 S3 对象。

检索和显示调查发现的敏感数据样本

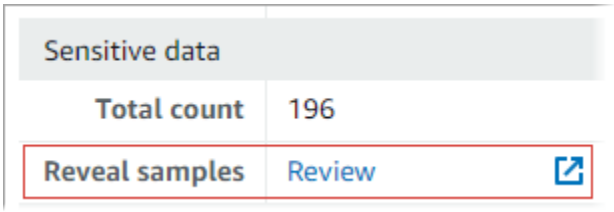
要检索和显示调查发现的敏感数据样本，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台检索和显示敏感数据样本以用于调查发现。

检索和显示调查发现的敏感数据样本

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 调查发现。
3. 在 调查发现页面上，选择该调查发现。详细信息面板会显示调查发现的信息。
4. 在详细信息面板中，滚动至敏感数据部分。然后，在显示样本字段中，选择查看：

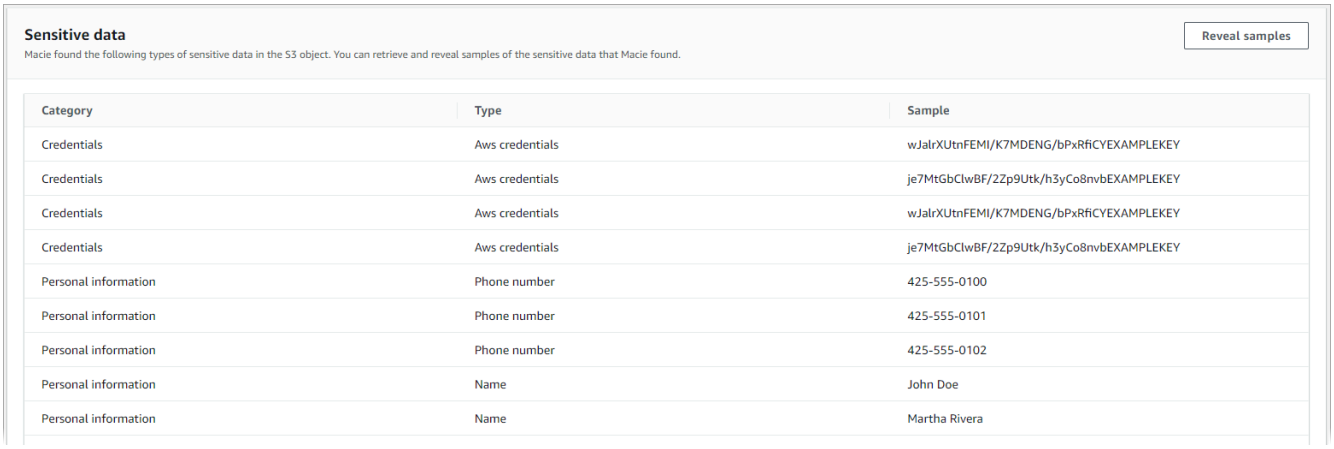


> **Note**
>
> 如果 查看样本字段中未显示 查看链接，则敏感数据样本不可用于调查发现。有关为什么会出现这种情况的信息，请参阅前面的主题。

选择 查看后，Macie 会显示一个页面，其中汇总了调查发现的关键细节。详细信息包括 Macie 在受影响的 S3 对象中发现的敏感数据的类别、类型和出现次数。

5. 在页面的 敏感数据部分，选择 显示样本。然后，Macie 将检索并显示了该调查发现报告的前 1-10 次敏感数据的样本。每个样本都包含敏感数据出现次数的前 1-128 个字符。可能需要几分钟时间才能检索和显示这些样本。

   如果调查发现报告了多种类型的敏感数据，Macie 会检索并显示最多 100 种类型的样本。例如，下图显示了涵盖多个类别和类型的敏感数据（AWS 凭证、美国电话号码和人员姓名）的示例。



样本首先按敏感数据类别进行组织，然后按敏感数据类型进行组织。

API

要以编程方式检索和显示查找结果的敏感数据样本，请使用 Amazon Macie API 的GetSensitiveDataOccurrences操作。提交请求时，使用 `findingId` 参数指定调查发现的唯一标识符。要获取此标识符，您可以使用ListFindings操作。

要使用 AWS Command Line Interface (AWS CLI) 检索和显示敏感数据样本，请运行get-sensitive-data-occurrences命令并使用`finding-id`参数指定查找结果的唯一标识符。例如：

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

其中 *1f1c2d74db5d8caa76859ec52example* 是该调查发现的唯一标识符。要使用获取此标识符 AWS CLI，可以运行 list-findings 命令。

如果您的请求成功，Macie 将开始处理您的请求，您将收到类似于以下内容的输出：

```
{
    "status": "PROCESSING"
}
```

处理您的申请可能需要几分钟时间。几分钟后，再次提交您的申请。

如果 Macie 可以定位、检索和加密敏感数据样本，则 Macie 会在 `sensitiveDataOccurrences` 地图中返回样本。该映射指定了调查发现报告的 1—100 种敏感数据类型，每种类型指定了 1—10 个样本。每个样本都包含调查发现报告的敏感数据的前 1-128 个字符。

在映射中，每个键都是检测到敏感数据的托管式数据标识符的 ID，或检测到敏感数据的自定义数据标识符的名称和唯一标识符。这些值是指定托管数据标识符或自定义数据标识符的样本。例如，以下响应提供了三个人员姓名样本和两个由托管数据标识符（NAME和AWS_CREDENTIALS）检测到的私有访问 AWS 密钥样本。

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

如果您的请求成功但敏感数据样本不可用于调查发现，则您会收到一条 UnprocessableEntityException 消息，说明样本不可用的原因。例如：

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

在前面的示例中，Macie 尝试从受影响的 S3 对象中检索样本，但该对象已不再可用。在 Macie 创建调查发现后，对象的内容发生了变化。

如果您的请求成功，但由于其他类型的错误使 Macie 无法检索和显示调查发现的敏感数据样本，则您会收到类似于以下内容的输出：

```
{
    "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"
}
```

该 `status` 字段的值为 `ERROR`，该 `error` 字段描述了发生的错误。前述主题 中的信息有助您调查错误。

敏感数据位置的 JSON 架构

Amazon Macie 使用标准化 JSON 结构存储有关在 Amazon Simple Storage Service (Amazon S3) 对象中发现的敏感数据的位置信息。这些结构用于敏感数据调查发现和敏感数据发现结果。对于敏感数据调查发现，这些结构是调查发现的 JSON 架构的一部分。要查看完整的 JSON 架构以了解调查发现，请参阅 Amazon Macie API 参考中的调查发现。要了解有关敏感数据发现结果的更多信息，请参阅 存储和保留敏感数据发现结果。

主题

- 敏感数据位置的 JSON 架构概述
- 敏感数据位置的 JSON 架构详细信息和示例

敏感数据位置的 JSON 架构概述

要报告 Amazon Macie 在受影响的 S3 对象中发现的敏感数据的位置，敏感数据调查发现和敏感数据发现结果的 JSON 架构包括一个 `customDataIdentifiers` 对象和一个 `sensitiveData` 对象。该 `customDataIdentifiers` 对象提供有关 Macie 使用自定义数据标识符检测到的数据的详细信息。该 `sensitiveData` 对象提供有关 Macie 使用托管数据标识符检测到的数据的详细信息。

每个 `customDataIdentifiers` 和 `sensitiveData` 对象都包含一个或多个 `detections` 数组：

- 在 `customDataIdentifiers` 对象中，`detections` 数组表示哪些自定义数据标识符检测到数据并得出了调查发现。对于每个自定义数据标识符，该数组还会指示该标识符检测到的数据出现次数。它还可以指示标识符检测到的数据的位置。

- 在 sensitiveData 对象中，detections 数组指示 Macie 使用托管数据标识符检测到的敏感数据的类型。对于每种类型的敏感数据，该数组还会指示数据的出现次数，还可以指示数据的位置。

对于敏感数据调查发现，detections 数组可以包含 1-15 个 occurrences 对象。每个 occurrences 对象都指定 Macie 在何处检测到特定类型的敏感数据的单个事件。

例如，以下 detections 数组表示 Macie 在 CSV 文件中发现的三次敏感数据（美国社会安全号码）的位置。

```
"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"
          }
```

detections 数组中 occurrences 对象的位置和数量因 Macie 在自动敏感数据发现分析周期或敏感数据发现作业运行期间检测到的敏感数据的类别、类型和出现次数而异。对于每个分析周期或作业运

行，Macie 都使用深度优先搜索算法，使用 Macie 在 S3 对象中检测到的 1-15 次敏感数据的位置数据填充结果调查发现。这些事件表明受影响的 S3 存储桶和对象可能包含的敏感数据的类别和类型。

`occurrences` 对象可以包含以下任何结构，具体取决于受影响的 S3 对象的文件类型或存储格式：

- `cells` 数组 – 此数组适用于微软 Excel 工作簿、CSV 文件和 TSV 文件。此数组中的对象指定 Macie 检测到其中存在敏感数据的单元格或字段。
- `lineRanges`数组 – 此数组适用于电子邮件 (EML) 文件以及 CSV、JSON、JSON Lines 和 TSV 文件以外的非二进制文本文件，例如 HTML、TXT 和 XML 文件。此数组中的对象指定 Macie 检测到存在敏感数据的一行或包含范围的行，以及数据在指定行上的位置。

  在某些情况下，`lineRanges` 数组中的对象以另一种类型的数组支持的文件类型或存储格式指定敏感数据检测的位置。这些情况是：在其他结构化文件的非结构化部分中检测到的情况，例如文件中的注释；在 Macie 分析为纯文本的格式错误中检测到的情况；以及 Macie 在 CSV 或 TSV 文件中检测到包含敏感数据的一个或多个列名。
- `offsetRanges` 数组 – 此数组保留供将来使用。如果存在此数组，则其值为空。
- `pages` 数组 – 此数组适用于 Adobe 便携式文档格式 (PDF) 文件。此数组中的对象指定 Macie 检测到其中存在敏感数据的页面。
- `records` 数组 – 此数组适用于 Apache Avro 对象容器、Apache Parquet 文件、JSON 文件和 JSON Lines 文件。对于 Avro 对象容器和 Parquet 文件，此数组中的对象指定记录索引和 Macie 检测到存在敏感数据的记录中字段的路径。对于 JSON 和 JSON Lines 文件，此数组中的对象指定 Macie 检测到其中存在敏感数据的字段或数组的路径。对于 JSON Lines 文件，它还指定包含数据的行的索引。

这些数组的内容因受影响的 S3 对象的文件类型或存储格式及其内容而异。

敏感数据位置的 JSON 架构详细信息和示例

Amazon Macie 会定制 JSON 结构的内容，以指示在特定类型的文件和内容中检测到敏感数据的位置。以下主题解释并提供了这些结构的示例。

主题

有关敏感数据调查发现中可以包含的 JSON 结构的完整列表，请参阅 Amazon Macie API 参考中的调查发现。

Cells 数组

适用于：微软 Excel 工作簿、CSV 文件和 TSV 文件

在 `cells` 数组中，`Cell` 对象指定 Macie 检测到其中存在敏感数据的单元格或字段。下表描述了 `Cell` 对象中每个字段的用途。

字段	类型	描述
`cellReference`	字符串	包含该事件的单元格的位置，作为绝对单元格引用。此字段仅适用于 Excel 工作簿。对于 CSV 和 TSV 文件，此值为空。
`column`	整数	包含该事件的列的列编号。对于 Excel 工作簿，此值与列标识符的字母字符相关联，例如，1 用于 A 列，2 用于 B 列，依此类推。
`columnName`	字符串	包含该事件的列名称（如果有）。
`row`	整数	包含该事件的行的行号。

以下示例显示了一个 `Cell` 对象的结构，该对象指定 Macie 在 CSV 文件中检测到的敏感数据出现的位置。

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
```

```
]
```

在前面的示例中，调查发现表明 Macie 在文件第三列（名为 SSN）第五行的字段中检测到了敏感数据。

以下示例显示了一个 `Cell` 对象的结构，该对象指定 Macie 在 Excel 工作簿中检测到的敏感数据出现的位置。

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

在前面的示例中，调查发现表明 Macie 在工作簿中名为 Sheet2 的工作表中检测到了敏感数据。在该工作表中，Macie 在第三列（C 列，名为 SSN）第五行的单元格中检测到敏感数据。

LineRanges 数组

适用于：电子邮件 (EML) 文件以及 CSV、JSON、JSON Lines 和 TSV 文件以外的非二进制文本文件，例如 HTML、TXT 和 XML 文件

在 `lineRanges` 数组中，`Range` 对象指定 Macie 检测到存在敏感数据的一行或包含范围的行，以及数据在指定行上的位置。

对于 `occurrences` 对象中其他类型的数组支持的文件类型，此对象通常为空。例外情况是：

- 其他结构化文件的非结构化部分中的数据，例如文件中的注释。
- 格式错误的文件中的数据，Macie 将其分析为纯文本。
- 包含一个或多个列名的 CSV 或 TSV 文件，Macie 在其中检测到敏感数据。

下表描述了 `lineRanges` 数组的 `Range` 对象中每个字段的用途。

字段	类型	描述
end	整数	从文件开头到事件结尾的行数。

字段	类型	描述
start	整数	从文件开头到事件开头的行数。
startColumn	整数	从包含事件的内容的第一行开头（start）到事件开头的字符数，包括空格并从 1 开始计数。

以下示例显示了一个 Range 对象的结构，该对象指定 Macie 在 TXT 文件中的单行上检测到的敏感数据出现的位置。

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

在前面的示例中，调查发现表明 Macie 检测到文件的第一行中完全出现了敏感数据（邮寄地址）。出现的第一个字符是从该行开头开始的 119 个字符（含空格）。

以下示例显示了一个 Range 对象的结构，该对象指定了 TXT 文件中跨越多行的敏感数据出现的位置。

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

在前面的示例中，调查发现表明 Macie 检测到存在跨越文件第 51 行到第 54 行的敏感数据（邮寄地址）。事件的第一个字符是文件第 51 行的第一个字符。

Page 数组

适用于：Adobe 便携式文档格式 (PDF) 文件

在 pages 数组中，Page 对象指定 Macie 检测到其中存在敏感数据的页面。对象包含一个 pageNumber 字段。该 pageNumber 字段存储一个整数，用于指定包含该事件的页面的页码。

以下示例显示了一个 Page 对象的结构，该对象指定 Macie 在 PDF 文件中检测到的敏感数据出现的位置。

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

在前面的示例中，调查发现表明该文件的第 10 页包含该事件。

记录数组

适用于：Apache Avro 对象容器、Apache Parquet 文件、JSON 文件和 JSON Lines 文件

对于 Avro 对象容器或 Parquet 文件，records 数组中的 Record 对象指定记录索引和 Macie 检测到存在敏感数据的记录中字段的路径。对于 JSON 和 JSON Lines 文件，Record 对象指定 Macie 检测到其中存在敏感数据的字段或数组的路径。对于 JSON Lines 文件，它还会指定包含该事件的行的索引。

下表描述了 Record 对象中每个字段的用途。

字段	类型	描述
jsonPath	字符串	以 JSONPath 表达式的形式指向该事件的路径。 对于 Avro 对象容器或 Parquet 文件，这是记录 (recordIndex) 中包含具体值的字段的路径。对于 JSON 或 JSON Lines 文件，这是包含该事件的字段或数组的路径。如果数据是数组中的一个值，则路径还会指示哪个值包含该事件。

字段	类型	描述
		如果 Macie 在路径中任何元素的名称中检测到敏感数据，则 Macie 会从 Record 对象中省略该 jsonPath 字段。如果路径元素的名称超过 240 个字符，Macie 会通过删除名称开头的字符来截断该名称。如果生成的完整路径超过 250 个字符，Macie 还会从路径中的第一个元素开始截断路径，直到路径包含 250 个或更少的字符。
recordIndex	整数	对于 Avro 对象容器或 Parquet 文件，包含该事件的记录的索引，从 0 开始。对于 JSON Lines 文件，从 0 开始表示包含该事件的行的行索引。此值始终 0 适用于 JSON 文件。

以下示例显示了一个 Record 对象的结构，该对象指定 Macie 在 Parquet 文件中检测到的敏感数据出现的位置。

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

在前面的示例中，调查发现表明 Macie 在索引 7663（记录号 7664）的记录中检测到了敏感数据。在该记录中，Macie 在名为 abcdefghijklmnopqrstuvwxyz 的字段中检测到了敏感数据。记录中该字段的完整 JSON 路径为 $.abcdefghijklmnopqrstuvwxyz。该字段是根（外层级别）对象的直接后代。

以下示例还显示了 Macie 在 Parquet 文件中检测到的敏感数据出现时的 Record 对象结构。但是，在此示例中，Macie 截断了包含该匹配项的字段的名称，因为该名称超出了字符限制。

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

在前面的示例中，该字段是根（外层级别）对象的直接后代。

在以下示例中，同样对于 Macie 在 Parquet 文件中检测到的敏感数据，Macie 截断了包含该事件的字段的完整路径。完整路径超过字符限制。

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

在前面的示例中，调查发现表明 Macie 在索引 2335（记录号 2336）的记录中检测到了敏感数据。在该记录中，Macie 在名为 abcdefghijklmnopqrstuvwxyz 的字段中检测到了敏感数据。记录中该字段的完整 JSON 路径为：

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

以下示例显示了一个 Record 对象的结构，该对象指定 Macie 在 JSON 文件中检测到的敏感数据出现的位置。在此示例中，出现的是数组中的特定值。

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

在前面的示例中，调查发现表明 Macie 在名为 key 的数组的第二个值中检测到了敏感数据。该数组是名为 access 的对象的子项。

以下示例显示了一个 Record 对象的结构，该对象指定 Macie 在 JSON Lines 文件中检测到的敏感数据出现的位置。

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

在前面的示例中，调查发现表明 Macie 在文件中的第三个值（行）中检测到了敏感数据。在该行中，事件位于名为 key 的字段中，该字段是名为 access 的对象的子项。

抑制 Amazon Macie 调查发现

为了简化对调查发现的分析，您可以创建和使用抑制规则。抑制规则是一组基于属性的筛选标准，用于定义您希望 Amazon Macie 自动存档调查发现的情况。如果您已经查看了一类调查发现并且不想再次收到有关这些发现的通知，则抑制规则会很有用。

例如，您可以决定允许 S3 存储桶包含邮寄地址，前提是这些存储桶不允许公开访问，并且它们会自动使用特定的 AWS KMS key 加密新对象。在这种情况下，您可以创建一个抑制规则，为以下字段指定筛选标准：敏感数据检测类型、S3 存储桶公共访问权限和 S3 存储桶加密 KMS 密钥 ID。该规则会抑制未来符合筛选标准的调查发现。

如果您使用抑制规则抑制调查发现，Macie 会继续针对后续出现的敏感数据以及符合该规则标准的潜在策略违规行为生成调查发现。但是，Macie 会自动将调查发现的状态更改为已存档。这意味着默认情况下，调查发现不会出现在 Amazon Macie 主机上，但它们会一直存在于 Macie 中，直到过期。Macie 会将您的调查发现存储 90 天。

此外，Macie 不会将抑制的调查发现作为事件发布给 Amazon EventBridge 或 AWS Security Hub。但是，Macie 会继续创建和存储与您抑制的敏感数据调查发现相关的敏感数据发现结果。这有助于确保您拥有敏感数据调查发现的不可变历史记录，用于您执行的数据隐私和保护审计或调查。

> **Note**
>
> 如果您的账户属于集中管理多个 Macie 账户的组织，则抑制规则对您的账户的使用方式可能会有所不同。这取决于您想要抑制的调查发现的类别，以及您拥有的是 Macie 管理员账户还是成员账户：
>
> - 策略调查发现 - 只有 Macie 管理员才能抑制组织账户的政策调查发现。
>
> 如果您拥有 Macie 管理员账户并创建了抑制规则，则除非您将该规则配置为排除特定账户，否则 Macie 会将该规则应用于组织中所有账户的策略调查发现。如果您拥有 Macie 成员账户，并且想要抑制账户的策略调查发现，请联系您的 Macie 管理员。
> - 敏感数据调查发现 – Macie 管理员和个人成员可以抑制其敏感数据发现作业产生的敏感数据调查发现。Macie 管理员还可以抑制 Macie 在为组织执行自动敏感数据发现时生成的调查发现。
>
> 只有创建敏感数据发现作业的账户才能抑制或以其他方式访问该作业产生的敏感数据调查发现。只有组织的 Macie 管理员账户才能抑制或以其他方式访问自动敏感数据发现为组织中的账户生成的调查发现。
>
> 有关管理员和成员可以执行的任务的更多信息，请参阅了解 Amazon Macie 管理员和成员账户之间的关系。

要创建和管理抑制规则，您可以使用 Amazon Macie 控制台或 Amazon Macie API。以下主题说明如何使用。对于 API，主题包括如何使用 AWS Command Line Interface(AWS CLI) 执行这些任务的示例。您也可以使用当前版本的其他 AWS 命令行工具或 AWS SDK，或者直接向 Macie 发送 HTTPS 请求。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

主题

创建抑制规则

在创建抑制规则之前，请务必注意，您无法恢复（取消存档）使用抑制规则抑制的调查发现。但是，您可以在 Amazon Macie 控制台上查看抑制的调查发现，也可以使用 Amazon Macie API 访问抑制的调查发现。

创建抑制规则时，需要指定筛选标准、名称以及该规则的描述（可选）。您可以使用 Amazon Macie 控制台或 Amazon Macie API 创建抑制规则。

Console

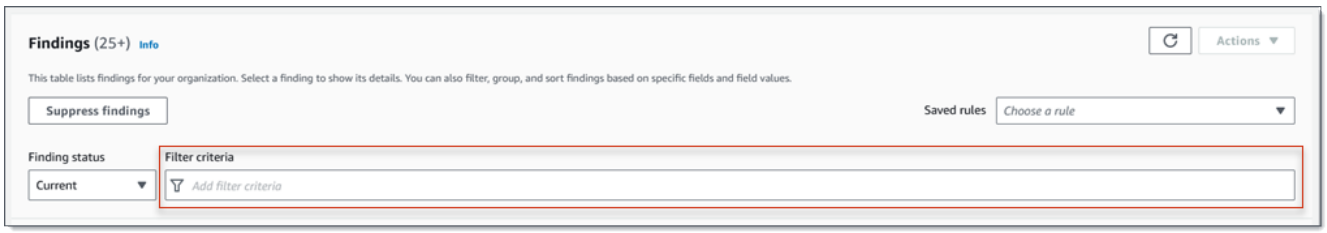
按照以下步骤，使用 Amazon Macie 控制台创建抑制规则。

创建禁止规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。

> **Tip**
>
> 要使用现有的抑制或筛选规则作为起点，请从已保存的规则列表中选择该规则。
> 您还可以通过首先透视和深入研究预定义逻辑组的调查发现来简化规则的创建。如果您这样做，Macie 会自动创建并应用适当的筛选条件，这可能是创建规则的有用起点。据此，请在导航窗格选择按存储桶、按类型或 按作业（调查发现下），然后选择表内的项目。在详细信息面板中，为字段选择要转置的链接。

3. 在筛选标准框中，添加筛选条件，以指定您希望规则抑制的调查发现的属性。



要了解如何添加筛选条件，请参阅创建筛选条件并将其应用于调查发现。

4. 在添加完规则的筛选条件后，请选择抑制调查发现。
5. 在抑制规则下，输入规则的名称和描述（可选）。
6. 选择 Save（保存）。

API

要以编程方式创建抑制规则，请使用 Amazon Macie API 的 CreateFindingsFilter 操作并为所需参数指定相应的值：

- 对于 `action` 参数，请指定 `ARCHIVE` 以确保 Macie 抑制符合规则标准的调查发现。
- 对于 `criterion` 参数，请指定定义规则筛选条件的条件映射。

  在映射中，每项条件都应为该字段指定一个字段、一个运算符以及一个或多个值。值的类型和数量取决于您选择的字段和运算符。有关可在条件中使用的字段、运算符和值类型的信息，请参阅用于筛选调查发现的字段、在条件中使用运算符和为字段指定值。

要使用 AWS CLI 创建抑制规则，请运行 create-findings-filter 命令并为所需参数指定适当的值。以下示例创建了一个抑制规则，该规则返回当前 AWS 区域 中的所有敏感数据调查发现，并报告 S3 对象中出现的邮件地址（没有其他类型的敏感数据）。

此示例针对 Linux、macOS 或 Unix 进行格式化，并使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

其中：

- *my_suppression_rule* 是该规则的自定义名称。
- `criterion` 是该规则的筛选条件映射：
  - *classificationDetails.result.sensitiveData.detections.type* 是 敏感数据检测类型字段的 JSON 名称。

- *eqExactMatch* 指定等于精确匹配运算符。
- *##* 是 敏感数据检测类型字段的枚举值。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

其中 `arn` 是已创建的抑制规则的 Amazon 资源名称（ARN），`id` 也是该规则的唯一标识符。

有关筛选标准的其他示例，请参阅 使用 Amazon Macie API 以编程方式筛选调查发现。

查看抑制结果

默认情况下，Macie 不会在 Amazon Macie 主机上显示抑制的调查发现。但是，您可以通过更改筛选条件设置在控制台上查看这些调查发现。

在控制台上查看抑制的调查发现

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。调查发现页面显示 Macie 于过去 90 天内在当前的 AWS 区域 为您的账户创建或更新的调查发现。默认情况下，这不包括被抑制规则隐藏的调查发现。
3. 对于调查发现状态，请执行下面的一项操作：
   - 要仅显示抑制的调查发现，请选择已存档。
   - 要同时显示抑制和未抑制的调查发现，请选择全部。
   - 要再次隐藏抑制的调查发现，请选择当前。

您也可以使用 Amazon Macie API 访问抑制的调查发现。要检索抑制的调查发现列表，请使用 ListFindings 操作并包括为 `archived` 字段指定 `true` 的筛选条件。有关如何使用 AWS CLI 执行此操作的示例，请参阅 以编程方式筛选调查发现。然后，要检索一个或多个抑制的调查发现的详细信息，请使用 GetFindings 操作并为要检索的每个调查发现指定唯一标识符。

更改抑制规则

您可以随时使用 Amazon Macie 主机或 Amazon Macie API 更改抑制规则的设置。您还可以为规则分配和管理标签。

标签是您定义并分配给某些类型的 AWS 资源的标记。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。要了解更多信息，请参阅 为 Amazon Macie 资源添加标签。

Console

按照以下步骤，使用 Amazon Macie 控制台对现有抑制规则的设置进行更改。

创建抑制规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。
3. 在已保存的规则列表中，选择要更改的抑制规则旁边的编辑图标 ( )。
4. 执行以下任一操作：
   - 要更改规则的标准，请使用筛选标准框输入条件，指定您希望规则抑制的调查发现的属性。要了解如何操作，请参阅创建筛选条件并将其应用于调查发现。
   - 要更改规则的名称，请在抑制规则下的名称框中输入新名称。
   - 要更改规则的描述，请在抑制规则下的描述框中输入新的描述。
   - 要为规则分配、查看或编辑标签，请选择抑制规则下的管理标签。然后根据需要查看并更改标签。一个规则可具有最多 50 个标签。
5. 完成更改后，选择 Save (保存)。

API

要以编程方式更改抑制规则，请使用 Amazon Macie API 的 UpdateFindingsFilter 操作。提交请求时，请使用支持的参数为要更改的每个设置指定一个新值。

对于 `id` 参数，请为待更改规则指定唯一标识符。您可以使用 ListFindingsFilter 操作来检索账户的抑制和筛选规则列表，从而获取此标识符。如果您使用的是 AWS CLI，请运行 list-findings-filters 命令来检索此列表。

要使用 AWS CLI 更改抑制规则，请运行 update-findings-filter 命令并使用支持的参数为要更改的每个设置指定新值。例如，以下命令会更改现有抑制规则的名称。

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

其中：

- *8a3c5608-aa2f-4940-b347-d1451example* 是该规则的唯一标识符。
- *mailing_addresses_only* 是该规则的新名称。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

其中 arn 是已更改规则的 Amazon 资源名称（ARN），id 是该规则的唯一标识符。

同样，以下示例通过将 action 参数的值从 NOOP 更改为 ARCHIVE，将筛选规则转换为抑制规则。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

其中：

- *8a1c3508-aa2f-4940-b347-d1451example* 是该规则的唯一标识符。
- *ARCHIVE* 是 Macie 对符合规则标准的调查发现执行的新操作——抑制调查发现。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

其中 arn 是已更改规则的 Amazon 资源名称（ARN），id 是该规则的唯一标识符。

删除抑制规则

您可以随时使用 Amazon Macie 主机或 Amazon Macie API 删除抑制规则。如果您删除抑制规则，Macie 将停止抑制符合该规则标准且未被其他规则抑制的新调查发现和后续出现的调查发现。但请注意，Macie 可能会继续抑制其目前正在处理且符合规则标准的调查发现。

删除抑制规则后，符合该规则标准的新出现和后续出现的调查发现的状态为当前（未存档）。这意味着它们默认显示在 Amazon Macie 主机上。此外，Macie 还会将这些调查发现作为事件发布到 Amazon EventBridge。根据您账户的发布设置，Macie 还会将调查发现发布到 AWS Security Hub。

Console

按照以下步骤使用 Amazon Macie 控制台删除抑制规则。

删除抑制规则

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 在导航窗格中，选择 Findings (结果)。
3. 在已保存的规则列表中，选择要删除的抑制规则旁边的编辑图标 ()。
4. 在抑制规则下，选择删除。

API

要以编程方式删除抑制规则，请使用 Amazon Macie API 的 DeleteFindingsFilter 操作。为 id 参数指定要删除的抑制规则的唯一标识符。您可以使用 ListFindingsFilter 操作来检索账户的抑制和筛选规则列表，从而获取此标识符。如果您使用的是 AWS CLI，请运行 list-findings-filters 命令来检索此列表。

要使用 AWS CLI 删除抑制规则，请运行 delete-findings-filter 命令。例如：

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

其中 *8a3c5608-aa2f-4940-b347-d1451example* 是要删除的抑制规则的唯一标识符。

如果命令运行成功，Macie 会返回一个空 HTTP 200 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

Amazon Macie 调查发现的严重性评分

当 Amazon Macie 生成策略或敏感数据调查发现时，它会自动为该调查发现指定严重性。调查发现的严重性反映了调查发现的主要特征，可以帮助您评测调查发现并确定其优先级。调查发现的严重性并不意味着或以其他方式表明受影响的资源可能对您的组织具有的关键性或重要性。

对于策略调查发现，严重性取决于您的 Amazon Simple Storage Service (Amazon S3) 数据安全或隐私可能存在的问题的性质。对于敏感数据调查发现，严重性基于 Macie 在 S3 对象中发现的敏感数据的性质和出现次数。

在 Macie 中，调查发现的严重性有两种表现方式。

严重性级别

这是严重程度的定性表示。严重程度从表示最不严重的 Low 到表示最严重的 High 不等。

严重级别直接显示在 Amazon Macie 控制台上。它们还以 Macie 控制台上调查发现的 JSON 表示形式、Amazon Macie API 以及与敏感数据调查发现相关联的敏感数据调查发现提供。严重性级别还包含在 Macie 发布到 Amazon EventBridge 的调查发现事件以及 Macie 向 AWS Security Hub 发布的调查发现中。

严重性分数

这是严重程度的数字表示。严重性分数介于 1 到 3 之间，并直接映射到严重性级别：

严重性分数	严重性级别
1	低
2	中
3	高

严重性分数不会直接显示在 Amazon Macie 主机上。但是，它们以 Macie 控制台上调查发现的 JSON 表示形式、Amazon Macie API 以及与敏感数据发现结果相关的敏感数据调查发现提供。在 Macie 发布到 Amazon EventBridge 的调查发现事件中，也会包含严重性分数。它们未包含在 Macie 发布到 AWS Security Hub 的调查发现中。

本节中的主题说明了 Macie 如何确定策略调查发现和敏感数据调查发现的严重性。

主题

策略调查发现的严重性评分

策略调查发现的严重性基于 S3 存储桶安全或隐私方面的潜在问题的性质。下表列出了 Macie 为每种类型的策略调查发现分配的严重性级别。有关每种类型的说明，请参阅 调查发现的类型。

结果类型	严重性级别
Policy:IAMUser/S3BlockPublicAccessDisabled	高
Policy:IAMUser/S3BucketEncryptionDisabled	低
Policy:IAMUser/S3BucketPublic	高
Policy:IAMUser/S3BucketReplicatedExternally	高
Policy:IAMUser/S3BucketSharedExternally	高
Policy:IAMUser/S3BucketSharedWithCloudFront	中

策略调查发现的严重性不会根据调查发现的发生次数而变化。

敏感数据调查发现的严重性分数

敏感数据调查发现的严重性基于 Macie 在 S3 对象中发现的敏感数据的性质和出现次数。以下主题说明了 Macie 如何确定每种敏感数据调查发现的严重性：

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

有关 Macie 可以在敏感数据调查发现中检测和报告的敏感数据类型的详细信息，请参阅使用托管数据标识符和构建自定义数据标识符。

SensitiveData:S3Object/Credentials

SensitiveData:S3Object/Credentials 的调查发现表明 S3 对象包含敏感的凭证数据。对于此类调查发现，Macie 会根据 Macie 在对象中找到的凭证数据的类型和出现次数来确定严重性。

下表显示了 Macie 为报告 S3 对象中出现凭证数据的调查发现分配的严重性级别。

敏感数据类型	1 次出现	2—99 次出现	100 或更多次出现
AWS秘密访问密钥	高	高	高
Google Cloud API 密钥	高	高	高
HTTP 基本授权标头	高	高	高
JSON Web 令牌 (JWT)	高	高	高
OpenSSH 私有密钥	高	高	高
PGP 私有密钥	高	高	高
公有密钥加密标准 (PKCS, Public-Key Cryptography Standard) 私有密钥	高	高	高
PuTTY 私有密钥	高	高	高
Stripe API 密钥	高	高	高

SensitiveData:S3Object/CustomIdentifier

SensitiveData:S3Object/CustomIdentifier 的调查发现表明 S3 对象包含的文本与一个或多个自定义数据标识符的检测标准相匹配。该对象可能包含多种类型的敏感数据。

默认情况下，Macie 会为此类调查发现分配中等严重性级别，如果 S3 对象包含至少一次符合至少一个自定义数据标识符的检测标准的文本，则 Macie 会自动为该调查发现分配中等严重性级别。调查发现的严重性不会根据符合自定义数据标识符标准的文本出现次数而变化。

但是，如果您为生成调查发现的自定义数据标识符定义了自定义严重性设置，则此类调查发现的严重性可能会有所不同。如果是这样的话，Macie 会按以下方式确定严重性：

- 如果 S3 对象包含的文本仅匹配一个自定义数据标识符的检测标准，则 Macie 会根据该标识符的严重性设置来确定调查发现的严重性。
- 如果 S3 对象包含的文本与多个自定义数据标识符的检测标准相匹配，则 Macie 会通过评测每个自定义数据标识符的严重性设置、确定其中哪些设置产生的严重性最高，然后将该最高严重性分配给调查发现，从而确定调查发现的严重性。

要查看自定义数据标识符的严重性设置，请在 Amazon Macie 控制台的导航窗格中选择自定义数据标识符。然后选择自定义数据标识符的名称。严重性部分显示了设置。有关更多信息，请参阅为自定义数据标识符定义调查发现严重性设置。

SensitiveData:S3Object/Financial

SensitiveData:S3Object/Financial 的调查发现表明 S3 对象包含敏感的财务信息。对于此类调查发现，Macie 根据 Macie 在对象中发现的财务信息的类型和出现次数来确定严重性。

下表显示了 Macie 为报告 S3 对象中出现财务信息的调查发现分配的严重性级别。

敏感数据类型	1 次出现	2—99 次出现	100 或更多次出现
银行账号 [1]	高	高	高
信用卡到期日期	低	中	高
信用卡磁条数据	高	高	高
信用卡号 [2]	高	高	高
信用卡验证码	中	高	高

1. 任何类型的银行账号（基本银行账号 (BBAN)、国际银行账号 (IBAN) 或加拿大或美国银行账号）的严重程度都相同。
2. 对于靠近或不靠近关键字的信用卡号，严重级别相同。

如果某项调查发现报告对象中存在多种类型的财务信息，则 Macie 会通过计算 Macie 发现的每类财务信息的严重性、确定哪种类型的严重性最高，并将该最高严重性分配给调查发现来确定该调查发现的严重性。例如，如果 Macie 在对象中检测到 10 个信用卡到期日期（中等严重性级别）和 10 个信用卡号（高严重性级别），则 Macie 会为调查发现分配高严重性级别。

SensitiveData:S3Object/Personal

SensitiveData:S3Object/Personal 的调查发现表明 S3 对象包含敏感的个人信息——个人健康信息 (PHI)、个人身份信息（PII）或两者的组合。对于此类调查发现，Macie 根据 Macie 在对象中发现的个人信息的类型和出现次数来确定严重性。

下表显示了 Macie 为报告 S3 对象中出现的 PHI 的敏感数据调查发现分配的严重性级别。

敏感数据类型	1 次出现	2—99 次出现	100 或更多次出现
毒品管理局 (DEA) 注册号	高	高	高
健康保险索赔编号 (HICN)	高	高	高
健康保险或医疗识别号	高	高	高
医疗保健通用程序编码系统 (HCPCS) 代码	高	高	高
国家药品编码 (NDC)	高	高	高
国家提供商识别码 (NPI)	高	高	高
唯一设备标识符 (UDI)	低	中	高

下表显示了 Macie 为报告 S3 对象中出现的 PII 的敏感数据调查发现分配的严重性级别。

敏感数据类型	1 次出现	2—99 次出现	100 或更多次出现
出生日期	低	中	高
驾驶执照识别号	低	中	高
选民名册编号	高	高	高
全名	低	中	高
全球定位系统 (GPS) 坐标	低	中	中
HTTP cookie	低	中	高
邮寄地址	低	中	高
身份证号码	高	高	高
国民保险号码 (NINO)	高	高	高
护照编号	中	高	高
永久居留号码	高	高	高
电话号码	低	中	高
社会保险号码 (SIN)	高	高	高
社会保障号码（SSN）	高	高	高
纳税人识别号或参考号	高	高	高
车辆识别号码 (VIN)	低	低	中

如果某项发现结果报告对象中存在多种类型的 PHI、PII，或者同时报告了 PHI 和 PII，则 Macie 会通过计算每种类型的严重性、确定哪种类型产生的严重性最高，并将该最高严重性分配给调查发现来确定该发现结果的严重性。

例如，如果 Macie 在对象中检测到 10 个全名（中等严重性级别）和 5 个护照号码（高严重性级别），则 Macie 会为调查发现分配高严重性级别。同样，如果 Macie 在对象中检测到 10 个全名（中等严重级别）和 10 个健康保险标识号（高严重性级别），则 Macie 会为调查发现分配高严重性级别。

SensitiveData:S3Object/Multiple

SensitiveData:S3Object/Multiple 调查发现表明 S3 对象包含跨越多个敏感数据类别的数据，即符合一个或多个自定义数据标识符检测标准的凭证数据、财务信息、个人信息或文本的任意组合。

对于此类调查发现，Macie 通过计算 Macie 发现的每类敏感数据的严重性（如前面的主题所示）、确定哪种类型的严重性最高，然后为调查发现指定最高严重性来确定严重性。

例如，如果 Macie 在对象中检测到 10 个全名（中等严重性级别）和 10 个AWS秘密访问密钥（高严重性级别），则 Macie 会为调查发现分配高严重性级别。

监控和处理 Amazon Macie 调查发现

为了支持与其他应用程序、服务和系统（例如监控或事件管理系统）集成，Amazon Macie 会自动将调查发现作为事件发布到 Amazon EventBridge。要对组织的安全状况进行更多、更广泛的分析，您也可以将调查发现发布到 AWS Security Hub。

Amazon EventBridge

Amazon EventBridge（以前称为 Amazon CloudWatch Events）是一种无服务器事件总线服务，可提供来自应用程序和服务的实时数据流，并将该数据路由到诸如 AWS Lambda 函数、Amazon Simple Notification Service 主题和 Amazon Kinesis 流等目标。借助 EventBridge，您可以自动监控和处理某些类型的事件，包括 Macie 为调查发现发布的事件。要了解有关 EventBridge 的更多信息，请参阅 Amazon EventBridge 用户指南。

如果您将 AWS 用户通知服务与 Macie 集成，您还可以使用 EventBridge 事件自动生成有关 Macie 为调查发现发布的事件的通知。通过用户通知服务，您可以创建自定义规则并配置传送通道以接收有关感兴趣的 EventBridge 事件的通知。交付通道包括电子邮件、AWS Chatbot 聊天通知和 AWS Console Mobile Application 推送通知。您还可以在 AWS Management Console 的中心位置查看通知。要了解有关用户通知服务的更多信息，请参阅 AWS 用户通知服务用户指南。

AWS Security Hub

AWS Security Hub 是一项安全服务，可让您在整个 AWS 环境中全面查看安全状态。它从 AWS 服务 和支持的 AWS Partner Network 安全解决方案中收集安全数据，并帮助您检查所在环境是否符合安全行业标准和最佳实践。它还可以帮助您分析安全趋势并确定最高优先级的安全问题。借助 Security Hub，您可以查看 Macie 调查发现，以此作为对组织安全状况进行更广泛分析的一部分。您还可以聚合来自多个 AWS 区域的调查发现，并监控和处理来自单个区域的聚合调查发现数据。要了解有关 Security Hub 的更多信息，请参阅 AWS Security Hub 用户指南。

当 Macie 创建调查发现时，它会自动将该调查发现作为新事件发布到 EventBridge。根据您为账户选择的发布设置，Macie 还可以将调查发现发布到 Security Hub。Macie 在处理完调查发现后会立即发布每个新的调查发现。如果 Macie 检测到后续出现现有策略调查发现，它会针对该调查发现发布对现有 EventBridge 事件的更新。根据您的发布设置，Macie 还可以将更新发布到 Security Hub。Macie 使用您在账户的发布设置中指定的发布频率定期发布这些更新。

主题

- Amazon Macie 与 AWS Security Hub 集成
- Amazon Macie 与 AWS 用户通知服务集成
- 用于 Amazon Macie 调查发现的 Amazon EventBridge 事件架构

为 Amazon Macie 调查发现配置发布设置

为了支持与其他应用程序、服务和系统的集成，Amazon Macie 会自动将政策调查结果和敏感数据调查结果 EventBridge 作为事件发布给亚马逊。有关如何使用 EventBridge 来监控和处理结果的信息，请参阅Amazon Macie与 Amazon EventBridge 集成。

您可以使用在账户发布设置中指定的目标选项， AWS Security Hub 将 Macie 配置为自动向其发布搜索结果。您可通过这些选项，将 Macie 配置为仅向 Security Hub 发布策略调查发现、仅敏感数据调查发现，或策略和敏感数据调查发现。您也可以将 Macie 配置为停止将任何调查发现发布至 Security Hub。有关如何使用 Security Hub 监控和处理调查发现的信息，请参阅 Amazon Macie 与 AWS Security Hub 集成。

对于策略调查发现，Macie 向其他 AWS 服务 发布调查发现的时间，取决于此调查发现是否为新发现和您为账户指定的发布频率。敏感数据调查发现为实时发布：Macie 在处理完敏感数据调查发现后立即发布敏感数据调查发现。与策略调查发现不同的事，Macie 将所有敏感数据调查发现视为新调查发现（唯一）。

请注意，Macie 不会发布按隐藏规则自动存档的策略或敏感数据调查发现。换句话说，Macie 不会向其他 AWS 服务发布隐藏调查发现。

主题

- 为调查发现选择发布目标
- 确定调查发现发布频率
- 更改调查发现发布频率

为调查发现选择发布目标

除了亚马逊之外，您还可以将 Amazon Macie 配置为 AWS Security Hub 自动发布策略和敏感数据调查结果。 EventBridge默认情况下，Macie 仅向 Security Hub 发布新的和更新的策略调查发现。若要更改或扩展默认配置，请调整您账户的发布目标设置。

调整目标设置时，您可以选择希望 Macie 发布到 Security Hub 的发现结果类别，仅限策略发现结果，仅限敏感数据发现结果，或者同时选择策略和敏感数据查找结果。您也可以选择停止将任何类别的调查发现发布至 Security Hub。

如果您更改了目的设置，则所做的更改仅适用于当前 AWS 区域。如果您是组织的 Macie 管理员，则更改仅适用于您的账户。它不适用于任何关联成员账户。有关更多信息，请参阅管理多个 账户。

为调查发现选择发布目的地

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Settings（设置）。
3. 在 发布调查发现 部分的 目标下，从以下选项中进行选择：

   - 将策略调查结果发布到 Security Hub — 选中此复选框可开始自动将新的和更新的策略结果发布到 Security Hub。要停止向 Security Hub 发布最新策略结果，请清除此复选框。

     如果您选中此复选框并且已有策略发现，则 Macie 不会自动将其发布到 Security Hub。相反，Macie 仅发布在您保存更改后创建或更新的政策调查结果。
   - 将敏感数据发现发布到 Security Hub — 选中此复选框可开始自动将新的敏感数据发现发布到 Security Hub。要停止向 Security Hub 发布新的敏感数据发现，请清除此复选框。

     如果您选中此复选框并且已发现敏感数据，则 Macie 不会自动将其发布到 Security Hub。相反，Macie 仅发布在您保存更改后创建的敏感数据发现。
4. 选择保存。

如果您选择将任何类别的调查结果发布到 Security Hub，请确保同时在当前区域中启用 Security Hub，并将其配置为接受 Macie 的调查结果。否则，您将无法在 Security Hub 中访问调查发现。要了解如何在 Security Hub 中接收调查发现，请参阅AWS Security Hub 用户指南中的管理产品集成。

确定调查发现发布频率

Amazon Macie 的每个调查发现都有唯一的标识符。Macie 使用此标识符确定何时向其他 AWS 服务发布调查发现：

- 新调查发现 – 当 Macie 创建新策略或敏感数据调查发现时，它会在处理调查发现的过程中为此调查发现分配唯一的标识符。在 Macie 完成对调查结果的处理后，它会立即将调查结果作为新的亚马逊 EventBridge 活动发布。根据您账户的发布设置，Macie 还会在 AWS Security Hub中以新调查发现的形式发布调查发现。

- 更新的调查发现-当 Macie 检测到现有策略调查发现的后续事件时，它会通过添加有关后续事件的详细信息并增加发生次数，以更新现有调查发现。Macie 还会发布现有 EventBridge活动的这些更新，并根据您账户的发布设置，发布现有 Security Hub 发现的更新。Macie 仅针对策略调查发现执行此操作。与策略调查发现不同，敏感数据调查发现都被视为新调查发现（唯一）。

  默认情况下，根据定期发布周期，Macie 每 15 分钟发布一次更新调查发现。这意味着，在最近的发布周期之后更新的任何策略调查发现都将被保留，必要时再次更新，并纳入下一发布周期（大约 15 分钟后）。您可以通过选择不同的发布频率，更改此计划。例如，如果您将 Macie 配置为每小时发布一次更新调查发现，并且发布发生在 12:00，则在 12:00 之后发生的任何更新都将在 13:00 发布。

请注意，这两种情况都不适用于通过隐藏规则自动存档的调查发现。Macie 不会向其他人发布隐蔽的发现。 AWS 服务

更改调查发现发布频率

您可以更改 Amazon Macie 在其他版本中发布现有政策调查结果更新的时间表。 AWS 服务默认情况下，Macie 每 15 分钟发布一次最新调查发现。如果您更改此计划，则您的更改仅适用于当前 AWS 区域。如果您是组织的 Macie 管理员，则您的更改也适用于该区域的所有关联成员账户。有关更多信息，请参阅管理多个 账户。

更改调查发现的发布频率

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 在导航窗格中，选择 Settings（设置）。
3. 在调查发现发布部分的更新策略调查发现频率下，选择您想要 Macie 向其他 AWS 服务发布最新策略调查发现的频率。
4. 选择保存。

Amazon Macie与 Amazon EventBridge 集成

Amazon EventBridge（以前称为 Amazon CloudWatch Events）是一项无服务器事件总线服务。EventBridge 提供来自应用程序和服务的实时数据流，并将该数据路由到 AWS Lambda 函数、Amazon Simple Notification Service (Amazon SNS) 主题和 Amazon Kinesis 流等目标。要了解有关 EventBridge 的更多信息，请参阅 Amazon EventBridge 用户指南。

借助 EventBridge，您可以自动监控和处理某些类型的事件。这包括 Amazon Macie 针对新策略调查发现和敏感数据调查发现自动发布的事件。这还包括 Macie 针对后续出现的现有策略调查发现自动发布的事件。有关 Macie 如何以及何时发布这些事件的详细信息，请参阅为调查发现配置发布设置。

通过使用 EventBridge 和 Macie 为调查发现发布的事件，您可以近乎实时地监控和处理调查发现。然后，您可以通过使用其他应用程序和服务根据调查发现采取行动。例如，您可以使用 EventBridge 将特定类型的新调查发现发送到 AWS Lambda 函数。然后 Lambda 函数可能会处理该数据并将其发送到您的安全事故和事件管理 (SIEM) 系统。如果您将 AWS 用户通知服务与 Macie 集成，则还可以使用事件通过您指定的交付渠道自动收到有关调查发现的通知。

除了自动监控和处理外，使用 EventBridge 还可以长期保留您的调查发现数据。Macie 会将您的调查发现存储 90 天。借助 EventBridge，您可以将调查发现数据发送到首选存储平台，并根据您所需要的存储时长存储数据。

> **Note**
>
> 若要长期留存，还可以配置 Macie 以将您的敏感数据发现结果存储在 S3 存储桶中。敏感数据发现结果是记录 Macie 对 S3 对象执行的分析的详细信息的记录，以确定该对象是否包含敏感数据。要了解更多信息，请参阅 存储和保留敏感数据发现结果。

主题

使用 Amazon EventBridge

使用 Amazon EventBridge，您可以创建规则来指定要监控的事件以及要为这些事件执行自动操作的目标。目标是 EventBridge 向其发送事件的目标。

要自动执行调查发现的监控和处理任务，您可以创建一个 EventBridge 规则，该规则自动检测 Amazon Macie 调查发现事件并将这些事件发送到另一个应用程序或服务以进行处理或其他操作。您可以调整规则，使其仅发送那些符合特定条件的事件。为此，请指定源自用于调查发现的 EventBridge 事件架构的标准。

例如，您可以创建一个规则，将特定类型的新调查发现发送到 AWS Lambda 函数。然后，Lambda 函数可以执行诸如下列各项的任务：处理数据并将其发送到您的 SIEM 系统；自动对 S3 对象应用某种类型的服务器端加密；或者通过更改 S3 对象的访问控制列表（ACL）来限制对该对象的访问。或者，您

可以创建一条规则，自动向 Amazon SNS 主题发送新的高严重性调查发现，然后将调查发现通知您的事件响应团队。

除了调用 Lambda 函数和通知 Amazon SNS 主题之外，EventBridge 还支持其他类型的目标和操作，例如将事件中继到 Amazon Kinesis 流，激活 AWS Step Functions 状态机，并调用 AWS Systems Manager 运行命令。有关支持的目标信息，请参阅 Amazon EventBridge 用户指南中的 Amazon EventBridge 目标。

为调查发现创建 Amazon EventBridge 规则

以下过程说明了如何使用 Amazon EventBridge 控制台和 AWS Command Line Interface (AWS CLI) 为 Amazon Macie 调查发现创建 EventBridge 规则。该规则会检测对 Macie 调查发现使用事件架构和模式的 EventBridge 事件，然后将这些事件发送到 AWS Lambda 函数进行处理。

AWS Lambda 是一项计算服务，您可用来运行代码而无需预配置或管理服务器。您可将代码打包并上载到 AWS Lambda 作为 Lambda 函数。然后在调用该函数时，AWS Lambda 会运行该函数。您可以手动调用函数，自动调用函数以响应事件，或者响应来自应用程序或服务的请求。有关创建和调用 Lambda 函数的信息，请参阅 AWS Lambda 开发者指南。

Console

此过程说明如何使用 Amazon EventBridge 控制台创建规则，自动将所有 Macie 调查发现事件发送到 Lambda 函数进行处理。该规则对收到特定事件时运行的规则使用默认设置。有关规则设置的详细信息或要了解如何创建使用自定义设置的规则，请参阅 Amazon EventBridge 用户指南中的创建对事件做出反应的规则。

> **Tip**
>
> 您还可以创建一个规则，使用自定义模式仅检测 Macie 调查发现事件的子集并对其采取行动。该子集可以基于 Macie 在调查发现事件中包含的特定字段。要了解可用字段，请参阅用于调查发现的 EventBridge 事件架构。要了解如何创建此类规则，请参阅 Amazon EventBridge 用户指南中的事件模式中的内容筛选。

在创建规则之前，请创建您希望该规则用作目标的 Lambda 函数。创建规则时，需要将此函数指定为规则的目标。

通过使用控制台创建事件规则

1. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。

2. 在导航窗格中的事件下，选择规则。
3. 在规则部分中，选择创建规则。
4. 在定义规则详细信息页面上，执行以下操作：

   - 对于名称，输入规则的名称。
   - （可选）对于描述，输入规则的简要描述。
   - 对于事件总线，请确保选择默认值，以及在选定的事件总线上启用该规则已开启。
   - 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。
5. 完成后，选择 Next (下一步)。
6. 在构建事件模式页面上，执行以下操作：

   - 对于事件源，选择 AWS 事件或 EventBridge 合作伙伴。
   - （可选）对于示例事件，请查看 Macie 的示例调查发现事件，以了解事件可能包含的内容。为此，请选择 AWS 事件。然后，对于示例事件，选择 Macie 调查发现。
   - 对于事件模式，选择事件模式表。然后输入以下设置：
     - 对于事件源，选择 AWS 服务。
     - 对于 AWS 服务，输入 Macie。
     - 对于事件类型，输入 Macie 调查发现。
7. 完成后，选择 Next (下一步)。
8. 在选择目标页面上，执行以下操作：

   - 对于 Target types（目标类型），选择 AWS 服务。
   - 对于选择目标，输入 Lambda 函数。然后，对于函数，选择您要将调查发现发送到的 Lambda 函数。
   - 对于配置版本/别名，输入目标 Lambda 函数的版本和别名设置。
   - （可选）对于其他设置，输入自定义设置以指定要向 Lambda 函数发送哪些事件数据。您还可以指定如何处理未成功传递到函数的事件。
9. 完成后，选择 Next (下一步)。
10. 在配置标签页面上，可以选择输入要分配给规则的一个或多个标签。然后选择下一步。
11. 在查看并创建页面上，查看规则的设置并验证它们是否正确。

    要更改设置，选择包含该设置的部分中的编辑，然后输入正确的设置。您也可以使用导航选项卡转到包含设置的页面。
12. 在输入完验证设置后，请选择创建规则。

AWS CLI

此过程说明如何使用 AWS CLI 来创建 EventBridge 规则，将所有 Macie 调查发现事件发送到 Lambda 函数进行处理。该规则对收到特定事件时运行的规则使用默认设置。在该过程中，这些命令是针对 Microsoft Windows 进行格式化的。对于 Linux、macOS 或 Unix，请将插入符号 (^) 行继续符替换为反斜杠 (\)。

在创建规则之前，请创建您希望该规则用作目标的 Lambda 函数。创建函数时，请记下函数的 Amazon Resource Name (ARN)。为规则指定目标时，需要输入此 ARN。

通过使用 AWS CLI 创建事件规则

1. 为 Macie 发布到 EventBridge 的所有调查发现创建一条检测事件的规则。为此，请使用 EventBridge put-rule 命令。例如：

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

其中 *MacieFindings* 是您要为规则使用的名称。

如果该命令成功运行，EventBridge 将使用规则的 ARN 作出响应。记下此 ARN。您需要在步骤 3 中输入该 ARN。

> **Tip**
>
> 您还可以创建一个规则，使用自定义模式仅检测 Macie 调查发现事件的子集并对其采取行动。该子集可以基于 Macie 在调查发现事件中包含的特定字段。要了解可用字段，请参阅用于调查发现的 EventBridge 事件架构。要了解如何创建此类规则，请参阅 Amazon EventBridge 用户指南中的事件模式中的内容筛选。

2. 指定要用作规则目标的 Lambda 函数。为此，请使用 EventBridge put-targets 命令。例如：

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

其中 *MacieFindings* 是您在步骤 1 中为规则指定的名称，Arn 参数的值是要将规则用作目标的函数的 ARN。

3. 添加允许规则调用目标 Lambda 函数的权限。为此，请使用 Lambda add-permission 命令。例如：

```
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
```

其中：

- *my-findings-function* 是要将规则用作目标的 Lambda 函数的名称。
- *Sid* 是您定义的唯一标识符，用来描述 Lambda 函数策略中的语句。
- source-arn 是 EventBridge 规则的 ARN。

如果命令成功运行，则您将收到类似于以下内容的输出：

```
{
  "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\"}}}"
}
```

Statement 值是已添加到 Lambda 函数策略的语句的 JSON 字符串版本。

Amazon Macie 与 AWS Security Hub 集成

AWS Security Hub 是一种服务，提供了您在 AWS 中的安全状态的全面视图，可帮助您检查环境是否符合安全行业标准和最佳实践。它部分通过使用、汇总、整理来自多个 AWS 服务 和受支持 AWS Partner Network 安全解决方案的调查发现，并对其进行优先级排序。Security Hub 帮助您分析安全趋

势并确定最高优先级的安全问题。通过 Security Hub，您还可以聚合来自多个 AWS 区域的调查发现，然后监控和处理来自单个区域的所有聚合调查调查发现数据。要了解有关 Security Hub 的更多信息，请参阅 AWS Security Hub 用户指南。

Amazon Macie 与 Security Hub 集成，这意味着你可以自动将调查结果从 Macie 发布到 Security Hub。随后，Security Hub 可以在对您的安全状况进行分析时使用这些调查发现。此外，您还可以使用 Security Hub 监控和处理策略和敏感数据发现，将其作为AWS环境中更大的、聚合的发现数据集的一部分。换句话说，您可以分析 Macie 的调查结果，同时对组织的安全状况进行更广泛的分析，并在必要时对发现的结果进行补救。Security Hub 减少了处理来自多个提供商的大量结果的复杂性。此外，它对所有调查发现（包括 Macie 调查发现）都使用标准格式。使用这种格式，即AWS安全调查发现格式 (ASFF)，您无需执行耗时的数据转换工作。

主题

Amazon Macie 如何向其调查发现发布至 AWS Security Hub

在 AWS Security Hub 中，安全问题以调查发现的形式进行跟踪。部分调查发现来自AWS 服务（如 Amazon Macie）或支持的AWS Partner Network安全解决方案所检测到的问题。Security Hub 还有一套用于检测安全问题和生成结果的规则。

Security Hub 提供了管理来自所有这些来源的结果的工具。您可以查看和筛选结果列表，并查看单个调查发现的详细信息。要了解如何操作，请参阅AWS Security Hub用户指南中的查看调查发现列表和详细信息。您还可以跟踪调查发现的调查状态。要了解更多信息，请参阅 AWS Security Hub 用户指南中的对调查发现采取措施。

Security Hub 中的所有调查发现都使用名为 AWS 安全检测结果格式 (ASFF) 的标准 JSON 格式。ASFF 包括有关问题根源、受影响资源以及调查发现当前状态的详细信息。有关更多信息，请参阅 AWS Security Hub 用户指南中的 AWS Security Finding 格式 (ASFF)。

Macie 发布的调查发现类型

根据您为 Macie 账户选择的发布设置，Macie 可以将其创建的所有调查发现（包括敏感数据调查发现和策略调查发现）发布至 Security Hub。有关这些设置以及如何更改它们的信息，请参阅 为调查发现

配置发布设置。默认情况下，Macie 仅向 Security Hub 发布新的和更新的策略调查发现。Macie 不会向 Security Hub 发布敏感数据调查发现。

敏感数据调查发现

如果您将 Macie 配置为将敏感数据调查发现发布至 Security Hub，则 Macie 会自动发布它为账户创建的每个敏感数据查找调查发现，并在处理完调查发现后立即发布。Macie 会对所有未按隐藏规则自动存档的敏感数据调查发现执行此操作。

如果您是组织的 Macie 管理员，则仅可发布您运行的敏感数据发现作业的调查发现，以及 Macie 为组织执行的自动敏感数据发现活动的调查发现。仅作业创建账户才能发布此作业产生的敏感数据调查发现。仅 Macie 管理员账户可为组织发布自动敏感数据发现活动中生成的敏感数据调查发现。

当 Macie 向 Security Hub 发布敏感数据调查发现时，它会使用AWS安全调查发现格式 (ASFF)，这是 Security Hub 中所有调查发现的标准格式。在 ASFF 中，该 Types 字段表示调查发现的类型。此字段使用的分类法与 Macie 中的调查发现类型分类法略有不同。

下表列出了 Macie 可以为每类敏感数据调查发现创建的 ASFF 调查发现类型。

Macie 调查发现类型	ASFF 结果类型
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

策略调查发现

如果您将 Macie 配置为将策略调查发现发布至 Security Hub，则 Macie 会自动发布它创建的每个新策略调查发现，并在处理完调查发现后立即发布。如果 Macie 检测到后续发生现有策略调查发现，则使用您为账户指定的发布频率，自动在 Security Hub 中发布现有调查发现更新。Macie 对所有未按隐藏规则自动存档的策略调查发现执行此任务。

如果您是组织的 Macie 管理员，则发布内容仅限直属于您账户的 S3 存储桶的策略调查发现。对于组织中的成员账户创建或更新的策略调查发现，Macie 不会发布。这有助于确保 Security Hub 中没有重复的调查发现数据。

与敏感数据调查发现一样，Macie 在向 Security Hub 发布新的和更新策略调查发现时使用AWS安全调查发现格式 (ASFF)。在 ASFF 中，该 `Types` 字段使用的分类法与 Macie 中的调查发现类型分类法略有不同。

下表列出了 Macie 可针对每种策略调查发现创建的 ASSF 调查发现类型。如果 Macie 在 2021 年 1 月 28 日当天或之后在 Security Hub 中创建或更新了策略调查发现，则在 Security Hub 中，该调查发现包含以下 ASFF `Types`字段值。

Macie 调查发现类型	ASFF 结果类型
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
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

Macie 调查发现类型	ASFF 结果类型
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

如果 Macie 在 2021 年 1 月 28 日之前创建或最新更新策略调查发现则在 Security Hub 中，该调查发现包含以下 ASFF Types字段值：

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

前面列表中的值直接映射至 Macie 中调查发现类型 (`type`) 字段的值。

> **Note**
>
> 在 Security Hub 中查看和处理策略调查发现时，请注意以下例外情况：
>
> - 在特定 AWS 区域，早在 2021 年 1 月 25 日，Macie 就开始使用 ASFF 调查发现类型来获取新的和更新的发现。
> - 如果您在 Macie 开始在您的AWS 区域中使用 ASFF 调查发现类型之前在 Security Hub 中对策略调查发现进行了操作，则此调查发现的 ASFF `Types` 字段的值将是前面列表中的 Macie 调查发现类型之一。它不会是上表列出的 ASFF 调查发现类型之一。当您使用AWS Security Hub控制台或 AWS Security Hub API 的 BatchUpdateFindings操作，策略调查发现正是如此。

调查发现发布的延迟

当 Macie 创建新策略或敏感数据调查发现时，它会在处理完调查发现后立即将调查发现发布至 Security Hub。

当 Macie 检测到后续出现现有策略调查发现时，它会对现有 Security Hub 调查发现发布更新。更新的时间取决于您为 Macie 账户选择的发布频率。默认情况下，Macie 每 15 分钟发布一次更新。有关更多信息（包括如何更改账户设置），请参阅 为调查发现配置发布设置。

Security Hub 不可用时重新发布

如果 Security Hub 不可用，Macie 会创建 Security Hub 尚未收到的调查发现队列。系统恢复后，Macie 会重试发布，直到 Security Hub 收到调查发现。

更新 Security Hub 中的现有 结果

在 Macie 向 Security Hub 发布策略调查发现后，Macie 会更新调查发现，以反映该调查发现活动中出现的任何其他事件。Macie 仅针对策略调查发现执行此操作。与策略调查发现不同，敏感数据调查发现都被视为新调查发现（唯一）。

当 Macie 发布策略调查发现的更新时，Macie 会更新该调查发现的 更新于 (`UpdatedAt`) 字段值。当 Macie 近期检测到后续调查发现生成过程中会发生潜在策略违规行为或问题时，您可通过此值进行判定。

如果此字段的现有值不是ASFF 调查发现类型，则 Macie 也可以更新类型 (`Types`) 字段值。这取决于您是否对 Security Hub 中的调查发现执行了操作。如果您尚未对调查发现执行操作，Macie 会将该字段的值更改为相应的 ASFF 调查发现类型。如果您使用 AWS Security Hub 控制台或 AWS Security Hub API 的BatchUpdateFindings操作对调查发现执行操作，则 Macie 不会更改此字段值。

AWS Security Hub中的 Amazon Macie 调查发现示例

当 Amazon Macie 向AWS Security Hub发布调查发现时，它会使用AWS安全调查发现格式 (ASFF) 。这是 Security Hub 中所有调查发现的标准格式。以下示例使用示例数据演示 Macie 以此格式发布至 Security Hub 的调查发现数据的结构和性质：

- 敏感数据调查发现示例
- 策略调查发现示例

在 Security Hub 中敏感数据调查发现的示例

以下是 Macie 向 Security Hub 发布的、ASFF 形式的敏感数据调查发现示例。


```
{
    "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"
}
```

Security Hub 中的策略调查发现示例

以下是 Macie 向 Security Hub 发布的、ASFF 形式的新策略调查发现示例。

```
{
    "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
}
```

启用和配置 AWS Security Hub 集成

要将 Amazon Macie 与集成AWS Security Hub，请为你启用 Security Hub。AWS 账户要了解如何操作，请参阅《AWS Security Hub用户指南》中的 “启用 Security Hub”。

当您同时启用 Macie 和 Security Hub 时，集成将自动启用。默认情况下，Macie 开始自动向 Security Hub 发布新的和更新的政策调查结果。您无需采取其他步骤来配置集成。如果您在启用集成时已有策略发现，Macie 不会将其发布到 Security Hub。相反，Macie 仅发布其在启用集成后创建或更新的政策调查结果。

您可以选择通过选择 Macie 在 Security Hub 中发布策略调查发现更新的频率，以自定义您的配置。您也可以选择将敏感数据发现结果发布到 Security Hub。要了解如何操作，请参阅 为调查发现配置发布设置。

停止向 AWS Security Hub 发布调查发现

要停止向AWS Security Hub发布调查发现，您可以更改 Amazon Macie 账户的发布设置。要了解如何操作，请参阅 为调查发现选择发布目标。您也可以使用 Security Hub 控制台或 Security Hub API 执行此操作。要了解如何操作，请参阅 AWS Security Hub 用户指南中的禁用和启用来自集成的结果流（控制台）或禁用来自集成的结果流（Security Hub API、AWS）。

Amazon Macie 与 AWS 用户通知服务集成

AWS 用户通知服务是您在AWS Management Console上获取AWS通知的中心位置。这包括 Amazon CloudWatch 警报、AWS Support案例以及来自其他AWS 服务通信形式的通知。借此用户通知服务，您可配置自定义规则，并为接收特定类型 Amazon EventBridge 事件通知提供传递通道。交付通道包括电子邮件、AWS Chatbot 聊天通知和 AWS Console Mobile Application 推送通知。您也可以在 AWS 用户通知服务上查看通知。要了解有关用户通知服务的更多信息，请参阅 AWS 用户通知服务用户指南。

Macie 与 AWS 用户通知服务集成后，您可以配置用户通知服务，以获知 Macie 发布至 EventBridge 的、关于策略和敏感数据的调查发现信息。如果调查发现符合您指定的标准，则用户通知服务会生成通知。该通知包括相关调查发现的关键细节，例如调查发现的类型和严重性，以及受影响资源的名称。用户通知服务还可将通知发送至您指定的一个或多个传递通道。您可以根据您的安全和合规工作流程，自定义选择传递通道。

例如，您可配置用户通知服务，以生成关于特定类型的新建、高严重性调查发现通知。您也可以将 AWS Chatbot指定为此通知的传递通道。然后，用户通知服务会检测调查发现的 EventBridg 事件，生成包含调查发现数据的通知，并将通知发送至 AWS Chatbot。然后，AWS Chatbot可能会将通知发送至 Slack 通道或 Amazon Chime 聊天室，以通知您的事件响应团队。

主题

使用 AWS 用户通知服务

借此 AWS 用户通知服务，您可创建规则，以指定您想要监控和接收通知的目标 Amazon EventBridge 事件类型。EventBridge 必须匹配规则定义的条件，才能生成通知。您也可以选择一个或多个规则传递通道。传递通道是指您想要按规则条件接收事件通知的位置。

如果用户通知服务检测到 EventBridge 事件符合规则条件，则它会执行以下常规任务：

1. 从事件中提取数据子集。
2. 生成包含提取数据的通知。

3. 将通知发送至指定类型的事件传递通道。

通知的设计和结构针对每个目标传递通道进行了优化。

若要管理收到通知的频率或数量，您可以为规则配置聚合设置。如果您启用此设置，则用户通知服务会将多个事件的数据合并至一个通知中。严重性较高的调查发现事件，您可选择快速、频繁地发送聚合事件通知。或者对于严重性较低的调查发现事件，您可选择降低发送频率以减少收到的通知数量。如您合并事件数据，您可以使用 AWS 用户通知服务控制台深入查看每个聚合事件的详细信息。您还可在此导航至 Amazon Macie 控制台上的每个相关调查发现信息。

针对 Amazon Macie 调查发现，启用和配置 AWS 用户通知服务

要让 AWS 用户通知服务生成有关 Amazon Macie 调查发现的通知，请在用户通知服务中为 Macie 创建通知配置。通知配置指定规则标准。它还指定传递通道和其他设置，用于监控和发送符合规则标准的 Amazon EventBridge 事件通知。有关创建通知配置的详细信息，请参阅 AWS 用户通知服务用户指南中的AWS 用户通知服务入门。

要为 Macie 调查发现创建通知配置，请选择以下事件规则选项：

- 对于 AWS 服务名称，请选择 Macie。
- 对于 事件类型，选择 Macie 调查发现。
- 对于 区域，选择您使用 Macie 并希望收到调查发现通知的每个 AWS 区域。

用户通知服务可通过此配置监控AWS 账户的 EventBridge 事件，并在您指定的区域生成所有 Macie 调查发现事件通知。事件匹配以下条件：

- `sourceequalsaws.macie`
- `detail-typeequalsMacie Finding`

事件规则的基础 JSON 模式为：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

要完善规则并仅针对调查发现子集生成通知，您可为此规则生成自定义 JSON 模式。据此，请指定从Macie 调查发现的 EventBridge 事件架构派生的附加条件。

如果您创建使用自定义 JSON 模式的规则，则可以为 Macie调查发现创建多个通知配置。然后，您可以为每种配置自定义传递通道和其他设置，使其与针对特定调查发现类型的安全和合规工作流程保持一致。

例如，您可创建一个规则，当 Macie 生成或更新 Policy:IAMUser/S3BucketPublic 调查发现时通知您。在这种情况下，规则模式可能是：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

您还可可以创建另一条规则，在 Macie 为可公开访问的 S3 存储桶生成敏感数据调查发现时通知您。在这种情况下，规则模式可能是：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

如果您为 Macie 调查发现创建了多个通知配置，则最好确保每项配置规则的唯一性。否则，您可能会收到有关个别调查发现的重复通知。

要了解有关为规则自定义事件模式的更多信息，请参阅 AWS 用户通知服务用户指南中的使用自定义 JSON 事件模式。

将 AWS 用户通知服务字段映射至 Amazon Macie 调查发现字段

当 AWS 用户通知服务针对 Amazon Macie 调查发现生成通知时，它会在通知中填充相应 Amazon EventBridge 事件中的字段子集数据。此字段包括相关调查发现的关键细节，例如调查发现的类型和严重性以及受影响资源的名称。

如果您在 AWS 用户通知服务控制台上查看通知，则该通知包含该字段子集的所有数据。此外还提供了指向 Amazon Macie 控制台上的相关调查发现的链接。如果您通过其他传递通道查看该通知，则可能仅包含部分字段数据。原因是用户通知服务会自定义通知的设计和结构，以适应其所支持的每种类型传递通道。

下表列出了调查发现通知中可能包含的字段。在表中，通知字段列描述（斜体）或表示通知中字段的名称。调查发现事件字段 列使用点符号表示调查发现 EventBridge 事件中的相应 JSON 字段名称。描述列描述了存储在此字段内的数据。

通知字段	调查发现事件字段	描述
消息标题	`detail.type`	结果类型。 例如：`Policy:IAMUser/S3BucketPublic` 或 `SensitiveData:S3Object/Financial` 。
摘要	`detail.title`	调查发现的简要描述 例如：`The S3 object contains financial information.`
描述	`detail.description`	调查发现的完整描述 例如：`The S3 object contains financial information such as bank account numbers or credit card numbers.`
严重性	`detail.severity.description`	调查发现严重程度的定性表示：`Low`、`Medium`或`High`。
结果 ID	`detail.id`	调查发现的唯一标识符。

通知字段	调查发现事件字段	描述
已创建	`detail.createdAt`	Macie 创建调查发现的日期和时间。
Updated	`detail.updatedAt`	Macie 最近更新调查发现的日期和时间。 对于敏感数据调查发现，此值与创建 (`detail.createdAt`) 字段值相同。所有敏感数据调查发现均被视为新发现（唯一的）。
受影响的 S3 存储桶	`detail.resourcesAffected.s3Bucket.arn`	S3 存储桶的 Amazon 资源名称（ARN）。
受影响的 S3 对象	`detail.resourcesAffected.s3Object.path`	受影响的 S3 对象名称（密钥），包括存储对象和对象前缀（如适用）的存储桶名称。 此字段不包含在策略调查发现通知中。

通知字段	调查发现事件字段	描述

敏感数据检测	`detail.classificationDetails.result.sensitiveData.detections...`
	
	AND 或 &&
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		这串联了事件中的多个字段，用于敏感数据的调查发现。此字段不包含在策略调查发现通知中。
		
		如果托管数据标识符检测到敏感数据，则此字段指定所检测到的敏感数据的类别、类型和出现次数 (count)。例如：`PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences` 。
		
		如果自定义数据标识符检测到敏感数据，则此字段指定自定义数据标识符的名称，以及检测到的敏感数据出现次数 (count)。例如：`Employee ID 20 occurrences` 。
		
		如果调查发现报告多种类型敏感数据，则通知包含最多四类数据。数据中首先填充适当的自定义标识符，然后填充适当的托管数据标识符。

更改 Amazon Macie 调查发现的 AWS 用户通知服务设置

您可以随时更改 Amazon Macie 调查发现的 AWS 用户通知服务设置。为此，请在用户通知服务中编辑通知配置。要了解操作方法，请参阅 AWS 用户通知服务用户指南中的管理通知配置。

如果您的 Macie 调查发现包含多种通知配置，则更改一项通知配置不会影响其他配置设置。您可以编辑全部或部分配置。

对 Amazon Macie 调查发现禁用 AWS 用户通知服务

要停止生成和接收来自 AWS 用户通知服务的 Amazon Macie 调查发现通知，请删除用户通知服务中的通知配置。要了解操作方法，请参阅 AWS 用户通知服务用户指南中的管理通知配置。

如果您的 Macie 调查发现包含多种通知配置，则删除一项通知配置不会影响其他配置设置。您可以删除全部或部分配置。

用于 Amazon Macie 调查发现的 Amazon EventBridge 事件架构

为了支持与其他应用程序、服务和系统（例如监控或事件管理系统）集成，Amazon Macie 会自动将调查发现以事件形式发布至 Amazon EventBridge。EventBridge，前身为 Amazon CloudWatch Events，是一项无服务器事件总线服务，可将来自应用程序和其他AWS 服务的实时数据流式传输至 AWS Lambda函数、Amazon Simple Notification Service 主题以及 Amazon Kinesis 流等目标。要了解有关 EventBridge 的更多信息，请参阅 Amazon EventBridge 用户指南。

> **Note**
>
> 如果您目前使用的是 CloudWatch Events，请注意 EventBridge 和 CloudWatch Events 是相同的基础服务和 API。但是，EventBridge 包含其他功能，让您能够从软件即服务（SaaS）应用程序和您自己的应用程序接收事件。由于基础服务和 API 相同，因此 Macie 发现的事件架构也相同。

Macie 会自动发布所有新调查发现和现有策略的后续调查发现的事件，但使用隐藏规则自动存档的调查发现除外。事件是符合 AWS 事件 EventBridge 架构的 JSON 对象。每个事件都包含特定调查发现的 JSON 表示。由于该数据采用 EventBridge 事件的结构，因此可以使用其他应用程序、服务和工具更轻松地监控、处理调查发现，以及相应采取行动。要详细了解 Macie 如何以及何时发布有关调查发现的事件，请参阅 为调查发现配置发布设置。

主题

- 事件架构
- 策略调查发现事件示例
- 敏感数据调查发现事件示例

事件架构

以下示例显示了 Amazon Macie 调查发现的Amazon EventBridge 事件架构。有关调查发现事件中包含字段的详细描述，请参阅 Amazon Macie API 引用 中的调查发现。调查发现事件的结构和字段与 Amazon Macie API 的调查发现对象非常接近。

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "AWS ## ID (string)",
    "time": "event timestamp (string)",
    "region": "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
}
```

策略调查发现事件示例

以下示例使用示例数据演示 Amazon EventBridge 事件策略调查发现对象和字段的结构和特性。

在此示例中，该事件报告了后续出现的现有策略调查发现：禁用 “阻止 S3 存储桶公开访问设置”。以下字段和值可帮助您确定情况是否如此：

- 该 `type` 字段设置为 `Policy:IAMUser/S3BlockPublicAccessDisabled`。
- `createdAt` 和 `updatedAt` 字段的值不同。此指标表明，该事件报告了现有策略调查发现的后续发生。如果事件报告了新调查发现，则这些字段的值将相同。
- `count` 字段设置为 `2`，表示这是调查发现的第二次出现。
- 该 `category` 字段设置为 `POLICY`。

- classificationDetails 字段值为 null，这有助于将此策略调查发现事件与敏感数据调查发现事件区分开来。对于敏感数据调查发现，此值将是一组对象和字段，这些对象和字段提供有关敏感数据的查找方式及数据内容。

请注意，sample 字段值设置为 true。此值强调这是文档中所使用的示例事件。


```
{
    "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
    }
}
```

敏感数据调查发现事件示例

以下使用示例数据演示：用于敏感数据调查发现的 Amazon EventBridge 事件的对象和字段的结构和性质。

在此示例中，该事件报告了一项新的敏感数据调查发现：Amazon Macie 在 S3 对象中发现了不止一类敏感数据。以下字段和值可帮助您确定情况是否如此：

- 该 `type` 字段设置为 `SensitiveData:S3Object/Multiple`。
- `createdAt` 和 `updatedAt` 字段值相同。与策略调查发现不同的是，敏感数据调查发现总是如此。所有敏感数据调查发现均被视为新调查发现。

- count 字段设置为 1，表示这是一项新调查发现。与策略调查发现不同的是，敏感数据调查发现总是如此。所有敏感数据调查发现都被认为具有唯一性（新）。
- 该 category 字段设置为 CLASSIFICATION。
- policyDetails 字段值为 null，这有助于将敏感数据调查发现事件与策略调查发现事件区分开来。对于策略调查发现，此值将是一组对象和字段，这些对象和字段提供有关 S3 存储桶可能违反策略、安全性或隐私问题的信息。

请注意，sample 字段值设置为 true。此值强调这是文档中所使用的示例事件。

```
{
    "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
  }
}
```

预测和监控 Amazon Macie 成本

为了帮助您预测和监控使用 Amazon Macie 的成本，Macie 会计算并提供您账户的估计使用成本。利用这些数据，您可以确定是否要调整服务的使用或账户配额。如果您目前正在参与 Macie 的 30 天免费试用，则可以在免费试用期结束后使用这些数据估算使用 Macie 的成本。您还可以查看试用状态。

您可以在 Amazon Macie 控制台上查看您的估计使用成本，并使用 Amazon Macie API 以编程方式访问它们。如果您是组织的 Macie 管理员，则可以查看和访问组织的聚合数据以及组织中账户的数据明细。

除了 Macie 提供的估计使用成本外，您还可以使用 AWS Billing and Cost Management 来查看和监控实际成本。AWS Billing and Cost Management 提供的功能旨在帮助您跟踪和分析您的 AWS 服务 的成本，并管理您的账户或组织的预算。它还提供可帮助您根据历史数据预测使用成本的功能。要了解有关更多信息，请参阅 AWS Billing 用户指南。

主题

了解如何计算 Amazon Macie 的估计使用成本

Amazon Macie 的定价基于以下维度。

预防性控制监控

这些成本来自维护 Amazon Simple Storage Service (Amazon S3) 存储桶清单，以及评测和监控存储桶的安全性和访问控制。有关更多信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。

按照 Macie 为您的账户监控的 S3 存储桶总数向您收费。费用按天按比例分配。

用于自动化敏感数据发现的对象监控

这些成本来自监控和评测您的 S3 存储桶清单，以识别符合通过自动化敏感数据发现进行分析的 S3 对象。有关更多信息，请参阅 自动敏感数据发现的工作原理。

按照 Macie 为您的账户监控的 S3 对象总数向您收费。费用按天按比例分配。

通过敏感数据发现作业和自动化敏感数据发现进行对象分析

这些成本来自分析 S3 对象和报告 Macie 在对象中发现的敏感数据。这包括通过敏感数据发现作业和自动化敏感数据发现进行的分析和报告。

按照 Macie 在 S3 对象中分析的未压缩数据量向您收费。对于 Macie 因使用不支持的 Amazon S3 存储类别、不支持的文件或存储格式或权限设置等原因而无法分析的对象，不收取任何费用。有关更多信息，请参阅 发现敏感数据。此外，这些成本不会因您的作业或自动化敏感数据发现而产生的敏感数据调查发现的数量而变化。

要管理自动化敏感数据发现的成本，您可以将单个 S3 存储桶排除在分析之外。例如，您可以排除已知符合组织安全性和合规性要求的存储桶。要排除存储桶，您可以更新账户的配置设置。在查看存储桶清单中各个存储桶的详细信息时，您也可以根据具体情况排除存储桶。

敏感数据发现作业的成本受您账户每月的敏感数据发现配额的限制。（默认配额为 5 TB 数据。）如果作业正在运行且对符合条件的对象的分析达到此配额，Macie 会自动暂停该作业，直到下一个日历月开始（并且您的账户的每月配额已重置），或者您增加账户的配额。

如果您是组织的 Macie 管理员，则敏感数据发现作业的费用将受到您分析数据的每个账户的每月敏感数据发现配额的限制。成员账户的配额定义了在一个日历月内，您的作业以及成员账户的作业可以为该账户分析的最大数据量。如果作业正在运行，并且对符合条件的对象的分析达到成员账户的此配额，Macie 将停止分析该账户拥有的对象。当 Macie 完成对所有其他未达到配额的账户的对象的分析后，Macie 会自动暂停作业。如果这是一次性作业，Macie 将在下一个日历月开始时或所有受影响账户的配额增加时（以先发生者为准）自动恢复该作业。如果是定期作业，Macie 将在计划下一次运行开始或下一个日历月开始时（以先发生者为准）自动恢复该作业。如果计划运行在下一个日历月开始之前开始，或者受影响账户的配额增加，Macie 不会分析该账户拥有的对象。

> **Tip**
>
> 有关管理或降低敏感数据发现成本的有用建议，请参阅AWS安全博客上的《如何使用 Amazon Macie 降低发现敏感数据的成本》博文。

有关使用成本的详细信息和示例，请参阅 Amazon Macie 定价。

当您使用 Macie 查看您的估计使用成本时，了解成本估计的计算方式非常重要。请考虑以下事项：

- 估算值以美元报告，仅适用于当前的 AWS 区域。如果您在多个区域使用 Macie，则不会汇总您使用 Macie 的所有地区的数据。

- 在控制台上，估算值包含当前日历月至今的数值。如果您使用 Amazon Macie API 以编程方式查询数据，则可以为估算选择一个包含的时间范围。这可以是前 30 天的滚动时间范围，也可以是当前日历月至今的滚动时间范围。
- 估算值并未反映可能适用于您账户的所有折扣。唯一的例外是区域批量定价套餐产生的折扣，如 Amazon Macie 定价 中所述。如果您的账户有资格享受此类折扣，则估算值将反映该折扣。
- 如果您是组织的 Macie 管理员，则估算值不会反映您组织的总使用量折扣。有关这些折扣的信息，请参阅AWS Billing《用户指南》中的批量折扣。
- 对于预防性控制监测，估算值基于适用时间范围内的平均每日成本。费用按每天依比例分配。
- 对于自动化敏感数据发现，总体估算基于对象监控的平均每日成本（每天按比例分配），以及 Macie 迄今为止在适用时间范围内分析的未压缩数据量。如果您是组织的 Macie 管理员并且您分析成员账户的数据，则这些活动的估计成本将包含在每个适用账户的估算中。
- 对于敏感数据发现作业，则估算基于您的作业迄今为止在适用时间范围内分析的未压缩数据量。如果您是组织的 Macie 管理员，并且正在运行分析成员账户数据的作业，则这些工作的估计成本将包含在相应成员账户的估算中。
- 如果您的账户是组织中的成员账户，并且您的 Macie 管理员执行自动化敏感数据发现或运行敏感数据发现作业来分析您的数据，则这些活动的估计费用将包含在您的账户的估算中。
- 该估算不包括您因使用具有某些 Macie 功能的其他 AWS 服务 而产生的成本。例如，使用客户托管 AWS KMS keys 解密要检查敏感数据的 S3 对象。

另请注意，Macie 提供了每月免费套餐，允许通过敏感数据发现作业和自动化敏感数据发现来分析 S3 对象。每个月，分析最多 1 GB 的数据以发现和报告 S3 对象中的敏感数据，无需支付任何费用。如果在给定月份分析的数据超过 1 GB，则在前 1 GB 数据之后，您的账户将开始计入敏感数据发现费用。如果在规定月份中分析的数据少于 1 GB，则剩余的分配不会转入下个月。如果您的账户属于采用整合账单的组织，则免费套餐适用于为您的组织分析的合并数据量。换句话说，每月为组织中的所有账户分析最多 1 GB 的数据不收取任何费用。

查看 Amazon Macie 的估计使用成本

要查看当前的 Amazon Macie 估计使用成本，您可以使用 Amazon Macie 控制台或 Amazon Macie API。控制台和 API 都提供了 Macie 定价维度的估计成本。如果您目前正在参与 30 天免费试用，则可以使用此数据来估算免费试用结束后使用 Macie 的费用。有关 Macie 定价维度和注意事项的信息，请参阅 了解如何计算估计使用成本。有关使用成本的详细信息和示例，请参阅 Amazon Macie 定价。

在 Macie 中，估计使用成本以美元报告，并且仅适用于当前的 AWS 区域。如果您使用控制台查看数据，则成本估算为当前日历月至今（含）。如果您使用 Amazon Macie API 以编程方式查询数据，您

可以为估算值指定一个包含的时间范围，可以是前 30 天的滚动时间范围，也可以是当前日历月至今的滚动时间范围。

主题

查看 Amazon Macie 控制台上的估计使用成本

在 Amazon Macie 控制台上，成本估算方式如下：

- 预防性控制监控 – 这是维护您的 Amazon Simple Storage Service (Amazon S3) 存储桶库存以及评测和监控存储桶以确保安全和访问控制的估计成本。
- 敏感数据发现作业 – 这是您运行的敏感数据发现作业的估计成本。
- 自动化敏感数据发现 – 这是执行自动化敏感数据发现的估计成本。这包括监控和评测您的 S3 存储桶清单，以确定符合分析条件的 S3 对象。它还包括分析符合条件的对象并报告敏感数据统计、调查发现和其他类型的结果。

按照以下步骤使用 Amazon Macie 控制台查看您的估计使用成本。

在控制台上查看您的估计使用成本

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要查看估计成本的区域。
3. 在导航窗格中，选择使用情况。

如果您拥有独立的 Macie 账户或者您的账户是组织中的成员账户，则 使用情况页面会显示您账户的估计使用成本的明细。

如果您是组织的 Macie 管理员，使用情况页面会列出您组织中的账户：

- 表中的 总计字段显示了每个账户的总估计成本。
- 估计成本部分显示了您组织的总估计成本和明细。

要查看组织中特定账户的估计成本明细，请在表中选择该账户。然后，估计成本部分将显示明细。要显示其他账户的此数据，请在表中选择该账户。要清除账户选择，请选择账户 ID 旁边的 X。

使用 Amazon Macie API 查询估计使用成本

要以编程方式查询您的估计使用成本，可以使用 Amazon Macie API 的以下操作：

- GetUsageTotals – 此操作会返回您账户的总估计使用成本，按使用指标分组。如果您是组织的 Macie 管理员，此操作将返回组织中所有账户的汇总成本估算。要了解有关此操作的更多信息，请参阅《Amazon Macie API 参考》中的使用情况总计。
- GetUsageStatistics – 此操作会返回您账户的使用情况统计数据和相关数据，按账户分组，然后按使用指标分组。该数据包括总估计使用成本和当前账户配额。如果适用，它还会显示您的 Macie 30 天免费试用和自动敏感数据发现的开始时间。如果您是组织的 Macie 管理员，此操作将返回组织中所有账户的数据细目。您可以通过对查询结果进行排序和筛选来自定义查询。要了解有关此操作的更多信息，请参阅《Amazon Macie API 参考》中的使用情况统计。

当您使用任一操作时，您可以选择性地为数据指定包含的时间范围。此时间范围可以是前 30 天的滚动时间范围 (PAST_30_DAYS) ，或当前日历月初至今 (MONTH_TO_DATE) 的滚动时间范围。如果未指定时间范围，则 Macie 将返回前 30 天的数据。

以下示例说明了如何使用 AWS Command Line Interface(AWS CLI) 查询估计使用成本和统计数据。您也可以使用其他 AWS 命令行工具或 AWS SDK 的当前版本，或者直接向 Macie 发送 HTTPS 请求来查询数据。有关 AWS 工具和 SDK 的信息，请参阅在 AWS 上构建的工具。

示例

- 示例 1：查询总估计使用成本
- 示例 2：查询使用情况统计信息

示例 1：查询总估计使用成本

要使用 AWS CLI 查询总估计使用成本，请运行 get-usage-totals 命令，也可以指定数据的时间范围。例如：

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

其中，*MONTH_TO_DATE* 指定当前日历月至今作为数据的时间范围。

如果命令成功运行，则您将收到类似于以下内容的输出：

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

estimatedCost 是关联使用指标 (type) 的总估计使用成本：

- SENSITIVE_DATA_DISCOVERY，用于通过敏感数据发现作业分析 S3 对象。
- AUTOMATED_SENSITIVE_DATA_DISCOVERY，用于通过自动化敏感数据发现来分析 S3 对象。
- DATA_INVENTORY_EVALUATION，用于监控和评测 S3 存储桶以确保安全性和访问控制。
- AUTOMATED_OBJECT_MONITORING，用于评测和监控您的 S3 存储桶清单，以识别符合通过自动化敏感数据发现进行分析的 S3 对象。

示例 2：查询使用情况统计信息

要使用 AWS CLI 查询使用情况统计信息，请运行 get-usage-statistics 命令。您可以选择对查询结果进行排序、筛选和指定时间范围。以下示例检索了过去 30 天内 Macie 管理员账户的使用情况统计信息。结果按 AWS 账户 ID 按升序排列。

对于 Linux、macOS 或 Unix，使用反斜杠 (\) 行继续符来提高可读性：

```
$ aws macie2 get-usage-statistics \
```

```
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

对于 Microsoft Windows，使用脱字符 (^) 行继续符来提高可读性：

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

其中：

- *accountId* 指定用于对结果进行排序的字段。
- *ASC* 是基于指定字段（*accountId*）的值应用于结果的排序顺序。
- *PAST_30_DAYS* 指定前 30 天为数据的时间范围。

如果命令成功运行，Macie 将返回一个 `records` 数组。该数组包含查询结果中包含的每个账户的对象。例如：

```
{
    "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"
}
```

estimatedCost 是账户关联使用指标 (type) 的总估计使用成本：

- DATA_INVENTORY_EVALUATION，用于监控和评测 S3 存储桶以确保安全性和访问控制。
- AUTOMATED_SENSITIVE_DATA_DISCOVERY，用于通过自动化敏感数据发现来分析 S3 对象。
- SENSITIVE_DATA_DISCOVERY，用于通过敏感数据发现作业分析 S3 对象。
- AUTOMATED_OBJECT_MONITORING，用于评测和监控账户的 S3 存储桶清单，以识别符合通过自动化敏感数据发现进行分析的 S3 对象。

参与 Amazon Macie 免费试用

当您首次启用 Amazon Macie 时，您的 AWS 账户 会自动注册 30 天的 Macie 免费试用。这包括 AWS Organizations 组织中的个人成员账户。

在免费试用期间，在以下特定 AWS 区域 用途中使用 Macie 不收取任何费用：

- 执行预防性控制监控 – 这包括生成和维护该区域中的 Amazon Simple Storage Service (Amazon S3) 存储桶清单。它还包括评测和监控这些存储桶以确保安全性和访问控制。有关更多信息，请参阅 Macie 如何监控 Amazon S3 数据安全性。
- 自动化敏感数据发现 – 这包括监控和评测您在该区域的 S3 存储桶清单，以识别符合分析条件的 S3 对象。它还包括分析符合条件的对象并报告敏感数据统计、调查发现和其他类型的结果。有关更多信息，请参阅 自动敏感数据发现的工作原理。

  自动化敏感数据发现仅适用于 Macie 管理员账户和独立 Macie 账户。如果您拥有 Macie 管理员账户，则可以使用此功能来分析您的成员账户拥有的 S3 存储桶中的对象。

有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。

免费试用期为连续 30 天。开始后您无法暂停。免费试用结束后，执行预防性控制监控将开始产生费用。执行自动敏感数据发现也会开始产生费用。如果您是组织的 Macie 管理员，则组织中的每个账户都会产生适用的费用。您可以使用 Macie 来查看组织中各个账户的估计使用成本明细。

> **Note**
>
> 免费试用版不包括通过敏感数据发现作业对 S3 对象进行分析。如果您在免费试用期间创建并运行敏感数据发现作业，这些作业分析的未压缩数据超过 1 GB，则会产生费用。（Macie 每月

提供免费的敏感数据发现套餐。每个月可以免费分析 S3 对象中最多 1 GB 的未压缩数据。在分析完第一个 1 GB 数据后，就会产生费用。）您还可能会因为与某些 Macie 功能一起使用的其他 AWS 服务 而产生费用，例如，使用客户托管 AWS KMS keys 来解密您想要检查敏感数据的 S3 对象。

在免费试用期间查看您的状态和估计成本

在免费试用期间，您可以查看试用状态并查看账户的估计使用成本。成本估算基于您在免费试用期间迄今为止对 Macie 的使用情况。它们可以帮助您了解试用期结束后可能产生的部分使用成本。有关 Macie 如何计算这些值的详细信息，请参阅 了解如何计算估计使用成本。

按照以下步骤在 Amazon Macie 控制台上查看您的试用状态并查看您的估计使用成本。您也可以使用 Amazon Macie API 的 getuSageStatistics 操作以编程方式访问这些数据。

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要查看免费试用状态和估计使用成本的区域。
3. 在导航窗格中，选择使用情况。

使用情况页面会显示免费试用的剩余天数。它还显示了您的估计使用成本（以美元为单位）明细：

- 预防性控制监控 – 这是免费试用期结束后维护 S3 存储桶清单以及评测和监控存储桶的安全性和访问控制的总估计成本。
- 敏感数据发现作业 – 这是您运行的任何敏感数据发现作业的总估计成本。免费试用版不包括敏感数据发现作业。
- 自动化敏感数据发现 – 这些是免费试用结束后执行自动敏感数据发现的总估计成本，按定价维度（对象监控和对象分析）细分。

如果您是组织的 Macie 管理员，则 使用情况页面将提供组织中的 Maciee 成员的详细信息：

- 表中的 免费试用 字段显示了某个账户当前是否正在参与预防性控制监控或自动敏感数据发现的免费试用。如果账户适用的免费试用已结束，则 免费试用 字段为空。总计字段显示了每个账户的总估计成本。
- 估计成本部分显示了组织的总体估计成本。

要查看组织中特定账户的估计成本明细，请在表中选择该账户。然后，估计成本部分将显示明细。要显示其他账户的此数据，请在表中选择该账户。要清除账户选择，请选择账户 ID 旁边的 X。

> **Note**
>
> 如果账户在 Amazon S3 中存储的数据超过 150 TB，则该账户用于自动化敏感数据发现的估计成本和实际成本可能高于 Macie 在 30 天免费试用期间提供的成本预测。这是因为当已为注册免费试用版的账户分析了 150 GB 的未压缩数据时，通过自动化敏感数据发现进行的对象分析将暂停。免费试用结束后，将恢复该账户的对象分析。
>
> 如需帮助预测在 Amazon S3 中存储超过 150 TB 数据的账户的成本，请联系AWS Support。
>
> 要在免费试用期结束后管理自动化敏感数据发现的费用，您可以将单个 S3 存储桶排除在后续分析之外。要排除存储桶，您可以更新账户的配置设置。在查看存储桶清单中各个存储桶的详细信息时，您也可以根据具体情况排除存储桶。

管理多个 Amazon Macie 账户

如果您的 AWS 环境有多个账户，则可以将环境中的 Amazon Macie 账户关联起来，并在 Macie 中将其作为一个组织进行集中管理。通过此配置，指定的 Macie 管理员可以评测和监控贵组织的 Amazon Simple Storage Service (Amazon S3) 数据资产的整体安全状况，并发现组织的 S3 存储桶中的敏感数据。管理员还可以大规模执行各种账户管理任务，例如监控预计使用成本和评测账户配额。

在 Macie 中，组织由指定的 Macie 管理员账户和一个或多个关联的成员账户组成。您可以通过两种方式关联账户：将 Macie 与 AWS Organizations 集成，或者在 Macie 中发送和接受会员邀请。我们建议将 Macie 集成到 AWS Organizations。

AWS Organizations 是一项全球账户管理服务，使 AWS 管理员能够整合和集中管理多个 AWS 账户。它提供账户管理和整合账单功能，这些功能旨在支持预算、安全性和合规性需求。它不收取额外费用，并且可以与多个 AWS 服务 集成，包括 Macie、AWS Security Hub 和 Amazon GuardDuty。要了解有关更多信息，请参阅 AWS Organizations 用户指南。

如果您希望在不使用 AWS Organizations 的情况下集中管理多个 Macie 账户，则可以改用会员邀请。如果您发送邀请并被另一个账户接受，则您的账户将成为另一个账户的 Macie 管理员账户。如果您收到并接受邀请，则您的账户将成为 Macie 成员账户，Macie 管理员账户可以访问和管理您的 Macie 账户的某些设置、数据和资源。

主题

了解 Amazon Macie 管理员和成员账户之间的关系

如果您作为一个组织集中管理多个 Amazon Macie 账户，则 Macie 管理员可以访问 Amazon Simple Storage Service (Amazon S3) 清单数据、策略调查发现以及关联成员账户的某些 Macie 设置和资源。管理员还可以执行自动敏感数据发现并运行敏感数据发现作业，以检测成员账户拥有的 S3 存储桶中的敏感数据。对特定任务的支持会有所不同，具体视 Macie 管理员账户是通过 AWS Organizations 还是通过邀请与成员账户关联而定。

下表提供了有关 Macie 管理员和成员账户之间关系的详细信息。它表示每种账户类型的默认权限。要进一步限制对 Macie 功能和操作的访问，您可以使用自定义 AWS Identity and Access Management (IAM) 策略。

在此表格中：

- 自身表示该账户无法为任何关联账户执行任务。
- 任何表示该账户可以为单个关联账户执行任务。
- 全部表示该账户可以执行任务，并且该任务适用于所有关联账户。

短划线 (–) 表示该账户无法执行任务。

Task	通过 AWS Organizations		通过邀请	
	管理员	成员	管理员	成员
Enable Macie	Any	–	Self	Self
Review the organization'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	Self	Self	Self	Self

sensitive data discovery results				
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. AWS Organizations中组织的管理员可以查看组织中的所有账户，包括尚未启用 Macie 的账户。基于邀请的组织的管理员只能查看他们添加到其清单中的那些账户。
2. 只有管理员才能抑制策略调查发现。如果管理员创建了抑制规则，则 Macie 会将该规则应用于组织中所有账户的策略调查发现，除非该规则被配置为排除特定账户。如果成员创建了抑制规则，则 Macie 不会将该规则应用于该成员账户的策略调查发现。
3. 只有拥有受影响资源的账户才能将该资源的策略调查发现发布到 AWS Security Hub。管理员账户和成员账户都会自动将受影响资源的策略调查发现发布到 Amazon EventBridge。
4. 成员可以配置作业以仅分析其账户拥有的 S3 存储桶中的对象。管理员可以配置作业以分析其账户拥有或成员账户拥有的存储桶中的对象。有关如何为多账户作业应用限额和计算成本的信息，请参阅了解如何计算估计使用成本。
5. 只有创建作业的账户才能访问该作业的详细信息。这包括 S3 存储桶清单中与作业相关的详细信息。
6. 只有创建作业的账户才能访问、抑制或发布该作业生成的敏感数据调查发现。只有管理员才能访问、抑制或发布自动敏感数据发现生成的敏感数据调查发现。
7.

如果敏感数据调查发现适用于成员账户拥有的 S3 对象，则管理员也许能够检索该调查发现报告的敏感数据样本。这取决于调查发现的来源，以及管理员账户和成员账户中的配置设置和资源。有关更多信息，请参阅 检索敏感数据样本的配置选项和要求。

8. 管理员要想为自己的账户暂停 Macie，必须先取消其账户与所有成员账户的关联。

9. 管理员要想为自己的账户禁用 Macie，必须先取消其账户与所有成员账户的关联，然后删除其账户与所有这些账户之间的关联。AWS Organizations 中组织的管理员可以使用该组织的管理账户将其他账户指定为管理员账户，从而实现此目的。

   要使 AWS Organizations 组织的成员禁用 Macie，管理员必须首先取消该成员账户与其管理员账户的关联。对于基于邀请的组织，成员可以取消其账户与管理员账户的关联，然后禁用 Macie。

10. AWS Organizations 中组织的管理员可以在取消成员账户与其管理员账户的关联后删除与该成员账户的关联。该账户继续出现在管理员的账户清单中，但其状态表明它不是成员账户。在基于邀请的组织中，管理员和成员在取消其账户与另一个账户的关联后，可以删除与另一个账户的关联。然后，另一个账户将停止出现在他们的账户清单中。

使用 AWS Organizations 管理 Amazon Macie 账户

如果您使用 AWS Organizations 集中管理多个 AWS 账户，则可以将 Amazon Macie 与 AWS Organizations 集成，然后集中管理组织中账户的 Macie。通过这种配置，指定的 Macie 管理员可为多达 10,000 个账户启用和管理 Macie。管理员还可以访问 Amazon Simple Storage Service (Amazon S3) 清单数据，并发现账户的 S3 存储桶中有敏感数据。有关管理员可执行任务的详细信息，请参阅 了解 Amazon Macie 管理员和成员账户之间的关系。

若要将 Macie 与 AWS Organizations 集成，您需要首先指定一个账户作为组织的委派 Macie 管理员账户。然后，Macie 管理员为组织中的其他账户启用 Macie，将这些账户添加为 Macie 成员账户，并为这些账户配置 Macie 设置和资源。

> **Tip**
>
> 如果您已通过邀请将 Macie 管理员账户与成员账户相关联，则您可以在 AWS Organizations 中将该账户指定为贵组织的委派 Macie 管理员账户。如果执行此操作，则所有当前关联的成员账户仍会保持成员身份，并且您可以通过使用 AWS Organizations 来充分利用管理账户的好处。有关更多信息，请参阅 从基于邀请的组织过渡。

本节中的主题说明了如何将 Macie 与 AWS Organizations 集成，以及如何管理组织中账户的 Macie。

主题

使用 Amazon Macie 的注意事项和建议 AWS Organizations

在将 Amazon Macie 与 Macie 集成 AWS Organizations 并在 Macie 中配置您的组织之前，请考虑以下要求和建议。此外还应确保您了解 Macie 管理员账户和成员账户之间的关系。

主题

指定 Macie 管理员账户

在确定哪个账户应为组织委派的 Macie 管理员账户时，请记住以下几点：

- 一个组织只能有一个委派的 Macie 管理员账户。
- 一个账户不能同时是 Macie 管理员账户和成员账户。
- 只有组织的 AWS Organizations 管理账户才能为该组织指定委派的 Macie 管理员帐户，并且只有管理账户随后可以更改或删除该指定。
- 组织的 AWS Organizations 管理帐户也可以是该组织委派的 Macie 管理员帐户。但是，基于 AWS 安全最佳实践和最小权限原则，我们不建议使用此配置。出于计费目的有权访问管理账户的用户可能与出于信息安全目的需要访问 Macie 的用户不同。

如果您更喜欢这种配置，则必须至少在一个中为该组织的管理账户启用 Macie， AWS 区域 然后才能将该账户指定为委派的 Macie 管理员帐户。否则，该账户将无法访问和管理 Macie 成员账户的设置和资源。

- 不同的是 AWS Organizations，Macie 是一项区域服务。这意味着 Macie 管理员账户的指定是区域指定。这也意味着 Macie 管理员和成员账户之间的关联是区域性的。例如，如果管理账户指定了在美国东部（弗吉尼亚州北部）地区的 Macie 管理员账户，则 Macie 管理员只能为该地区的成员账户管理 Macie。

  要集中管理多个 Macie 账户 AWS 区域，管理账户必须登录到组织当前使用或将要使用 Macie 的每个区域，然后在每个区域中指定 Macie 管理员账户。然后，Macie 管理员账户可以在每个区域中配置组织。有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。
- 一个账户一次只能与一个 Macie 管理员账户关联。如果您的组织在多个区域使用 Macie，则在所有这些区域中指定的 Macie 管理员账户必须相同。但是，组织的管理账户必须在每个地区分别指定管理员账户。
- 一个账户一次只能是为一个组织委派的 Macie 管理员账户。如果您在中管理多个组织 AWS Organizations，则必须为每个组织指定不同的 Macie 管理员帐户。这是出于一项 AWS Organizations 要求——一个账户一次只能是一个组织的成员。
- 如果 Macie 管理员的账户 AWS 账户 被暂停、隔离或关闭，则所有关联的 Macie 成员账户都将自动移除为 Macie 成员账户，但这些账户不会禁用 Macie。

更改或移除 Macie 管理员账户的指定

只有组织的 AWS Organizations 管理账户才能更改或删除该组织委托的 Macie 管理员帐户的指定。

如果管理账户移除了该指定，则所有关联的成员账户都将作为 Macie 成员账户被移除，但不会为这些账户禁用 Macie。要使账户同时暂停或停止使用 Macie，该账户的用户必须挂起（暂停）或禁用（停止）该账户的 Macie。

添加和移除 Macie 成员账户

在为您的组织添加、移除和以其他方式管理成员账户时，请注意以下几点：

- 一个 Macie 管理员账户只能与每个 AWS 区域中不超过 10,000 个活跃（已启用）的 Macie 成员账户相关联。如果您的组织超过此配额，Macie 管理员将无法添加成员账户，直到他们移除该地区必要数量的现有成员账户。

当组织达到此配额时，我们会通过为其账户创建 AWS Health 和 Amazon CloudWatch 活动来通知 Macie 管理员。我们也会发送电子邮件到与他们的账户相关联的地址。

如果您是组织的 Macie 管理员，则可以通过亚马逊 Macie 控制台上的账户页面或DescribeOrganizationConfiguration亚马逊 Macie API 的操作来确定当前有多少活跃成员账户与您的账户关联。有关更多信息，请参阅 查看组织的 Amazon Macie 账户。

- 一个账户一次只能与一个 Macie 管理员账户关联。这意味着，如果一个账户已经与 AWS Organizations中组织的 Macie 管理员账户关联，则该账户无法接受来自其他账户的 Macie 邀请。

  同样，如果账户已接受邀请，则所在组织的 Macie 管理员 AWS Organizations 无法将该账户添加为 Macie 成员账户。该账户必须先取消与其当前基于邀请的管理员账户的关联。
- 要将 AWS Organizations 管理账户添加为 Macie 成员账户，管理账户的用户必须先为该账户启用 Macie。不允许 Macie 管理员为管理账户启用 Macie。
- 成员账户无法与 Macie 管理员账户取消关联。只有 Macie 管理员才能将账户移除为 Macie 成员账户。
- 如果 Macie 管理员移除了 Macie 成员账户，则该账户将继续启用 Macie。要同时暂停或停止使用 Macie，该账户的用户必须挂起（暂停）或禁用（停止）该账户的 Macie。

从基于邀请的组织过渡

如果您已通过使用 Macie 成员邀请将 Macie 管理员账户与成员账户相关联，我们建议您可以在 AWS Organizations中将该账户指定为组织的委派 Macie 管理员账户。这简化了从基于邀请的组织的过渡。

如果您这样做，则所有当前关联的成员账户都将继续成为成员。如果成员账户是您所在组织的一部分 AWS Organizations，则该账户的关联会自动从 “受邀请” 更改为 “ AWS Organizations在 Macie 中通过 V ia”。如果成员账户在 AWS Organizations中不属于您的组织，则该账户的关联仍为通过邀请。在这两种情况下，账户都将继续作为成员账户与委派的 Macie 管理员账户关联。

我们建议采用这种方法，因为一个账户不能同时与多个 Macie 管理员账户关联。如果您在中将其他帐户指定为组织的 Macie 管理员帐户 AWS Organizations，则指定的管理员将无法通过邀请管理已与其他 Macie 管理员帐户关联的帐户。每个成员账户必须首先与其当前的基于邀请的管理员账户解除关联。然后，在 AWS Organizations 中您组织的 Macie 管理员可以将该账户添加为 Macie 成员账户并开始管理该账户。

将 Macie 与 Macie 集成 AWS Organizations 并在 Macie 中配置组织后，您可以选择为该组织指定不同的 Macie 管理员帐户。您也可以继续使用邀请来关联和管理 AWS Organizations中不属于您的组织的成员账户。

在 Amazon Macie 中集成和配置组织

要开始将 Amazon Macie 与 AWS Organizations 一起使用，组织的 AWS Organizations 管理账户将指定一个账户作为该组织的委派 Macie 管理员账户。这将启用 Macie 作为 AWS Organizations 中的可信服务。它还为指定的管理员账户启用当前 AWS 区域中的 Macie，并允许指定的管理员账户为该区域组织中的其他账户启用和管理 Macie。有关如何授予这些权限的信息，请参阅 AWS Organizations 用户指南中的将 AWS Organizations 与其他 AWS 服务一起使用。

然后，委派的 Macie 管理员在 Macie 中配置组织，主要是通过添加该组织的账户作为该区域中的 Macie 成员账户。然后，管理员可以访问该区域中这些账户的某些 Macie 设置、数据和资源。

本主题说明如何为组织指定委托的 Macie 管理员以及如何添加该组织的账户作为 Macie 成员账户。在执行这些任务之前，请确保您了解管理员账户和成员账户之间的关系。查看将 Macie 与 AWS Organizations 一起使用的注意事项和建议也是一个好主意。

任务

- 第 1 步：验证权限
- 步骤 2：为组织指定委派的 Macie 管理员账户
- 步骤 3：自动启用并添加新组织账户作为 Macie 成员账户
- 步骤 4：启用并添加现有组织账户作为 Macie 成员账户

要在多个区域中整合和配置组织，AWS Organizations 管理账户和委派的 Macie 管理员会在每个其他区域中重复这些步骤。

第 1 步：验证权限

在为组织指定委派的 Macie 管理员账户之前，请确认您（作为 AWS Organizations 管理账户的用户）是否被允许执行以下 Macie 操作：`macie2:EnableOrganizationAdminAccount`。此操作允许您使用 Macie 为您的组织指定委派的 Macie 管理员账户。

另请验证您是否有权执行以下 AWS Organizations 操作：

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

这些操作允许您：检索有关您的组织的信息；将 Macie 与 AWS Organizations 集成；检索有关您已将哪些 AWS 服务与 AWS Organizations 集成的信息；以及为您的组织指定一个委托的 Macie 管理员账户。

要授予这些权限，请在您的账户的 AWS Identity and Access Management (IAM) policy 中包括以下语句：

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

如果您想要将您AWS Organizations的管理账户指定为组织的委派 Macie 管理员账户，您的账户还需要执行以下 IAM 操作的权限：`CreateServiceLinkedRole`。此操作允许您为管理账户启用 Macie。但是，基于 AWS 安全最佳实践和最低权限原则，我们不建议您这样做。

如果您决定授予此权限，请将以下语句添加到您的 AWS Organizations 管理账户的 IAM policy 中：

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

在语句中，将 *111122223333* 替换为管理账户的账户 ID。

如果要在某个选择加入型 AWS 区域（默认情况下被禁用的区域）中管理 Macie，则还要更新 `Resource` 元素和 `iam:AWSServiceName` 条件中的 Macie 服务主体值。该值必须指定该区域的区域代码。例如，要管理中东（巴林）区域（区域代码为 me-south-1）中的 Macie，请执行以下操作：

- 在 `Resource` 元素中，请将

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  替换为

  `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`

  其中 *111122223333* 指定了管理账户的账户 ID，*me-south-1* 指定了该区域的区域代码。
- 在 `iam:AWSServiceName` 条件中，请将 `macie.amazonaws.com` 替换为 `macie.me-south-1.amazonaws.com`，其中 *me-south-1* 指定了该地区的区域代码。

有关 Macie 当前可用区域的列表以及每个区域的区域代码，请参阅 AWS 一般参考 中的 Amazon Macie 端点和限额。有关选择加入型区域的信息，请参阅《AWS Account Management 参考指南》中的 Specifying which AWS 区域 your account can use。

步骤 2：为组织指定委派的 Macie 管理员账户

验证您的权限后，您（作为 AWS Organizations 管理账户的用户）可以为您的组织指定委派的 Macie 管理员账户。

为组织指定委派的 Macie 管理员账户

要为您的组织指定委派 Macie 管理员账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。只有 AWS Organizations 管理账户的用户才能执行此任务。

Console

请按照以下步骤操作，使用 Amazon Macie 控制台指定 Macie 委派管理员账户。

指定委派的 Macie 管理员账户

1. 使用 AWS Organizations 管理账户登录 AWS Management Console。

2. 通过使用页面右上角的 AWS 区域选择器，选择您要在其中为您的组织指定委派 Macie 管理员账户的区域。
3. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
4. 根据您的管理账户在当前区域中是否启用 Macie，执行以下操作之一：
   - 如果未启用 Macie，请在欢迎页面上选择开始使用。
   - 如果已启用 Macie，请在导航窗格中选择设置。
5. 在委托管理员下方，为要指定为 Macie 管理员账户的 AWS 账户输入 12 位数账户 ID。
6. 选择委托。

在您想要将组织与 Macie 集成的每个其他区域中重复上述步骤。您必须在每个区域中指定相同的 Macie 管理员账户。

API

要以编程方式指定委派的 Macie 管理员账户，请使用 Amazon Macie API 的 EnableOrganizationAdminAccount 操作。要在多个区域中指定账户，请为要在其中将您的组织与 Macie 集成的每个区域提交该指定。您必须在每个区域中指定相同的 Macie 管理员账户。

当您提交指定时，请使用所需 `adminAccountId` 参数为要指定为组织的 Macie 管理员账户的 AWS 账户指定 12 位账户 ID。另外，请务必指定该指定所适用的区域。

要通过使用 AWS Command Line Interface (AWS CLI) 指定 Macie 管理员账户，请运行 enable-organization-admin-account 命令。对于 `admin-account-id` 参数，请为要指定的 AWS 账户指定 12 位账户 ID。使用 `region` 参数指定该指定所适用的区域。例如：

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333
```

其中 *us-east-1* 是该指定适用的区域（美国东部（弗吉尼亚州北部）区域），*111122223333* 是要指定的账户的账户 ID。

为组织指定 Macie 管理员账户后，Macie 管理员便可以开始在 Macie 中配置组织。

步骤 3：自动启用并添加新组织账户作为 Macie 成员账户

默认情况下，在 AWS Organizations 中将新账户添加到您的组织时，不会自动为这些账户启用 Macie。此外，不会自动添加这些账户作为 Macie 成员账户。这些账户会显示在 Macie 管理员的账户

清单中。但是，不一定要为这些账户启用 Macie，Macie 管理员也不一定能访问这些账户的 Macie 设置、数据和资源。

如果您是该组织的委派 Macie 管理员，则可以更改组织的这个配置设置。如果您开启自动启用设置，则在 AWS Organizations 中将新账户添加到您的组织时，会自动为这些账户启用 Macie，并且这些账户将作为成员账户自动与您的 Macie 管理员账户关联。开启此设置不会影响组织中的现有账户。要为现有账户启用和管理 Macie，必须手动添加这些账户作为 Macie 成员账户。下一步介绍如何执行此操作。

> **Note**
>
> 如果您开启了自动启用设置，请注意以下例外情况：
>
> - 如果新账户已与其他 Macie 管理员账户关联，则 Macie 不会自动添加该账户作为组织中的成员账户。
>
> 该账户必须先取消与其当前 Macie 管理员账户的关联，然后才能在 Macie 中加入您的组织。然后，您可以手动添加该账户。要确定存在这种情况的账户，您可以为您的组织查看账户清单。
> - 如果您的组织达到了一个 AWS 区域中 10,000 个 Macie 成员账户的限额，则 Macie 会自动关闭该区域中的这一设置。
>
> 如果发生这种情况，我们会通过为您的 Macie 管理员账户创建 AWS Health 和 Amazon CloudWatch Events 来通知您。我们还会向与该账户关联的地址发送电子邮件。如果账户总数随后减少到少于 10,000 个账户，则 Macie 会自动再次开启该设置。

自动启用并添加新组织账户作为 Macie 成员账户

要自动启用并添加新账户作为 Macie 成员账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。只有组织委派的 Macie 管理员才能执行此任务。

Console

要使用控制台执行此任务，必须允许您执行以下 AWS Organizations 操作：`organizations:ListAccounts`。此操作允许您检索和显示有关组织中账户的信息。如果您拥有这些权限，请按照以下步骤自动启用并添加新组织账户作为 Macie 成员账户。

自动启用并添加新组织账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 通过使用页面右上角的 AWS 区域选择器，选择要在其中自动启用并添加新账户作为 Macie 成员账户的区域。
3. 在导航窗格中的设置下，选择账户。
4. 在账户页面上的添加账户旁边，打开自动启用设置。

在您想要在 Macie 中配置组织的每个其他区域中重复上述步骤。

要随后更改此设置以及停止自动启用并添加新账户，请重复上述步骤并关闭自动启用设置。

API

要以编程方式自动启用并添加新的 Macie 成员账户，请使用 Amazon Macie API 的 UpdateOrganizationConfiguration 操作。提交请求时，将 `autoEnable` 参数的值设置为 `true`。（默认值为 `false`。）另外，请务必指定您的请求适用的区域。要在其他区域中自动启用并添加新账户，请为每个其他区域提交请求。

如果您使用 AWS CLI 来提交请求，请运行 update-organization-configuration 命令并指定 `auto-enable` 参数以自动启用并添加新账户。例如：

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

其中 *us-east-1* 是自动在其中启用并添加新账户的区域，即美国东部（弗吉尼亚州北部）区域。

要随后更改此设置以及停止自动启用并添加新账户，请再次运行相同的命令并在每个适用区域中使用 `no-auto-enable` 参数，而不是 `auto-enable` 参数。

步骤 4：启用并添加现有组织账户作为 Macie 成员账户

在将 Macie 与 AWS Organizations 集成时，不会自动为组织中的所有现有账户启用 Macie。此外，这些账户不会作为 Macie 成员账户自动与委派的 Macie 管理员账户关联。

因此，在 Macie 中集成和配置组织的最后一步是添加现有组织账户作为 Macie 成员账户。当您添加现有账户作为 Macie 成员账户时，系统会自动为该账户启用 Macie，并且您（作为委派的 Macie 管理员）可以访问该账户的某些 Macie 设置、数据和资源。

请注意，您无法添加当前与其他 Macie 管理员账户关联的账户。要添加账户，请与账户所有者合作，以先取消该账户与其当前管理员账户的关联。此外，如果 Macie 当前被暂停使用现有账户，则无法添

加该账户。账户所有者必须先为账户重新启用 Macie。最后，如果您要添加 AWS Organizations 管理账户作业为成员账户，该账户的用户必须首先为该账户启用 Macie。

启用并添加现有组织账户作为 Macie 成员账户

要启用并添加现有组织账户作为 Macie 成员账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。只有组织委派的 Macie 管理员才能执行此任务。

Console

要使用控制台执行此任务，必须允许您执行以下 AWS Organizations 操作：`organizations:ListAccounts`。此操作允许您检索和显示有关组织中账户的信息。如果您拥有这些权限，请按照以下步骤启用并添加现有账户作为 Macie 成员账户。

启用并添加现有组织账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 通过使用页面右上角的 AWS 区域选择器，选择要在其中启用并添加现有账户作为 Macie 成员账户的区域。
3. 在导航窗格中的设置下，选择账户。

   账户页面将打开并显示与您的 Macie 账户关联的账户表。如果账户属于 AWS Organizations 中的组织，则其类型为通过 AWS Organizations。如果账户不是 Macie 成员账户，则其状态为非成员。
4. 在账户表中，为要添加作为 Macie 成员账户的每个账户选中复选框。

   > **Tip**
   >
   > 要更轻松地识别要添加的账户，您可以筛选表。为此，请将光标放在表上方的筛选框中，然后选择状态。然后选择状态 = 非成员。
5. 在操作菜单上，选择添加成员。
6. 确认您要添加所选账户作为成员账户。

在确认添加所选账户后，账户的状态将更改为正在创建/正在启用，然后更改为已启用。

在您想要在 Macie 中配置组织的每个其他区域中重复上述步骤。

API

要以编程方式启用并添加一个或多个现有账户作为 Macie 成员账户，请使用 Amazon Macie API 的 CreateMember 操作。提交请求时，请使用支持的参数指定要启用并添加的每个 AWS 账户的 12 位数账户 ID 和电子邮件地址。此外，请指定请求适用的区域。要在其他区域中启用并添加现有账户，请提交每个其他区域的请求。

要检索待启用并添加的 AWS 账户的账户 ID 和电子邮件地址，您可以选择使用 Amazon Macie API 的 ListMembers 操作。此操作提供有关与您的 Macie 账户关联的账户的详细信息，包括非 Macie 成员账户的账户。如果账户`relationshipStatus`属性的值不是`Enabled`，则该账户不是 Macie 成员账户。

要通过使用 AWS CLI 来启用并添加一个或多个现有账户，请运行 create-member 命令。使用`region`参数指定要在其中启用并添加账户的区域。使用`account`参数指定要添加的每个 AWS 账户的账户 ID 和电子邮件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

其中 *us-east-1* 是要在其中启用并添加账户作为 Macie 成员账户的区域（美国东部（弗吉尼亚州北部）区域），`account`参数为该账户指定账户 ID (*123456789012*) 和电子邮件地址 (*janedoe@example.com*)。

如果您的请求成功，则指定账户的状态 (`relationshipStatus`) 将更改为您的账户清单中的`Enabled`。

查看组织的 Amazon Macie 账户

AWS Organizations 组织在 Amazon Macie 中集成和配置完成后，其委派的 Macie 管理员可以在 Macie 中访问该组织账户的清单。作为组织的 Macie 管理员，您可以使用此清单查看组织 Macie 账户在 AWS 区域 中的统计数据和详细信息。您还可以使用此清单来管理某个地区的 Macie 会员账户。

查看组织的 Macie 账户

您可以使用 Amazon Macie 控制台或 Amazon Macie API 查看组织的账户。

Console

按照以下步骤使用 Amazon Macie 控制台查看组织的 Macie 账户。

要查看组织的账户

1. 通过以下网址打开 Amazon Macie 控制台： https://console.aws.amazon.com/macie/。
2. 通过使用页面右上角的 AWS 区域 选择器，选择要在其中查看组织账户的区域。
3. 在导航窗格中的设置下，选择账户。

账户页面将打开并显示汇总统计数据以及与当前 AWS 区域 中的 Macie 账户关联的账户表。

在账户页面的顶部，您可以找到以下汇总统计数据。

经由 AWS Organizations

活动报告通过 AWS Organizations 与您的账户关联的账户总数，这些账户目前是您组织中的 Macie 成员账户。已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员。

所有报告通过 AWS Organizations 与您的账户关联的账户总数，包括当前不是 Macie 成员账户的账户。

通过邀请

活动报告通过 Macie 邀请与您的账户关联的账户总数，并且这些账户目前是 Macie 成员账户。（这些账户未通过 AWS Organizations 与您的账户关联。）已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员，因为他们接受了您的成员资格邀请。

所有报告通过 Macie 邀请与您的账户关联的账户总数，包括尚未回复您的邀请的账户。

活动/全部

活动报告您账户当前通过 AWS Organizations 或 Macie 邀请成为 Macie 成员账户的账户总数。已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员。

所有报告通过 AWS Organizations 或 Macie 邀请与您的账户关联的账户总数。这包括属于您的组织在 AWS Organizations 中但目前不是 Macie 成员账户的账户，以及任何尚未回复您的 Macie 会员邀请的账户。

在表中，您将找到有关当前区域中每个账户的详细信息。该表包含通过 AWS Organizations 或 Macie 邀请与您的 Macie 账户关联的所有账户。

账户 ID

AWS 账户 的账户 ID 和电子邮件地址。

名称

AWS 账户 的账户名称。对于通过 Macie 邀请与您的账户关联的账户，此值通常为不适用。

类型

账户如何与您的账户关联，通过 AWS Organizations 或通过 Macie 邀请。

状态

您的账户与该账户之间的关系状态。对于 AWS Organizations 组织中的账户（类型为 经由 AWS Organizations），可能的值为：

- 账户已挂起 – AWS 账户 已挂起。
- 已创建/启用 - Macie 正在处理启用该账户并将其添加为 Macie 成员账户的请求。
- 已启用 – 该账户是 Macie 成员账户。已为该账户启用 Macie，并且您是该账户的 Macie 管理员。
- 不是会员 – 该账户是您所在组织在 AWS Organizations 中的一部分，但不是 Macie 成员账户。
- 已暂停（已挂起） – 该账户是 Macie 成员账户，但 Macie 目前对该账户已挂起。
- 已禁用区域 – 该账户是您所在组织在 AWS Organizations 中的一部分，但当前区域已对 AWS 账户 被禁用。
- 已移除（已解除关联） – 该账户以前是 Macie 成员账户，但后来作为成员账户被移除。您取消该账户与 Macie 管理员账户的关联。Macie 继续为该账户启用。

上次操作

当您或关联的账户最近执行了影响您账户之间关系的操作时。

要按特定字段对表格进行排序，请点击该字段的列标题。若要更改排序顺序，请再次点击列标题。若要筛选表，请将光标放在筛选条件框中，然后为字段添加筛选条件。若要进一步优化结果，请为其他字段添加筛选条件。

API

要以编程方式查看组织的账户，请使用 Amazon Macie API 的 ListMembers 操作，并确保指定您的请求适用的区域。要查看其他区域中的账户，请在每个其他区域提交您的请求。

提交请求时，请使用 `onlyAssociated` 参数指定要包含在响应中的账户。默认情况下，Macie 仅返回指定区域中通过 AWS Organizations 或 Macie 邀请成为 Macie 成员账户的那些账户的详

细信息。要检索所有与 Macie 账户关联的账户（包括非成员账户）的详细信息，请在请求中包含 onlyAssociated 参数，并将该参数的值设置为 false。

要使用 AWS Command Line Interface (AWS CLI) 查看组织的账户，请运行 list-members 命令。对于 only-associated 参数，指定是包括所有关联账户还是仅包含 Macie 成员账户。要仅包含成员账户，请省略此参数或将参数的值设置为 true。要包括所有账户，请将此值设置为 false。例如：

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

其中 *us-east-1* 是请求适用的区域，即美国东部（弗吉尼亚州北部）区域。

如果请求成功，Macie 将返回一个 members 数组。该数组包含满足请求中指定标准的每个账户的 member 对象。在该对象中，relationshipStatus 字段指示您的账户与指定区域中的其他账户之间的关联的当前状态。对于 AWS Organizations 组织中的账户，可能的值为：

- AccountSuspended – AWS 账户 已挂起。
- Created – Macie 正在处理启用该账户并将其添加为 Macie 成员账户的请求。
- Enabled – 该账户是 Macie 成员账户。已为该账户启用 Macie，并且您是该账户的 Macie 管理员。
- Paused – 该账户是 Macie 成员账户，但 Macie 当前对该账户已挂起（暂停）。
- RegionDisabled – 该账户是您所在组织在 AWS Organizations 中的一部分，但当前区域已对 AWS 账户 被禁用。
- Removed – 该账户以前是 Macie 成员账户，但后来作为成员账户被移除。您取消该账户与 Macie 管理员账户的关联。Macie 继续为该账户启用。

有关 member 对象中其他字段的信息，请参阅 Amazon Macie API 参考中的成员。

管理组织的 Amazon Macie 成员账户

在 Amazon Macie 中集成和配置AWS Organizations组织后，该组织委派的 Macie 管理员可以访问成员账户的某些 Macie 设置、数据和资源。

作为组织的 Macie 管理员，您可以在 Macie 中集中执行某些账户管理任务。例如：

- 添加和删除 Macie 成员账户。

- 管理个人账户的 Macie 状态，例如为账户启用或暂停 Macie
- 监控 Macie 配额以及个人账户和整个组织的估算使用成本

您还可以查看 Macie 成员账户的 Amazon Simple Storage Service (Amazon S3) 库存数据和策略调查发现。此外，您还可以在账户拥有的 S3 存储桶中发现敏感数据。有关您可以执行的任务的详细列表，请参阅了解 Amazon Macie 管理员和成员账户之间的关系。

默认情况下，Macie 允许您查看组织中所有 Macie 成员账户的相关数据和资源。您还可以深入查看个人账户的数据和资源。例如，如果您使用摘要控制面板来评测组织的 Amazon S3 安全状况，则可以按账户筛选数据。同样，如果您监控估算使用成本，则可以访问个人成员账户的估算费用明细。

除了管理员和成员账户常见的任务外，您还可以为组织执行各种管理任务。

任务

- 向组织添加 Amazon Macie 成员账户
- 暂停组织成员账户的 Amazon Macie
- 从组织中删除 Amazon Macie 成员账户

作为组织的 Macie 管理员，您可以使用 Amazon Macie 控制台或 Amazon Macie API 来执行这些任务。如果您更喜欢使用控制台，请注意必须允许您执行以下 AWS Organizations 操作：`organizations:ListAccounts`。此操作允许您检索和显示有关 AWS Organizations 中属于您的组织的账户的信息。

向组织添加 Amazon Macie 成员账户

在部分情况下，您可能需要手动添加账户作为 Macie 成员账户。对于您之前作为成员账户删除（取消关联）的账户，情况就是这样。如果您没有将 Macie 配置为在 AWS Organizations 中向您的组织中添加账户时自动启用和添加新账户作为成员账户，也会出现这种情况。

当您将账户添加为 Macie 成员账户时，如果该区域尚未启用 Macie，则会为当前 AWS 区域 中启用 Macie，并且该账户作为该地区的成员账户与您的 Macie 管理员账户关联。成员账户不会收到您在账户之间建立这种关系的邀请或其他通知。

请注意，您无法添加已与另一个 Macie 管理员账户关联的账户。该账户必须先解除与其当前管理员账户的关联。此外，除非管理账户已为该账户启用 Macie，否则您无法将 AWS Organizations 管理账户添加为成员账户。要了解其他要求，请参阅使用 Amazon Macie 的注意事项和建议 AWS Organizations。

将 Macie 成员账户添加到组织

要将一个或多个 Macie 成员账户添加到您的组织，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台添加一个或多个 Macie 成员账户。

添加 Macie 会员账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中添加成员账户的区域。
3. 在导航窗格中的 Settings 下，选择 Accounts。账户页面打开并显示与您的账户关联的账户表。
4. （可选）要更轻松地识别 AWS Organizations 中属于您的组织但不是 Macie 成员账户的账户，请使用表格上方的筛选框添加以下筛选条件：

   - 类型 = 组织
   - 状态 = 不是会员

   要同时显示您之前删除并可能想要添加为成员账户的账户，还需要添加状态 = 已删除筛选条件。
5. 在 账户表中，选中要添加为成员账户的每个账户的复选框。
6. 在操作菜单上，选择添加成员。
7. 确认要将选定数量的账户添加为会员账户。

确认选择后，账户清单中选定账户的状态将更改为 已创建/启用，然后更改为启用。

在您要在其中添加成员账户的每个附加区域中重复上述步骤。

API

要以编程方式添加一个或多个 Macie 成员账户，请使用 Amazon Macie API 的 CreateMember 操作。

提交请求时，请使用支持的参数为您要添加的每个 AWS 账户 指定 12 位数的账户 ID 和电子邮件地址。此外，请指定请求适用的区域。要在其他地区添加账户，请在每个其他地区提交您的申请。

要检索要添加的账户的账户 ID 和电子邮件地址，您可以将 AWS Organizations API 的 ListAccounts 操作的输出与 Amazon Macie API 的 ListMembers 操作的输出关联起来。对于 Macie API 的 ListMembers 操作，请在请求中包含 `onlyAssociated` 参数并将参数的值设置为 `false`。如果操作成功，Macie 将返回一个 `members` 数组，该数组提供指定区域中与您的 Macie 管理员账户关联的所有账户的详细信息，包括当前不是成员账户的账户。注意数组中的以下内容：

- 如果某个账户的 `relationshipStatus` 属性值不是 `Enabled`，则该账户与你的账户相关联，但它不是 Macie 成员账户。
- 如果某个账户未包含在数组中，但包含在 AWS Organizations API 的 ListAccounts 操作的输出中，则该账户是 AWS Organizations 中您的组织的一部分，但它与您的账户无关联，因此不是 Macie 成员账户。

要使用 AWS CLI 添加成员账户，请运行 create-member 命令。使用 `region` 参数指定要在其中添加账户的区域。使用 `account` 参数为要添加的每个账户指定账户 ID 和电子邮件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

其中 *us-east-1* 是将账户添加为成员账户的区域（美国东部（弗吉尼亚州北部）区域），而 `account` 参数为账户指定账户 ID (*123456789012*) 和电子邮件地址 (*janedoe@example.com*)。

如果您的请求成功，则指定账户的状态 (`relationshipStatus`) 将更改为您的账户清单中的`Enabled`。

暂停组织成员账户的 Amazon Macie

作为 AWS Organizations 中组织的 Macie 管理员，您可以暂停组织成员账户的 Macie。如果你这样做，您也可以在以后为该账户重新启用 Macie。

当您暂停成员账户的 Macie 时：

- 在当前 AWS 区域 中，Macie 无法访问该账户的 Amazon S3 数据，并停止提供有关该账户的 Amazon S3 数据的元数据。
- Macie 停止在该区域中为账户执行所有活动。这包括监控 S3 存储桶的安全性和访问控制、执行自动敏感数据发现，以及运行当前正在进行的敏感数据发现作业。
- Macie 会取消该账户在该区域创建的所有敏感数据发现作业。作业取消后无法恢复或重新启动。

如果您创建的作业是为了分析成员账户拥有的数据，Macie 不会取消您的作业。相反，这些作业会跳过该账户拥有的资源。

账户被暂停后，Macie 会在相应区域保留该账户的 Macie 会话标识符、设置和资源。例如，该账户的调查发现保持不变，最长可在 90 天内不受影响。当 Macie 在适用区域的账户被暂停使用时，您的组织不会对该区域的账户产生 Macie 费用。

暂停组织中成员账号的 Macie

要暂停组织中成员账户的 Macie，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台暂停成员账户的 Macie。

暂停成员账户的 Macie

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中暂停成员账户的 Macie 的区域。
3. 在导航窗格中的 Settings 下，选择 Accounts。
4. 在账户表中，选中要暂停的账户的复选框。
5. 在操作菜单上，选择暂停 Macie。
6. 确认您要暂停该账户的 Macie。

确认暂停后，账户清单中的账户状态会更改为已暂停（已挂起）。

在要暂停账户 Macie 的每个附加区域中重复上述步骤。

API

要以编程方式暂停成员账户的 Macie，请使用 Amazon Macie API 的 UpdateMemberSession 操作。

提交请求时，请使用 `id` 参数为要暂停 Macie 的 AWS 账户 指定 12 位数的账户 ID。对于 `status` 参数，将 PAUSED 指定为 Macie 账户的新状态。此外，请指定请求适用的区域。要在其他区域暂停账户，请在每个其他区域提交您的申请。

要检索要暂停的账户的账户 ID，您可以使用 Amazon Macie API 的 ListMembers 操作。如果执行此操作，请考虑通过在请求中包含 `onlyAssociated` 参数来筛选结果。如果将此参数的值设置为

true，则 Macie 将返回一个 members 数组，该数组仅提供有关当前为成员账户的账户的详细信息。

要使用 AWS CLI 暂停成员账户的 Macie，请运行 update-member-session 命令。使用 region 参数指定要暂停 Macie 的区域，并使用 id 参数指定要暂停 Macie 的 AWS 账户 的账户 ID。对于 status 参数，请指定 PAUSED。例如：

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

其中 *us-east-1* 是要暂停 Macie 的区域（美国东部（弗吉尼亚州北部）区域），而 *123456789012* 是要暂停 Macie 的账户的账户 ID，PAUSED 是该账户的 Macie 的新状态。

如果请求成功，Macie 将返回空响应，并且指定账户的状态将在账户清单中更改为 Paused。

从组织中删除 Amazon Macie 成员账户

如果您想停止访问成员账号的 Macie 设置、数据和资源，可以将该账户作为 Macie 成员账号移除。为此，请取消该账户与 Macie 管理员账户的关联。请注意，只有您才能为成员账户执行此操作。AWS Organizations 成员账户无法与其 Macie 管理员账户取消关联。

当您移除 Macie 成员账户时，Macie 在当前 AWS 区域 中仍处于启用状态。但是，该账户已与您的 Macie 管理员账户取消关联，它成为独立的 Macie 账户。这意味着您将无法访问该账户的所有 Macie 设置、数据和资源，包括该账户 Amazon S3 数据的元数据和策略调查发现。这也意味着您无法再使用 Macie 发现账户拥有的 S3 存储桶中的敏感数据。如果您已经创建了敏感的发现作业来执行此操作，则这些作业会跳过该账户拥有的存储桶。

移除 Macie 成员账户后，该账户将继续出现在您的账户库存中。Macie 不会通知账户所有者您已删除该账户。

从组织中删除 Macie 成员账户

要从您的组织中移除 Macie 成员账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 主机删除 Macie 会员账户。

移除 Macie 会员账号

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/

2. 使用页面右上角的 AWS 区域 选择器，选择要删除成员账户的区域。
3. 在导航窗格中的 Settings 下，选择 Accounts。
4. 在 账户表中，选中要删除为成员账户的每个账户的复选框。
5. 在操作菜单上，选择取消关联账户。
6. 确认您要作为成员账户移除的选定账户。

确认选择后，账号清单中的账号状态会更改为已移除（已解除关联）。

在您要移除成员账户的每个附加区域中重复上述步骤。

API

要以编程方式移除 Macie 成员账户，请使用 Amazon Macie API 的 DisassociateMember 操作。

提交请求时，请使用 `id` 参数为要移除的成员账户指定 12 位数的 AWS 账户 ID。此外，请指定请求适用的区域。要移除其他区域的账户，请在每个其他区域提交您的申请。

要检索要移除的成员账户的账户 ID，您可以使用 Amazon Macie API 的 ListMembers 操作。如果执行此操作，请考虑通过在请求中包含 `onlyAssociated` 参数来筛选结果。如果将此参数的值设置为 `true`，则 Macie 将返回一个 `members` 数组，该数组仅提供有关当前是 Macie 成员账户的账户的详细信息。

要使用 AWS CLI 移除 Macie 成员账户，请运行 disassociate-member 命令。使用 `region` 参数指定要移除账户的区域。使用 `id` 参数为要移除的成员账户指定账户 ID。例如：

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要移除账户的区域（美国东部（弗吉尼亚州北部）区域），*123456789012* 是要移除的账户的账户 ID。

如果请求成功，Macie 将返回空响应，并且指定账户的状态将在账户清单中更改为 `Removed`。

为组织指定不同的 Amazon Macie 管理员账户

在 Amazon Macie 中整合并配置 AWS Organizations组织后， AWS Organizations 管理账户可以将不同的账户指定为该组织委派的 Macie 管理员账户。

作为组织 AWS Organizations 管理账户的用户，在为组织指定其他 Macie 管理员帐户之前，请先验证自己是否满足以下权限要求：

- 您必须拥有最初为您的组织指定 Macie 管理员账户所需的相同权限。还必须允许您执行以下 AWS Organizations 操作:`organizations:DeregisterDelegatedAdministrator`. 此附加操作允许您删除当前指定。
- 如果您的账户目前是 Macie 成员账户，则当前 Macie 管理员必须将您的账户移除为 Macie 成员账户。否则，您将无法访问用于指定其他管理员账户的 Macie 操作。在您指定新的管理员账户后，新的 Macie 管理员可以再次将您的账户添加为 Macie 成员账户。

如果您的组织在多个区域中使用 Macie AWS 区域，还要确保在组织使用 macie 的每个区域中更改委托的 Macie 管理员帐户，所有这些区域中委托的 Macie 管理员帐户必须相同。如果您在中管理多个组织 AWS Organizations，另请注意，一个账户一次只能是为一个组织委托的 Macie 管理员帐户。要了解其他要求，请参阅使用 Amazon Macie 的注意事项和建议 AWS Organizations。

为组织指定不同的 Macie 管理员账户

要为您的组织指定不同的 Macie 管理员账户，您可以使用亚马逊 Macie 控制台或亚马逊 Macie 和 API 的组合。 AWS Organizations 只有 AWS Organizations 管理账户的用户才能更改其组织的名称。

Console

要使用 Amazon Macie 控制台更改指定，请遵循以下步骤。

指定不同的 Macie 管理员账户

1. AWS Management Console 使用您的 AWS Organizations 管理账户登录。
2. 使用页面右上角的选择 AWS 区域 器，选择要更改名称的区域。
3. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
4. 根据您的管理账户在当前区域中是否启用 Macie，执行以下操作之一：
   - 如果未启用 Macie，请在欢迎页面上选择开始使用。
   - 如果已启用 Macie，请在导航窗格中选择设置。
5. 在指定管理员下，选择移除。要更改指定，必须先删除当前指定。
6. 确认您要删除当前指定。
7. 在 “委托管理员” 下，输入 12 位数的账户 ID AWS 账户 ，以指定为该组织的新 Macie 管理员账户。
8. 选择 Delegate（委派）。

在您将 Macie 与 AWS Organizations集成的每个其他区域中重复上述步骤。

API

要以编程方式更改名称，您需要使用 Amazon Macie API 的两个操作和一个 API 的操作。 AWS Organizations 这是因为在提交新名称 AWS Organizations 之前，您必须移除 Macie 中的当前名称。

要删除当前指定：

1. 使用 Macie API 的DisableOrganizationAdminAccount操作。在必填adminAccountId参数中，为当前被指定为组织的 Macie 管理员账户指 AWS 账户 定 12 位数的账户 ID。
2. 使用 AWS Organizations API 的DeregisterDelegatedAdministrator操作。在必填 AccountId 参数中，为当前被指定为组织 Macie 管理员账户的账户指定 12 位数的账户 ID。此值应与您在之前的 Macie 请求中指定的账户 ID 相匹配。对于 ServicePrincipal 参数，指定 Macie 服务主体 (macie.amazonaws.com)。

删除当前名称后，使用 Macie API 的EnableOrganizationAdminAccount操作提交新的名称。在必填adminAccountId参数中，指定 12 位数的帐户 ID， AWS 账户 以指定为该组织的新 Macie 管理员帐户。

要使用更改名称 AWS CLI，请运行 Macie API 的disable-organization-admin-account命令和 API 的deregister-delegated-administrator AWS Organizations 命令。这些命令分别删除 Macie 和 AWS Organizations中的当前名称。在admin-account-id和account-id参数中，指定 AWS 账户 要删除的 12 位数帐户 ID 作为当前 Macie 管理员帐户。使用 region 参数指定移除所适用的区域。例如：

```
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
```

其中：

- *us-east-1* 是删除适用的区域，即美国东部（弗吉尼亚州北部）区域。
- *111122223333* 是要作为 Macie 管理员账户删除的账户的账户 ID。
- macie.amazonaws.com 是 Macie 的服务主体。

移除当前名称后，运行 Macie API 的enable-organization-admin-account命令提交新的名称。在admin-account-id参数中，指定 12 位数的帐户 ID， AWS 账户 以指定为该组织的新 Macie 管理员帐户。使用 region 参数指定该指定所适用的区域。例如：

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

其中 *us-east-1* 是该指定适用的区域（美国东部（弗吉尼亚州北部）区域），*444455556666* 是指定为新 Macie 管理员账户的账户 ID。

禁用 Amazon Macie 与 AWS Organizations 的集成

AWS Organizations 组织与 Amazon Macie 集成后，AWS Organizations 管理账户随后可以禁用该集成。作为 AWS Organizations 管理账户的用户，您可以通过在 AWS Organizations 中禁用可信服务访问权限来实现此目的。

当您禁用 Macie 的可信服务访问权限时，会出现以下情况：

- Macie 失去其作为 AWS Organizations 中可信任服务的状态。
- 该组织的 Macie 管理员账户无法访问所有 AWS 区域 中的所有Macie 成员账户的所有 Macie 设置、数据和资源。
- 所有 Macie 成员账户都将成为独立的 Macie 账户。如果在一个或多个区域为成员账户启用 Macie，则这些地区的账户将继续启用 Macie。但是，该账户不再与任何地区的 Macie 管理员账户关联。

有关禁用受信任服务访问的结果的其他信息，请参阅 AWS Organizations 用户指南中的与其他 AWS 服务 一起使用 AWS Organizations。

禁用 Macie 的信任服务访问权限

要禁用信任服务访问权限，您可以使用 AWS Organizations 控制台或 AWS Organizations API。只有 AWS Organizations 管理账户的用户，可以禁用 Macie 的可信服务访问权限。有关所需权限的详细信息，请参阅 AWS Organizations 用户指南中的禁用可信访问所需的权限。

在禁用可信服务访问权限之前，可以选择与组织指定的 Macie 管理员合作，暂停或禁用成员账户的 Macie，并清理这些账户的 Macie 资源。

Console

要使用 AWS Organizations 控制台禁用可信服务访问权限，请按照以下步骤操作。

禁用信任服务访问权限

1. 使用 AWS Organizations 管理账户登录 AWS Management Console。

2. 访问 https://console.aws.amazon.com/organizations/ 并打开 AWS Organizations 控制台。
3. 在导航窗格中，选择服务。
4. 在集成服务下，选择 Amazon Macie。
5. 选择 Disable trusted access (禁用信任访问权限)。
6. 确认您要禁用可信访问权限。

API

要以编程方式禁用可信服务访问权限，请使用 AWS Organizations API 的 DisableAWSServiceAccess 操作。对于 `ServicePrincipal` 参数，指定 Macie 服务主体 (`macie.amazonaws.com`)。

要使用 AWS Command Line Interface (AWS CLI) 禁用可信服务访问权限，请运行 AWS Organizations API 的 disable-aws-service-access 命令。对于 `service-principal` 参数，指定 Macie 服务主体 (`macie.amazonaws.com`)。例如：

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

通过邀请管理 Amazon Macie 账户

您可以通过两种方式集中管理多个 Amazon Macie 账户，即通过 AWS Organizations集成 Macie 或使用成员邀请。如果您使用成员邀请，则指定的 Macie 管理员最多可管理 1,000 个 Macie 账户。管理员还可以访问 Amazon Simple Storage Service (Amazon S3) 清单数据，并发现账户的 S3 存储桶中有敏感数据。有关管理员可执行任务的详细信息，请参阅 了解 Amazon Macie 管理员和成员账户之间的关系。

在基于邀请的组织中，您可以通过在 Macie 中发送和接受成员邀请，将 Macie 账户相互关联。如果您发送邀请并被另一账户接受，则您将成为另一个账户的 Macie 管理员，而另一个账户将成为您组织的成员账户。如果您收到和接受邀请，则您的账户成为成员账户，Macie 管理员可访问您账户中指定的 Macie 设置、数据和资源。

> **Tip**
>
> 如果您在 Macie 中创建基于邀请的组织，则随后可以改为使用AWS Organizations。您也可以同时使用这两种方法管理多个 Macie 账户。例如，如果您的 AWS 环境中包含测试账户，则可通过AWS Organizations将这些账户从您的组织中排除，并通过邀请单独管理它们。

本节介绍了如何创建和参与基于邀请的组织以及如何为组织执行各类管理任务。

主题

Amazon Macie 中基于邀请的组织的注意事项和建议

在 Amazon Macie 中创建或开始管理基于邀请的组织之前，请考虑以下要求和建议。此外还应确保您了解 Macie 管理员账户和成员账户之间的关系。

主题

选择 Macie 管理员账号

在确定哪个账户应为组织的 Macie 管理员账户时，请记住以下几点：

- 一个组织只能有一个 Macie 管理员账户。
- 一个账户不能同时是 Macie 管理员账户和成员账户。

- Macie 是一项区域性服务。这意味着 Macie 管理员账户和成员账户之间的关联是区域性的，关联仅存在于发送和接受邀请的 AWS 区域 中。例如，如果 Macie 管理员向美国东部（弗吉尼亚州北部）区域发送邀请并且这些邀请被接受，Macie 管理员只能管理该区域中的成员账户。

  要集中管理多个 AWS 区域 中的 Macie 账户，Macie 管理员可以登录到组织当前使用或将要使用 Macie 的每个区域，并向每个区域中的适当账户发送邀请。有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。
- 一个成员账户一次只能与一个 Macie 管理员账户关联。如果您的组织在多个区域使用 Macie，则在所有这些区域中的 Macie 管理员账户必须相同。但是，管理员和成员账户必须在每个地区分别发送和接受邀请。
- 如果 Macie 管理员的 AWS 账户 账户被暂停、隔离或关闭，则所有关联的成员账户都将自动从成员账户移除，但这些账户继续启用 Macie。

发送邀请和管理 Macie 成员账号

作为基于邀请的组织的 Macie 管理员，在组织中发送邀请和管理账户时，请记住以下几点：

- 如果您发送邀请，相关数据可能会在 AWS 区域 中传输。之所以如此，是因为 Macie 使用仅在美国东部（弗吉尼亚州北部）地区运营的电子邮件验证服务来验证接收账户的电子邮件地址。
- 您可以向任何活跃 AWS 账户 发送邀请，包括尚未启用 Macie 的账户。但是，要接受或拒绝邀请，您必须在发出邀请的地区启用 Macie。
- 一个 Macie 管理员账户在每个 AWS 区域 中能与不超过 1,000 个账户相关联。这包括尚未回复邀请的账户。如果您的账户满足此配额，则在您删除必要数量的关联账户、收到必要数量的已拒绝邀请或两者结合之前，您无法添加或邀请其他账户。

  要确定当前有多少账户与您的账户关联，您可以使用 Amazon Macie 控制台上的账户页面或 Amazon Macie API 的 ListMembers 操作。有关更多信息，请参阅查看基于邀请的组织的 Amazon Macie 账户。
- 一个账户一次只能与一个 Macie 管理员账户关联。这意味着如果一个账户已经与另一个 Macie 管理员账户关联，则该账户将无法接受您的邀请。该账户必须先解除与其当前 Macie 管理员账户的关联。
- 在基于邀请的组织中，成员账户可以随时取消与其 Macie 管理员账户的关联。如果发生这种情况，则该账户将继续启用 Macie，该账户将变为独立的 Macie 账户。如果成员账户与您的管理员账户取消关联，Macie 不会通知您。但是，该账户会继续出现在您的账户库存中，并且其状态为成员已退出。
- 如果从组织中删除成员账户，Macie 将继续为该账户启用，并且该账户将成为独立的 Macie 账户。

回复和管理成员邀请

作为邀请的接收者或基于邀请的组织的成员，在回复和管理收到的邀请时，请记住以下几点：

- 在接受邀请之前，请确保您了解 Macie 管理员账户和成员账户之间的关系。
- 您的账户一次只能与一个 Macie 管理员账户关联。如果您接受邀请并随后想加入其他组织（通过邀请或通过 AWS Organizations），则必须先取消您的账户与其当前 Macie 管理员账户的关联。然后，您可以加入另一个组织。
- 要接受或拒绝邀请，您必须在发出邀请的 AWS 区域 中启用 Macie。发送邀请的账户无法在该地区为您启用 Macie。拒绝邀请是可选的。如果您拒绝邀请，则可以选择在拒绝邀请后在适用的地区禁用 Macie。
- 如果您是 Macie 管理员，则不能接受成为成员账户的邀请，一个账户不能同时是 Macie 管理员和成员账户。要成为成员账户，您必须先从当前组织中移除所有成员账户，从而取消账户与其所有成员账户的关联。
- Macie 是一项区域性服务。如果接受邀请，则您的账户与 Macie 管理员账户之间的关联是区域性的 - 该关联仅存在于发送邀请并接受邀请的 AWS 区域 中。
- 如果您在多个区域中使用 Macie，则您的账户的 Macie 管理员账户必须在所有这些区域中相同。但是，Macie 管理员必须在每个区域分开向您发送邀请，并且您必须在每个区域分别接受邀请。
- 您可以随时取消您的账户与 Macie 管理员账户的关联。如果您这样做，Macie 将继续为您的账户启用，您的账户将成为一个独立的 Macie 账户。
- 如果 Macie 管理员将您的账户从其组织中删除，Macie 将继续为您的账户启用，并且您的账户将成为独立的 Macie 账户。

转换为 AWS Organizations

在 Macie 中创建基于邀请的组织后，您可以转换为使用 AWS Organizations。为了简化过渡，我们建议您将现有的基于邀请的管理员账户指定为 AWS Organizations 中组织的 Macie 管理员账户。

如果您这样做，则所有当前关联的成员账户都将继续成为成员。如果成员账户在 AWS Organizations 中属于组织，则该账户的关联在 Macie 中会自动从通过邀请更改为经由AWS Organizations。如果成员账户在 AWS Organizations 中不属于组织，则该账户的关联仍为通过邀请。在这两种情况下，账户都将继续作为成员账户与 Macie 管理员账户关联。

我们建议使用这种方法，因为一个成员账户一次只能与一个 Macie 管理员账户相关联。如果您在 AWS Organizations 中将其他账户指定为组织的 Macie 管理员账户，则指定的管理员将无法通过邀请管理已与其他 Macie 管理员账户关联的账户。每个成员账户必须首先与其当前的基于邀请的管理员账户解除

关联。只有这样，AWS Organizations 组织的 Macie 管理员才能将该成员账户添加到其组织中，并开始管理该账户的 Macie。

将 Macie 与 AWS Organizations 集成并在 Macie 中配置组织后，您可以选择为该组织指定不同的 Macie 管理员账户。您也可以继续使用邀请来关联和管理 AWS Organizations 中不属于您的组织的成员账户。

在 Amazon Macie 中创建和管理基于邀请的组织

要在 Amazon Macie 中创建基于邀请的组织，您首先要确定要使用哪个账户作为该组织的 Macie 管理员账户。然后，您可以使用该账户添加成员账户 – 向其他 AWS 账户 发送成员资格邀请，邀请这些账户作为当前 AWS 区域 的 Macie 成员账户加入组织。要在多个区域中创建组织，请从其他账户当前或将要使用 Macie 的每个区域发送成员资格邀请。

账户接受邀请后，就会成为 Macie 成员账户，并与相应地区的 Macie 管理员账户相关联。然后，Macie 管理员账户就可以访问该区域中成员账户的某些 Macie 设置、数据和资源。

作为基于邀请的组织的 Macie 管理员，您可以查看成员账户的 Amazon Simple Storage Service (Amazon S3) 清单数据和策略调查发现。您还可以执行自动敏感数据发现并运行敏感数据发现作业，以检测成员账户拥有的 S3 存储桶中的敏感数据。有关您可执行的任务的详细列表，请参阅 了解 Amazon Macie 管理员和成员账户之间的关系。

默认情况下，Macie 可让您查看整个组织的相关数据和资源。您还可以深入查看组织内各个账户的数据和资源。例如，如果您使用摘要控制面板来评测组织的 Amazon S3 安全状况，则可以按账户筛选数据。同样，如果您监控估算使用成本，则可以访问个人成员账户的估算费用明细。

除了管理员和成员账户共有的任务外，您还可以为组织集中执行各种管理任务。在执行这些任务之前，最好先查看一下在 Macie 中管理基于邀请的组织的注意事项和建议。

任务

- 将 Amazon Macie 成员账户添加到基于邀请的组织
- 暂停使用基于邀请的组织中的成员账户的 Amazon Macie
- 从基于邀请的组织中删除 Amazon Macie 成员账户
- 删除与其他账户的关联

将 Amazon Macie 成员账户添加到基于邀请的组织

作为基于邀请的组织的 Macie 管理员，您可以通过执行两个主要步骤将成员账户添加到您的组织：

1. 将账户添加到 Macie 的账户清单中。这会将账户与您的账户关联起来。
2. 向账户发送成员资格邀请。

受邀账户接受邀请后，它将成为您组织中的成员账户。

步骤 1：添加账户

要将一个或多个账户添加到您的账户清单中，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

借助 Amazon Macie 控制台，您可以一次添加一个账户，也可以通过上传逗号分隔值 (CSV) 文件来同时添加多个账户。请按照以下步骤使用控制台添加一个或多个账户。

添加一个账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要添加账户的区域。
3. 在导航窗格中的设置下，选择账户。
4. 选择添加账户。
5. 在输入账户详细信息部分，选择添加账户选项卡。然后执行以下操作：
   - 对于账户 ID ，请输入要添加的 AWS 账户 的 12 位数账户 ID。
   - 对于电子邮件地址，请输入要添加的 AWS 账户 的电子邮件地址。
6. 选择添加，然后选择下一步。

Macie 会将该账户添加到您的账户清单中。该账户的类型为通过邀请，其状态为已创建。在您要添加账户的每个其他区域中重复上述步骤。

要管理多个账户

1. 使用文本编辑器创建 CSV 文件，如下所示：
   a. 添加以下标头作为文件的第一行：`Account ID,Email`
   b. 对于每个账户，创建一个新行，其中包含要添加的 AWS 账户 的 12 位数账户 ID 以及该账户的电子邮件地址。用逗号分隔各个条目，例如：`111111111111,janedoe@example.com`

电子邮件地址必须和与 AWS 账户 关联的电子邮件地址相匹配。

c. 确认文件内容的格式如下例所示，其中包含三个账户所需的标头和信息：

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

d. 将该文件保存到您的计算机。

2. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
3. 使用页面右上角的 AWS 区域 选择器，选择要添加账户的区域。
4. 在导航窗格中的设置下，选择账户。
5. 选择添加账户。
6. 在输入账户详细信息部分，选择上传列表 (CSV) 选项卡。
7. 选择浏览，然后选择已在步骤 1 中创建的 CSV 文件。
8. 选择添加账户，然后选择下一步。

Macie 会将这些账户添加到您的账户清单中。其类型为通过邀请，状态为已创建。在您要添加账户的每个其他区域中重复步骤 3 到 8。

API

要以编程方式添加一个或多个账户，请使用 Amazon Macie API 的 CreateMember 操作。提交请求时，请使用支持的参数指定要添加的每个 AWS 账户 的 12 位数账户 ID 和电子邮件地址。此外，请指定请求适用的区域。要在其他区域中添加账户，请在每个其他区域中提交请求。

要使用AWS Command Line Interface (AWS CLI)添加账户，请运行create-member命令。使用 `region` 参数指定要添加账户的区域。使用`account`参数指定要添加的每个AWS 账户的账户 ID 和电子邮件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

其中，*us-east-1*是要添加账户的区域（美国东部（弗吉尼亚州北部）区域），`account`参数指定要添加账户的账户 ID (*111111111111*) 和电子邮件地址 (*janedoe@example.com*)。

如果您的请求成功，Macie 会将每个账户添加到您的账户清单中，其状态为 `Created`，并且您会收到类似于以下内容的输出：

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

其中 `arn` 是为您的账户与您添加的账户之间的关联而创建的资源的 Amazon 资源名称（ARN）。在此示例中，`123456789012` 是创建关联的账户的账户 ID，`111111111111` 是已添加账户的账户 ID。

步骤 2：向账户发送成员资格邀请

将账户添加到账户清单后，您可以邀请该账户以 Macie 成员账户的身份加入您的组织。为此，请向该账户发送成员资格邀请。当您发送邀请时，如果收件人的账户已启用 Macie，则该账户的 Amazon Macie 控制台上会显示账户徽章和通知。Macie 还为该账户创建了一个 AWS Health 事件。

根据您是使用 Amazon Macie 控制台还是 API 发送邀请，Macie 还会将邀请发送到您在添加账户时为收件人账户指定的电子邮件地址。该电子邮件表明您希望成为他们账户的 Macie 管理员，其中包括您的 AWS 账户 账户 ID 和收件人的 AWS 账户 账户 ID。该消息还说明了如何访问邀请。您可以选择在消息中添加自定义文本。

要向一个或多个账户发送成员资格邀请，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

请按照以下步骤使用 Amazon Macie 控制台发送成员资格邀请。

发送成员资格邀请

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要发送邀请的区域。
3. 在导航窗格中的设置下，选择账户。
4. 在账户表中，选中要向其发送邀请的每个账户的复选框。

> **Tip**
>
> 为了更轻松地识别您已添加但尚未向其发送邀请的账户，您可以筛选该表。为此，请将光标放在表上方的筛选框中，然后选择状态。然后选择状态 = 已创建。

5. 在操作菜单上，选择邀请。
6. （可选）在消息框中，输入要包含在含有邀请的电子邮件中的任何自定义文本。该文本可包含多达 80 个字母数字字符。
7. 选择邀请。

要在其他 AWS 区域 中发送邀请，请在每个其他区域中重复上述步骤。

发送邀请后，您账户清单中的收件人账户状态将更改为正在进行电子邮件验证。如果 Macie 可以验证账户的电子邮件地址，则该账户的状态随后会更改为已邀请。如果 Macie 无法验证地址，则账户的状态将更改为电子邮件验证失败。如果发生这种情况，请与账户所有者合作以获取正确的电子邮件地址。然后删除账户之间的关联，再次添加账户，并再次发送邀请。

当收件人接受邀请时，收件人的账户状态将在您的账户清单中更改为 已启用。如果收件人拒绝接受邀请，则该收件人的账户将与您的账户解除关联，并从您的账户清单中移除。

API

要以编程方式发送邀请，请使用 Amazon Macie API 的 CreateInvitations 操作。提交请求时，请使用支持的参数为每个 AWS 账户 指定要向其发送邀请的 12 位数账户 ID。账户 ID 必须与您的账户清单中某个账户的账户 ID 一致。否则将出错。此外，指定要从中发送邀请的区域。要从其他区域发送邀请，请在每个其他区域提交请求。

在请求中，您还可以指定是否以电子邮件形式发送邀请，以及是否在该消息中包含自定义文本。如果您选择发送电子邮件，Macie 会将邀请发送到您在将账户添加到账户清单时为该账户指定的电子邮件地址。要以电子邮件形式发送邀请，请省略 `disableEmailNotification` 参数或将参数值设置为 `false`。（默认值为 `false`。）要在信息中添加自定义文本，请使用 `message` 参数指定要添加的文本。该文本可包含多达 80 个字母数字字符。

要使用 AWS CLI 发送邀请，请运行 create-invitations 命令。使用 `region` 参数指定要从中发送邀请的区域。使用 `account-ids` 参数为要向其发送邀请的每个 AWS 账户 指定账户 ID。例如：

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

其中，*us-east-1* 是要从中发送邀请的区域（美国东部（弗吉尼亚州北部）区域），`account-ids` 参数指定了要向其发送邀请的三个账户的账户 ID。要将邀请作为电子邮件发送，还需包含 `no-disable-email-notification` 参数，并可选择包含 `message` 参数，以指定要添加到邮件中的自定义文本。

发送邀请后，每个收件人账户的状态将更改为 EmailVerificationInProgress。如果 Macie 可以验证账户的电子邮件地址，则该账户的状态随后会更改为 Invited。如果 Macie 无法验证地址，则账户的状态将更改为 EmailVerificationFailed。如果发生这种情况，请与账户所有者合作以获取正确的地址。然后删除账户之间的关联，再次添加账户，并再次发送邀请。

当收件人接受邀请时，收件人的账户状态将在您的账户清单中更改为 Enabled。如果收件人拒绝接受邀请，则该收件人的账户将与您的账户解除关联，并从您的账户清单中移除。

暂停使用基于邀请的组织中的成员账户的 Amazon Macie

作为组织的 Macie 管理员，您可以在特定 AWS 区域 暂停组织中单个成员账户的 Macie。但请注意，暂停成员账户后，您无法为其重新启用 Macie。之后只有该账户的用户才能为该账户重新启用 Macie。

当您暂停成员账户的 Macie 时：

- Macie 会失去对该区域中账户的 Amazon S3 数据的访问权限，并停止提供有关该账户的 Amazon S3 数据的元数据。
- Macie 停止在该区域中为账户执行所有活动。这包括监控 S3 存储桶的安全性和访问控制、执行自动敏感数据发现，以及运行当前正在进行的敏感数据发现作业。
- Macie 会取消该账户在该区域创建的所有敏感数据发现作业。作业取消后无法恢复或重新启动。

  如果您创建了作业来分析成员账户拥有的数据，Macie 不会取消这些作业。相反，这些作业会跳过该账户拥有的资源。

账户被暂停后，Macie 会在相应区域保留该账户的 Macie 会话标识符、设置和资源。例如，该账户的调查发现保持不变，最长可在 90 天内不受影响。在适用区域中使用 Macie 不会向该账户收费，而该区域中的账户会暂停 Macie。

要暂停基于邀请的组织中成员账户的 Macie

要暂停基于邀请的组织中成员账户的 Macie，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台暂停成员账户的 Macie。

暂停成员账户的 Macie

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。

2. 使用页面右上角的 AWS 区域 选择器，选择要暂停成员账户 Macie 的区域。
3. 在导航窗格中的设置下，选择账户。
4. 在账户表中，选中要暂停的账户的复选框。
5. 在操作菜单上，选择暂停 Macie。
6. 确认您要暂停所选账户的 Macie。

确认暂停后，账户清单中的账户状态会更改为已暂停（已挂起）。

在要暂停账户 Macie 的每个附加区域中重复上述步骤。

API

要以编程方式暂停成员账户的 Macie，请使用 Amazon Macie API 的 UpdateMemberSession 操作。提交请求时，请使用 `id` 参数指定要暂停 Macie 的 AWS 账户 的 12 位账户 ID。对于 `status` 参数，将 PAUSED 指定为 Macie 账户的新状态。此外，请指定请求适用的区域。要在其他区域暂停 Macie，请在每个其他区域提交您的请求。

要检索成员账户的账户 ID，您可以使用 Amazon Macie API 的 ListMembers 操作。如果执行此操作，请考虑通过在请求中包含 `onlyAssociated` 参数来筛选结果。如果将此参数的值设置为 `true`，则 Macie 将返回一个 `members` 数组，该数组仅提供有关当前是管理员账户的成员账户的账户的详细信息。

要使用 AWS CLI 暂停成员账户的 Macie，请运行 update-member-session 命令。使用 `region` 参数指定要暂停 Macie 的区域，并使用 `id` 参数指定要暂停 Macie 的账户的账户 ID。对于 `status` 参数，请指定 PAUSED。例如：

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

其中 *us-east-1* 是要暂停 Macie 的区域（美国东部（弗吉尼亚州北部）区域），而 *123456789012* 是要暂停 Macie 的账户的账户 ID，PAUSED 是该账户的 Macie 的新状态。

如果请求成功，Macie 将返回空响应，并且指定账户的状态将在账户清单中更改为 `Paused`。

从基于邀请的组织中删除 Amazon Macie 成员账户

作为 Macie 管理员，您可以从您的组织中删除成员账户。为此，请取消该账户与 Macie 管理员账户的关联。

如果您移除成员账户，Macie 将继续为该账户启用，并且该账户会继续显示在您的账户清单中。但是，该账户将成为独立的 Macie 账户。当您移除账户时，Macie 不会通知账户的所有者。因此，请考虑与账户所有者联系，以确保他们开始管理其账户的设置和资源。

删除成员账户后，您将无法访问该账户的所有 Macie 设置、资源和数据。这包括账户拥有的 S3 存储桶的策略调查发现和元数据。此外，您无法再使用 Macie 发现账户拥有的 S3 存储桶中的敏感数据。如果您已创建敏感数据发现作业来执行此操作，则这些作业将跳过账户拥有的存储桶。

删除成员账户后，您可以随后通过向该账户发送新邀请，将其再次添加到您的组织中。您还可以通过删除账户之间的关联将其从账户清单中完全移除。

要从基于邀请的组织中删除成员账户

要从组织中删除帐员账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台删除成员账户。

要删除成员账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 使用页面右上角的 AWS 区域 选择器，选择要删除成员账户的区域。
3. 在导航窗格中的设置下，选择账户。
4. 在账户表中，选中要删除的账户的复选框。
5. 在操作菜单上，选择取消关联账户。
6. 确认您要作为成员账户移除的选定账户。

确认选择后，账号清单中的账号状态会更改为已移除（已解除关联）。

在您要移除成员账户的每个附加区域中重复上述步骤。

API

要以编程方式删除成员账户，请使用 Amazon Macie API 的 DisassociateMember 操作。提交请求时，请使用 `id` 参数为要移除的成员账户指定 12 位数的 AWS 账户 ID。此外，请指定请求适用的区域。要移除其他区域的账户，请在每个其他区域提交您的申请。

要检索要删除的账户的账户 ID，您可以使用 Amazon Macie API 的 ListMembers 操作。如果执行此操作，请考虑通过在请求中包含 `onlyAssociated` 参数来筛选结果。如果将此参数的值设置为

`true`，则 Macie 将返回一个 `members` 数组，该数组仅提供有关当前是您账户的成员账户的账户的详细信息。

要使用 AWS CLI 删除成员账户，请运行 disassociate-member 命令。使用 `region` 参数指定要移除账户的区域。使用 `id` 参数指定要删除的账户的账户 ID。例如：

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要移除账户的区域（美国东部（弗吉尼亚州北部）区域），*123456789012* 是要移除的账户的账户 ID。

如果请求成功，Macie 将返回空响应，并且指定账户的状态将在账户清单中更改为 `Removed`。

删除与其他账户的关联

将账户添加到账户清单后，您可以删除您的账户与其他账户之间的关联。您可以对库存中的任何账号执行此操作，但以下情况除外：

- 属于 AWS Organizations 中您的组织的账户。这种类型的关联是通过 AWS Organizations 而不是 Macie 控制的。
- 接受 Macie 成员资格邀请以加入您的组织的成员账户。如果是这种情况，您必须先删除成员账户，然后才能删除关联。

当您删除关联时，Macie 会从您的账户清单中移除该账户。如果随后要恢复关联，则必须再次添加该账户，就好像它是一个全新的账户一样。

要删除与其他账户的关联

要删除您的账户与其他账户之间的关联，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

要使用 Amazon Macie 控制台删除与其他账户的关联，请执行以下步骤。

删除关联

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 通过使用页面右上角的 AWS 区域 选择器，选择要删除关联的区域。

3. 在导航窗格中的设置下，选择账户。
4. 在账户表中，选中要删除其关联的账户的复选框。
5. 在操作菜单上，选择删除账户。
6. 确认要删除所选关联。

在要删除关联的每个其他区域中重复上述步骤。

API

要以编程方式删除与其他账户的关联，请使用 Amazon Macie API 的 DeleteMember 操作。提交请求时，请使用 `id` 参数指定要删除关联的 AWS 账户 的 12 位账户 ID。此外，请指定请求适用的区域。要删除其他区域中的关联，请在每个其他区域中提交您的请求。

要检索账户的账户 ID，您可以使用 Amazon Macie API 的 ListMembers 操作。如果执行此操作，请在请求中包含 `onlyAssociated` 参数，并将参数的值设置为 `false`。如果操作成功，Macie 将返回一个 `members` 数组，该数组提供有关与您的账户关联的所有账户的详细信息，包括当前不是成员账户的账户。

要使用 AWS CLI 删除与其他账户的关联，请运行 delete-member 命令。使用 `region` 参数指定要删除关联的区域，并使用 `id` 参数指定账户的账户 ID。例如：

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要删除与其他账户关联的区域（美国东部（弗吉尼亚州北部）区域），*123456789012* 是账户的账户 ID。

如果请求成功，Macie 将返回空响应，并删除您的账户与其他账户之间的关联。之前关联的账号将从您的账号清单中移除。

查看基于邀请的组织的 Amazon Macie 账户

为了帮助您管理组织中的账户，Amazon Macie 在您使用 Macie 的每个 AWS 区域 中提供了与您的 Macie 账户关联的账户清单。通过使用此清单，您可以检查各个账户的状态，并查看组织的账户统计信息和详细信息。您还可以管理您的账户与个人账户之间的关系状态。

要查看基于邀请的组织的账户

要查看组织中的账户，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

按照以下步骤使用 Amazon Macie 控制台查看组织的账户。

要查看组织的账户

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 通过使用页面右上角的 AWS 区域 选择器，选择要在其中查看组织账户的区域。
3. 在导航窗格中的设置下，选择账户。

账户页面将打开并显示汇总统计数据以及与当前 AWS 区域 中的 Macie 账户关联的账户表。

在账户页面的顶部，您可以找到以下汇总统计数据。

经由 AWS Organizations

如果您是 AWS Organizations 中某个组织的 Macie 管理员，则活动会报告通过 AWS Organizations 与您的账户关联的账户总数，这些账户目前是您组织中的 Macie 成员账户。已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员。

所有报告通过 AWS Organizations 与您的账户关联的账户总数，包括当前不是 Macie 成员账户的账户。

通过邀请

活动报告基于邀请的组织中当前属于 Macie 成员账户的账户总数。已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员，因为他们接受了您的成员资格邀请。

所有报告通过 Macie 邀请与您的账户关联的账户总数，包括尚未回复您的邀请的账户。

活动/全部

活动报告您账户当前是 Macie 成员账户的账户总数，通过 AWS Organizations 或通过邀请。已为这些账户启用 Macie，并且您是这些账户的 Macie 管理员。

所有报告与您的账户关联的账户总数，可以通过 AWS Organizations 或邀请。这包括尚未接受您的 Macie 会员资格邀请的账户。这还包括通过 AWS Organizations 与您的账户关联但当前不是 Macie 成员账户的账户。

在表中，您将找到有关当前区域中每个账户的详细信息。该表包含通过 Macie 邀请或通过 AWS Organizations 与您的 Macie 账户关联的所有账户。

账户 ID

AWS 账户 的账户 ID 和电子邮件地址。

名称

AWS 账户 的账户名称。对于通过邀请与您的账户关联的账户，此值通常为不适用。

Type

该账户如何通过邀请或通过 AWS Organizations 与您的账户关联。

状态

您的账户与该账户之间的关系状态。对于基于邀请的组织（类型为通过邀请）中的账户，可能的值为：

- 账户已挂起 – AWS 账户 已挂起。
- 已创建（邀请） – 您已添加账户，但尚未向其发送成员资格邀请。
- 电子邮件验证失败 – 您尝试向该账户发送成员资格邀请，但指定的电子邮件地址对该账户无效。
- 电子邮件验证正在进行中 – 您向该账户发送了会员邀请，Macie 正在处理该请求。
- 已启用 – 该账户是成员账户。已为该账户启用 Macie，并且您是该账户的 Macie 管理员。
- 已邀请 – 您向该账户发送了成员资格邀请，但该账户尚未响应您的邀请。
- 成员已退出 – 该账户以前是成员账户。但是，该账户通过取消与您的账户的关联而从您的组织辞职。
- 已暂停（暂停） – 该账户是成员账户，但 Macie 目前已暂停该账户。
- 区域已禁用 – 当前区域已为 AWS 账户 禁用。
- 已删除（取消关联） – 该账户以前是成员账户。但是，您通过取消将其与您的账户关联来将其作为成员账户删除。

上次操作

当您或关联的账户最近执行了影响您账户之间关系的操作时。

要按特定字段对表格进行排序，请点击该字段的列标题。若要更改排序顺序，请再次点击列标题。若要筛选表，请将光标放在筛选条件框中，然后为字段添加筛选条件。若要进一步优化结果，请为其他字段添加筛选条件。

API

要以编程方式查看组织的账户，请使用 Amazon Macie API 的 ListMembers 操作，并确保指定您的请求适用的区域。要查看其他区域的详细信息，请在每个其他区域中提交您的请求。

提交请求时，请使用 onlyAssociated 参数指定要包含在响应中的账户。默认情况下，Macie 仅通过邀请或通过 AWS Organizations 返回有关指定区域中成员账户的账户的详细信息。要检索所有关联账户（包括非成员账户）的详细信息，请在请求中包含 onlyAssociated 参数，并将该参数的值设置为 false。

要使用 AWS Command Line Interface (AWS CLI) 查看组织的账户，请运行 list-members 命令。对于 only-associated 参数，指定是包括所有关联账户还是仅包含成员账户。要仅包含成员账户，请省略此参数或将参数的值设置为 true。要包括所有账户，请将此值设置为 false。例如：

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

其中 *us-east-1* 是请求适用的区域，即美国东部（弗吉尼亚州北部）区域。

如果请求成功，Macie 将返回一个 members 数组。该数组包含满足请求中指定标准的每个账户的 member 对象。在该对象中，relationshipStatus 字段指示您的账户与指定区域中的其他账户之间的关联当前状态。对于基于邀请的组织中的账户，可能的值为：

- AccountSuspended – AWS 账户 已挂起。
- Created – 您添加了账户，但尚未向其发送成员资格邀请。
- EmailVerificationFailed – 您尝试向该账户发送成员资格邀请，但指定的电子邮件地址对该账户无效。
- EmailVerificationInProgress – 您向该账户发送了成员资格邀请，Macie 正在处理该请求。
- Enabled – 该账户是成员账户。已为该账户启用 Macie，并且您是该账户的 Macie 管理员。
- Invited – 您向该账户发送了成员资格邀请，但该账户尚未响应您的邀请。
- Paused – 该账户是成员账户，但 Macie 当前已停用（暂停）该账户。
- RegionDisabled – 当前区域已禁用 AWS 账户。
- Removed – 该账户以前是成员账户。但是，您通过取消将其与您的账户关联来将其作为成员账户删除。
- Resigned – 该账户以前是成员账户。但是，该账户通过取消与您的账户的关联而从您的组织辞职。

有关 `member` 对象中其他字段的信息，请参阅 Amazon Macie API 参考中的成员。

为基于邀请的组织指定不同的 Amazon Macie 管理员账户

在创建和建立基于邀请的组织后，您可以更改该组织的 Amazon Macie 管理员账户。为此，管理员和组织成员应执行以下步骤：

1. 当前 Macie 管理员可以选择导出组织的活动成员账户的当前清单。这通过帮助您确定应继续成为组织一部分的成员账户来简化转换。
2. 当前 Macie 管理员从当前组织中删除所有成员账户。这会取消账户与当前管理员账户的关联，但会继续为这些账户启用 Macie。
3. 新的 Macie 管理员将以前的成员账户添加到新组织。这会将账户与新的管理员账户相关联。
4. 每个成员账户都接受加入新组织的邀请。当账户接受邀请时，该账户将成为新组织中的活动成员账户。然后，新的 Macie 管理员就可以访问该账户的 Macie 设置、数据和资源。

如果您的组织在多个 AWS 区域 中使用 Macie，请在每个区域中执行上述步骤。

要导出活动成员账户的当前清单，当前 Macie 管理员可以使用 Amazon Macie 控制台或 Amazon Macie API。使用控制台，当前管理员可以将数据导出到逗号分隔值 (CSV) 文件。然后，新管理员可以使用控制台上传 CSV 文件，并将所有账户（批量）添加到新组织。

使用控制台导出成员账户数据

1. 使用当前的 Macie 管理员账户登录 AWS Management Console。
2. 使用页面右上角的 AWS 区域 选择器，选择要导出数据的区域。
3. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
4. 在导航窗格中的设置下，选择账户。
5. （可选）要筛选账户表并仅显示组织中当前处于活动状态的 Macie 成员账户，请使用表上方的筛选条件框添加以下筛选条件：
   - 类型 = 邀请
   - 状态 = 已启用
6. 在账户表中，选中要包含在导出数据中的每个活动成员账户的复选框。
7. 选择 导出 CSV。
8. 指定文件的名称和位置。

借助 Amazon Macie API，当前的 Macie 管理员可以检索 JSON 格式的数据。然后，新的 Macie 管理员可以使用该数据为要添加和邀请到新组织的账户生成账户 ID 和电子邮件地址列表。要检索 JSON 格式的数据，请使用 Amazon Macie API 的 ListMembers 操作。如果操作成功，Macie 将返回一个 `members` 数组，该数组提供有关与管理员账户关联的所有账户的详细信息。如果账户是当前基于邀请的组织中的活动 Macie 成员账户，则该账户的 `relationshipStatus` 属性值为 `Enabled`，`invitedAt` 属性指定日期和时间。

在 Amazon Macie 中管理您在基于邀请的组织中的成员资格

如果您被邀请加入 Amazon Macie 中的组织，则可以选择接受或拒绝邀请。在 Macie 中，组织是作为一组相关账户进行集中管理的一组账户。一个组织由一个指定的 Macie 管理员账户和一个或多个关联的成员账户组成。

如果您接受邀请，您的账户将成为组织中的成员账户。当您接受邀请后，发送邀请的账户将成为您账户的 Macie 管理员账户，您将自己的账户与其他账户关联，并在账户之间启用管理员-成员关系。然后，Macie 管理员账户就可以访问适用的 AWS 区域 中您账户的某些 Macie 设置、数据和资源。有关更多信息，请参阅了解 Amazon Macie 管理员和成员账户之间的关系。

如果您拒绝邀请，则您的 Macie 账户的当前状态和设置不会更改。

主题

- 回应组织的成员资格邀请
- 从 Amazon Macie 管理员账户取消关联

回应组织的成员资格邀请

当您收到加入某个组织的邀请时，Amazon Macie 会通过多种方式通知您。默认情况下，Macie 会以电子邮件的形式向您发送邀请。Macie 还会为您的 AWS 账户 创建 AWS Health 活动. 如果您已经在发送邀请的 AWS 区域 中使用了 Macie，Macie 还会在 Macie 控制台中显示账户徽章和通知。

收到邀请后，您可以选择接受或拒绝邀请。在回应之前，请注意以下事项：

- 您一次只能是一个组织的成员。如果您收到多个邀请，则只能接受一个邀请。或者，如果您已经是某个组织的成员，则必须先取消账户与其当前 Macie 管理员账户的关联，然后才能加入其他组织。
- 如果您在多个地区使用 Macie，则您的账户在所有这些地区都必须拥有相同的 Macie 管理员账户。Macie 管理员必须从每个区域分开向您发送邀请，并且您必须在每个区域分别接受邀请。

- 要接受或拒绝邀请，您必须在发出邀请的地区启用 Macie。拒绝邀请是可选的。如果您允许 Macie 拒绝邀请，则可以在拒绝邀请后在该地区禁用 Macie。这有助于确保您不会因为在该地区使用 Macie 而产生不必要的费用。

有关其他注意事项，请参阅 回复和管理成员邀请。

回应组织的成员资格邀请

要回应成员资格邀请，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

请按照以下步骤使用 Amazon Macie 控制台回应成员资格邀请。

回应成员资格邀请

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择接受邀请的区域。
3. 如果您尚未在该地区启用 Macie，请选择开始，然后选择启用 Macie。在接受或拒绝邀请之前，必须启用 Macie。
4. 在导航窗格中的设置下，选择账户。
5. 在管理员账户下，执行以下操作之一：
   - 要接受邀请，请打开邀请旁边的接受 ( )。然后选择接受邀请或更新，具体取决于您之前是否接受了其他邀请。
   - 要拒绝邀请，请选择邀请旁边的拒绝邀请，然后确认您要拒绝邀请。

如果您已收到并想在其他地区回复邀请，请在每个其他地区重复上述步骤。

API

要以编程方式回复邀请，请使用 Amazon Macie API 的接受邀请或拒绝邀请操作，具体取决于您要接受还是拒绝邀请。提交请求时，请务必指定发出邀请的区域。要回应其他区域的邀请，请在每个其他区域提交您的请求。

在 `AcceptInvitation` 请求中，使用 `administratorAccountId` 参数为发送邀请的 AWS 账户 指定 12 位数的账户 ID。使用 `invitationId` 参数为要接受的邀请指定唯一的 ID。

在 DeclineInvitations 请求中，使用 accountIds 参数为要拒绝发送邀请的 AWS 账户 指定 12 位数的账户 ID。

要检索 ID，您可以使用 Amazon Macie API 的 ListInvitations 操作。如果操作成功，Macie 将返回一个 invitations 数组，其中提供有关您收到的邀请的详细信息，包括发送每个邀请的账户的 ID 和每个邀请的唯一 ID。如果邀请 relationshipStatus 属性的值为 Invited，则表示您尚未回复邀请。

要使用 AWS Command Line Interface (AWS CLI) 回应邀请，请运行接受邀请或拒绝邀请命令，具体取决于您要接受还是拒绝邀请。使用 region 参数指定发送邀请的区域。例如：

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

其中 *us-east-1* 是发送邀请的区域（美国东部（弗吉尼亚州北部）地区），*123456789012* 是发送邀请的账户的账户 ID，*d8bdad0e203fd1242e0a4721bexample* 是要接受的邀请的唯一 ID。

如果接受邀请的请求成功，Macie 会返回一个空的响应。如果拒绝邀请的请求成功，Macie 会返回一个空的 unprocessedAccounts 数组。

在您拒绝邀请后，该邀请将作为您的 Macie 账户的资源保留。您可以选择使用删除邀请操作将其删除，或者对于 AWS CLI 使用删除邀请命令将其删除。

从 Amazon Macie 管理员账户取消关联

如果您接受加入某组织 Amazon Macie 的邀请，则可以通过取消您的账户与其当前 Macie 管理员账户的关联来退出该组织。请注意，如果您的账户是 AWS Organizations 组织中的成员账户，则您无法执行此操作。要退出 AWS Organizations 组织，请与您的 Macie 管理员合作，将您的账户从 Macie 成员账户移除。

如果您取消账户与其 Macie 管理员账户的关联，Macie 管理员将失去对您 Macie 账户的所有设置、数据和资源的访问权限。这包括您拥有的 Amazon S3 数据的元数据和策略调查发现。这也意味着管理员无法再通过执行自动敏感数据发现或运行敏感数据发现作业来分析您的 Amazon S3 数据。

当您取消关联账户后，Macie 将继续在相应区域为您的账户启用。但是，在区域中，您的账户将成为独立的 Macie 账户。在管理员的账户清单中，您的账户状态将更改为成员已退出。

要解除与 Macie 管理员账户的关联

要取消您的账户与其当前 Macie 管理员账户的关联，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

使用 Amazon Macie 控制台，按照以下步骤取消您的账户与其 Macie 管理员账户的关联。

要从管理员账户取消关联

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要将您的账户与其管理员账户解除关联的区域。
3. 在导航窗格中的设置下，选择账户。
4. 在管理员账户下，关闭邀请旁边的接受
   ()，
   然后选择更新。

该账户继续显示在账户页面上。如果您决定重新加入该组织，则可以使用此页面再次接受原始邀请。或者，您可以拒绝并删除邀请，这也会删除您的账户与其他账户之间的关联。为此，请选择拒绝邀请。

如果您想在其他区域取消账户与其 Macie 管理员账户的关联，请在每个其他区域重复上述步骤。

API

要以编程方式解除您的账户与其 Macie 管理员账户的关联，请使用 Amazon Macie API 的 DisassociateFromAdministratorAccount 操作。提交请求时，请务必指定该请求适用的区域。要解除与其他区域的账户关联，请在每个其他区域提交您的请求。

要使用 AWS CLI 解除您的账户与其 Macie 管理员账户的关联，请运行 disassociate-from-administrator-account 命令。使用 `region` 参数指定要在其中解除账户关联的区域。

如果请求成功，Macie 将返回空响应。

取消与该账户的关联后，除非您将其删除，否则原始邀请将作为您的 Macie 账户的资源保留。如果您决定重新加入该组织，则可以使用此资源再次接受原始邀请。或者，您可以选择使用删除邀请操作将其删除，或者对于 AWS CLI 使用删除邀请命令将其删除。如果您删除了邀请，您也删除了您的账户和另一个账户之间的关联。

Amazon Macie 中的安全性

AWS 十分重视云安全性。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 客户，您也将从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。shared responsibility model（责任共担模式）（责任共担模式）（责任共担模式）将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS 合规性计划的一部分。要了解适用于 Amazon Macie 的合规性计划，请参阅按合规性计划提供的范围内 AWS 服务。
- 云中的安全性 – 您的责任由您使用的 AWS 服务 决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Macie 时应用责任共担模式。以下主题说明如何配置 Macie 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务 以帮助您监控和保护 Macie 资源。

主题

Amazon Macie 中的数据保护

AWS责任共担模式适用于 Amazon Macie 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当您采用 Macie 或使用控制台、API、AWS CLI或 SDK 的其他 AWS 服务AWS时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，我们强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

Amazon Macie 使用 AWS 加密解决方案安全地存储您的静态数据。Macie 通过AWS Key Management Service的AWS 托管式密钥(AWS KMS) 加密调查发现等数据。

如果您禁用 Macie，它会永久删除所有存储或保留的资源，例如敏感数据发现任务、自定义数据标识符和调查发现。

传输中加密

Macie 会对AWS 服务中的所有传输中数据进行加密。

Amazon Macie 分析来自 Amazon S3 的数据，并将敏感数据调查发现结果导出至 S3 存储桶。Macie 从 S3 对象中获取所需信息后，它们将被丢弃。

Macie 使用由AWS PrivateLink支持的 VPC 端点访问 Amazon S3。因此，Macie 和 Amazon S3 之间的流量保留在 Amazon 网络上，不会通过公共互联网传输。有关更多信息，请参阅AWS PrivateLink。

适用于 Amazon Macie 的身份和访问管理

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Macie 资源的人员。IAM 是一项无需额外费用即可使用的 AWS 服务。

主题

受众

使用 AWS Identity and Access Management(IAM) 的方式因您可以在 Macie 中执行的操作而异。

服务用户 – 如果使用 Macie 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Macie 特征来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Macie 中的特征，请参阅 Amazon Macie 身份和访问问题排查。

服务管理员 – 如果您在公司负责管理 Macie 资源，则您可能具有 Macie 的完全访问权限。您有责任确定您的服务用户应访问哪些 Macie 特征和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Macie 搭配使用的更多信息，请参阅 Amazon Macie 如何与 AWS Identity and Access Management协同工作。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Macie 的访问权限的详细信息。要查看您可在 IAM 中使用的 Macie 基于身份的策略示例，请参阅 Amazon Macie 基于身份的策略示例。

使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过担任 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center(IAM Identity Center) 用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接担任角色。

根据用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的如何登录到您的 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS 中使用多重身份验证（MFA）。

AWS 账户 根用户

创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实操，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、网络身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份源提供的凭证来访问 AWS 服务 的用户。当联合身份访问 AWS 账户时，他们担任角色，而角色提供临时凭证。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到自己的身份源中的一组用户和组以跨所有 AWS 账户 和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和群组

IAM 用户是 AWS 账户 内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用群组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用群组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人担任。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是 AWS 账户 中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时担任 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义网址以代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为座席）。要了解用于跨账户存取的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 AWS 服务 使用其他 AWS 服务 中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

- 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的政策详情，请参阅转发访问会话。
- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。
- 服务相关角色 - 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 Amazon EC2 上运行的应用程序 - 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以担任角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户群组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、群组或角色中。托管策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户管理型策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可以为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 字段中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。

如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。

- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的策略评测逻辑。

Amazon Macie 如何与 AWS Identity and Access Management协同工作

在使用 AWS Identity and Access Management (IAM) 管理对 Amazon Macie 的访问之前，您应该了解哪些 IAM 功能可用于 Macie。

将 IAM 功能与 Amazon Macie 一起使用

IAM 特征	Macie 支持
基于身份的策略	可以
基于资源的策略	不可以
策略操作	可以
策略资源	可以
策略条件键	可以
访问控制列表 (ACL)	不可以
基于属性的访问控制 (ABAC) – 策略中的标签	可以
临时凭证	可以
转发访问会话 (FAS)	可以

IAM 特征	Macie 支持
服务角色	不可以
服务相关角色	可以

要了解 Macie 和其他 AWS 服务如何与大多数 IAM 功能一起使用，请参阅 AWS 服务IAM 用户指南中的与 IAM 一起使用的 。

Amazon Macie 基于身份的策略

支持基于身份的策略	可以

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Macie 支持基于身份的策略。有关示例，请参阅Amazon Macie 基于身份的策略示例。

Amazon Macie 基于资源的策略

支持基于资源的策略	不可以

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 AWS

账户 中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

Macie 不支持基于资源的策略。也就是说，您不能将策略直接附加至 Macie 资源。

Amazon Macie 的策略操作

支持策略操作	可以

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与相关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

Macie 策略操作在操作前使用以下前缀：

```
macie2
```

例如，若要授权某人访问有关 Macie 提供的所有托管数据标识符信息 (该操作与 Amazon Macie API 的`ListManagedDataIdentifiers`操作相对应)，请在他们的策略中纳入 `macie2:ListManagedDataIdentifiers` 操作：

```
"Action": "macie2:ListManagedDataIdentifiers"
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。例如：

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

您也可以使用通配符 (*) 指定多项操作。例如，要指定以单词 `List` 开头的所有操作，包括以下操作：

```
"Action": "macie2:List*"
```

但作为最佳实践，您应创建遵循最低权限 原则的策略。换句话说，您应创建仅包含执行特定任务所需的权限的策略。

有关 Amazon Macie 操作的列表，请参阅 Amazon Macie 服务授权参考中定义的操作。有关涉及 Macie 操作的策略示例，请参阅 Amazon Macie 基于身份的策略示例。

Amazon Macie 的策略资源

支持策略资源	可以

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件 下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN)指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Macie 定义了以下资源类型：

- 允许列表
- 自定义数据标识符
- 筛选或隐藏规则，也称为调查发现筛选条件
- 成员账户
- 敏感数据发现作业，也称为分类作业

您可以通过使用 ARN 在政策中指定这些类型的资源。

例如，要为作业 ID 为3ce05dbb7ec5505def334104bexample 的敏感数据调查发现任务创建策略，您可以使用以下 ARN：

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

或者，要为某个账户指定所有敏感数据调查发现任务，请使用通配符 (*)：

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

其中 *123456789012* 是创建任务的AWS 账户账户 ID。作为最佳实践，您应创建遵循最低权限原则的策略。换句话说，您应创建仅包含在特定资源上执行任务所需的权限的策略。

部分 Macie 操作可应用于多种资源。例如，macie2:BatchGetCustomDataIdentifiers 操作可以检索多个自定义数据标识符的详细信息。在这些情况下，主体必须有权访问该操作的所有适用资源。要在单个语句中指定多个资源，请使用逗号分隔 ARN：

```
"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"
]
```

有关 Macie 资源类型以及每种资源的 ARN 句法，请参阅服务授权参考中的 Amazon Macie 定义的资源类型。要了解您可以为每种资源类型指定的操作类型，请参阅服务授权引用中的按 Amazon Macie 定义操作。有关指定资源的策略示例，请参阅 Amazon Macie 基于身份的策略示例。

Amazon Macie 的策略条件密钥匙

支持特定于服务的策略条件键	可以

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，您可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个密钥，则 AWS 使用逻辑 AND 运算评估它们。如果您要为单个条件密钥指定多个值，则 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

您也可以在指定条件时使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件密钥，请参阅《IAM 用户指南》中的 AWS 全局条件上下文密钥。

要查看 Macie 条件密钥的列表，请参阅服务授权参考中的 Amazon Macie 的条件密钥。要了解您可以对哪些操作和资源使用条件密钥，请参阅 Amazon Macie 定义的操作。有关使用条件密钥的策略示例，请参阅 Amazon Macie 基于身份的策略示例。

Amazon Macie 中的访问控制列表（ACL）

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon Simple Storage Service (Amazon S3) 就是这种支持 ACL 的 AWS 服务 示例。要了解更多信息，请参阅 Amazon Simple Storage Service 用户指南 中的访问控制列表（ACL）概览。

Macie 不支持 ACL。也就是说，你无法将 ACL 附加至 Macie 资源。

使用 Amazon Macie 基于属性的访问权限控制（ABAC）

支持 ABAC（策略中的标签）	可以

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 AWS 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，需要使用 `aws:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件密钥在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制 (ABAC)。

您可以向 Macie 资源添加标签，包括允许列表、自定义数据标识符、筛选规则和禁止规则、成员账户以及敏感数据发现作业。您还可以通过在策略的 `Condition` 元素中提供标签信息，控制对这些类型资源的访问权限。有关标记 Macie 资源的信息，请参阅 为 Amazon Macie 资源添加标签。有关基于标签控制资源访问权的基于身份的策略示例，请参阅Amazon Macie 基于身份的策略示例。

将临时凭证用于 Amazon Macie

支持临时凭证	可以

某些 AWS 服务 在使用临时凭证登录时无法正常工作。有关更多信息，包括 AWS 服务 与临时凭证配合使用，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。

如果您不使用用户名和密码而用其他方法登录到 AWS Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Macie 支持使用临时凭证。

Amazon Macie 的转发访问会话

支持转发访问会话（FAS）	可以

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的政策详情，请参阅转发访问会话。

Macie 会在您执行以下任务时向下游 AWS 服务发出 FAS 请求：

- 为存储在 S3 存储桶中的允许列表创建或更新 Macie 设置。
- 检查存储在 S3 存储桶中的允许列表的状态。
- 使用 IAM 用户凭证检索受影响的 S3 对象中的敏感数据样本。
- 对使用 IAM 用户凭证或 IAM 角色检索的敏感数据样本进行加密。
- 启用 Macie 与 AWS Organizations 的集成。
- 为 AWS Organizations 中的组织指定委派 Macie 管理员账户。

对于其他任务，Macie 使用服务相关角色来代表您执行操作。有关此角色的详细信息，请参阅Amazon Macie 的服务相关角色。

Amazon Macie 的服务角色

支持服务角色	不可以

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。

Macie 不承担或使用服务角色。Macie 主要使用服务相关角色来代表您执行操作。有关此角色的详细信息，请参阅Amazon Macie 的服务相关角色。

Amazon Macie 的服务相关角色

支持服务相关角色	可以

服务相关角色是一种与 AWS 服务 相关的服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Macie 使用服务相关角色代表您执行操作。有关此角色的详细信息，请参阅Amazon Macie 的服务相关角色。

Amazon Macie 基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Macie 资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface（AWS CLI）或 AWS API 执行任务。要授予用户对所需资源

执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 创建 IAM policy。

有关 Macie 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考中的 Amazon Macie 的操作、资源和条件密钥。

创建策略时，请务必先解决来自 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) 的安全警告、错误、一般警告和建议，然后再保存策略。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成结果并提供可操作的建议，可帮助您编写可操作且符合安全最佳实践的策略。要了解通过使用 IAM Access Analyzer 验证策略，请参阅 IAM 用户指南中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 可以返回的警告、错误和建议列表，请参阅 IAM 用户指南中的 IAM Access Analyzer 策略检查参考。

主题

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Macie 资源。这些操作可能会使 AWS 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略 或 工作职能的 AWS 托管式策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- Require multi-factor authentication（MFA）[需要多重身份验证（MFA）] – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Amazon Macie 控制台

要访问 Amazon Macie 控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您的 AWS 账户 账户中的 Macie 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色可以使用 Amazon Macie 控制台，请创建为他们提供控制台访问权限的 IAM 策略。有关更多信息，请参阅 IAM 用户指南中的 IAM 中的策略和权限。

如果您创建的策略允许用户或角色使用 Amazon Macie 控制台，请确保该策略允许执行 `macie2:GetMacieSession` 操作。否则，这些用户或角色将无法访问控制台上的任何 Macie 资源或数据。

另请确保该策略允许为这些用户或角色需要在控制台上访问的资源执行适当的 `macie2:List` 操作。否则，他们将无法在控制台上导航到这些资源或显示有关这些资源的详细信息。例如，要通过使用控制台查看敏感数据发现作业的详细信息，必须允许用户为该作业执行 `macie2:DescribeClassificationJob` 操作以及执行 `macie2:ListClassificationJobs` 操作。如果不允许用户执行 `macie2:ListClassificationJobs` 操作，则该用户将无法在控制台的作业页面上显示作业列表，因此将无法选择作业来显示其详细信息。要使详细信

息包括有关作业使用的自定义数据标识符的信息，还必须允许用户为自定义数据标识符执行 `macie2:BatchGetCustomDataIdentifiers` 操作。

示例：允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "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": "*"
        }
    ]
}
```

示例：允许用户创建敏感数据发现作业

此示例展示如何创建允许用户创建敏感数据发现作业的策略。

在示例中，第一条语句向用户授予 macie2:CreateClassificationJob 权限。这些权限允许用户创建作业。该语句还授予 macie2:DescribeClassificationJob 权限。这些权限允许用户访问现有作业的详细信息。尽管创建作业不需要这些权限，但访问这些详细信息可以帮助用户创建具有唯一配置设置的作业。

示例中的第二条语句允许用户通过使用 Amazon Macie 控制台来创建、配置和查看作业。这些 macie2:ListClassificationJobs 权限允许用户在控制台的作业页面上显示现有作业。语句中的所有其他权限允许用户通过使用控制台上的创建作业页面来配置和创建作业。

```
{
    "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": "*"
        }
    ]
}
```

示例：允许用户管理敏感数据发现作业

此示例展示如何创建策略，以允许用户访问特定敏感数据发现作业（该作业 ID 为 3ce05dbb7ec5505def334104bexample）的详细信息。该示例还允许用户根据需要更改作业的状态。

在示例中，第一条语句向用户授予 macie2:DescribeClassificationJob 和 macie2:UpdateClassificationJob 权限。这些权限分别允许用户检索作业的详细信息和更改作业的状态。第二条语句向用户授予 macie2:ListClassificationJobs 权限，允许用户通过使用 Amazon Macie 控制台上的作业页面访问作业。

```
{
   "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": "*"
 }
   ]
}
```

您也可以允许用户访问 Macie 为该作业发布到 Amazon CloudWatch Logs 的记录数据（日志事件）。为此，您可以添加语句，授予对作业的日志组和流执行 CloudWatch Logs (logs) 操作的权限。例如：

```
"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"
        ]
    }
]
```

有关管理对 CloudWatch Logs 的访问的信息，请参阅 Amazon CloudWatch Logs 用户指南中的管理对 CloudWatch Logs 资源的访问权限的概述。

示例：允许用户查看调查发现

此示例展示如何创建允许用户访问调查发现数据的策略。

在此示例中，`macie2:GetFindings` 和 `macie2:GetFindingStatistics` 权限允许用户通过使用 Amazon Macie API 或 Amazon Macie 控制台来检索数据。这些 `macie2:ListFindings` 权限允许用户通过使用 Amazon Macie 控制台上的摘要控制面板和调查发现页面来检索和查看数据。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

您也可以允许用户为调查发现创建和管理筛选规则和抑制规则。为
此，您可以包括一条语句来授予以下权
限：macie2:CreateFindingsFilter、macie2:GetFindingsFilter、macie2:UpdateFindingsF
和 macie2:DeleteFindingsFilter。要允许用户通过使用 Amazon Macie 控制台来管理规则，还
需要在策略中包括 macie2:ListFindingsFilters 权限。例如：

```
{
    "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": "*"
        }
    ]
}
```

示例：允许用户查看基于标签的自定义数据标识符

在基于身份的策略中，您可以使用条件根据标签控制对 Amazon Macie 资源的访问。此示例展示如何创建策略，用以允许用户通过使用 Amazon Macie 控制台或 Amazon Macie API 来查看自定义数据标识符。但是，仅当Owner标签的值为用户的用户名时才会授予权限。

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

在此示例中，如果拥有用户名 `richard-roe` 的用户尝试查看自定义数据标识符的详细信息，则必须将自定义数据标识符标记为 `Owner=richard-roe` 或 `owner=richard-roe`。否则，该用户将被拒绝访问。条件标签密钥 `Owner` 与 `Owner` 和 `owner` 都匹配，因为条件密钥名称不区分大小写。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

Amazon Macie 的服务相关角色

亚马逊 Macie 使用名为的 AWS Identity and Access Management (IAM) 服务相关角色。AWSServiceRoleForAmazonMacie此服务相关角色是直接链接到 Macie 的独特 IAM 角色。它是由 Macie 预定义的，它包含 Macie 代表你调用其他资源 AWS 服务 和监控 AWS 资源所需的所有权限。Macie 在所有 Macie 可用 的 AWS 区域 使用这个与服务相关的角色。

您可以使用服务相关角色轻松设置 Macie，因为您不必手动添加所需的权限。Macie 定义此服务相关角色的权限，除非另外定义，否则只有 Macie 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

必须配置权限，以允许 IAM 实体（例如用户或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。只有在删除服务相关角色的相关资源后，您才能删除该角色。这可以保护您的资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的AWS 服务，并查找 Service-linked roles（服务相关角色）列中显示为 Yes（是）的服务。请选择是与查看该服务的服务相关角色文档的链接。

主题

Amazon Macie 的服务相关角色权限

Amazon Macie 使用名为 `AWSServiceRoleForAmazonMacie` 的服务相关角色。该服务相关角色信任 `macie.amazonaws.com` 服务担任该角色。

名为 `AmazonMacieServiceRolePolicy` 的角色的权限策略允许 Macie 在指定资源上执行以下任务：

- 使用 Amazon S3 操作检索有关 S3 存储桶和对象的信息。
- 使用 Amazon S3 操作检索 S3 对象。
- 使用 AWS Organizations 操作来检索有关关联账户的信息。
- 使用 Amazon Log CloudWatch s 操作记录敏感数据发现任务的事件。

该角色配置有以下权限策略。

```
{
  "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:*"
      ]
    }
  ]
}
```

有关 AmazonMacieServiceRolePolicy 策略更新的详细信息，请参阅 Amazon Macie AWS 托管式策略更新。要获得有关此政策变更的自动提醒，请在 Macie 文档历史记录页面上订阅 RSS feed。

必须配置权限，以允许 IAM 实体（例如用户或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Amazon Macie 创建服务相关角色

无需手动为 Amazon Macie 创建 AWSServiceRoleForAmazonMacie 服务相关角色。当你为你的启用 Macie 时 AWS 账户，Macie 会自动为你创建与服务相关的角色。

如果删除此 Macie 服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。当您再次启用 Macie 时，Macie 将再次为您创建服务相关角色。

为 Amazon Macie 编辑服务相关角色

Amazon Macie 不允许您编辑 AWSServiceRoleForAmazonMacie 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

为 Amazon Macie 删除服务相关角色

如果您不再使用 Amazon Macie，我们建议您删除 AWSServiceRoleForAmazonMacie 服务相关角色。当您禁用 Macie 时，Macie 不会为您删除该角色。

在删除角色之前，必须在每个启用该角色 AWS 区域 的地方禁用 Macie。您还必须手动清理该角色的资源。要删除角色，您可以使用 IAM 控制台 AWS CLI、或 AWS API。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

> **Note**
>
> 在您尝试删除资源时，如果 Macie 正在使用 AWSServiceRoleForAmazonMacie 角色，删除操作可能会失败。如果发生这种情况，请等待几分钟，然后再次尝试操作。

如果您删除了 AWSServiceRoleForAmazonMacie 服务相关角色然后需要再次创建它，则可以通过为您的账户启用 Macie 再次创建它。当您再次启用 Macie 时，Macie 将再次为您创建服务相关角色。

支持 AWS 区域 Amazon Macie 服务相关角色

Amazon Macie 支持在所有 Macie 可用 AWS 区域 的地方使用AWSServiceRoleForAmazonMacie服务相关角色。有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。

适用于 Amazon Macie 的 AWS 托管式策略

AWS 托管式策略是由 AWS 创建和管理的独立策略。AWS 托管式策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管式策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新在 AWS 托管式策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

Amazon Macie 提供了多种 AWS 托管式策略：AmazonMacieFullAccess策略、AmazonMacieReadOnlyAccess策略和 AmazonMacieServiceRolePolicy策略。

主题

- AWS托管策略：AmazonMacieFullAccess
- AWS托管策略：AmazonMacieReadOnlyAccess
- AWS托管策略：AmazonMacieServiceRolePolicy
- Amazon Macie AWS 托管式策略更新

AWS托管策略：AmazonMacieFullAccess

您还能将 AmazonMacieFullAccess 策略附加到您的 IAM 实体。

该策略授予完全的管理权限，允许 IAM 身份（主体）创建 Amazon Macie 服务相关角色并为 Amazon Macie 执行所有读写操作。这些权限包括创建、更新或删除等转换功能。如果将此策略附加到主体，则主体可以创建、检索和以其他方式访问其账户的所有 Macie 资源、数据和设置。

在主体可以为其账户启用 Macie 之前，必须先将此策略附加到主体 — 必须允许主体创建 Macie 服务相关角色才能为其账户启用 Macie。

权限详细信息

此策略包含以下权限：

- `macie2` – 允许主体为 Amazon Macie 执行所有读写操作。
- `iam` – 允许主体创建服务相关角色。`Resource`元素为 Macie 指定服务相关角色。`Condition`元素使用 `iam:AWSServiceName` 条件密钥和 `StringLike` 条件运算符来为 Macie 限制服务相关角色的权限。
- `pricing` – 允许主体从 AWS Billing and Cost Management 中检索其 AWS 账户的定价数据。当主体创建和配置敏感数据发现作业时，Macie 会使用此数据来计算和显示估计成本。

```
{
   "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": "*"
      }
   ]
}
```

AWS托管策略：AmazonMacieReadOnlyAccess

您还能将 AmazonMacieReadOnlyAccess 策略附加到您的 IAM 实体。

此策略授予只读权限，允许 IAM 身份（主体）为 Amazon Macie 执行所有读操作。权限不包括创建、更新或删除等转换功能。如果将此策略附加到主体，则主体可以检索但不能以其他方式访问其账户的所有 Macie 资源、数据和设置。

权限详细信息

此策略包含以下权限：

macie2 – 允许主体为 Amazon Macie 执行所有读操作。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

AWS托管策略：AmazonMacieServiceRolePolicy

您不能将 AmazonMacieServiceRolePolicy 策略附加到您的 IAM 实体。此策略附加到服务相关角色，允许 Macie 代表您执行操作。有关更多信息，请参阅Amazon Macie 的服务相关角色。

Amazon Macie AWS 托管式策略更新

查看自该服务开始跟踪这些更改以来，有关适用于 Amazon Macie 的 AWS 托管式策略更新的详细信息。要获得有关此页面更改的自动提示，请订阅 Macie 文档历史记录页面上的 RSS 源。

更改	说明	日期
AmazonMacieReadOnlyAccess – 添加了一个新策略	Macie 添加了一个新策略，即 AmazonMacieReadOnlyAccess 策略。此策略授予只读权限，允许主体检索其账户的所有 Macie 资源、数据和设置。	2023 年 6 月 15 日
AmazonMacieFullAccess – 更新了一个现有策略	在 AmazonMacieFullAccess 策略中，Macie 更新了 Macie 服务相关角色（aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie ）的 Amazon 资源名称（ARN）。	2022 年 6 月 30 日
AmazonMacieServiceRolePolicy – 更新了一个现有策略	Macie 从 AmazonMacieServiceRolePolicy 策略中删除了 Amazon Macie Classic 的操作和资源。Amazon Macie Classic 已停用，不再可用。	2022 年 5 月 20 日

更改	说明	日期
	更具体地说，Macie 删除了所有 AWS CloudTrail 操作。Macie 还删除了针对以下资源的所有 Amazon S3 操作：`arn:aws:s3:::awsmacie-*` 、`arn:aws:s3:::awsmacietrail-*` 和 `arn:aws:s3:::*-awsmacietrail-*` 。	
AmazonMacieFullAccess – 更新了一个现有策略	Macie 向 `AmazonMacieFullAccess` 策略中添加了 AWS Billing and Cost Management (`pricing`) 操作。此操作允许主体检索其账户的定价数据。当主体创建和配置敏感数据发现作业时，Macie 会使用此数据来计算和显示估计成本。 Macie 还从 `AmazonMacieFullAccess` 策略中删除了 Amazon Macie Classic (`macie`) 操作。	2022 年 3 月 7 日
AmazonMacieServiceRolePolicy – 更新了一个现有策略	Macie 向 `AmazonMacieServiceRolePolicy` 策略中添加了 Amazon CloudWatch Logs 操作。这些操作允许 Macie 为敏感数据发现作业向 CloudWatch Logs 发布日志事件。	2021 年 4 月 13 日
Macie 开启了跟踪更改	Macie 为其 AWS 托管式策略开启了跟踪更改。	2021 年 4 月 13 日

Amazon Macie 身份和访问问题排查

以下信息可帮助您诊断和修复在使用 Amazon Macie 和 AWS Identity and Access Management (IAM) 时可能会遇到的常见问题。

主题

我无权在 Amazon Macie 中执行操作

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `macie2:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `macie2:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。管理员是向您提供登录凭证的人。

我希望允许我的 AWS 账户以外的人访问我的 Amazon Macie 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Macie 是否支持这些特征，请参阅 Amazon Macie 如何与 AWS Identity and Access Management协同工作。
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方AWS 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的 AWS 账户提供访问权限。

- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Amazon Macie 中的日志记录和监控

Amazon Macie 与 AWS CloudTrail 集成，后者是一项服务，提供用户、角色或其他 AWS 服务 在 Macie 中执行的操作的记录。这包括来自 Amazon Macie 控制台的操作，以及对 Amazon Macie API 操作的编程调用。通过使用 CloudTrail 收集的数据，您可以确定向 Macie 发出的请求内容。对每一个请求，您可以识别请求的时间、发出请求的源 IP 地址以及其他详细信息。有关更多信息，请参阅使用 AWS CloudTrail 记录 Amazon Macie API 调用。

Amazon Macie 的合规性验证

要了解某个 AWS 服务 是否在特定合规性计划范围内，请参阅合规性计划范围内的 AWS 服务 ，然后选择您感兴趣的合规性计划。有关常规信息，请参阅 AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告、。

您使用 AWS 服务 的合规性责任取决于数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南——这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计 – 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

> **Note**
>
> 并非所有 AWS 服务 都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。

- AWS 客户合规指南：从合规角度了解责任共担模式。这些指南总结了保护 AWS 服务 的最佳实践，并将指南映射到跨多个框架的安全控制，包括美国国家标准与技术研究院（NIST）、支付卡行业安全标准委员会（PCI）和国际标准化组织（ISO）。
- 《AWS Config 开发人员指南》中的使用规则评估资源 – 此 AWS Config 服务评测您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub——此 AWS 服务 向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实操。有关受支持服务及控制的列表，请参阅 Security Hub 控制参考。
- AWS Audit Manager – 此 AWS 服务 可帮助您持续审计您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

Amazon Macie 中的恢复能力

AWS 全球基础设施围绕 AWS 区域和可用区而构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

Amazon Macie 中的基础设施安全性

作为一项托管式服务，Amazon Macie 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅安全性支柱 AWS Well-Architected Framework中的基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Macie。客户端必须支持以下内容：

- 传输层安全性协议（TLS） 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（Ephemeral Diffie-Hellman）或 ECDHE（Elliptic Curve Ephemeral Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

Amazon Macie 和接口 VPC 端点 (AWS PrivateLink)

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 托管 AWS 资源，则可以在您的 VPC 和 Amazon Macie 之间建立连接。Amazon VPC 是一项 AWS 服务，可用来启动在虚拟网络中定义的 AWS 资源。借助 VPC，您可以控制您的网络设置，如 IP 地址范围、子网、路由表和网络网关。

要将 VPC 连接到 Macie，请为 Macie 定义一个接口 VPC 端点。接口端点由 AWS PrivateLink 提供支持，该技术支持您通过私有连接访问 Amazon Macie API，而无需采用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例即使没有公有 IP 地址也可与 Amazon Macie API 进行通信。您的 VPC 和 Macie 之间的流量不会脱离 Amazon 网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用接口 VPC 端点访问 AWS 服务。

主题

- Amazon Macie VPC 端点注意事项
- 为 Amazon Macie 创建接口 VPC 端点

Amazon Macie VPC 端点注意事项

Amazon Macie 在除亚太地区（大阪）和以色列（特拉维夫）区域外的所有当前可用 AWS 区域 区域均支持 VPC 端点。有关当前已推出 Macie 的所有区域的列表，请参阅 AWS 一般参考 中的 Amazon Macie 端点和配额。此外，Macie 支持从一个 VPC 调用其所有 API 操作。

如果您为 Macie 创建接口 VPC 端点，请考虑对其他提供 VPC 支持并与 Macie 集成的 AWS 服务（例如 Amazon EventBridge 和 AWS Security Hub）执行同样的操作。然后，Macie 和这些服务就可以使用 VPC 端点进行集成。例如，如果您为 Macie 创建一个 VPC 端点，为 Security Hub 创建一个 VPC 端点，则 Macie 可以在将调查发现发布到 Security Hub 时使用其 VPC 端点，Security Hub 可以在收到调查发现时使用其 VPC 端点。有关支持 VPC 端点的服务的信息，请参阅 Amazon VPC 用户指南中与与 AWS PrivateLink 集成的 AWS 服务。

有关其他注意事项，请参阅 Amazon VPC 用户指南中的使用接口 VPC 端点访问 AWS 服务。

请注意，Macie 不支持 VPC 端点策略。默认情况下，允许通过端点对 Macie 进行完全访问。有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 端点和 VPC 端点服务的身份和访问管理。

为 Amazon Macie 创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 Amazon Macie 服务创建接口 VPC 端点。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC 端点。

当您为 Macie 创建 VPC 端点时，请使用以下服务名称：

- com.amazonaws.*region*.macie2

其中*##*是适用的区域代码AWS 区域。

如果为端点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Macie 发出 API 请求，例如，美国东部（弗吉尼亚州北部）区域为 `macie2.us-east-1.amazonaws.com`。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用接口 VPC 端点访问 AWS 服务。

使用 AWS CloudTrail 记录 Amazon Macie API 调用

Amazon Macie 与 AWS CloudTrail 集成，后者是一项服务，提供用户、角色或其他 AWS 服务 在 Macie 中执行的操作的记录。CloudTrail 将 Macie 的所有 API 调用作为事件捕获。捕获的调用中包括通过 Amazon Macie 控制台的调用和对 Amazon Macie API 操作的编程调用。

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶（包括 Macie 事件）。如果不配置跟踪，则仍可以使用 AWS CloudTrail 控制台上的事件历史记录来查看最近的事件。使用 CloudTrail 收集的信息，您可以确定向 Macie 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

主题

AWS CloudTrail 中的 Amazon Macie 信息

当您创建 AWS 账户 账户时，即针对该账户启用了 AWS CloudTrail。当 Amazon Macie 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 事件一起保存在事件历史记录中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参见《AWS CloudTrail 用户指南》的 使用 CloudTrail 事件历史记录。

要持续记录 AWS 账户 中的事件（包括 Macie 的事件），请创建跟踪。跟踪记录让 CloudTrail 可以将日志文件发送至 Amazon Simple Storage Service (Amazon S3) 存储桶。默认情况下，使用 AWS CloudTrail 控制台创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区所有区域的事件，将日志文件传送至指定的 S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日记账中收集的事件数据并采取行动。有关更多信息，请参阅 AWS CloudTrail 用户指南 中的以下主题：

- 为您的 AWS 账户 创建跟踪
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件
- 从多个账户接收 CloudTrail 日志文件

所有 Macie 操作都由 CloudTrail 记录，并记录在 Amazon Macie API 参考中。例如，对 `CreateClassificationJob`、`DescribeBuckets` 和 `ListFindings` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务 发出。

有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 CloudTrail userIdentity 元素。

了解 Amazon Macie 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon Simple Storage Service（Amazon S3）存储桶。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。AWS CloudTrail 日志文件包含有关事件的一个或多个日志条目。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例演示了说明 Amazon Macie 操作的 CloudTrail 日志条目。要详细了解日志条目可能包含的信息，请参阅《AWS CloudTrail 用户指南》中的 CloudTrail 日志事件参考。

示例：列出调查发现

以下示例演示的 CloudTrail 日志条目说明了一个有关 Macie ListFindings 操作的事件。在此示例中，一个 AWS Identity and Access Management（IAM）用户（`Mary_Major`）使用 Amazon Macie 控制台来检索其账户中有关当前策略调查发现的部分信息。


```
{
    "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"
}
```

示例：检索调查发现的敏感数据样本

此示例演示的 CloudTrail 日志条目说明了有关检索和显示 Macie 在调查发现中所报告敏感数据样本的事件。在此示例中，一个 JohnDoe（IAM）用户使用 Amazon Macie 控制台来检索和显示敏感数据样本。该用户的 Macie 账户配置通过代入 IAM 角色（MacieReveal）来检索和显示敏感数据样本。

以下日志事件演示了有关该用户请求通过执行 Macie GetSensitiveDataOccurrences 操作来检索和显示敏感数据样本的详细信息。


```
{
    "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"
}
```

下一个日志事件演示了有关 Macie 随后通过执行 AWS Security Token Service（AWS STS）AssumeRole 操作，来代入指定的 IAM 角色（MacieReveal）的详细信息。

```
{
    "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"
}
```

为 Amazon Macie 资源添加标签

标签是一个可选标签，您可以将其定义并分配给 AWS 资源，包括某些类型的 Amazon Macie 资源。标签可以帮助您以不同的方式识别、分类和管理资源，例如，按用途、所有者、环境或其他标准。例如，您可以使用标签来应用策略、分配成本、区分资源版本，或识别支持特定合规性要求或工作流的资源。

您可以将标签分配给以下类型的 Macie 资源：允许列表、自定义数据标识符、调查发现的筛选规则和抑制规则，以及敏感数据发现作业。如果您是组织的 Macie 管理员，还可以将标签分配给组织中的成员账户。

主题

标签基础知识

一个资源可具有最多 50 个标签。每个标签都包含您定义的一个标签键和一个可选的标签值。标签键是一种常见的标签，充当更具体的标签值的类别。标签值 充当标签键的描述符。

例如，如果您创建自定义数据标识符和敏感数据发现作业来分析工作流程中不同点的数据（一组用于暂存数据，另一组用于生产数据），您可以为这些资源分配一个 `Stack` 标签键。此标签键的标签值可能为 `Staging`，适用于分析暂存数据的自定义数据标识符和作业，以及 `Production`，适用于其他标识符和作业。

在为资源定义并分配标签时，请注意以下几点：

- 每个资源最多可以有 50 个标签。
- 对于每个资源，每个标签键都必须是唯一的，并且只能有一个标签值。
- 标签键和值区分大小写。作为最佳实践，我们建议您定义标签大写的策略，并在您的资源中一致地实施该策略。
- 标签键最多可以包含 128 个 UTF-8 字符。标签值最多可以包含 256 个 UTF-8 字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @

- aws：前缀专门预留供 AWS 使用。您不能在您定义的任何标签键或值中使用它。此外，您无法更改或删除使用此前缀的标签键或值。使用此前缀的标签不计入每个资源的 50 个标签配额中。
- 您分配的任何标签仅适用于您的 AWS 账户 并且仅在您分配它们的 AWS 区域 中可用。
- 如果删除资源，则分配给该资源的所有标签也将被删除。

有关其他限制、提示和最佳实践，请参阅《标签AWS资源用户指南》。

> **Important**
>
> 不要在标签中存储机密或其他类型的敏感数据。标签可供许多 AWS 服务 访问，包括 AWS Billing and Cost Management。它们不适合用于敏感数据。

要为 Macie 资源添加和管理标签，您可以使用 Amazon Macie 控制台、Amazon Macie API、AWS Resource Groups 控制台上的标签编辑器或AWS Resource Groups Tagging API。借助 Macie，在创建资源时，您可以将标签添加到资源中。您还可以为单个现有资源添加和管理标签。通过资源组，您可以为跨多个 AWS 服务（包括 Macie）的多个现有资源批量添加和管理标签。有关更多信息，请参阅标记 AWS 资源用户指南。

在 IAM policy 中使用标签

开始为资源添加标签后，您可以在AWS Identity and Access Management (IAM) policy 中定义基于标签的资源级权限。通过这种方式使用标记，您可以更全面地控制您 AWS 账户 中的哪些用户和角色有权创建和标记资源，以及哪些用户和角色有权添加、编辑和删除标签。要基于标签控制访问，您可以在 IAM policy 的条件元素中使用与标签相关的条件密钥。

例如，您可以创建一个策略，允许用户拥有对所有 Amazon Macie 资源的完全访问权限，前提是该资源的 Owner 标签指定了他们的用户名：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
```

```
            }
        }
    ]
}
```

如果您定义基于标签的资源级权限，该权限立即生效。这意味着，您的资源在创建后会更安全，而且您可以快速开始将标签用于新资源。您还可以使用资源级权限来控制哪些标签键和值可以与新的和现有资源关联。有关更多信息，请参阅 IAM 用户指南中的使用标签控制对 AWS 资源的访问权限。

向 Amazon Macie 资源添加标签

要向单个 Amazon Macie 资源添加标签，您可以使用 Amazon Macie 控制台或 Amazon Macie API。要同时向多个 Macie 资源添加标签，请使用 AWS Resource Groups 控制台上的标签编辑器或 AWS Resource GroupsTagging API 的标签操作。

> **Important**
>
> 向资源添加标签可能会影响对该资源的访问。在向资源添加标签之前，请查看任何可能使用标签控制资源访问权限的AWS Identity and Access Management (IAM) policy。

Console

当您创建允许列表、自定义数据标识符或敏感数据发现作业时，Amazon Macie 控制台会提供向资源添加标签的选项。创建资源时，请按照控制台上的说明为这些类型的资源添加标签。要向组织中的筛选规则或抑制规则或成员账户添加标签，必须先创建资源，然后才能向其添加标签。

要使用 Amazon Macie 控制台向现有资源添加一个或多个标签，请按照以下步骤操作。

要将标签添加到资源中

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 根据要添加标签的资源类型，请执行以下操作之一：

   - 要查看允许列表，请在导航窗格中选择 允许列表。

     然后在表格中选择该列表的复选框。然后在 操作菜单中选择 管理标签。
   - 要获取自定义数据标识符，请在导航窗格中选择自定义数据标识符。

     然后，在表中选中自定义数据标识符的复选框。然后在操作菜单中选择管理标签。

- 要查看筛选规则或抑制规则，请在导航窗格中选择 调查发现。

  然后，在 已保存的规则列表中，选择规则旁边的编辑图标
  ()。
  然后选择 Manage tags（管理标签）。
- 对于组织中的成员账户，请在导航窗格中选择账户。

  然后，在表中选中账户的复选框。然后在 操作菜单中选择 管理标签。
- 对于敏感数据发现作业，请在导航窗格中选择 作业。

  然后，在表中选中作业的复选框。然后在 操作菜单中选择 管理标签。

  管理标签窗口列出了当前分配给资源的所有标签。

3. 在 管理标签中，选择 编辑标签。
4. 选择 Add tag (添加标签)。
5. 在键框中，输入要添加到资源的标签键。随后，在值框中，可以选择为键输入一个标签值。

   一个标签键可以包含多达 128 个字符。一个标签值可以包含多达 256 个字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @
6. （可选）要向资源添加另一个标签，请选择添加标签，然后重复前面的步骤。您可以为资源分配多达 50 个标签。
7. 完成添加标签后，选择 保存。

API

要创建资源并以编程方式向其添加一个或多个标签，请对要创建的资源类型使用相应的 `Create` 操作：

- 允许列表 – 使用 createAllowList 操作，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，则运行 create-allow-list 命令。
- 自定义数据标识符 – 使用 createCustomDataidentifier 操作，或者，如果您使用的是 AWS CLI，则运行 create-customDataidentifier 命令。
- 筛选或抑制规则 – 使用 createFindingsFilter 操作，或者，如果您使用的是 AWS CLI，则运行 create-findings-filter 命令。
- 成员账户 – 使用 CreateMember 操作，或者，如果您使用的是 AWS CLI，则运行 create-Member 命令。

- 敏感数据发现作业 – 使用 CreateClassivationJob 操作，或者，如果您使用的是 AWS CLI，则运行 create-classification-job 命令。

在您的请求中，使用 tags 参数为要添加到资源的每个标签指定标签键（key）和可选的标签值（value）。tags 参数指定标签键及其关联标签值的字符串到字符串映射。

要向现有资源添加一个或多个标签，请使用 Amazon Macie API 的 tagResource 操作，或者，如果您使用的是 AWS CLI，则运行 tag-resource 命令。在您的请求中，指定您要向其添加标签的资源的 Amazon 资源名称（ARN）。使用 tags 参数为要添加到资源的每个标签指定标签键 (key) 和可选的标签值 (value)。与 Create 操作和命令一样，tags 参数指定标签键及其关联标签值的字符串到字符串的映射。

例如，以下 AWS CLI 命令将具有 Production 标签值的 Stack 标签键添加到指定作业：此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

其中：

- resource-arn 指定要添加标签的作业的 ARN。
- *Stack* 是要添加到作业的标签的标签键。
- *Production* 是指定标签键的标签值 (*Stack*)。

在以下示例中，该命令向作业添加了多个标签：

```
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\"}
```

对于 tags 映射中的每个标签，都需要 key 和 value 参数。但是，value 参数的值可以是空字符串。如果您不想将标签值与标签键相关联，请不要为 value 参数指定值。例如，以下 AWS CLI 命令添加了一个没有关联标签值的 Owner 标签键：

```
C:\> aws macie2 tag-resource ^
```

```
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

如果标签操作成功，Macie 将返回一个空的 HTTP 204 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

查看 Amazon Macie 资源的标签

您可以使用 Amazon Macie 控制台或 Amazon Macie API 查看 Amazon Macie 资源的标签（包括标签键和标签值）。如果您希望同时对多个 Macie 资源执行此操作，则可以使用 AWS Resource Groups 控制台上的标签编辑器或 AWS Resource GroupsTagging API 的标签操作。

Console

使用 Amazon Macie 控制台，按照以下步骤来查看资源的标签。

要查看资源的标签

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 根据您要查看其标签的资源类型，请执行以下操作之一：

   - 要查看允许列表，请在导航窗格中选择允许列表。

     然后在表格中选择该列表的复选框。然后在 操作菜单中选择 管理标签。
   - 要获取自定义数据标识符，请在导航窗格中选择 自定义数据标识符。

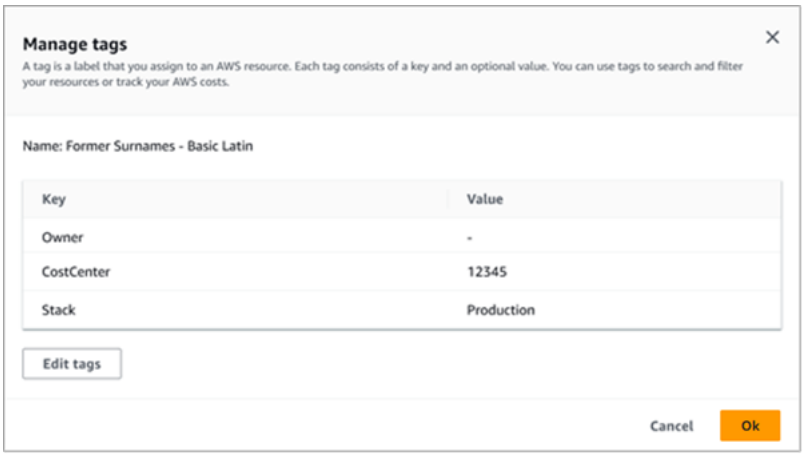
     然后，在表中选中自定义数据标识符的复选框。然后在 操作菜单中选择 管理标签。
   - 要查看筛选规则或抑制规则，请在导航窗格中选择 调查发现。

     然后，在 已保存的规则列表中，选择规则旁边的编辑图标 ()。
     然后选择 Manage tags（管理标签）。
   - 对于组织中的成员账户，请在导航窗格中选择 账户。

     然后，在表中选中账户的复选框。然后在 操作菜单中选择 管理标签。
   - 对于敏感数据发现作业，请在导航窗格中选择 作业。

     然后，在表中选中作业的复选框。然后在 操作菜单中选择 管理标签。

管理标签窗口列出了当前分配给资源的所有标签。例如，下图显示分配给自定义数据标识符的标签。



在此示例中，为自定义数据标识符分配了三个标签：没有关联标签值的 Owner 标签键；以 12345 作为关联标签值的 CostCenter 标签键；以及以 Production 作为关联标签值的 Stack 标签键。

3. 查看完标签后，选择取消关闭窗口。

API

要以编程方式检索和查看现有资源的标签，您可以对要查看标签的资源类型使用相应的 `Get` 或 `Describe` 操作。例如，如果您使用 getCustomDataidentifier 操作或从 AWS Command Line Interface (AWS CLI) 中运行 get-custom-data-identifier 命令，则响应将包含一个 `tags` 对象。该对象列出了当前分配给资源的所有标签（包括标签键和标签值）。

还可以使用 Amazon Macie API 的 ListTagsForResource 操作。在您的请求中，使用 `resourceArn` 参数指定资源的Amazon 资源名称（ARN）。如果您使用的是 AWS CLI，请运行 list-tags-for-resource 命令并使用参数 `resource-arn` 指定资源的 ARN。例如：

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

在前面的示例中，*arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample* 是现有敏感数据发现作业的 ARN。

如果操作成功，Macie 将返回一个 `tags` 对象，其中列出了当前分配给资源的所有标签（包括标签键和标签值）。例如：

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

其中 Stack、CostCenter 和 Owner 是分配给资源的标签键。Production 是与 Stack 标签键关联的标签值。 12345 是与 CostCenter 标签键关联的标签值。Owner 标签键没有关联的标签值。

要检索所有带有标签的 Macie 资源以及分配给每个资源的所有标签的列表，请使用 AWS Resource GroupsTagging API 的 GetResources 操作。在您的请求中，将 ResourceTypeFilters 参数的值设置为 macie2。要执行此操作，使用 AWS CLI，并请运行 get-resources 命令并将 resource-type-filters 参数的值设置为 macie2。例如：

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

如果操作成功，Resource Groups 将返回一个 ResourceTagMappingList 数组，其中包含所有带有标签的 Macie 资源的 ARN，以及分配给每个资源的标签键和值。

编辑 Amazon Macie 资源的标签

要编辑 Amazon Macie 资源的标签（标签键或标签值），您可以使用 Amazon Macie 控制台或 Amazon Macie API。要同时对多个 Macie 资源执行此操作，请使用 AWS Resource Groups 控制台上的标签编辑器或标记 AWS Resource Groups API 的标记操作。

> **Important**
>
> 编辑资源的标签可能会影响对资源的访问。在编辑资源的标签键或值之前，请查看可能使用该标签控制资源访问权限的任何 AWS Identity and Access Management (IAM) policy 。

Console

按照以下步骤使用 Amazon Macie 控制台编辑资源的标签。

要编辑资源的标签

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 根据要编辑标签的资源类型，执行下列操作之一：

   - 要查看允许列表，请在导航窗格中选择 允许列表。

     然后在表格中选择该列表的复选框。然后在 操作菜单中选择 管理标签。
   - 要获取自定义数据标识符，请在导航窗格中选择 自定义数据标识符。

     然后，在表中选中自定义数据标识符的复选框。然后在 操作菜单中选择 管理标签。
   - 要查看筛选规则或抑制规则，请在导航窗格中选择 调查发现。

     然后，在 已保存的规则列表中，选择规则旁边的编辑图标
     ()。
     然后选择 Manage tags（管理标签）。
   - 对于组织中的成员账户，请在导航窗格中选择 账户。

     然后，在表中选中账户的复选框。然后在 操作菜单中选择 管理标签。
   - 对于敏感数据发现作业，请在导航窗格中选择 作业。

     然后，在表中选中作业的复选框。然后在 操作菜单中选择 管理标签。

   管理标签窗口列出了当前分配给资源的所有标签。
3. 在 管理标签中，选择 编辑标签。
4. 执行以下任一操作：

   - 要向标签键添加标签值，请在标签键旁边的 值框中输入该值。
   - 要更改现有标签键，请选择标签旁边的 移除。然后选择 添加标签。在出现的 键框中，输入新的标签键。在值框中，可以选择输入相关的标签值。
   - 要更改现有标签值，请在包含该值的 值框中选择 X。然后在值框中键入新的标签值。
   - 要删除现有标签值，请在包含该值的 值框中选择 X。
   - 要删除现有标签（标签键和标签值），请选择标签旁边的 移除。

   一个资源可具有最多 50 个标签。一个标签键可以包含多达 128 个字符。一个标签值可以包含多达 256 个字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @

5. 完成对标签的编辑之后，选择 保存。

API

当您以编程方式编辑资源的标签时，会用新值覆盖现有标签。因此，编辑标签的最佳方法取决于您是要编辑标签键、标签值还是两者都有。要编辑标签键，请删除当前标签并添加新标签。

要仅编辑或删除与标签键关联的标签值，请使用 Amazon Macie API 的 TagResource 操作覆盖现有值，或者如果您使用的是 AWS Command Line Interface (AWS CLI)，则运行 tag-resource 命令。在您的请求中，指定要编辑或删除标签值的资源的 Amazon 资源名称（ARN）。

要编辑标签键的标签值，请使用 `tags` 参数指定要更改其标签值的标签键，并为该键指定新的标签值。例如，以下命令将分配给指定敏感数据发现作业的 `Stack` 标签键的标签值从 `Production` 更改为 `Staging`。此示例针对 Microsoft Windows 进行格式化，并使用脱字号 (^) 行继续符来提高可读性。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

其中：

- `resource-arn` 指定作业的 ARN。
- *`Stack`* 是与要更改的标签值关联的标签键。
- *`Staging`* 是指定标签键 (*`Stack`*) 的新标签值。

要从标签键中删除标签值，请不要为 `tags` 参数中的 `value` 参数指定值。例如：

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

如果操作成功，Macie 将返回一个空的 HTTP 204 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

从 Amazon Macie 资源中删除标签

要从 Amazon Macie 资源中删除标签，您可以使用 Amazon Macie 控制台或 Amazon Macie API。要同时对多个 Macie 资源执行此操作，请使用 AWS Resource Groups 控制台上的标签编辑器或标记 AWS Resource Groups API 的标记操作。

> **Important**
>
> 从资源中删除标签可能对影响资源访问。在删除标签之前，请查看可能使用该标签控制资源访问权限的任何 AWS Identity and Access Management(IAM) policy 。

Console

按照以下步骤使用 Amazon Macie 控制台从资源中删除一个或多个标签。

要从资源中删除标签

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/。
2. 根据您要从中删除标签的资源类型，执行以下任一操作：

   - 要查看允许列表，请在导航窗格中选择 允许列表。

     然后在表格中选择该列表的复选框。然后在 操作菜单中选择 管理标签。
   - 要获取自定义数据标识符，请在导航窗格中选择 自定义数据标识符。

     然后，在表中选中自定义数据标识符的复选框。然后在 操作菜单中选择 管理标签。
   - 要查看筛选规则或抑制规则，请在导航窗格中选择 调查发现。

     然后，在 已保存的规则列表中，选择规则旁边的编辑图标 ( )。然后选择 Manage tags（管理标签）。
   - 对于组织中的成员账户，请在导航窗格中选择 账户。

     然后，在表中选中账户的复选框。然后在 操作菜单中选择 管理标签。
   - 对于敏感数据发现作业，请在导航窗格中选择 作业。

     然后，在表中选中作业的复选框。然后在 操作菜单中选择 管理标签。

管理标签窗口列出了当前分配给资源的所有标签。

3. 在 管理标签中，选择 编辑标签。
4. 执行以下任一操作：
   - 如果仅删除标签的标签值，请在包含要删除的值的 值框中选择 X。
   - 要同时删除标签的标签键和标签值（成对），请在要删除的标签旁边选择 移除。
5. （可选）要从资源中删除更多标签，请对每个要删除的其他标签重复上述步骤。
6. 完成删除标签后，选择 保存。

API

要以编程方式从资源中删除一个或多个标签，请使用 Amazon Macie API 的 UntagResource 操作。在您的请求中，使用 `resourceArn` 参数指定要删除标签的资源的 Amazon 资源名称（ARN）。使用 `tagKeys` 参数指定要删除的标签的标签键。如果仅从资源中删除特定的标签值（而不是标签键），请编辑标签而不是删除标签。

如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行 untag-resource 命令并使用 `resource-arn` 参数指定要删除标签的资源的 ARN。使用 `tag-keys` 参数指定要删除的标签的标签键。例如，以下命令从指定的敏感数据发现作业中删除 `Stack` 标签（标签键和标签值）：

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

其中，`resource-arn` 指定要删除标签的作业的 ARN，*`Stack`* 是要删除的标签的标签键。

要从资源中删除多个标签，请添加每个额外的标签键作为 `tag-keys` 参数的参数。例如：

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

其中，`resource-arn` 指定要删除标签的作业的 ARN，*`Stack`* 和 *`Owner`* 是要删除的标签的标签键。

如果操作成功，Macie 将返回一个空的 HTTP 204 响应。否则，Macie 会返回一个 HTTP 4xx 或 500 响应，说明操作失败的原因。

使用 AWS CloudFormation 创建 Amazon Macie 资源

Amazon Macie 与 AWS CloudFormation 集成，后者是一项服务，可帮助您对 AWS 资源进行建模和设置，这样您只需花较少的时间来创建和管理资源与基础设施。您可以创建一个描述所需的全部 AWS 资源的模板（例如自定义数据标识符），AWS CloudFormation 将为您预置和配置这些资源。

在您使用 AWS CloudFormation 时，可重复使用您的模板来不断地重复设置您的 Macie 资源。描述您的资源一次，然后在多个 AWS 账户 和 AWS 区域 中反复预置相同的资源。

主题

Amazon Macie 和AWS CloudFormation模板

要为 Amazon Macie 和相关服务设置和配置资源，您必须了解 AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述要在 AWS CloudFormation 堆栈中调配的资源。

如果您不熟悉 JSON 或 YAML，可以使用 AWS CloudFormation 设计器，此图形工具可用于创建和修改 AWS CloudFormation 模板。通过使用 Designer，您可以使用拖放界面以图表形式查看模板资源，然后使用集成的 JSON 和 YAML 编辑器编辑其详细信息。有关更多信息，请参阅AWS CloudFormation用户指南中的什么是 AWS CloudFormation Designer？。

您可以为以下类型的 Macie 资源创建AWS CloudFormation模板：

- 允许列表
- 自定义数据标识符
- 调查发现的筛选规则和抑制规则，也称为调查发现筛选条件

有关更多信息（包括此类资源的 JSON 和 YAML 模板示例），请参阅 AWS CloudFormation 用户指南中的 Amazon Macie 资源类型参考。

了解有关 AWS CloudFormation 的更多信息

要了解有关 AWS CloudFormation 的更多信息，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 参考
- AWS CloudFormation 命令行界面用户指南

暂停或禁用 Amazon Macie

您可以使用 Amazon Macie 主机或 Amazon Macie API 在特定 AWS 区域 中暂停或禁用 Amazon Macie。Macie 将停止在该区域中为您的账户执行所有活动。在 Macie 暂停或禁用期间，您无需支付在该区域使用 Macie 的费用。

如果您暂停或禁用 Macie，则可以在以后重新启用。

主题

暂停 Amazon Macie

如果您暂停了 Amazon Macie，Macie 将在适用的 AWS 区域 中保留您账户的会话标识符、设置和资源。例如，您的现有调查发现保持不变，最多可保留 90 天。但是，当您暂停 Macie 时，它会停止在适用区域中为您的账户执行所有活动。这包括监控您的 Amazon Simple Storage Service (Amazon S3) 数据、执行自动敏感数据发现以及运行当前正在进行的任何敏感数据发现作业。Macie 还会取消您在该区域的所有敏感数据发现作业。

暂停 Macie 后，您可以重新启用它。然后，您可以重新访问适用区域中的设置和资源，并且 Macie 会恢复您的账户在该区域中的活动。这包括为您的账户更新 S3 存储桶清单，并监控这些存储桶以实现安全性和访问控制。这不包括恢复或重启您的敏感数据发现作业。敏感数据发现作业在取消后无法恢复或重新启动。

本主题介绍如何使用 Amazon Macie 主机暂停 Macie。如果您倾向于以编程方式执行此操作，则可以使用 Amazon Macie API 的 UpdateMacieSession 操作。

> **Note**
>
> 如果您是组织的 Macie 管理员，则必须删除与您的账户关联的所有成员账户，然后您才能为您的账户暂停 Macie。有关更多信息，请参阅管理多个 账户。

要暂停 Macie

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中暂停 Macie 的区域。

3. 在导航窗格中，选择设置。
4. 选择 暂停 Macie。
5. 提示进行确认时，输入 **Suspend**，然后选择 暂停。

要在其他区域暂停 Macie，请在每个其他区域重复上述步骤。

禁用 Amazon Macie

当您禁用 Amazon Macie 时，Macie 将停止在适用 AWS 区域 中为您的账户执行所有活动。这包括监控您的 Amazon Simple Storage Service (Amazon S3) 数据、执行自动敏感数据发现以及运行当前正在进行的任何敏感数据发现作业。Macie 还会删除在适用区域为您的账户存储或维护的所有现有设置和资源，包括您的调查发现和敏感数据发现作业。您存储或发布给其他 AWS 服务 的数据保持不变且不受影响，例如，Amazon S3 中的敏感数据调查发现以及 Amazon EventBridge 中的调查发现事件。

> **Warning**
>
> 如果您禁用 Macie，则还会永久删除 Macie 在适用区域为您的账户存储或维护的所有现有调查发现、敏感数据发现作业、自定义数据标识符和其他资源。这些资源在删除后将无法恢复。要保留资源并仅暂停使用 Macie，请暂停而不是禁用 Macie。

本主题介绍如何使用 Amazon Macie 主机禁用 Macie。如果您倾向于以编程方式执行此操作，则可以使用 Amazon Macie API 的 DisableMacie 操作。

> **Note**
>
> 如果您的账户属于集中管理多个 Macie 账户的组织，则必须执行以下操作，然后您才能禁用 Macie：
>
> - 如果您的账户是 Macie 成员账户，请与您的 Macie 管理员合作，将您的账户作为成员账户移除。
> - 如果您的账户是 Macie 管理员账户，请移除与您的账户关联的所有成员账户，并删除您的账户与这些账户之间的关联。
>
> 完成上述任务的方式取决于您的 Macie 账号是通过 AWS Organizations 还是通过邀请与其他账号关联。有关更多信息，请参阅管理多个 账户。

要禁用 Macie

1. 通过以下网址打开 Amazon Macie 控制台：https://console.aws.amazon.com/macie/
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中禁用 Macie 的区域。
3. 在导航窗格中，选择设置。
4. 选择禁用 Macie 。
5. 提示进行确认时，输入 **`Disable`**，然后选择 禁用。

要在其他区域禁用 Macie，请在每个其他区域重复上述步骤。

Amazon Macie 限额

对于每项 AWS 服务，您的 AWS 账户都有某些默认限额（以前称为限制）。这些限额是您账户的服务资源或操作的最大数量。本主题列出了适用于您的账户的 Amazon Macie 资源和操作的限额。除非另有说明，否则每个限额均适用于您在每个 AWS 区域中的账户。

一些限额可以提升，而另一些限额不能提升。要请求增加配额，您可以使用服务限额控制台。要了解如何申请增加配额，请参阅服务限额用户指南中的请求增加配额。如果服务限额控制台上没有限额，请使用 AWS Support Center Console 上的提高服务限制表单请求增加限额。

账户

- 通过邀请的成员账户：1,000 个
- 通过 AWS Organizations 的成员账户：10,000 个

调查发现

- 每个账户的筛选规则和抑制规则：1,000 个
- 每次运行敏感数据发现作业的调查发现：100,000 + 达到 100,000 阈值后任何剩余调查发现的 5%

  此限额仅适用于 Amazon Macie 控制台和 Amazon Macie API。Macie 发布到 Amazon EventBridge 的调查发现事件数量或 Macie 为每次作业运行创建的敏感数据发现结果数量没有限额。
- 每个敏感数据调查发现的检测位置：15 个
- 从 Amazon S3 对象中检索和显示敏感数据样本的请求数量：每天 100 个

  此限额每 24 小时在 00:00:01 UTC+0 重置一次。
- 用于检索和泄露敏感数据样本的 Amazon S3 对象的大小：
  - Apache Avro 对象容器 (.avro) 文件：70 MB
  - Apache Parquet (.parquet) 文件：100 MB
  - CSV (.csv) 文件：255 MB
  - GNU Zip 压缩存档（.gz 或 .gzip）文件：90 MB
  - JSON 或 JSON Lines（.json 或.jsonl）文件：25 MB
  - Microsoft Excel 工作簿 (.xlsx) 文件：20 MB
  - 非二进制文本 (text/plain) 文件大小：100 MB
  - TSV (.tsv) 文件：75 MB

- ZIP 压缩存档 (.zip) 文件：355 MB

如果调查发现适用于为相应 敏感数据发现结果 生成多个 .gz 文件的存档文件，则无法从该存档文件中检索和显示敏感数据样本。

敏感数据发现

- 每个账户按敏感数据发现作业进行的每月分析：5 TB

  此限额仅适用于敏感数据发现作业。要将限额增加到 1,000 TB (1 PB)，请使用服务限额控制台。要申请增加超过 1 PB 的费用，请使用 AWS Support Center Console 上的提高服务限制表单。
- 每个账户的自定义数据标识符：10,000 个
- 每个账户的允许列表：10 个，1–5 个允许列表用于指定预定义文本，1–5 个允许列表用于指定正则表达式

  其他限额适用于指定预定义文本的允许列表。该列表不能包含超过 100,000 个条目，列表的存储大小不能超过 35 MB。
- 要从自动敏感数据发现中排除的 S3 存储桶：1,000 个

  如果您的账户是组织的 Macie 管理员账户，则此限额适用于您的整个组织。
- 每个敏感数据发现作业的 S3 存储桶：1,000 个

  此限额不适用于使用运行时系统存储桶标准来确定要分析哪些存储桶的作业。仅当您将作业配置为分析所选的特定存储桶时，它才适用于该作业。如果您的账户是组织的 Macie 管理员账户，您可以选择多达 1,000 个存储桶，涵盖组织中多达 1,000 个账户。
- 每个敏感数据发现作业的自定义数据标识符：30 个
- 每个敏感数据发现作业的允许列表：10 个，1–5 个允许列表用于指定预定义文本，1–5 个允许列表用于指定正则表达式
- CreateClassificationJob 操作：每秒 0.1 个请求
- 分析单个文件所需的时间：10 小时
- 要分析的单个文件的大小：
  - Adobe 便携式文档格式 (.pdf) 文件：1,024 MB
  - Apache Avro 对象容器 (.avro) 文件：8 GB
  - Apache Parquet (.parquet) 文件：8 GB
  - 电子邮件消息 (.eml) 文件：20 GB

  - GNU Zip 压缩存档（.gz 或 .gzip）文件：8 GB
  - Microsoft Excel 工作簿（.xls 或 .xlsx）文件：512 MB
  - Microsoft Word 文档（.doc 或 .docx）文件：512 MB
  - 非二进制文本文件：20 GB
  - TAR 存档 (.tar) 文件：20 GB
  - ZIP 压缩存档 (.zip) 文件：8 GB

  如果文件大于适用限额，则 Macie 不会分析该文件中的任何数据。
- 提取和分析压缩或存档文件中的数据：
  - 存储大小（压缩）：GNU Zip 压缩存档（.gz 或 .gzip）文件或 ZIP 压缩存档（.zip）文件为 8 GB；TAR 存档 (.tar) 文件为 20 GB
  - 嵌套存档深度：10 级
  - 提取的文件：1,000,000 个
  - 提取的字节：总共有 10 GB 的未压缩数据。使用支持的文件类型或存储格式的每个提取文件都有 3 GB 的未压缩数据。

  如果压缩或存档文件的元数据表明该文件包含 10 个以上的嵌套级别，或者超过了存储大小或提取字节的适用限额，则 Macie 不会提取或分析该文件中的任何数据。如果 Macie 开始提取和分析压缩或存档文件中的数据，并随后确定该文件包含超过 1,000,000 个文件或超过提取字节的限额，则 Macie 会停止分析文件中的数据，并仅就已处理的数据创建敏感数据调查发现和发现结果。
- 分析结构化数据中的嵌套元素：每个文件 256 级

  此限额仅适用于 JSON (.json) 和 JSON Lines (.jsonl) 文件。如果任一类型的文件的嵌套深度超过此限额，则 Macie 不会分析该文件中的任何数据。
- 每个敏感数据发现结果的检测位置：每种敏感数据检测类型 1,000 个
- 检测全名：每个文件 1,000 个，包括存档文件

  Macie 检测到文件中出现前 1,000 次全名后，Macie 停止递增计数并报告全名的位置数据。
- 邮寄地址检测：每个文件 1,000 个，包括存档文件

  Macie 检测到文件中出现的前 1,000 次邮寄地址后，Macie 停止递增计数并报告邮寄地址的位置数据。

Amazon Macie 用户指南的文档历史记录

下表列出了自 Amazon Macie 上一次发布以来对文档所做的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

最新文档更新：2024 年 2 月 20 日

变更	说明	日期
新功能	AWS Security Hub 现在提供了用于检查 Macie 状态的安全控件，并自动发现账户的敏感数据。如果启用了这些控件，Security Hub 会定期运行安全检查，以确定是否为 AWS 账户（Macie .1 控件）启用了 Maci e，以及是否为 Macie 账户（Macie.2 控件）启用了自动敏感数据发现。	2024年2月20日
新功能	Macie 现在可以分析使用双层服务器端加密 AWS KMS keys (DSSE-KMS) 加密的 Amazon S3 对象。现在，当 Macie 执行自动敏感数据发现或您运行敏感数据发现任务时，可以对这些对象进行分析。此外，使用 DSSE-KMS 加密的 S3 存储桶和对象现在包含在 Macie 提供的有关您的 Amazon S3 数据的统计数据和元数据中。	2024 年 1 月 17 日
新特征	现在，您可以将 Macie 配置为在选择检索和显示 Macie 在调查结果中报告的敏感数据样本时担任 AWS Identity and Access Management (IAM)	2023 年 11 月 16 日

	角色。这些样本有助于您验证 Macie 所发现的敏感数据的性质，并定制对受影响的 Amazon S3 对象和存储桶的调查。	
新功能	Macie 现在提供托管数据标识符，旨在检测另外 47 个国家和地区的国际银行账户（IBAN）。现在，您可以使用 Macie 来检测和报告 50 多个国家和地区的 IBAN 出现情况。	2023 年 11 月 1 日
新功能	Macie 现在提供托管数据标识符，旨在检测以下类型的敏感数据：Google Cloud API 密钥、Stripe API 密钥和 Aadhaar 号码、永久账户 (PAN) 以及印度的驾驶执照识别号。	2023 年 9 月 25 日
新配额	为了帮助您验证调查发现报告的敏感数据的性质，我们增加了从 Amazon S3 对象中检索和显示敏感数据示例的大小配额。现在，您可以从存储大小超过 10 MB 的 S3 对象中检索和显示示例。有关新配额的列表，请参阅 Amazon Macie 配额。	2023 年 9 月 7 日
区域可用性	Macie 现已在以色列（特拉维夫）区域推出。有关 Macie 当前可用位置的完整 AWS 区域列表，请参阅 AWS 一般参考中的 Amazon Macie 端点和配额。	2023 年 8 月 28 日

更新了功能	我们实施了一组新的动态默认托管数据标识符，用于自动化敏感数据发现。默认集包括我们推荐用于自动化敏感数据发现的托管数据标识符。它旨在检测常见的敏感数据类别和类型，同时还能优化您的自动化敏感数据发现结果。	2023 年 8 月 2 日
更新了功能	为了帮助您定位 Macie 在敏感数据发现和敏感数据调查发现中报告的敏感数据的出现位置，我们将对象中 JSON 路径元素名称的字符限制从 20 更改为 240。`Record`此更改会影响 Apache Avro 对象容器、Apache Parquet 文件、JSON 文件和 JSON Lines 文件的新敏感数据调查发现和发现结果。	2023 年 7 月 24 日
更新了功能	如果您是中某个组织的委托 Macie 管理员 AWS Organizations，那么您现在可以管理组织中最多 10,000 个账户的 Macie。	2023 年 6 月 30 日
新特征	现在，您可以创建和配置敏感数据发现作业，以自动使用我们为作业推荐的托管数据标识符集。这组推荐的托管数据标识符旨在检测常见的敏感数据类别和类型，同时还可以优化您的工作结果。	2023 年 6 月 28 日

新策略	我们添加了一个新的AWS托管策略，即 AmazonMacieReadOnlyAccess 策略。此策略授予只读权限，允许 IAM 身份（主体）检索其账户的所有 Macie 资源、数据和设置。	2023 年 6 月 15 日
新特征	为了帮助您评测和监控 Amazon S3 数据的自动化敏感数据发现覆盖范围，Macie 控制台现在包含 资源覆盖范围页面。该页面提供了所有 S3 存储桶的覆盖率统计数据和数据的统一视图，包括每个存储桶最近发生的分析问题（如果有）的汇总。如果出现问题，该页面还会提供补救指导。	2023 年 5 月 15 日
新特征	Macie 与集成 AWS 用户通知服务，这是一个新功能 AWS 服务 ，可作为你在 Macie 上 AWS 接收通知的中心位置。AWS Management Console 借助 用户通知服务，您可以配置自定义规则和传递渠道，以生成和发送有关 Amazon EventBridge 事件的通知，这些通知由 Macie 发布以获取策略和敏感数据发现。	2023 年 5 月 5 日

更新的内容	更新了 Macie 提供的有关 S3 存储桶默认加密设置的统计数据和元数据的描述。还更新了 Policy:IAMUser/S3BucketEncryptionDisabled 策略调查发现的描述。Amazon S3 现在自动应用服务器端加密，并使用 Amazon S3 托管密钥 (SSE-S3) 作为添加到新存储桶和现有存储桶的对象的基本加密级别。如需了解 Amazon S3 中此更改的信息，请参阅 Amazon Simple Storage Service 用户指南中的设置 S3 存储桶的默认服务器端加密行为。	2023 年 2 月 27 日
新功能	Macie 现在可以为 S3 存储桶生成另一种类型的策略调查发现：`Policy:IAMUser/S3BucketSharedWithCloudFront` 。此类发现表明存储桶的策略已更改，允许与 Amazon CloudFront 原始访问身份 (OAI)、源站访问控制 (OAC) 或两者共享该存储桶。CloudFront 此外，在 Macie 提供的有关您的 Amazon S3 数据的统计数据和元数据中，与 CloudFront OAI 或 OAC 共享的存储桶现在被视为外部共享。	2023 年 2 月 24 日

新功能	Macie 现在支持 Amazon S3 Glacier Instant Retrieval 存储类，用于发现敏感数据。现在，当 Macie 执行自动敏感数据发现或您运行敏感数据发现作业时，使用此存储类别的 S3 对象现在可以进行分析。在 Macie 提供的有关您的 Amazon S3 数据的统计数据和元数据中，它们也被视为可分类对象。	2022 年 12 月 21 日
新特征	现在，您可以将 Macie 配置为对您的账户或组织执行自动化敏感数据发现。通过自动化敏感数据发现，Macie 可以持续评测您的 Amazon S3 数据，并使用采样技术识别、选择和分析 S3 存储桶中的代表性对象，检查对象中是否有敏感数据。您可以在 Macie 提供的有关您的 Amazon S3 数据的统计数据、调查发现和其他信息中评测分析结果。	2022 年 11 月 28 日
新特征	现在，您可以创建和使用允许列表来指定您希望 Macie 在检查 Amazon S3 对象中是否有敏感数据时忽略的文本和文本模式。通过使用允许列表，您可以针对您的特定场景或环境定义敏感数据例外情况，例如，您组织的公众代表姓名、特定电话号码或组织用于测试的示例数据。	2022 年 8 月 30 日

新特征	要验证 Macie 在 S3 对象中发现的敏感数据的性质，您现在可以配置并使用 Macie 来检索调查发现报告的敏感数据示例。	2022 年 7 月 26 日
更新了功能	在 AmazonMacieFullAccess 策略中，我们更新了 Macie 服务相关角色 (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`) 的 Amazon 资源名称（ARN）。	2022 年 6 月 30 日
更新了功能	我们更新了 AmazonMacieServiceRolePolicy 策略，这是附加到 Macie 服务相关角色 (`AWSServiceRoleForAmazonMacie`) 的策略。该策略不再为 Amazon Macie Classic 指定操作和资源。Amazon Macie Classic 已停用，不再可用。	2022 年 5 月 11 日
新功能	Macie 现在在其发布到 AWS Security Hub的敏感数据发现中包含了该`OriginType`字段。`OriginType`字段指定 Macie 如何找到产生调查发现的敏感数据。	2022 年 5 月 11 日
更新的内容	阐明了关键字和最大匹配距离设置如何适用于自定义数据标识符。	2022 年 4 月 22 日

新功能	Macie 现在提供托管数据标识符，旨在检测 HTTP 基本授权标头、HTTP Cookie 和 JSON 网络令牌。	2022 年 4 月 21 日
新增内容	添加了 Macie 关键概念和术语的描述和定义。	2022 年 3 月 16 日
新功能	为了计算和显示创建和配置敏感数据发现任务时的估计成本，Macie 现在会从中检索定价数据。 AWS 账户 AWS Billing and Cost Management为了支持此功能，我们在AmazonMacieFullAccess策略中添加了 Billing and Cost Management (账单和成本管理) 操作。	2022 年 3 月 7 日
新功能	Macie现在将该Sample领域纳入其发布给 AWS Security Hub 的调查结果中。Sample 字段指定调查发现是否为 示例调查发现。	2022 年 2 月 24 日
新增内容	添加了有关使用 Amazon Virtual Private Cloud 在 VPC 和 Macie 之间建立私有连接的信息。	2022 年 1 月 19 日

新功能	现在，您可以使用 Amazon Macie 控制台为自定义数据标识符、调查发现的筛选和抑制规则、敏感数据发现作业以及组织中的成员账户（如果您是组织的 Macie 管理员）分配和管理标签。标签是您可以选择为某些类型的 AWS 资源定义和分配的标签。	2022 年 1 月 12 日
新增内容	添加了有关使用 AWS Identity and Access Management 管理 Macie 访问权限的信息。	2021 年 12 月 20 日
新特征	在创建自定义数据标识符时，您现在可以为其生成的敏感数据调查发现定义严重性设置。使用这些设置，您可以根据与自定义数据标识符的检测条件匹配的文本出现次数来指定要为调查发现分配哪个严重性。	2021 年 11 月 4 日
新功能	要了解 Macie 提供的不同类型的调查发现，您可以生成示例调查发现。样本调查发现使用示例数据和占位符值来演示 Macie 可能包含在每类调查发现中的信息类型。	2021 年 10 月 28 日
新功能	Macie现在将该OwnerAccountId 领域纳入其发布给 AWS Security Hub的调查结果中。此字段为拥有受影响的 AWS 账户 S3 存储桶的指定账户 ID。	2021 年 10 月 27 日

新增内容	添加了有关集中管理多个 Macie 账户的信息。你可以通过两种方式做到这一点：将 Macie 与 Macie 集成， AWS Organizations 或者从 Macie 发送会员邀请。	2021 年 10 月 13 日
新功能	现在，您的 S3 存储桶清单会显示存储桶的权限设置是否阻止 Macie 检索有关存储桶或存储桶对象的信息，以及评测和监控存储桶数据的安全性和隐私性。此外，我们还更新了参考文献 AWS KMS keys 和客户管理的密钥，以反映当前的术语。	2021 年 10 月 5 日
新功能	现在，Macie 会将策略和敏感数据调查发现存储 90 天，而不是 30 天。如果 Macie 在 2021 年 8 月 31 日当天或之后创建或更新了调查发现，则您可以使用 Macie 控制台或 Macie API 在最长 90 天内访问该调查发现。当然 AWS 区域，早在2021年9月27日，Macie就开始将调查结果保留90天。	2021 年 10 月 1 日
新特征	在创建敏感数据发现作业时，您现在可以指定希望该作业在分析 S3 对象时使用哪些托管数据标识符。使用此功能，您可以定制作业分析，将重点放在某些类型的敏感数据上。	2021 年 9 月 17 日

新功能	现在，敏感数据调查发现提供其他信息，可帮助您在 JSON 和 JSON Lines 文件中查找敏感数据。	2021 年 7 月 6 日
更新了功能	Macie 现在在其发布到 AWS Security Hub的结果中使用该AwsS3Bucket 资源类型。（Macie 之前将此值设置为AWS::S3::Bucket 。）AwsS3Bucket 是 AWS 安全调查结果格式 (ASFF) 中用于 S3 存储桶的资源类型值。	2021 年 6 月 28 日
新特征	在创建敏感数据发现作业时，您现在可以定义运行时系统标准来确定作业分析哪些 S3 存储桶。通过此功能，作业的分析范围可以根据存储桶清单的变化动态调整。	2021 年 5 月 15 日
新功能	您的 S3 存储桶清单和摘要控制面板现在提供加密元数据和统计数据，显示存储桶策略是否要求对新对象进行服务器端加密。此外，您现在可以按需刷新存储桶清单中各个存储桶的对象元数据。	2021 年 4 月 30 日
新特征	现在，您可以使用 Amaz CloudWatch on Logs 来监控和分析在运行敏感数据发现任务时发生的事件。为了支持此功能，我们在 Macie 服务相关角色的 AWS 托管策略中添加了 CloudWatch 日志操作。	2021 年 4 月 14 日

区域可用性	Macie 现已在 AWS 亚太地区（大阪）地区上市。	2021 年 4 月 5 日
新特征	现在，您可以将 Macie 配置为将敏感数据调查发现发布到 AWS Security Hub。	2021 年 3 月 22 日
新增内容	添加了有关监控和预测 Macie 成本以及参与免费试用的信息。	2021 年 2 月 26 日
更新的内容	我们将主账户一词替换为管理员账户。管理员账户用于集中管理多个账户。	2021 年 2 月 12 日
新功能	现在，您可以通过在自定义包含和排除条件中使用 S3 对象前缀来缩小敏感数据发现作业的范围。	2021 年 2 月 2 日
更新的内容	现在，Macie 在向发布政策调查结果时遵循 AWS 安全调查结果格式 (ASFF) 的发现类型分类法。 AWS Security Hub	2021 年 1 月 28 日
新增内容	添加了有关监控 Amazon S3 数据以及评测该数据的安全性和隐私性的信息。	2021 年 1 月 8 日
区域可用性	Macie 现已在 AWS 非洲（开普敦）地区、 AWS 欧洲（米兰）地区和 AWS 中东（巴林）地区推出。	2020 年 12 月 21 日

新功能	如果您的账户是 Macie 管理员账户，那么您现在可以创建和运行敏感数据发现作业，以分析组织中多达 1,000 个账户的 1,000 个存储桶的数据。	2020 年 11 月 25 日
新功能	现在，您的 S3 存储桶清单会显示您是否配置了任何一次性或定期的敏感数据发现作业来分析存储桶中的数据。如果有，它还会提供有关最近运行的作业的详细信息。	2020 年 11 月 23 日
新增内容	添加了有关筛选调查发现的信息。	2020 年 11 月 12 日
新功能	现在，敏感数据调查发现提供了其他信息，可帮助您在 Apache Avro 对象容器、Apache Parquet 文件和 Microsoft Excel 工作簿中查找敏感数据。	2020 年 11 月 9 日
新特征	现在，您可以使用敏感数据调查发现来查找 S3 对象中出现的单个敏感数据。	2020 年 10 月 22 日
新特征	现在，您可以暂停和恢复敏感数据发现作业。	2020 年 10 月 16 日
新增内容	添加了有关策略调查发现和敏感数据调查发现的严重性评分系统详细信息。	2020 年 10 月 6 日

新功能	现在，您可以查看统计信息，这些统计数据表明 Macie 在运行敏感数据发现作业时可以在单个 S3 存储桶中分析多少数据。此外，您现在可以在创建作业时查看作业的估计成本。	2020 年 9 月 3 日
新增内容	添加了有关配置、运行和管理敏感数据发现作业的信息。	2020 年 8 月 31 日
新功能	托管数据标识符现在可以检测巴西某些类型的个人身份信息。	2020 年 7 月 31 日
更新的内容	添加了有关自定义数据标识符中正则表达式支持的语法的信息。	2020 年 7 月 30 日
更新的内容	增加了对托管数据标识符的关键字要求，并增加了每个敏感数据发现作业可以产生的调查发现数量的配额。	2020 年 7 月 17 日
新增内容	添加了有关使用 Amazon EventBridge 以及 AWS Security Hub 监控和处理调查结果的信息。这包括调查结果 EventBridge 的事件架构以及策略和敏感数据发现的事件示例。	2020 年 6 月 22 日
新增内容	添加了有关分析和隐藏调查发现的信息。	2020 年 6 月 17 日
新增内容	添加了有关配置 Macie 以在 S3 存储桶中存储详细发现结果的说明。	2020 年 6 月 2 日

新增内容	添加了有关 Macie 可以检测的敏感数据类型以及检测 Amazon S3 对象中的敏感数据的加密要求信息。	2020 年 5 月 28 日
通用版	这是 Amazon Macie 用户指南的第一个公开发行版。	2020 年 5 月 13 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。