aws

用户指南

Amazon Audit Manager

Amazon Audit Manager: 用户指南

Table of Contents

什么是 AWS Audit Manager？

欢迎阅读 AWS Audit Manager 用户指南。

AWS Audit Manager 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。Audit Manager 可自动收集证据，因此您可以更轻松评测您的策略、程序和活动（也称为控件）是否有效运作。当需要进行审计时，Audit Manager 可帮助您管理利益相关者对控件的审核。这意味着您可以用更少的人工生成审计就绪报告。

Audit Manager 提供了预先构建的框架，用于根据特定合规标准或法规，构造和自动执行评测。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据指定的合规标准或法规要求进行分组。您还可以根据自己的具体要求，自定义框架和控件，以支持内部审计。

您可对任何框架创建评测。当您创建评测时，Audit Manager 会自动运行资源评测。这些评测会收集您定义的、审计范围内的AWS 账户和服务数据。收集的数据会自动转换至便于审计的证据。然后，将其附加至相关控件中，以帮助您证明在安全、变更管理、业务连续性和软件许可方面的合规性。此证据收集过程为持续进程，从您创建评测时开始。在您完成审计并且不再需要 Audit Manager 收集证据后，您可以停止收集证据。为此，请将您的评测状态更改为非活动。

Audit Manager 的特点

您可通过 AWS Audit Manager执行以下任务：

- 快速入门 — 从支持一系列合规标准和法规的预先构建框架中选择，创建您的第一项评测。然后，启动自动证据收集，以审计您的AWS 服务使用情况。
- 上传和管理来自混合或多云环境的证据 — 除了 Audit Manager 从您的 AWS 环境中收集的证据外，您还可以上传和集中管理来自本地或多云环境的证据。
- 支持常见的合规标准和法规 — 选择其中一项 AWS Audit Manager 标准框架。这些框架根据常见的合规性标准和法规，提供了预先构建的控件映射。其中包括 CIS Foundation Benchmark、PCI DSS、GDPR、 HIPAA、SOC2、GxP 以及 AWS 运营最佳实践标准。
- 监控您的有效评测-使用 Audit Manager 控制面板查看进行中的评测的分析数据，并快速识别需要补救的不合规证据。
- 搜索证据 — 使用证据查找器功能快速查找与您的搜索查询相关的证据。您可以根据搜索结果生成评测报告，也可以导出 CSV 格式的搜索结果。
- 创建自定义控件-从头开始创建自己的控件或自定义现有控件以满足需求。您还可以通过自定义控件特征来创建风险评测问题，并将这些问题的答案存储为手动证据。

- 自定义框架 — 根据内部审计的具体要求，使用标准或自定义控件创建自己的框架。
- 共享自定义框架 — 您可以与其他 AWS 账户 共享您的自定义 Audit Manager 框架，也可将其复制到您自有账户下的其他 AWS 区域。
- 支持跨团队协作— 将控件委托给主题专家，他们可以审核相关证据、添加评论并更新每个控制的状态。
- 创建审计师报告-生成评测报告，汇总为审计收集的相关证据，并链接至包含详细证据的文件夹。
- 确保证据的完整性 — 将证据存储 至安全位置，使其保持不变。

> **Note**
>
> AWS Audit Manager 协助收集与核实特定合规性标准和法规遵守情况相关的证据。但是，它本身并不能评测您的合规情况。因此，通过 AWS Audit Manager 收集的证据可能不包括审计所需的、有关您的 AWS 使用情况的所有信息。AWS Audit Manager 不能代替法律顾问或合规专家。

Audit Manager 定价

有关定价的更多信息，请参阅 AWS Audit Manager 定价。

您是 Audit Manager 的新用户吗？

如果您是首次接触 Audit Manager 的用户，我们建议您从以下页面开始：

1. AWS Audit Manager概念和术语 — 了解 Audit Manager 中使用的关键概念和术语，例如评测、框架和控制。
2. 如何 AWS Audit Manager 收集证据 — 了解 Audit Manager 如何为收集资源评测证据。
3. 设置 — 了解 Audit Manager 的设置要求。
4. 入门 — 按照教程创建您的第一项 Audit Manager 评测。
5. AWS Audit Manager API 参考 — 熟悉 Audit Manager API 操作和数据类型。

更多 Audit Manager 资源

浏览以下资源可了解有关 Audit Manager 的更多信息。

- 使用 AWS Audit Manager 收集证据并管理审计数据
- 通过AWS 研讨会手动配置自定义 Audit Manager 评测
- 整合三行模型（第 2 部分）：将AWS Config合规包转换为AWS管理和治理博客中的AWS Audit Manager评测

AWS Audit Manager 概念和术语

为了帮助您开始使用，此页面定义了 AWS Audit Manager 的术语并介绍了一些主要概念。

A

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

评测

您可以使用 Audit Manager 评测功能，自动收集与审计相关的证据。

此评测基于一个框架，该框架是一组与您的审计相关的控件。根据您的业务需求，您可以通过标准框架或自定义框架创建评测。标准框架包含支持特定合规标准或法规的预先构建控件。相比之下，自定义框架包含控件，您可以根据内部审计要求对这些控件进行自定义和分组。以框架为起点，您可以创建评测，指定要包含在审计范围内的 AWS 账户和服务。

创建评测时，Audit Manager 会根据框架中定义的控件自动开始评测您的 AWS 账户 和服务中的资源。接下来，它会收集相关证据，并将其转换为便于审计师使用的格式。完成此操作后，它会将证据附加至您的评测控件。当需要进行审计时，您（或您选择的委托人）可以查看收集的证据，然后将其添加至评测报告。此评测报告可帮助您证明您的控件是否按预期运行。

证据收集是一个持续的过程，从您创建评测时开始。您可以通过将评测状态更改为非活动，以停止证据收集。或者，您可在控制层停止证据收集。为此，您可以将评测中特定控件的状态更改为非活动。

有关如何创建和管理评测的说明，请参阅 AWS Audit Manager中的评测。

评测报告

评测报告是通过 Audit Manager 评测生成的最终文档。这些报告汇总了为审计所收集的相关证据。它们链接至相关的证据文件夹。这些文件夹是根据评测中指定的控件命名和组织的。对于每项评测，您可以查看 Audit Manager 收集的证据，并决定要在评测报告中包含的证据。

要了解有关评测报告的更多信息，请参阅评测报告。若要了解如何生成评测报告，请参阅生成评测报告。

评测报告目标

评测报告目标是 Audit Manager 保存评测报告的默认 S3 桶。要了解更多信息，请参阅 评测报告目标（可选）。

审核

审计是指对贵组织的资产、运营或业务诚信的独立审核。信息技术 (IT) 审计专门检查贵组织信息系统内部的控件。IT 审计旨在确定信息系统是否能保护资产、有效运行和维护数据完整性。所有这些对于满足合规标准或法律规定的监管要求很重要。

审计负责人

根据上下文，审计负责人一词有两种不同的含义。

在 Audit Manager 环境中，审计负责人是管理评测及其相关资源的用户或角色。Audit Manager 角色的职责包括创建评测、审核证据和生成评测报告。Audit Manager 是一项协作服务，当其他利益相关者参与评测，审计负责人将从中受益。例如，您可以将其他审计负责人添加至评测中以共享管理任务。或者，如果您是审计负责人，并且需要帮助解读为控件收集的证据，则可以将控件委托至在此领域有专长的利益相关者。这样的人被称为委托人角色。

从业务角度来看，审计负责人负责协调和监督其公司的审计准备工作，并向审计师提供证据。通常是指治理、风险和合规 (GRC) 专业人员，例如合规官或 GDPR 数据保护专员。GRC 专业人员拥有管理审计准备工作的专长和权力。更具体地说，他们了解合规性要求，可以分析、解释和编制报告数据。但是，其他业务角色也可以客串 Audit Manager 的审计负责人角色，不仅是负责此角色的 GRC 专业人员。例如，您可以选择由来自以下团队的技术专家设置和管理 Audit Manager 评测：

- SecOps
- IT/DevOps
- 安全运营中心/事件响应
- 拥有、开发、修复和部署云资产、并了解贵组织云基础架构的类似团队

您在 Audit Manager 评测中选择的指定审计负责人，在很大程度上取决于您的组织。这还取决于您的安全运营架构及审计的具体细节。在 Audit Manager 中，同一个人可以在一项评测中客串审计负责人角色，在另一项评测中客串委托人角色。

无论您选择如何使用 Audit Manager，您都可以使用审计负责人/委托人角色、并向每个用户授予特定的 IAM 策略，以管理整个组织的职责分工。通过这种两步方法，Audit Manager 可确保您完全控制个人评测的所有细节。有关更多信息，请参阅AWS Audit Manager中的用户角色推荐策略。

C

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

更改日志

对于评测中的每个控件，Audit Manager 都会捕获变更日志，以追踪该控件的用户活动。然后，您可以审核与特定控件相关活动的审计跟踪记录。有关变更日志中捕获的用户活动的更多信息，请参阅更改日志选项卡。

云合规性

云合规性是一般性原则，即云交付的系统必须符合云客户所面临的标准。

合规法规

合规法规是由机构规定的法律、规则或者其他命令，通常用于规范行为。示例为 GDPR。

合规性标准

合规性标准是一套结构化的指导方针，详细说明了该组织遵守既定法规、规范或立法的流程。示例包括 PCI DSS 和 HIPAA。

控件

控件是为信息系统或组织规定的保障措施或对策。控件旨在保护您的信息的机密性、完整性和可用性，并满足一系列已定义的安全要求。它们可以确保您的资源按预期运行，您的数据可靠，并且您的组织遵守适当的法律和法规。

在 Audit Manager 中，控件也可以提出供应商风险评测问卷。在这种情况下，控件一个特定的问题，它询问有关组织安全与合规状况的信息。

当您的 Audit Manager 评测中处于活动状态时，控件会持续收集证据。您还可以手动将证据添加到任何控件中。每份证据都变成了一份记录，帮助您证明遵守了控件要求。

Audit Manager 中有两种类型的控件：

- 标准控件 — 此控件是与 Audit Manager 中的特定框架关联的预先构建控件。使用标准控件协助您为各种合规性标准和法规做好审计准备。
- 自定义控件 — 这些控件是您作为 Audit Manager 用户定义的自定义控件。使用自定义控件来帮助您满足特定的内部审计或供应商风险评测合规要求。

有关更多信息，请参阅 AWS Audit Manager 控件示例。有关如何创建和管理控件的说明，请参阅控件库。

控件域

你可以将控件域视为一类一般的控件，它不是任何一个框架所特有的。控件域分组是 Audit Manager 控制面板最强大的功能之一。Audit Manager 会突出显示评测中存在不合规证据的控件，并按控件域对它们进行分组。这使您能够在准备审计时将补救工作重点放在特定主题域。

> **Note**
>
> 控件域不同于控件集。控件集是特定于框架的控件组合，通常由监管机构定义。例如，PCI DSS 框架有一个名为要求 8：识别和验证系统组件的访问权限的控件集。此控件集属于身份和访问管理控件域。

Audit Manager 将控件归入以下控件域。

控件域名	描述这些控件所控制的内容
业务连续性与应急计划	如何建立流程，以保护关键业务运营免受重大系统和网络中断影响。
变更管理	如何测试、批准、实施和记录云基础架构更改。
数据安全和隐私	您如何保护数据的隐私、可用性和完整性。
开发和配置管理	如何将云基础架构保持为必要且一致的状态。
治理和监督	如何使云计算的使用符合法律、监管和道德义务。
身份和访问管理	如何确保合适的用户获得适当的技术资源访问权限。
事件管理	如何制定责任和程序，确保对安全事件做出快速有效响应。
日志记录和监控	如何审核用户活动，以了解否有迹象表明有人企图或已进行未经授权的活动。
网络管理	如何使用网络管理系统管理和操作数据网络。
人员管理	如何在组织层面评测和管理人员安全风险。
人身安全	如何检测和避免设施中的人身安全问题。

控件域名	描述这些控件所控制的内容
风险管理	如何评测潜在风险和损失，以及如何减少或消除此类威胁。
供应链管理	如何识别、评测和减少与 IT 产品、供应商和供应链相关的风险。
用户设备管理	如何降低员工的 IT 硬件丢失、损坏或受损风险。
漏洞管理	如何定义、评测和修复云基础设施资产的所有已知漏洞。

D

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

数据来源

Audit Manager 使用数据来源为控件收集证据。以下术语描述了数据来源的概念和工作原理。

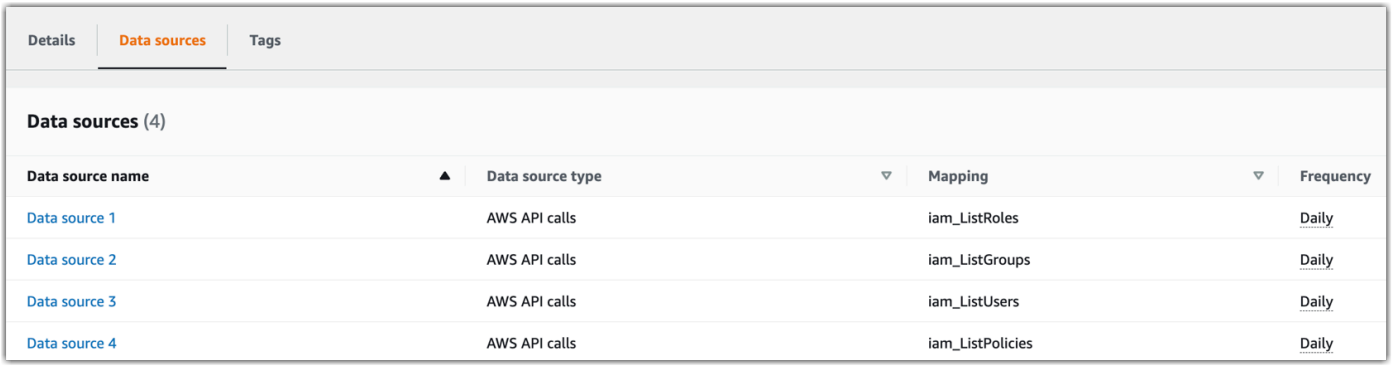
- 数据来源类型定义了 Audit Manager 从控件中收集证据的位置。如果您上传自己的证据，则数据来源类型为 手动。如果 Audit Manager 代表您收集证据，则数据来源类型为以下类型之一：AWS Security Hub、AWS Config、AWS CloudTrail 或 AWS API 调用。Audit Manager API 将数据来源类型称为 sourceType （单数）或 controlSources（复数）。
- 映射是与数据来源类型相关的特定关键字。例如，这可能是 CloudTrail 事件名称或AWS Config名称。Audit Manager API 将此称为 sourceKeyword（单数）或 controlMappingSources（复数）。
- 数据来源名称是为数据来源指定的名称。换句话说，数据来源名称标记了数据来源类型和映射的组合。对于标准控件，Audit Manager 提供了默认的数据来源名称（例如数据来源 1 和数据来源 2）。对于自定义控件，您可以提供自己的数据来源名称。这可能有助于您区分属于相同数据来源类型的多个映射。Audit Manager API 将数据来源命名为sourceName。

单个控件可包含多种数据来源类型和多个映射。例如，控件可能会从混合数据来源类型 (例如AWS Config和 Security Hub) 中收集证据。另一个控件可能通过多个AWS Config规则映射，将AWS Config作为其唯一的数据来源类型。

下表列出了自动数据来源类型，并显示了一些相应映射的示例。

数据来源类型	描述	映射示例
AWS Security Hub	使用此数据来源类型捕获资源安全状况的快照。Audit Manager 使用 Security Hub 控件的名称作为映射关键字，并直接通过 Security Hub 报告该安全检查结果。	`1.1 – Avoid the use of the "root" account`
AWS Config	使用此数据来源类型捕获资源安全状况的快照。Audit Manager 使用 AWS Config 规则的名称作为映射关键字，并直接通过 AWS Config 报告该安全检查结果。	`EC2_INSTANCE_MANAGED_BY_SSM`
AWS CloudTrail	使用此数据来源类型，跟踪审计中所需的特定用户活动。Audit Manager 使用 CloudTrail 事件的名称作为映射关键字，并从您的 CloudTrail 日志中收集相关用户活动。	`CreateAccessKey`
AWS API 调用	使用此数据来源类型，通过对特定AWS 服务的 API 调用来拍摄资源配置的快照。Audit Manager 使用 API 调用名称作为映射关键字，并收集 API 响应。	`ec2_DescribeSecurityGroups`

下图显示了 Audit Manager 控制台中的不同数据来源示例。



> **Note**
>
> 尽管有些数据来源类型是 AWS 服务，但数据来源类型不同于范围内的服务。有关更多信息，请参阅本指南故障排除部分的范围内服务和数据来源类型之间有何区别？。

委托人

委托人是权限有限的 AWS Audit Manager 用户。委托人通常具有专业的业务或技术专长。例如，这些专长可能涉及数据留存政策、培训计划、网络基础设施或身份管理。作为委托人，您可以帮助审计负责人审核收集到的证据，以了解属于您专长的控件。委托人可以审核控件集及其相关证据、添加评论、上传其他证据，以及更新各个控件的状态（您分配给它们以供审核）。

审计负责人将特定的控件分配给委托人，而非整个评测。因此，委托人的评测访问权限有限。有关如何委托控件集的说明，请参阅AWS Audit Manager 中的委托。

E

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

证据

证据是一种记录，其中包含遵守控件要求所需的信息。证据示例包括用户调用变更活动和系统配置快照。

Audit Manager 主要包含两类证据：自动证据和手动证据。

- 自动证据 — Audit Manager 自动收集的证据。包含以下三类自动证据：
  - 合规性检查 — 合规性检查的结果是从AWS Security Hub、AWS Config或两者中捕获的。合规性检查的示例包括来自 Security Hub 的 PCI DSS 控件的安全检查结果，以及 HIPAA 控件的

AWS Config规则评测。有关更多信息，请参阅AWS ConfigAWS Audit Manager支持的规则 和 AWS Security HubAWS Audit Manager支持的控件。

- 用户活动 — 对于更改资源配置的用户活动，其将在该活动发生时从 CloudTrail 日志中捕获。用户活动的示例包括路由表更新、Amazon RDS 实例备份设置更改以及 S3 桶加密策略更改。有关更多信息，请参阅AWS Audit Manager支持的AWS CloudTrail 控件。
- 配置数据 — 每天、每周或每月直接从AWS 服务中捕获资源配置的快照。配置快照的示例包括 VPC 路由表的路由列表、Amazon RDS 实例备份设置以及 S3 桶加密策略。有关更多信息，请参阅 AWS Audit Manager 支持的 API 调用。

- 手动证据 — 这是您自己添加至 Audit Manager 的证据。您可通过三种方式添加自己的证据：
  - 从 Amazon S3 导入文件
  - 从浏览器上传文件
  - 输入风险评测问题的文字回答

  有关更多信息，请参阅在AWS Audit Manager中添加手动证据。

自动收集证据从您创建评测开始。这是一个持续的进程，Audit Manager 根据证据类型和基础数据来源，以不同的频率收集证据。有关证据收集的更多信息，请参阅AWS Audit Manager 如何收集证据。有关如何审核评测证据的说明，请参阅审核评测中的证据。

证据收集方法

控件可以通过两种方式收集证据。

- 自动控件自动从 AWS 数据来源收集证据。这种自动证据可以帮助您证明完全或部分遵守了控件要求。
- 手动控件要求您上传自己的证据，以证明遵守了控件要求。

> **Note**
>
> 您可以将手动证据附加至任何自动控件中。在许多情况下，需要将自动和手动证据相结合，以证明完全遵守控件。尽管 Audit Manager 可以提供有用且关联的自动证据，但有些自动证据可能只能证明部分合规。在这种情况下，您可以用自己的证据补充 Audit Manager 提供的自动证据。
>
> 例如：
>
> - AWS生成式人工智能最佳实践框架包含一个名为 `Error analysis` 的控件。此控件要求您识别何时在模型使用中检测到不准确之处。它还要求您进行彻底的错误分析，以了解根本原因并采取纠正措施。

- 为支持这种控制，Audit Manager 会自动收集证据，显示您的评测运行的AWS 账户地点是否启用了 CloudWatch 警报。您可以使用这些证据证明您的警报和检查配置正确，从而证明部分遵守了控件。
- 为了证明完全合规，您可以用手动证据补充自动证据。例如，您可以上传显示错误分析流程、上报和报告的阈值、以及根本原因分析结果的策略或程序。您可以使用此手动证据证明既定政策已经到位，并且在出现提示时已采取纠正措施。

有关更详细的示例，请参阅具有混合数据来源的控件。

导出目的地

导出目标为默认 S3 桶，Audit Manager 会保存您从证据查找器中导出的文件。要了解更多信息，请参阅 导出目标（可选）。

F

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

框架

Audit Manager 框架是一个用于组织和自动执行特定标准或风险治理原则的评测文件。这些框架有助于将您的 AWS 资源映射到控件中的需求。它们包括一系列预先构建或客户定义的控件。该集合包含每种对照的描述与测试程序。这些控件根据指定的合规性标准或法规要求进行组织和分组。示例包括 PCI DSS 和 GDPR。

Audit Manager 中有两种类型的框架：

- 标准框架 — 基于各种合规性标准和法规的AWS最佳实践的预先构建框架。您可以使用这些框架协助审计准备。
- 自定义框架 — Audit Manager 用户定义的自定义框架。您可以使用这些框架，根据您的具体合规或风险治理要求协助进行审计准备。

有关如何创建和管理框架的说明，请参阅框架库。

> **Note**
>
> AWS Audit Manager 协助收集与核实特定合规性标准和法规遵守情况相关的证据。但是，它本身并不能评测您的合规情况。因此，通过 AWS Audit Manager 收集的证据可能不包括

审计所需的、有关您的 AWS 使用情况的所有信息。AWS Audit Manager 不能代替法律顾问或合规专家。

框架共享

您可以使用 Audit Manager 的自定义框架共享特征，在各个 AWS 账户和区域之间快速共享您的自定义框架。若要共享自定义框架，请创建共享请求。然后，共享请求的接收者有 120 天的时间接受或拒绝此请求。当他们接受时，Audit Manager 会将共享自定义框架复制到其框架库中。除了复制自定义框架外，Audit Manager 还会复制该框架中包含的、所有自定义控件。这些自定义控件已添加至收件人的控件库。Audit Manager 不复制标准框架或控件。这是因为默认情况下，这些资源已可用于每账户和区域。

R

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

资源

资源是在审计过程中评测的有形资产或信息资产。AWS 资源示例包括 Amazon EC2 实例、Amazon RDS 实例、Amazon RDS 实例、Amazon S3 桶、Amazon VPC 子集。

资源评测

资源评测是评测单个资源的进程。该评测基于控件要求。当评测处于活动状态时，Audit Manager 会对评测范围内的每个资源进行资源评测。资源评测运行以下一系列任务：

1. 收集证据，包括资源配置、事件日志和调查结果
2. 转换证据并将其映射至控件
3. 存储和追踪证据谱系以实现完整性

资源合规性

资源合规性是指在收集合规性检查证据时评测的资源评测状态。

Audit Manager 会为使用 AWS Config 并以 Security Hub 为数据来源的控件收集合规检查证据。在收集证据期间，可能需要评测多种资源。因此，一份合规性检查证据可包含一个或多个资源。

您可以使用证据查找器中的资源合规性筛选条件来浏览资源级别的合规状态。搜索完成后，您可以预览与您的搜索查询匹配的资源。

在证据查找器中，资源合规性包含三个可能得值：

- 不合规 — 指存在合规性检查问题的资源。如果 Security Hub 报告了资源的失败结果，或者AWS Config报告了不合规结果，就会发生这种情况。
- 合规 — 这是指没有合规性检查问题的资源。如果 Security Hub 报告了资源的 通过 结果，或者 AWS Config报告了合规结果，就会发生这种情况。
- 尚无定论 — 这是指无法进行合规检查或不适用的资源。如果 AWS Config 或 Security Hub 是基础数据来源类型，但这些服务未启用，则会发生这种情况。如果基础数据来源类型不支持合规性检查（例如手动证据、AWS API 调用或 CloudTrail），也会发生这种情况。

S

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

范围内的服务

这是包含在评测范围内的AWS 服务。当您将某项服务指定为评测范围时，Audit Manager 会评测此服务的资源。Audit Manager 可以评测范围内服务的各种资源。一些资源示例包括下面这些：

- 一个 Amazon EC2 实例
- 一个 S3 存储桶
- 用户或角色
- DynamoDB 表
- 网络组件，如 Amazon 虚拟私有云（VPC）、安全组，或网络访问控制列表 (ACL)

当您使用 Audit Manager 控制台从标准框架创建或更新评测时，默认情况下会预先选择范围内的 AWS 服务 列表。此列表无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于标准框架要求。如果您选择的标准框架仅包含手动控制，则 AWS 服务 不在您的评测范围内，且无法在评测中添加任何服务。

如果您需要编辑标准框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

> **Note**
>
> 切记，范围内的服务不同于数据来源类型，后者也可以是AWS 服务或其他类型。有关更多信息，请参阅本指南故障排除部分的范围内服务和数据来源类型之间有何区别？。

AWS Audit Manager 如何收集证据

AWS Audit Manager中的每项主动评测都会自动从一系列数据来源收集证据。每项目评测都有一个明确的范围，用于指定 Audit Manager 从中收集数据的 AWS 服务和账户。这些定义的服务和范围内账户都包含多个资源，每个资源都是您拥有的系统资产清单。Audit Manager 中的证据收集涉及对每个范围内资源评测。这被称为资源评测。

以下步骤描述了 Audit Manager 收集每次资源评测方法的证据：

1. 评测来自数据来源的资源

为了开始收集证据，Audit Manager 会评测来自数据来源范围内的资源。它通过捕获配置快照、相关的合规性检查结果和任何用户活动实现此目的。然后，它会运行分析以确定该数据支持的控件类型。然后，资源评测结果将被保存并转化为证据。有关不同证据类型的更多信息，请参阅本指南 AWS Audit Manager概念和术语部分中的 证据。

2. 将评测结果转化为证据

资源评测的结果既包含从该资源中捕获的原始数据，也包含说明数据支持哪种控件的元数据。AWS Audit Manager将原始数据转换为便于审计师使用的格式。然后，转换后的数据和元数据将保存为 Audit Manager 证据，然后再附加至控件。

3. 将证据随附至关联控件

Audit Manager 读取证据元数据。然后，它将已保存的证据附加至评测中的相关对照中。随附证据将在 Audit Manager 中可见。资源评测周期完成。

> **Note**
>
> 根据控件配置，在某些情况下，可以将相同的证据附加制来自多个 Audit Manager 评测的多个控件中。当多个控件附带相同证据时，Audit Manager 会精确计量一次资源评测。原因是同样的证据仅收集一次。但是，Audit Manager 评测中的控件可以包含来自多个数据来源的多个证据。

证据收集频率

证据收集是一个持续的进程，从您创建评测时开始。AWS Audit Manager以不同的频率从多个数据来源收集证据。因此，对于证据收集频率，没有一个放之四海而皆准的答案。证据收集频率取决于证据类型及其数据来源，如下所述。

- 合规性检查 — Audit Manager 从AWS Security Hub和AWS Config收集此类证据。
  - 对于AWS Security Hub，证据收集频率遵循您的 Security Hub 检查的时间表。有关 Security Hub 检查时间表的更多信息，请参阅AWS Security Hub 用户指南中的运行安全检查计划。有关 Audit Manager 支持的 Security Hub 检查的更多信息，请参阅 AWS Security Hub 支持的控件 AWS Audit Manager。
  - 对于 AWS Config，证据收集频率遵循 AWS Config 规则中定义的触发因素。有关AWS Config规则触发器的更多信息，请参阅AWS Config 用户指南中的 触发器类型。有关 Audit Manager 支持的 AWS Config 规则 的更多信息，请参阅AWS Config 规则 由... 支持 AWS Audit Manager。
- 用户活动 — Audit Manager 会持续从AWS CloudTrail收集此类证据。这种频率是持续的，原因是用户活动可以在一天中的任何时间发生。有关更多信息，请参阅AWS CloudTrail 支持的事件名称 AWS Audit Manager。
- 配置数据 — Audit Manager 使用其他AWS 服务(如 Amazon EC2、Amazon S3 或 IAM) 的 API 调用，收集此证据类型。您可以要调用哪些 API 操作。您还可以在 Audit Manager 中将频率设置为每天、每周或者每月。在控件库中创建或编辑控件时，可以指定此频率。有关如何编辑或创建控件的说明，请参阅控件库。有关 Audit Manager 如何使用 API 调用创建证据的更多信息，请参阅 支持的 API 调用 AWS Audit Manager。

无论数据来源的证据收集频率如何，只要控件和评测处于活动状态，就会自动收集新的证据。

AWS Audit Manager 控件的示例

您可以查看本页上的示例，详细了解AWS Audit Manager中的控件工作原理。这些示例描述了控件的外观、Audit Manager 为该控件生成证据的方式，以及为证明合规性可以采取的后续步骤。

> **Tip**
>
> 我们建议您在 Audit Manager 中启用 AWS Config 和 AWS Security Hub，以获得最佳体验。启用这些服务后，它们可用作 Audit Manager 评测控件的数据来源类型。换句话说，Audit Manager 可以使用 Security Hub 调查发现和AWS Config 规则自动生成证据。
>
> - 启用 AWS Security Hub后，确保您还 支持所有安全标准 ，并 打开整合控件调查发现设置。此步骤可确保 Audit Manager 可以导入所有支持合规标准的调查发现。
> - 启用 AWS Config后，请确保您还启用了相关 AWS Config 规则 或部署合规包，以满足审计相关的标准要求。此步骤可确保 Audit Manager 可以导入所启用的所有支持 AWS Config 规则 的调查发现。

包含以下每种类型的控件示例：

主题

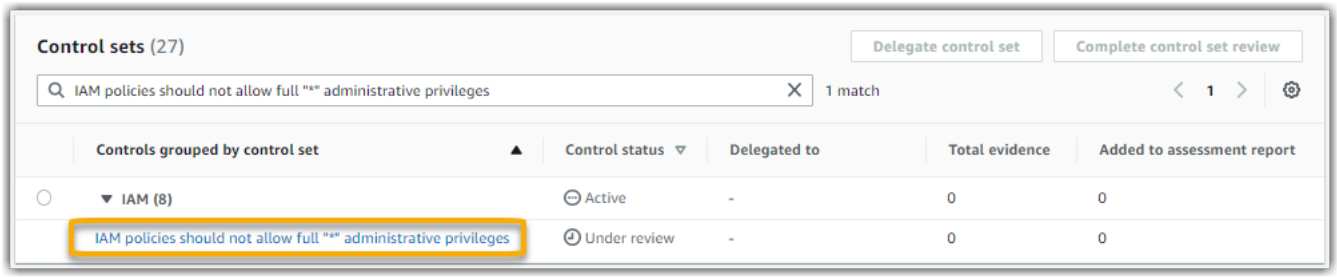
将 AWS Security Hub 用作数据来源类型的自动控件

此示例显示了将AWS Security Hub用作其数据来源类型的控件。此标准控件取自 AWS基础安全最佳实践标准 (FSBP) 框架。Audit Manager 使用此控件生成证据，以帮助使您的 AWS 环境符合 FSBP 要求。

控件细节示例

- 控件名称 — `IAM policies should not allow full "*" administrative privileges`
- 控件集 — 此控件属于 IAM 控件集。这是一组与身份和访问管理相关的控件。
- 数据来源类型 — AWS Security Hub
- 证据类型 — 合规性检查

在以下示例中，此控件位于基于 FSBP 框架创建的 Audit Manager 评测。



评测显示控件状态。它还显示了迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

Audit Manager 可以使用此控件检查您的 IAM 策略是否过于宽泛，进而无法满足 FSBP 的要求。更具体地说，它可以检查您的客户托管 IAM 策略是否具有管理员访问权限，其中包括以下通配符语句：`"Effect": "Allow" with "Action": "*" over "Resource": "*"`。

Audit Manager 如何为此控件收集证据

Audit Manager 采取以下措施来为此控件收集证据：

1. 对于每项控件，Audit Manager 都会评测您的范围内资源。它使用控件设置中指定的数据来源来执行此操作。在此示例中，您的 IAM 策略是资源，Security Hub 和 AWS Config 是数据来源类型。Audit Manager 会查找特定的 Security Hub 检查 ([IAM.1]) 结果，该检查反过来又使用 AWS Config 规则评测你的 IAM 策略 (iam-policy-no-statements-with-admin-access)。
2. 资源评测结果将被保存并转化为审计员友好证据。Audit Manager 会为使用 Security Hub 作为数据来源类型的控件生成合规检查证据。该证据包含直接从 Security Hub 中报告的合规检查结果。
3. Audit Manager 将已保存证据附加至您命名为`IAM policies should not allow full "*" administrative privileges`的评测。

如何使用 Audit Manager 证明该控件的合规性

将证据附至控件后，您（或您选择的委托人）可以审核证据，了解是否需要采取任何补救措施。

在此示例中，Audit Manager 可能会显示来自 Security Hub 的失败仲裁。如果您的 IAM 策略中包含通配符 (*) 并且过于宽泛，无法满足控制要求，则可能会发生这种情况。在这种情况下，您可以更新 IAM 策略，使其不允许拥有完全的管理权限。为此，您可以先确定用户需要执行的任务，然后拟定仅限用户执行这些任务的策略。此纠正措施有助于使您的 AWS 环境符合 FSBP 要求。

当您的 IAM 策略与控件一致时，请将控件标记为已审核，并将证据添加至您的评测报告中。然后，您可以与审计员共享此报告，以证明控件按预期运行。

将 AWS Config 用作数据来源类型的自动控件

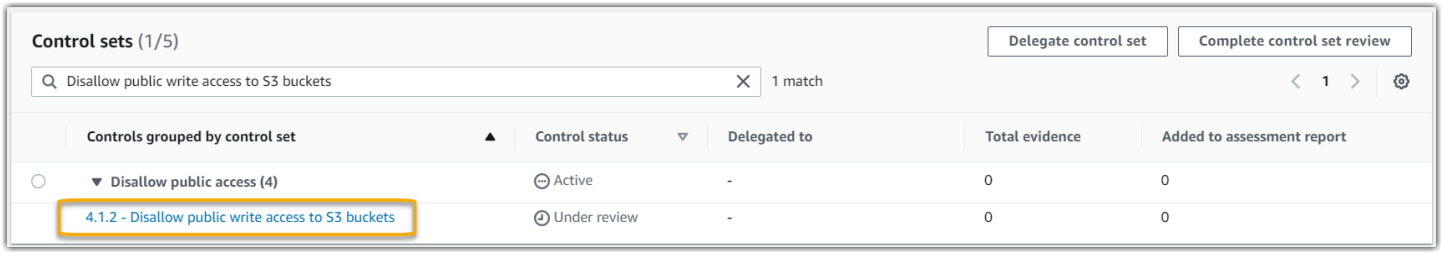
此示例显示了将AWS Config用作其数据来源类型的控件。这是取自 AWS Control Tower防护机制 框架的标准控件。Audit Manager 使用控件生成证据，以帮助使您的 AWS 环境与 AWS Control Tower 防护机制保持一致。

控件细节示例

- 控件名称 — `4.1.2 - Disallow public write access to S3 buckets`

- 控件集 — 此控件属于 `Disallow public access` 控件集。这是一组与访问管理相关的控件。
- 数据来源类型 — AWS Config
- 证据类型 — 合规性检查

在以下示例中，此控件位于通过 AWS Control Tower 防护机制框架创建的 Audit Manager 评测中。



该评测显示了控件状态、迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

Audit Manager 可以使用此控制来检查您的 S3 桶策略的访问级别是否过于宽松，是否满足AWS Control Tower要求。更具体地说，它可以检查阻止公共访问设置、桶策略和桶访问控制列表 (ACL)，以确认您的桶是否允许公共写入权限。

Audit Manager 如何为此控件收集证据

Audit Manager 采取以下措施来为此控件收集证据：

1. 对于每个控件，Audit Manager 都会使用控件设置中指定的数据来源评测您的范围内的资源。在这种情况下，您的 S3 桶是资源，AWS Config 是数据来源类型。Audit Manager 会查找特定AWS Config 规则 (s3-bucket-public-write-prohibited) 以评测评测范围内的 S3 桶的设置、策略和 ACL。
2. 资源评测结果将被保存并转化为审计员友好证据。Audit Manager 会为使用 AWS Config 作为数据来源类型的控件生成合规检查证据。该证据包含直接从 AWS Config 中报告的合规检查结果。
3. Audit Manager 将已保存证据附加至您命名为`4.1.2 - Disallow public write access to S3 buckets`的评测。

如何使用 Audit Manager 证明该控件的合规性

将证据附至控件后，您（或您选择的委托人）可以审核证据，了解是否需要采取任何补救措施。

在此示例中，Audit Manager 可能会显示一项 AWS Config 声明 S3 桶不合规 的仲裁。如果您的一个 S3 桶具有不限制公共策略的“阻止公共访问”设置，并且当前策略允许公共写入权限，则可能会发生这种情况。若要纠正此问题，您可以更新“阻止公共访问”设置，以限制公共策略。或者，您可使用不允许公共写入权限的其他桶策略。此纠正措施有助于使您的 AWS 环境符合 AWS Control Tower 要求。

如果您确信自己的 S3 桶访问权限级别与控件一致，则可以将控件标记为 已审核，并将证据添加至评测报告。然后，您可以与审计员共享此报告，以证明控件按预期运行。

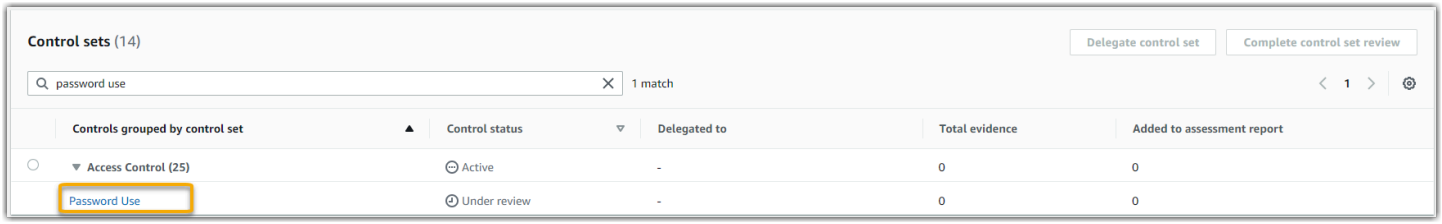
将 AWS API 调用用作数据来源类型的自动控件

此示例显示了将 AWS API 调用用作其数据来源类型的自定义控件。Audit Manager 使用此控件生成证据，以帮助使您的 AWS 环境符合特定要求。

控件细节示例

- 控件名称 — `Password Use`
- 控件集 — 此控件属于名为 `Access Control` 的控件集。这是一组与身份和访问管理相关的控件。
- 数据来源类型 — AWS API 调用
- 证据类型 — 配置数据

在以下示例中，此控件位于通过自定义框架创建的 Audit Manager 评测中。



评测显示控件状态。它还显示了迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

Audit Manager 可以使用此自定义控件来帮助您确保有足够的访问控制策略。此控件要求您在选择和使用密码时遵循良好安全规范。Audit Manager 可以通过检索评测范围内的 IAM 主体的所有密码策略列表，帮助您验证这一点。

Audit Manager 如何为此控件收集证据

Audit Manager 采取以下措施来为此自定义控件收集证据：

1. 对于每个控件，Audit Manager 都会使用控件设置中指定的数据来源评测您的范围内的资源。在这种情况下，您的 IAM 主体是资源，AWS API 调用是数据来源类型。Audit Manager 会查找特定 IAM API 调用 (getAccountPasswordPolicy) 结果。然后，它会为AWS 账户返回您的评测范围内的密码策略。
2. 资源评测结果将被保存并转化为审计员友好证据。Audit Manager 为使用 API 调用作为数据来源的控件生成 配置 数据证据。此证据包含从 API 响应中捕获的原始数据，以及表明具体的数据支持控件的其他元数据。
3. Audit Manager 将已保存证据附加至您命名为 `Password Use` 的评测中的自定义控件。

如何使用 Audit Manager 证明该控件的合规性

将证据附至控件后，您（或您选择的委托人）可以审核证据，了解是否充足或是否需要采取任何补救措施。

在此示例中，您可以查看证据，查看 API 调用响应。GetAccountPasswordPolicy 响应描述了您账户中用户密码的复杂性要求和强制轮换周期。您可以使用此 API 响应作为证据，证明您已经为评测范围内的 AWS 账户 制定了足够的密码访问控制策略。如果需要，您还可以通过向控件添加评论，来提供有关这些政策的其他注释。

如果您确信自己的 IAM 主体的密码策略与自定义控件一致，则可以将控件标记为已审核，并将证据添加至评测报告。然后，您可以与审计员共享此报告，以证明控件按预期运行。

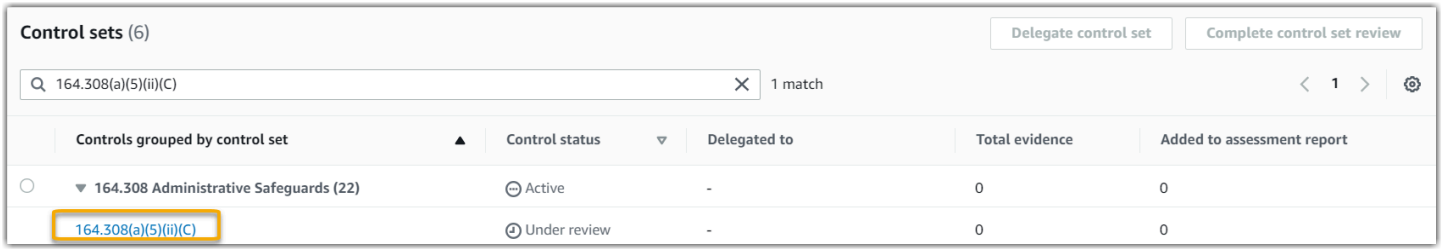
将 AWS CloudTrail 用作数据来源类型的自动控件

此示例显示了将AWS CloudTrail用作其数据来源类型的控件。这是取自 HIPAA 框架的标准控件。Audit Manager 使用此控件生成证据，以帮助使您的 AWS 环境符合 HIPAA 要求。

控件细节示例

- 控件名称 — `164.308(a)(5)(ii)(C)`
- 控件集 — 此控件属于名为 `164.308 Administrative Safeguards` 的控件集。
- 数据来源类型 — AWS CloudTrail
- 证据类型 — 用户活动

以下是基于 HIPAA 框架创建的 Audit Manager 评测中的控件：



评测显示控件状态。它还显示了迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

此控件需要通过监控程序检测不当登录。不当登录的例子：当有人多次输入用户名和密码组合，试图访问信息系统。Audit Manager 通过提供评测范围内所有检测资源的登录尝试列表，帮助您验证此控件。

Audit Manager 如何为此控件收集证据

Audit Manager 采取以下措施来为此控件收集证据：

1. 对于每个控件，Audit Manager 都会使用控件设置中指定的数据来源评测您的范围内的资源。在这种情况下，您的用户是资源，CloudTrail 是数据来源类型。Audit Manager 会查找 CloudTrail 记录的所有 AWS 管理控制台登录事件的结果。然后，它会返回评测范围内的相关事件的日志。
2. 资源评测结果将被保存并转化为审计员友好证据。Audit Manager 为使用 CloudTrail 作为数据来源类型的控件生成用户活动证据。此证据包含从您的用户中捕获的原始数据，以及表明具体的数据支持控件的其他元数据。
3. Audit Manager 将已保存证据附加至您命名为`164.308(a)(5)(ii)(C)`的评测。

如何使用 Audit Manager 证明该控件的合规性

将证据附至控件后，您（或您选择的委托人）可以审核证据，了解是否需要采取任何补救措施。

在此示例中，您可查看证据，查看 CloudTrail 记录的登录事件。此日志描述了您的用户控制台登录活动，其中包括以下信息：

- 每次成功登录
- 每次失败登录
- 验证何时强制执行多重身份验证 (MFA)
- 每个登录事件的 IP 地址

您可以使用此日志作为证据，证明您已经为评测范围内的 AWS 账户 制定了足够的监控程序。如果需要，您还可以通过向控件添加评论来提供其他注释。例如，如果日志显示任何差异（例如多次登录尝试失败），则可以添加一条评论，描述您是如何修复问题的。定期监控控制台登录，可以帮助您防止因差异和不当登录尝试而导致的安全问题。反过来，这种最佳方案有助于使您的 AWS 环境符合 HIPAA 的要求。

如果您确信自己的监控程序与控件一致，则可以将控件标记为已审核，并将证据添加至评测报告。然后，您可以与审计员共享此报告，以证明控件按预期运行。

手动控件

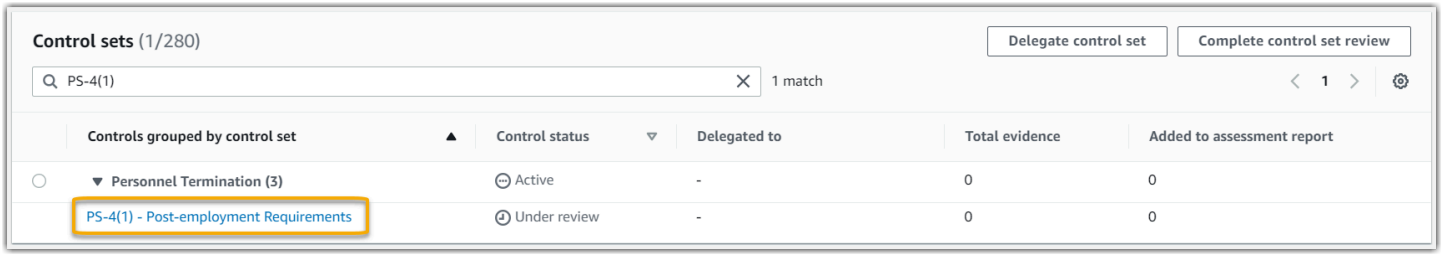
部分控件不支持自动证据收集。这包括依赖于提供实物记录和签名的控件，以及观察、访谈和其他非在云中生成的事件。在这些情况下，您可手动上传证据，以证明您满足了控件要求。

此示例显示了 Audit Manager 无法收集自动证据的手动控件。这是取自 NIST 800-53 (Rev. 5) 框架的标准控件。您可以使用 Audit Manager 上传和存储证明该控件合规的证据。

控件细节示例

- 控件名称 — `PS-4(1) - Post-employment Requirements`
- 控件集 — 此控件属于 `Personnel Termination` 控件集。这是一组与解雇程序背景下的信息安全相关的控件。
- 数据来源类型 — 手动
- 证据类型 — 手动

以下是根据 NIST 800-53 (Rev. 5) 低中高框架创建的、Audit Manager 评测中显示的控件：



评测显示控件状态。它还显示了迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

如果员工被解雇，您可以使用此控件确认您是否在保护组织信息。具体而言，您可以证明您始终如一地将适用的、具有法律约束力的离职后要求通知被解雇个人，以保护组织信息。此外，您可以证明所有被解雇的个人都签署了离职后要求确认书，这是组织解雇流程的一部分。

如何手动上传此控件的证据

您可以通过以下步骤上传支持此控件的手动证据：

1. 将您要上传的手动证据置于 Amazon Simple Storage Service (S3) 桶，并记下 S3 URI。
2. 在 Audit Manager 评测中，打开控件，进入证据文件夹选项卡，然后输入 S3 URI 上传证据。有关说明，请参阅AWS Audit Manager中的上传手动证据。
3. Audit Manager 会创建一个以您的证据上传日期命名的证据文件夹。然后它会将已上传的证据附加至命名为 `PS-4(1) - Post-employment Requirements` 的评测中的控件。

如何使用 Audit Manager 证明该控件的合规性

如果您有支持此控件的文档，则可将其作为手动证据上传。例如，您可上传人力资源部门向解雇的员工发出的、具有法律约束力的离职后要求的最新副本。如果在审计期间有任何个人被解雇，您也可以上传发给这些被解雇人员的、注明日期的副本。

就像自动控件一样，您可以将手动控件委托给利益相关者，他们可以帮助您审核证据（或者在本例中提供证据）。例如，当您查看此控件时，您可能会意识到自己只能部分满足其要求。如果您没有被解雇的个人亲自签署的确认信，则可能出现这种情况。您可以将控制权委托给人力资源利益相关者，然后该利益相关者可上传已签署信函的副本。或者，如果在审计期间没有员工被解雇，你可以留下评论，说明控件中没有附上签名信函的原因。

如果您确信自己与控件一致，则可以将其标记为已审核，并将证据添加至评测报告。然后，您可以与审计员共享此报告，以证明控件按预期运行。

具有混合数据来源类型（自动和手动）的控件

在许多情况下，需要将自动和手动证据相结合以满足控制措施。尽管 Audit Manager 可以提供与控件相关的自动证据，但您可能需要通过自己识别和上传的手动证据补充这些数据。

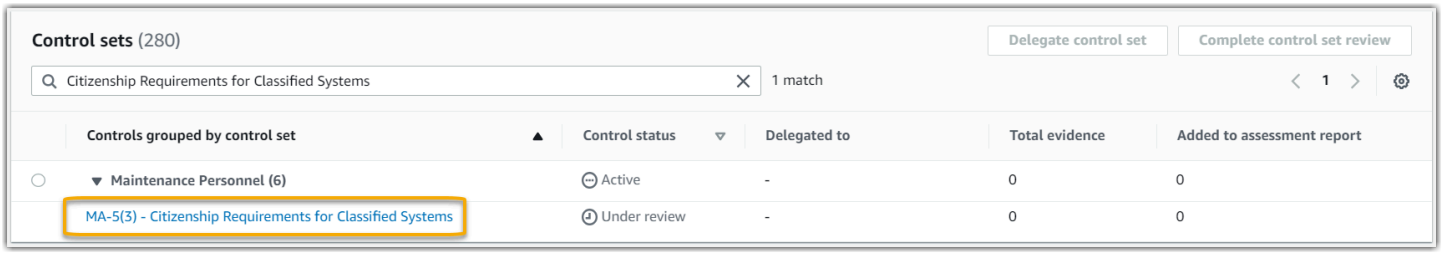
此示例显示的控件结合了手动证据和来自 AWS API 调用的自动证据。这是取自 NIST 800-53 (Rev. 5) 框架的标准控件。Audit Manager 使用此控件生成证据，以帮助使您的 AWS 环境符合 NIST 要求。

控件细节示例

- 控件名称 — `MA-5(3) - Citizenship Requirements for Classified Systems`

- 控件集 — 此控件属于 `Maintenance Personnel` 控件集。这组控件与在组织系统上执行硬件或软件维护的人员有关。
- 数据来源类型 — AWS API 调用，以及补充手册证据
- 证据类型 — 配置数据

以下是根据 NIST 800-53 (Rev. 5) 框架创建的 Audit Manager 评测中显示的控件：



评测显示控件状态。它还显示了迄今为止为这种控件收集的证据数量，以及您的评测报告中包含的证据数量。在这里，您可以委托控件审阅，也可以自己完成审阅。选择控件名称会打开详情页面，其中包含更多信息，包括该控件的证据。

此控件的作用

Audit Manager 可以使用此控件来帮助您确保执行维护和诊断活动的人员具有所需的公民身份。如果您的系统处理、存储或传输机密信息，则必须证明您的维护人员为美国公民。Audit Manager 可帮助您验证这一点。它通过返回评测范围内的所有 IAM 策略和主体完整列表来实现此目的。然后，您可以验证并证明此用户列表满足必要的公民身份要求。您可以通过手动上传其公民身份的补充证据，证明这一点。

Audit Manager 如何为此控件收集证据

Audit Manager 采取以下措施来为此控件收集证据：

1. 对于每个控件，Audit Manager 都会使用控件设置中指定的数据来源评测您的范围内的资源。在这种情况下，您的 IAM 策略和主体是资源，AWS API 调用是数据来源。Audit Manager 会查找四个特定的 IAM API 调用 (ListUsers/ListRoles/ListGroups/ListPolicies) 的结果，并返回您评测范围内的 IAM 策略和主体列表。
2. 资源评测结果将被保存并转化为审计员友好证据。Audit Manager 为使用 API 调用作为数据来源的控件生成配置数据证据。此证据包含从 API 响应中捕获的原始数据，以及表明具体的数据支持控件的其他元数据。
3. Audit Manager 将已保存证据附加至您命名为`MA-5(3) - Citizenship Requirements for Classified Systems`的评测。

如何手动上传此控件的证据

您可以通过以下步骤上传作为自动证据补充的手动证据：

1. 将公民身份证件置于 Amazon Simple Storage Service (Amazon S3) 桶，并记下 S3 URI。
2. 在 Audit Manager 评测中，打开控件，进入证据文件夹选项卡，然后上传证据。您可通过输入 S3 URI 完成此操作。有关说明，请参阅在 AWS Audit Manager 中添加手动证据。
3. Audit Manager 将已上传的证据附加至命名为 `MA-5(3) - Citizenship Requirements for Classified Systems` 的评测中的控件。

如何使用 Audit Manager 证明该控件的合规性

将证据附至控件后，您（或您选择的委托人）可以审核证据，了解是否充足或是否需要采取任何补救措施。

在此示例中，您可能会查看证据，并看到包含 20 个用户的列表。如果您不确定如何识别维护人员用户或其公民身份，则可以将控件委托给主题专家进行验证。委托人可以确认维护人员名单，并手动上传补充证据，以作为其公民身份文件。确认所有列出的相关用户的公民身份有助于使您的 AWS 环境符合 NIST 的要求。或者，如果您的系统不处理、存储或传输保密信息，则可以发表评论，说明此控件不适用的原因。

如果您确信自己与控件一致，则可以将控件标记为已审核，并将证据添加至评测报告。然后，您可以与审计员共享此报告，以证明控件按预期运行。

与相关 AWS 服务集成

AWS Audit Manager与多个AWS 服务集成，可自动收集可包含在评测报告中的证据。

AWS Security Hub

AWS Security Hub使用基于AWS最佳实践标准和行业标准的自动安全检查来监控您的环境。Audit Manager 通过直接从 Security Hub 报告安全检查结果，以捕获资源安全状况快照。有关 Security Hub 的更多信息，请参阅AWS Security Hub 用户指南中的什么是 AWS Security Hub？。

AWS CloudTrail

AWS CloudTrail 帮助您监控对您账户中 AWS 资源的调用。其中包括AWS管理控制台、AWS CLI 等 AWS 服务发出的调用。Audit Manager 可直接从 CloudTrail 收集日志数据，并将处理后的日志转换

为用户活动证据。有关 CloudTrail 的更多信息,请参阅 AWS CloudTrail 用户指南中的什么是 AWS CloudTrail？。

AWS Config

AWS Config 可以提供关于您的 AWS 账户中 AWS 资源的配置的详细信息。这些信息包括资源之间的关联方式以及资源以前的配置方式。Audit Manager 通过报告从AWS Config中直接发现的结果，捕获您的资源安全状况快照。有关 AWS Config 的更多信息，请参阅《AWS Config 用户指南》中的什么是 AWS Config？。

AWS License Manager

AWS License Manager 简化了将软件供应商许可证迁移到云的过程。在 AWS 上构建云基础设施时，您可以将现有的许可证清单重新用于云资源来节省成本。Audit Manager 提供了许可证管理器框架，可帮助您做好审计准备。此框架可与 License Manager 集成，可根据客户定义的许可规则汇总许可证使用信息。有关 License Manager 的更多信息，请参阅AWS License Manager 用户指南中的什么是 AWS License Manager？。

AWS Control Tower

AWS Control Tower 为云基础架构实施预防和侦查防护机制。Audit Manager 提供了 AWS Control Tower 防护机制框架，可帮助您做好审计准备。该框架包含所有基于AWS Control Tower防护机制的 AWS Config规则。有关 AWS Control Tower 的更多信息，请参阅《AWS Control Tower 用户指南》中的什么是 AWS Control Tower？。

AWS Artifact

AWS Artifact 是自助审核构件检索门户，可按需访问AWS基础设施的合规性文档和认证。AWS Artifact 提供证据，证明AWS云基础架构符合合规性要求。相比之下，AWS Audit Manager可以帮助您收集、审核和管理证据，以证明您的AWS 服务使用合规。有关 AWS Artifact 的更多信息，请参阅《AWS Artifact 用户指南》中的什么是 AWS Artifact？。您可以在AWS Management Console中下载AWS报告列表。

有关特定合规性计划范围内的 AWS 服务 的列表，请参阅合规性计划范围内的 AWS 服务。有关更多一般信息，请参阅 AWS 合规性计划。

与第三方 GRC 产品集成

AWS Audit Manager 支持与此页面上列出的第三方合作伙伴 GRC 产品集成。

如果您的公司使用混合云模型或多云模型，则很可能会使用 GRC 产品管理来自这些环境的证据。当该产品与 Audit Manager 集成后，您可以将有关 AWS 使用情况的证据直接提取至 GRC 环境中。这简化了合规性管理方式，在您准备审计时，为您提供了一个审核和补救证据的集中场所。

阅读本页面，概述可以从 Audit Manager 提取证据的第三方 GRC 产品。您还可以查看关于可直接在这些产品中执行的 Audit Manager API 操作的参考。

主题

了解第三方集成如何用于 Audit Manager

GRC 合作伙伴可以通过 Audit Manager 的公共 API 将其产品与 Audit Manager 集成。通过此集成，您可以将 GRC 环境中的企业控件映射至 Audit Manager 提供的控件。

完成此一次性控件映射实践后，您可以直接在 GRC 产品中创建 Audit Manager 评测。此操作将开始收集有关您的 AWS 使用情况的证据。然后，您可以在与企业控件相同的环境中，看到这些AWS证据以及从混合环境中收集的其他证据。

当您将 Audit Manager 与第三方 GRC 产品集成时，请记住以下几点：

- 集成适用于所有支持 Audit Manager 的AWS 区域。
- 您在 GRC 合作伙伴产品中创建的任何 Audit Manager 资源也将反映在 Audit Manager。
- 除了第三方 GRC 产品定价外，您还需要支付AWS Audit Manager 定价。
- Audit Manager 收集的证据是不可变。第三方 GRC 产品中的证据呈现方式与 Audit Manager 控制台的呈现方式完全相同。但是，如果您使用第三方集成，则可以通过在报告中提供其他背景信息，强化这些证据的可信度。
- 适用于 Audit Manager 的相同限额也适用于第三方 GRC 产品。例如，每个AWS 账户最多可包含 100 项有效 Audit Manager 评测。无论您是在 Audit Manager 控制台还是在第三方 GRC 产品中创建评测，此账户级别限额都适用。大多数 Audit Manager（但不是全部）都列在服务限额控制台中的 AWS Audit Manager 命名空间下。若要了解如何请求提高限额，请参阅 管理您的 Audit Manager 限额。

如果您有合规解决方案，并且有兴趣与 Audit Manager 集成，请发送电子邮件至 `auditmanager-partners@amazon.com`。

与 Audit Manager 集成的第三方 GRC 合作伙伴产品

以下第三方 GRC 产品可以从 Audit Manager 提取证据。

MetricStream

要使用此集成，请联系 MetricStream 以获取和购买 MetricStream GRC 软件。

MetricStream Enterprise GRC 解决方案基于 MetricStream 平台上，允许对企业范围内的 GRC 活动和流程采取全面的协作方法。通过将来自 Audit Manager 的证据引入 MetricStream，您可以主动识别 AWS 环境中的不合规证据，并将其与来自本地数据来源或其他云合作伙伴的证据一起进行审核。这为您提供了一种便捷而集中的方式，可以在准备审计阶段审核和改进您的云安全与合规状况。

通过 MetricStream 和 Audit Manager 的集成，您可执行以下 API 操作。

任务	API 操作
设置 Audit Manager 集成	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
审核 Audit Manager 资源	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
创建 Audit Manager 资源	• CreateAssessment • CreateAssessmentFramework
更新 Audit Manager 资源	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
管理证据	• StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)
删除 Audit Manager 资源	• DeleteAssessmentFramework

相关 MetricStream 链接

- AWS Marketplace 链接
- 产品链接
- 产品定价

将 Audit Manager 与 AWS SDK 配合使用

AWS 软件开发工具包（SDK）适用于许多常用编程语言。每个 SDK 都提供 API、代码示例和文档，使开发人员能够以其首选语言构建应用程序。

SDK 文档	Audit Manager 特定文档	代码示例	
AWS SDK for C++	AWS SDK for C++Audit Manager 的 API 参考	AWS SDK for C++ 代码示例	
AWS SDK for Go	AWS SDK for GoAudit Manager 的 API 参考	AWS SDK for Go 代码示例	
AWS SDK for Java	AWS SDK for Java 2.xAudit Manager 的 API 参考	AWS SDK for Java 代码示例	
AWS SDK for JavaScript	AWS SDK for JavaScriptAudit Manager 的 API 参考	AWS SDK for JavaScript 代码示例	
AWS SDK for .NET	AWS SDK for .NETAudit Manager 的 API 参考	AWS SDK for .NET 代码示例	
AWS SDK for PHP	AWS SDK for PHPAudit Manager 的 API 参考	AWS SDK for PHP 代码示例	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto)Audit Manager 的 API 参考	AWS SDK for Python (Boto3) 代码示例	
AWS SDK for Ruby	AWS SDK for RubyAudit Manager 的 API 参考	AWS SDK for Ruby 代码示例	

有关特定于 Audit Manager 的示例，请参阅AWS Audit Manager代码示例。

> **Note**
>
> Audit Manager 可用于AWS SDK for Python (Boto3) botocore 版本 1.19.32 及更高版本。开始使用 SDK 之前，请确保您使用的是相应的 botocore 版本。

设置 AWS Audit Manager

在开始使用 Audit Manager 之前，请确保您已完成以下设置任务。

主题

先决条件

按照以下步骤创建 AWS 账户 和具有 Audit Manager 设置权限的管理员用户。

步骤

> **Important**
>
> 如果您已经设置 AWS 和 IAM，则可以跳过步骤 1 和步骤 2。但是，您必须完成步骤 3 才能确保您拥有设置 Audit Manager 所需的权限。

注册 AWS 账户

如果您还没有 AWS 账户，请完成以下步骤来创建一个。

注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

当您注册 AWS 账户时，系统将会创建一个 AWS 账户根用户。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为管理用户分配管理访问权限，并且只使用根用户执行需要根用户访问权限的任务。

注册过程完成后，AWS 会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建管理用户

注册 AWS 账户 后，保护您的 AWS 账户根用户，启用 AWS IAM Identity Center，创建一个管理用户，以避免使用根用户执行日常任务。

保护您的 AWS 账户根用户

1. 选择根用户并输入您的 AWS 账户电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。
2. 对您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅《IAM 用户指南》中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建管理用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为管理用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《AWS IAM Identity Center 用户指南》中的使用默认 IAM Identity Center 目录 配置用户访问权限。

作为管理用户登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

要获取使用 IAM Identity Center 用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的登录 AWS 访问门户。

添加访问和启用 Audit Manager 所需的权限

您必须向用户授予启用 Audit Manager 所需的权限。对于需要有 Audit Manager 的完全访问权限的用户，请使用 AWSAuditManagerAdministratorAccess 托管式策略。这是在 AWS 账户 中可用的 AWS 托管式策略，也是 Audit Manager 管理员的推荐策略。

> **Tip**
>
> 作为一项安全最佳实践，我们建议您开始使用 AWS 托管策略，然后转向最低权限。AWS 托管策略将权限授予针对许多常用用例的权限。然而，请记住，由于 AWS 托管策略可供所有 AWS 客户使用，因此它们可能不会为您的特定用例授予最低权限。因此，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减少许可。有关更多信息，请参阅 AWS Identity and Access Management IAM 用户指南中的 AWS 托管式策略。

要提供访问权限，请为您的用户、群组或角色添加权限：

- AWS IAM Identity Center 中的用户和群组：

  创建权限集。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以代入的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户群组。按照 IAM 用户指南中向用户添加权限（控制台）中的说明进行操作。

启用了 AWS Audit Manager

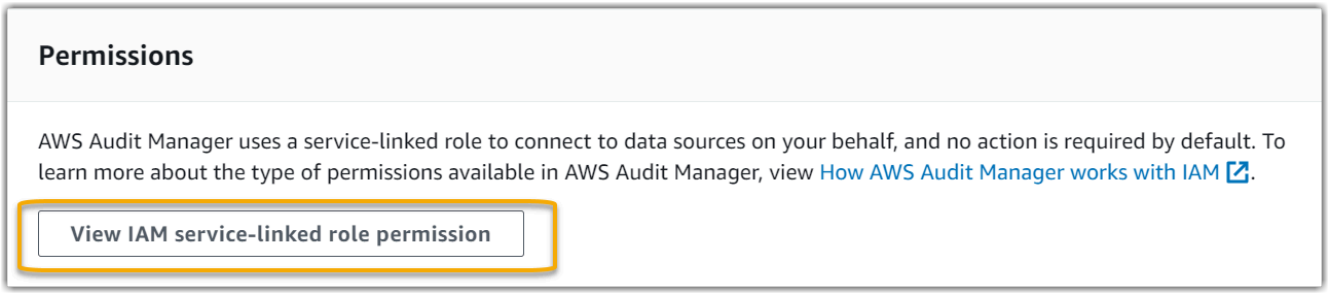
您可以使用 AWS Management Console、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 启用 Audit Manager。

Audit Manager console

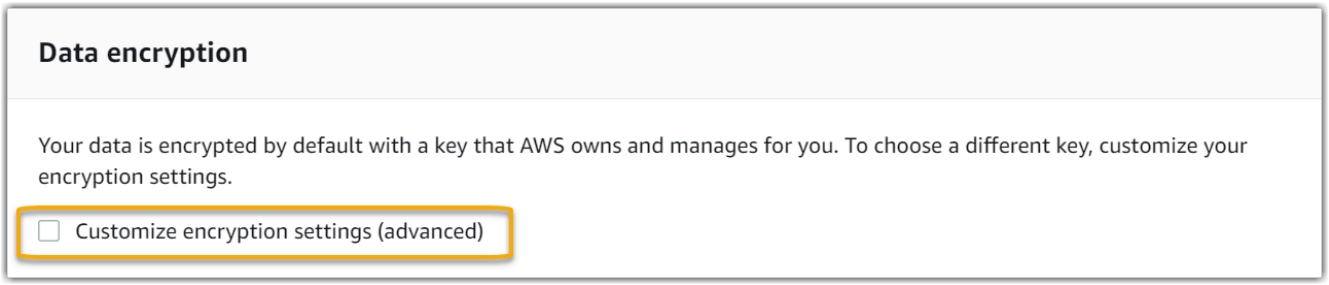
使用控制台启用 Audit Manager

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 使用您的 IAM 身份凭证登录。
3. 选择设置 AWS Audit Manager。

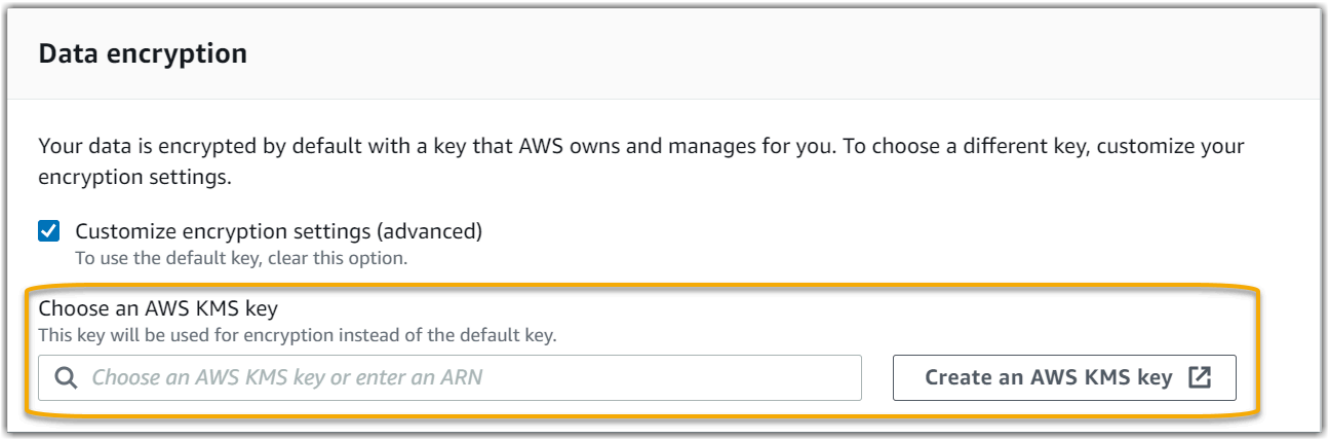
4. 在权限下，无需执行任何操作。这是因为 Audit Manager 使用服务相关角色代表您连接到数据来源。您可以通过选择查看 IAM 服务相关角色权限来查看服务相关角色。



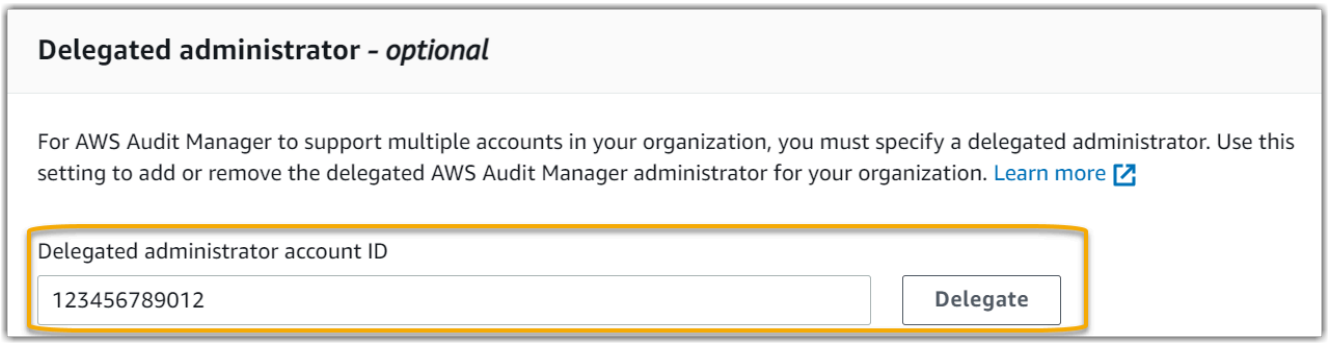
5. 在数据加密下，默认选项是 Audit Manager 创建和管理用于安全存储数据的 AWS KMS key。



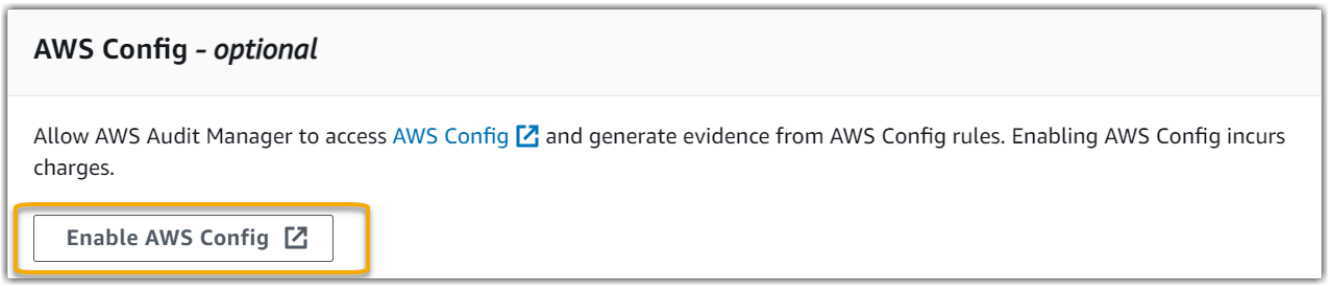
如果您要使用自己的客户托管密钥对 Audit Manager 中的数据进行加密，请选中自定义加密设置（高级）旁边的复选框。您可以选择现有 KMS 密钥或创建新的密钥。



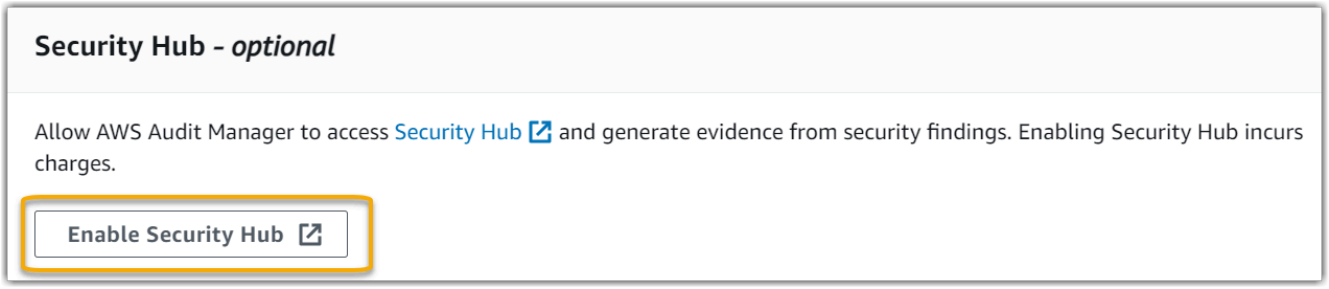
6. （可选）在委托的管理员 — 可选下，如果您希望 Audit Manager 为多个账户运行评测，则可以指定委托管理员账户。有关更多信息和建议，请参阅启用和设置 AWS Organizations 以与 Audit Manager 配合使用。



7. （可选）在 AWS Config — 可选下，我们建议您启用 AWS Config 以获得最佳体验。这使 Audit Manager 能够使用 AWS Config 规则生成证据。有关说明和推荐设置，请参阅启用和设置 AWS Config 以与 Audit Manager 配合使用。



8. （可选）在 Security Hub — 可选下，我们建议您启用 Security Hub 以获得最佳体验。这使 Audit Manager 能够使用 Security Hub 检查生成证据。有关说明和推荐设置，请参阅启用和设置 AWS Security Hub 以与 Audit Manager 配合使用。



9. 选择完成设置以完成设置过程。

AWS CLI

使用 AWS CLI 启用 Audit Manager

在命令行中，使用以下设置参数运行 register-account 命令：

- `--kms-key`（可选）— 使用此参数以使用您自己的客户托管密钥加密您的 Audit Manager 数据。如果您未在此处指定选项，Audit Manager 会代表您创建并管理 AWS KMS key，以安全存储您的数据。
- `--delegated-admin-account`（可选）— 使用此参数为 Audit Manager 指定您组织的委托管理员账户。如果您未在此处指定选项，则不会注册任何委托管理员。

输入示例（将*#####*替换为您自己的信息）：

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

输出示例：

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

有关 AWS CLI 的更多信息以及 AWS CLI 工具的安装说明，请参阅 AWS Command Line Interface 用户指南中的以下内容。

- AWS 命令行界面用户指南
- 开始设置 AWS Command Line Interface

Audit Manager API

使用 Audit Manager API 启用 Audit Manager

将 RegisterAccount 操作与以下设置参数结合使用：

- kmsKey（可选）— 使用此参数以使用您自己的客户托管密钥加密您的 Audit Manager 数据。如果您未在此处指定选项，Audit Manager 会代表您创建并管理 AWS KMS key，以安全存储您的数据。
- delegatedAdminAccount（可选）— 使用此参数为 Audit Manager 指定您组织的委托管理员账户。如果您未指定，则不会注册任何委托管理员。

输入示例（将*#####*替换为您自己的信息）：

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

输出示例：

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

建议

为在 Audit Manager 中获得最佳体验，我们建议您设置以下功能并启用以下 AWS 服务。

主题

设置推荐的 Audit Manager 功能

在启用 Audit Manager 之后，我们建议您启用证据查找器功能。

证据查找器 提供了一种在 Audit Manager 中搜索证据的强大功能。您可以使用证据查找器快速查询证据，而不必通过浏览嵌套程度很高的证据文件夹来查找所需内容。如果您以委派管理员的身份使用证据查找器，则可以在组织中的所有成员帐户中搜索证据。使用筛选条件和分组的组合，可以逐步缩小搜索查询的范围。例如，如果您想从高层次查看系统运行状况，请进行广泛搜索并按评测、日期范围以及资源合规性进行筛选。如果您的目标是修复特定资源，则可以执行狭窄搜索，以瞄准特定控件或资源 ID 的证据。定义筛选条件后，您可分组并预览匹配的搜索结果，然后再创建评测报告。

若要使用证据查找器，必须从 Audit Manager 设置中启用此功能。有关说明，请参阅 证据查找器设置。

设置与其他 AWS 服务 的推荐集成

我们强烈建议您启用以下 AWS 服务，以在 Audit Manager 中获得最佳体验。

- AWS Organizations — 您可以使用组织对多个账户运行 Audit Manager 评测，并将证据整合到委托管理员账户中。
- AWS Security Hub 和 AWS Config — 启用这些 AWS 服务 后，它们可用作 Audit Manager 评测中控件的数据来源类型。然后，Audit Manager 可以直接从这些服务中报告合规性检查的结果。

主题

启用和设置 AWS Config（可选）

Audit Manager 中的许多控件都使用 AWS Config 作为数据来源类型。要支持这些控件，您必须在支持 Audit Manager 的每个 AWS 区域 中的所有账户上启用 AWS Config。如果 Audit Manager 尝试为使用

AWS Config 作为数据来源类型的控件收集证据，但相关 AWS Config 规则未启用，则不会为这些控件收集任何证据。

Audit Manager 不为您管理 AWS Config。您可以按照以下步骤启用 AWS Config 并配置其设置。

将 AWS Config 与 Audit Manager 集成的任务

- 步骤 1：启用 AWS Config
- 第 2 步：配置 AWS Config 设置以用于 Audit Manager。

步骤 1：启用 AWS Config

您可以使用 AWS Config 控制台或 API 启用 AWS Config。有关说明，请参阅 AWS Config 开发人员指南的 AWS Config 入门。

第 2 步：配置 AWS Config 设置以用于 Audit Manager。

> **Important**
>
> 启用 AWS Config 是一项可选建议。但是，如果您启用 AWS Config，则以下设置是必需的。

启用 AWS Config后，请确保您还启用了 AWS Config 规则或部署了合规包，以满足审计相关的标准要求。此步骤可确保 Audit Manager 可以导入所启用的 AWS Config 规则的调查发现。

启用 AWS Config 规则后，我们建议您查看该规则的参数。然后，您应根据所选合规性框架的要求验证这些参数。如果需要，您可以更新 AWS Config 中规则的参数，以确保其符合框架要求。这将有助于确保您的评测收集给定框架的正确合规性检查证据。

例如，假设您正在为 CIS v1.2.0 创建评测。该框架有一个名为 1.4 — 确保访问密钥每 90 天或更短时间轮换一次的控件。在 AWS Config 中，access-keys-rotated 规则有一个包含 90 天默认值的 `maxAccessKeyAge` 参数。因此，该规则与控件要求保持一致。如果您未使用默认值，请确保使用的值大于等于 CIS v1.2.0 中要求的 90 天。

您可在 AWS Config 文档中找到每条托管规则的默认参数详细信息。有关如何配置规则的说明，请参阅使用 AWS Config 托管规则。

启用和设置 AWS Security Hub（可选）

Audit Manager 中的许多控件都使用 Security Hub 作为数据来源类型。要支持这些控件，必须对支持 Audit Manager 的每个区域中的所有账户启用 Security Hub。如果 Audit Manager 尝试为使用 Security

Hub 作为数据来源类型的控件收集证据，但相关的 Security Hub 标准未启用，则不会为这些控件收集任何证据。

Audit Manager 不为您管理 Security Hub。您可以按照以下步骤启用 Security Hub 并配置其设置。

将 AWS Security Hub 与 Audit Manager 集成的任务

- 步骤 1：启用 AWS Security Hub
- 第 2 步：配置 Security Hub 设置以用于 Audit Manager。

步骤 1：启用 AWS Security Hub

您可以使用控制台或 API 来启用 Security Hub。有关说明，请参阅 AWS Security Hub 用户指南中的设置 AWS Security Hub。

第 2 步：配置 Security Hub 设置以用于 Audit Manager。

> **Important**
>
> 启用 Security Hub 是一项可选建议。但是，如果您启用 Security Hub，则以下设置是必需的。

在启用 Security Hub 之后，请确保您还执行以下操作：

- 启用 AWS Config 并配置资源记录 — Security Hub 使用服务相关的 AWS Config 规则对控件进行大部分的安全检查。要支持这些控件，必须启用 AWS Config 并配置为记录您在每个启用的标准中启用的控件所需的资源。
- 启用所有安全标准 — 此步骤可确保 Audit Manager 可以导入所有支持合规标准的调查发现。
- 在 Security Hub 中开启合并控件调查发现设置 — 如果您在 2023 年 2 月 23 日当天或之后启用 Security Hub，则此设置默认处于启用状态。

> **Note**
>
> 启用合并的调查发现时，Security Hub 会为每项安全检查生成一个结果（即使在多个标准中使用相同的检查结果也是如此）。每项 Security Hub 调查发现都作为一项独特的资源评测收集在 Audit Manager 中。因此，合并的调查发现会减少 Audit Manager 针对 Security Hub 的调查结果执行的独特资源评测总数。因此，使用合并的调查发现通常可以降低您的 Audit Manager 使用成本。有关使用 Security Hub 作为数据来源类型的更多信息，请参阅 AWS

Security Hub 支持的控件 AWS Audit Manager。有关 Audit Manager 定价的更多信息，请参阅 AWS Audit Manager 定价。

如果您使用 AWS Organizations 并想从您的成员账户中收集 Security Hub 证据，则还必须在 Security Hub 中执行以下步骤。

设置组织的 Security Hub 设置

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Security Hub 控制台：https://console.aws.amazon.com/securityhub/。
2. 使用您的 AWS Organizations 管理账户，将一个账户指定为 Security Hub 的委托管理员。有关更多信息，请参阅 AWS Security Hub 用户指南中的指定 Security Hub 管理员账户。

   > **Note**
   >
   > 确保您在 Security Hub 中指定的委托管理员账户与您在 Audit Manager 中使用的委托管理员账户相同。

3. 使用您的组织委托管理员账户，转到设置、账户，选择所有账户，然后通过选择自动注册将其添加为成员。有关更多信息，请参阅 AWS Security Hub 用户指南中的启用组织中的成员账户。
4. 为组织的每个成员账户启用 AWS Config。有关更多信息，请参阅 AWS Security Hub 用户指南中的启用组织中的成员账户。
5. 为组织的每个成员账户启用 PCI DSS 安全标准。默认情况下，AWS CIS 基金会基准标准和 AWS 基础最佳实践标准已启用。有关更多信息，请参阅 AWS Security Hub 用户指南中的启用安全标准。

启用 AWS Organizations（可选）

Audit Manager 通过与 AWS Organizations 集成，支持多个账户。Audit Manager 可跨多个账户运行评测，将证据合并至委托管理员账户。委托管理员有权以组织作为信任区域创建和管理 Audit Manager 资源。只有管理账户才能指定委托管理员。

将 AWS Organizations 与 Audit Manager 集成的任务

- 步骤 1：创建或加入组织
- 步骤 2：启用组织中的所有功能。

- 步骤 3：为 Audit Manager 指定委托管理员

步骤 1：创建或加入组织

如果您的 AWS 账户 不是组织的成员，则可以创建或加入组织。有关更多说明，请参阅 AWS Organizations 用户指南中的创建并管理组织。

步骤 2：启用组织中的所有功能。

接下来，您必须启用组织中的所有功能。有关更多说明，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。

步骤 3：为 Audit Manager 指定委托管理员

我们建议您使用组织管理账户启用 Audit Manager，然后指定委托管理员。之后，您可以使用委托管理员账户登录并运行评测。作为最佳做法，我们建议您仅使用委托管理员账户而不是管理账户创建评测。

> **Warning**
>
> 使用组织管理账户指定委托管理员后，您的管理账户将无法再在 Audit Manager 中创建其他评测。此外，对于管理账户创建的任何现有评测，证据收集将停止。相反，Audit Manager 收集证据并将其附加到委托管理员，后者是管理组织的评测的主账户。

要在启用 Audit Manager 后添加或更改委托管理员，请参阅AWS Audit Manager 设置、委派管理员。

要考虑的问题：

- 您不能在 Audit Manager 中以委托管理员的身份使用您的管理账户。
- 如果要在多个 AWS 区域 中启用 Audit Manager，则必须在每个区域中分别指定一个委托管理员账户。在您的 Audit Manager 设置中，您应该在所有区域指定相同的委托管理员账户。
- 如果您在启用 Audit Manager 时提供了客户托管密钥，请确保委托管理员账户有权访问该 KMS 密钥。要查看和更改您的 Audit Manager 加密设置，请参阅 数据加密。
- 有关 Audit Manager 中常见的组织和委托管理员问题的解决方案，请参阅 委托管理员和 AWS Organizations 问题排查。

接下来如何操作？

既然您已经设置 Audit Manager，就可以开始使用该服务了。您也可以访问控制台的设置页面，更新您在设置 Audit Manager 时选择的任何设置。

开始使用 Audit Manager

您可以按照教程开始使用 Audit Manager，该教程将引导您完成如何创建首个评测。有关更多信息，请参阅审计负责人教程：创建评测。

更新您的 Audit Manager 设置

您可以随时更新设置。有关更多信息，请参阅AWS Audit Manager 设置。

AWS Audit Manager 入门

使用本部分的教程，了解如何使用 AWS Audit Manager 执行任务。

> **Tip**
>
> 以下教程可按受众分类。根据您的角色是审计负责人还是委托人，选择适用于您的教程。
>
> - 审计负责人是负责创建和管理评测的 Audit Manager 用户。在商业额领域，审计负责人通常是治理、风险管理和合规 (GRC) 专业人员。但是，在 Audit Manager 的背景下，来自 SecOps 或 DevOps 团队的人员也可以客串审计负责人的用户角色。审计负责人可以请求主题专家（也称为委托人）的帮助，以审核特定的控制措施并验证证据。审计负责人必须具有管理评测的所需权限。
> - 委托人是具有专业技术或业务专长的主题专家。尽管他们不负责或管理 Audit Manager 评测，但他们仍然可以为评测做出贡献。委托人协助审计负责人完成任务，例如验证属于其专业领域的控制措施证据。委托人在 Audit Manager 中的权限有限。原因是审计负责人委托人指定要审核的控件集，而非整体评测。
>
> 有关这些角色和其他 Audit Manager 概念的更多信息，请参阅本指南 AWS Audit Manager 概念和术语 部分的审计负责人和委托人。有关针对每个角色推荐的 IAM 权限的更多信息，请参阅 中针对用户角色的推荐策略 AWS Audit Manager。

Audit Manager 教程

创建评测

受众：审计负责人

概述：按照分布说明创建您的首次评测，并快速启动和运行。本教程将向您介绍如何使用标准框架创建评测并开始自动收集证据。

审核控件集

受众：委托人

概述：通过审核属于您专长的控件的证据，为审计负责人提供协助。学习审核控件集及其相关证据、添加评论、上传其他证据，以及更新控件的状态。

审计负责人教程：创建评测

本教程介绍了 AWS Audit Manager 的实际操作。在本教程中，您将使用 AWS Audit Manager 示例框架创建评测。通过创建评测，您可以开始持续为该框架内的控件自动收集证据。

本教程介绍如何执行以下操作：

- 选择要从中创建评测的标准框架
- 指定要纳入评测中的 AWS 账户
- 指定要纳入评测中的 AWS 服务
- 为您的评测指定审计负责人
- 审核和创建您的评测

开始本教程之前，请确保满足以下条件：

- 您已完成 设置 AWS Audit Manager 中描述的所有先决条件。您必须使用您的 AWS 账户和 AWS Audit Manager 控制台以完成本教程。
- 您的 IAM 身份被授予在 AWS Audit Manager 中创建和管理评测的相应权限。授予这些权限的两个建议策略是示例 2：允许完全管理员访问权限和示例 3：允许管理访问权限。
- 您熟悉 Audit Manager 的术语与功能。有关一般概述，请参阅 什么是 AWS Audit Manager？ 和 AWS Audit Manager 概念和术语。

> **Note**
>
> AWS Audit Manager 协助收集与核实特定合规框架和法规遵守情况相关的证据。但是，它本身并不能评测您的合规情况。因此，通过 AWS Audit Manager 收集的证据可能不包括审计所需的、有关您的 AWS 使用情况的所有信息。AWS Audit Manager不能代替法律顾问或合规专家。

第 1 步：指定评测详细信息

在第一步，为您的评测选择一个框架并提供基本信息。

若要指定评测详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。

2. 选择启动AWS Audit Manager。
3. 在导航窗格中，选择入门，然后选择从框架开始。
4. 选择所需的框架，然后选择使用框架创建评测。此示例使用 AWS Audit Manager 示例框架。
5. 在评测名称下，输入评测的名称。
6. （可选）在评测描述下，输入评测的描述。
7. 在评测报告目标下，选择要保存评测报告的目标 Amazon S3 桶。
8. 在框架下，确认已选中 AWS Audit Manager 示例框架（或您选择的框架）。
9. 在标签下，选择添加新标签以将标签与您的评测相关联。可为每个标签指定密钥和值。标签密钥为必填项，在搜索此评测时可用作搜索标准。有关 AWS Audit Manager 中的标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签。
10. 选择 Next（下一步）。

步骤 2：指定范围内的 AWS 账户

接下来，指定想要纳入评测范围的 AWS 账户。

AWS Audit Manager 与 AWS Organizations 集成，因此您可以对多个账户运行 Audit Manager 评测，并将证据整合至委托管理员账户。要在 Audit Manager 中启用组织（如您尚未启用），请参阅本指南的设置页面上的 启用 AWS Organizations（可选）。

> **Note**
>
> 在评测范围内，Audit Manager 最多可支持大约 150 个账户。如果您尝试纳入超过 150 个账户，则评测创建可能会失败。

若要指定范围内的账户

1. 在 AWS 账户下，选择要纳入评测范围的 AWS 账户。
   - 如果您在 AWS Audit Manager 中启用了组织，则会列出多个账户。
   - 如果您没有在 Audit Manager 中启用组织，则只会列出您的往来账户。
2. 选择 Next（下一步）。

步骤 3：指定范围内的 AWS 服务

您之前选择的框架定义了 Audit Manager 从中监控和收集证据的 AWS 服务。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的服务列表为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于标准框架要求。如果未选择列出的 AWS 服务，则 Audit Manager 不会从与该服务相关的资源中收集证据。如果选中后未在自己的环境中订阅，也会出现这种情况。

在本教程的这一步中，您可以根据框架定义查看评测范围内的 AWS 服务。要了解有关框架、以及如何访问和查看框架的更多信息，请参阅本指南的 框架库 部分。

若要指定范围内的 AWS 服务

1. 在 AWS服务下，查看此评测范围内的服务列表。
2. 选择 Next（下一步）。

> **Tip**
>
> 如果您需要编辑范围内的服务列表，则可以使用 Audit Manager 提供的 CreateAssessment API 完成此操作。
> 或者，您可以自定义标准框架，然后通过自定义框架创建评测。

步骤 4：指定审计负责人

在此步骤中，您将为评测指定审计负责人。审计负责人是工作场所中负责管理 Audit Manager 评测的人员，通常来自 GRC、SecOps 或者 DevOps 团队。我们建议他们使用 AWSAuditManagerAdministratorAccess 策略。

若要指定审计负责人

1. 在审计负责人下，为您的评测选择审计负责人。要查找其他审计负责人，请使用搜索栏按姓名或 AWS 账户进行搜索。
2. 选择 Next（下一步）。

步骤 5：审核并创建

审核您的评测信息。若要更改步骤信息，请选择编辑。完成后，选择创建评测以启动您的第一项评测，并开始持续收集数据。

创建评测后，将继续收集证据，直至您将评测状态更改为非活动。或者，您可以通过将控制状态更改为非活动，停止收集特定控件证据。

> **Note**
>
> 创建评测后，系统会在 24 小时内提供自动证据。AWS Audit Manager 自动从多个数据来源收集证据，收集证据的频率取决于证据类型。有关更多信息，请参阅本指南中的 证据收集频率。

接下来该做什么？

我们建议您继续详细了解本教程中介绍的概念与工具。为此，您可查看以下资源：

- 审核评测— 向您介绍评测页面，您可以在其中浏览不同的评测组成部分。
- AWS Audit Manager中的评测— 以本教程为基础，针对管理评测的概念和任务，提供全面详实的信息。本文档中，我们特别建议您查看以下主题：
  - 如何通过不同的框架创建评测
  - 如何审核评测证据和生成评测报告
  - 如何更改评测状态或删除评测
- 框架库— 介绍框架库，并说明如何创建自定义框架以满足自己的特定合规需求。
- 控件库— 介绍控件库，并说明如何创建自定义控件以用于自定义框架。
- AWS Audit Manager 概念和术语— 提供 Audit Manager 中所用概念和术语的定义。
- [视频] 使用 AWS Audit Manager 收集证据和管理审计数据 — 显示本教程中描述的评测创建过程以及其他任务，例如审核控件和生成评测报告。

委托人教程：审核控件集

本教程介绍如何在 AWS Audit Manager 中审核审计负责人与您共享的控件集。

审计负责人使用 Audit Manager，为该评测中列出的控件创建评测并收集证据。有时，审计负责人在验证控件集证据时可能会有疑问或需要帮助。在这种情况下，审计负责人可以将控件集委托至主题专家进行审核。

作为委托人，您可以帮助审计负责人审核收集到的证据，以了解属于您专长的控件。

本教程介绍如何执行以下操作：

- 访问审计负责人向您发送的通知
- 审核控件集及其相关证据
- 上传手动证据以支持控件
- 为您正在审核的控件添加评论
- 更新控件状态
- 审核完成后，将已审核的控件集提交给审计负责人

开始本教程之前，请确保满足以下条件：

- 您的 AWS 账户已设置完毕。要完成本教程，您必须使用您的 AWS 账户和 AWS Audit Manager 控制台。有关更多信息，请参阅设置 AWS Audit Manager。
- 您熟悉 Audit Manager 的术语与功能。有关 Audit Manager 的总体概述，请参阅 什么是 AWS Audit Manager？ 和 AWS Audit Manager 概念和术语。

第 1 步：访问您的通知

首先登录至 AWS Audit Manager，您可在那里访问通知以查看已委托给您审核的控件集。

若要访问您的通知

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择通知。或者在页面顶部的蓝色闪存栏中，选择查看通知以打开通知页面。
3. 在 通知 页面，您可以查看已委托给您的控件集列表。该通知表格包含以下信息：
    - 日期 — 委托控件集的日期。
    - 评测 — 与控件集关联的评测名称。您可以选择评测名称以打开评测详情页面。
    - 控件集 — 委托给您进行审核的控件集的名称。
    - 来源 — 将控件集委托给您的用户或角色。

- 描述 — 审计负责人提供的审核说明。

> **Tip**
>
> 您还可以订阅 SNS 主题，以便在控件集分配给您进行审核时接收电子邮件提醒。有关更多信息，请参阅 AWS Audit Manager 中的通知。

第 2 步：检查控件集和相关证据

下一步是查看审计负责人委托给您的控件集。通过检查控件及其证据，您可以确定是否需要采取任何其他措施来进行控制。其他操作可能包括手动上传其他证据以证明合规性，或者对控制措施发表评论。

若要审核控件集

1. 在通知页面，审核已委托给您的控件集列表。然后确定要审核的项目，并选择相关评测名称。
2. 在评测详情页面的控制选项卡下，向下滚动至控件集表格。
3. 在按控件集分组的控件列下，展开控件集的名称以显示其控件。然后，选择控件名称以打开控件详情页面。
4. （可选）选择更新控件状态以更改控件的状态。审核进行期间，您可以将状态标记为 正在审核。
5. 在证据文件夹、数据来源、评论和更改日志选项卡中查看有关控件的信息。有关每个选项卡、以及如何解释其中包含数据的更多信息，请参阅查看评测中的控件。

若要审核控件证据

1. 在控件详细信息页面，选择证据文件夹选项卡。
2. 导航至 证据文件夹 表格，其中将显示包含该控件证据的文件夹列表。这些文件夹的组织和命名基于文件夹内的证据的收集日期。
3. 选择证据文件夹名称以将其打开。您可在此查看该日期收集的所有证据摘要。此摘要还包括直接从 AWS Security Hub、AWS Config 或两者兼而有之报告的合规性检查问题总数。有关如何解释此页面数据的说明，请参阅查看证据文件夹。
4. 在证据文件夹摘要页面，导航至证据表格。在 时间 列下，选择要打开的行项目，并查看当时收集的证据的详细信息。有关如何解释报告详细信息页面数据的说明，请参阅审核单个证据。

步骤 3 上传手动证据（可选）

尽管AWS Audit Manager自动收集很多控件的证据，但是有时候您可能需要提供其他证据。在这些情况下，您可以手动上传证据，以帮助证明此控件合规。

在将手动证据上传评测之前，必须先将证据放入 S3 存储桶。有关说明，请参阅 Amazon Simple Storage Service 用户指南中的创建桶和上传对象。

> **Important**
>
> 每个 AWS 账户每天只能将最多 100 个证据文件手动上传至一个控件。超过此每日限额，会导致该控件的任何其他手动上传失败。如果您需要将大量手动证据上传至单个控件，请在几天内分批上传证据。

若要将手动证据上传至控件

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在通知页面，您可以审核已委托给您的控件集列表。确定您要添加证据的目标控件集，然后选择相关评测名称以打开评测详情页面。
3. 选择控件选项卡，向下滚动至控件集，然后选择控件的名称将其打开。
4. 选择证据文件夹选项卡，然后选择上传手动证据。
5. 在下一页输入证据的 S3 URI。要查找 S3 URI，您可在 Amazon S3 控制台中导航至对象，然后选择复制 S3 URI。
6. 选择上传以上传手动证据。

> **Note**
>
> 当控件处于非活动状态时，您无法为该控件上传手动证据。要上传手动证据，您必须先将控件状态更改为正在审核或已审核。有关如何更改控制状态的说明，请参阅 第 5 步：将控件标记为“已审核”（可选）。

第 4 步。为控件添加评论（可选）

您可以为所审核的任何控件添加评论。审计负责人可查看这些评论。例如，您可以发表评论以提供状态更新，确认您已修复该控件的所有问题。

若要向控件添加评论

1. 在通知页面，审核已委托给您的控件集列表。找到您要为其留下评论的目标控件集，然后选择相关评测的名称。
2. 选择控件选项卡，向下滚动至控件集表格，然后选择控件的名称将其打开。
3. 选择评论选项卡。
4. 在发送评论下，在文本框中输入您的评论。
5. 选择提交评论以添加您的评论。现在，您的评论以及有关此控件的任何其他评论都显示在页面的以前的评论部分中。

第 5 步：将控件标记为“已审核”（可选）

可选择更改控件状态。但是，我们建议您在完成对每个控件的审核后，该控件的状态更改为已审核。无论每个控件的状态如何，您仍然可以将控控件提交给审计负责人。

若要将控件标记为“已审核”

1. 在通知页面，审核已委托给您的控件集列表。找到包含要标记为“已审核”的控件的控件集。然后，选择相关评测的名称以打开评测详细信息页面。
2. 在评测详情页面的控制选项卡下，向下滚动至控件集表格。
3. 在按控件集分组的控件列下，展开控件集的名称以显示其控件。选择控件的名称以打开控件详细信息页面。
4. 选择更新控制状态，然后将状态更改为已审核。
5. 在出现的弹出窗口中，选择更新控件状态以确认您已完成对控件的审核。

第 6 步。将已审核的控件集提交回给审计负责人

审核完所有控件后，请将控件集提交回给审计负责人，让他们知道您已完成审核。

若要将已审核的控件集提交回给负责人

1. 在通知页面，审核分配给您的控件集列表。找到要提交给审计负责人的控件集，然后选择相关评测的名称。
2. 向下滚动至控件集表格，选择要提交回给审计责任人的控件集，然后选择提交以供审核。
3. 在显示的弹出窗口中，在选择提交以供审核之前，您可以添加有关该控件集的任何高级评论。

将控件提交给审计负责人后，审计负责人可以查看您留给他们的任何评论。

接下来该做什么？

您可以继续详细了解本教程中介绍的概念。以下是部分推荐资源：

- 审核评测— 向您介绍评测页面，您可以在其中浏览 AWS Audit Manager 中不同的评测组成部分。
- 审核评测中的控件和审核评测中的证据 — 提供定义，帮助您解读每项评测的控件和证据。
- AWS Audit Manager 概念和术语 — 提供 Audit Manager 中所用概念和术语的定义。

使用 Audit Manager 控制面板

利用 Audit Manager 控制面板，您可以在处于活动状态的评测中可视化不合规的证据。这是一种方便快捷的方式，可以监控您的评测、随时了解情况并主动修复问题。默认情况下，控制面板提供所有处于活动状态的评测的自上而下的汇总视图。使用此视图，您可以直观地识别评测中的问题，而无需先筛选大量的个人证据。

控制面板是您登录 Audit Manager 控制台时看到的第一个屏幕。它包含两个小部件，用于显示与您最相关的数据和关键绩效指标 (KPI)。使用评测筛选器，您可以优化这些数据，将重点放在特定评测的 KPI 上。然后，您可以查看控件域分组，以确定哪些控件的不合规证据最多。然后，您可以浏览底层控件以检查和修复问题。

> **Note**
>
> 如果您是 Audit Manager 的首次用户，或者没有任何正在进行的评测，则控制面板中不会显示任何数据。要开始使用，请创建评测。这将开始持续收集证据。24 小时后，聚合的证据数据将开始出现在控制面板中。您可以阅读以下章节以学习如何理解和解释这些数据。

本页将介绍以下主题：

主题

控制面板概念和术语

本节介绍在开始使用 Audit Manager 控制面板之前需要了解的重要事项。

权限和可见性

审计负责人和委托人都可以访问控制面板。这意味着这两个角色都可以看到您 AWS 账户中所有处于活动状态的评测的指标和汇总。访问相同的信息可以让您的所有团队专注于相同的 KPI 和目标。

筛选器

Audit Manager 提供了一个页面级别 the section called “评测筛选器”，您可以将其应用于控制面板上的所有小部件。

不合规的证据

控制面板会突出显示评测中包含合规性检查证据并得出不合规结论的控件。合规性检查证据与使用 AWS Config 或 AWS Security Hub 作为数据来源类型的控件有关。对于这种证据类型，Audit Manager 会直接报告这些服务的合规性检查结果。如果 Security Hub 报告失败结果，或者 AWS Config 报告了不合规的结果，则 Audit Manager 会将证据归类为不合规。

证据尚无定论

如果合规性检查不可用或不适用，则证据尚无定论。因此，无法进行合规性评测。如果控件使用 AWS Config 或 AWS Security Hub 作为数据来源类型，但您没有启用这些服务，则会出现这种情况。如果控件使用的数据来源类型不支持合规性检查，例如手动证据、AWS API 调用或 AWS CloudTrail，则也会出现这种情况。

如果控制台中证据的合规性检查状态为不适用，则在控制面板中将其归类为尚无定论。

合规证据

如果合规性检查没有报告任何问题，则证据合规。如果 Security Hub 报告了通过结果，或者 AWS Config 报告了合规结果，就会发生这种情况。

控件域

控制面板引入了控件域的概念。您可以将控件域视为一类一般的控件，它不是任何一个框架所特有的。控件域分组是控制面板最强大的功能之一。Audit Manager 会突出显示评测中存在不合规证据的控件，并按控件域对它们进行分组。通过使用此功能，您可以在为审计做准备时将补救工作集中在特定主题域上。

> **Note**
>
> 控件域不同于控件集。控件集是特定于框架的控件组合，通常由监管机构定义。例如，PCI DSS 框架有一个名为要求 8：识别和验证系统组件的访问权限的控件集。此控件集属于身份和访问管理控件域。

Audit Manager 将控件归入以下控件域。

控件域名	描述这些控件所控制的内容
业务连续性与应急计划	如何建立流程，以保护关键业务运营免受重大系统和网络中断影响。
变更管理	如何测试、批准、实施和记录云基础架构更改。
数据安全和隐私	您如何保护数据的隐私、可用性和完整性。
开发和配置管理	如何将云基础架构保持为必要且一致的状态。
治理和监督	如何使云计算的使用符合法律、监管和道德义务。
身份和访问管理	如何确保合适的用户获得适当的技术资源访问权限。
事件管理	如何制定责任和程序，确保对安全事件做出快速有效响应。
日志记录和监控	如何审核用户活动，以了解否有迹象表明有人企图或已进行未经授权的活动。
网络管理	如何使用网络管理系统管理和操作数据网络。
人员管理	如何在组织层面评测和管理人员安全风险。
人身安全	如何检测和避免设施中的人身安全问题。
风险管理	如何评测潜在风险和损失，以及如何减少或消除此类威胁。
供应链管理	如何识别、评测和减少与 IT 产品、供应商和供应链相关的风险。
用户设备管理	如何降低员工的 IT 硬件丢失、损坏或受损风险。
漏洞管理	如何定义、评测和修复云基础设施资产的所有已知漏洞。

最终的数据一致性

控制面板数据最终是一致的。这意味着，当您从控制面板读取数据时，它可能不会立即反映最近完成的写入或更新操作的结果。如果您在几个小时内再次检查，控制面板应显示最新数据。

来自已删除和已停止的评测的数据

控制面板显示来自处于活动状态的评测的数据。如果您在查看控制面板的同一天删除评测或将其状态更改为已停止状态，则该评测的数据将包含如下。

- 已停止的评测 — 如果 Audit Manager 在将评测更改为已停止之前收集了证据，则该证据数据将包含在当天的控制面板计数中。
- 已删除的评测 — 如果 Audit Manager 在您删除评测之前收集了证据，则该证据数据不会包含在当天的控制面板计数中。

控制面板元素

以下章节介绍控制面板的不同组件。

主题

评测筛选器

您可以使用评测筛选器将重点放在特定的处于活动状态的评测上。

默认情况下，控制面板显示所有处于活动状态的评测的聚合数据。如果要查看特定评测的数据，可以应用评测筛选器。这是一个页面级筛选器，适用于控制面板上的所有小部件。

要应用评测筛选器，从控制面顶部的下拉列表中选择评测。此列表最多显示 10 个处于活动状态的评测。最近创建的评测显示在最前面。如果您有许多处于活动状态的评测，则可以先键入评测的名称以快速找到它。选择评测后，控制面板将仅显示该评测的数据。

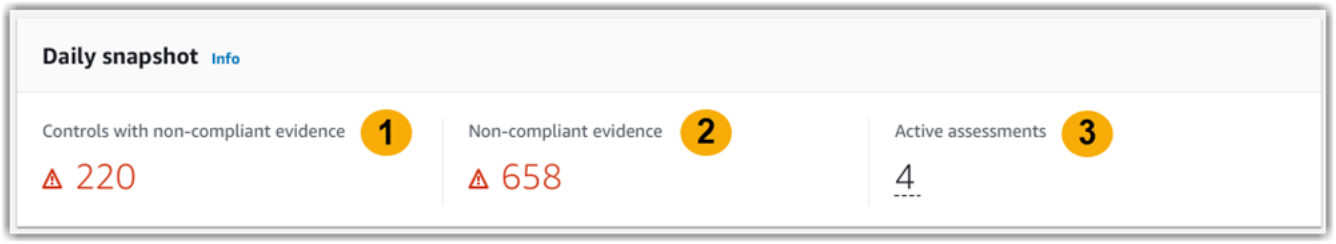
每日快照

此小部件显示处于活动状态的评测的当前合规状态的快照。

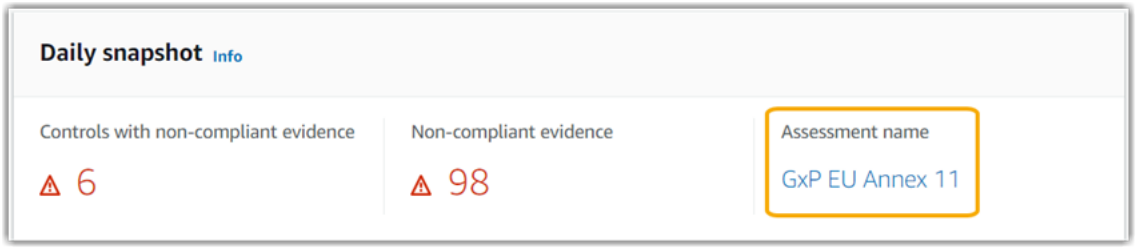
每日快照反映了在控制面板顶部的日期当天收集的最新数据。控制面板上的日期和时间以协调世界时 (UTC) 表示。了解这些数字是基于此时间戳的每日计数，这一点非常重要。到目前为止，它们还不是总和。

默认情况下，每日快照会显示所有处于活动状态的评测的以下数据：

1. 包含不合规证据的控件 — 与不合规证据相关的控件总数。
2. 不合规证据 — 得出不合规结论的合规性检查证据总量。
3. 处于活动状态的评测 — 处于活动状态的评测的总数。选择此数字可查看这些评测的链接。



每日快照数据会根据您应用的 the section called “评测筛选器” 而变化。指定评测时，数据仅反映该评测的每日计数。在这种情况下，每日快照会显示您指定的评测的名称。您可以选择评测名称将其打开。

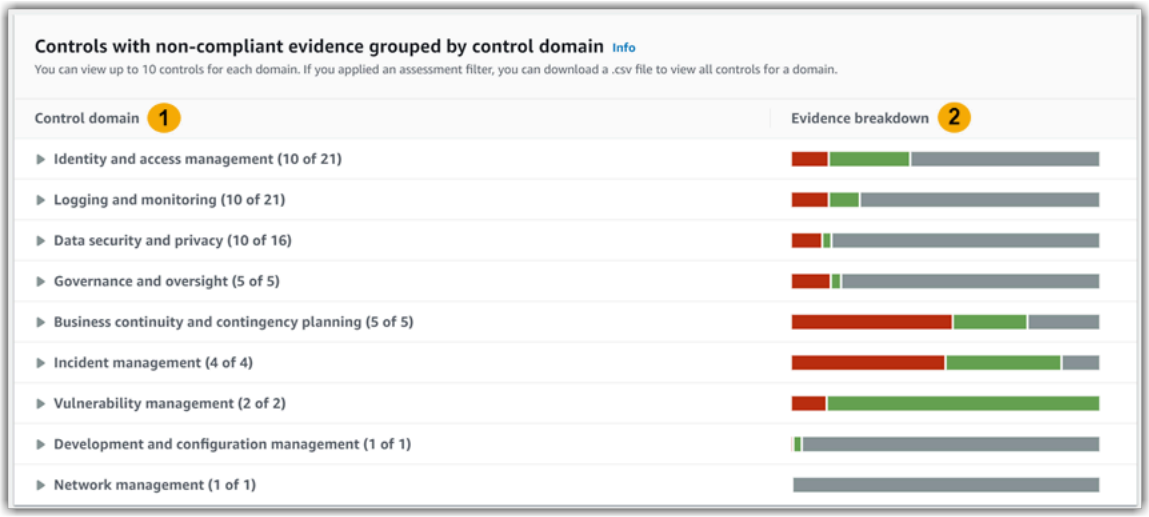


按控件域分组的包含不合规证据的控件

您可以使用此小部件来确定哪些控件的不合规证据最多。

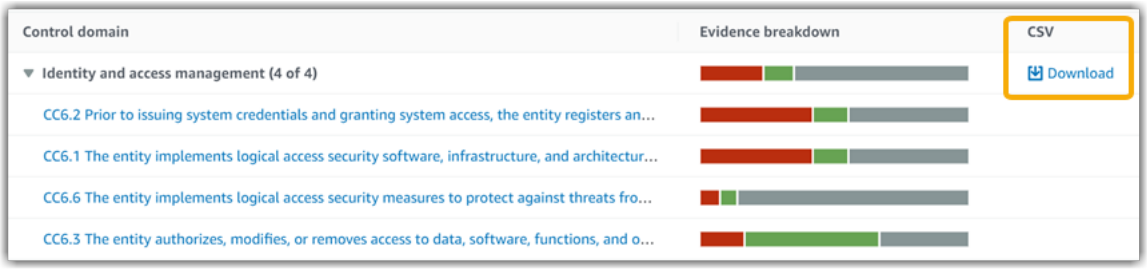
默认情况下，该小部件会显示所有处于活动状态的评测的以下数据：

1. 控件域 — 与您的处于活动状态的评测相关的 control domains 列表。
2. 证据明细 — 显示证据合规状态明细的条形图。



要展开控件域，请选择其名称旁边的箭头。展开后，控制台会为每个域显示最多 10 个控件。这些控件根据不合规证据的最高总数进行排名。

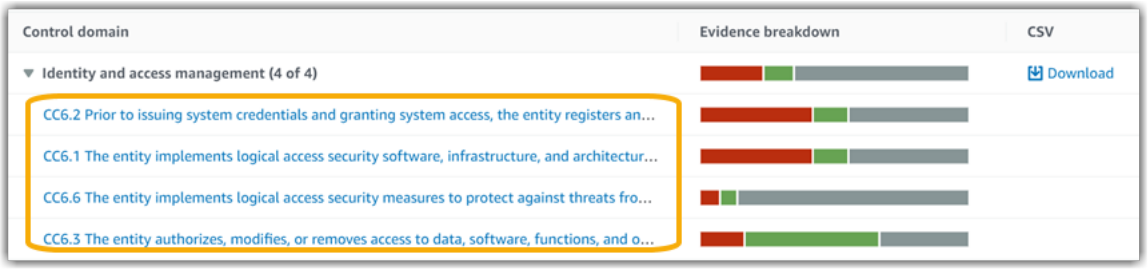
此小部件中的数据会根据您应用的 the section called “评测筛选器” 而变化。指定评测时，您只能看到该评测的数据。此外，您还可以为评测中的每个可用控件域下载 .csv 文件。



.csv 文件包含域中与不合规证据相关的控件的完整列表。以下示例显示值为虚构值的 .csv 数据列。

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

最后，当您应用评测筛选器时，每个域下的控件名称都有超链接。选择任意控件以在指定评测中打开控件详细信息页面。



Tip

使用控件详细信息页面作为起点，您可以从一个详细级别移动到下一个详细级别。

1. 控件详细信息页面 — 在此页面上，证据文件夹选项卡列出了包含 Audit Manager 为该控件收集的每日证据的文件夹。要了解更多详细信息，请选择一个文件夹。
2. 证据文件夹 — 接下来，您可以查看文件夹摘要和该文件夹中的证据列表。有关更多详细信息，请选择单个证据项目。
3. 单个证据 — 最后，您可以浏览单个证据的详细信息。这包括该证据的任何适用属性和资源数据。这是最精细级别的证据数据。

接下来如何操作？

以下是您在查看控制面板后可以采取的一些后续步骤。

- 下载.csv 文件 — 找到您想要重点关注的评测和控件域，并下载包含不合规证据的相关控件的完整列表。
- 查看控件 — 确定需要纠正的控件后，可以查看该控件。
- 委托控件进行审查 — 如果您在审查控件时需要帮助，可以委托控件集进行审查。
- 编辑您的评测 — 如果您想更改正在进行的评测的范围，可以编辑评测。
- 更新评测状态 — 如果要停止为评测收集证据，您可以将评测更改为已停止。

故障排除

要查找常见问题和答案，请参阅本指南疑难解答部分中的解决控制面板问题。

AWS Audit Manager中的评测

Audit Manager 评测基于控件分组框架。您可以框架为起点，对于框架控件中收集到的证据进行评测。评测过程中，您还可以定义审计范围。这包括指定您要为其收集证据的 AWS 账户 和服务。

您可对任何框架创建评测。或者可以使用 Audit Manager 提供的标准框架。或者，您可根据自己构建的自定义框架创建评测。标准框架包含支持特定合规标准或法规的预先构建控件。相比之下，自定义框架包含控件，您可以根据内部审计要求对这些控件进行自定义和分组。有关标准框架和自定义框架之间差异的更多信息，请参阅本指南概念和术语部分中的 框架。

此证据收集过程为持续进程，从您创建评测时开始。当需要进行审计时，您（或您选择的代表）可以查看收集的证据，然后将其添加至评测报告。

> **Note**
>
> AWS Audit Manager 协助收集与核实特定合规性标准和法规遵守情况相关的证据。但是，它本身并不能评测您的合规情况。因此，通过 AWS Audit Manager 收集的证据可能不包括审计所需的、有关您的 AWS 使用情况的所有信息。AWS Audit Manager 不能代替法律顾问或合规专家。

主题

创建评测

本主题以 入门：创建评测教程为基础。它包含有关如何根据框架创建评测的详细说明。按以下步骤创建评测并开始持续收集证据。

任务

- 第 1 步：指定评测详细信息
- 步骤 2：指定范围内的 AWS 账户
- 步骤 3：指定范围内的 AWS 服务
- 步骤 4：指定审计负责人
- 第 5 步：审核并创建
- 接下来如何操作？

第 1 步：指定评测详细信息

首先选择框架并提供评测的基本信息。

若要指定评测详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择 评测模板，然后选择 创建。
   - 或者在导航窗格中选择入门，然后选择创建评测。
3. 在评测名称下，输入评测的名称。
4. （可选）在评测描述下，输入评测的描述。
5. 在评测报告目标下，选择要保存评测报告的目标 Amazon S3 存储桶。

> **Tip**
>
> 默认的评测报告目标基于您的 Audit Manager 设置。有关更多信息，请参阅AWS Audit Manager设置、评测报告目标。你可根据偏好创建和使用多个 S3 存储桶，以帮助您整理评测报告。

6. 在 框架 下，选择要从中创建评测的框架。您也可以使用搜索栏，按名称、合规性标准或法规查找框架。

> **Tip**
>
> 若要了解有关框架的更多信息，请选择框架名称。打开框架详细信息页面。您可在此页面查看此框架内容。这包括框架的控件和数据来源。

7. 在 标签 下，选择 添加新标签，将标签与您的评测相关联。可为每个标签指定密钥和值。标签密钥为必填项，在搜索此评测时可用作搜索标准。有关 Audit Manager 中标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签
8. 选择下一步。

> **Note**
>
> 务必确保您的评测为指定框架收集适当证据。在开始收集证据前，我们建议您查看选定框架要求。然后，根据您当前的 AWS Config 规则参数验证这些要求。为确保您的规则参数与此框架要求保持一致，您可以在AWS Config中更新规则。
> 例如，假设您正在为 CIS v1.2.0 创建评测。此框架包含名为 1.9 – 确保 IAM 密码策略的最小长度为 14 或以上字符的控件。在AWS Config中，iam-password-policy规则中包含检查密码长度的`MinimumPasswordLength`参数。该参数的默认值为 14 个字符。因此，该规则与控件要求保持一致。如果您未使用默认参数值，请确保使用的值大于等于 CIS v1.2.0 中要求的 14 个字符。您可在AWS Config文档中找到每条托管规则的默认参数详细信息。

步骤 2：指定范围内的 AWS 账户

您可在评测范围内指定多个AWS 账户。Audit Manager 通过与AWS Organizations集成，支持多个账户。这意味着 Audit Manager 评测可跨多个账户进行，收集的证据将合并至委托管理员账户。若要在 Audit Manager 中启用 “组织”，请参阅 启用 AWS Organizations（可选）。

> **Note**
>
> 在评测范围内，Audit Manager 最多可支持大约 150 个账户。如果您尝试纳入超过 150 个账户，则评测创建可能会失败。

若要指定范围内的 AWS 账户

1. 在AWS 账户账户下，选择要纳入评测范围的 AWS 账户。

- 如果您在 Audit Manager 中启用了组织，则会显示多个帐户。您可从列表中选择一个或多个帐户。或者，您也可以按帐户名、ID 或电子邮件搜索帐户。
- 如果您没有在 Audit Manager 中启用组织，则只会列出您现有的 AWS 账户。

2. 选择下一步。

> **Note**
>
> 从您的组织中移除范围内的帐户后，Audit Manager 将不再为该账户收集证据。但是，该账户会继续在您的评测中的AWS 账户选项卡下显示。要将该账户从范围内账户列表中移除，您可以编辑评测。在编辑过程中，已移除的账户不再显示在列表中，该账户不在范围内不影响变更的保存。

步骤 3：指定范围内的 AWS 服务

您之前选择的框架定义了 Audit Manager 从中监控和收集证据的 AWS 服务 服务。如果未选中列出的 AWS 服务，或者已选中但您未在环境中启用它，则 Audit Manager 不会从与此服务相关的资源中收集证据。

您可按以下方式指定范围内AWS 服务。

适用于按标准框架创建的评测

当您使用 Audit Manager 控制台从标准框架创建评测时，会默认选择范围内的 AWS 服务 列表。此列表无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于标准框架要求。如果您选择的标准框架仅包含手动控制，则 AWS 服务 不在您的评测范围内，且无法在评测中添加任何服务。

审核列表并选择下一步以继续。

> **Tip**
>
> 如果您需要编辑范围内的服务列表，则可以使用 Audit Manager 提供的 CreateAssessment API 完成此操作。
> 或者，您可以自定义标准框架，然后通过自定义框架创建评测。

适用于按自定义框架创建的评测

如果您在第 1 步 中选择了自定义框架，则可以查看和修改评测范围内的AWS 服务列表。如果您选择的自定义框架仅包含手动控件，则会显示AWS 服务，但不选中。您可选择零个或多个服务作为评测范围。

若要指定范围内 AWS 服务（仅适用于根据自定义框架创建的评测）

1. 在 AWS 服务下，选择要纳入评测的服务。若要查找其他服务，您可以使用搜索栏，按服务、类别或描述搜索。若要添加服务，请选中服务名称旁边的复选框。若要删除服务，请清除此复选框。
2. 完成后，选择AWS 服务下一步。

步骤 4：指定审计负责人

在此步骤中，您将为评测指定审计负责人。审计负责人是工作场所中负责管理 Audit Manager 评测的人员，通常来自 GRC、SecOps 或者 DevOps 团队。我们建议他们使用 AWSAuditManagerAdministratorAccess 策略。

若要指定审计负责人

1. 在 审计负责人下，查看当前的审计负责人列表。审计负责人 列显示用户 ID 和角色。该AWS 账户列显示该审计负责人的关联AWS 账户。
2. 选中复选框的审计负责人将纳入您的评测。清除任何审计负责人的复选框，以将其从评测中删除。要查找其他审计负责人，请使用搜索栏，以按姓名或 AWS 账户 搜索。
3. 完成后，选择下一步。

第 5 步：审核并创建

审核您的评测信息。若要更改步骤信息，请选择 编辑。完成后，选择创建评测。

此操作将开始持续收集评测证据。创建评测后，将继续收集证据，直至您将评测状态更改为非活动。或者，您可以通过将控制状态更改为非活动，停止收集特定控件证据。

> **Note**
>
> 评测创建后 24 小时可获得自动证据。Audit Manager 会自动从多个数据来源收集证据，证据收集的频率取决于证据类型。要了解更多信息，请参阅本指南中的 证据收集频率。

接下来如何操作？

创建评测后，您可以了解以下详细信息：

- 访问评测
- 审核评测
- 编辑评测
- 审核评测中的控件
- 审核评测中的证据
- 将手动证据上传至评测
- AWS Audit Manager 中的委托
- 生成评测报告
- 更改评测状态
- 删除评测
- 对评测和证据收集问题进行排查

访问AWS Audit Manager中的评测

您可以在 Audit Manager 控制台的 评测 页面上查看所有评测。您还可在此编辑评测、删除评测或创建评测。

您也可以通过 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 查看您的评测。

Audit Manager console

若要查看您的评测（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择评测，查看您活动的和过去的评测。您也可通过搜索栏搜索评测。
3. 选择任何评测名称以打开摘要页面，您可以在此查看该评测的详细信息。

AWS CLI

若要查看您的评测（CLI）

若要在 Audit Manager 中查看评测，请运行list-assessments命令。您可以使用 `--status` 子命令查看处于活动状态或非活动状态的评测。

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

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

Audit Manager API

若要查看您的评测（API）

若要在 Audit Manager 中查看评测，请运行ListAssessments 命令。您可以使用状态属性查看处于活动状态或非活动状态的评测。

如需了解更多信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用 `ListAssessments` 操作和参数的信息。

编辑评测

您可以在 Audit Manager 中编辑正在进行的评测，以更改描述、范围、审计负责人和评测报告目标等信息。

任务

- 第 1 步：编辑评测详细信息
- 第 2 步：编辑范围内的 AWS 账户
- 第 3 步：编辑范围内的 AWS 服务
- 第 4 步：编辑审计负责人
- 步骤 5：审核并创建

第 1 步：编辑评测详细信息

按以下步骤编辑评测详细信息。

若要编辑评测

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。

2. 在导航窗格中选择评测，以查看您当前的评测列表。
3. 选择一项评测，然后选择 编辑。
   - 或者，您可以打开评测，然后在页面的右上方选择 编辑。
4. 在编辑评测详细信息下，编辑您的评测名称、描述和评测报告目标。
5. 选择下一步。

> **Tip**
>
> 若要编辑评测标签，请打开评测并选择 标签选项卡。您可查看和编辑与评测关联的标签。

第 2 步：编辑范围内的 AWS 账户

在此步骤中，您可以更改评测范围内的账户列表。

Audit Manager 通过与AWS Organizations集成，支持多个账户。这意味着 Audit Manager 评测可跨多个账户进行，收集的证据将合并至委托管理员账户。要添加或更改 Audit Manager 的委派管理员，请参阅AWS Audit Manager设置、委派管理员。

> **Note**
>
> 在评测范围内，Audit Manager 最多可支持大约 150 个账户。如果您尝试纳入超过 150 个账户，则评测创建可能会失败。

若要编辑范围内的 AWS 账户

1. 编辑范围内AWS 账户下，选择其他AWS账户。您也可以通过移除列表中的账户以清除它们。
2. 选择下一步。

第 3 步：编辑范围内的 AWS 服务

此步骤指定了监控和收集证据的AWS 服务 Audit Manager。如果未选中列出的AWS 服务，或者已选中但您未在环境中启用它，则 Audit Manager 不会从与此服务相关的资源中收集证据。

您可以按如下方式查看和编辑范围内的AWS 服务。

适用于按标准框架创建的评测

当您使用 Audit Manager 控制台编辑根据标准框架创建的评测时，您可以查看范围 AWS 服务 内的列表，但不能编辑此列表。这是因为基于标准框架的设计，Audit Manager 会自动为您映射和选择数据来源和服务。如果评测是使用仅包含手动控制的框架创建的，则 AWS 服务 不在评估范围内，也无法添加任何服务。

审核列表并选择下一步以继续。

> **Tip**
>
> 如果您需要编辑范围内的服务列表，则可以使用 Audit Manager 提供的 UpdateAssessment API 完成此操作。

适用于按自定义框架创建的评测

如果您使用自定义框架创建评测，则可以编辑评测范围内的AWS 服务。您可选择零个或多个服务作为评测范围。

若要编辑范围内 AWS 服务（仅适用于根据自定义框架创建的评测）

1. 在编辑范围内的 AWS 服务 中，选择其他 AWS 服务 账户。您也可以通过移除列表中的服务以清除它们。
2. 选择下一步。

第 4 步：编辑审计负责人

您也可以更改评测的审计负责人。审计负责人是工作场所中负责管理 Audit Manager 评测的人员，通常来自 GRC、SecOps 或者 DevOps 团队。他们的职责包括委托控件集，以供审核和生成评测报告。我们建议您使用AWSAuditManagerAdministratorAccess策略。

编辑审计负责人

1. 选择新的审计负责人，以添加至评测。若要删除审计负责人，请将其从列表中删除。
2. 选择下一步。

步骤 5：审核并创建

审核您的评测信息。若要更改步骤信息，请选择 编辑。编辑完成后，选择保存更改以确认改动。

> **Note**
>
> 完成编辑后，对评测的更改将在世界标准时间 (UTC) 第二天 00:00 生效。

审核评测

在 Audit Manager 中创建评测后，您可以随时打开和查看评测。

打开和查看评测

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择评测，查看您的评测。
3. 选择评测名称以打开。

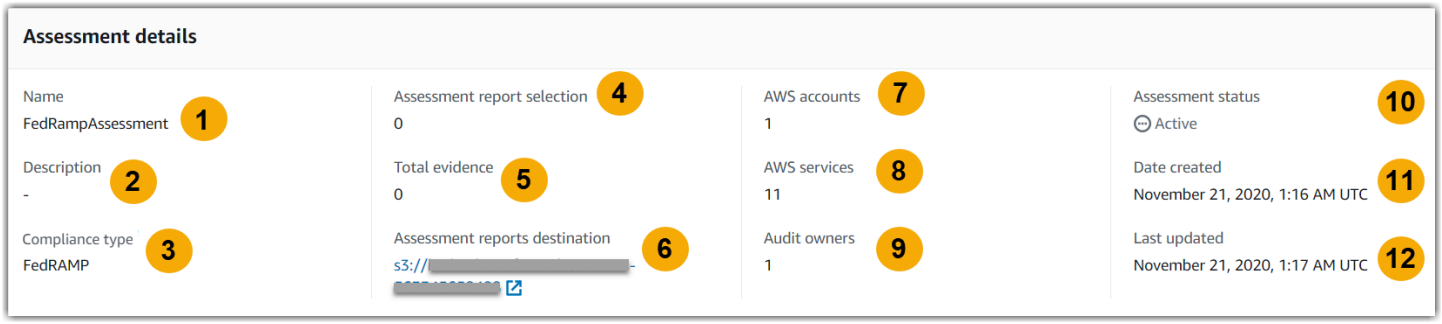
打开评测时，您会看到包含多个部分的摘要页面。本页各个部分及其内容如下所述。

评测页面的各部分

- 评测详细信息
- “控件” 选项卡
- 评测报告选择选项卡
- AWS 账户 选项卡
- AWS 服务 选项卡
- “审计负责人” 选项卡
- 标签选项卡
- 更改日志选项卡

评测详细信息

评测详细信息部分提供了评测的概述。



其中包含以下信息：

1. 姓名 — 您为评测提供的名称。
2. 描述 — 您为评测提供的可选描述。
3. 合规类型 — 框架支持的合规标准或法规。
4. 评测报告选择 — 您选择纳入评测报告中的证据项目数量。
5. 证据总数 — 为本次评测收集的证据项目总数。
6. 评测报告目标 — Audit Manager 在其中保存评测报告的 Amazon S3 存储桶。
7. AWS 账户 — 本次评测范围内的AWS 账户数量。
8. AWS 服务 — 本次评测范围内的AWS 服务数量。
9. 审计负责人 — 此评测的审计负责人编号。
10. 评测状态 — 评测的状态。
    - 活动 — 表示评测当前正在收集证据。新创建的评测包含此状态。
    - 非活动 — 表示评测不再收集证据。有关非活动评测报告的更多信息，请参阅更改非活动评测状态。
11. 创建日期 — 评测的创建日期。
12. 上次更新时间 — 上次编辑此框架的日期。

“控件” 选项卡

控件选项卡显示评测中的控件摘要，以及完整的控件列表。每个评测可以包含多个控件集，每个控件集包含多个控件。控件和控件集的组织方式使其与相关的合规性标准或法规中定义的布局相匹配。

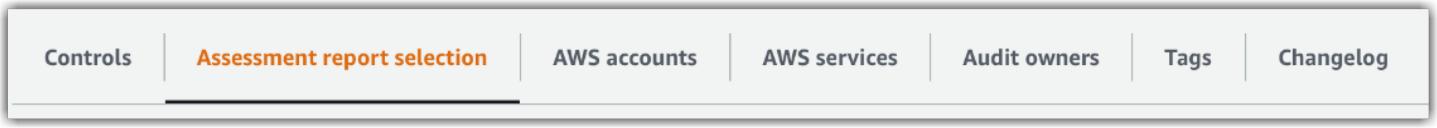
在 控件状态摘要，您可以查看此评测的控件摘要。摘要表包含以下信息：

- 控件总数 — 此评测中的控件总数。
- 已审核 — 审计责任人或代表审核的控件数量。
- 正在审核 — 当前正在审核的控件数量。
- 非活动 — 不再主动收集证据的控件数量。

在 控件集 表格下，将显示控件列表，并按控件集分组。您可以展开或折叠每个控件集内的控件。如果要查询特定控件，也可以按控件名称搜索。以下数据列显示在 按控件集分组的控件 表中：

- 按控件集分组的控件 — 控件集的名称。
- 控件状态 — 控件的状态。
  - 正在审核 表示此控件尚未审核。仍在为这种控件收集证据，您可以上传手动证据。这是默认设置。
  - 已审核 表示已审核此控件的证据。但是，证据仍在收集中，您可以上传手动证据。
  - 非活动 表示已停止为该控件自动收集证据。您无法再通过手动上传证据。
- 受托人 — 此控件的审阅者，前提是该控件已分配给受托人进行审阅。
- 证据总数 — 为本控件收集的证据项目总数。

评测报告选择选项卡



此选项卡显示要纳入评测报告中的证据列表，按证据文件夹分组。这些证据文件夹根据其创建日期进行组织和命名。您可浏览这些文件夹，然后选择要纳入评测报告中的证据。您也可以使用搜索栏，按证据文件夹名称或控件名称进行搜索。若要了解添加至评测报告中的证据项的总数，参见页面顶部的评测详细信息部分。

评测报告选择 表显示了包含以下数据的证据文件夹列表：

- 证据文件夹 — 证据文件夹的名称。文件夹名称基于证据收集的日期。
- 选定证据 — 评测报告中包含的、文件夹内的证据项。
- 控件名称 — 与此证据文件夹关联的控件名称。

有关向评测报告添加证据的信息，请参阅 生成评测报告。

AWS 账户 选项卡

此选项卡将显示评测中的范围内AWS 账户列表。若要了解账户总数，参见页面顶部的评测详细信息部分。

该 AWS 账户 表显示包含以下数据的账户列表：

- 账户 ID - AWS 账户 的 ID。
- 账户名称 - AWS 账户 的名称。
- 电子邮件 - 与 AWS 账户 关联的电子邮件地址。

AWS 服务 选项卡

此选项卡将显示评测中的范围内AWS 服务列表。换句话说，这些是您的评测收集证据的相关AWS 服务。

服务总数汇总在页面顶部的评测详细信息部分内。

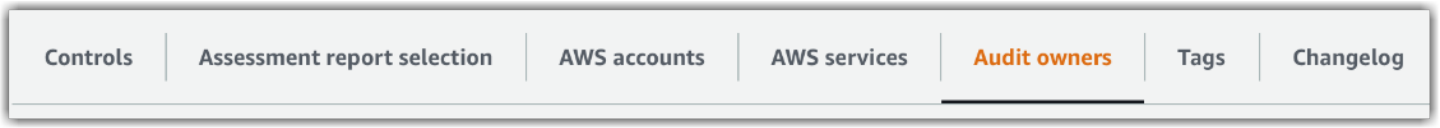
该 AWS 服务 表显示包含以下数据的服务列表：

- AWS 服务 - AWS 服务 的名称。
- 类别 — 服务类别，例如计算或数据库。

Audit Manager 对下表中的服务执行资源评测。例如，如果列出了 Amazon S3，则 Audit Manager 可收集有关您的 S3 存储桶的证据。收集的确切证据由控件数据来源决定。例如，如果数据来源类型为AWS Config，而数据来源映射是AWS Config规则（例如`s3-bucket-public-write-prohibited`），则 Audit Manager 会收集此规则评测的结果作为证据。有关更多信息，请参阅本指南的服务和数据来源类型之间有何区别？

> **Note**
>
> 如果您在控制台中通过标准框架创建评测，则 Audit Manager 会为您选中服务，并根据框架要求映射其数据来源。如果此标准框架仅包含手动控件，则 AWS 服务 不在范围内。如果您需要编辑范围内的服务列表，您可使用UpdateAssessment API。

“审计负责人” 选项卡

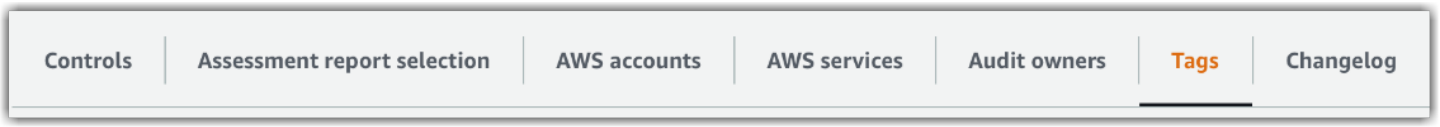


此选项卡显示评测的审计负责人。页面顶部的评测详细信息部分还汇总了审计负责人的总数。

审计负责人表包含以下数据的账户列表：

- 审计负责人 — 审计负责人的姓名。
- AWS 账户 - 与审计负责人关联的电子邮件地址。

标签选项卡



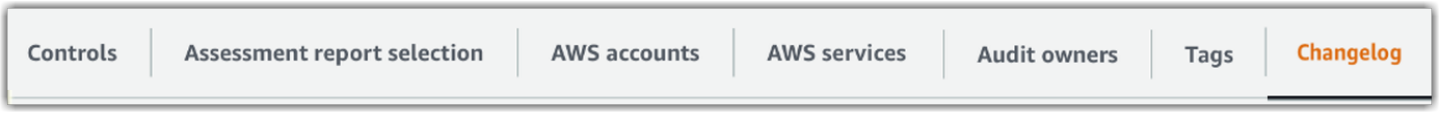
此选项卡显示从框架继承的标签列表，这些标签旨在用于创建评测 标签总数汇总在页面顶部的评测详细信息内。

标签表包含以下数据的标签列表：

- 密钥 — 标签密钥（如合规性标准、法规或类别）。
- 值 - 指标签的值。

有关 Audit Manager 中标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签

更改日志选项卡



此选项卡显示与评测相关的用户活动列表。

更改日志表显示包含以下数据的账户列表：

- 日期 — 活动日期。
- 用户 — 执行操作的用户。
- 操作 — 发生的操作，例如正在创建的评测。
- 类型 — 已更改的对象类型，例如评测。
- 资源 — 受变更影响的资源，例如创建评测所依据的框架。

审核评测中的控件

Audit Manager 中的控件可帮助您在审计中满足常见和独特的合规标准与法规。您可以随时在 Audit Manager 评测中打开和查看控件。

若要打开控件摘要页面

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中选择评测，然后选择要打开的评测的名称。
3. 在评测页面中选择控件选项卡，向下滚动至控件集表，然后选择控件的名称将其打开。

打开控件时，您会看到包含多个部分的摘要页面。本页各个部分及其内容如下所述。

控件页面的各个部分

- 控件详细信息
- 更新控件状态
- “证据文件夹” 选项卡
- 数据来源选项卡
- “评论” 选项卡
- 更改日志选项卡

控件详细信息

控件详细信息 部分概览控件。

其中包含以下信息：

1. 控件名称 — 为该控件指定的名称。
2. 控件描述 — 为此控件提供的描述。
3. 测试信息 — 此控件的推荐测试程序。
4. 行动计划 — 如果控件未正常运行，建议采取的行动。

更新控件状态

在该页面的更新控件状态部分，您可查看和更新评测控件的状态。

以下是可能的状态：

- 正在审核 - 表示此控件尚未审核完成。仍在为这种控件收集证据，您可以上传手动证据。这是默认设置。
- 已审核 — 表示此控件证据已经过审核。证据仍在收集中，您可以上传手动证据。
- 非活动 - 表示已停止为该控件自动收集证据。您无法再通过手动上传证据。

> **Note**
>
> 将控件状态更改为 已审核 是最终决定。将控件的状态设置为 已审核 后，您无法再更改该控件的状态或恢复至以前的状态。

“证据文件夹” 选项卡

证据文件夹 选项卡列出了为此控件自动收集的证据。它每天都被整理至文件夹中。

证据文件夹 表显示包含以下数据的文件夹列表：

- 证据文件夹 — 证据文件夹的名称。该名称基于收集或手动添加证据的日期。
- 合规性检查 — 在证据文件夹中发现的问题数量。此数字表示直接从AWS Security Hub、AWS Config或两者报告的安全问题总数。如果您看到 不适用，则表示您未启用AWS Security Hub 或 AWS Config，或证据来自不同的数据来源类型。

- 证据总数 — 文件夹内证据项的总数。
- 评测报告选择 — 您选择纳入评测报告中的证据项目数量。

在 证据文件夹选项卡，您可以执行以下操作：

- 查看个人证据 — 选择证据文件夹以打开。然后，您可以在证据文件夹摘要页面中选择要查看的单个证据。
- 添加手动证据 — 有关更多信息，请参阅 在AWS Audit Manager中添加手动证据。
- 向评测报告中添加证据 - 更多信息，请参阅生成评测报告。

数据来源选项卡

此选项卡显示有关控件数据来源的信息。其中包含以下信息：

- 数据来源名称 — 这仅适用于自定义控件。它指的是您为每个数据来源提供的描述性名称。您可以通过此名称区分属于相同数据来源类型的多个数据来源
- 数据来源类型 — 指定了证据数据的来源。
  - 如果由 Audit Manager 收集证据，则数据来源类型为以下四种之一：AWS Security Hub、AWS Config、AWS CloudTrail 或 AWS API 调用。
  - 如果您上传自己的证据，则数据来源类型为 手动。描述说明所需的手动证据是文件上传还是文字回复。
- 映射 — 用于识别和检索自动数据来源中数据的映射属性。
  - 如果数据来源类型为AWS Config，则映射为特定 AWS Config 规则的名称 (例如`EC2_INSTANCE_MANAGED_BY_SSM`)。Audit Manager 使用此映射报告来自AWS Config的规则检查报告。
  - 如果数据来源类型为AWS Security Hub，则映射为特定 Security Hub 控件的名称 (例如 `1.1 – Avoid the use of the "root" account`)。Audit Manager 使用此映射直接报告来自 Security Hub 的安全检查结果。
  - 如果数据来源类型为 AWS API 调用，则映射为特定的 API 调用名称（例如 `ec2_DescribeSecurityGroups`）。Audit Manager 使用此映射收集 API 响应。
  - 如果数据来源类型为 AWS CloudTrail，则映射为特定 CloudTrail 事件的名称（例如 `CreateAccessKey`）。Audit Manager 使用此映射从您的 CloudTrail 日志中收集相关用户活动。
- 频率 — 从该数据来源收集证据的频率。频率因数据来源而异。有关更多信息，请选择列中的值或参见 证据收集频率。

“评论” 选项卡

在 评论 选项卡中，您可以添加有关控件及其证据的评论。它还会显示先前的评论列表。

若要在 发送评论 下添加评论，您可以输入文本，然后选择 提交评论。

在 以前的评论下，您可以查看之前的评论列表，以及发表评论的日期和关联用户 ID。

更改日志选项卡

更改日志 选项卡显示与控件相关的用户活动列表。提供与AWS CloudTrail的审计跟踪记录相同的信息。通过直接在 Audit Manager 中捕获的用户活动，您可轻松查看指定控件的活动审计跟踪记录。

在 更改日志 下，表格显示了以下数据列：

- 日期 — 活动的日期和时间，用世界标准时间 (UTC) 表示。
- 用户 — 执行活动的用户或角色。
- 操作 — 对活动的描述。
- 类型 — 进一步描述活动的关联属性。
- 资源 — 相关资源（如果适用）。

Audit Manager 在变更日志中追踪以下用户活动：

- 创建评测
- 编辑评测
- 完成评测
- 删除评测
- 委托控件集以供审核
- 将已审核的控件集提交至审计负责人
- 上传手动证据
- 更新控件状态
- 生成评测报告

审核评测中的证据

Audit Manager 中的活动评测会从一系列数据来源自动收集证据。有关更多信息，请参阅AWS Audit Manager 如何收集证据。您可以随时在 Audit Manager 评测中打开和查看控件证据。

若要打开控件证据

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择控件选项卡，向下滚动至控件表，然后选择控件的名称将其打开。
4. 在控件页面，选择证据文件夹选项卡。在证据文件夹表格中，将显示该控件的所有证据文件夹的列表。这些文件夹是根据收集文件夹内证据的日期进行组织和命名的。
5. 选择证据文件夹名称以将其打开。

您可在此查看该控件的证据文件夹，按需进一步查看单独的证据。

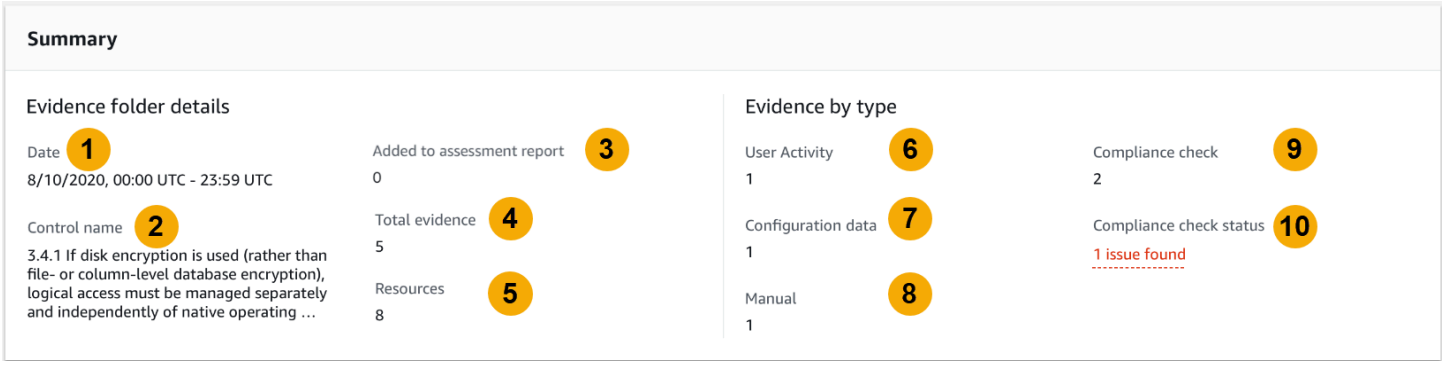
主题

查看证据文件夹

当您打开证据文件夹，你会看到包含两个部分的证据文件夹摘要页面：摘要部分和证据表。本页各个部分及其内容如下所述。

证据文件夹摘要

本页的 摘要 部分提供了证据文件夹中证据的高级概述。



其中包含以下信息：

1. 日期 — 证据文件夹的创建时间和日期，用世界标准时间 (UTC) 表示。
2. 控件名称 — 与此证据文件夹关联的控件名称。
3. 已添加至评测报告 — 您选择纳入评测报告中的证据项目数量。
4. 证据总数 — 证据文件夹内证据项的总数。
5. 资源 — 在此文件夹中生成证据时评测的 AWS 资源总数。
6. 用户活动-属于用户活动类别的证据项数量。这些证据收集自 AWS CloudTrail 日志。
7. 配置数据 — 属于配置数据类别的证据项数量。这些证据是从 Amazon EC2、Amazon S3 或 IAM 等其他AWS 服务 配置快照中收集的。
8. 手动 — 属于手动类别的证据项的数量。此证据为手动上传。
9. 合规性检查 — 属于合规性检查类别的证据项目数量。这些证据收集自 AWS Config 或 AWS Security Hub。
10. 合规性检查状态 - 直接从 AWS Security Hub 或 AWS Config 或二者中报告的问题总数

> **Tip**
>
> 有关不同证据类型（用户活动、配置数据、合规性检查和手动）的更多信息，请参阅 证据。

证据表

证据表列出了证据文件夹中包含的各种证据。

其中包含以下信息：

1. 时间 — 指定收集证据的时间，也可以用作证据的名称。时间以世界标准时间 (UTC) 格式表示。从此栏中选择时间将打开证据详细信息页面。本页将在后续章节中介绍。
2. 按类型划分的证据 — 证据的类别。
   - 合规性检查证据是从AWS Config或AWS Security Hub收集的。
   - 用户活动 证据是从AWS CloudTrail日志中收集的。
   - 配置数据证据是从 Amazon EC2、Amazon S3 或 IAM 等其他服务的快照中收集的。
   - 手动 证据是您手动上传的证据。
3. 合规性检查 — 属于合规性检查类别的证据评估状态。
   - 对于从AWS Security Hub中收集的证据，将直接通过AWS Security Hub报告合格 或 不合格。
   - 对于从 AWS Config 中收集的证据，将直接通过 AWS Config 报告合规或不合规。
   - 如果您看到 不适用，则表示您未启用 AWS Security Hub 或 AWS Config，或证据来自不同的数据来源类型。
4. 数据来源 — 从中收集证据的数据来源。
5. 事件名称 — 证据中包含的事件名称。
6. 资源 - 为生成证据评测的资源数。
7. 评测报告选择 — 指明是否手动选择该证据以纳入评测报告。
   - 若要证据，请选择证据，然后选择 添加至评测报告。
   - 若要排除证据，请选择证据，然后选择从评测报告中移除。

若要将手动证据上传至证据文件夹，请选择上传手动证据，输入证据的 S3 URI，然后选择上传。更多信息，请参阅在 AWS Audit Manager 中上传手动证据。

若要查看任何单个证据的详细信息，请在 时间 列下选择超链接的证据名称。随即打开证据详细信息页面，以下部分将介绍此页面。

审核个人证据

当您打开单个证据时，你会看到包含三个部分的证据详细信息页面：证据详细信息部分、属性表和包含的资源表。本页各个部分及其内容如下所述。

- 证据详细信息
- 属性
- 要包含的资源

证据详细信息

页面的证据详细信息 部分显示了证据概述。

其中包含以下信息：

1. 日期和时间 — 收集证据的日期和时间，用世界标准时间 (UTC) 表示。
2. 证据文件夹名称 — 包含证据的证据文件夹的名称。
3. 控件名称 — 与此证据关联的控件名称。
4. 事件源 — 创建证据事件的资源名称。
5. 事件名称 — 证据事件的名称。
6. 数据来源 — 从中收集证据的数据来源。
7. 按类型划分的证据 — 证据的类别。
   - 合规性检查证据是从AWS Config或AWS Security Hub收集的。
   - 用户活动 证据是从AWS CloudTrail日志中收集的。
   - 配置数据证据是从 Amazon EC2、Amazon S3 或 IAM 等其他 AWS 服务 的快照中收集的。
   - 手动 证据是您手动上传的证据。
8. 合规性检查 — 属于合规性检查类别的证据评估状态。
   - 对于从AWS Security Hub中收集的证据，将直接通过AWS Security Hub报告合格 或 不合格。
   - 对于从AWS Config中收集的证据，将直接通过AWS Config报告合格 或 不合格。
   - 如果您看到不适用，则表示您未启用 AWS Security Hub 或 AWS Config，或证据来自不同的数据来源类型。
9. 纳入的资源 — 为生成证据而评测的资源数量。

10属性 — 证据中的事件属性总数。

11AWS账户 — 证据收集的AWS 账户。

12JAM ID — 相关的用户或角色（如适用）。

13.已添加至评测报告 — 表示您是否选择在评测报告中纳入证据。

属性

属性 表显示事件在此证据中使用的名称和值。其中包含以下信息：

- 属性名称 — 对证据的要求，例如allowUsersToChangePassword。
- 值 — 属性值，例如真或假。

要包含的资源

“纳入的资源” 表显示了为生成此证据而评测的资源清单。其中包含以下一个或多个字段：

- ARN - 资源的 Amazon 资源名称（ARN）。有的证据类型可能不适用 ARN。
- 值 — 该资源的值（如果适用）。
- JSON — 用于查看该资源的 JSON 文件链接。

在AWS Audit Manager中添加手动证据

Audit Manager 可自动收集许多控件的证据。但是，部分控件要求您手动添加自己的证据。

考虑以下示例：

- 部分控件与提供实物记录（例如签名）或非在云中生成的事件（例如观察和访谈）有关。在这些情况下，您可手动上传文件作为证据。例如，如果控件需要有关您的组织结构的信息，则可以上传公司组织结构图的副本，以作为手动证据。
- 部分控件代表了供应商风险评测问题。风险评测问题可能需要文件作为证据（如组织结构图）。或者它可能只需要一个简单的文字回复（例如职位列表）。对于后者，您可回答问题并将您的回答保存为人工证据。

您还可以使用手动上传功能管理来自多个环境的证据。如果您的公司使用混合云模型或多云模型，则可上传来自本地环境、云端托管环境或 SaaS 应用程序的证据。这使您可以通过将证据存储在 Audit Manager 评测的结构中来组织证据（无论它来自哪里），其中每份证据都映射至特定控件。

要详细了解 Audit Manager 中不同类型的证据，请参阅本指南概念和术语部分中的证据。

如何添加手动证据

您可以使用以下任意方法将自己的手动证据添加至评测控件中。

记住以下内容：

- 每次只能使用一种方法来添加手动证据。
- 单个手动证据文件的最大限制为 100 MB。
- 支持手动证据文件格式 在本页下方进一步列出。
- 每个 AWS 账户 每天只能将最多 100 个证据文件手动上传至一个控件。超过此每日配额，会导致该控件的任何其他手动上传失败。如果您需要将大量手动证据上传至单个控件，请在几天内分批上传证据。
- 当控件处于非活动状态，您无法上传该控件的手动证据。若要上传手动证据，您必须先将控件状态更改为 正在审核或 已审核。有关说明，请参阅 更新控件状态。

从 Amazon S3 导入文件

按以下步骤从 S3 桶中导入手动证据。

AWS console

若要从 S3 导入文件（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择 控件 选项卡，向下滚动至 控件集，然后选择控件的名称将其打开。
4. 在 证据文件夹 选项卡，选择 添加手动证据，然后选择 从 S3 导入文件。
   - 或者，在 “证据文件夹” 选项卡中选择证据文件夹名称，以查看证据文件夹摘要，然后选择 添加手动证据、从 S3 导入文件。
5. 在下一页输入证据的 S3 URI。若要查找 S3 URI，你可在Amazon S3 控制台导航至对象，然后选择复制 S3 URI。
6. 选择上传。

AWS CLI

在后续流程中，将#####替换为您自己的信息。

从 S3 导入文件（CLI）

1. 运行 list-assessments 命令以查看您的评测列表。

```
aws auditmanager list-assessments
```

在回复中，找到您要上传证据的评测，并记下其评测编号。

2. 运行 get-assessment 命令并指定第一步中的评测 ID。

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

在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。

3. 以下列参数运行 batch-import-evidence-to-assessment-control 命令：

- --assessment-id — 使用第一步中的评测 ID。
- --control-set-id— 使用第二步中的控件集 ID。
- --control-id — 使用第二步中的控件 ID。
- --manual-evidence — 将 s3ResourcePath 用作手动证据类型，并指定证据的 S3 URI。若要查找 S3 URI，你可在Amazon S3 控制台导航至对象，然后选择复制 S3 URI。

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

Audit Manager API

从 S3 导入文件（API）

1. 调用 ListAssessments 操作以查看您的评测清单。在回复中，找到您要上传证据的评测，并记下其评测编号。
2. 调用 GetAssessment 命令并指定第一步中的评测 ID。在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。
3. 按照以下参数调用 BatchImportEvidenceToAssessmentControl 操作：

- `assessmentId` — 使用第一步中的评测 ID。
- `controlSetId`— 使用第二步中的控件集 ID。
- `controlId` — 使用第二步中的控件 ID。
- `manualEvidence` — 将 `s3ResourcePath` 用作手动证据类型，并指定证据的 S3 URI。若要查找 S3 URI，你可在Amazon S3 控制台导航至对象，然后选择复制 S3 URI。

如需了解更多信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

从浏览器上传文件

按以下步骤从浏览器上传手动证据。

AWS console

从浏览器（控制台）上传文件

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择 控件 选项卡，向下滚动至 控件集，然后选择控件的名称将其打开。

   您可在此通过三种方式上传文件：

   - （选项 1）在蓝色通知横幅，选择上传手动证据。
   - （选项2）在 证据文件夹 选项卡，选择 添加手动证据，然后选择 从浏览器上传文件。
   - （选项 3）选择证据文件夹名称以查看该文件夹摘要，选择 添加手动证据，然后选择 从浏览器上传文件。
4. 选择你要上传的文件。
5. 选择上传。

AWS CLI

在以下示例中，将#####替换为您自己的信息。

从浏览器（CLI）上传文件

1. 运行 list-assessments 命令以查看您的评测列表。

```
aws auditmanager list-assessments
```

在回复中，找到您要上传证据的评测，并记下其评测编号。

2. 运行 get-assessment 命令并指定第一步中的评测 ID。

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

在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。

3. 运行 get-evidence-file-upload-url 命令并指定要上传的文件。

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

在响应中，记录预签名 URL 和evidenceFileName。

4. 使用第三步中的预签名 URL，从浏览器上传文件。此操作会将您的文件上传至 Amazon S3，并在那里将其另存为可以附加至评测控件的对象。在接下来的步骤中，您将使用evidenceFileName参数引用新创建对象。

> **Note**
>
> 当您使用预签名 URL 上传文件时，Audit Manager 会通过AWS Key Management Service，使用服务器端加密来保护和存储您的数据。为了支持这一点，在使用预签名 URL 上传文件时，必须在请求中使用 x-amz-server-side-encryption 标头。如果您使用的是 Audit Manager 数据加密设置中的客户托管AWS KMS key，请确保在请求中纳入x-amz-server-side-encryption-aws-kms-key-id标头。如果请求中没有该 x-amz-server-side-encryption-aws-kms-key-id 标头，Amazon S3 会假定您想要使用 AWS 托管式密钥。
>
> 有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的借助使用 AWS Key Management Service 密钥（SSE-KMS）的服务器端加密保护数据。

5. 以下列参数运行 batch-import-evidence-to-assessment-control 命令：

- --assessment-id — 使用第一步中的评测 ID。

- `--control-set-id`— 使用第二步中的控件集 ID。
- `--control-id` — 使用第二步中的控件 ID。
- `--manual-evidence` — 将`evidenceFileName` 用作手动证据类型，并指定第三步中的证据文件名。

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

Audit Manager API

上传来自浏览器的文件 (API)

1. 调用 ListAssessments 操作。在回复中，找到您要上传证据的评测，并记下其评测编号。
2. 调用 GetAssessment 操作并指定第一步中的 `assessmentId`。在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。
3. 调用 GetEvidenceFileUploadUrl 操作并指定要上传的`fileName`。在响应中，记录预签名 URL 和`evidenceFileName`。
4. 使用第三步中的预签名 URL，从浏览器上传文件。此操作会将您的文件上传至 Amazon S3，并在那里将其另存为可以附加至评测控件的对象。在接下来的步骤中，您将使用`evidenceFileName`参数引用新创建对象。

> **Note**
>
> 当您使用预签名 URL 上传文件时，Audit Manager 会通过AWS Key Management Service，使用服务器端加密来保护和存储您的数据。为了支持这一点，在使用预签名 URL 上传文件时，必须在请求中使用 `x-amz-server-side-encryption` 标头。如果您使用的是 Audit Manager 数据加密设置中的客户托管AWS KMS key，请确保在请求中纳入`x-amz-server-side-encryption-aws-kms-key-id`标头。如果请求中没有该 `x-amz-server-side-encryption-aws-kms-key-id` 标头，Amazon S3 会假定您想要使用 AWS 托管式密钥。
>
> 有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的借助使用在 AWS Key Management Service (SSE-KMS) 中存储 KMS 密钥的服务器端加密保护数据。

5. 按照以下参数调用 BatchImportEvidenceToAssessmentControl 操作：

   - assessmentId — 使用第一步中的评测 ID。
   - controlSetId— 使用第二步中的控件集 ID。
   - controlId — 使用第二步中的控件 ID。
   - manualEvidence — 将evidenceFileName 用作手动证据类型，并指定第三步中的证据文件名。

如需了解更多信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

输入文字回复

按以下步骤输入风险评测问题的答案，并将您的回答保存为手动证据。

AWS console

若要输入文字回复（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择 控件 选项卡，向下滚动至 控件集，然后选择控件的名称将其打开。

   您可在此通过三种方式输入文字回复：

   - (选项 1) 在蓝色通知横幅，选择输入回复。
   - （选项 2）在 证据文件夹 选项卡，选择 添加手动证据，然后选择 输入文字回复。
   - （选项 3）选择证据文件夹名称以查看该文件夹摘要，选择 添加手动证据，然后选择 输入文本回复。
4. 在所示弹出窗口中，以纯文本格式输入您的回复。
5. 选择确认。

AWS CLI

在以下示例中，将#####替换为您自己的信息。

输入文字回复 (CLI)

1. 运行 list-assessments命令。

```
aws auditmanager list-assessments
```

在回复中，找到您要上传证据的评测，并记下其评测编号。

2. 运行 get-assessment 命令并指定第一步中的评测 ID。

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

在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。

3. 以下列参数运行 batch-import-evidence-to-assessment-control 命令：

- --assessment-id — 使用第一步中的评测 ID。
- --control-set-id— 使用第二步中的控件集 ID。
- --control-id — 使用第二步中的控件 ID。
- --manual-evidence — 将 textResponse 用作手动证据类型，然后输入要另存为手动证据的文本。

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

Audit Manager API

输入文字回复 (API)

1. 调用 ListAssessments 操作。在回复中，找到您要上传证据的评测，并记下其评测编号。
2. 调用 GetAssessment 操作并指定第一步中的 assessmentId。在响应中，找到要向其上传证据的目标控件集和控件，并记下它们的 ID。
3. 按照以下参数调用 BatchImportEvidenceToAssessmentControl 操作：

- assessmentId — 使用第一步中的评测 ID。

- controlSetId— 使用第二步中的控件集 ID。
- controlId — 使用第二步中的控件 ID。
- manualEvidence — 将 textResponse 用作手动证据类型，然后输入要另存为手动证据的文本。

如需了解更多信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

支持手动证据文件格式

下表列出并描述了您可以手动证据形式上传的文件类型。对于每种文件类型，该表还列出了所支持的文件扩展名。

文件类型	描述	支持的文件扩展名
压缩或存档	GNU Zip 压缩档案与 ZIP 压缩档案	.gz, .zip
文档	常见文档文件，例如 PDF 和 Microsoft Office 文件	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx
图像	图像和图形文件	.jpeg, .jpg, .png, .svg
文本	其他非二进制文本文件，例如纯文本文档以及标记语言文件	.cer, .csv, .html, .jmx, .json, .md, .out, .rtf, .txt, .xml, .yaml, .yml

生成评测报告

评测报告总结了您的评测，并提供指向包含相关证据的、一组有组织的文件夹链接。有关更多信息，请参阅评测报告。

生成评测报告之前，您可以选择要在评测报告中纳入的证据。新收集的证据不会自动纳入评测报告。

任务

- 向评测报告添加证据

- 从评测报告中移除证据
- 生成评测报告
- 接下来如何操作？

向评测报告添加证据

在生成评测报告之前，您必须至少向评测报告添加一份证据。您可添加整个证据文件夹，也可以从文件夹中添加单个证据项目。

向评测报告添加证据

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择 控件 选项卡，向下滚动至 控件集，然后选择控件的名称将其打开。
4. 选择您要向评测报告中添加证据的方式。
   a. 若要添加整个证据文件夹，请向下滚动至证据 文件夹，选择要添加的文件夹，然后选择 添加至评测报告。
      - 如果您看不到要查找的文件夹，请将下拉筛选条件更改为始终。否则，在默认情况下，您将看到最近七天的文件夹。
      - 如果 添加至评测报告 显示为灰色，则表示证据文件夹已添加至评测报告中。
   b. 若要添加特定证据，请选择一个证据文件夹以打开其内容。从列表中选择一个或多个项目，然后选择添加至评测报告。
      - 如果 添加至评测报告 显示为灰色，请确保选中了证据旁边的复选框，然后重试。
5. 将证据添加至评测报告后，会显示绿色的成功横幅。选择 在评测报告中查看证据以查看将纳入评测报告的证据。
   - 或者，您可以返回评测并选择 评测报告选择 选项卡，查看评测报告中将包含的证据。

从评测报告中移除证据

如果您需要从评测报告中移除证据，请按以下步骤操作。您可以删除整个证据文件夹，也可以从文件夹中删除特定的证据项目。

若要从评测报告中移除证据

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中选择评测，然后选择要打开的评测的名称。
3. 选择 控件 选项卡，向下滚动至 控件集，然后选择控件的名称将其打开。
4. 选择如何从评测报告中删除证据。

   a. 要删除整个证据文件夹，请向下滚动到 证据文件夹，选择要删除的文件夹，然后选择从评测报告中删除。

      - 如果您看不到要查找的文件夹，请将下拉筛选条件更改为始终。否则，在默认情况下，您将看到最近七天的文件夹。
      - 如果从评测报告中移除显示为灰色，则表明证据文件夹已从评测报告中删除。

   b. 要删除特定证据，请选择一个证据文件夹以打开其内容。从列表中选择一个或多个项目，然后选择从评测报告中删除。

      - 如果 从评测报告中删除显示为灰色，请确保选中了证据旁边的复选框，然后重试。

5. 将证据添加至评测报告后，会显示绿色的成功横幅。选择 在评测报告中查看证据以查看将纳入评测报告的证据。
   - 或者，您可以返回评测并选择 评测报告选择 选项卡，查看评测报告中将包含的证据。

生成评测报告

向评测报告添加证据后，您可以生成最终评测报告，以与审计师共享。生成评测报告时，它会被放入您作为评测报告目标的 S3 存储桶中。

> **Tip**
>
> 为确保您的评测报告成功生成，请查看我们的 评测报告目标的配置提示。

要生成评测报告

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择评测。
3. 选择要为其生成评测报告的评测名称。

4. 选择评测报告选择选项卡，然后选择 生成评测报告。
   - 如果 生成评测报告 显示为灰色，则表示尚未向评测报告中添加任何证据。
5. 在弹出窗口，提供评测报告的名称和描述，并查看评测报告的详细信息。
6. 选择 生成评测报告，等待几分钟，即可生成评测报告。
7. 从 Audit Manager 控制台下载中心页面查找并下载您的评测报告。
   - 或者，您可以前往评测报告目标 S3 存储桶，然后在此下载评测报告。

评测报告包含文件校验和，以确保评测报告的完整性。您可通过由 Audit Manager 提供ValidateAssessmentReportIntegrity API 操作进行验证。

接下来如何操作？

生成评测报告后，您可了解有关以下内容的更多信息：

- 查找并下载您的评测报告 — 了解如何从下载中心或 Amazon S3 下载您的评测报告。
- 浏览您的评测报告 — 了解如何导航评测报告并浏览其内容。
- 验证您的评测报告 — 了解如何使用 ValidateAssessmentReportIntegrity API 操作验证您的评测报告。
- 删除不必要评测报告 — 了解如何从下载中心或 Amazon S3 中 删除不需要的报告。

更改非活动评测状态

如果不再需要为评测收集证据，可以将评测状态更改为非活动。当评测的状态变为非活动时，评测将停止收集证据。因此，您不再需要为该评测支付任何费用。

除了停止收集证据外，Audit Manager 还对非活动评测中的控件执行了以下更改：

- 所有控件集都更改为 已审核 状态。
- 所有处于审核中 状态的控件都更改为 已审核 状态。
- 非活动评测的受托人无法再查看或编辑其控件和控件集。

> **Warning**
>
> 此操作不可逆。我们建议您谨慎行事，确保将评测标记为非活动状态。当评测处于非活动状态时，您对其内容具有只读访问权限。这意味着您仍然可以查看之前收集的证据并生成评测报告。但是，您无法编辑非活动评测、添加注释或上传任何手动证据。

Audit Manager console

将评测状态更改为非活动（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择评测。
3. 选择评测名称以打开。
4. 在页面右上角，选择更新评测状态，然后选择 非活动。
5. 在弹出窗口中选择 更新状态，以确认您要将状态更改为非活动状态。

评测及其控件的更改将在大约一分钟后生效。

AWS CLI

将评测状态更改为非活动（AWS CLI）

1. 首先确定要更新的评测。为此，请运行list-assessments命令。

   ```
   aws auditmanager list-assessments
   ```

   响应可返回评测列表。找到您将停用的评测，并记下评测编号。

2. 接下来，运行update-assessment-status 命令并指定以下参数：

   - `--assessment-id` — 使用此参数指定要停用的评测。
   - `--status` – 将该值设置为 `INACTIVE`。

   在以下示例中，将*#####*替换为您自己的信息。

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

评测及其控件的更改将在大约一分钟后生效。

Audit Manager API

将评测状态更改为非活动（API）

1. 使用 ListAssements操作查找要停用的评测，并记下评测 ID。
2. 使用UpdateAssessmentStatus操作并指定以下参数：
   - assessmentId - 使用此参数指定要停用的评测。
   - 状态 — 将此值设置为 INACTIVE。

评测及其控件的更改将在大约一分钟后生效。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

删除评测

您可以删除任何不再需要的 Audit Manager 评测。您可以使用 Audit Manager 控制台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 删除评测。

> **Warning**
>
> 此操作将永久删除评测及其收集的所有证据。您无法恢复此数据。因此，我们建议您谨慎行事，并且确定要删除评测。

Audit Manager console

删除评测报告（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择评测。
3. 选择要删除的评测，然后选择删除。
   - 或者，您可以打开评测，然后在页面的右上方选择删除。

AWS CLI

若要删除评测 (AWS CLI)

1. 首先，确定要删除的评测。为此，请运行list-assessments命令。

   ```
   aws auditmanager list-assessments
   ```

   响应可返回评测列表。找到您要删除的评测，并记下评测编号。
2. 接下来，运行 delete-assessment 命令并指定待删除评测的 `--assessment-id`。

   在以下示例中，将*#####*替换为您自己的信息：

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

Audit Manager API

删除评测（API）

1. 使用 ListAssessments 操作查找要删除的评测。

   在回复中记录评测 ID。
2. 使用 DeleteAssessment 操作，并指定要删除的评测的 assessmentId。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

> **Tip**
>
> 如果您的目标是降低成本，请考虑将评测状态更改为非活动，而不是将其删除。此操作会停止证据收集，并将评测置于只读状态，您可以在其中查看先前收集的证据。非活动评测不会产生任何费用。

AWS Audit Manager 中的委托

审计负责人使用 AWS Audit Manager，为该评测中列出的控件创建评测并收集证据。有时，审计负责人在验证控件集的证据时可能会有疑问或需要帮助。在这种情况下，审计负责人可以将控件集委托给主题专家进行审核。

概括来说，委托流程如下所述。

1. 审计负责人在其评测中选择一个控件集，并将其委托进行审核。
2. 受托人审核这些控件及其证据，并在完成后将控件集交还给审计负责人。
3. 审计负责人会收到审核已完成的通知，并检查已审核的控件中是否有受托人的任何备注。

使用本指南的以下章节，详细了解如何在 AWS Audit Manager 中管理委托任务。

主题

> **Note**
>
> 账户可以是不同 AWS 地区的审计负责人或委托人。

审计负责人的委托任务

作为 AWS Audit Manager 中的审计负责人，您可能需要主题专家的帮助，以帮助您审核控件和证据。在这种情况下，您可以委托控件集以进行审核。

以下主题说明了如何在 AWS Audit Manager 中管理委托。

委托任务

委托控件集以进行审核

当您需要主题专家的帮助时，可以选择想要帮助您的 AWS 账户，然后将控件集委托给其进行审核。

您可以使用下列任一过程委托控件集。

从评测页面委托控件集

从评测页面委托控件集

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择评测。
3. 选择包含您要委托的控件集的评测的名称。
4. 在评测页面中，选择控件选项卡。这将显示评测中的控件状态摘要和控件列表。
5. 选择一个控件集并选择委托控件集。
6. 在委托选择下，将显示用户和角色列表。选择用户或角色，或使用搜索栏进行查找。
7. 在委托详细信息下，查看控件集名称和评测名称。
8. （可选）在工作人员注释下，添加一条包含说明的评论，以帮助委托人完成审核任务。请勿在评论中包含任何敏感信息。
9. 选择委托控件集。
10. 绿色成功横幅确认控件集的成功委托。选择查看委托以查看委托请求。您也可以通过在 AWS Audit Manager 控制台的左侧导航窗格中选择委托，随时查看委托。

从委托页面委托控件集

从委托页面委托控件集

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择委托。
3. 从委托页面中，选择创建委托。
4. 在选择评测和控件集下，指定您要委托的评测和控件集。
5. 在委托选择下，您将看到用户和角色列表。选择用户或角色，或使用搜索栏进行查找。
6. （可选）在工作人员注释下，添加一条包含说明的评论，以帮助委托人完成审核任务。请勿在评论中包含任何敏感信息。
7. 选择创建委托。

8. 绿色成功横幅确认控件集的成功委托。选择查看委托以查看委托请求。您也可以通过在 AWS Audit Manager 控制台的左侧导航窗格中选择委托，随时查看委托。

当您委托控件集以进行审核时，受托人会收到通知，然后可以开始审核该控件集。委托人的委托任务中描述了受托人要遵循的流程。

> **Tip**
>
> 受托人可以订阅 SNS 主题，以便在向他们委托审核任务时接收电子邮件提醒。有关如何识别和订阅与 AWS Audit Manager 关联的 SNS 主题的更多信息，请参阅 AWS Audit Manager 中的通知。

访问处于活动状态的委托和已完成的委托

您也可以通过在 AWS Audit Manager 的左侧导航窗格中选择委托，随时访问您的委托列表。委托页面包含您处于活动状态的和已完成的委托列表，以及每个委托的以下详细信息：

- 受托人 — 您向其委托控件集的 AWS 账户。
- 日期 — 您委托控件集的日期。
- 状态 — 委托的当前状态。
- 评测 — 评测的名称，带有指向评测详细页面的链接。
- 控件集 — 委托进行审核的控件集的名称。

委托完成后，您将在 AWS Audit Manager 中收到通知。您还可能收到受托人的评论和备注。以下过程说明了如何在委托完成后在 Audit Manager 中查看您的通知，以及如何查看受托人可能留给您的任何评论。

查看已完成的委托并检查是否有评论

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择通知。或者，在屏幕顶部的蓝色闪存栏中选择通知，以打开通知页面。
3. 查看通知页面，其中包括一个含有以下信息的表格：
    - 日期 — 通知的日期。
    - 评测 — 与控件集关联的评测的名称。

- 控件集 — 控件集的名称。
- 来源 — 向您交回已完成的控件集的受托人的用户或角色。
- 描述 — 受托人提供的高级备注。

4. 找到受托人审核并提交给您的评测和控件集，然后选择评测名称将其打开。
5. 在评测详情页面的控制选项卡下，向下滚动至控件集表格。在按控件集分组的控件列下，展开控件集的名称以显示其控件。然后，选择控件名称以打开控件详细信息页面。
6. 选择评论选项卡可查看受托人为该特定控件添加的所有备注。
7. 如果您对控件集审核已完成感到满意，请选择该控件集并选择完成控件集审核。

> **Important**
>
> Audit Manager 持续收集证据。因此，在委托人完成对控件的审核后，可能会收集更多的新证据。
> 如果您只想在评测报告中使用经过审核的证据，则可以参考控件审核时间戳来确定何时审核证据。该时间戳可以在控件详细信息页面的更改日志选项卡上找到。然后，您可以使用该时间戳来确定您在评测报告中添加了哪些证据。

删除处于活动状态的和已完成的委托

在某些情况下，您可能创建了一个委托，但以后不再需要帮助来审核该控件集。出现这种情况时，您可以删除 AWS Audit Manager 中处于活动状态的委托。您还可以删除不再希望在委托页面上显示的已完成委托。

要删除委托

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择委托。
3. 在委托页面上，选择您要取消的委托，然后选择移除委托。
4. 在出现的弹出窗口中，选择删除以确认您的选择。

委托人的委托任务

委托人通常在几个不同领域拥有专业的业务或技术专长。这些专长可能包括数据留存政策、培训计划、网络基础设施和身份管理。他们可以帮助审计负责人审核收集到的控件证据，而这些属于其专长的范围。

作为受托人，您可能会收到审计负责人的请求，要求您审核与控件集相关的证据。此请求表明审计负责人需要您的帮助来验证这些证据。您可以通过以下方式帮助审计负责人：审核控件集及其相关证据、添加评论、上传其他证据，以及更新所审核的每个控件的状态。

以下主题说明了如何在 AWS Audit Manager 中管理委托。

> **Note**
>
> 审计负责人委托特定控件集进行审核，而非整体评测。因此，委托人的评测访问权限有限。委托人可以查看证据、添加评论、上传手动证据，以及更新控件集中每个控件的状态。有关 Audit Manager 中的角色及权限的更多信息，请参阅 中针对用户角色的推荐策略 AWS Audit Manager。

委托任务

- 查看您收到的委托请求的通知
- 审核委托的控件集及相关证据
- 向控件添加评论
- 将控件标记为已审核
- 将已审核的控件集交回给审计负责人

查看您收到的委托请求的通知

当审计负责人请求您协助审核控件集时，您会收到一条通知，告知您他们委托给您的控件集。

> **Tip**
>
> 您还可以订阅 SNS 主题，以便在控件集委托给您进行审核时接收电子邮件提醒。有关更多信息，请参阅 AWS Audit Manager 中的通知。

查看通知

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择通知。或者，在屏幕顶部的蓝色闪存栏中，选择查看通知以打开通知页面。
3. 在通知页面，查看已委托给您进行审核的控件集列表。该表包含以下信息：
   - 日期 — 委托控件集的日期。
   - 评测 — 与控件集关联的评测的名称。
   - 控件集 — 控件集的名称。
   - 来源 — 将控件集委托给您的用户或角色。
   - 描述 — 审计负责人提供的说明。

审核委托的控件集及相关证据

您可以通过审核审计负责人委托给您的控件集来帮助他们。您可以检查这些控件及其相关证据，以确定是否需要执行任何其他操作。此类其他操作可能包括手动上传额外证据以证明合规性，或者留下详细说明您所遵循的纠正步骤的评论。

要审核控件集

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择通知。或者，在蓝色闪存栏中，选择查看通知以打开通知页面。
3. 在通知页面，将显示委托给您的控件集列表。确定您要审核的控件集，然后选择相关评测的名称以打开评测详细信息页面。
4. 在评测详情页面的控制选项卡下，向下滚动至控件集表格。
5. 在按控件集分组的控件列下，展开控件集的名称以显示其控件，然后选择控件的名称以打开控件详细信息页面。
6. （可选）选择更新控件状态以更改控件的状态。审核进行期间，您可以将状态标记为正在审核。
7. 在证据文件夹、数据来源、评论和更改日志选项卡中查看有关控件的信息。有关每个选项卡、以及如何解释其中信息的更多信息，请参阅审核评测中的控件。

审核控件证据

1. 在控件详细信息页面，选择证据文件夹选项卡。

2. 导航至证据文件夹表格，其中将显示包含该控件的证据的文件夹列表。这些文件夹的整理和命名基于收集证据的日期。
3. 选择证据文件夹名称以将其打开。然后，查看在该日期收集的所有证据的摘要。此摘要包括直接从 AWS Security Hub、AWS Config 或两者兼而有之报告的合规性检查问题总数。有关如何解释此页面数据的说明，请参阅查看证据文件夹。
4. 在证据文件夹摘要页面，导航至证据表格。在时间列下，选择要打开的行项目。然后，审核当时收集的证据的详细信息。有关如何解释此页面数据的说明，请参阅查看单个证据。

> **Tip**
>
> 尽管 AWS Audit Manager 自动收集很多控件的证据，但有时您可能需要提供其他证据以确定合规性。在这些情况下，您可以手动上传证据。有关说明，请参阅上传手动证据。

向控件添加评论

您可以为所审核的任何控件添加评论。审计负责人可查看这些评论。

向控件添加评论

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择通知。或者，在屏幕顶部的蓝色闪存栏中，选择查看通知以打开通知页面。
3. 在通知页面，您可以查看已委托给您的控件集列表。找到包含要为其添加评论的控件的控件集，然后选择相关评测的名称。
4. 选择控件选项卡，向下滚动至控件集表格，然后选择控件的名称将其打开。
5. 选择评论选项卡。
6. 在发送评论下，在文本框中输入您的评论。
7. 选择提交评论以添加您的评论。然后，您的评论以及有关此控件的任何其他评论都显示在页面的之前的评论部分。

将控件标记为已审核

您可以通过更新控件集内各个控件的状态来指示您的审核进度。更改控件状态是可选的。但是，我们建议您在完成对每个控件的审核后，将该控件的状态更改为已审核。无论每个控件的状态如何，您仍然可以将控件交回给审计负责人。

将控件标记为已审核

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择通知。或者，在屏幕顶部的蓝色闪存栏中，选择查看通知以打开通知页面。
3. 在通知页面，您可以查看已委托给您的控件集列表。找到您要将其标记为已审核的控件集，然后选择相关评测名称。
4. 在评测详情页面的控制选项卡下，向下滚动至控件集表格。
5. 在按控件集分组的控件列下，展开控件集的名称以显示其控件。选择控件的名称，以打开控件详细信息页面。
6. 选择更新控制状态，然后将状态更改为已审核。
7. 在出现的弹出窗口中，选择更新控件状态以确认您已完成对控件的审核。

将已审核的控件集交回给审计负责人

审核完委托给您的控件后，将控件集提交给审计负责人。委托过程到此结束。

将已审核的控件集交回给审计负责人

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择通知。
3. 查看已委托给您的控件集列表。找到要提交回审计负责人的控件集，然后选择相关评测的名称。
4. 向下滚动至控件集表格，选择您要提交给审计负责人的控件集，然后选择提交以供审核。
5. 在显示的弹出窗口中，您可以添加评论，然后选择提交以供审核。将控件提交给审计负责人后，审计负责人可以查看您留给他们的任何评论。

评测报告

评测报告汇总了为评测收集的选定证据。它还包含指向 PDF 文件的链接，其中包含有关每份证据的详细信息。评测报告的具体内容、组织和命名惯例取决于您在生成报告时选择的参数。

评测报告可帮助您选择和汇编与审计相关的证据。但是，它不评测证据本身的合规性。相反，Audit Manager 只是将选定的证据详细信息作为输出提供给审计员。

评测报告文件夹结构

下载评测报告时，Audit Manager 会生成一个 zip 文件夹。它包含嵌套子文件夹中的评测报告和相关证据文件。

zip 文件夹的结构如下：

- 评测文件夹（例如：myAssessmentName-a1b2c3d4）— 根文件夹。
  - 评测报告文件夹（例如：reportName-a1b2c3d4e5f6g7）— 一个子文件夹，您可以在其中找到 AssessmentReportSummary.pdf、digest.txt 和 README.txt 文件。
    - 按控件分类的证据文件夹（例如：controlName-a1b2c3d4e5f6g）— 按相关控件对证据文件进行分组的子文件夹。
      - 按数据来源分类的证据文件夹（例如：CloudTrail、Security Hub）— 按数据来源类型对证据文件进行分组的子文件夹。
        - 按日期列出的证据文件夹（例如：2022-07-01）— 按证据收集日期对证据文件进行分组的子文件夹。
          - 证据文件 — 包含有关单个证据的详细信息的文件。

如何浏览评测报告

首先打开 zip 文件夹，然后向下导航到评测报告文件夹。在这里，您可以找到评测报告 PDF 和 README.txt 文件。

您可以查看 README.txt 文件以了解 zip 文件夹的结构和内容。它还提供了有关每个文件的命名约定的参考信息。如果您要查找特定项目，此信息可以帮助您直接导航到子文件夹或证据文件。

否则，要浏览证据并找到所需的信息，请打开评测报告 PDF。这可为您提供有关报告的概要信息以及创建报告所依据的评测摘要。

接下来，使用目录 (TOC) 浏览报告。您可以选择目录中的任何超链接控件直接跳转到该控件的摘要。

当您准备好查看控件的证据细节时，可以通过选择超链接的证据名称来进行。对于自动证据，超链接会打开一个新的 PDF 文件，其中包含有关该证据的详细信息。对于手动证据，超链接会将您带到包含证据的 S3 存储桶。

> **Tip**
>
> 当您浏览控件和证据时，每页顶部的页面导览痕迹导航会显示您在评测报告中的当前位置。选择超链接的目录可随时导航回目录。

评测报告章节

使用以下信息了解有关评测报告各章节的更多信息。

> **Note**
>
> 当您在以下章节中的任何属性旁边看到连字符 (-) 时，这表示该属性的值为空或值不存在。

- 封面页
- 概述页面
- 目录页面
- 控件页面
- 证据摘要页面
- 证据详细信息页面

封面页

封面包含评测报告的名称。它还会显示报告的生成日期和时间，以及生成报告的用户的账户 ID。

封面格式如下。Audit Manager 将*###*替换为与您的报告相关的信息。

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

概述页面

概述页面分为两部分：报告本身的摘要和正在报告的评测的摘要。

报告摘要

本节概要介绍了评测报告。

- 报告名称 — 报告的名称。
- 描述 — 审计负责人在生成报告时输入的描述。
- 生成日期 — 生成报告的日期。时间以世界标准时间 (UTC) 格式表示。
- 包括的控件总数 — 报告中包含并已收集证据的控件数量。这是评测中控件总数的一部分。
- 包括的 AWS 账户 — 报告中包含并已收集证据的 AWS 账户 数量。这是评测中 AWS 账户 总数的一部分。
- 评测报告选择 — 选择纳入报告的证据项目数量。这包括在报告中发现的合规性检查问题总数。

评测摘要

本节概述了报告所涉及的评测。

- 评测名称 — 生成报告所依据的评测的名称。
- 状态 — 生成报告时的评测状态。
- 评测区域 — 创建评测所在的 AWS 区域。
- 范围内的 AWS 账户 — 包含在评测范围内的 AWS 账户 的完整列表。
- 范围内的 AWS 服务 — 包含在评测范围内的 AWS 服务 的完整列表。
- 框架名称 — 创建评测所依据的框架的名称。
- 审计负责人 — 评测的审计负责人的用户或角色。
- 上次更新时间 — 上次更新评测的日期。时间以 UTC 格式表示。

目录页面

目录显示评测报告的全部内容。根据评测中包含的控件集对内容进行分组和组织。控件列在各自的控件集之下。

选择目录中的任何一项即可直接导航到报告中的该章节。您可以选择控件集，也可以直接进入控件。

控件页面

控件页面分为两部分：控件本身的摘要和为控件收集的证据的摘要。

控件摘要

本节包含以下信息。

- 控件名称 — 控件的名称。
- 描述 — 控件的描述。
- 控件集 — 控件所属的控件集的名称。
- 测试信息 — 此控件的推荐测试程序。
- 行动计划 — 如果控件未正常运行，建议采取的行动。
- 评测报告选择 — 评测报告中包含的与该控件相关的证据项目的数量。这包括在该控件的证据中发现的合规性检查问题的数量。

收集的证据

本节显示了为控件收集的证据。证据按文件夹分组，文件夹按证据收集日期进行整理和命名。每个证据文件夹名称旁边是该文件夹的合规性检查问题总数。

每个证据文件夹名称下方都有一个超链接的证据名称列表。

- 自动证据名称以证据收集时间戳开头，后面是服务代码、事件名称（最多 20 个字符）、账户 ID 和一个由 12 个字符组成的 唯一 ID。

  例如：`21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  对于自动证据，超链接的名称会打开一个包含摘要和更多详细信息的新 PDF 文件。
- 手动证据名称以证据上传时间戳开头，然后是 `manual` 标签、账户 ID 和一个由 12 个字符组成的唯一 ID。它还包括文件名的前 10 个字符和文件扩展名（最多 10 个字符）。

  例如：`00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  对于手动证据，超链接的名称会将您带到包含该证据的 S3 存储桶。

每个证据名称旁边都是该姓名的合规性检查结果。

- 对于从 AWS Security Hub 或 AWS Config 收集的自动证据，将报告合规、不合规或不确定的结果。
- 对于从 AWS CloudTrail 和 API 调用中收集的自动证据，以及所有手动证据，都会显示不确定的结果。

证据摘要页面

证据摘要页面包含以下信息：

- ID — 证据的唯一标识符。
- 收集日期 — 创建或上传证据的日期。
- 描述 — 对证据的描述，包括账户 ID 和数据来源类型。
- 评测名称 — 生成报告所依据的评测的名称。
- 框架名称 — 创建评测所依据的框架的名称。
- 控件名称 — 证据支持的控件的名称。
- 控件集名称 — 相关控件所属的控件集的名称。
- 控件描述 — 对证据支持的控件的描述。
- 测试信息 — 为此控件推荐的测试程序。
- 行动计划 — 如果控件未正常运行，建议采取的行动。
- AWS 区域 — 与证据关联的区域的名称。
- IAM ID — 与证据关联的用户或角色的 ARN。
- AWS 账户 — 与证据关联的 AWS 账户 ID。
- AWS 服务 — 与证据关联的 AWS 服务 的名称。
- 包括的资源 — 为生成证据而评测的 AWS 资源。此属性不适用于来自 AWS Config 的合规性检查证据。对于这种证据类型，您可以在证据 PDF 的 证据详细信息页面 中找到表格所列的所有资源。
- 事件名称 — 证据事件的名称。
- 事件时间 — 发生证据事件时的时间戳。
- 数据来源 — 收集或上传证据的地方。数据来源类型可以是 AWS Config、Security Hub 、AWS API 调用、CloudTrail 或手动。
- 按类型划分的证据 — 证据的类别
  - 合规性检查证据是从 AWS Config 或 Security Hub 收集的。
  - 用户活动证据是从 CloudTrail 日志中收集的。
  - 配置数据证据是从其他 AWS 服务 的快照中收集的。

  - 手动证据是您手动上传的证据。
- 合规性检查状态 — 属于合规性检查类别的证据的评测状态。
  - 对于从 AWS Security Hub 或 AWS Config 收集的自动证据，将报告合规、不合规或不确定的结果。
  - 对于从 AWS CloudTrail 和 API 调用中收集的自动证据，以及所有手动证据，都会显示不确定的结果。

证据详细信息页面

证据详细信息页面显示证据名称和证据详细信息表。此表提供了每个证据要素的详细细分，以便您可以理解数据并验证其正确性。根据证据的数据来源，证据详细信息页面的内容会有所不同。

> **Tip**
>
> 当您浏览证据详细信息时，每页顶部的页面导览痕迹导航会显示您的当前位置。选择证据摘要，可随时导航回证据摘要。

评测报告完整性检查

生成评测报告时，Audit Manager 会生成一个名为 `digest.txt` 的校验和报告文件。您可以使用此文件来验证报告的完整性，并确保在报告创建后没有修改任何证据。它包含一个带有签名和哈希的 JSON 对象，如果报告存档的任何部分被更改，则这些签名和哈希值将失效。

要验证评测报告的完整性，请使用 Audit Manager 提供的 ValidateAssessmentReportIntegrity API。

评测报告疑难解答

要查找常见问题和答案，请参阅本指南疑难解答部分中的解决评测报告问题。

证据查找器

证据查找器提供了一种在 Audit Manager 中搜索证据的强大功能。现在，您可以使用证据查找器快速查询证据，而不必通过浏览嵌套程度很高的证据文件夹来查找所需内容。如果您以委派管理员的身份使用证据查找器，则可以在组织中的所有成员帐户中搜索证据。

使用筛选条件和分组的组合，可以逐步缩小搜索查询的范围。例如，如果您想从高层次查看系统运行状况，请进行广泛搜索并按评测、日期范围以及资源合规性进行筛选。如果您的目标是修复特定资源，则可以执行狭窄搜索，以瞄准特定控件或资源 ID 的证据。定义筛选条件后，您可分组并预览匹配的搜索结果，然后再创建评测报告。

若要使用证据查找器，必须从 Audit Manager 设置中启用此功能。

主题

了解证据查找器如何与 CloudTrail Lake 配合使用

证据查找器使用 AWS CloudTrailLake 的查询和存储功能。开始使用证据查找器之前，进一步了解 CloudTrail Lake 的工作原理会很有帮助。

CloudTrail Lake 将数据聚合至单个可搜索的事件数据存储中，该存储支持强大的 SQL 查询。这意味着您可在组织中搜索自定义时间范围内的数据。您可借助证据查找器，直接在 Audit Manager 控制台中使用此搜索功能。

当您请求启用证据查找器，Audit Manager 会代表您创建事件数据存储。启用证据查找器后，所有未来的 Audit Manager 证据都将导入事件数据存储中，供证据查找器搜索查询。启用证据查找器后，我们还会通过您过去两年的证据数据回填新创建的事件数据存储库。如果您以委派管理员的身份使用证据查找器，我们会回填您组织中所有成员账户的数据。

您的所有证据数据，无论是回填的还是新证据，都将在事件数据存储中保留 2 年。您可以随时更改默认留存期。有关说明信息，请参阅AWS CloudTrail 用户指南中的更新事件数据存储。您可以在事件数据存储中保存事件数据长达七年，即2555天。

> **Note**
>
> 启用此功能后，如果在 2023 年 11 月之前完成，则将免费执行数据回填进程。
> 今后向事件数据存储中添加新证据数据时，CloudTrail Lake 会产生数据存储和提取费用。
> 对于 CloudTrail Lake 查询，需要按实际使用量付费。这意味着，对于您在证据查找器中运行的每项搜索查询，您都需要为扫描的数据付费。
> 有关 CloudTrail Lake 定价的更多信息，请参阅：AWS CloudTrail 定价。

启用证据查找器

您可以从 Audit Manager 设置中启用证据查找器。有关说明，请参阅本指南 AWS Audit Manager设置页面上的证据查找器。

证据查找器疑难解答

若要查找常见问题和答案，请参阅本指南疑难解答章节中的证据查找器疑难解答问题。

搜索证据

按以下步骤在 Audit Manager 控制台中搜索证据。

> **Note**
>
> 您还可使用 CloudTrail API 查询您的证据数据。有关更多信息，请参阅 AWS CloudTrail API 参考中的 StartQuery。如果您偏好使用 AWS CLI，请参阅AWS CloudTrail 用户指南中的开始查询。

本页内容

执行搜索查询

按以下步骤在证据查找器中执行搜索查询。

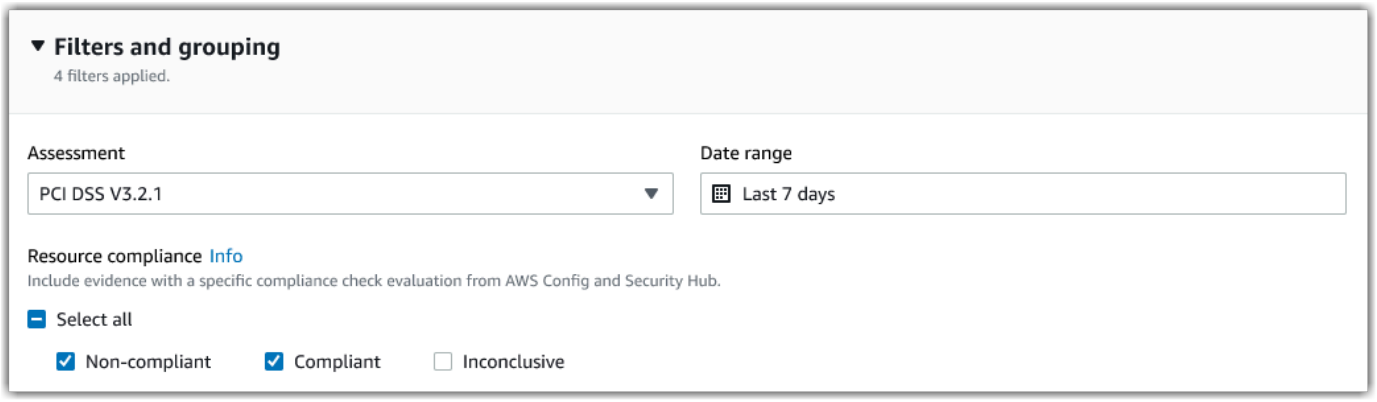
若要搜索证据

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择证据查找器。
3. 接下来，应用筛选条件以缩小搜索范围。

   a. 对于评测，请选择一项评测。

   b. 对于日期范围，选择一个范围。

   c. 对于资源合规性，请选择评测状态。

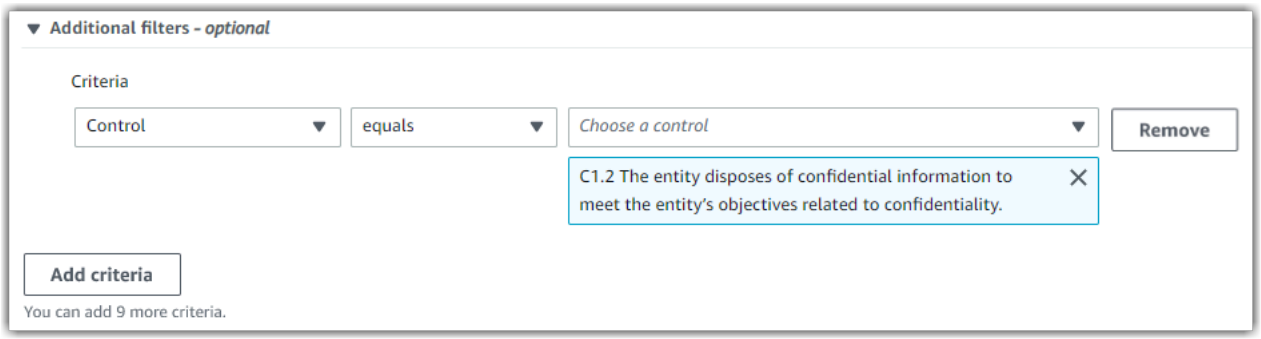


4. （可选）选择 其他筛选条件（可选）以进一步缩小搜索范围。

   a. 选择 添加标准，选择一项标准，然后为该标准选择一个或多个值。

   b. 继续按同样的方式构建更多筛选条件。

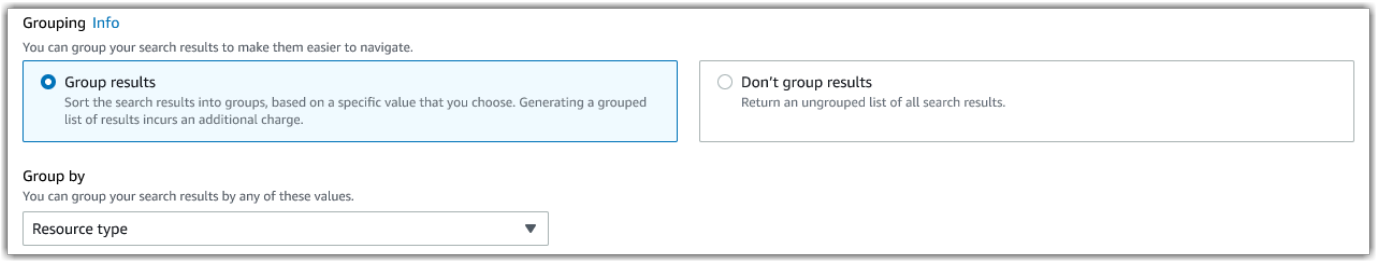
   c. 若要移除不需要的筛选条件，请选择 移除。



5. 在分组下，指定是否要对搜索结果进行分组。

   a. 如果要对结果分组，请选择一个值作为此结果分组依据。

   b. 如果不想对结果分组，请继续执行第 6 步。



6. 选择搜索。

您的搜索可能需要几分钟，具体取决于您的证据数据量。在搜索过程中，您可随意离开证据查找器。搜索结果准备就绪时，您会获得闪光栏通知。

> **Tip**
>
> 有关可以在此过程中使用的筛选条件和分组的更多信息，请参阅筛选和分组选项。

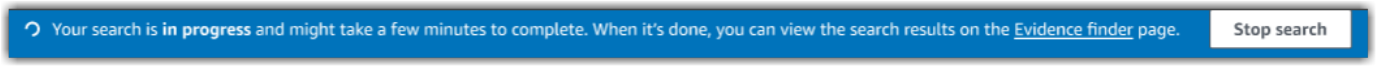
停止搜索查询

如果出于任何原因要停止搜索查询，请按下列步骤操作。

> **Note**
>
> 停止搜索查询，仍会产生费用。对于停止搜索查询之前扫描的证据数据量，您需要支付费用。停止后，您可查看返回的部分结果。

若要停止正在进行的搜索查询

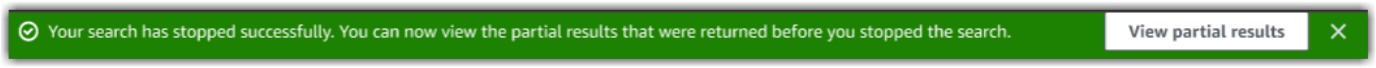
1. 在屏幕顶部的蓝色进度闪烁栏中，选择 停止搜索。



2. （可选）查看在停止搜索查询前返回的部分结果。

   a. 如果您在证据查找器页面，则屏幕上会显示部分结果。

   b. 如果您离开了证据查找器，请在绿色确认闪光栏中选择 查看部分结果。



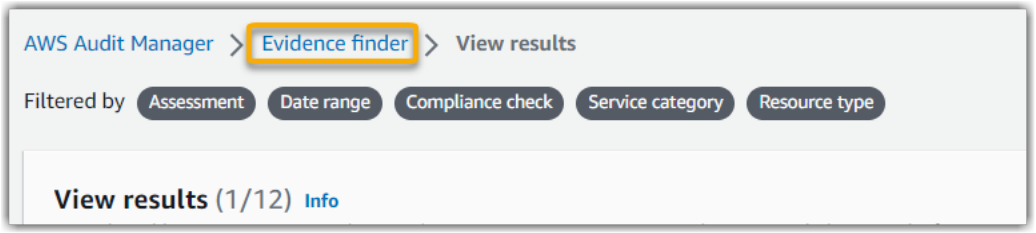
编辑搜索筛选条件

您可以返回至最近的搜索查询，并根据需要更改筛选条件。

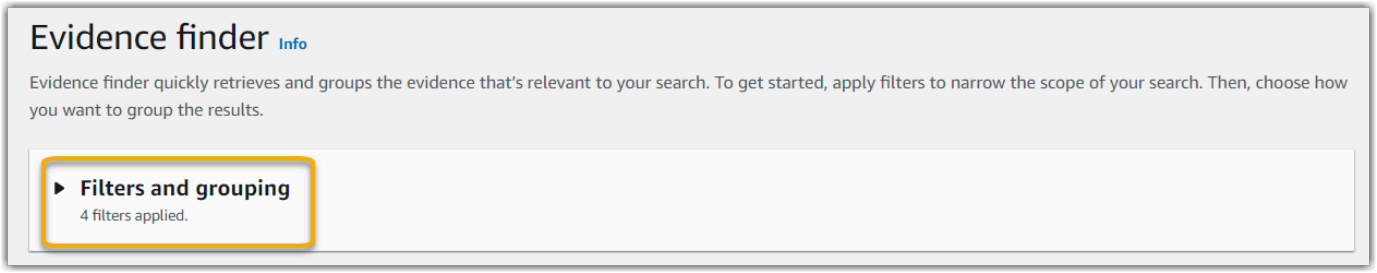
> **Note**
>
> 当您编辑筛选条件并选择 搜索 时，将启动一个新的搜索查询。

若要编辑最近的搜索查询

1. 在 查看结果 页面，从页面导览痕迹导航菜单中选择 证据查找器。



2. 选择 筛选条件和分组 以展开筛选条件选择。



3. 接下来，编辑您的筛选条件或开始新搜索。

a. 要编辑筛选条件，请调整或移除当前的筛选条件和分组选择。

b. 要重新开始，请选择 清除筛选条件，然后应用您选择的筛选条件和分组选项。

4. 完成此操作后，选择搜索。

查看证据查找器中的结果

搜索完成后，您可查看符合搜索条件的结果。

请记住，在收集证据期间，可能需要评测多种资源。因此，证据中可能包含一个或多个相关资源。在证据查找器中，结果以资源级别显示，每种资源对应一行。您无需离开页面即可预览每种资源摘要。

查看搜索结果后，您可生成包含该证据的评测报告。您可以将资源搜索查询结果导出为逗号分隔值（.csv）文件。

> **Important**
>
> 浏览完搜索结果之前，我们建议您保持证据查找器处于打开状态。当您离开查看结果表格时，您的搜索结果将被丢弃。如有必要，您可在https://console.aws.amazon.com/cloudtrail/的 CloudTrail 控制台中查看近期结果。在此，您的搜索查询结果可保留七天。但是，切记，您无法在 CloudTrail 控制台中根据搜索结果生成评测报告。

本页内容

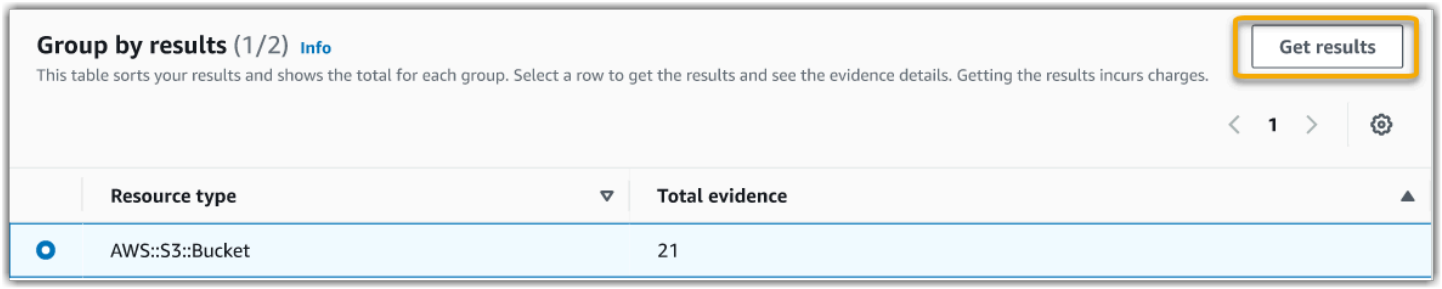
- 导出您的搜索结果

查看分组结果

如果您对结果进行了分组，则可以在更深入地研究证据前查看分组。

> **Note**
>
> 如果您没有对结果分组，则证据查找器不会显示 按结果分组表。相反，您看到直接进入查看结果表。

使用按结果分组表了解匹配证据的广度，及其在特定维度的分布情况。结果按您选定的值分组。例如，如果您按资源类型分组，则该表将显示 AWS资源类型列表。证据总数列显示每种资源类型的匹配结果数。



若要获取分组结果

1. 从 按结果分组 表中，选择要获得的结果所在的行。
2. 选择获取结果。启动一项新搜索查询，并将您重定向至查看结果表，您可以在其中查看该组的结果。

查看搜索结果

查看结果 表显示您的搜索结果。在控制面板中，您可以执行以下操作：

- 管理查看首选项
- 预览资源摘要
- 根据您的搜索结果生成评测报告
- 导出您的搜索结果

管理查看首选项

您的查看首选项控制您在结果页面看到的内容。

若要管理您的观看首选项

1. 在查看结果表顶部选择设置图标 (#)。
2. 按需要查看和更改以下设置：
   a. 选择可见表格列 — 使用切换选项更改所示列。
   b. 页面大小 — 选择一个单选按钮，以指定每页显示的结果数量。
   c. 换行文本 — 选中此复选框，可将长行文本换行以提高可读性。
3. 选择确认以保存首选项。

预览资源摘要

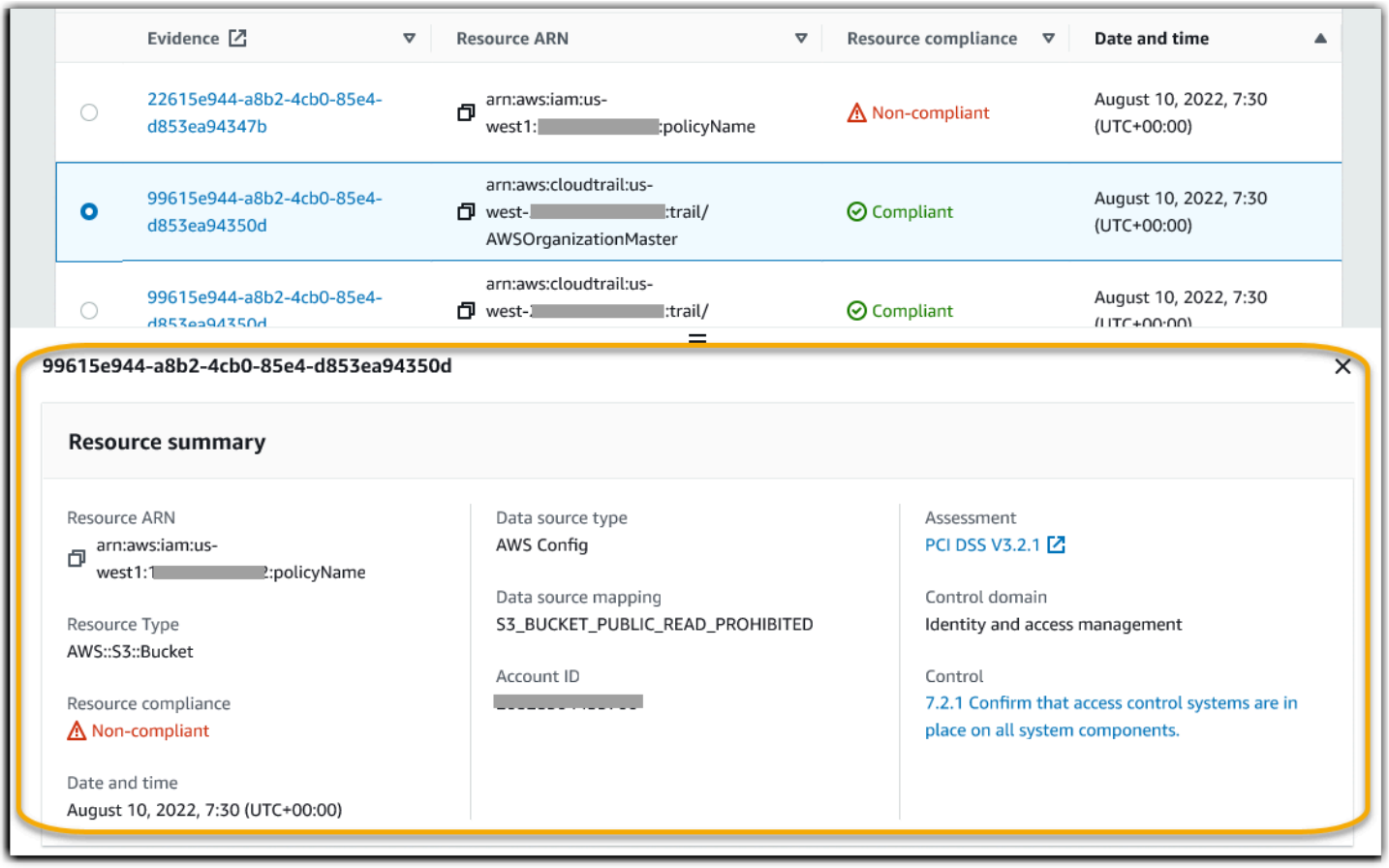
您可以预览与您的搜索查询匹配的证据的相关资源。这可以帮助您确定搜索查询是否返回了预期结果，或者您是否需要调整筛选条件和重新运行搜索查询。

切记，证据可能包含一个或多个相关资源。在证据查找器中，结果以资源级别显示，每种资源对应一行。

> **Note**
>
> 证据查找器返回自动和手动证据结果。但是，您只能预览自动证据资源摘要。原因是 Audit Manager 不对手动证据进行资源评测，因此没有可用的资源摘要。
> 若要查看有关人工证据的详细信息，请选择证据名称以打开证据详细信息页面。如果您根据证据搜索结果生成评测报告，则评测报告中将纳入手动证据详细信息。

预览资源摘要

1. 选中结果旁的单选按钮。打开当前页面上的资源摘要面板。
2. （可选）若要查看相关证据的完整详细信息，请选择证据名称。
3. （可选）使用水平线 (=) 拖动资源摘要窗格，并调整其大小。
4. 选择 (x) 以关闭资源摘要窗格。



根据您的搜索结果生成评测报告

对搜索结果感到满意后，可生成评测报告。

根据您的搜索结果生成评测报告

1. 在查看结果 表顶部，选择生成评测报告。
2. 输入评测报告的名称与描述，然后查看评测报告的详细信息。
3. 选择生成评测报告。

评测报告的生成需要几分钟时间。发生这种情况时，您可以离开证据查找器，绿色成功通知将确认报告准备就绪的时间。然后，您可以前往 Audit Manager 下载中心下载您的评测报告。

> **Note**
>
> Audit Manager 仅通过搜索结果中的证据生成一次性报告。该报告不包括从评测页面手动添加至报告的任何证据。

评测报告中包含的证据数量有一定限制。更多信息，请参阅故障排除证据查找器。

导出您的搜索结果

对于证据查找器搜索结果，您可能需要可移植版本。在这种情况下，您可以将搜索结果导出为 CSV 格式文件。

导出搜索结果后，CSV 文件可在 Audit Manager 下载中心保留七天，以供下载。CSV 文件的副本还会传送至您的首选 S3 存储桶，即所谓的导出目标。您的 CSV 文件在此存储桶中仍可用，直至您删除该文件。

Audit Manager 使用 CloudTrail Lake功能，从证据查找器中导出和交付 CSV 文件。以下因素定义了 CSV 导出过程的运行原理：

- 您的所有搜索结果都包含在 CSV 格式文件中。如果您只想纳入特定搜索结果，我们建议您编辑搜索筛选条件。这样，您可以缩小结果范围，即仅针对要导出的证据。
- CSV 文件以压缩 GZIP 格式导出。默认 CSV 文件名为 `queryID/result.csv.gz`，其中 `queryID` 是您的搜索查询的 ID。
- 导出的最大 CSV 格式文件为 1 TB。如果您要导出超过 1 TB 的数据，则该结果将拆分为多个文件。每个 CSV 文件都以`result_`*`number`*`.csv.gz`命名。您获得的 CSV 文件数量，取决于搜索结果的总大小。例如，导出 2 TB 的数据会为您提供两个查询结果文件：即 `result_1.csv.gz` 和 `result_2.csv.gz`。
- 除了 CSV 文件外，您的 S3 存储桶还会收到 JSON 签名文件。该文件充当校验和，用于验证 CSV 文件中的信息是否准确。若要了解更多信息，请参阅AWS CloudTrail 开发人员指南中的CloudTrail 签名文件结构。要确定查询结果是否已被修改、删除或未经更改，您可以使用 CloudTrail 查询结果完整性验证。若要了解更多信息，请参阅AWS CloudTrail 开发人员指南中的验证已保存的查询结果。

> **Note**
>
> 目前，证据查找器预览或 CSV 导出中不包含手动证据文字回复。要查看文本响应数据，请在证据查找器结果中选择手动证据名称以打开证据详细信息页面。如果您需要在 Audit Manager 控制台之外查看文字回复数据，我们建议您根据证据查找器的结果生成评测报告。所有手动证据细节（包括文字答复）都包含在评测报告中。

首次导出结果

按以下步骤首次导出搜索结果。您可通过此程序选项，指定所有未来导出的默认导出目标。如果您现在不想保存默认导出目标，可以稍后通过更新导出目标设置进行保存。

> **Important**
>
> 在开始之前，请确保您有 S3 存储桶可用作导出目标。您可以使用现有的 S3 存储桶之一，也可以在 Amazon S3 中创建新存储桶。此外，您的 S3 存储桶必须具有所需权限策略，才能允许 CloudTrail 向其中写入导出文件。更具体地说，存储桶策略必须包括 `s3:PutObject` 操作和存储桶 ARN，并将 CloudTrail 列为服务主体。我们提供了一个权限策略示例以供您使用。有关如何将此策略附加至 S3 存储桶的说明，请参阅使用 Amazon S3 控制台添加存储桶策略。有关更多提示，请参阅 导出目标配置提示。如果您在导出 CSV 文件时遇到任何问题，请参阅证据查找器 CSV 导出疑难解答。

导出搜索结果（首次运行体验）

1. 在查看结果表顶部，选择导出 CSV。
2. 指定要将文件导出的目标 S3 存储桶。
   - 选择 浏览 S3，从您的存储桶列表中选择。
   - 或者，您可以输入以下格式的存储桶 URI：**`s3://bucketname/prefix`**

   > **Tip**
   >
   > 要使目标存储桶井井有条，您可以为 CSV 的导出创建一个可选文件夹。为此，请在 资源 URI 框中的值前后附加一个斜杠 (**`/`**) 和一个前缀（例如**`/evidenceFinderExports`**）。然后，Audit Manager 在将 CSV 文件添加至存储桶时会包含此前缀，而且 Amazon S3 会生成由该前缀指定的路径。有关 Amazon S3 前缀的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 控制台中的组织对象。
3. （可选）如果您不想将此存储桶保存为默认导出目标，请清除复选框 将此存储桶保存为证据查找器设置中的默认导出目标。
4. 选择 Export（导出）。

保存导出目标后导出您的结果

将默认 S3 存储桶保存为默认导出目标后，您可继续执行以下步骤。

若要导出搜索结果（在保存默认导出目标之后）

1. 在查看结果表顶部，选择导出 CSV。
2. 在出现的提示中，查看保存导出文件的默认 S3 存储桶。
   a. （可选）要继续使用此存储桶并继续隐藏此消息，请选中 不再提醒 复选框。
   b. （可选）若要更改此存储桶，请按步骤更新您的导出目标设置。
3. 选择 Confirm（确认）。

根据您要导出的数据量，导出过程可能需要几分钟完成。在导出过程中，您可随意离开证据查找器。当您离开证据查找器后，搜索将停止，搜索结果将被丢弃在控制台。但是，CSV 导出进程将在后台继续进行。CSV 文件将包含与您的查询匹配的完整搜索结果集。

导出结果后查看

要查找 CSV 文件并查看其状态，请前往 Audit Manager 下载中心。导出文件准备就绪后，您可以从下载中心下载 CSV 文件。

您也可从导出目标 S3 存储桶中查找和下载 CSV 文件。

若要在 Amazon S3 控制台中查找您的 CSV 文件和签名文件

1. 打开 Amazon S3 控制台。
2. 选择您在导出 CSV 文件时所指定的导出目标存储桶。
3. 在对象层次结构中导航，直至找到 CSV 文件和签名文件。CSV `.csv.gz`文件具有扩展名，符号`.json`文件具有扩展名。

您将看到一个与下面示例类似的对象层次结构，但具体存储桶名称、账户 ID、日期和查询 ID 有所不同。

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
```

```
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

筛选条件和组选项

本页介绍证据查找器中可用的筛选条件和分组选项。

本页内容

筛选条件参考

您可以使用以下筛选条件查找符合特定标准的证据，例如评测、对照或AWS 服务。

主题

必要筛选条件

使用这些筛选条件，开始对评测中的证据进行简要概述。

筛选条件名称	描述	注意
评测	返回特定评测证据。	您只能按一项评测筛选。
日期范围	返回特定时间段内的证据。	或者，您也可以使用相对范围定义相对于今天日期的范围（例如**`Last 30 days`**）。

筛选条件名称	描述	注意
		或者，您可以使用绝对范围 指定特定的日期范围（例如**`June 27th - July 4th`**）。
资源合规性	返回经特定合规性检查评测的资源。	Audit Manager 会为使用 AWS Config 并以 Security Hub 为数据来源的控件收集合规检查证据。在收集证据期间，可能需要评测多种资源。因此，一份合规性检查证据可包含一个或多个资源。您可以使用此筛选条件浏览资源级别的合规性状态。 您可以选择以下选项之一： • 不合规 - 该筛选条件可查找存在合规性检查问题的资源。如果 Security Hub 报告了资源的失败 结果，或者AWS Config报告了不合规结果，就会发生这种情况。 • 合规 — 此筛选条件可查找没有合规性检查问题的资源。如果 Security Hub 报告了资源的通过结果，或者AWS Config报告了合规结果，就会发生这种情况。 • 尚无定论 — 该筛选条件可以查找无法进行或不适用合规检查的资源。如果某一资源以 AWS Config 或 Security Hub 作为基础数据来源类型，但这些服务未启用，则会发生这种情况。如果资源使用的基础数据来源类型不支持合规性检查（例如手动证据、AWS API 调用或 CloudTrail），也会发生这种情况。

其他筛选条件（可选）

使用这些筛选条件缩小搜索查询范围。例如，使用服务查看与 Amazon S3 关联的所有证据。使用资源类型功能，可以仅关注 S3 存储桶。或者，使用资源 ARN 定位特定的 S3 存储桶。

您可使用以下条件创建其他筛选条件。

条件名称	描述	何时使用此条件
账户 ID	按AWS 账户向下钻取。	使用此条件查找与特定AWS 账户相关的证据。
控件	按控件名称向下钻取。	使用此条件查找与特定控件相关的证据。
控件域	按控件域向下钻取。	为审计做准备时，使用此标准将重点放在特定的主题领域。如果您要查询按标准框架创建的评测，则可以按控制域进行筛选。 控制域的示例包括身份和访问管理、日志记录和监控以及网络管理。
数据源类型	按数据来源类型向下钻取。	使用此条件将重点放在特定数据来源。 将该值设置为 `Manual`，以查找您手动上传的证据。否则，您可以根据自动证据的来源（例如AWS Config、CloudTrail 、Security Hub 或 AWS API calls）筛选自动证据。
事件名称	按事件名称向下钻取。	使用此条件，将重点放在与证据相关的特定事件。事件指的是 AWS 账户 中的某一活动的记录。 例如，您可以搜索 API 调用的名称，如用于配置权限的 IAM `AttachRolePolicy` 操作。或者搜索 CloudTrail 关键字，例如用户登录账户时 CloudTrail 记录的 `ConsoleLogin` 事件。
资源 ARN	按Amazon 资源名称（ARN）向下钻取。	使用此条件查找与特定 AWS 资源相关的证据。
资源类型	按资源类型向下钻取。	使用此条件，重点关注正在评测的资源类型，例如 Amazon EC2 实例或 S3 存储桶。
服务	按 AWS 服务 名称向下钻取。	使用此标准查找与特定 AWS 服务 内容相关的证据，例如 Amazon EC2、Amazon S3 或 AWS Config。
服务类别	按 AWS 服务 类别向下钻取。	使用此条件将重点放在特定的 AWS 服务 类别。

条件名称	描述	何时使用此条件
		示例包括安全性、身份和合规性、数据库以及存储。

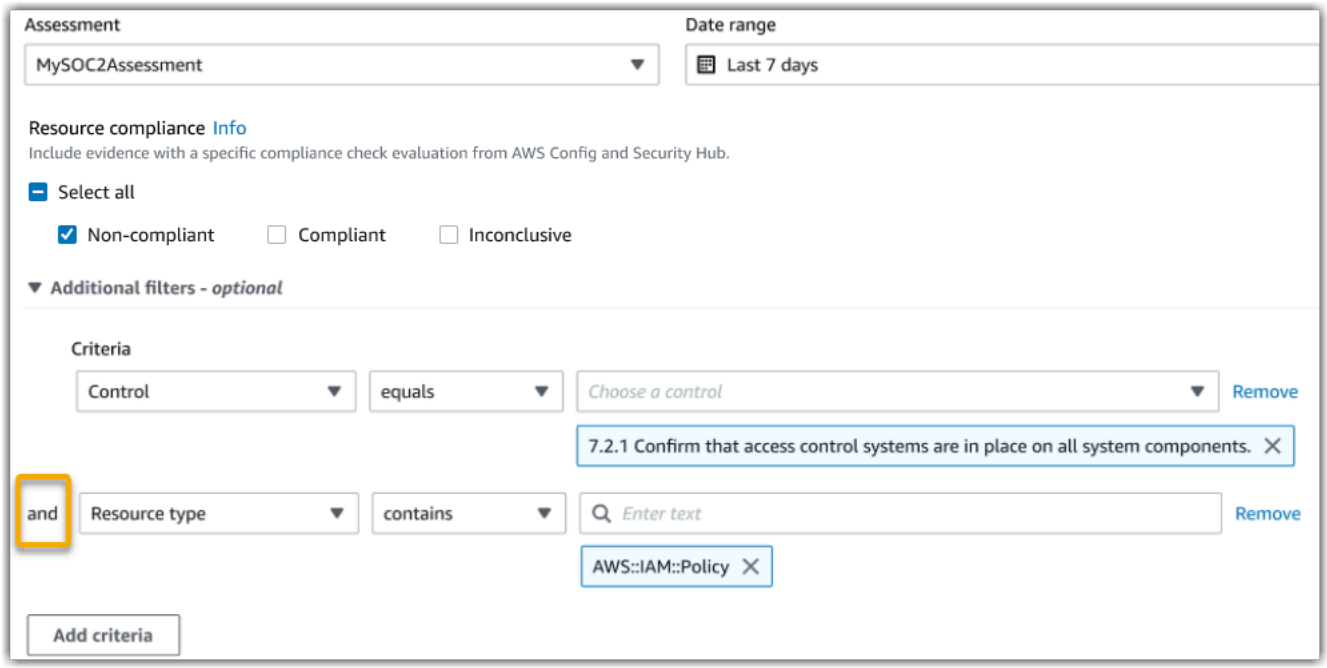
组合筛选条件

条件行为

指定多个条件时，Audit Manager 会针对您的选择应用 AND 运算符。这意味着所有条件都被分组至同一查询中，并且结果必须与所有组合条件相匹配。

示例

在以下筛选条件设置中，证据查找器返回过去 7 天内调用的**MySOC2Assessment**不合规评测资源。此外，结果与 IAM policy 以及指定控件有关。

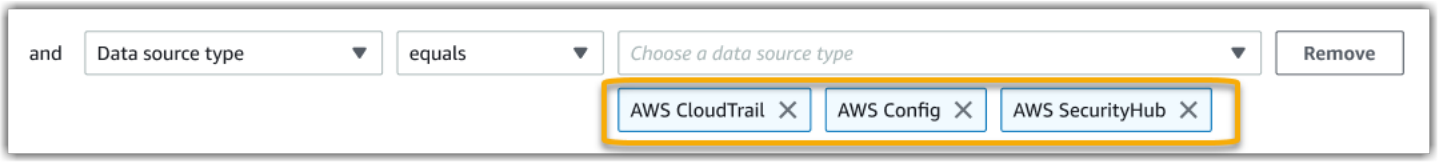


条件值行为

当您指定多个条件值时，这些值将与 OR 运算符相关联。证据查找器返回与这些条件值中的任何一个都匹配的结果。

示例

在以下筛选条件设置中，证据查找器返回来自AWS CloudTrail、AWS Config或 AWS Security Hub的搜索结果。



分组引用

您可以对搜索结果进行分组，以更快导航。分组显示搜索结果的广度，及其在特定维度上的分布情况。

您可使用以下任意分组值。

Group by (分组依据)	描述
账户 ID	按AWS 账户对结果分组。
控件	按控件名称对结果分组。
控件域	按控件域对结果分组。
数据源类型	按证据来源的数据来源类型对结果分组。
事件名称	按事件名称对结果分组。
资源 ARN	按Amazon 资源名称（ARN）对结果分组。
资源类型	按资源类型对结果分组。
服务	按 AWS 服务 名称对结果分组。
服务类别	按AWS 服务类别对结果分组。

使用案例示例

证据查找器可以帮助您解决多个用例问题。本页提供了一些示例，并建议了您可以在每种情况下使用的搜索筛选条件。

主题

- 用例 1：查找不合规的证据并组织委派
- 用例 2：识别合规证据

用例 1：查找不合规的证据并组织委派

如果您是监管审计准备工作的合规官、数据保护官员或 GRC 专业人员，则此用例非常理想。

在监控组织的合规状况时，您可依靠合作伙伴团队帮助您修复问题。您可以使用证据查找器，帮助您为合作伙伴团队组织工作。

通过应用筛选条件，您可以每次专注于一个区域的证据。此外，您还可以与您合作的每个伙伴团队的职责和范围保持一致。通过以这种方式执行有针对性搜索，您可以使用搜索结果确定每个学科领域中需要补救的内容。然后，您可以将不合规的证据委托至相应的合作伙伴团队，以进行补救。

对于此工作流程，请按此步骤 搜索证据。使用以下筛选条件查找不合规证据。

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

下一步，为你关注的区域应用其他筛选条件。例如，使用服务类别筛选条件，查找与 IAM 相关的不合规资源。然后，与为您的组织中拥有 IAM 资源的团队共享这些结果。或者，如果您要查询按标准框架创建的评测，则可以使用控件域 筛选条件查找与身份和访问管理域相关的不合规证据。

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS ## category that you're focusing on>
```

找到所需的证据后，请按步骤从搜索结果中生成评测报告。您可与合作伙伴团队共享此报告，他们可以将其用作补救清单。

用例 2：识别合规证据

如果您在 SecOps、IT/DevOps 或其他拥有和修复云资产的部门工作，则此用例非常理想。

在审计过程中，可能会要求您修复自己所拥有的资源的问题。完成此项工作后，您可以使用证据查找器验证资源是否合规。

对于此工作流程，请按此步骤 搜索证据。使用以下筛选条件查找合规证据。

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

接下来，应用其他筛选条件，以仅显示您应负责的证据。根据您的所有权范围，按需要进行有针对性的搜索。以下筛选条件示例按从最宽到最精确的顺序排列。为您选择合适的选项，然后用您自己的值替换*<placeholder text>*。

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS ## that you own>
Service | <a specific AWS ## that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

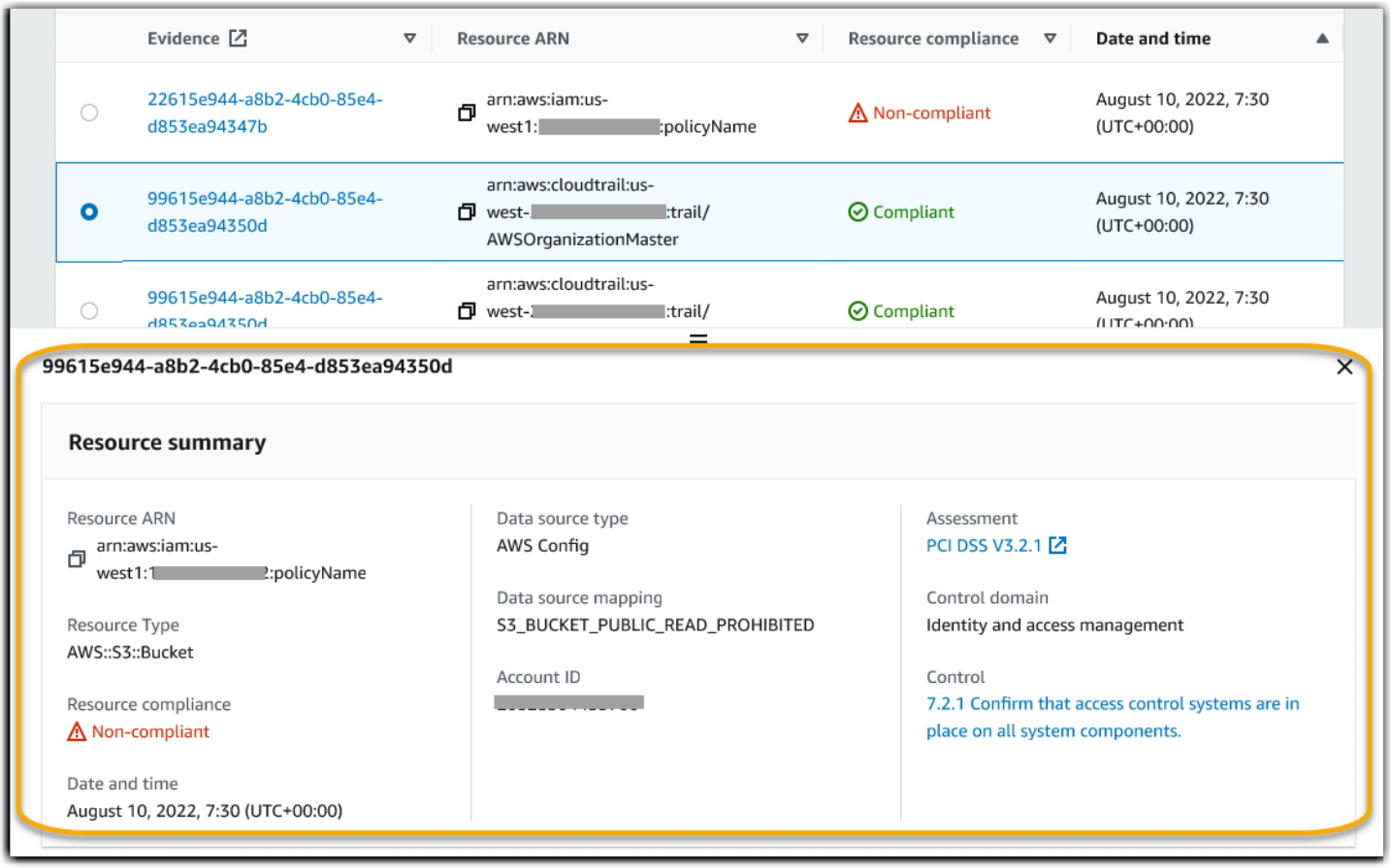
如果您负责同一标准的多个实例（例如，您拥有多个AWS 服务），则可以按该值对结果分组。这为您提供了每种AWS 服务的全部匹配结果。然后，您可以获得自己的服务结果。

用例 3：快速预览证据资源

此用例非常适合所有 Audit Manager 客户。

以前，审查个人证据细节非常耗时。如果您想预览证据，你必须直接进入评测，然后浏览深度嵌套的证据文件夹。现在，证据查找器提供了一种便捷的方式预览这些信息。对于与您的搜索查询相匹配的每个证据项目，您可预览该证据的各个资源。

首先，请按步骤 搜索证据。然后，选中结果旁边的单选按钮，查看当前页面的资源摘要。您可以预览与证据项目相关的每项单独资源。要查看任何资源的完整证据的详细信息，请选择证据名称。有关更多信息，请参阅 预览资源摘要。


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Audit Manager 下载中心

您可以在下载中心查找和管理所有可下载的 Audit Manager 文件。当您生成评测报告或从证据查找器导出搜索结果时，文件会显示在下载中心中。

主题

浏览下载中心

要访问下载中心，请在 https://console.aws.amazon.com/auditmanager/home 处打开 Audit Manager 控制台，然后在左侧导航窗格中选择下载中心。

您可以在以下选项卡之间切换，按类别浏览文件。

“评测报告”选项卡

此选项卡显示您生成的所有评测报告。评测报告将在下载中心保存，直到您将其删除。

要查看评测报告的最新状态，请选择刷新图标 (#) 以重新加载表格。评测报告表中的每一行都显示报告的名称、其创建日期以及以下状态之一：

- 进行中 — Audit Manager 正在生成评测报告。
- 准备就绪 — 评测报告可供您下载。
- 错误 — 无法生成评测报告。在这种情况下，Audit Manager 会显示一条描述错误的消息。有关如何解决这些错误的信息，请参阅评测报告疑难解答。

“导出”选项卡

此选项卡显示您在过去七天内导出的所有证据查找器搜索结果。CSV 文件将在七天后从下载中心移除，但它们仍保存在您的导出目标 S3 存储桶中。有关如何在 S3 目标存储桶中查找证据查找器 CSV 导出的说明，请参阅 导出结果后查看。

要查看 CSV 导出的最新状态，请选择刷新图标 (#) 以重新加载表格。导出表中的每一行都显示文件名、其导出日期和以下状态之一：

- 进行中 — Audit Manager 正在准备 CSV 文件。
- 准备就绪 — 导出成功，文件可供您下载。

- 错误 — 导出失败。在这种情况下，Audit Manager 会显示一条描述错误的消息。有关如何解决这些错误的信息，请参阅解决证据查找器 CSV 导出问题。

> **Note**
>
> 请记住，“导出”选项卡还可能显示您直接在 AWS CloudTrail Lake 中运行的查询的 CSV 文件。这包括在 CloudTrail 控制台中或使用 CloudTrail API 进行的查询。如果您查询了 Audit Manager 事件数据存储，并且选择将结果保存到 Amazon S3，则此选项卡上会显示 CloudTrail 导出。

下载文件

按照以下步骤从下载中心下载文件。

下载文件

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择下载中心。
3. 选择评测报告选项卡或导出选项卡。
4. 选择要下载的文件，然后选择下载。

有关如何从 S3 目标存储桶下载文件的说明，请参阅 Amazon Simple Storage Service (Amazon S3) 用户指南中的下载对象。

删除文件

按照以下步骤删除下载中心中不再需要的所有评测报告。

> **Note**
>
> 当前不支持从下载中心中删除 CSV 导出。CSV 导出将在七天后自动从下载中心移除。

删除评测报告

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。

2. 在左侧导航窗格中，选择下载中心。
3. 选择评测报告选项卡。
4. 选择要删除的评测报告，然后选择删除。

如果您想从 S3 目标存储桶中删除评测报告或 CSV 导出，我们建议您直接在 Amazon S3 中完成此任务。有关说明，请参阅 Amazon Simple Storage Service (Amazon S3) 用户指南中的删除 Amazon S3 对象。

框架库

您可以通过AWS Audit Manager中的框架库访问和管理框架。

框架决定了一段时间内在环境中测试的控件。它按指定的合规标准或法规定义控件及其数据来源映射。它还用于组织和自动执行 Audit Manager 评测。您可以将框架作为起点，以审计您的AWS 服务使用情况并开始自动收集证据。

框架库包含标准和自定义框架目录。

- 标准框架是AWS提供的预先构建的框架。这些框架基于AWS的最佳实践标准，以满足不同合规标准和法规。包括 GDPR 和 HIPAA。标准框架包括根据框架支持的合规标准或法规组织成控件集的控件。

  您可查看标准框架的内容，但不能对其进行编辑或删除。但是，您可以自定义任何标准框架，创建新的框架以满足您的特定要求。
- 自定义框架是您所拥有的自定义框架。您可从头开始创建自定义框架，也可以通过自定义现有框架来创建。您可以按特定要求，通过自定义框架将控件组织成控件集。若要了解有关如何管理控件的更多信息，请参阅 控件库。

您可以通过标准框架或自定义框架创建评测。要了解如何创建和管理评测，请参阅 AWS Audit Manager中的评测。

> **Note**
>
> AWS Audit Manager 协助收集与核实特定合规性标准和法规遵守情况相关的证据。但是，它本身并不能评测您的合规情况。因此，通过 AWS Audit Manager 收集的证据可能不包括审计所需的、有关您的 AWS 使用情况的所有信息。AWS Audit Manager 不能代替法律顾问或合规专家。

本节介绍如何在 Audit Manager 中创建和管理自定义框架。

主题

- 访问AWS Audit Manager中的可用框架
- 查看框架详细信息
- 创建自定义框架

- 编辑自定义框架
- 删除自定义框架
- 共享自定义框架
- AWS Audit Manager 中支持的框架

访问AWS Audit Manager中的可用框架

您可以在 Audit Manager 控制台的框架库页面查看所有可用框架。在此，您还可以根据框架创建评测、创建自定义框架 或 自定义现有框架。

您还可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 查看所有可用框架。

Audit Manager console

若要查看可用框架（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择 框架库。
3. 选择 标准框架 选项卡或 自定义框架 选项卡，浏览可用的标准框架和自定义框架。
4. 选择任意框架名称，以查看该框架的详细信息。

AWS CLI

若要查看可用框架（AWS CLI）

若要在 Audit Manager 中查看框架，请使用list-assessment-frameworks命令并指定`--framework-type`。或者您可以检索标准框架列表。或者您可以检索自定义框架列表。

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

若要查看可用框架（API）

使用 ListAssessmentFrameworks 操作并指定 frameworkType。或者您可以返回标准框架列表。或者您可以返回自定义框架列表。

如需了解更多信息，请选择前面的任一链接，在 AWS Audit Manager API 参考中阅读更多内容。其中包括：如何在其中一个指定语言的AWS软件开发工具包中使用ListAssessmentFrameworks操作和参数的信息。

查看框架详细信息

您可以通过 Audit Manager 控制台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 查看框架的详细信息。

Audit Manager console

若要查看框架详细信息（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择框架库以查看可用框架列表。
3. 选择 标准框架 选项卡或 自定义框架 选项卡，浏览可用的框架。
4. 选择要打开的框架名称。

打开框架时，将会显示框架详细信息页面。本页各个部分及其内容如下所述。

框架详细信息部分

本节提供框架的概述。其中包含以下信息：

- 框架名称 - 框架的名称。
- 合规类型 - 框架支持的合规标准或法规。
- 描述 - 框架描述（如已提供）。
- 框架类型 - 指定框架是标准框架还是自定义框架。
- 控件集 - 与框架关联的控件集的数量。
- 控件 - 框架中控件的总数。
- 控件数据来源 - Audit Manager 从中收集证据的控件数据来源编号。
- 标签 - 与框架关联的标签。

如果您正在查看自定义框架，将显示以下详细信息：

- 创建者 - 创建自定义框架的账户。
- 创建日期 – 创建自定义框架的日期。
- 上次更新时间 - 上次编辑此框架的日期。

“控件” 选项卡

此选项卡列出了框架内的控件，按控件集分组。其中包含以下信息：

- 按控件集分组的控件 - 选择树视图图标，可查看属于每个控件集的控件。
- 类型 - 指定控件是标准控件还是自定义控件。
- 数据来源 - 指定 Audit Manager 从中收集该控件证据的数据来源。

标签选项卡

此选项卡列出与框架关联的标签。其中包含以下信息：

- 键 — 标签密钥（如合规性标准、法规或类别）。
- 值 - 标签值。

AWS CLI

查看框架详细信息 (AWS CLI)

1. 若要识别待审核框架，请运行list-assessment-frameworks 命令并指定 `--framework-type`。或者您可以检索标准框架列表。或者您可以检索自定义框架列表。

   在以下示例中，将*#####*替换为 `Custom` 或 `Standard`。

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   响应返回框架列表。找到待审核框架，并记下框架 ID 和Amazon 资源名称（ARN）。

2. 若要获取框架的详细信息，请运行 get-assessment-framework 命令并指定 `--framework-id`。

   在以下示例中，将*#####*替换为您自己的信息。

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

返回 JSON 格式的框架详细信息。若要了解此数据，请参见AWS CLI 命令引用中的get-assessment-framework 输出。

3. 若要查看框架标签，使用list-tags-for-resource 命令并为框架指定 `--resource-arn`。

   在以下示例中，将 ##### 替换为您自己的信息。

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   有关 Audit Manager 中标签的更多信息，请参阅标签 AWS Audit Manager 资源。

Audit Manager API

查看框架详细信息 (API)

1. 若要识别待审核框架，请运行ListAssessmentFrameworks 操作并指定frameworkType。或者您可以返回标准框架列表。或者您可以返回自定义框架列表。

   从响应中找到待审核框架，并记下框架 ID 和 Amazon 资源名称（ARN）。

2. 若要获取框架的详细信息，请使用GetAssessmentFramework操作。在请求中，指定您从第 1 步中获得的 frameworkId。

   返回 JSON 格式的框架详细信息。要了解这些数据，请参阅 AWS Audit Manager API 参考中的GetAssessmentFramework 响应元素。

3. 若要查看框架标签，请使用 ListTagsForResource 操作。在请求中，指定您从第 1 步中获得的resourceArn。

有关 Audit Manager 中标签的更多信息，请参阅标签AWS Audit Manager 资源。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

创建自定义框架

您可以通过AWS Audit Manager中的框架库访问和管理框架。您可以按特定要求，通过创建自定义框架将控件组织成控件集。

您可通过两种方式创建自定义框架。您可以自定义现有框架，也可从头开始创建新框架。

主题

从头开始创建新自定义框架

您可以按特定要求，使用 AWS Audit Manager 中的自定义框架将控件组织成控件集。您可按以下步骤，在框架库内从头开始创建新自定义框架。

主题

第 1 步：指定框架详细信息

首先指定要包含在自定义框架内的控件。

若要指定框架详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择框架库，然后选择创建自定义框架。
3. 在框架详细信息，输入名称、合规性标准或法规（可选）以及框架描述（可选）。输入合规性标准或法规关键字，例如 PCI_DSS 或 GDPR，以通过此关键字搜索您的框架。
4. 在 标签 下，选择 添加新标签，将标签与您的框架相关联。可为每个标签指定密钥和值。标签密钥为必填项。当在框架库中搜索此框架时，可以将其用作搜索条件。有关 AWS Audit Manager 中的标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签。
5. 选择 下一步。

第 2 步：指定控件集中的控件

接下来，您可以指定要向框架中添加的控件及其添加方式。首先将控件集添加至框架，然后将控件添加至控件集。

> **Note**
>
> 使用 AWS Audit Manager 控制台创建自定义框架时，您最多可以为每个框架添加 10 个控件集。
>
> 使用 Audit Manager API 创建自定义框架时，可以创建 10 个以上的控件集。要添加超过控制台当前允许的控件集，请使用 Audit Manager 提供的CreateAssessmentFramework API。

若要指定控件集中的控件

1. 在 控件集名称下，输入控件集名称。
2. 在 添加新控件至控件集，选择控件类型下，使用下拉列表选择两个控件类型之一：标准控件 或 自定义控件。标准控件由 Audit Manager 提供，自定义控件则由您创建。
3. 根据您在上一步中选择的选项，显示标准控件或自定义控件列表。您可浏览列表，也可以通过输入控件名称、合规性或标签进行搜索。选择一个或多个控件，然后选择 添加至控件集，将其添加至控件集中。
4. 在出现的弹出窗口中，选择 添加至控件集 以确认您的添加。
5. 在 审核控件集中的选定控件 下，查看选定控件列表中显示的控件。要向控件集添加更多控件，请重复第 2 步至第 4 步。通过选择一个或多个控件并选择移除控件，可以从控件集中移除不需要的控件。
6. 要向框架添加新控件集，请选择页面底部的添加控件集。您可以通过选择移除控件集来移除不需要的控件集。
7. 添加完控件集和控件后，选择 下一步。

第 3 步：审核并创建框架

审核您的框架信息。若要更改步骤信息，请选择 编辑。

完成后，选择 创建自定义框架。

接下来如何操作？

创建新的自定义框架后，您可根据框架创建评测。有关更多信息，请参阅创建评测。

您也通过使用现有框架创建自定义框架。有关更多信息，请参阅自定义现有框架。

有关如何编辑自定义框架的说明，请参阅 编辑自定义框架。

自定义现有框架

通过 AWS Audit Manager 中的自定义框架，您可以按特定要求将控件组织成控件集。与其从头开始创建自定义框架，不如以现有框架为起点并对其进行自定义。执行此操作时，现有框架将保留在框架库内，通过您的自定义设置创建新的自定义框架。

您可以选择对任何现有框架进行最定义操作。它可以是标准框架或自定义框架。

在框架库中，从 创建自定义框架 下拉列表中选择 自定义现有框架。按以下步骤自定义框架。

主题

第 1 步：指定框架详细信息

除标签外，所有框架详细信息均来自原始框架。根据需要检查和修改这些详细信息。

若要指定框架详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择 框架库。
3. 选择您想要自定义的框架，从 创建自定义框架 下拉列表中选择 自定义现有框架。
4. 在所示弹出窗口中，输入新自定义框架的名称，然后选择 自定义。
5. 在 框架详细信息下，查看框架的名称、合规性类型和描述，并根据需要进行修改。合规性类型应指明与框架相关的合规性标准或法规。您可以通过此关键字搜索框架。
6. 在 标签 下，选择 添加新标签，将标签与您的框架相关联。可为每个标签指定密钥和值。标签密钥为必填项，在框架库中搜索此框架时可用作搜索标准。有关 AWS Audit Manager 中的标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签。
7. 选择下一步。

第 2 步：指定控件，以添加到控件集

控件集来自原始框架。根据需要，通过添加更多控件或删除现有控件自定义当前配置。

> **Note**
>
> 使用 AWS Audit Manager 控制台自定义框架时，您最多可以为每个框架添加 10 个控件集。使用 Audit Manager API 创建自定义框架时，可以添加 10 个以上的控件集。要添加超过控制台当前允许的控件集，请使用 Audit Manager 提供的CreateAssessmentFramework API。

若要指定控件集中的控件

1. 在 控件集名称下，根据需要自定义控件集名称。
2. 在 添加新控件至控件集下，使用下拉列表选择两个控件类型之一：标准控件 或 自定义控件，以添加新控件。
3. 根据您在上一步中选择的选项，显示标准控件或自定义控件列表。您可浏览此列表，也可以通过输入控件名称、合规性或标签定位您想要添加的控件。选择一个或多个控件，然后选择添加至控件集，将其添加至控件集中。
4. 在出现的弹出窗口中，选择 添加至控件集 以确认您的添加。
5. 在 审核控件集中的选定控件 下，查看选定控件列表中显示的控件。要向控件集添加更多控件，请重复第 2 步至第 4 步。通过选择一个或多个控件并选择移除控件，可以从控件集中移除不需要的控件。
6. 要向框架添加新控件集，请选择页面底部的添加控件集。您可以通过选择移除控件集来移除不需要的控件集。
7. 添加完控件集和控件后，选择 下一步。

第 3 步：审核并创建框架

审核您的框架信息。若要更改步骤信息，请选择 编辑。

完成后，选择 创建自定义框架。

接下来如何操作？

创建新的自定义框架后，您可根据框架创建评测。有关更多信息，请参阅创建评测。

有关如何编辑自定义框架的说明，请参阅 编辑自定义框架。

编辑自定义框架

您可以按特定要求，使用 AWS Audit Manager 中的自定义框架将控件组织成控件集。您可以按照以下步骤，使用框架库查找和编辑自定义框架。

主题

第 1 步：编辑框架详细信息

首先审核和编辑现有框架详细信息。

若要编辑框架详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择框架库，然后选择自定义框架选项卡。
3. 选择想要编辑的框架，选择 操作，然后选择 编辑。
   - 或者，您可以打开自定义框架，然后选择评测摘要页面右上角的 操作、编辑。
4. 在框架详细信息下，查看框架的名称、合规性类型和描述，并根据需要进行修改。
5. 选择 下一步。

> **Tip**
>
> 若要编辑框架的标签，请打开框架并选择框架标签选项卡。您可查看和编辑与框架关联的标签。

第 2 步：编辑控件集中的控件

接下来，查看和编辑框架中的控件和控件集。

> **Note**
>
> 使用 AWS Audit Manager 控制台编辑自定义框架时，您最多可以为每个框架添加 10 个控件集。
> 使用 Audit Manager API 编辑自定义框架时，可以创建 10 个以上的控件集。要添加超过控制台当前允许的控件集，请使用 Audit Manager 提供的UpdateAssessmentFramework API。

若要编辑控件

1. 在 控件集名称 下，根据需要查看和编辑控件集的名称。
2. 在 向控件集中添加新控件 下，可添加控件。使用下拉列表选择以下两种控件类型之一：标准控件或自定义控件。
3. 根据您在上一步中选择的选项，显示标准控件或自定义控件表格列表。您可以浏览控件集列表。或者，您可以通过输入控件名称、数据来源或标签进行搜索，以找到要添加的控件。选择一个或多个控件，然后选择 添加至控件集，将其添加至控件集中。
4. 在出现的弹出窗口中，选择 添加至控件集 以确认您的添加。
5. 在 审核控件集中的选定控件 下，查看并编辑选定控件列表中当前显示的控件。要向控件集添加更多控件，请重复第 2 步至第 4 步。通过选择一个或多个控件并选择移除控件，可以从控件集中移除不需要的控件。
6. 要向框架添加新控件集，请选择页面底部的添加控件集。通过选择移除控件集来移除不需要的控件集。
7. 添加完控件集和控件后，选择 下一步。

第 3 步 审核和更新框架

审核您的框架信息。若要更改步骤信息，请选择 编辑。

完成后，选择 保存更改。

删除自定义框架

您可以使用框架库查找和删除不必要的自定义框架。您还可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 删除自定义框架。

> **Note**
>
> 删除自定义框架，不会影响删除前按此框架创建的任何现有评测。

Audit Manager console

若要删除自定义框架（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中选择框架库，然后选择自定义框架选项卡。
3. 选择要删除的框架，选择操作，然后选择 删除。
   - 或者，您可以打开自定义框架，然后选择评测摘要页面右上角的 操作、删除。
4. 在弹出窗口中，选择 删除以确认删除。

AWS CLI

若要删除自定义框架 (AWS CLI)

1. 首先标识要删除的自定义框架。为此，请运行list-assessment-frameworks 命令并将 `--framework-type` 指定为 `Custom`。

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   响应返回自定义框架列表。找到要删除的自定义框架，记下框架 ID。

2. 接下来，运行delete-assessment-framework 命令并指定待删除框架的 `--framework-id`。

   在以下示例中，将 *#####* 替换为您自己的信息。

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

Audit Manager API

若要删除自定义框架 (API)

1. 使用 ListAssessmentFrameworks 操作并指定 frameworkType 为 `Custom`。从响应中找到要删除的自定义框架，记下框架 ID。
2. 使用DeleteAssessmentFramework操作删除框架。按请求使用 frameworkId 参数指定要删除的框架。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit ManagerAPI 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

共享自定义框架

您可以使用AWS Audit Manager的框架共享功能，快速复制您创建的自定义框架。现在，您可以与其他AWS 账户共享您的自定义框架，也可将其复制到您自有账户下的其他AWS 区域。然后，接收者可以访问您的自定义框架并将其用于创建评测。完成此操作时，您不需要对此框架重复任何配置。

若要共享自定义框架，请创建共享请求。然后，共享请求的接收者有 120 天的时间接受或拒绝此请求。当他们接受共享请求时，Audit Manager 会将共享自定义框架复制到其框架库中。除了复制自定义框架外，Audit Manager 还会复制该框架中包含的自定义控件集和自定义控件。这些自定义控件已添加至接收者的控件库。Audit Manager 不复制标准框架或控件。默认情况下，它们可用于支持 Audit Manager 的所有AWS 账户和区域。

框架共享功能仅适用于付费级。但是，共享自定义框架或接受共享请求将不会产生额外费用。要了解有关 AWS Audit Manager 定价的更多信息，请参阅 AWS Audit Manager 定价页面。

> **Important**
>
> 如果标准框架被指定为不符合AWS共享条件，则不得共享源自标准框架的自定义框架，除非您已获得标准框架所有者的许可。若要查看不符合共享条件的标准框架并了解更多信息，请参阅框架共享资格。

本指南的以下各节描述了您应该了解的、有关框架共享的重要信息。它们还提供了关于如何共享自定义框架和响应共享请求的说明。

主题

> **Tip**
>
> 如果您不熟悉 Audit Manager 自定义框架及其创建方式，可以在本指南的创建自定义框架页面了解更多信息。

框架共享概念和术语

如果您了解了以下关键概念，则可以从 AWS Audit Manager 自定义框架共享功能中获得更多收益。

发件人

这是共享请求的创建者，也是自定义框架所在的AWS 账户。发送方可以与任何AWS 账户共享自定义框架。或者，他们将自定义框架复制到自己账户下支持的AWS 区域。

收件人

这是共享框架使用者。接收者可以接受或拒绝发送方的共享请求。

> **Note**
>
> 接收者可能是委托管理员账户。但是，您不能与 AWS Organizations 管理账户共享自定义框架。

框架资格

您只能共享自定义框架。默认情况下，所有标准框架都置于AWS 账户，以及支持AWS Audit Manager的AWS 区域。另外，您共享的自定义框架不得包含敏感数据。这包括在框架本身、其控件集以及自定义框架中的任何自定义控件所包含的数据。

> **Important**
>
> AWS Audit Manager提供的某些标准框架包含受许可协议约束的、受版权保护的材料。自定义框架可能包含源自此类框架的内容。如果标准框架被指定为不符合 AWS 的共享条件，则不得共享源自标准框架的自定义框架，除非您已获得标准框架所有者的许可。
> 要了解符合共享条件的标准框架，请参阅下表。

标准框架名称	符合共享条件的自定义版本
澳大利亚网络安全中心 (ACSC) 八大要点	 是
澳大利亚网络安全中心 (ACSC) 信息安全手册	 是
AWS Audit Manager 示例框架	 是
AWS Control Tower防护机制	 是
AWS生成式人工智能最佳实践框架 v1	 是
AWS License Manager	 是
AWS 基础安全最佳实践	 是

标准框架名称	符合共享条件的自定义版本
AWS运营最佳实践	 是
AWS Well-Architected Framework	 是
加拿大网络安全中心 - 中型	 否
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级	 否
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级和 2 级	 否
CIS Amazon Web Services 基金会基准的 CIS 基准， v1.3.0，1 级	 否
CIS Amazon Web Services 基金会基准的 CIS 基准， v1.3.0，1 级和 2 级	 否
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级	 否
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级和 2 级	 否

标准框架名称	符合共享条件的自定义版本
CIS Controls v7.1 IG1	 是
CIS Controls v8 IG1	 否
FedRAMP Moderate Baseline	 是
GDPR	 是
Gramm-Leach-Bliley 法案 (GLBA)	 是
GxP 21 CFR 第 11 部分	 是
GxP 欧盟附录 11	 是
2003 年 HIPAA 安全规则	 是
2013 HIPAA 最终综合安全规则	 是

标准框架名称	符合共享条件的自定义版本
ISO/IEC 27001:2013 附录 A	否
NIST 800-53 (第 5 版) Low-Moderate-High	是
NIST Cybersecurity Framework 1.1 版	是
NIST SP 800-171，第 2 版	是
PCI DSS v3.2.1	否
PCI DSS v4.0	否
SOC 2	否

共享请求

若要共享自定义框架，请创建共享请求。共享请求指定接收者，并通知他们可用的自定义框架。接收者有 120 天的时间回复共享请求，即接受或拒绝。如果在 120 天内未采取任何行动，则共享请求将过期，接收者将无法将自定义框架添加到其框架库中。发送方和接收者可通过框架库的共享请求页面查看共享请求并对其采取行动。

共享请求状态

共享请求可具有以下任一状态。

- 激活 — 这表示共享请求已成功发送给接收者，并正在等待其响应。
- 即将到期 — 这表示共享请求将在未来 30 天内到期。
- 已共享 — 这表示接收者接受了共享请求。
- 非活动 — 这表示接收者采取行动之前，共享请求已被撤销、拒绝或过期。
- 复制 — 这表示已接受的共享请求正在复制到接收者的框架库。
- 失败 — 这表示共享请求未成功发送至接收者。

共享请求通知

当接收者收到共享请求时，Audit Manager 会通知他们。当共享请求在接下来的 30 天内到期时，接收者和发送方都会收到通知。

- 对于接收者，在收到的处于 激活 或即将到期 状态的请求旁边会出现一个蓝色的通知点。接收者可以通过接受或拒绝共享请求，以解决通知。
- 对于发送方，已发送的请求处于即将到期状态时，旁边会出现一个蓝色的通知点。接收者接受或拒绝请求时，通知解决。否则，其将在请求到期时解决。此外，发送方可通过撤消共享请求，以不再收到通知。

发送方所有权

发送方保留对其共享的自定义框架的完全访问权限。他们可以通过在请求到期前 撤销共享请求，随时取消活跃的共享请求。但是，在接收者接受共享请求后，发送方将无法再撤消接收者对该自定义框架的访问权限。原因是当接收者接受请求时，Audit Manager 会在接收者的框架库中创建自定义框架的独立副本。

除了复制发送方的自定义框架外，Audit Manager 还会复制该框架中包含的自定义控件集和自定义控件。但是，Audit Manager 不会复制附加至自定义框架的任何标签。

接收者所有权

接收者对他们接受的自定义框架拥有完全访问权限。当接收者接受请求时，Audit Manager 会将自定义框架复制到其框架库中的自定义框架选项卡。然后，接收者可以像管理任何其它自定义框架一样管理共享的自定义框架。接收者可以共享他们从其他发送方那里收到的自定义框架。接收者无法阻止发送方发送共享请求。

共享框架到期

当发送方创建共享请求时，Audit Manager 会将该请求有效期设置为 120 天。在请求到期之前，接收者可以接受并获得对共享框架的访问权限。如果接收者在这段时间内不接受，则共享请求将过

期。此后，过期共享请求的记录将保留在其历史记录中。出于审计目的，过期共享框架的快照会存档至 S3 存储桶中，TTL 为期一年。

在共享请求到期之前，发送方可以随时选择撤销共享请求。

共享框架数据存储和备份

创建共享请求时，Audit Manager 会在美国东部（弗吉尼亚州北部）AWS 区域存储您的自定义框架的快照。Audit Manager 还会在美国西部（俄勒冈州）AWS 区域存储同一快照的备份。

发生以下事件之一时，Audit Manager 会删除快照与备份快照：

- 发送方撤销共享请求。
- 接收者拒绝共享请求。
- 接收者遇到错误且未成功接受共享请求。
- 共享请求将在接收者回复请求之前过期。

当发送方重新发送共享请求时，快照将替换为与最新版本自定义框架对应的更新版本。

当接收者接受共享请求后，快照将复制到共享请求中指定的AWS 区域下方的AWS 账户。

共享框架版本控制

当您共享自定义框架时，Audit Manager 会在指定 AWS 账户 和区域中创建该框架的独立副本。这意味着您应该记住以下几点：

- 接收者接受的共享框架是共享请求创建时的框架快照。如果您在发送共享请求后更新原始自定义框架，则该请求无法自动更新。若要共享最新版本的更新框架，您可以重新发送共享请求。此新快照的到期日期为重新共享之日起 120 天。
- 当您与其他AWS 账户共享自定义框架然后将其从框架库中删除时，共享自定义框架将保留在接收者框架库中。
- 当您在自己的账户下与其他 AWS 区域 共享自定义框架，然后在第一个 AWS 区域 中删除该自定义框架时，该自定义框架将保留在第二个区域中。
- 当您在接受共享自定义框架后将其删除时，自定义框架中复制的所有自定义控件都将保留在您的控件库中。

发送自定义框架共享请求

本教程介绍如何跨AWS 账户和AWS 区域共享您的自定义框架。

当您共享自定义框架时，Audit Manager 会创建您的框架的快照，并向接收者发送共享请求。接收者有 120 天的时间接受共享框架。当他们接受时，Audit Manager 会将共享自定义框架复制到指定 AWS 区域 中的框架库中。如果您想使用自己的账户将自定义框架复制到另一个区域，请使用以下教程并输入您自己的 AWS 账户 ID，后者作为接收者账户 ID。

本教程包含以下步骤：

1. 选择要共享的框架 - 浏览框架库以查找要共享的自定义框架。
2. 发送共享请求 - 指定接收者并向他们发送自定义框架共享请求。
3. 查看已发送的请求 - 查看您的共享请求历史记录，并查看已发送的请求的状态。
4. （可选）撤销共享请求 - 在共享请求到期之前将其撤销。

先决条件

开始本教程之前，请确保满足以下条件：

- 您熟悉 Audit Manager 框架共享概念和术语。
- 您要共享的自定义框架符合共享条件，并且存在于您的AWS Audit Manager环境框架库中。
- 接收者已在您要共享自定义框架的AWS 区域位置中启用AWS Audit Manager。
- 接收者不是 AWS Organizations 管理账户。

> **Tip**
>
> 开始之前，请记下您要与之共享自定义框架的 AWS 账户 ID。如果您的目标是将框架复制到您账户下的其他AWS 区域，则这可以是您自己的账户 ID。您在教程的第 2 步中需要此信息。

> **Important**
>
> 切勿共享包含敏感数据的自定义框架。这包括在框架本身、其控件集以及自定义框架中的任何自定义控件所包含的数据。有关更多信息，请参阅 框架资格 。

第 1 步：识别要共享的自定义框架

首先识别要共享的自定义框架 您可以在 Audit Manager 中的框架库页面查看所有可用自定义框架的列表。

若要查看可用的自定义框架

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择 框架库。
3. 选择 自定义框架 选项卡。此操作会显示可用自定义框架列表。选择任意框架名称，以查看该自定义框架的详细信息。

第 2 步：发送共享请求

接下来，指定接收者并向他们发送自定义框架共享请求。在共享请求到期之前，接收者有 120 天的时间回复。

若要发送共享请求

1. 在框架库的自定义框架选项卡中，选择框架的名称以打开详细信息页面。您可在此选择操作，然后选择 共享自定义框架。
   - 或者，从框架库的列表中选择一个自定义框架，选择 操作，然后选择 共享自定义框架。根据自定义框架的大小，当 Audit Manager 准备共享请求时，此方法可能需要几秒钟。
2. 查看对话框内显示的通知。
   - 如果您不确定是否可共享您的自定义框架，请查看框架资格以获取更多指导。
   - 如果您的框架包含使用自定义AWS Config规则作为数据来源的控件，我们建议您联系接收者。然后，接收者可以在自己的AWS Config实例中创建和启用相同的AWS Config规则。有关更多信息，请参阅我的共享框架包含使用自定义 AWS Config 规则作为数据来源的控件。收件人能否为这些控件收集证据？。
3. 输入**agree**，然后选择 同意继续。
4. 在下一个屏幕上执行以下步骤：
   - 在 AWS 账户下，输入接收者的账户 ID。可以是您自己的账户 ID。
   - 在 AWS 区域下，从下拉列表中选择接收者所在的区域。
   - （可选）在 接收者的消息下，输入有关您正在共享的自定义框架的可选评论。
   - 在 自定义框架详细信息下，查看详细信息以确认您要共享此框架。
5. 选择 共享。

> **Note**
>
> 请记住以下几点：
>
> - 当您与其他AWS 账户共享自定义框架时，该框架仅复制到指定AWS 区域。接受共享请求后，接收者可以根据需要跨区复制框架。
> - 跨AWS 区域共享自定义框架时，处理共享请求操作可能需要长达 10 分钟。发送跨区域共享请求后，我们建议您稍后再回来查看，以确认您的共享请求已成功发送。
> - 当您发送共享请求时，Audit Manager 会在创建共享请求时拍摄自定义框架快照。如果您在发送共享请求后更新自定义框架，则该请求无法自动更新。若要共享最新版本的更新框架，您可以重新发送共享请求。此新快照的到期日期为重新共享之日起 120 天。

第 3 步：查看您已发送的请求

您可以选择 已发送的请求 选项卡，以查看您发送的所有共享请求的列表。您可根据需要筛选此列表。例如，您可以应用筛选条件，仅显示在未来 30 天内到期的请求。

查看和筛选您已发送的请求

1. 在导航窗格中，请选择 共享请求。
2. 选择 已发送的请求 选项卡。
3. （可选）应用筛选条件微调可见的已发送的请求。为此，您可以找到 所有状态下拉列表，然后将筛选条件更改为以下选项之一。
   - 活动 — 此筛选条件显示正在等待接收者响应的共享请求。
   - 已共享 — 此筛选条件显示接收者已接受的共享请求。共享的自定义框架现已存在于接收者的框架库中。
   - 非活动 — 此筛选条件显示接收者采取行动之前，共享请求已被撤销、拒绝或过期。选择非活动以查看更多详细信息。
   - 即将到期 — 此筛选条件显示在未来 30 天内到期的共享请求。
   - 失败 — 此筛选条件显示未成功发送给接收者的共享请求。选择失败以查看更多详细信息。

> **Note**
>
> 此共享请求的处理可能最多需要 15 分钟。因此，如果在向接收者发送共享请求时出错，则可能不会立即显示失败状态。我们建议您稍后再回来查看，以确认您的共享请求已成功发送。有关遇到错误时如何继续操作的信息，请参阅共享请求故障排除。

第 4 步（可选）：撤消共享请求

如果您需要在激活的共享请求到期前将其取消，则可以随时撤销该请求。此为可选步骤。如果您不采取任何行动，则接收者将无法在到期日期之后接受共享请求。

若要撤销共享请求

1. 在导航窗格中，请选择 共享请求。
2. 选择 已发送的请求 选项卡。
3. 选择要撤消的框架，然后选择撤消请求。
4. 在出现的弹出窗口中，选择 撤消。

> **Note**
>
> 您只能撤消对状态为 活动 或 即将到期 的共享请求的访问权限。但是，在接收者接受共享请求后，您将无法再撤消接收者对该自定义框架的访问权限。原因是自定义框架副本现在存在于接收者框架库中。
>
> 跨AWS 区域共享框架时，处理共享请求操作可能需要长达 10 分钟。撤销跨区域共享请求后，我们建议您稍后再回来查看，以确认您的共享请求已成功撤销。

重新发送最新框架的共享请求

您可以发送自定义框架共享请求，然后更新相同框架。若要执行此操作，共享请求不会自动更新以反映框架的最新版本。但是，如果其状态为 活动、已共享或 即将到期，则可更新现有的共享请求。为此，您需要重新发送新的共享请求，其详细信息与当前请求应相同。在新的共享请求中，纳入相同的自定义框架 ID、接收者账户 ID 和接收者AWS 区域。您也可以按新的共享请求提供新的评论。

重新发送共享请求时，切记以下信息：

- 若要成功更新，新请求必须使用相同的自定义框架 ID。它还必须指定与现有请求相同的接收者账户 ID 和区域。
- 如果自定义框架的名称已更改，则更新共享请求将显示最新的名称。
- 如果您提供新评论，则更新后的共享请求会显示最新评论。
- 当您重新发送共享请求，到期日期将延长六个月。

若要重新发送最新框架的共享请求

1. 在框架库的自定义框架选项卡中，选择要共享的框架的名称。此操作将打开框架详细信息页面。您可在此选择操作，然后选择 共享自定义框架。

   - 或者，从框架库的列表中选择自定义框架，选择 操作，然后选择 共享自定义框架。根据自定义框架的大小，此方法可能需要几秒钟的时间让 Audit Manager 准备共享请求。

2. 查看对话框中显示的通知，输入**agree**，然后选择同意以继续。
3. 在下一个屏幕上执行以下步骤：

   - 在AWS 账户下，输入您在现有共享请求中指定的相同账户 ID。
   - 在AWS 区域下，选择您在现有共享请求中指定的相同区域。
   - （可选）在 接收者的消息下，输入有关最新自定义框架的可选评论。
   - 在 自定义框架详细信息下，查看详细信息以确认您要重新发送共享请求。

4. 选择 共享以重新发送和更新共享请求。

共享请求故障排除

若要针对共享自定义框架时可能遇到的问题查找解决方案，请参阅本指南的故障排除部分的框架共享问题排查。

响应共享请求

本教程介绍了在收到自定义框架共享请求时需执行的操作。当您收到共享请求时，Audit Manager 会通知您。当共享请求在接下来的 30 天内到期时，接收者和发送方都会收到通知。

本教程包含以下步骤：

1. 查看您的共享请求通知 - 查看活动且即将到期的共享请求列表。
2. 对共享请求采取行动 - 接受或拒绝自定义框架的共享请求。

3. 查看您从其他处收到的共享请求 - 查看您的共享请求历史记录。

先决条件

在开始之前，我们建议您首先了解有关 Audit Manager 框架共享概念和术语 的更多信息。

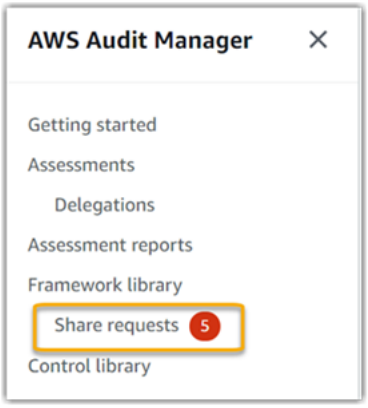
第 1 步：查看您收到的请求通知

首先查看您的共享请求通知。已收到的请求 选项卡显示您从其他AWS 账户那里收到的共享请求的列表。等待您响应的请求将显示一个蓝点。您也可以筛选此视图，仅显示在未来 30 天内到期的请求。

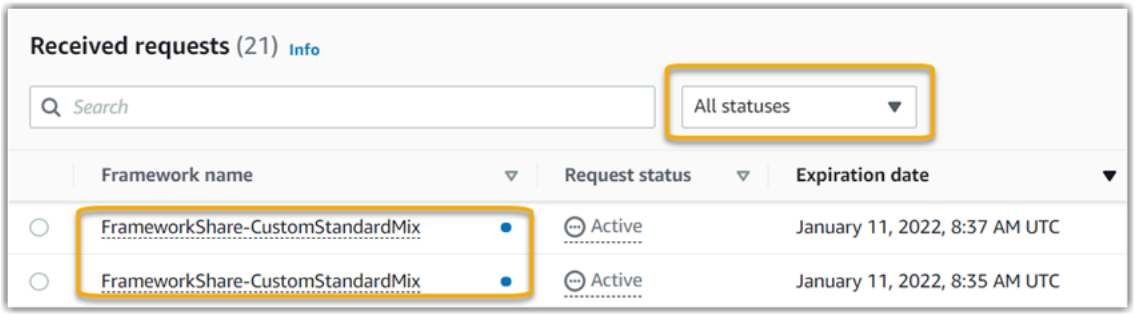
若要查看已收到的请求

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 如果您收到共享请求通知，Audit Manager 会在导航菜单图标旁边显示红点。

3. 展开导航窗格并查看 共享请求 旁边的内容。通知徽章指示需要您注意的共享请求数量。



4. 选择 共享请求。默认情况下，此页面在已收到的请求 选项卡中打开。
5. 通过查找带有蓝点的项目，识别需要您采取行动的共享请求。



6. (可选) 如仅需查看在未来 30 天内到期的请求，请找到所有状态下拉列表并选择即将到期。

第 2 步：对请求采取行动

若要删除蓝色通知点，您需要通过接受或拒绝共享请求来采取行动。

> **Note**
>
> 跨AWS 区域共享框架时，处理共享请求操作可能需要长达 10 分钟。对跨区域共享请求采取行动后，我们建议您稍后再回来查看，以确认您的共享请求已被成功接受或拒绝。

接受共享框架

当您接受共享请求时，Audit Manager 会将原始框架的快照复制到框架库的自定义框架选项卡。Audit Manager 使用您在 Audit Manager 设置中指定的 KMS 密钥复制和加密新的自定义框架。

若要接受共享请求

1. 打开共享请求页面，确保您正在查看已收到的请求选项卡。
2. （可选）从筛选条件下拉列表中选择 活动 或 即将到期。
3. （可选）选择框架名称，以查看共享请求的详细信息。这包括框架描述、框架中的控件数量以及发送方消息等信息。
4. 选择要接受的共享请求，然后依次选择 操作 和 接受。

接受共享请求后，当共享自定义框架添加至您的框架库时，状态将更改为正在复制。如果框架中包含自定义控件，则此时会将这些控件添加至您的控件库。

框架复制完成后，状态将更改为已共享。成功横幅会通知您自定义框架已准备就绪和可供使用。

> **Tip**
>
> 当您接受自定义框架后，它只会复制到您的当前AWS 区域。您可能需要在AWS 账户中拥有跨所有区域的新共享框架。如果是，在您接受共享请求后，您可以根据需要将框架共享至您账户下的其他区域。

拒绝共享框架

当您拒绝共享请求时，Audit Manager 不会将该自定义框架添至您的框架库。但是，已收到的请求选项卡中仍有被拒绝的共享请求记录，状态为 非活动。

若要拒绝共享请求

1. 打开共享请求页面，确保您正在查看已收到的请求选项卡。
2. （可选）从筛选条件下拉列表中选择 活动 或 即将到期。
3. （可选）选择框架名称，以查看共享请求的详细信息。这包括框架描述、框架中的控件数量以及发送方消息等信息。
4. 选择要拒绝的共享请求，选择操作，然后选择 拒绝。
5. 在出现的对话框中，选择 拒绝以确认您的选择。

> **Tip**
>
> 如果您在拒绝后改变主意并希望访问共享框架，请要求发送方向您发送新的共享请求。

第 3 步：查看您已收到的请求的历史记录

接受或拒绝共享框架后，您可以返回共享请求页面，以查看您的共享请求历史记录。您可根据需要筛选此列表。例如，您可以应用筛选条件，以仅显示您接受的请求。

若要查看您的共享请求历史记录

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择共享请求。
3. 选择 已收到的请求 选项卡。
4. 找到 所有状态 下拉列表，然后选择以下筛选条件之一。
   - 活动 — 此筛选条件显示您尚未接受或拒绝的共享请求。
   - 即将到期 — 此筛选条件显示在未来 30 天内到期的共享请求。
   - 已共享 – 此筛选条件显示您接受的共享请求。共享框架现在已在您的框架库内。
   - 非活动 - 此筛选条件显示被拒绝或已过期的共享请求。
   - 失败 — 此筛选条件显示未成功发送的共享请求。选择失败以查看更多详细信息。

接下来如何操作？

接受共享自定义框架后，可以在框架库的自定义框架选项卡中找到它。现在您可以使用此框架创建评测。要了解更多信息，请参阅 创建评测。有关如何编辑新自定义框架的说明，请参阅 编辑自定义框架。

删除共享请求

您可以删除不再需要的共享请求。

> **Note**
>
> 您无法删除状态为 活动 或 正在复制 的共享请求。
> 当您删除共享请求时，仅删除请求本身。共享框架本身仍保留在您的框架库内。

若要删除共享请求

1. 在导航窗格中，请选择 共享请求。
2. 选择 已发送的请求 或 已收到的请求 选项卡。
3. 选择不再需要的框架，然后选择 删除。
4. 在出现的弹出窗口中，选择 删除。

AWS Audit Manager 中支持的框架

AWS Audit Manager 提供了以下标准框架。这些预先构建框架基于各种合规性标准和法规的AWS最佳实践。您可以使用这些框架协助审计准备。

主题

- 澳大利亚网络安全中心 (ACSC) 八大要点
- 澳大利亚网络安全中心 (ACSC) 信息安全手册
- AWS Audit Manager 示例框架
- AWS Control Tower防护机制
- AWS 生成式人工智能最佳实践框架 v1
- AWS License Manager

- AWS 基础安全最佳实践
- AWS 运营最佳实践
- AWS Well-Architected
- 加拿大网络安全中心中型云控件配置文件
- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0
- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0
- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0
- CIS Controls v7.1 Implementation Group 1
- CIS Controls v8 Implementation Group 1
- FedRAMP Moderate Baseline
- 通用数据保护条例 (GDPR)
- Gramm-Leach-Bliley 法案
- GxP 21 CFR 第 11 部分
- GxP 欧盟附录 11
- 健康保险流通与责任法案 (HIPAA) 2003 年安全规则
- 《健康保险流通与责任法案》(HIPAA) 2013 最终综合安全规则
- ISO/IEC 27001:2013 附录 A
- NIST 800-53 (第 5 版) Low-Moderate-High
- NIST Cybersecurity Framework 1.1 版
- NIST SP 800-171 (第 2 版)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

澳大利亚网络安全中心 (ACSC) 八大要点

为了帮助您做好审计准备，AWS Audit Manager 提供了预先构建的标准框架，用于构造和自动执行八大要点框架的评测。

主题

- 什么是澳大利亚网络安全中心 (ACSC) 八大要点？

什么是澳大利亚网络安全中心 (ACSC) 八大要点？

澳大利亚网络安全中心 (ACSC) 是澳大利亚政府负责网络安全的牵头机构。为了防范网络安全威胁，ACSC 建议组织以 ACSC 的 网络安全迁移事件策略为基准，实施八大要点迁移策略。此基准被称为八大要点，使对手更难入侵系统。

由于八大要点概述了一组最低限度的预防措施，因此您的组织需要在环境允许的情况下实施其他措施。此外，尽管八大要点可以帮助缓解大多数网络威胁，但它并不能缓解所有网络威胁。因此，需要考虑其他缓解策略和安全控制措施，包括 网络安全事件迁移策略 和 信息安全手册 (ISM) 中的内容。

使用此框架支持您的审计准备

您可以使用AWS Audit Manager中的八大要点标准框架帮助为审计做准备。此框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据八大要点要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于八大要点框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
八大要点	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_EssentialEight.zip 文件。

此 AWS Audit Manager 框架中的控件不用于验证您的系统是否符合八大要点控件。此外，他们无法保证你会通过八大要点审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到八大要点框架。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于八大要点框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何使用此框架创建评测的说明，请参阅 创建评测。有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多八大要点资源

- ACSC 八大要点

澳大利亚网络安全中心 (ACSC) 信息安全手册

为了帮助您做好审计准备，AWS Audit Manager 提供了预先构建的标准框架，用于构造和自动执行 ACSC 信息安全手册框架的评测。

主题

- 什么是澳大利亚网络安全中心 (ACSC) 信息安全手册？
- 使用此框架支持您的审计准备
- 更多 ACSC 信息安全手册资源

什么是澳大利亚网络安全中心 (ACSC) 信息安全手册？

澳大利亚网络安全中心 (ACSC) 是澳大利亚政府负责网络安全的牵头机构。ACSC 编制《信息安全手册》(ISM)，该手册是一套网络安全原则。这些原则旨在为组织保护其系统和数据免受网络威胁提供战略指导。该网络安全原则分为四个关键活动：治理、保护、检测和响应。组织应该能够证明其组织内

遵守了网络安全原则。ISM 适用于首席信息安全官、首席信息官、网络安全专业人员以及信息技术经理。

ISM 框架由澳大利亚网络安全中心根据Creative Commons Attribution 4.0 International License提供，版权信息可在 ACSC | Copyrigh 上找到。© 版权所有，澳大利亚联邦 2022。

使用此框架支持您的审计准备

您可以使用AWS Audit Manager中的 ACSC 信息安全手册标准框架帮助为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件按照《ACSC 信息安全手册》的要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于《ACSC 信息安全手册》框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
ACSC 信息安全手册	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip 文件。

此 AWS Audit Manager 框架中的控件不用于验证您的系统是否符合 ACSC 信息安全手册控件。此外，他们无法保证你会通过 ACSC 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架 选项卡下找到 ACSC 信息安全手册框架。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 ACSC 信息安全手册框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何使用此框架创建评测的说明，请参阅 创建评测。有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 ACSC 信息安全手册资源

- ACSC 信息安全手册

AWS Audit Manager 示例框架

AWS Audit Manager 提供了示例框架，可帮助您开始审计准备。

主题

- 什么是 AWS Audit Manager 示例框架？
- 使用此框架支持您的审计准备

什么是 AWS Audit Manager 示例框架？

AWS Audit Manager示例框架是一个简单的框架，可将其用于使用 Audit Manager。相比之下，Audit Manager 提供的其他一些预先构建框架要大得多，并且包含许多控件。通过使用示例框架代替较大的框架，您可以更轻松地查看和探索框架示例。此框架中的控件基于一系列 AWS Config 和 AWS API 调用。

使用此框架支持您的审计准备

您可以使用该框架帮助入门 AWS Audit Manager。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该AWS Audit Manager示例框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于框架中定义的控件执行此操作。接下来，它收集相关证据，然后将其附加至评测中的控件。

AWS Audit Manager 示例框架的详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS Audit Manager 示例框架	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Managemen t

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于AWS Audit Manager示例框架的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

AWS Control Tower防护机制

AWS Audit Manager提供了 AWS Control Tower 防护机制框架，以帮助您做好审计准备。

主题

- 什么是 AWS Control Tower？
- 使用此框架支持您的审计准备
- 更多AWS Control Tower资源

什么是 AWS Control Tower？

AWS Control Tower 是一项管理和治理服务，您可以使用它来浏览创建多账户AWS环境所涉及的设置过程和治理要求。

借助AWS Control Tower，你只需点击几下，即可预置符合公司或组织策略要求的新AWS 账户。AWS Control Tower 代表您创建编排 层，整合预集成多个其他AWS 服务的功能。这些服务包括AWS Organizations、AWS IAM Identity Center和AWS 服务目录。这有助于简化安全、合规的多账户AWS环境的设置和治理流程。

AWS Control Tower防护机制框架包含所有基于AWS Config 规则防护机制的AWS Control Tower。

使用此框架支持您的审计准备

您可以使用 AWS Control Tower防护机制 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据基于AWS Control Tower防护机制的AWS Config 规则进行分组。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与AWS Control Tower审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于AWS Control Tower防护机制框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

AWS Control Tower防护机制框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS Control Tower 防护机制	14	0	5	AWS Config

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip 文件。

此 AWS Audit Manager 框架中的控件并不旨在验证您的系统是否符合 AWS Control Tower 防护机制。此外，他们无法保证您通过审计。

您可以在框架库 Audit Manager 的标准框架选项卡下找到AWS Control Tower防护机制框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建或更新评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于AWS Control Tower防护机制的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多AWS Control Tower资源

- AWS Control Tower服务页面
- AWS Control Tower 用户指南

AWS 生成式人工智能最佳实践框架 v1

AWS Audit Manager 提供了一个预先构建的标准框架，可帮助您了解在 Amazon Bedrock 上实现的生成式人工智能与AWS推荐的最佳实践的结合方式。

Amazon Bedrock 是一项全托管服务，可通过 API 提供来自 Amazon 和其他领先人工智能公司的人工智能模型。您可通过 Amazon Bedrock，通过组织的数据私下调整现有模型。这使您能够利用基础模型 (FM) 和大型语言模型 (LLM) 安全地构建应用程序，而不会影响数据隐私。有关更多信息，请参阅《Amazon Bedrock 用户指南》中的什么是 Amazon Bedrock？。

主题

- 什么是 Amazon Bedrock 的AWS生成式人工智能最佳实践？
- 使用此框架支持您的审计准备
- 在 Amazon Bedrock 内手动验证提示
- 更多资源

什么是 Amazon Bedrock 的AWS生成式人工智能最佳实践？

生成式人工智能是人工智能的一个分支，专注于使机器能够生成内容。生成式人工智能模型旨在创建与训练示例非常相似的输出。人工智能可在此场景下模仿人类对话，生成创意内容，分析大量数据，并自动执行通常由人类完成的流程。生成式人工智能的快速发展带来了充满希望的创新。同时，它在如何负责任地使用生成式人工智能、并遵守治理要求方面提出了新的挑战。

AWS 致力于为您提供必要的工具和指导，以负责任地构建和管理应用程序。为了帮助您实现这一目标，Audit Manager 与 Amazon Bedrock 合作创建AWS生成式人工智能最佳实践框架 v1。该框架为您提供了一个专门构建的工具，用于监控和改进 Amazon Bedrock 生成式人工智能项目的治理。您可以使用此框架中的最佳实践标准，加强对模型使用情况的控制和可见性，并随时了解模型行为。

该框架中控件是与AWS人工智能专家、合规从业人员、安全保障专家合作开发的，并听取了德勤的意见。每个自动控制都映射至一个 AWS 数据来源，Audit Manager 从中收集证据。你可以根据以下八项原则，使用收集到的证据评测您的生成式人工智能：

1. 负责 — 为生成式人工智能模型的部署和使用制定并遵守道德准则
2. 安全 — 建立明确的参数和道德界限，以防止产生有害或问题产出
3. 公平 — 考虑并尊重人工智能系统对不同用户群体的影响方式
4. 可持续 — 努力提高效率和更可持续能源
5. 弹性 — 维护完整性和可用性机制，确保人工智能系统可靠运行
6. 隐私 — 确保敏感数据免遭盗窃与泄露
7. 准确性 — 构建准确、可靠、强大的 AI 系统
8. 安全 — 防止未经授权访问生成式人工智能系统

示例

假设您的应用程序采用 Amazon Bedrock 上提供的第三方基础模型。您可以使用 AWS 生成式人工智能最佳实践框架监控您对该模型的使用情况。通过使用此框架，您可以收集证据，证明您的使用符合生成式人工智能最佳实践标准。这为您提供了一种一致的方法，以追踪模型的使用情况和权限、标记敏感数据以及收到有关任何无意披露的警报。例如，此框架中的特定控件可以收集证据，帮助您证明您已经为以下方面实施了机制：

- 记录新数据的来源、性质、质量以及处理方式，以确保透明度并帮助进行故障排除或审计（负责）
- 使用预定义的性能指标定期评测模型，以确保其符合准确和安全基准（安全）
- 使用自动监控工具实时检测潜在的偏见结果或行为并发出警报（公平）

- 评测、识别和记录模型的使用情况，以及可以重复使用现有模型的场景，无论您是否生成了模型（可持续）
- 设置在 PII 无意泄露时的通知程序（隐私）
- 建立对 AI 系统的实时监控，并针对任何异常或中断设置警报（弹性）
- 检测不准确之处，并进行彻底的错误分析以了解其根本原因（准确性）
- 按最低行业标准对 AI 模型的输入和输出数据实施端到端加密（安全）

使用此框架支持您的审计准备

> **Note**
>
> - 如果您是 Amazon Bedrock 的客户，你可以直接在 Audit Manager 中使用这个框架。确保您使用框架，并在运行生成式人工智能模型和应用的AWS 账户和区域运行评测。
> - 如果您想使用自己的 KMS 密钥对 Amazon Bedrock 的 CloudWatch 日志进行加密，请确保 Audit Manager 可访问该密钥。为此，您可以将客户管理的密钥保存在 Audit Manager 数据加密 设置。
> - 该框架使用 Amazon Bedrock ListCustomModels 操作生成有关您的自定义模型使用情况的证据。目前仅美国东部（弗吉尼亚州北部）和美国西部（俄勒冈州）AWS 区域支持 API 操作。因此，您可能无法看到有关在亚太地区（东京）、亚太地区（新加坡）或欧洲地区（法兰克福）区域使用自定义模型的证据。

您可以使用此框架帮助您为审核自己在 Amazon Bedrock 上使用生成式人工智能的情况做好准备。它包括预先构建的控件集合，其中包含描述和测试程序。根据生成式人工智能最佳实践标准，这些控件被分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架为起点，您可以创建 Audit Manager 评测并开始收集证据，以帮助您监控预期策略的合规情况。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 AWS 生成式人工智能最佳实践标准框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	控件集数量	自动控件数量	手动控件数量	范围内 AWS 服务
AWS生成式人工智能最佳实践框架 v1	8	34 全自动 18 部分自动	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 要了解有关自动控件和手动控件的更多信息，请参阅 Audit Manager 的概念和术语，查看建议何时向部分自动控件中添加手动证据的示例。
> 要查看此标准框架中用作控制数据来源映射的 AWS Config 规则，请下载AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合生成式人工智能最佳实践。此外，他们无法保证你会通过关于生成式人工智能使用情况的审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。有关如何制作此框架的可编辑副本以支持您的具体要求的说明，请参阅自定义现有框架和自定义现有控件。

在 Amazon Bedrock 内手动验证提示

您可能需要根据特定模型评测不同的提示集。在这种情况下，您可以使用InvokeModel操作评测每个提示，并收集响应作为手动证据。

使用 **InvokeModel** 操作

若要开始使用，请创建预定义提示列表。您将使用这些提示验证模型响应。请确保您的提示列表中包含所有待评测用例。例如，您可能收到提示，可用来验证模型响应是否泄露任何个人身份信息 (PII)。

创建提示列表后，使用 Amazon Bedrock 提供的 InvokeModel 操作对每个提示进行测试。然后，您可以收集模型对这些提示的响应，并将这些数据作为手动证据上传至您的 Audit Manager 评测。

该 InvokeModel 操作包含三种使用方式。

1. HTTP 请求

   你可以使用 Postman 等工具创建 InvokeModelHTTP 请求调用并存储响应。

   > **Note**
   >
   > Postman 是由第三方公司开发的，它不是由AWS 开发或支持。要了解有关使用 Postman 的更多信息，或需要帮助以解决与 Postman 相关的问题，请参阅 Postman 网站上的支持中心。

2. AWS CLI

   您可以使用 AWS CLI 运行invoke-model命令。有关说明和更多信息，请参阅 Amazon Bedrock 用户指南中的在模型上运行推理。

   以下示例展示了如何通过 *“######”* 提示和 *Anthropic Claude V2* 模型，使用 AWS CLI 生成文本。该示例在响应中最多返回 *300*个标记，并将响应保存至 *invoke-model-output.txt* 文件中：

   ```
   aws bedrock-runtime invoke-model \
            --model-id anthropic.claude-v2 \
            --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
   \"max_tokens_to_sample\" : 300}" \
            --cli-binary-format raw-in-base64-out \
            invoke-model-output.txt
   ```

3. 自动验证

您可以使用 CloudWatch Synthetics Canary 监控您的模型响应。使用此解决方案，您可以验证预定义提示列表的 `InvokeModel` 结果，然后使用 CloudWatch 监控模型对这些提示的行为。

要开始使用此解决方案，您必须先创建 Synthetics Canary。创建 Canary 后，您可以使用以下代码片段验证您的提示和模型响应。

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> 或者，您也可以使用 Lambda 函数运行此脚本。如果您选择此解决方案，则需要先 创建一个 Lambda 函数。

提示示例

您可以以这些示例提示为起点测试模型响应。在以下示例中，用您自己的数据替换*#####*，以反映您的特定测试用例。

若要测试模型回复中是否存在不当内容

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

若要测试模型响应中的 PII

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

若要测试模型响应中的污言秽语内容

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

更多资源

- Amazon Bedrock
- Amazon Bedrock 用户指南
- 将负责任人工智能从理论转变为实践
- 保护消费者和促进创新—人工智能监管和建立对负责任的人工智能的信任
- 负责任地使用机器学习指南

AWS License Manager

AWS Audit Manager提供了 AWS License Manager 框架，以帮助您做好审计准备。

主题

- 什么是 AWS License Manager？
- 使用此框架支持您的审计准备
- 更多AWS License Manager资源

什么是 AWS License Manager？

借助AWS License Manager，您可跨AWS和本地环境集中管理来自不同软件供应商（例如 Microsoft、SAP、Oracle 或 IBM）的软件许可证。将所有软件许可证置于同一位置，可以提高控制和可见性，并有可能帮助您限制许可超额，并降低违规和误报问题风险。

此AWS License Manager框架可与许可证管理器集成，可根据客户定义的许可规则汇总许可证使用信息。

使用此框架支持您的审计准备

您可以使用AWS License Manager框架帮助为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据客户定义的许可规则进行分组。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于AWS License Manager框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

AWS License Manager框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS License Manager	27	0	6	AWS License Manager

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合许可规则。此外，他们无法保证您通过许可使用审计。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于AWS License

Manager框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多AWS License Manager资源

许可证管理器链接

- AWS License Manager服务页面
- AWS License Manager 用户指南

许可证管理器 API

在此框架中，Audit Manager 使用名为`GetLicenseManagerSummary`的自定义活动来收集证据。该`GetLicenseManagerSummary` 活动调用以下三个许可证管理器 API：

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

然后，返回的数据将转换为证据，并附于评测中的相关控件中。

例如：假设您使用了两个许可产品 (SQL Service 2017 和 Oracle Database Enterprise Edition)。首先，该 `GetLicenseManagerSummary` 活动调用 ListLicenseConfigurations API，提供账户中许可证配置的详细信息。接下来，它通过调用 ListUsageForLicenseConfiguration 和 ListAssociationsForLicenseConfiguration 为每个许可证配置添加额外的上下文数据。最后，它将许可证配置数据转换为证据，并将其附加到框架中的相应控件中（4.5 —SQL Server 2017 的客户托管许可证和 3.0.4 — Oracle Database Enterprise Edition 的客户管理许可证）。如果您使用的许可产品不受框架中的任何控件保护，则该许可证配置数据将作为证据附加至以下控件中：5.0 - 其他许可证的客户托管许可证。

AWS 基础安全最佳实践

AWS Audit Manager 提供了支持 AWS 基础安全最佳实践的预先构建标准框架。

主题

- 什么是AWS基础安全最佳实践标准？
- 使用此框架支持您的审计准备

- 更多AWS基础安全最佳实践资源

什么是AWS基础安全最佳实践标准？

AWS 基础安全最佳实践标准是一组控件，用于检测部署的账户和资源偏离安全最佳实践的情况。

通过该标准，您可以持续评测所有 AWS 账户 和工作负载，以快速识别偏离最佳实践的领域。该标准针对如何改善和维护组织安全状况，提供了可操作的规范性指导。

这些控件包括来自多种 AWS 服务 的最佳实践。为每个控件分配一个类别以反映它应用于的安全功能。有关更多信息，请参阅AWS Security Hub 用户指南中的 控件类别。

使用此框架支持您的审计准备

您可以使用AWS基础安全最佳实践框架帮助您为审计做好准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 AWS 基础安全最佳实践要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 账户 中的资源和服务。它基于 AWS 基础安全最佳实践框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

AWS 基础安全最佳实践框架的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS 基础安全最佳实践	154	0	29	AWS Security Hub

此 AWS Audit Manager 框架中的控件并不旨在验证您的系统是否符合 AWS 基础安全最佳实践。此外，他们无法保证您一定会通过 AWS 基础安全最佳实践审计。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 AWS 基础安全最佳实践要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多AWS基础安全最佳实践资源

- AWS Security Hub用户指南中的AWS基础安全最佳实践标准。
- AWS Security Hub 用户指南中的控件类别

AWS 运营最佳实践

AWS Audit Manager提供了预先构建的 AWS 运营最佳实践 (OBP) 框架，以帮助您做好审计准备。该框架提供了AWS基础安全最佳实践标准中的一部分控件。这些控件可作为基准检查，以检测所部署账户和资源偏离安全最佳实践的情况。

主题

- 什么是AWS基础安全最佳实践标准？
- 使用此框架支持您的审计准备
- 更多 AWS OBP 资源

什么是AWS基础安全最佳实践标准？

您可以使用AWS基础安全最佳实践标准评测您的账户和工作负载，并快速确定偏离最佳实践的领域。该标准针对如何改善和维护组织安全状况，提供了可操作的规范性指导。

这些控件包括来自多种 AWS 服务 的最佳实践。为每个控件分配一个类别以反映它应用于的安全功能。有关更多信息，请参阅AWS Security Hub 用户指南中的 控件类别。

使用此框架支持您的审计准备

您可以使用AWS运营最佳实践框架帮助您为审计做好准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 AWS 运营最佳实践要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 账户 中的资源和服务。它基于 AWS 运营最佳实践框架中

定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

AWS 运营最佳实践框架的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS 运营最佳实践	52	0	20	AWS Security Hub

此框架中的控件并不旨在验证您的系统是否符合AWS运营最佳实践。此外，他们无法保证您一定会通过 AWS 运营最佳实践审计。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择是根据 AWS 运营最佳实践要求进行的。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 AWS OBP 资源

- AWS Security Hub用户指南中的AWS基础安全最佳实践标准。
- AWS Security Hub 用户指南中的控件类别

AWS Well-Architected

AWS Audit Manager 提供了一个预先构建的框架，该框架基于AWS最佳实践来构建 AWSWell-Architected 框架并自动进行评测。

主题

什么是 AWS Well-Architected？

AWS Well-Architected 是能够帮助您为各种应用程序和工作负载构建安全、高性能、弹性和高效基础设施的框架。AWS Well-Architected 基于六大支柱 - 卓越运营、安全性、可靠性、性能效率、成本优化和可持续性，为您和您的合作伙伴提供了评测架构和实施可扩展设计的一致方法。

使用此框架支持您的审计准备

你可以使用AWS Well-Architected 框架来帮助你为审计做准备。此框架介绍了在云中设计和运行工作负载的关键概念、设计原则与架构最佳实践。在AWS Well-Architected 所依据的六大支柱中，安全性和可靠性支柱是AWS Audit Manager提供预先构建框架和控件的支柱。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于AWS Well-Architected 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

AWS Well-Architected 框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
AWS Well-Architected 框架	16	0	2	AWS Config

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip 文件。

此框架中的控件并不旨在验证您的系统是否合规。此外，他们无法保证你会通过与AWS Well-Architected 框架相关的审计。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于AWS Well-Architected 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多AWS Well-Architected 资源

- AWS Well-Architected
- AWSWel-Architect 框架文档

加拿大网络安全中心中型云控件配置文件

AWS Audit Manager 提供了一个预先构建的标准框架，用于构建和自动化加拿大网络安全中心的评测。

主题

- 什么是加拿大网络安全中心？
- 使用此框架支持您的审计准备

什么是加拿大网络安全中心？

加拿大网络安全中心 (CCCS) 是加拿大网络安全专家指导、服务和支持的权威来源。CCCS 向加拿大政府、行业和公众提供这种专长。加拿大全国各地的公共部门组织都依靠他们对云服务提供商的严格评测，做出明智的云采购决策。

2020 年 5 月，CCCS 中型云控件配置文件取代了加拿大政府的 PROTECTED B/Medium Integrity/Medium Availability (PBMM) 配置文件。如果您的组织使用公共云服务来支持具有中等机密性、完整性和可用性 (AIC) 要求的业务活动，CCCS 中型云控件配置文件非常适合您。如工作负载为中等 AIC 要求，则意味着未经授权的披露、修改或无法访问业务活动所使用的信息或服务，可以合理地预期会对个人或组织造成严重伤害，或对一组个体造成有限伤害。伤害等级示例如下：

- 对年利润产生显著影响
- 主要账户损失
- 商誉损失
- 明显违规
- 大量侵犯隐私
- 影响程序性能
- 导致精神障碍或疾病
- 破坏活动
- 声誉受损
- 个人经济困难

使用此框架支持您的审计准备

您可以使用中型云控件配置文件的AWS Audit Manager框架，为审计做好准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 CCCS 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与 CCCS 中型云控件配置文件审计相关的证据。在评测过程中，您可以指定要包含在审计范围内的 AWS 账户 和服务。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CCCS 中型云控件配置文件框架中定义的控件。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
加拿大网络安全中心 - 中型	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip 文件。

此 AWS Audit Manager 框架中的控件不用于验证您的系统是否符合 CCCS 中型云控件配置文件标准。此外，他们无法保证你会通过 CCCS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。该选择是根据加拿大网络安全中心 — 中型框架的要求进行的。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0

AWS Audit Manager提供了两个支持 CIS AWS Foundations Benchmark v1.2.0 的预先构建框架：

- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级
- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级和 2 级

> **Note**
>
> - 有关支持 v1.3.0 的 Audit Manager 框架的信息，请参阅 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0。
> - 有关支持 v1.4.0 的 Audit Manager 框架的信息，请参阅 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0。

主题

什么是 CIS？

互联网安全中心 (CIS) 是一家非营利组织，开发了CIS AWS Foundations Benchmark. 该基准测试可作为一组AWS安全配置最佳实践。这些业界认可的最佳实践超越了现有的高级安全指南，原因是它们为您提供了清晰的分步实施和评测程序。

有关更多信息，请参阅AWS 安全博客中的 CIS AWS Foundations Benchmark 博文。

CIS 基准测试和 CIS 控件之间的区别

CIS 基准测试 是针对供应商产品的最佳安全实践指南。从操作系统到云服务和网络设备，基准测试中的设置可以保护您的组织使用的特定系统。CIS 控件是组织级系统的基本最佳实践指南，可帮助抵御已知的网络攻击媒介。

示例

- CIS 基准为规范性。它们通常引用可在供应商产品中查看和设置的具体设定。

示例：CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 确保为 “根用户” 账户启用 MFA

此建议提供以下规范性指导：如何检查这一点；如何在AWS环境中针对根账户进行设置。

- CIS 控件适用于您的整个组织。它们并不只针对单独的供应商产品。

  示例：CIS Controls v7.1 - Sub-Control 4.5 使用多因素身份验证用于所有管理员访问

  此控件描述了预计应用于您组织的内容。它没有描述您应该如何将其应用于正在运行的系统和工作负载（无论在何处）。

使用这些框架支持您的审计准备

您可以在AWS Audit Manager中使用 CIS AWS Foundations Benchmark v1.2 框架，帮助您为 CIS 审计做好准备。您还可以根据具体要求，自定义这些框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CIS 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0，1 级和 2 级	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

这些框架中的控件并不旨在验证您的系统是否符合 CIS 标准。此外，他们无法保证你会通过 CIS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到这些框架。

有关如何使用这些框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 CIS Benchmarks 的要求。如果您需要编辑这些框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义这些框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

使用这些框架的先决条件

CIS AWS Foundations Benchmark v1.2 中的很多控件的数据来源类型都是AWS Config。要支持这些控件，必须对支持 Audit Manager 的每个AWS 区域中的所有账户启用 AWS Config。您还必须确保启用了特定 AWS Config 规则，并且这些规则配置正确。

需要通过以下AWS Config规则和参数，收集正确的证据，并采集准确的 CIS AWS Foundations Benchmark v1.2 合规状态。有关如何启用或配置规则的说明，请参阅使用 AWS Config 托管规则。

必填 AWS Config 规则	必需参数
ACCESS_KEYS_ROTATED	**maxAccessKeyAge** • 不轮换天数最大值。

必填 AWS Config 规则	必需参数
	• 类型：Int • 原定设置：90 天 • 合规性要求：最长 90 天
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	不适用
CLOUD_TRAIL_ENCRYPTION_ENABLED	不适用
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	不适用
CMK_BACKING_KEY_ROTATION_ENABLED	不适用
IAM_PASSWORD_POLICY	**MaxPasswordAge** （可选） • 密码到期前的天数。 • 类型：int • 原定设置：90 • 合规性要求：最长 90 天
IAM_PASSWORD_POLICY	**MinimumPasswordLength** （可选） • 密码的最小长度。 • 类型：int • 默认值：14 • 合规性要求：至少 14 个字符
IAM_PASSWORD_POLICY	**PasswordReusePrevention** （可选） • 允许重用前的密码数。 • 类型：int • 默认值：24 • 合规性要求：重用前至少有 24 个密码

必填 AWS Config 规则	必需参数
IAM_PASSWORD_POLICY	**RequireLowercaseCharacters** （可选） • 密码中要求至少包含一个小写字符。 • 类型：布尔值 • 默认值：True • 合规性要求：至少有一个小写字符。
IAM_PASSWORD_POLICY	**RequireNumbers** （可选） • 密码中要求至少包含一个数字。 • 类型：布尔值 • 默认值：True • 合规性要求：至少包含一个数字字符
IAM_PASSWORD_POLICY	**RequireSymbols** （可选） • 密码中要求至少包含一个符号。 • 类型：布尔值 • 默认值：True • 合规性要求：至少包含一个符号字符
IAM_PASSWORD_POLICY	**RequireUppercaseCharacters** （可选） • 密码中要求至少包含一个大写字符。 • 类型：布尔值 • 默认值：True • 合规性要求：至少有一个大写字符。

必填 AWS Config 规则	必需参数
IAM_POLICY_IN_USE	**policyARN** • 要检查的 IAM policy ARN。 • 类型：字符串 • 合规性要求：通过AWS创建用于托管事件的 IAM 角色。 **policyUsageType** （可选） • 指定您希望将策略附加至用户、组还是角色。 • 类型：字符串 • 有效值：IAM_USER | IAM_GROUP | IAM_ROLE | ANY • 默认值：ANY • 合规性要求：将信任策略附加至创建的 IAM 角色
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	不适用
IAM_ROOT_ACCESS_KEY_CHECK	不适用
IAM_USER_NO_POLICIES_CHECK	不适用
IAM_USER_UNUSED_CREDENTIALS_CHECK	**maxCredentialUsageAge** • 不使用凭证天数的最大值。 • 类型：Int • 原定设置：90 天 • 合规性要求：90 天或以上
INCOMING_SSH_DISABLED	不适用
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	不适用
MULTI_REGION_CLOUD_TRAIL_ENABLED	不适用

必填 AWS Config 规则	必需参数
RESTRICTED_INCOMING_TRAFFIC	**blockedPort1** （可选） • 已阻止的 TCP 端口号。 • 类型：int • 默认值：20 • 合规性要求：确保任何安全组都不允许进入被封锁端口 **blockedPort2** （可选） • 已阻止的 TCP 端口号。 • 类型：int • 默认值：21 • 合规性要求：确保任何安全组都不允许进入被封锁端口 **blockedPort3** （可选） • 已阻止的 TCP 端口号。 • 类型：int • 默认值：3389 • 合规性要求：确保任何安全组都不允许进入被封锁端口 **blockedPort4** （可选） • 已阻止的 TCP 端口号。 • 类型：int • 默认值：3306 • 合规性要求：确保任何安全组都不允许进入被封锁端口 **blockedPort5** （可选） • 已阻止的 TCP 端口号。 • 类型：int • 默认值：4333 • 合规性要求：确保任何安全组都不允许进入被封锁端口
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	不适用

必填 AWS Config 规则	必需参数
ROOT_ACCOUNT_MFA_ENABLED	不适用
S3_BUCKET_LOGGING_ENABLED	**targetBucket** （可选） • 用于存储服务器访问日志的目标 S3 存储桶。 • 类型：字符串 • 合规性要求：支持日志记录 **targetPrefix** （可选） • 用于存储服务器访问日志的 S3 存储桶的前缀。 • 类型：字符串 • 合规性要求：标识用于 CloudTrail 日志记录的 S3 存储桶
S3_BUCKET_PUBLIC_READ_PROHIBITED	不适用
VPC_DEFAULT_SECURITY_GROUP_CLOSED	不适用
VPC_FLOW_LOGS_ENABLED	**trafficType** （可选） • 流日志的 `trafficType` 。 • 类型：字符串 • 合规性要求：启用流日志记录

更多 CIS 资源

- CIS AWS Foundations Benchmark v1.2.0
- AWS 安全博客中的CIS AWS Foundations Benchmark 博文

CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0

AWS Audit Manager提供了两个支持 CIS AWS Foundations Benchmark v1.3 的预先构建框架：

- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0，1 级

- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0，1 级和 2 级

> **Note**
>
> 有关 CIS AWS Foundations Benchmark v1.2.0 和支持此版本基准的AWS Audit Manager框架的更多信息，请参阅 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0。

主题

什么是 CIS？

互联网安全中心 (CIS) 开发了 CIS AWS Foundations Benchmark v1.3.0，这是一套用于AWS的安全配置最佳实践标准。这些业界认可的最佳实践标准超越了现有的高级安全指南，原因是它们为AWS用户提供了清晰的分步实施和评测程序。

有关更多信息，请参阅AWS 安全博客中的 CIS AWS Foundations Benchmark 博文。

CIS AWS Foundations Benchmark v1.3.0 通过强调基础的、可测试的和与架构无关的设置，为配置 AWS 服务子集安全选项提供了指南。本文档范围内的一些特定 Amazon Web Services 包括：

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service(Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud （默认）

CIS 基准测试和 CIS 控件之间的区别

CIS 基准测试是针对供应商产品的最佳安全实践标准指南。从操作系统到云服务和网络设备，基准测试中的设置可以保护您的组织使用的系统。CIS 控件是您的组织的基本最佳实践指南，可帮助抵御已知的网络攻击媒介。

示例

- CIS 基准为规范性。它们通常引用可在供应商产品中查看和设置的具体设定。

  示例：CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 确保为 “根用户” 账户启用 MFA

  此建议提供以下规范性指导：如何检查这一点；如何在AWS环境中针对根账户进行设置。
- CIS 控件适用于您的整个组织，并不只针对一个供应商产品。

  示例：CIS Controls v7.1 - Sub-Control 4.5 使用多因素身份验证用于所有管理员访问

  此控件描述了预计在组织内应用的内容，但没有说明应如何将其应用于正在运行的系统和工作负载（无论其置于何处）。

使用这些框架支持您的审计准备

您可以使用AWS Audit Manager中的 CIS AWS Foundations Benchmark v1.3 框架，帮助您为 CIS 审计做好准备。您还可以根据具体要求，自定义这些框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CIS 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0，1 级	33	5	6	• Amazon CloudWatch

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0，1 级和 2 级	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看用作这些标准框架数据来源映射的 AWS Config 规则列表，请下载以下文件：
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

这些框架中的控件并不旨在验证您的系统是否符合 CIS 标准。此外，他们无法保证你会通过 CIS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到这些框架。

有关如何使用这些框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 CIS Benchmarks 的要求。如果您需要编辑这些框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义这些框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 CIS 资源

- AWS 安全博客中的CIS AWS Foundations Benchmark 博文

CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0

AWS Audit Manager 提供了两个预先构建的标准框架，支持互联网安全中心 (CIS) AWS Foundations Benchmark v1.4.0：

- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级
- CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级和 2 级

> **Note**
>
> - 有关支持 v1.2.0 的 Audit Manager 框架的信息，请参阅 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.2.0。
> - 有关支持 v1.3.0 的 Audit Manager 框架的信息，请参阅 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.3.0。

主题

什么是 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0？

CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0（1 级和 2 级）为配置 Amazon Web Services 子集安全选项提供了规范性指导。它侧重于基础、可测试以及与架构无关的设置。本文档范围内的一些特定 Amazon Web Services 包括：

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service(Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

CIS 基准测试和 CIS 控件之间的区别

CIS 基准测试是针对供应商产品的最佳安全实践标准指南。从操作系统到云服务和网络设备，基准测试中的设置可以保护使用的系统。CIS 控件是您的组织的基本最佳实践指南，可帮助抵御已知的网络攻击媒介。

示例

- CIS 基准为规范性。它们通常引用可在供应商产品中查看和设置的具体设定。

  示例：CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 确保为 “根用户” 账户启用 MFA

  此建议提供以下规范性指导：如何检查这一点；如何在AWS环境中针对根账户进行设置。
- CIS 控件适用于您的整个组织，并不只针对一个供应商产品。

  示例：CIS Controls v7.1 - Sub-Control 4.5 使用多因素身份验证用于所有管理员访问

  此控件描述了预计应用于您组织的内容。它没有描述您应该如何将其应用于正在运行的系统和工作负载（无论在何处）。

使用这些框架支持您的审计准备

您可以使用AWS Audit Manager中的 CIS AWS Foundations Benchmark v1.4.0 框架，帮助您为 CIS 审计做好准备。您还可以根据具体要求，自定义这些框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CIS 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0，1 级和 2 级	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS Security Hub

> **Tip**
>
> 要查看用作这些标准框架数据来源映射的 AWS Config 规则列表，请下载以下文件：
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

这些框架中的控件并不是为了验证您的系统是否符合 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4.0 标准。此外，他们无法保证你会通过 CIS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到这些框架。

有关如何使用这些框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 CIS Benchmarks 的要求。如果您需要编辑这些框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义这些框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 CIS 资源

- 互联网安全中心的CIS Benchmarks
- AWS 安全博客中的CIS AWS Foundations Benchmark 博文

CIS Controls v7.1 Implementation Group 1

AWS Audit Manager 提供了支持互联网安全中心 (CIS) Controls v7.1 Implementation Group 1 的预先构建框架。

> **Note**
>
> 有关 CIS Controls v8 IG1 以及支持该标准的 AWS Audit Manager 框架的信息，请参阅CIS Controls v8 Implementation Group 1。

AWS Audit Manager提供了支持互联网安全中心 (CIS) 的预先构建框架，以帮助您做好审计准备。

主题

什么是 CIS 控件？

CIS 控件是一组按优先顺序排列的行动，它们共同构成了一套深度防御最佳实践标准。这些最佳实践标准可以缓解对系统和网络的最常见攻击。Implementation Group 1 通常是针对资源和网络安全专业知识有限、且可用于实施子控制的组织定义的。

CIS 控件和 CIS 基准之间的区别

CIS 控件是基本的最佳实践指南，组织可以遵循这些指导方针来防范已知的网络攻击媒介。CIS 基准测试是针对供应商产品的最佳安全实践标准指南。从操作系统到云服务和网络设备，基准测试中的设置可以保护使用的系统。

示例

- CIS 基准为规范性。它们通常引用可在供应商产品中查看和设置的具体设定。
  - 示例：CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 确保为 “根用户” 账户启用 MFA
  - 此建议提供以下规范性指导：如何检查这一点；如何在AWS环境中针对根账户进行设置。
- CIS 控件适用于您的整个组织，并不只针对一个供应商产品。
  - 示例：CIS Controls v7.1 - Sub-Control 4.5 使用多因素身份验证用于所有管理员访问
  - 此控件描述了预计应用于您组织的内容。它没有描述您应该如何将其应用于正在运行的系统和工作负载（无论在何处）。

使用此框架支持您的审计准备

您可以使用CIS Controls v7.1 IG1 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 CIS 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CIS Controls v7.1 IG1 框架中定义的控件。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

CIS Controls v7.1 IG1 框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Controls v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip 文件。

此框架中的控件并不旨在验证您的系统是否符合 CIS Controls。此外，他们无法保证你会通过 CIS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 CIS Controls 的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 CIS 资源

- CIS Controls v7.1 IG1

CIS Controls v8 Implementation Group 1

AWS Audit Manager 提供了支持互联网安全中心 (CIS) Controls v8 Implementation Group 1 的预先构建标准框架。

> **Note**
>
> 有关 CIS Controls v7.1 IG1 以及支持该标准的 AWS Audit Manager 框架的信息，请参阅CIS Controls v7.1 Implementation Group 1。

主题

什么是 CIS 控件？

CIS 关键安全控制（CIS Controls）是一套优先保护措施，用于缓解针对系统和网络的最常见网络攻击。它们与多项法律、监管和政策框架对应。CIS Controls v8 已得到增强，可以跟上现代系统和软件的创新步伐。向基于云的计算、虚拟化、移动性、外包、在家办公以及不断变化的攻击者策略的转变，促使了这一更新。此更新支持企业迁移至完全云和混合环境时的安全。

CIS 控件和 CIS 基准之间的区别

CIS 控件是基本的最佳实践指南，组织可以遵循这些指导方针来防范已知的网络攻击媒介。CIS 基准测试是针对供应商产品的最佳安全实践标准指南。从操作系统到云服务和网络设备，基准测试中的设置可以保护使用的系统。

示例

- CIS 基准为规范性。它们通常引用可在供应商产品中查看和设置的具体设定。
  - 示例：CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 确保为 “根用户” 账户启用 MFA
  - 此建议提供以下规范性指导：如何检查这一点；如何在AWS环境中针对根账户进行设置。
- CIS 控件适用于您的整个组织，并不只针对一个供应商产品。
  - 示例：CIS Controls v7.1 - Sub-Control 4.5 使用多因素身份验证用于所有管理员访问
  - 此控件描述了预计应用于您组织的内容。它没有描述您应该如何将其应用于正在运行的系统和工作负载（无论在何处）。

使用此框架支持您的审计准备

您可以使用CIS Controls v8 IG1框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 CIS 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 CIS Controls v8 框架中定义的控件。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

CIS Controls v8 框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
CIS Controls v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip 文件。

此框架中的控件并不旨在验证您的系统是否符合 CIS Controls。此外，他们无法保证你会通过 CIS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 CIS Controls 的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 CIS 资源

- CIS Controls v8

FedRAMP Moderate Baseline

AWS Audit Manager 提供了 FedRAMP Moderate Baseline 框架，可帮助您做好审计准备。

主题

什么是 FedRAMP？

联邦风险与授权管理计划 (FedRAMP) 成立于 2011 年。它为美国联邦政府采用和使用云服务提供了具有成本效益、基于风险的方法。FedRAMP 授权联邦机构使用现代云技术，重点是联邦信息的安全与保护。

有关 FedRAMP Moderate Baseline 控件的更多信息，请参阅FedRAMP 中等安全测试案例程序模板。

使用此框架支持您的审计准备

您可以使用 FedRAMP Moderate Baseline框架来帮助您为审计做好准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 FedRAMP 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

FedRAMP Moderate Baseline 框架的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
FedRAMP Moderate Baseline	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip 文件。

此框架中的控件并不旨在验证您的系统是否符合 FedRAMP。此外，他们无法保证你会通过 FedRAMP 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择依据 FedRAMP Moderate Baseline 要求作出。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 FedRAMP 资源

- AWSFedRAMP 合规性页面
- AWSFedRamp 博客文章

通用数据保护条例 (GDPR)

AWS Audit Manager 提供了支持《通用数据保护条例》(GDPR) 的预先构建标准框架。默认情况下，该框架仅包含手动控件。这些手动控件不会自动收集证据。但是，如果您想按 GDPR 自动收集某些控件的证据，则可以使用AWS Audit Manager中的自定义控件功能。有关更多信息，请参阅使用此框架支持您的审计准备。

主题

- 什么是《通用数据保护条例》(GDPR)？
- 使用此框架支持您的审计准备
- 更多 GDPR 资源

什么是《通用数据保护条例》(GDPR)？

《通用数据保护条例》(GDPR) 是一项新发布的欧洲隐私法，于 2018 年 5 月 25 日生效。GDPR 取代了《欧盟数据保护指令》，后者也称为第 95/46/EC 号指令。它旨在协调整个欧盟 (EU) 的数据保护法规。它通过应用对每个欧盟成员国都具有约束力的单一数据保护法，实现这一点。

GDPR 适用于在欧洲设立的组织，以及（无论是否在欧洲设立）处理欧盟数据主体个人数据的组织，涉及范围为向欧盟的数据主体提供产品或服务，或监控欧盟发生的行为。个人数据是指与已识别或可识别自然人相关的任何信息。

您可在AWS Audit Manager框架库页面找到 GDPR 框架。有关更多信息，请参阅《通用数据保护条例》(GDPR) 中心。

使用此框架支持您的审计准备

你可以使用AWS Audit Manager中的 GDPR 框架来帮助你为审计做准备。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
GDPR	0	371	10	无

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到 GDPR 框架。由于此标准框架仅包含手动控件，因此 AWS 服务 不在范围内。

> **Note**
>
> 如果你想自动收集 GDPR 证据，可以使用 Audit Manager 为 GDPR 创建自己的自定义控件。下表提供了有关 AWS 数据来源的建议，您可以在自定义控件中将这些数据来源映射至 GDPR 要求。尽管以下部分数据来源已映射至多个控件，但切记，每次资源评测仅向您收取一次费用。
>
> 以下建议使用 AWS Config 和 AWS Security Hub 作为数据来源。要成功地从这些数据来源收集证据，请确保执行以下操作：
>
> - 确认您已按说明在AWS 账户中 启用和设置 AWS Config 和 AWS Security Hub。

- 确认您已将 AWS Config 和 Security Hub 纳入范围中的服务。若要查看评测范围内的服务列表，请参阅 查看评测AWS 服务 选项卡。若要编辑此列表，请参阅在范围中编辑AWS 服务。

以这种方式设置这两项服务后，每次对指定 AWS Config 规则或 Security Hub 控件进行评测时，Audit Manager 都会收集证据。

控件名称	控件集	推荐的控件数据来源映射
第 25 条按设计和默认数据保护。1	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 • AWS CloudTrail 存储桶未公开 • 显示所有带`Allow:*:*` 的策略，列出所有使用这些策略的主体和服务 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20)

控件名称	控件集	推荐的控件数据来源映射
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12)

控件名称	控件集	推荐的控件数据来源映射
		• 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 25 条按设计和默认数据保护。2	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 • AWS CloudTrail 存储桶未公开 • 显示所有带`Allow:*:*` 的策略，列出所有使用这些策略的主体和服务 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5

控件名称	控件集	推荐的控件数据来源映射
		• 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 25 条按设计和默认数据保护。3	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 • AWS CloudTrail 存储桶未公开 • 显示所有带`Allow:*:*` 的策略，列出所有使用这些策略的主体和服务 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5

控件名称	控件集	推荐的控件数据来源映射
		• 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 30 条处理活动的记录。1	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 30 条处理活动的记录。2	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 30 条处理活动的记录。3	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 • AWS CloudTrail 存储桶未公开 • 显示所有带`Allow:*:*` 的策略，列出所有使用这些策略的主体和服务 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 30 条处理活动的记录。4	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 • AWS CloudTrail 存储桶未公开 • 显示所有带`Allow:*:*` 的策略，列出所有使用这些策略的主体和服务 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 30 条处理活动的记录。5	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 按日期显示所有根账号事件 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED 选择AWS Security Hub作为数据来源类型，然后选择以下 Security Hub 控件作为数据来源映射： • Config.1

控件名称	控件集	推荐的控件数据来源映射
第 32 条处理的安全性。1	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 显示用于所有服务的静态数据加密 • 显示用于所有服务的传输中数据加密 • Amazon S3 已启用 MFA Delete • 所有 Amazon Inspector 扫描 • 显示所有未启用 Amazon Inspector 的实例 • 显示所有在 HTTPS (SSL) 上侦听的负载均衡器 • AWS CloudTrail静态加密 • Amazon CloudWatch 会提醒 AWS Config 显示所有更改和所有已评论的设置 • 所有根活动 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

控件名称	控件集	推荐的控件数据来源映射
		• SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控件名称	控件集	推荐的控件数据来源映射
第 32 条处理的安全性。2	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 显示用于所有服务的静态数据加密 • 显示用于所有服务的传输中数据加密 • Amazon S3 已启用 MFA Delete • 所有 Amazon Inspector 扫描 • 显示所有未启用 Amazon Inspector 的实例 • 显示所有在 HTTPS (SSL) 上侦听的负载均衡器 • AWS CloudTrail静态加密 • Amazon CloudWatch 会提醒 AWS Config 显示所有更改和所有已评论的设置 • 所有根活动 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

控件名称	控件集	推荐的控件数据来源映射
		• SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控件名称	控件集	推荐的控件数据来源映射
第 32 条处理的安全性。3	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 显示用于所有服务的静态数据加密 • 显示用于所有服务的传输中数据加密 • Amazon S3 已启用 MFA Delete • 所有 Amazon Inspector 扫描 • 显示所有未启用 Amazon Inspector 的实例 • 显示所有在 HTTPS (SSL) 上侦听的负载均衡器 • AWS CloudTrail静态加密 • Amazon CloudWatch 会提醒 AWS Config 显示所有更改和所有已评论的设置 • 所有根活动 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

控件名称	控件集	推荐的控件数据来源映射
		• SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

控件名称	控件集	推荐的控件数据来源映射
第 32 条处理的安全性。4	第 4 章 - 控制者和处理者	您可以在AWS Audit Manager中创建支持此 GDPR 控件的自定义控件。 指定控件详细信息时，请在测试信息下输入以下内容： • 显示用于所有服务的静态数据加密 • 显示用于所有服务的传输中数据加密 • Amazon S3 已启用 MFA Delete • 所有 Amazon Inspector 扫描 • 显示所有未启用 Amazon Inspector 的实例 • 显示所有在 HTTPS (SSL) 上侦听的负载均衡器 • AWS CloudTrail静态加密 • Amazon CloudWatch 会提醒 AWS Config 显示所有更改和所有已评论的设置 • 所有根活动 在设置控件数据来源时，我们建议您纳入以下所有数据来源： 选择 AWS Config 作为数据来源类型，然后选择以下AWS Config托管规则作为数据来源映射： • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

控件名称	控件集	推荐的控件数据来源映射
		• SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

创建新的 GDPR 自定义控件后，您可以将它们添加至自定义 GDPR 框架。有关更多信息，请参阅 创建自定义框架 和 编辑自定义框架：您可通过自定义 GDPR 框架创建评测。这样，AWS Audit Manager 就可以自动收集您添加的自定义控件证据。有关如何使用此框架创建评测的说明，请参阅 创建评测。

更多 GDPR 资源

- 通用数据保护条例 (GDPR) 中心
- AWS GDPR 博客文章

Gramm-Leach-Bliley 法案

AWS Audit Manager 提供了支持《Gramm-Leach-Bliley 法案》(GLBA) 的预先构建框架。

主题

- 什么是《Gramm-Leach-Bliley 法案》(GLBA)？
- 使用此框架支持您的审计准备

什么是《Gramm-Leach-Bliley 法案》(GLBA)？

《Gramm-Leach-Bliley 法案》(GLB 法案或 GLBA)，也称为《1999 年金融服务现代化法》，是美国颁布的一项联邦法律，旨在控制金融机构处理个人信息的方式。该法案包含三个部分。第一部分是金融隐私规则，它规范了私人财务信息的收集与披露。第二部分是保障规则，它规定金融机构必须实施安全计划保护此类信息。第三部分是借口条款，它禁止借口（使用虚假借口访问私人信息）的行为。该法规还要求金融机构向客户提供书面隐私声明，解释其信息共享做法。

使用此框架支持您的审计准备

你可以使用 Gramm-Leach-Bliley 法案 (GLBA) 框架帮助为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 GLBA 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以 GLBA 框架作为起点，您可以创建 Audit Manager 评测并开始收集与 GLBA 审计相关的证据。在评测过程中，您可以指定要包含在审计范围内的 AWS 账户 和服务。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 GLBA 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

GLBA 框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
《Gramm-Leach-Bliley 法案》(GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_GLBA.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 GLBA 标准。此外，他们无法保证你会通过 GLBA 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到 GLBA 框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 GLBA 的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

GxP 21 CFR 第 11 部分

AWS Audit Manager 基于AWS最佳实践标准，提供了支持 GxP CFR 第 11 部分法规的预先构建框架。

> **Note**
>
> 有关 GxP 欧盟附录 11 以及支持附件的 Audit Manager 框架的信息，请参阅 GxP 欧盟附录 11。

主题

什么是 GxP CFR 第 11 部分？

GxP 是适用于生产食品和医疗产品的生命科学组织的法规和指导方针。适用范围内的医疗产品包括药品、医疗器械和医疗软件应用程序。GxP 要求的总体目的是确保食品和医疗产品对消费者而言是安全的。这也是为了确保用于产品相关安全决策数据的完整性。

GxP 一词包含一系列与合规性相关的活动。其中包括良好实验室规范 (GLP)、良好临床规范 (GCP) 以及良好生产规范 (GMP)。这些不同类型的活动都涉及生命科学组织必须实施的、特定产品要求。这取决于组织生产的产品类型以及其产品的销售国家。当生命科学组织使用计算机化系统执行某些 GxP 活动时，他们必须确保计算机化 GxP 系统的开发、验证和运行符合系统预期用途要求。

有关在 GxP 系统中使用 AWS 云的全面方法，请参阅《在 GxP 系统中使用AWS产品的注意事项》白皮书。

使用此框架支持您的审计准备

您可以使用GxP 21 CFR 第 11 部分 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 GxP 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 GxP 21 CFR 第 11 部分框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

GxP CFR 第 11 部分框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
GxP 21 CFR 第 11 部分	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 GxP 法规。此外，他们无法保证你会通过 GxP 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 GxP CFR 第 11 部分框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 GxP 资源

- AWSGxP 合规性页面
- 在 GxP 系统中使用AWS 产品的注意事项

GxP 欧盟附录 11

AWS Audit Manager 基于AWS最佳实践标准，提供了支持 GxP 欧盟附录 11 法规的预先构建框架。

> **Note**
>
> 有关 GxP 21 CFR 第 11 部分及支持它的 Audit Manager 框架的信息，请参阅 GxP 21 CFR 第 11 部分。

主题

什么是 GxP 欧盟附录 11？

GxP 欧盟附录 11 框架与美国的 FDA 21 CFR 第 11 部分框架类似。此附录适用于良好生产规范 (GMP) 监管活动包含的、所有形式的计算机化系统。计算机化系统是一组软件和硬件组件，共同实现某些功能。应验证应用程序，并对 IT 基础架构认证。当计算机化系统取代手动操作时，不应因此而降低产品质量、过程控制或质量保证。不应增加这一过程的总体风险。

附录 11 是欧洲 GMP 指南的一部分，它定义了制药行业组织使用的计算机化系统的职权范围。附录 11 可用作检查清单，使欧洲监管机构能够确定与药品和医疗器械相关的计算机化系统的要求。欧盟委员会制定的指导方针与美国食品和药物管理局 FDA (21 CFR Part 11) 类似。附录 11 界定了电子记录和电子签名托管标准。

使用此框架支持您的审计准备

您可以使用GxP 欧盟附录 11 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 GxP 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 GxP 欧盟附录 11 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

GxP 欧盟附录 11 框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
GxP 欧盟附录 11	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip 文件。

此框架中的控件并不旨在验证您的系统是否符合 GxP 欧盟附录 11 的要求。此外，他们无法保证你会通过 GxP 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 GxP 欧盟附录 11 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

健康保险流通与责任法案 (HIPAA) 2003 年安全规则

AWS Audit Manager 提供了支持 HIPAA 规则的预先构建框架，可帮助您做好审计准备。

> **Note**
>
> 该框架以前在框架库内被命名为 HIPAA。2023 年 3 月 8 日，我们将该框架的名称更新为 2003 HIPAA 安全规则，以将其与 2013 HIPAA 最终综合安全规则区分开来。
> 有关 2013 HIPAA 最终综合安全规则和支持该标准的 Audit Manager 框架的信息，请参阅《健康保险流通与责任法案》(HIPAA) 2013 最终综合安全规则。

主题

什么是 HIPAA 和 2003 HIPAA 安全规则？

《1996 年健康保险流通与责任法案》(HIPAA) 是一项立法，旨在帮助美国工人在跳槽或失业时保留健康保险。该立法还寻求鼓励电子健康记录，通过改善信息共享来提高美国医疗保健系统的效率和质量。

除了越来越多地使用电子病历外，HIPAA 还包括保护受保护健康信息 (PHI) 安全和隐私的规定。PHI 包括大量可识别个人身份的健康与健康相关数据。包括保险和账单信息、诊断数据、临床护理数据以及实验室结果，例如图像和测试结果。

美国卫生与公共服务部于 2003 年 2 月发布了最终 安全规则。该规则为受保护的电子健康信息的机密性、完整性和可用性设定了国家标准。

HIPAA 规则适用于受保实体。其中包括医院、医疗服务提供商、雇主赞助的健康计划、研究机构，以及直接接触患者和患者数据的保险公司。HIPAA 保护 PHI 的要求也延伸至商业伙伴。

有关 HIPAA 和 HITECH 如何保护健康信息的更多信息，请参阅美国卫生与公众服务部的健康信息隐私网页。

越来越多的医疗保健提供商、付款人和 IT 专业人员正在使用AWS公用事业云服务处理、存储和传输受保护的医疗信息 (PHI)。AWS使受 HIPAA 约束的相关实体及其业务伙伴能够使用安全 AWS 环境处理、维护和存储受保护的健康信息。

有关如何使用AWS处理和存储运行状况信息的说明，请参阅Amazon Web Services 上的 HIPAA 安全性和合规性架构白皮书。

使用此框架支持您的审计准备

您可以使用 2003 HIPAA 安全规则 框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 HIPAA 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 HIPAA 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

2003 HIPAA 安全规则框架的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
2003 年 HIPAA 安全规则	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 HIPAA 标准。此外，他们无法保证你会通过 HIPAA 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 HIPAA 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 HIPAA 资源

- 美国卫生与公众服务部的健康信息隐私
- 美国卫生与公众服务部的安全规则
- Amazon Web Services 上的 HIPAA 安全性和合规性架构
- AWSHIPAA 的合规性页面

《健康保险流通与责任法案》(HIPAA) 2013 最终综合安全规则

AWS Audit Manager 提供了支持 HIPAA 规则的预先构建框架，可帮助您做好审计准备。

> **Note**
>
> 有关 2003 HIPAA 安全规则和支持该标准的AWS Audit Manager 框架的信息，请参阅健康保险流通与责任法案 (HIPAA) 2003 年安全规则。

主题

什么是 HIPAA 和 HIPAA 最终综合安全规则？

《1996 年健康保险流通与责任法案》(HIPAA) 是一项立法，旨在帮助美国工人在跳槽或失业时保留健康保险。该立法还寻求鼓励电子健康记录，通过改善信息共享来提高美国医疗保健系统的效率和质量。

除了越来越多地使用电子病历外，HIPAA 还包括保护受保护健康信息 (PHI) 安全和隐私的规定。PHI 包括大量可识别个人身份的健康与健康相关数据。包括保险和账单信息、诊断数据、临床护理数据以及实验室结果，例如图像和测试结果。

HIPAA 最终综合安全规则于 2013 年生效，对先前通过的所有规则提出了多项更新。对“安全、隐私、违规通知”和“执法规则”的修改，旨在增强数据共享的保密性和安全性。

HIPAA 规则适用于受保实体。其中包括医院、医疗服务提供商、雇主赞助的健康计划、研究机构，以及直接接触患者和患者数据的保险公司。根据综合更新，适用于受保实体的许多 HIPAA 规则现在也适用于商业伙伴。

有关 HIPAA 和 HITECH 如何保护健康信息的更多信息，请参阅美国卫生与公众服务部的健康信息隐私网页。

越来越多的医疗保健提供商、付款人和 IT 专业人员正在使用AWS公用事业云服务处理、存储和传输受保护的医疗信息 (PHI)。AWS使受 HIPAA 约束的相关实体及其业务伙伴能够使用安全 AWS 环境处理、维护和存储受保护的健康信息。有关如何使用AWS处理和存储运行状况信息的说明，请参阅Amazon Web Services 上的 HIPAA 安全性和合规性架构白皮书。

使用此框架支持您的审计准备

您可以使用 2013 HIPAA 最终综合安全规则 框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 HIPAA 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 HIPAA 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

2013 HIPAA 最终综合安全规则框架的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
2013 HIPAA 最终综合安全规则	39	46	5	• Amazon Elastic Compute Cloud

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 HIPAA 标准。此外，他们无法保证你会通过 HIPAA 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 HIPAA 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 HIPAA 资源

- 美国卫生与公众服务部的健康信息隐私
- 美国卫生与公共服务部的综合 HIPAA 规则制定
- Amazon Web Services 上的 HIPAA 安全性和合规性架构

- AWSHIPAA 的合规性页面

ISO/IEC 27001:2013 附录 A

AWS Audit Manager 提供了预先构建的标准框架，用于自动化构建 ISO/IEC 27001:2013 附录 A 的评测。

主题

- 什么是 ISO/IEC 27001:2013 附录 A？
- 使用此框架支持您的审计准备
- 更多 ISO/IEC 27001:2013 附录 A 资源

什么是 ISO/IEC 27001:2013 附录 A？

国际电工委员会 (IEC) 和国际标准化组织 (ISO) 都是独立的非政府非营利组织，它们负责制定和发布完全基于共识的国际标准。

ISO/IEC 27001:2013 附录 A 是一项安全管理标准，它规定了遵循 ISO/IEC 27002 最佳实践标准指南的安全管理最佳实践和全面的安全控制措施。这项国际标准规定了如何在您的组织中建立、实施、维护和持续改进信息安全管理系统要求。这些标准中包括针对贵组织需求量身定制的信息安全风险评测与处理要求。该国际标准中包含一般性要求，旨在适用于所有组织，无论其类型、规模或性质如何。

使用此框架支持您的审计准备

您可以使用 ISO/IEC 27001:2013 附录 A 的 AWS Audit Manager 框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 ISO/IEC 27001:2013 附录 A 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与 ISO/IEC 27001:2013 附录 A 审计相关的证据。在评测过程中，您可以指定要包含在审计范围内的 AWS 账户 和服务。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 ISO/IEC 27001:2013 附录 A 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
ISO-IEC 27001:2013 附录 A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合此国际标准。此外，他们无法保证你会通过 ISO/IEC 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到ISO/IEC 27001:2013 附录 A 框架。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 ISO-IEC 27001:2013 附录 A 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何使用此框架创建评测的说明，请参阅 创建评测。有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 ISO/IEC 27001:2013 附录 A 资源

- 有关该国际标准的更多信息，请参阅 ANSI Webstore 的 ISO/IEC 27001:2013。

NIST 800-53 (第 5 版) Low-Moderate-High

AWS Audit Manager 提供了一个预先构建的框架，该框架基于AWS最佳实践来构建 NIST 800-53 合规性标准并自动进行评测。

> **Note**
>
> - 有关支持NIST 800-171的 Audit Manager 框架的信息，请参阅NIST SP 800-171 (第 2 版)。
> - 有关支持 NIST 网络安全框架的 Audit Manager 框架的信息，请参阅 NIST Cybersecurity Framework 1.1 版。

主题

什么是 NIST 800-53？

美国国家标准与技术研究所 (NIST) 成立于 1901 年，现在隶属于美国商业部。NIST 是美国历史最悠久的物理科学实验室之一。美国国会成立该机构旨在改善当时的二流测量基础设施。基础设施落后于英国和德国等经济大国，是美国工业竞争力面临的主要挑战。

NIST 800-53 安全控件通常适用于美国联邦信息系统。这些系统通常必须经过正式的评测与授权流程。此过程可确保充分保护信息和信息系统的机密性、完整性以及可用性。这取决于系统的安全类别和影响级别（低、中或高），以及风险确定性。安全控件从 NIST SP 800-53 安全控件目录中选择，系统是根据这些安全控件要求进行评测。

NIST 800-53（第 5 版）Low-Moderate-High 框架代表了 NIST SP 800-53 第 5 版中为联邦信息系统和组织推荐的安全控件和相关评测程序。有关本 NIST SP 800-53 框架与最新发布的 NIST 特别出版物 SP 800-53 第 5 版之间的任何差异，请参阅NIST 计算机安全资源中心发布的官方文档。

使用此框架支持您的审计准备

您可以使用 NIST 800-53（第 5 版）Low-Moderate-High 框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 NIST 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 NIST 800-53（第 5 版）Low-Moderate-High 框架中定义的控件来执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

NIST 800-53（第 5 版）Low-Moderate-High 框架的详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
NIST 800-53 (第 5 版) Low-Moderate-High	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 NIST 标准。此外，他们无法保证你会通过 NIST 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 NIST 800-53（第 5 版）Low-Moderate-High 框架的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 NIST 资源

- 美国国家标准与技术研究院 (NIST)
- NIST 计算机安全资源中心
- AWSNIST 合规性页面

NIST Cybersecurity Framework 1.1 版

AWS Audit Manager 提供了一个预先构建的框架，该框架基于AWS最佳实践来构建 NIST Cybersecurity Framework 框架并自动进行评测。

> **Note**
>
> - 有关支持 NIST 800-53 (第 5 版) Low-Moderate-High的 Audit Manager 框架的信息，请参阅 NIST 800-53 (第 5 版) Low-Moderate-High。
> - 有关支持 NIST SP 800-171 (第 2 版)的 Audit Manager 框架的信息，请参阅 NIST SP 800-171 (第 2 版)。

主题

- 什么是 NIST Cybersecurity Framework？
- 使用此框架支持您的审计准备
- 更多 NIST 资源

什么是 NIST Cybersecurity Framework？

美国国家标准与技术研究所 (NIST) 成立于 1901 年，现在隶属于美国商业部。NIST 是美国历史最悠久的物理科学实验室之一。美国国会成立该机构旨在改善当时的二流测量基础设施。基础设施落后于英国和德国等经济大国，是美国工业竞争力面临的主要挑战。

美国依赖于关键基础设施的可靠运行。网络安全威胁利用了关键基础设施系统日益增加的复杂性与互连性。它们使美国的安全、经济、公共安全以及健康处于危险之中。与财务和声誉风险类似的是，网络安全风险会影响公司利润。它会推高成本并影响收入。它可能会损害组织创新以及赢得和维护客户的能力。最终，网络安全可扩大组织的整体风险管理。

NIST Cybersecurity Framework (CSF) 得到了全球政府和行业的支持，是任何组织使用的推荐基准，无论其行业或规模如何。NIST Cybersecurity Framework 主要由三个部分组成：框架核心、配置文件和实施层。框架核心包含所需的网络安全活动和成果，这些活动和结果分为 23 个类别，涵盖了组织网络安全目标的广度。这些配置文件包含组织的要求和目标、风险偏好、以及使用框架核心的预期结果资源的独特一致性。实施层描述了组织的网络安全风险管理实践对于框架核心定义特点的用处。

使用此框架支持您的审计准备

您可以使用 NIST Cybersecurity Framework 1.1 版帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 NIST CSF 要求分组为控件集。Audit Manager 目前通过提供 56 个自动控件和 52 个手动控件，支持框架核心组件。这些控件与框架核心中定义的 23 个网络安全类别相匹配。Audit Manager 不支持此框架中的配置文件与实施组件。

您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 NIST Cybersecurity Framework 1.1 版中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

NIST Cybersecurity Framework 1.1 版的详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
NIST Cybersecurity Framework 1.1 版	56	52	23	• AWS Config

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip 文件。

Audit Manager 提供的控件并不是为了验证您的系统是否符合 NIST Cybersecurity Framework。此外，他们无法保证你会通过 NIST Cybersecurity 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择依据 NIST Cybersecurity Framework 1.1 版要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 NIST 资源

- 美国国家标准与技术研究院 (NIST)
- NIST 计算机安全资源中心
- AWSNIST 合规性页面
- NIST Cybersecurity Framework — 与AWS云端的 NIST CSF 保持一致

NIST SP 800-171 (第 2 版)

AWS Audit Manager 提供了一个预先构建的框架，该框架基于AWS最佳实践构造和自动执行 NIST SP 800-171 合规标准评测。

> **Note**
>
> - 有关支持 NIST 800-53 (第 5 版) Low-Moderate-High 的 Audit Manager 框架的信息，请参阅 NIST 800-53 (第 5 版) Low-Moderate-High。
> - 有关支持 NIST Cybersecurity Framework 1.1 版的 Audit Manager 框架的信息，请参阅 NIST Cybersecurity Framework 1.1 版。

主题

什么是 NIST SP 800-171？

NIST SP 800-171 重点保护非联邦系统和组织中受控非机密信息 (CUI) 的机密性。它对实现该目标提出了具体安全要求。NIST 800-171 标准概述了非联邦组织在其网络中处理 CUI 信息的必要安全和实践标准。它由 美国国家标准与技术研究所 (NIST) 于 2015 年 6 月首次出版。NIST 是美国政府机构，它发布了多项标准和出版物，旨在增强公共和私营部门的网络安全应变能力。根据新出现的网络威胁和不断变化的技术，NIST 800-171 定期更新。最新版本 (第 2 版) 已于 2020 年 2 月发布。

NIST 800-171 中的网络安全控件可保护政府承包商和分包商 IT 网络中的 CUI。它定义了政府承包商在其网络处理或存储 CUI 时必须遵守的做法与程序。NIST 800-171 仅适用于承包商网络中存在 CUI 的部分。

使用此框架支持您的审计准备

您可以使用 NIST SP 800-171 第 2 版 框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 NIST 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 NIST SP 800-171 第 2 版框架中定义的控

件来执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

NIST SP 800-171 第 2 版框架的详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
NIST SP 800-171 第 2 版	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 NIST 800-171。此外，他们无法保证你会通过 NIST 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于

NIST SP 800-171 第 2 版框架的要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 NIST 资源

- 美国国家标准与技术研究院 (NIST)
- NIST 计算机安全资源中心
- AWSNIST 合规性页面

PCI DSS V3.2.1

AWS Audit Manager 提供了支持 PCI DSS v3.2.1 的预先构建框架。

> **Note**
>
> 有关 PCI DSS v4 和支持该标准的 Audit Manager 框架的信息，请参阅 PCI DSS V4.0。

主题

- 什么是 PCI DSS？
- 使用此框架支持您的审计准备
- 更多 PCI DSS 资源

什么是 PCI DSS？

支付卡行业数据信息安全标准 (PCI DSS) 是一种专有信息安全标准。它由PCI 安全标准委员会管理，该委员会由 American Express、Discover Financial Services、JCB International、 MasterCard Worldwide 和 Visa Inc. 共同创立。PCI DSS 适用于存储、处理或传输持卡人数据 (CHD) 或敏感身份验证数据 (SAD) 的实体。这包括但不限于商家、处理方、收购方、发行人和服务提供商。PCI DSS 由多家支付卡品牌联合制定，由支付卡行业安全标准委员会管理。

AWS 已获得 PCI DSS 1 级服务提供商认证，这是现有的最高评测级别。合规评测由独立的合格安全评测机构 (QSA) Coalfire Systems Inc. 执行。PCI DSS 合规证明 (AOC) 和责任摘要可通过AWS Artifact

获得。这是一项自助服务门户，用于按需访问 AWS 合规报告。登录 AWS Artifact 管理控制台中的 AWS，或在 AWS Artifact入门了解更多。

您可以从 PCI 安全标准委员会文档库中下载 PCI DSS 标准。

使用此框架支持您的审计准备

您可以使用PCI DSS V3.2.1 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 PCI DSS 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于 PCI DSS V3.2.1 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

PCI DSS V3.2.1 框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 PCI DSS 标准。此外，他们无法保证你会通过 PCI DSS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。原因是 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于 PCI DSS V3.2.1 框架要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 PCI DSS 资源

- PCI 安全标准委员会
- PCI 安全标准委员会文档库。
- AWSPCI DSS 合规性页面

PCI DSS V4.0

AWS Audit Manager 提供了支持支付卡行业数据安全标准（PCI DSS）v4.0 的预构建框架。

> **Note**
>
> 有关 PCI DSS v3.2.1，以及支持该标准的 Audit Manager 框架的信息，请参阅 PCI DSS V3.2.1。

主题

- 什么是 PCI DSS？
- 使用此框架支持您的审计准备
- 更多 PCI DSS 资源

什么是 PCI DSS？

支付卡行业数据安全标准（PCI DSS）是一项全球标准，为保护支付数据提供了技术和操作要求的基准。PCI DSS v4.0 是该标准的升级。

PCI DSS 的开发旨在提高和加强支付卡账户数据的安全性。该标准还有助于在全球范围内广泛采用一致的数据安全措施。并提供了旨在保护账户数据的技术和操作要求的基准。虽然 PCI DSS 是专门针对支付卡账户数据环境而设计的，但您也可以使用 PCI DSS 来抵御威胁，保护支付生态系统中的其他元素。

PCI 安全标准委员会（PCI SSC）在 PCI DSS v3.2.1 和 v4.0 之间进行了多次更改。这些更新分为三类：

1. 不断变化的要求：为确保标准与新出现的威胁和技术，以及支付行业的变化保持一致而进行的更改。例如，新增或修改要求或测试程序，或删除要求。
2. 澄清或指南：对措辞、解释、定义、其他指南或说明的更新，以加深对特定主题的理解或提供进一步的信息或指南。
3. 结构或格式：内容重组，包括对要求进行组合、分离和重新编号，以使内容保持一致。

有关更改的更多信息，请参阅 PCI DSS 版本 3.2.1 至 4.0 的更改摘要。

使用此框架支持您的审计准备

> **Note**
>
> 此标准框架使用来自 Security Hub 的合并控件作为数据来源。要从合并控件中成功收集证据，确保在 Security Hub 中打开了合并控件结果设置。有关使用 Security Hub 作为数据来源类型的更多信息，请参阅 AWS Audit Manager 支持的 AWS Security Hub 控件。

您可以使用 PCI DSS V4.0 框架来帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 PCI DSS V4.0 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。Audit Manager 基于 PCI DSS V4.0 框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找

器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa l Database Service • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config

AWS Audit Manager 中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
				• AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> 要查看此标准框架中用作数据来源映射的 AWS Config 规则，请下载 AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否符合 PCI DSS 标准。此外，他们无法保证你会通过 PCI DSS 审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。这一选择是根据 PCI DSS V4 框架的要求而做出。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 PCI DSS 资源

- PCI DSS v4.0 资源中心
- PCI 安全标准委员会
- PCI 安全标准委员会文档库。

- AWSPCI DSS 合规性页面
- AWS 支付卡行业数据安全标准（PCI DSS）v4.0 合规指南
- PCI DSS 版本 3.2.1 至 4.0 的更改摘要

SOC 2

SOC 2 是一种审计程序，可确保公司的数据得到安全托管。 AWS Audit Manager 提供了支持 SOC 2 的预先构建框架。

主题

- 什么是 SOC 2？
- 使用此框架支持您的审计准备
- 更多 SOC 2 资源

什么是 SOC 2？

系统和组织控制 (SOC) 由美国注册会计师协会 (AICPA) 定义，是审计期间生成的一组报告的名称。它旨在供服务组织（向其他组织提供信息系统即服务的组织）使用，向这些服务的用户发布可靠的信息系统内部控制报告。这些报告侧重于分为五类的控制，即信托服务原则。

AWSSOC 报告是独立的第三方检查报告，阐明AWS如何达成关键合规性控制和目标。这些报告的目的是帮助您和您的审计员理解旨在支持运营和合规性的 AWS 控制措施。包含五份 AWS SOC 报告：

- AWSSOC 1 报告，AWS 客户可从AWS Artifact中获得。
- AWSSOC 2 安全、可用性和机密性报告，可供AWS客户从AWS Artifact中获得。
- AWSSOC 2 安全、可用性和机密性报告，可供AWS客户从AWS Artifact中获得（范围仅包括 Amazon DocumentDB）。
- AWSSOC 2 第一类隐私报告，可供AWS客户从AWS Artifact中获得。
- AWSSOC 3 安全、可用性和机密性报告，以白皮书的形式公开发布。

使用此框架支持您的审计准备

您可以使用此框架帮助您为审计做准备。框架包括预先构建的控件集合，其中包含描述和测试程序。这些控件根据 SOC 2 要求分组为控件集。您还可以根据具体要求，自定义此框架及其控件，以支持内部审计。

以该框架作为起点，您可以创建 Audit Manager 评测并开始收集与您的审计相关的证据。创建评测后，Audit Manager 会开始评测您的 AWS 资源。它基于框架中定义的控件执行此操作。当需要进行审计时，您或您选择的委托人可以查看 Audit Manager 收集的证据。或者，您可浏览评测的证据文件夹，然后选择要将哪些证据纳入评测报告。或者，如果启用了证据查找器，则可以搜索特定证据并将其以 CSV 格式导出，或根据搜索结果创建评测报告。无论采用哪种方式，此评测报告可帮助您证明您的控件是否按预期运行。

框架详细信息如下：

AWS Audit Manager中的框架名称	自动控件数量	手动控件数量	控件集数量	范围内 AWS 服务
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 要查看此标准框架中的数据来源映射AWS Config规则，请下载 AuditManager_ConfigDataSourceMappings_SOC2.zip 文件。

此AWS Audit Manager框架中的控件并不旨在验证您的系统是否合规。此外，他们无法保证你会通过审计。 AWS Audit Manager不会自动检查需要手动收集证据的程序控件。

您可以在 Audit Manager 中框架库的 标准框架选项卡下找到此框架。

有关如何使用此框架创建评测的说明，请参阅 创建评测。

当您使用 Audit Manager 控制台从标准框架创建评测时，范围内的AWS 服务列表默认为预先选择且无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择依据 SOC 2 要求。如果您需要编辑此框架范围内的服务列表，则可以使用 CreateAssessment 或 UpdateAssessment API 操作执行。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

有关如何自定义此框架以支持您特定要求的说明，请参阅自定义现有框架和自定义现有控件。

更多 SOC 2 资源

- AWSSOC 合规性页面

控件库

您可以从 Audit Manager 的控件库中访问和管理控件。您可以随时通过在 Audit Manager 控制台的导航窗格中选择控件库来访问控件库。

控件库包含标准控件和自定义控件的目录。

- 标准控件是由 AWS提供的预定义控件。您可查看标准控件的配置详细信息，但不能对其进行编辑或删除。但是，您可以自定义任何标准控件，以创建满足您的特定要求的新控件。
- 自定义控件是您拥有和定义的定制控件。使用自定义控件，您可以指定要从哪些数据来源收集证据。然后，您可以向自定义框架添加自定义控件。

  要详细了解如何向自定义框架添加自定义控件，请参阅 框架库。要详细了解如何通过 Audit Manager 框架创建评测，请参阅 AWS Audit Manager中的评测。

本节介绍如何在 Audit Manager 中创建和管理自定义控件。

主题

访问 AWS Audit Manager中的可用控件

您可以在 Audit Manager 控制台的控件库页面查看所有可用控件。在这里，您还可以创建自定义控件或自定义现有控件。

您还可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 查看所有可用的控件。

Audit Manager console

查看可用控件（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库。
3. 选择标准控件选项卡或自定义控件选项卡，以浏览可用控件。
4. 选择控件名称，以查看该控件的详细信息。

AWS CLI

查看可用控件 (AWS CLI)

运行 list-controls 命令并指定 `--control-type`。您可以检索标准控件列表，或检索自定义控件列表。

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

查看可用控件 (API)

使用ListControls操作并指定控制类型。您可以返回标准控件列表，或返回自定义控件列表。

如需了解更多信息，请选择前面的链接之一，在 AWS Audit Manager API 参考中阅读更多内容。这包括有关如何使用某个特定语言 AWS 的 SDK 中的`ListControls`操作和参数的信息。

查看控件的详细信息

您可以通过 Audit Manager 控制台、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 查看控件的详细信息。

Audit Manager console

要查看控件详细信息（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库以查看可用控件列表。
3. 选择标准控件选项卡或自定义控件选项卡，以浏览可用控件。
4. 选择控件名称，以查看该控件的详细信息。

当您打开控件时，会看到一个控件详细信息页面。本页各个部分及其内容如下所述。

摘要部分

本部分提供控件概述。其中包含以下信息：

- 控件名称 - 控件的名称。
- 控件类型 - 指定控件是标准控件还是自定义控件。
- 标签 - 与控件关联的标签数量。
- 数据来源类型 - 用于此控件的数据来源类型的数量。
- 映射 - 用于从数据来源检索数据的映射属性的数量。

如果您正在查看自定义控件，将显示以下详细信息：

- 创建者 - 创建自定义控件的账户。
- 创建日期 - 创建自定义控件的日期。
- 上次更新时间 - 上次编辑自定义控件的日期。

详细信息选项卡

此选项卡提供了控件的基本概述。其中包含以下信息：

- 描述部分提供了控件的描述。
- 测试信息部分描述了该控件的推荐测试程序。
- 行动计划部分描述了在控件需要纠正时应采取的建议操作。

数据来源选项卡

此选项卡显示有关控件数据来源的信息。其中包含以下信息：

- 数据来源名称 - 这仅适用于自定义控件。它指的是您为每个数据来源提供的描述性名称。您可以通过此名称区分属于相同数据来源类型的多个数据来源。

- 数据来源类型 - 指定了证据数据的来源。
  - 如果 Audit Manager 收集证据，则数据来源为以下四种类型之一：AWS Security Hub、AWS Config、AWS CloudTrail 或 AWS API 调用。
  - 如果您上传自己的证据，则数据来源类型为手动。描述说明所需的手动证据是文件上传还是文字回复。
- 映射 - 用于识别和检索数据来源中数据的映射属性。
  - 如果数据源类型为 AWS Config，则映射为特定 AWS Config 规则的名称（例如，`EC2_INSTANCE_MANAGED_BY_SSM`）。Audit Manager 使用此映射直接从中报告该规则检查的结果 AWS Config。
  - 如果数据源类型为 AWS Security Hub，则映射为特定 Security Hub 控件的名称（例如，`1.1 – Avoid the use of the "root" account`）。Audit Manager 使用此映射直接报告来自 Security Hub 的安全检查结果。
  - 如果数据源类型为 AWS API 调用，则映射为特定 API 调用的名称（例如`ec2_DescribeSecurityGroups`）。Audit Manager 使用此映射收集 API 响应。
  - 如果数据源是 AWS CloudTrail，则映射为特定 CloudTrail 事件的名称（例如，`CreateAccessKey`）。Audit Manager 使用此映射从您的 CloudTrail 日志中收集相关的用户活动。
- 频率 - 它指定 Audit Manager 从数据来源收集证据的频率。频率因数据来源类型而异。有关更多信息，请选择列中的值或参见 证据收集频率。

标签选项卡

此选项卡列出与控件关联的标签。其中包含以下信息：

- 键 - 标签密钥（如合规性标准、法规或类别）。
- 值 - 标签值。

AWS CLI

要查看控件详细信息 (AWS CLI)

1. 要识别您要查看的控件，请运行 list-controls 命令并指定 `--control-type`。您可以检索标准控件列表，或检索自定义控件列表。

   在以下示例中，将`#####`替换为 `Custom` 或 `Standard`。

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

响应返回控件列表。找到您要查看的控件，并记下控件 ID 和 Amazon 资源名称（ARN）。

2. 要获取控件的详细信息，请运行 get-control 命令并指定 `--control-id`。

   在以下示例中，将*#####*替换为您自己的信息。

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   控制详细信息以 JSON 格式返回。若要了解此数据，请参见 AWS CLI 命令参考中的 get-control 输出。

3. 要查看控件的标签，请使用list-tags-for-resource命令`--resource-arn`并为控件指定。

   在以下示例中，将*#####*替换为您自己的信息：

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   有关 Audit Manager 中标签的更多信息，请参阅标签 AWS Audit Manager 资源。

Audit Manager API

要查看控件详细信息 (API)

1. 要确定要查看的控件，请使用ListControls操作并指定 controlType。您可以返回标准控件列表，或返回自定义控件列表。

   在响应中找到您要查看的控件，并记下控件 ID 和 Amazon 资源名称（ARN）。

2. 要获取控制细节，请使用GetControl操作。在请求中，指定您从第 1 步中获得的 controlId。

   控制详细信息以 JSON 格式返回。要了解这些数据，请参阅 AWS Audit Manager API 参考中的GetControl 响应元素。

3. 要查看控件的标签，请使用ListTagsForResource操作。在请求中，指定您从第 1 步中获得的 resourceArn。

有关 Audit Manager 中标签的更多信息，请参阅标签 AWS Audit Manager 资源。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit Manager API 参考中阅读更多内容。其中包括有关如何在某个特定语言 AWS 的 SDK 中使用这些操作和参数的信息。

创建自定义控件

您可以使用自定义控件从您定义的特定数据来源收集证据。

就像标准控件一样，自定义控件在您的评测中处于活动状态时会持续收集证据。您还可以向您创建的任何自定义控件添加手动证据。每份证据都变成了一份记录，帮助您证明遵守了自定义控件的要求。

首先，以下示例说明了如何使用自定义控件：

使用现有控件作为起点

您可以在 Audit Manager 中自定义任何控件。如果现有控件或多或少地满足您的目标，但您想扩展其指导范围或者调整一些属性以满足您的特定需求，那么这是一个不错的选择。例如，您可以更改控件收集证据的频率，然后更改控件的名称以反映这一点。

为内部审计创建自定义控件

为了支持内部审计，您可以创建与任何特定合规性框架或法规无关的专用自定义控件。这使您可以自由地根据特定区域定制控件要求，或者从特定业务资源中收集证据。例如，您可以创建一个自定义控件，该控件使用贵组织的自定义 AWS Config 规则作为证据收集的数据源。

创建供应商风险评测问题

您可以使用自定义控件来支持如何管理供应商风险评测。您创建的每个控件都可以代表一个单独的风险评测问题。在这种情况下，控件名称可以是一个问题，您可以通过上传文件或输入文本响应作为手动证据来提供回答。

您可通过两种方式创建自定义控件。您可以从头开始创建新控件，也可以自定义现有控件。

主题

- 从头开始创建新自定义控件
- 自定义现有控件

从头开始创建新自定义控件

您可以按照以下步骤从头开始创建新的自定义控件。

> **Important**
>
> 强烈建议您切勿将敏感的可识别信息放入自由格式字段，例如控件详细信息、测试信息或行动计划。如果您创建包含敏感信息的自定义控件，则无法共享任何包含这些控件的自定义框架。

主题

步骤 1：指定控件详细信息

首先指定您的自定义控件的详细信息。

指定控件详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库，然后选择创建自定义控件。
3. 在控件详细信息下，输入有关控件的以下信息。
   - 控件 - 输入合法名称、标题或风险评测问题。此值可帮助您在控件库中识别您的控件。
   - 描述（可选）- 输入详细信息以帮助其他人了解控件的目标。此描述显示在控件详细信息页面上。
4. 在测试信息下，输入测试控件的推荐步骤。
5. 在标签下，选择添加新标签，将标签与您的控件相关联。您可以为每个标签指定一个密钥，以恰当描述此控件支持的合规性框架。标签密钥为必填项，当您在控件库中搜索该控件时，可将其用作搜索条件。
6. 选择下一步。

步骤 2：设置数据来源

接下来，定义最多 10 个数据来源。数据来源决定您的自定义控件从何处收集证据。

如果要收集自动证据，则每个数据来源都必须包含数据来源类型和数据来源映射。这些细节与您的 AWS 使用情况相对应，并告诉 Audit Manager 从哪里收集证据。如果您想提供自己的证据，则需要命名数据来源，然后选择手动证据选项。

> **Important**
>
> 要成功使用 AWS Config 和 Security Hub 作为自动数据源，请务必执行以下操作：
>
> - 按照说明设置 AWS Config 和设置 Security Hub 以在 Audit Manager 中使用。
> - 将两者 AWS Config 和 Security Hub 作为服务包括在评估范围内。
>
> 然后，每次对您在此步骤中指定的 AWS Config 规则或 Security Hub 控件进行评估时，Audit Manager 都可以收集证据。

设置数据来源

1. 在数据来源名称下，将占位符文本替换为数据来源的描述性名称。
2. 在证据收集方法下，选择您要如何为此控件收集证据。

   a. 如果您希望 Audit Manager 收集证据，请选择自动并按照以下步骤操作：

      - 在数据来源类型下，指定 Audit Manager 从何处收集自动证据。
        - 对于 AWS CloudTrail，请从下拉列表中选择活动名称关键字。
        - 对于 AWS Config，选择规则类型，然后从下拉列表中选择规则标识符关键字。
        - 对于 AWS Security Hub，请从下拉列表中选择 Security Hub 控件。
        - 对于 AWS API 调用，请选择 API 调用，然后选择证据收集频率。

      > **Tip**
      >
      > 有关每种数据来源类型的概述和相关的疑难解答提示，请参阅 自动数据来源概述。如果您需要与领域专家一起验证数据来源配置，请暂时将证据收集方法设置为手动。这样，您就可以立即创建控件并将其添加到框架中，然后根据需要编辑控件。

   b. 如果您想提供自己的证据，请选择手动，然后选择手动证据选项。

      - 文件上传 - 如果控件要求文档作为证据，请选择此选项。

- 文本响应 - 如果控件要求回答风险评测问题，请选择此选项。

3. （可选）在其他详细信息下，输入数据来源描述和疑难解答描述。
4. （可选）要添加其他数据来源，请选择添加数据来源，然后重复步骤 1-3。
5. （可选）要移除数据来源，请选择数据来源配置框顶部的移除。
6. 完成后，选择下一步。

步骤 3（可选）：定义行动计划

接下来，指定需要纠正此控件时要采取的操作。

定义行动计划

1. 在标题下，输入行动计划的描述性标题。
2. 在行动计划说明下，输入行动计划的详细说明。
3. 选择下一步。

步骤 4：审核并创建控件

审核控件信息。若要更改步骤信息，请选择编辑。

完成后，选择创建自定义控件。

接下来如何操作？

创建新的自定义控件后，您可以将它们添加至自定义框架。要了解更多信息，请参阅 创建自定义框架 或 编辑自定义框架。

将自定义控件添加到自定义框架后，您可以根据该自定义框架创建评测并开始收集证据。要了解更多信息，请参阅创建评测。

有关故障排除提示，请参阅 控件和控制集问题排查。

自定义现有控件

与其从头开始创建自定义控件，不如以现有控件为起点并根据您的需要对其进行自定义。执行此操作时，现有控件将保留在控件库内，通过您的自定义设置创建新的自定义控件。

您可以选择对任何现有控件进行自定义。它可以是标准控件，也可以是自定义控件。

> **Important**
>
> 强烈建议您切勿将敏感的可识别信息放入自由格式字段，例如控件详细信息、测试信息或行动计划。如果您创建包含敏感信息的自定义控件，则无法共享任何包含这些控件的自定义框架。

主题

步骤 1：指定控件详细信息

控件的详细信息继承自原始控件。根据需要检查和修改这些详细信息。

指定控件详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库。
3. 选择要自定义的控件，然后选择自定义现有控件。
4. 指定控件的新名称，然后选择自定义。
5. 在控件详细信息下，根据需要自定义控件详细信息。
6. 在测试信息下，根据需要自定义测试信息。
7. 在标签下，根据需要自定义标签。
8. 选择下一步。

步骤 2：设置数据来源

数据来源继承自原始控件。您可以根据需要更改、添加或移除数据来源。

> **Important**
>
> 要成功使用 AWS Config 和 Security Hub 作为自动数据源，请务必执行以下操作：

- 按照说明设置 AWS Config 和设置 Security Hub 以在 Audit Manager 中使用。
- 将两者 AWS Config 和 Security Hub 作为服务包括在评估范围内。

然后，每次对您在此步骤中指定的 AWS Config 规则或 Security Hub 控件进行评估时，Audit Manager 都可以收集证据。

设置数据来源

1. 在数据来源名称下，根据需要自定义数据来源名称。
2. 在证据收集方法下，根据需要自定义选择。

   a. 如果您希望 Audit Manager 收集证据，请选择自动并按照以下步骤操作：

      - 在数据来源类型下，查看 Audit Manager 从哪里收集自动证据，并根据需要进行修改。
        - 对于 AWS CloudTrail，请从下拉列表中选择活动名称关键字。
        - 对于 AWS Config，选择规则类型，然后从下拉列表中选择规则标识符关键字。
        - 对于 AWS Security Hub，请从下拉列表中选择 Security Hub 控件。
        - 对于 AWS API 调用，请选择 API 调用，然后选择证据收集频率。

      > **Tip**
      >
      > 有关每种数据来源类型的概述和相关的疑难解答提示，请参阅 自动数据来源概述。如果您需要与领域专家一起验证数据来源配置，请暂时将证据收集方法设置为手动。这样，您就可以立即创建控件并将其添加到框架中，然后根据需要编辑控件。

   b. 如果您想提供自己的证据，请选择手动，然后选择手动证据选项。

      - 文件上传 - 如果控件要求文档作为证据，请选择此选项。
      - 文本响应 - 如果控件要求回答风险评测问题，请选择此选项。

3. （可选）在其他详细信息下，对数据来源描述或疑难解答描述进行任何必要的更改。
4. （可选）要添加其他数据来源，请选择添加数据来源。
5. （可选）要移除数据来源，请选择移除。
6. 选择下一步。

步骤 3：（可选）：定义行动计划

行动计划继承自原始控件。您可以根据需要编辑此行动计划。

定义行动计划

1. 在标题下，查看行动计划的标题，并根据需要对其进行自定义。
2. 在行动计划说明下，根据需要查看和自定义说明。
3. 选择下一步。

步骤 4：审核并创建控件

审核控件信息。若要更改步骤信息，请选择编辑。完成后，选择创建自定义控件。

接下来如何操作？

创建新的自定义控件后，您可以将它们添加至自定义框架。要了解更多信息，请参阅 创建自定义框架 或 编辑自定义框架。

将自定义控件添加到自定义框架后，您可以根据该自定义框架创建评测并开始收集证据。要了解更多信息，请参阅创建评测。

如果您需要编辑自定义控件，请参阅 编辑自定义控件。

有关故障排除提示，请参阅 控件和控制集问题排查。

编辑自定义控件

您可以按照以下步骤在 Audit Manager 中编辑自定义控件。

主题

步骤 1：编辑控件详细信息

首先，根据需要查看和编辑控件详细信息。

编辑控件详细信息

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库，然后选择自定义控件选项卡。
3. 选择要编辑的控件，然后选择编辑。
4. 在控件详细信息下，根据需要编辑控件详细信息。
5. 在测试信息下，根据需要编辑推荐的测试信息。
6. 选择下一步。

> **Tip**
>
> 要编辑控件的标签，请打开控件并选择标签选项卡。您可查看和编辑与控件关联的标签。

步骤 2：编辑数据来源

接下来，您可以编辑、移除或添加控件的数据来源。

> **Important**
>
> 要成功使用 AWS Config 和 Security Hub 作为自动数据源，请务必执行以下操作：
>
> - 按照说明设置 AWS Config 和设置 Security Hub 以在 Audit Manager 中使用。
> - 将两者 AWS Config 和 Security Hub 作为服务包括在评估范围内。
>
> 然后，每次对您在此步骤中指定的 AWS Config 规则或 Security Hub 控件进行评估时，Audit Manager 都可以收集证据。

要编辑数据来源

1. 在数据来源名称下，查看当前名称并根据需要进行编辑。
2. 在证据收集方法下，查看当前选择并根据需要进行编辑。
   a. 如果您希望 Audit Manager 收集证据，请选择自动并按照以下步骤操作：
      - 在数据来源类型下，查看 Audit Manager 从哪里收集自动证据，并根据需要进行编辑。

- 对于 AWS CloudTrail，请从下拉列表中选择活动名称关键字。
- 对于 AWS Config，选择规则类型，然后从下拉列表中选择规则标识符关键字。
- 对于 AWS Security Hub，请从下拉列表中选择 Security Hub 控件。
- 对于 AWS API 调用，请选择 API 调用，然后选择证据收集频率。

> **Tip**
>
> 有关每种数据来源类型的概述和相关的疑难解答提示，请参阅 自动数据来源概述。

b. 如果您想提供自己的证据，请选择手动，然后选择手动证据选项。

- 文件上传 - 如果控件要求文档作为证据，请选择此选项。
- 文本响应 - 如果控件要求回答风险评测问题，请选择此选项。

3. （可选）在其他详细信息下，对数据来源描述或疑难解答描述进行任何必要的更改。
4. （可选）要添加其他数据来源，请选择添加数据来源。
5. （可选）要移除数据来源，请选择移除。
6. 选择下一步。

步骤 3：（可选）编辑行动计划

接下来，查看和编辑可选的行动计划。

编辑行动计划

1. 在标题下，根据需要编辑标题。
2. 在行动计划说明下，根据需要编辑说明。
3. 选择下一步。

步骤 4：审核并更新控件

审核控件信息。若要更改步骤信息，请选择编辑。

完成后，选择保存更改。

> **Note**
>
> 编辑控件后，所做的更改将在包括该控件在内的所有处于活动状态的评测中生效，如下所示：
>
> - 对于以 AWS API 调用作为数据来源类型的控件，更改将在世界标准时间第二天 00:00 生效。
> - 对于所有其他控件，更改将立即生效。

删除自定义控件

您可以使用控件库删除不需要的自定义控件。删除控件后，该控件将不再出现在控件库中。您也可以使用 Audit Manager API 或 AWS Command Line Interface (AWS CLI) 删除自定义控件。

> **Important**
>
> 删除自定义控件时，此操作会将该控件从当前与之相关的所有自定义框架或评测中移除。因此，Audit Manager 将停止在您的所有评测中为该自定义控件收集证据。这包括您在删除自定义控件之前创建的评测。

Audit Manager console

删除自定义控件（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库，然后选择自定义控件选项卡。
3. 选择要删除的控件，然后选择删除。
4. 在出现的弹出窗口中，选择删除以确认删除。

AWS CLI

删除自定义控件 (AWS CLI)

1. 首先，识别要删除的自定义控件。为此，请运行 list-controls 命令并将 `--control-type` 指定为 `Custom`。

```
aws auditmanager list-controls --control-type Custom
```

响应返回自定义控件列表。找到要删除的控件，并记下控件 ID。

2. 接下来，运行 delete-control 命令并使用 `--control-id` 参数指定要删除的控件。

   在以下示例中，将*#####*替换为您自己的信息。

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

Audit Manager API

删除自定义控件 (API)

1. 使用ListControls操作并将 ControlType 指定为。`Custom`在响应中，找到要删除的控件并记下控件 ID。
2. 使用DeleteControl操作删除自定义控件。在请求中，使用 controlId 参数指定要删除的控件。

如需了解更多关于这些 API 操作的信息，请选择前面的任一链接，在 AWS Audit Manager API 参考中阅读更多内容。其中包括有关如何在某个特定语言 AWS 的 SDK 中使用这些操作和参数的信息。

更改控件的证据收集频率

AWS Audit Manager 以不同的频率从多个数据源收集证据。支持的证据收集频率取决于为控件收集的证据类型。

- 对于 AWS API 调用，Audit Manager 使用对另一个 AWS 服务的描述 API 调用来收集证据。您可以直接在 Audit Manager 中指定证据收集频率（仅适用于自定义控件）。
- 对于 AWS Config，Audit Manager 直接从中报告合规性检查的结果 AWS Config。频率遵循 AWS Config 规则中定义的触发条件。
- 对于 AWS Security Hub，Audit Manager 直接从 Security Hub 中报告合规性检查的结果。频率遵循 Security Hub 检查的时间表。
- 对于 AWS CloudTrail，Audit Manager 不断从中收集证据 CloudTrail。您无法更改此类证据的收集频率。

以下章节提供了有关每种控件数据来源类型的证据收集频率以及如何对其进行更改（如果适用）的更多信息。

主题

来自 AWS API 调用的配置快照

> **Note**
>
> 以下内容仅适用于自定义控件。对于使用 API 调用作为数据来源的标准控件，您无法更改证据收集频率。

如果自定义控件使用 AWS API 调用作为数据源类型，则可以按照以下步骤在 Audit Manager 中更改证据收集频率。

更改以 API 调用作为数据来源的自定义控件的证据收集频率

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在导航窗格中，选择控件库，然后选择自定义控件选项卡。
3. 选择要编辑的自定义控件，然后选择编辑。
4. 在编辑控件详细信息页面上，选择编辑。
5. 找到要编辑的数据来源框，并验证以下信息是否正确：
   - 证据收集方法为自动。
   - 数据来源类型为 AWS API 调用。
   - 所选 API 调用是您希望更改其频率的调用。
6. 在频率下，选择要为自定义控件收集证据的频率。
7. 根据需要对要编辑的任何其他 API 调用数据来源重复步骤 5-6。
8. 选择下一步。
9. 在编辑行动计划页面上，选择下一步。

10. 在查看和更新控件页面上，查看自定义控件的信息。若要更改步骤信息，请选择编辑。
11. 完成后，选择保存更改。

在编辑将 AWS API 调用作为数据来源类型的控件后，所做的更改将在第二天 00:00 UTC 在包含该控件的所有处于活动状态的评测中生效。

来自 AWS Config的合规性检查

> **Note**
>
> 以下内容适用于使用 AWS Config 规则 作为数据来源的标准控件和自定义控件。

如果控件 AWS Config 用作数据源类型，则无法直接在 Audit Manager 中更改证据收集频率。这是因为频率遵循 AWS Config 规则中定义的触发器。

有两种类型的触发器 AWS Config 规则：

1. 配置更改- AWS Config 在创建、更改或删除某些类型的资源时对规则进行评估。
2. 定期- AWS Config 按您选择的频率对规则进行评估（例如，每 24 小时一次）。

要了解有关触发器的更多信息 AWS Config 规则，请参阅《AWS Config 开发者指南》中的触发器类型。

有关如何管理的说明 AWS Config 规则，请参阅管理您的 AWS Config 规则。

来自 Security Hub 的合规性检查

> **Note**
>
> 以下内容适用于使用 Security Hub 检查作为数据来源的标准控件和自定义控件。

如果控件使用 Security Hub 作为数据来源类型，则无法直接在 Audit Manager 中更改证据收集频率。这是因为频率遵循了 Security Hub 检查的时间表。

- 在最近一次运行后的 12 小时内，将自动运行定期检查。您无法更改周期。

- 在关联的资源更改状态时，将运行更改触发的检查。即使资源没有更改状态，更改触发的检查的更新时间也将每 18 小时刷新一次。这有助于指明控件仍处于启用状态。通常，Security Hub 尽可能使用更改触发的规则。

要了解更多信息，请参阅 AWS Security Hub 用户指南中的安全检查运行时间表。

来自 AWS CloudTrail的用户活动日志

> **Note**
>
> 以下内容适用于使用 AWS CloudTrail 用户活动日志作为数据来源的标准控件和自定义控件。

对于使用活动日志 CloudTrail 作为数据源类型的控件，您无法更改证据收集频率。Audit Manager 会持续收集此类证据。 CloudTrail 这种频率是持续的，因为用户活动可以在一天中的任何时间发生。

支持用于自动证据的控件数据来源

在中创建自定义控件时 AWS Audit Manager，您可以将控件设置为从以下数据源类型收集自动证据：

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API 调用

以下主题总结了每种自动数据源类型，并列出了 Audit Manager 支持的特定 AWS Security Hub 控件、AWS Config 规则和 AWS API 调用。

主题

- 自动数据来源概述
- AWS Config 规则 由... 支持 AWS Audit Manager
- AWS Security Hub 支持的控件 AWS Audit Manager
- 支持的 API 调用 AWS Audit Manager
- AWS CloudTrail 支持的事件名称 AWS Audit Manager

自动数据来源概述

下表概述了每种自动数据来源类型。

数据来源类型	描述	证据收集频率	要使用此数据来源类型...	当此控件在评测中处于活动状态时...	相关的疑难解答提示
AWS CloudTrail	跟踪特定的用户活动。	持续。	从支持的事件名称列表中选择。	Audit Manager 会根据您选择的关键字筛选您的 CloudTrail 日志。结果将作为用户活动证据导入。	我的评测没有从 AWS CloudTrail 中收集用户活动证据
AWS Config	通过报告来自的调查结果，捕获资源安全态势的快照 AWS Config。	基于 AWS Config 规则中定义的触发器。	选择规则类型，然后选择规则。 • 对于托管规则，请从支持的托管规则关键字列表中进行选择。 • 对于自定义规则，请从可用规则列表中进行选择。	Audit Manager 直接从中获取此规则的调查结果 AWS Config。结果作为合规性检查证据导入。	我的评测没有从 AWS Config 中收集合规检查证据 AWS Config

数据来源类型	描述	证据收集频率	要使用此数据来源类型...	当此控件在评测中处于活动状态时...	相关的疑难解答提示
					集成问题
AWS Security Hub	通过报告来自 Security Hub 的调查发现，捕获您资源安全状况的快照。	基于 Security Hub 检查的时间表。	从支持的 Security Hub 控件 ID 列表中进行选择。	Audit Manager 直接从 Security Hub 获取安全检查的结果。结果作为合规性检查证据导入。	我的评测没有从 AWS Security Hub 中收集合规检查证据
AWS API 调用	通过对指定的 API 调用，直接拍摄资源配置的快照 AWS 服务。	每天、每周或每月。	从支持的 API 调用列表中选择，然后选择您的首选频率。	Audit Manager 根据您指定的频率进行 API 调用。响应作为配置数据证据导入。	我的评测没有收集 AWS API 调用的配置数据证据

AWS Config 规则 由... 支持 AWS Audit Manager

您可以使用 Audit Manager 捕获 AWS Config 评估作为审计证据。创建或编辑自定义控件时，可以将一个或多个 AWS Config 规则指定为证据收集的数据源映射。 AWS Config 根据这些规则执行合规性检查，然后 Audit Manager 将结果报告为合规性检查证据。

除了托管规则外，您还可以将自定义规则映射到控件数据来源。

> **Note**
>
> - Audit Manager 不从服务相关 AWS Config 规则中收集证据，但一致性数据包和来自 AWS Organizations的服务相关规则除外。有关更多信息，请参阅本指南的疑难解答部分。
> - Audit Manager 不为你管理 AWS Config 规则。在开始收集证据之前，我们建议您查看当前的 AWS Config 规则参数。然后，根据所选框架的要求验证这些参数。如果需要，您可以在 AWS Config中更新规则的参数，使其与框架要求保持一致。这将有助于确保您的评测收集该框架的正确合规性检查证据。
>
>   例如，假设您正在为 CIS v1.2.0 创建评测。此框架包含名为 1.9 – 确保 IAM 密码策略的最小长度为 14 或以上字符的控件。在中 AWS Config，该iam-password-policy规则有一个`MinimumPasswordLength`用于检查密码长度的参数。该参数的默认值为 14 个字符。因此，该规则与控件要求保持一致。如果您未使用默认参数值，请确保使用的值大于等于 CIS v1.2.0 中要求的 14 个字符。您可在 AWS Config 文档中找到每条托管规则的默认参数详细信息。

主题

- 在 Audit Manager 中使用 AWS Config 托管规则
- 在 Audit Manager 中使用 AWS Config 自定义规则
- 对 Audit Manager AWS Config 集成进行故障排除

在 Audit Manager 中使用 AWS Config 托管规则

Audit Manager 目前支持 326 条 AWS Config 托管规则。在为自定义控件设置数据来源时，可以使用以下任何托管规则标识符关键字。有关下面列出的任何托管规则的更多信息，请从列表中选择一个项目或参阅 AWS Config 用户指南中的 AWS Config 托管规则。

> **Tip**
>
> 当您在创建自定义控件期间在 Audit Manager 控制台中选择托管规则时，请务必查找以下规则标识符关键字之一，而不是规则名称。有关规则名称和规则标识符之间的区别以及如何查找托管规则标识符的信息，请参阅本用户指南的疑难解答部分。

支持的 AWS Config 托管规则关键字

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED

支持的 AWS Config 托管规则关键字

- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

支持的 AWS Config 托管规则关键字

- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED

支持的 AWS Config 托管规则关键字

- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

支持的 AWS Config 托管规则关键字

- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _ AWSVPC_NETWORKING 已启用
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK

支持的 AWS Config 托管规则关键字

- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED

支持的 AWS Config 托管规则关键字

- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK

支持的 AWS Config 托管规则关键字

- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

支持的 AWS Config 托管规则关键字

- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

支持的 AWS Config 托管规则关键字

- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

支持的 AWS Config 托管规则关键字

- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK

支持的 AWS Config 托管规则关键字

- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

在 Audit Manager 中使用 AWS Config 自定义规则

现在，您可以使用 AWS Config 自定义规则作为审计报告的数据源。当控件具有映射到 AWS Config 规则的数据源时，Audit Manager 会添加由该 AWS Config 规则创建的评估。

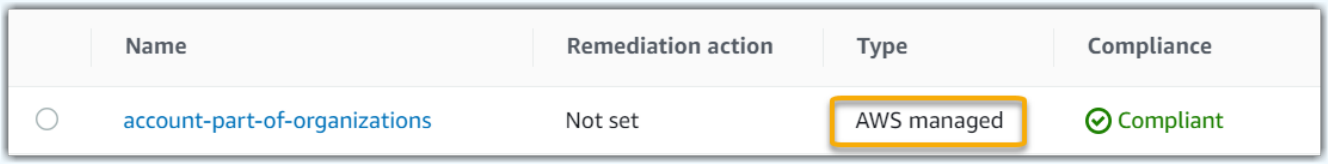
您可以使用的自定义规则取决于您登录 Aud AWS 账户 it Manager 时使用的规则。如果可以在中访问自定义规则 AWS Config，则可以将其用作 Audit Manager 中的数据源映射。

- 对于个人 AWS 账户 — 您可以使用您在账户中创建的任何自定义规则。
- 对于属于组织的账户 - 无论哪种情况，您都可以使用任何成员级别的自定义规则。或者，您可以使用 AWS Config中提供的任何组织级别的自定义规则。

有关如何创建使用自定义规则作为数据来源的控件的说明，请参阅从头开始创建新控件和自定义现有控件。

> **Tip**
>
> 请注意，托管规则不会显示在 Audit Manager 的自定义规则下拉列表中。

如果要验证 AWS Config 规则是托管规则还是自定义规则，则可以使用AWS Config 控制台执行此操作。从左侧导航菜单中，选择规则，然后在表格中查找规则。如果是托管规则，则类型列显示 AWS 托管。



要将托管规则映射为数据来源，可以在 Audit Manager 的托管规则下拉列表中查找托管规则标识符关键字。有关更多信息，请参阅本指南的疑难解答部分。

将自定义规则映射为控件的数据来源后，您可以将该控件与 Audit Manager 中的自定义框架相关联。有关如何创建使用自定义控件的自定义框架的说明，请参阅从头开始创建新框架和自定义现有框架。有关如何将控件添加到现有自定义框架的说明，请参阅编辑现有框架。

有关在中创建自定义规则的信息 AWS Config，请参阅《AWS Config 开发人员指南》 AWS Config中的开发自定义规则。

对 Audit Manager AWS Config 集成进行故障排除

要查找常见问题和答案，请参阅本指南疑难解答部分中的 AWS Config 集成。

AWS Security Hub 支持的控件 AWS Audit Manager

Audit Manager 允许您直接从 Security Hub 报告合规性检查的结果。为此，在 Audit Manager 中配置自定义控件时，您需要将一个或多个 Security Hub 控件指定为数据来源映射。

> **Note**
>
> - Audit Manager 不会从 Security Hub 创建的服务相关 AWS Config 规则中收集证据。有关更多信息，请参阅本指南的疑难解答部分。
> - 2022年11月9日，Security Hub推出了符合互联网安全中心（CIS）AWS 基金会基准1.4.0版本1和2级（CIS v1.4.0）的自动安全检查。在 Security Hub 中，除了 CIS v1.2.0 标准外，还支持 CIS v1.4.0 标准。

主题

- 在 Audit Manager 中使用 Security Hub 控件

- 支持的 Security Hub 控件

在 Audit Manager 中使用 Security Hub 控件

> **Tip**
>
> 如果尚未打开 Security Hub 中的合并的控件调查发现设置，我们建议您将其打开。如果您在 2003 年 2 月 23 日当天或之后启用 Security Hub，则默认情况下此设置处于打开状态。

启用合并的调查发现后，Security Hub 会为每项安全检查生成一个结果（即使同一检查适用于多个标准）。每项 Security Hub 调查发现都作为一项独特的资源评测收集在 Audit Manager 中。因此，合并的调查发现会减少 Audit Manager 针对 Security Hub 的调查结果执行的独特资源评测总数。因此，使用合并的调查发现通常可以在不牺牲证据质量和可用性的情况下降低您的 Audit Manager 使用成本。有关定价的更多信息，请参阅 AWS Audit Manager 定价。

开启或关闭合并的调查发现时的证据示例

以下示例比较了 Audit Manager 如何根据您的 Security Hub 设置收集和展示证据。

When consolidated findings is turned on

假设你已在 Security Hub 中启用了以下三个安全标准： AWS FSBP、PCI DSS 和 CIS Benchmark v1.2.0。

- 这三个标准都使用相同的控件 (IAM.4) 和相同的基本 AWS Config 规则 (iam-root-access-key-check)。
- 由于合并的控件调查发现设置已开启，因此 Security Hub 会为此控件生成一个调查结果。
- 针对该控件，Security Hub 将合并的调查发现发送给 Audit Manager。
- 在 Audit Manager 中，合并的调查发现算作一项独特的资源评测。因此，在您的评测中添加一份证据。

以下示例说明了这些证据可能是什么样子：

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
```

```
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
```

```
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```


When consolidated findings is turned off

假设你已在 Security Hub 中启用了以下三个安全标准： AWS FSBP、PCI DSS 和 CIS Benchmark v1.2.0。

- 这三个标准都使用相同的控件 (IAM.4) 和相同的基本 AWS Config 规则 (iam-root-access-key-check)。
- 由于合并的调查发现设置已关闭，因此 Security Hub 会根据每个启用的标准为每项安全检查生成一个单独的调查结果（在本例中为三个调查发现）。

- 针对此控件，Security Hub 将三个单独的特定于标准的调查发现发送给 Audit Manager。
- 在 Audit Manager 中，这三项调查发现算作三项独特的资源评测。因此，将三份独立的证据添加到您的评测中。

以下示例说明了这些证据可能是什么样子。请注意，在本示例中，以下三个有效负载均具有相同的安全控件 ID (*SecurityControlId":"IAM.4"*)。因此，当从 Security Hub 获得以下调查发现时，在 Audit Manager (IAM.4) 中收集这些证据的评测控件会收到三份单独的证据。

IAM.4 (FSBP) 的证据


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
```

```
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
```

```
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:07.395Z"
       }
    ]
  }
}
```

IAM.4（CIS 1.2）的证据

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
```

```
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
           "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
```

```
                "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
             }
          },
          "ProductFields":{
             "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
             "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
             "RuleId":"1.12",
             "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
             "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
             "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
             "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
             "aws/securityhub/ProductName":"Security Hub",
             "aws/securityhub/CompanyName":"AWS",
             "Resources:0/Id":"arn:aws:iam::111122223333:root",
             "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
          },
          "Resources":[
             {
                "Type":"AwsAccount",
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
```

```
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:13.436Z"
         }
      ]
   }
}
```

PCI.IAM.1 (PCI DSS) 的证据

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
```

```
            "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
```

```
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:05.950Z"
      }
   ]
```

```
  }
}
```

支持的 Security Hub 控件

Audit Manager 目前支持以下 Security Hub 控件。在为自定义控件设置数据来源时，可以使用以下任何特定于标准的控件 ID 关键字。

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI。AutoScaling.1	AutoScaling.1
PCI DSS	PCI。CloudTrail.1	CloudTrail.1
PCI DSS	PCI。CloudTrail.2	CloudTrail.2
PCI DSS	PCI。CloudTrail.3	CloudTrail.3

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
PCI DSS	PCI。 CloudTrail.4	CloudTrail.4
PCI DSS	PCI。 CodeBuild.1	CodeBuild.1
PCI DSS	PCI。 CodeBuild.2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
PCI DSS	PCI。GuardDuty.1	GuardDuty.1
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI。SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS 基础安全最佳实践	Account.1	Account.1
AWS 基础安全最佳实践	Account.2	Account.2
AWS 基础安全最佳实践	ACM.1	ACM.1
AWS 基础安全最佳实践	ACM.2	ACM.2
AWS 基础安全最佳实践	APIGateway.1	APIGateway.1
AWS 基础安全最佳实践	APIGateway.2	APIGateway.2

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	APIGateway.3	APIGateway.3
AWS 基础安全最佳实践	APIGateway.4	APIGateway.4
AWS 基础安全最佳实践	APIGateway.5	APIGateway.5
AWS 基础安全最佳实践	APIGateway.8	APIGateway.8
AWS 基础安全最佳实践	APIGateway.9	APIGateway.9
AWS 基础安全最佳实践	AppSync.2	AppSync.2
AWS 基础安全最佳实践	AppSync.5	AppSync.5
AWS 基础安全最佳实践	Athena.1	Athena.1
AWS 基础安全最佳实践	AutoScaling.1	AutoScaling.1
AWS 基础安全最佳实践	AutoScaling.2	AutoScaling.2
AWS 基础安全最佳实践	AutoScaling.3	AutoScaling.3
AWS 基础安全最佳实践	AutoScaling.4	AutoScaling.4
AWS 基础安全最佳实践	Autoscaling.5	Autoscaling.5
AWS 基础安全最佳实践	AutoScaling.6	AutoScaling.6
AWS 基础安全最佳实践	AutoScaling.9	AutoScaling.9
AWS 基础安全最佳实践	Backup.1	Backup.1
AWS 基础安全最佳实践	CloudFormation.1	CloudFormation.1

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	CloudFront.1	CloudFront.1
AWS 基础安全最佳实践	CloudFront.2	CloudFront.2
AWS 基础安全最佳实践	CloudFront.3	CloudFront.3
AWS 基础安全最佳实践	CloudFront.4	CloudFront.4
AWS 基础安全最佳实践	CloudFront.5	CloudFront.5
AWS 基础安全最佳实践	CloudFront.6	CloudFront.6
AWS 基础安全最佳实践	CloudFront.7	CloudFront.7
AWS 基础安全最佳实践	CloudFront.8	CloudFront.8
AWS 基础安全最佳实践	CloudFront.9	CloudFront.9
AWS 基础安全最佳实践	CloudFront.10	CloudFront.10
AWS 基础安全最佳实践	CloudFront.12	CloudFront.12
AWS 基础安全最佳实践	CloudFront.13	CloudFront.13
AWS 基础安全最佳实践	CloudTrail.1	CloudTrail.1
AWS 基础安全最佳实践	CloudTrail.2	CloudTrail.2
AWS 基础安全最佳实践	CloudTrail.3	CloudTrail.3
AWS 基础安全最佳实践	CloudTrail.4	CloudTrail.4
AWS 基础安全最佳实践	CloudTrail.5	CloudTrail.5
AWS 基础安全最佳实践	CloudTrail.6	CloudTrail.6

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	CloudTrail.7	CloudTrail.7
AWS 基础安全最佳实践	CloudWatch.1	CloudWatch.1
AWS 基础安全最佳实践	CloudWatch.2	CloudWatch.2
AWS 基础安全最佳实践	CloudWatch.3	CloudWatch.3
AWS 基础安全最佳实践	CloudWatch.4	CloudWatch.4
AWS 基础安全最佳实践	CloudWatch.5	CloudWatch.5
AWS 基础安全最佳实践	CloudWatch.6	CloudWatch.6
AWS 基础安全最佳实践	CloudWatch.7	CloudWatch.7
AWS 基础安全最佳实践	CloudWatch.8	CloudWatch.8
AWS 基础安全最佳实践	CloudWatch.9	CloudWatch.9
AWS 基础安全最佳实践	CloudWatch.10	CloudWatch.10
AWS 基础安全最佳实践	CloudWatch.11	CloudWatch.11
AWS 基础安全最佳实践	CloudWatch.12	CloudWatch.12
AWS 基础安全最佳实践	CloudWatch.13	CloudWatch.13
AWS 基础安全最佳实践	CloudWatch.14	CloudWatch.14
AWS 基础安全最佳实践	CloudWatch.15	CloudWatch.15
AWS 基础安全最佳实践	CloudWatch.16	CloudWatch.16
AWS 基础安全最佳实践	CloudWatch.17	CloudWatch.17

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	CodeBuild.1	CodeBuild.1
AWS 基础安全最佳实践	CodeBuild.2	CodeBuild.2
AWS 基础安全最佳实践	CodeBuild.3	CodeBuild.3
AWS 基础安全最佳实践	CodeBuild.4	CodeBuild.4
AWS 基础安全最佳实践	CodeBuild.5	CodeBuild.5
AWS 基础安全最佳实践	Config.1	Config.1
AWS 基础安全最佳实践	DMS.1	DMS.1
AWS 基础安全最佳实践	DMS.6	DMS.6
AWS 基础安全最佳实践	DMS.7	DMS.7
AWS 基础安全最佳实践	DMS.8	DMS.8
AWS 基础安全最佳实践	DMS.9	DMS.9
AWS 基础安全最佳实践	DocumentDB.1	DocumentDB.1
AWS 基础安全最佳实践	DocumentDB.2	DocumentDB.2
AWS 基础安全最佳实践	DocumentDB.3	DocumentDB.3
AWS 基础安全最佳实践	DocumentDB.4	DocumentDB.4
AWS 基础安全最佳实践	DocumentDB.5	DocumentDB.5
AWS 基础安全最佳实践	DynamoDB.1	DynamoDB.1
AWS 基础安全最佳实践	DynamoDB.2	DynamoDB.2

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	DynamoDB.3	DynamoDB.3
AWS 基础安全最佳实践	DynamoDB.4	DynamoDB.4
AWS 基础安全最佳实践	DynamodB.6	DynamodB.6
AWS 基础安全最佳实践	EC2.1	EC2.1
AWS 基础安全最佳实践	EC2.2	EC2.2
AWS 基础安全最佳实践	EC2.3	EC2.3
AWS 基础安全最佳实践	EC2.4	EC2.4
AWS 基础安全最佳实践	EC2.6	EC2.6
AWS 基础安全最佳实践	EC2.7	EC2.7
AWS 基础安全最佳实践	EC2.8	EC2.8
AWS 基础安全最佳实践	EC2.9	EC2.9
AWS 基础安全最佳实践	EC2.10	EC2.10
AWS 基础安全最佳实践	EC2.12	EC2.12
AWS 基础安全最佳实践	EC2.13	EC2.13
AWS 基础安全最佳实践	EC2.14	EC2.14
AWS 基础安全最佳实践	EC2.15	EC2.15
AWS 基础安全最佳实践	EC2.16	EC2.16
AWS 基础安全最佳实践	EC2.17	EC2.17

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	EC2.18	EC2.18
AWS 基础安全最佳实践	EC2.19	EC2.19
AWS 基础安全最佳实践	EC2.20	EC2.20
AWS 基础安全最佳实践	EC2.21	EC2.21
AWS 基础安全最佳实践	EC2.22	EC2.22
AWS 基础安全最佳实践	EC2.23	EC2.23
AWS 基础安全最佳实践	EC2.24	EC2.24
AWS 基础安全最佳实践	EC2.25	EC2.25
AWS 基础安全最佳实践	EC2.28	EC2.28
AWS 基础安全最佳实践	EC2.51	EC2.51
AWS 基础安全最佳实践	ECR.1	ECR.1
AWS 基础安全最佳实践	ECR.2	ECR.2
AWS 基础安全最佳实践	ECR.3	ECR.3
AWS 基础安全最佳实践	ECS.1	ECS.1
AWS 基础安全最佳实践	ECS.2	ECS.2
AWS 基础安全最佳实践	ECS.3	ECS.3
AWS 基础安全最佳实践	ECS.4	ECS.4
AWS 基础安全最佳实践	ECS.5	ECS.5

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	ECS.8	ECS.8
AWS 基础安全最佳实践	ECS.9	ECS.9
AWS 基础安全最佳实践	ECS.10	ECS.10
AWS 基础安全最佳实践	ECS.12	ECS.12
AWS 基础安全最佳实践	EFS.1	EFS.1
AWS 基础安全最佳实践	EFS.2	EFS.2
AWS 基础安全最佳实践	EFS.3	EFS.3
AWS 基础安全最佳实践	EFS.4	EFS.4
AWS 基础安全最佳实践	EKS.1	EKS.1
AWS 基础安全最佳实践	EKS.2	EKS.2
AWS 基础安全最佳实践	EKS.8	EKS.8
AWS 基础安全最佳实践	ElastiCache.1	ElastiCache.1
AWS 基础安全最佳实践	ElastiCache.2	ElastiCache.2
AWS 基础安全最佳实践	ElastiCache.3	ElastiCache.3
AWS 基础安全最佳实践	ElastiCache.4	ElastiCache.4
AWS 基础安全最佳实践	ElastiCache.5	ElastiCache.5
AWS 基础安全最佳实践	ElastiCache.6	ElastiCache.6
AWS 基础安全最佳实践	ElastiCache.7	ElastiCache.7

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS 基础安全最佳实践	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS 基础安全最佳实践	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS 基础安全最佳实践	ELB.1	ELB.1
AWS 基础安全最佳实践	ELB.2	ELB.2
AWS 基础安全最佳实践	ELB.3	ELB.3
AWS 基础安全最佳实践	ELB.4	ELB.4
AWS 基础安全最佳实践	ELB.5	ELB.5
AWS 基础安全最佳实践	ELB.6	ELB.6
AWS 基础安全最佳实践	ELB.7	ELB.7
AWS 基础安全最佳实践	ELB.8	ELB.8
AWS 基础安全最佳实践	ELB.9	ELB.9
AWS 基础安全最佳实践	ELB.10	ELB.10
AWS 基础安全最佳实践	ELB.12	ELB.12
AWS 基础安全最佳实践	ELB.13	ELB.13
AWS 基础安全最佳实践	ELB.14	ELB.14

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	ELB.16	ELB.16
AWS 基础安全最佳实践	ELBv2.1	ELB.1
AWS 基础安全最佳实践	EMR.1	EMR.1
AWS 基础安全最佳实践	EMR.2	EMR.2
AWS 基础安全最佳实践	ES.1	ES.1
AWS 基础安全最佳实践	ES.2	ES.2
AWS 基础安全最佳实践	ES.3	ES.3
AWS 基础安全最佳实践	ES.4	ES.4
AWS 基础安全最佳实践	ES.5	ES.5
AWS 基础安全最佳实践	ES.6	ES.6
AWS 基础安全最佳实践	ES.7	ES.7
AWS 基础安全最佳实践	ES.8	ES.8
AWS 基础安全最佳实践	EventBridge.3	EventBridge3。
AWS 基础安全最佳实践	EventBridge.4	EventBridge.4
AWS 基础安全最佳实践	fsx.1	fsx.1
AWS 基础安全最佳实践	GuardDuty.1	GuardDuty.1
AWS 基础安全最佳实践	IAM.1	IAM.1
AWS 基础安全最佳实践	IAM.2	IAM.2

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	IAM.3	IAM.3
AWS 基础安全最佳实践	IAM.4	IAM.4
AWS 基础安全最佳实践	IAM.5	IAM.5
AWS 基础安全最佳实践	IAM.6	IAM.6
AWS 基础安全最佳实践	IAM.7	IAM.7
AWS 基础安全最佳实践	IAM.8	IAM.8
AWS 基础安全最佳实践	IAM.9	IAM.9
AWS 基础安全最佳实践	IAM.10	IAM.10
AWS 基础安全最佳实践	IAM.11	IAM.11
AWS 基础安全最佳实践	IAM.12	IAM.12
AWS 基础安全最佳实践	IAM.13	IAM.13
AWS 基础安全最佳实践	IAM.14	IAM.14
AWS 基础安全最佳实践	IAM.15	IAM.15
AWS 基础安全最佳实践	IAM.16	IAM.16
AWS 基础安全最佳实践	IAM.17	IAM.17
AWS 基础安全最佳实践	IAM.18	IAM.18
AWS 基础安全最佳实践	IAM.19	IAM.19
AWS 基础安全最佳实践	IAM.21	IAM.21

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	IAM.22	IAM.22
AWS 基础安全最佳实践	Kinesis.1	Kinesis.1
AWS 基础安全最佳实践	KMS.1	KMS.1
AWS 基础安全最佳实践	KMS.2	KMS.2
AWS 基础安全最佳实践	KMS.3	KMS.3
AWS 基础安全最佳实践	KMS.4	KMS.4
AWS 基础安全最佳实践	Lambda.1	Lambda.1
AWS 基础安全最佳实践	Lambda.2	Lambda.2
AWS 基础安全最佳实践	Lambda.3	Lambda.3
AWS 基础安全最佳实践	Lambda.5	Lambda.5
AWS 基础安全最佳实践	Macie.1	Macie.1
AWS 基础安全最佳实践	MQ.5	MQ.5
AWS 基础安全最佳实践	MQ.6	MQ.6
AWS 基础安全最佳实践	MSK.1	MSK.1
AWS 基础安全最佳实践	MSK.2	MSK.2
AWS 基础安全最佳实践	Neptune.1	Neptune.1
AWS 基础安全最佳实践	Neptune.2	Neptune.2
AWS 基础安全最佳实践	Neptune.3	Neptune.3

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	Neptune.4	Neptune.4
AWS 基础安全最佳实践	Neptune.5	Neptune.5
AWS 基础安全最佳实践	Neptune.6	Neptune.6
AWS 基础安全最佳实践	Neptune.7	Neptune.7
AWS 基础安全最佳实践	Neptune.8	Neptune.8
AWS 基础安全最佳实践	Neptune.9	Neptune.9
AWS 基础安全最佳实践	NetworkFirewall.1	NetworkFirewall.1
AWS 基础安全最佳实践	NetworkFirewall.2	NetworkFirewall.2
AWS 基础安全最佳实践	NetworkFirewall.3	NetworkFirewall.3
AWS 基础安全最佳实践	NetworkFirewall.4	NetworkFirewall.4
AWS 基础安全最佳实践	NetworkFirewall.5	NetworkFirewall.5
AWS 基础安全最佳实践	NetworkFirewall.6	NetworkFirewall.6
AWS 基础安全最佳实践	NetworkFirewall.9	NetworkFirewall.9

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	Opensearch.1	Opensearch.1
AWS 基础安全最佳实践	Opensearch.2	Opensearch.2
AWS 基础安全最佳实践	Opensearch.3	Opensearch.3
AWS 基础安全最佳实践	Opensearch.4	Opensearch.4
AWS 基础安全最佳实践	Opensearch.5	Opensearch.5
AWS 基础安全最佳实践	Opensearch.6	Opensearch.6
AWS 基础安全最佳实践	Opensearch.7	Opensearch.7
AWS 基础安全最佳实践	Opensearch.8	Opensearch.8
AWS 基础安全最佳实践	Opensearch.10	Opensearch.10
AWS 基础安全最佳实践	PCA.1	PCA.1
AWS 基础安全最佳实践	RDS.1	RDS.1
AWS 基础安全最佳实践	RDS.2	RDS.2
AWS 基础安全最佳实践	RDS.3	RDS.3
AWS 基础安全最佳实践	RDS.4	RDS.4
AWS 基础安全最佳实践	RDS.5	RDS.5
AWS 基础安全最佳实践	RDS.6	RDS.6
AWS 基础安全最佳实践	RDS.7	RDS.7
AWS 基础安全最佳实践	RDS.8	RDS.8

安全标准	Audit Manager 中支持的关键字 （Security Hub 中的标准控件 ID）	相关控件文档 （Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	RDS.9	RDS.9
AWS 基础安全最佳实践	RDS.10	RDS.10
AWS 基础安全最佳实践	RDS.11	RDS.11
AWS 基础安全最佳实践	RDS.12	RDS.12
AWS 基础安全最佳实践	RDS.13	RDS.13
AWS 基础安全最佳实践	RDS.14	RDS.14
AWS 基础安全最佳实践	RDS.15	RDS.15
AWS 基础安全最佳实践	RDS.16	RDS.16
AWS 基础安全最佳实践	RDS.17	RDS.17
AWS 基础安全最佳实践	RDS.18	RDS.18
AWS 基础安全最佳实践	RDS.19	RDS.19
AWS 基础安全最佳实践	RDS.20	RDS.20
AWS 基础安全最佳实践	RDS.21	RDS.21
AWS 基础安全最佳实践	RDS.22	RDS.22
AWS 基础安全最佳实践	RDS.23	RDS.23
AWS 基础安全最佳实践	RDS.24	RDS.24
AWS 基础安全最佳实践	RDS.25	RDS.25
AWS 基础安全最佳实践	RDS.26	RDS.26

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	RDS.27	RDS.27
AWS 基础安全最佳实践	RDS.34	RDS.34
AWS 基础安全最佳实践	RDS.35	RDS.35
AWS 基础安全最佳实践	Redshift.1	Redshift.1
AWS 基础安全最佳实践	Redshift.2	Redshift.2
AWS 基础安全最佳实践	Redshift.3	Redshift.3
AWS 基础安全最佳实践	Redshift.4	Redshift.4
AWS 基础安全最佳实践	Redshift.6	Redshift.6
AWS 基础安全最佳实践	Redshift.7	Redshift.7
AWS 基础安全最佳实践	Redshift.8	Redshift.8
AWS 基础安全最佳实践	Redshift.9	Redshift.9
AWS 基础安全最佳实践	Redshift.10	Redshift.10
AWS 基础安全最佳实践	Route53.2	Route53.2
AWS 基础安全最佳实践	S3.1	S3.1
AWS 基础安全最佳实践	S3.2	S3.2
AWS 基础安全最佳实践	S3.3	S3.3
AWS 基础安全最佳实践	S3.4	S3.4
AWS 基础安全最佳实践	S3.5	S3.5

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	S3.6	S3.6
AWS 基础安全最佳实践	S3.7	S3.7
AWS 基础安全最佳实践	S3.8	S3.8
AWS 基础安全最佳实践	S3.9	S3.9
AWS 基础安全最佳实践	S3.11	S3.11
AWS 基础安全最佳实践	S3.12	S3.12
AWS 基础安全最佳实践	S3.13	S3.13
AWS 基础安全最佳实践	S3.14	S3.14
AWS 基础安全最佳实践	S3.15	S3.15
AWS 基础安全最佳实践	S3.17	S3.17
AWS 基础安全最佳实践	S3.19	S3.19
AWS 基础安全最佳实践	S3.19	S3.20
AWS 基础安全最佳实践	SageMaker.1	SageMaker.1
AWS 基础安全最佳实践	SageMaker.2	SageMaker.2
AWS 基础安全最佳实践	SageMaker.3	SageMaker.3
AWS 基础安全最佳实践	SecretsManager.1	SecretsManager.1

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	SecretsManager.2	SecretsManager.2
AWS 基础安全最佳实践	SecretsManager.3	SecretsManager.3
AWS 基础安全最佳实践	SecretsManager.4	SecretsManager.4
AWS 基础安全最佳实践	SNS.1	SNS.1
AWS 基础安全最佳实践	SNS.2	SNS.2
AWS 基础安全最佳实践	SQS.1	SQS.1
AWS 基础安全最佳实践	SSM.1	SSM.1
AWS 基础安全最佳实践	SSM.2	SSM.2
AWS 基础安全最佳实践	SSM.3	SSM.3
AWS 基础安全最佳实践	SSM.4	SSM.4
AWS 基础安全最佳实践	StepFunctions.1	StepFunctions.1
AWS 基础安全最佳实践	WAF.1	WAF.1
AWS 基础安全最佳实践	WAF.2	WAF.2
AWS 基础安全最佳实践	WAF.3	WAF.3
AWS 基础安全最佳实践	WAF.4	WAF.4
AWS 基础安全最佳实践	WAF.6	WAF.6

安全标准	Audit Manager 中支持的关键字（Security Hub 中的标准控件 ID）	相关控件文档（Security Hub 中相应的安全控件 ID）
AWS 基础安全最佳实践	WAF.7	WAF.7
AWS 基础安全最佳实践	WAF.8	WAF.8
AWS 基础安全最佳实践	WAF.10	WAF.10
AWS 基础安全最佳实践	WAF.11	WAF.11
AWS 基础安全最佳实践	WAF.12	WAF.12

支持的 API 调用 AWS Audit Manager

Audit Manager 会调用 API AWS 服务 来收集 AWS 资源配置详细信息的快照。在 Audit Manager 中配置自定义控件时，您可以将这些 API 调用指定为数据来源映射。

对于 API 调用范围内的每项资源，Audit Manager 都会捕获配置快照并将其转换为证据。这会导致每个资源只有一份证据，而不是每个 API 调用有一份证据。

例如，如果 `ec2_DescribeRouteTables` API 调用从五个路由表中捕获配置快照，那么对于单个 API 调用，您总共将获得五份证据。每份证据都是单个路由表的配置的快照。

本页内容

支持自定义控件数据来源的 API 调用

在您的自定义控件中，您可以使用以下 API 调用中的任何一个作为数据来源。然后，Audit Manager 可以使用这些 API 调用来收集有关您的 AWS 使用情况的证据。

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
acm_ GetAccountConfiguration	收集与您的 AWS 账户账户关联的账户配置选项快照。
acm_ ListCertificates	检索证书 ARN 和域名列表。
cloudtrail_ DescribeTrails	收集与您的 AWS 账户当前区域关联的一个或多个跟踪记录的设置快照。
云监视_ DescribeAlarms	收集用于 AWS 账户的警报配置快照。
config_ DescribeConfigRules	检索有关您的 AWS Config 规则的详细信息。
config_ DescribeDeliveryChannels	收集 AWS 账户中传递通道的配置快照。
直接连接_ DescribeDirectConnectGateways	检索所有 AWS Direct Connect 网关的列表。
直接连接_ DescribeVirtualGateways	检索 AWS 账户拥有的虚拟专用网关列表。
docdb_ DescribeCertificates	收集 AWS 账户的证书列表。
docdb_describedB ClusterParameterGroups	收集 AWS 账户的 `DBClusterParameterGroup` 描述列表。
docdb_DescribeDBInstances	收集有关为 AWS 账户预置的 Amazon DynamoDB 实例的信息。
dynamodb_ DescribeTable	收集 AWS 账户中 DynamoDB 表的配置快照。 当您将此 API 用作数据来源时，无需提供特定 DynamoDB 表格的名称。相反，Audit Manager 使用 `ListTables` 操作来列出您的所有表格。然后，对于列出的每个表格，Audit Manager 都会执行 `DescribeTable` 操作以生成该资源的证据。
dynamodb_ ListBackups	检索与您的 AWS 账户关联的 DynamoDB 备份列表。
dynamodb_ ListGlobalTables	检索当前 AWS 账户中所有全局表的列表。

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
dynamodb_ ListTables	检索与您的 AWS 账户 和当前端点关联的所有表名称列表。
ec2_ DescribeAddresses	收集弹性 IP 地址快照。
ec2_ DescribeCustomerGateways	收集 VPN 客户网关快照。
ec2_ DescribeEgressOnlyInternetGateways	收集仅限出口的互联网网关快照。
ec2_ DescribeFlowLogs	收集流日志快照。
ec2_ DescribeInstances	收集实例的快照。
ec2_ DescribeInternetGateways	收集互联网网关快照。
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	收集您的虚拟接口组与本地网关路由表之间关联的描述 AWS 账户。
ec2_ DescribeLocalGateways	收集本地网关快照。
ec2_ DescribeLocalGatewayVirtualInterfaces	收集本地网关虚拟接口的快照。
ec2_ DescribeNatGateways	收集 NAT 网关快照。
ec2_ DescribeNetworkAcls	收集网络 ACL 快照。
ec2_ DescribeRouteTables	收集路由表快照。
ec2_ DescribeSecurityGroups	收集安全组快照。
ec2_ DescribeTransitGateways	收集中转网关快照。
ec2_ DescribeVolumes	收集 VPC 端节的快照。

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
ec2_ DescribeVpcs	收集 VPC 的快照。
ec2_ DescribeVpcEndpoints	收集 VPC 端节的快照。
ec2_ DescribeVpcPeering Connections	收集 VPN 连接的快照。
ec2_ DescribeVpnConnect ions	收集 VPN 连接的快照。
ec2_ DescribeVpnGateways	收集虚拟专用网关的快照。
ec2_ GetEbsDefaultKmsKeyId	为您在当前区域收集默认 AWS KMS key 的 EBS AWS 账户 加密快照。
ec2_ GetEbsEncryptionBy Default	描述当前区域中的 AWS 账户 是否默认启用了 EBS 加密。
ecs_ DescribeClusters	收集 ECS 集群的快照。
eks_ DescribeAddonVersions	收集附加组件版本的快照。
elasticache_ DescribeC acheClusters	收集预置集群的快照。
elasticache_ DescribeS erviceUpdates	收集 Amazon 服务更新的快照 ElastiCache。
弹性文件系统_ DescribeA ccessPoints	收集您的 Amazon EFS 接入点的快照 AWS 账户。
弹性文件系统_ DescribeF ileSystems	收集 Amazon EFS 文件系统的快照。
弹性负载均衡 v2_ DescribeL oadBalancers	收集您的 AWS 账户负载均衡器的快照。

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
elasticloadbalancingv2_DescribeSSLPolicies	收集用于 SSL 协商的策略快照。
弹性负载均衡 v2_ DescribeTargetGroups	收集 ELB 目标组的快照。
elasticmapreduce_ ListSecurityConfigurations	检索对 AWS 账户可见的安全配置列表，以及创建日期和时间及其名称。
活动_ ListConnections	检索您的 Amazon EventBridge 连接列表 AWS 账户。
活动_ ListEventBuses	检索您的中的 Amazon EventBridge 事件总线列表 AWS 账户，包括默认事件总线、自定义事件总线和合作伙伴事件总线。
活动_ ListEventSources	检索已与 AWS 账户共享的合作伙伴事件源的列表。
活动_ ListRules	检索您的 Amazon EventBridge 规则列表。
消防水带_ ListDeliveryStreams	检索传输流的列表。
fsx_ DescribeFileSystems	收集 AWS 账户拥有的文件系统快照。
guardduty_ ListDetectors	检索您的 Amazon GuardDuty 探测器资源的列表。`detectorIds`
我是 _ GenerateCredentialReport	为您的 AWS 账户生成凭证报告。
我是 _ GetAccountPasswordPolicy	收集 AWS 账户的密码策略快照。
我是 _ GetAccountSummary	收集 AWS 账户中 IAM 实体使用情况和 IAM 配额的快照。
我是 _ ListGroupPolicies	检索嵌入在您可用的 IAM 群组中的内联策略列表 AWS 账户。
我是 _ ListGroups	检索与您的可用路径前缀关联的 IAM 群组列表 AWS 账户。

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
我是 _ 身份证 ListOpen ConnectProviders	检索 AWS 账户中定义的 IAM OpenID Connect（OIDC）提供商资源对象列表。
我是 _ ListPolicies	检索 AWS 账户中可用的所有托管策略列表，包括您自己的客户定义的托管策略和所有 AWS 托管策略。
我是 _ ListRoles	检索与您的可用路径前缀关联的 IAM 角色列表 AWS 账户。
iam_ListSAMLProviders	检索 AWS 账户的 IAM 中定义的 SAML 提供商资源对象列表。
我是 _ ListUsers	检索您的中的 IAM 用户列表 AWS 账户。
iam_ mfa ListVirtual Devices	检索 AWS 账户中定义的虚拟 MFA 设备列表。
kafka_ ListClusters	检索您的 AWS 账户中的 Amazon MSK 集群列表。
kafka_ ListKafkaVersions	检索 AWS 账户中 Apache Kafka 版本对象列表。
运动学_ ListStreams	检索 Kinesis 数据流列表。
kms_ GetKeyPolicy	Audit Manager 使用此 API 收集 AWS 账户中 AWS KMS keys 密钥策略的快照。 当您将此 API 用作数据源时，无需提供特定的 API 的名称 AWS KMS key。相反，Audit Manager 使用 `ListKeys` 操作来列出您的所有 KMS 密钥。然后，对于列出的每个 KMS 密钥，Audit Manager 都会执行 `GetKeyPolicy` 操作以生成该资源的证据。
kms_ GetKeyRotationStatus	Audit Manager 使用此 API 来收集您的 AWS KMS keys 中是否启用了自动轮换的快照 AWS 账户。 当您将此 API 用作数据源时，无需提供特定的 API 的名称 AWS KMS key。相反，Audit Manager 使用 `ListKeys` 操作来列出您的所有 KMS 密钥。然后，对于列出的每个 KMS 密钥，Audit Manager 都会执行 `GetKeyRotationStatus` 操作以生成该资源的证据。
kms_ ListKeys	检索您的列表 AWS 账户. AWS KMS keys

支持的 API 调用	Audit Manager 如何使用此 API 收集证据
lambda_ ListFunctions	检索您的中的 Lambda 函数列表 AWS 账户，以及每个函数的版本特定配置。
rds_DescribeDBClusters	收集您的 AWS 账户现有 Amazon Aurora 数据库集群和多可用区数据库集群的快照。
rds_DescribeDBInstances	收集 AWS 账户中预置的 RDS 实例的快照。
redshift_ DescribeClusters	收集 AWS 账户中预置的 Amazon Redshift 集群的快照。
s3_ GetBucketEncryption	收集显示 S3 存储桶默认加密配置的快照。 当您将此 API 用作数据来源时，无需提供特定 S3 存储桶的名称。相反，Audit Manager 使用 `ListBuckets` 操作来列出您的所有存储桶。然后，对于列出的每个存储桶，Audit Manager 都会执行 `GetBucketEncryption` 操作以生成该资源的证据。 Audit Manager 只能为与您的评估 AWS 区域 相同创建的存储桶提供加密状态。如果您需要查看多个 S3 存储桶中的所有 S3 存储桶的加密状态 AWS 区域，我们建议您在每个拥有 S3 存储桶 AWS 区域 的地方创建评估。
s3_ ListBuckets	检索您的 AWS 账户中的 S3 存储桶列表。
sns_ ListTopics	检索您 AWS 账户的 SNS 主题列表。
sqs_ ListQueues	检索您 AWS 账户的 SQS 队列列表。

分页的 API 调用

许多人 AWS 服务 收集和存储大量数据。因此，当`list`、`describe` 或 `get` API 调用尝试返回您的数据时，可能会产生很多结果。如果数据量太大而无法在单个响应中返回，则可以通过使用分页将结果分成更易于管理的部分。这会将结果分为“多页”的数据，从而使响应更易于处理。

Audit Manager 支持的某些 API 调用是分页的。这意味着它们首先返回部分结果，并要求后续请求返回整个结果集。例如，Amazon RDS DescribeDBInstances 操作一次最多返回 100 个实例，并且需要后续请求才能返回下一页的结果。

自 2023 年 3 月 8 日起，Audit Manager 支持将分页的 API 调用作为证据收集的数据来源。以前，如果将分页的 API 调用用作数据来源，则 API 响应中只会返回您的一部分资源（最多 100 个结果）。现在，Audit Manager 多次调用分页的 API 操作，并获取每页结果，直到返回所有资源。然后，对于每项资源，Audit Manager 都会捕获配置快照并将其保存为证据。由于您的完整资源集现已在 API 响应中捕获，因此您很可能会注意到收集的证据数量有所增加。

Audit Manager 会自动为您处理 API 调用分页。如果您创建使用分页的 API 调用作为数据来源的自定义控件，则无需指定任何分页参数。

AWS License Manager 标准框架中使用的 API 调用

在 AWS License Manager 标准框架中，Audit Manager 使用名为 `GetLicenseManagerSummary` 的自定义活动来收集证据。该活动调用以下三个 License Manager API：

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

然后，返回的数据将转换为证据，并附加到评测中的相关控件中。

示例

假设您使用了两个许可产品 (SQL Service 2017 和 Oracle Database Enterprise Edition)。首先，该`GetLicenseManagerSummary`活动会调用ListLicenseConfigurationsAPI，它会提供您账户中许可证配置的详细信息。接下来，它通过调用ListUsageForLicenseConfiguration和ListAssociationsForLicenseConfiguration为每个许可证配置添加其他上下文数据。最后，它将许可证配置数据转换为证据，并将其附加到框架中的相应控件中（4.5—SQL Server 2017 的客户托管许可证和 3.0.4 - Oracle Database Enterprise Edition 的客户管理许可证）。

如果您使用的许可产品不受框架中的任何控件保护，则该许可证配置数据将作为证据附加至以下控件中：5.0 - 其他许可证的客户托管许可证。

AWS CloudTrail 支持的事件名称 AWS Audit Manager

您可以在 Audit Manager 中捕获 AWS CloudTrail 管理事件和全球服务事件作为证据。为此，请在创建自定义控件时将 CloudTrail 事件名称指定为数据源映射关键字。

> **Note**
>
> Audit Manager 仅捕获管理事件和全局服务事件。数据事件和见解事件不能作为证据。有关不同类型 CloudTrail 事件的更多信息，请参阅《AWS CloudTrail 用户指南》中的CloudTrail 概念。

除上述情况外，Audit Manager 不支持以下 CloudTrail 事件：

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- kinesis 视频_ GetDataEndpoint
- kinesis 视频_ GetSignalingChannelEndpoint
- kinesis 视频_ DescribeSignalingChannel
- kinesis 视频_ DescribeStream

自 2023 年 5 月 11 日起，Audit Manager 不再支持只读 CloudTrail 事件作为证据收集的关键词。我们总共删除了 3,135 个只读关键词。由于客户和 AWS 服务 都对 API 进行读取调用，因此只读事件干扰很多。因此，只读关键字会收集大量不可靠或与审计无关的证据。只读关键词包括`List`、`Describe`、和 `Get` API 调用（例如，GetObject和 Amazon S3 ListBuckets的只读关键词）。如果您使用其中一个关键字来收集证据，则无需执行任何操作。这些关键词已自动从 Audit Manager 控制台和您的评测中删除，并且不再为这些关键词收集证据。

AWS Audit Manager 设置

您可以随时查看和配置您的 AWS Audit Manager 设置。

访问您的设置

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择设置。

可供使用的设置如下：

- 常规设置
  - 权限
  - 数据加密
  - 委托管理员（可选）
  - AWS Config（可选）
  - Security Hub（可选）
  - 禁用 AWS Audit Manager
- 评测设置
  - 默认审计负责人（可选）
  - 评测报告目标（可选）
  - 通知（可选）
- 证据查找器设置
  - 证据查找器（可选）
  - 导出目标（可选）

常规设置

常规设置选项卡是 Audit Manager 控制台中设置页面的默认视图。使用此选项卡可查看和更新您的常规 Audit Manager 设置。

主题

- 权限

- 数据加密
- 委托管理员（可选）
- AWS Config（可选）
- Security Hub（可选）
- 禁用 AWS Audit Manager

权限

AWS Audit Manager 使用服务相关角色代表您连接到数据来源。有关更多信息，请参阅将服务相关角色用于 AWS Audit Manager。

要查看 Audit Manager 使用的服务相关角色的详细信息，请选择查看 IAM 服务相关角色权限。

有关服务相关角色的更多信息，请参见 IAM 用户指南中的使用服务相关角色。

数据加密

Audit Manager 会自动创建用于安全存储数据的唯一 AWS 托管式密钥。默认情况下，您的 Audit Manager 数据使用此 KMS 密钥进行加密。或者，如果您想自定义数据加密设置，则可以指定自己的对称加密客户托管密钥。使用您自己的 KMS 密钥可以提高灵活性，包括提供创建、轮换和禁用密钥的能力。

> **Important**
>
> 要成功生成评测报告并导出证据查找器搜索结果，您的客户托管密钥（如果您提供）必须与您的评测在相同的 AWS 区域。有关 Audit Manager 区域列表，请参阅Amazon Web Services 一般参考中的 AWS Audit Manager 端点和限额。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更新您的数据加密设置。

Audit Manager console

更新您的数据加密设置（控制台）

1. 在常规设置选项卡中，转到数据加密部分。

2. 要使用 Audit Manager 提供的默认 KMS 密钥，请清除自定义加密设置（高级）复选框。
3. 要使用客户托管密钥，请选中自定义加密设置（高级）复选框。然后您可以选择现有 KMS 密钥或创建新密钥。

AWS CLI

更新您的数据加密设置 (AWS CLI)

运行 update-settings 命令并使用 `--kms-key` 参数指定您自己的客户托管密钥。

在以下示例中，将*#####*替换为您自己的信息。

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

更新您的数据加密设置 (API)

调用 UpdateSettings 操作并使用 kmsKey 参数指定您自己的客户托管密钥。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

> **Note**
>
> 当您更改 Audit Manager 数据加密设置时，这些更改将应用于您创建的任何新评测。这包括您根据新评测创建的任何评测报告和证据查找器导出。
> 这些更改不适用于您在更改加密设置之前已创建的评测。除了现有评测报告和 CSV 导出之外，这还包括您根据现有评测创建的新评测报告和 CSV 导出。现有评测 — 及其所有评测报告和 CSV 导出 — 将继续使用旧的 KMS 密钥。
> 如果生成评测报告的 IAM 身份无法使用旧的 KMS 密钥，则在密钥政策级别授予权限。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。

有关如何创建密钥的说明，请参阅 AWS Key Management Service 用户指南中的创建密钥。

委托管理员（可选）

如果您使用 AWS Organizations 并想要启用 Audit Manager 的多账户支持，则可以将组织中的一个成员账户指定为 Audit Manager 的委托管理员。

先决条件

- 您的账户必须是组织的一部分。有关更多信息，请参阅 AWS Organizations 用户指南中的创建并管理组织。
- 在指定委托管理员之前，您必须启用组织中的所有功能。您还必须配置组织的 Security Hub 设置。这样，Audit Manager 就可以从您的成员账户中收集 Security Hub 证据。
- 委托管理员账户必须有权访问您在设置 Audit Manager 时提供的 KMS 密钥。要查看和更改您的加密设置，请参阅 数据加密。

Audit Manager 中委托管理员的重要注意事项

请注意以下因素，它们定义了委托管理员在 Audit Manager 中如何操作：

管理账户使用

您不能在 Audit Manager 中以委托管理员的身份使用您的 AWS Organizations 管理账户。

跨多个 AWS 区域 使用委托管理员

如果要在多个 AWS 区域 中启用 Audit Manager，则必须在每个区域中分别指定一个委托管理员账户。在您的 Audit Manager 设置中，您应该在所有区域使用相同的委托管理员账户。

证据查找器清理任务

在使用管理账户移除或更改委托管理员之前，请确保当前的委托管理员账户登录到 Audit Manager 并禁用证据查找器。禁用证据查找器会自动删除启用证据查找器时在账户中创建的事件数据存储。

如果此任务未完成，则事件数据存储将保留在其账户中。在这种情况下，我们建议最初的委托管理员使用 CloudTrail Lake 手动删除事件数据存储。

此清理任务是必要的，可确保您最终不会得到多个事件数据存储。移除或更改委托管理员账户后，Audit Manager 会忽略未使用的事件数据存储。但是，如果您不删除未使用的事件数据存储，CloudTrail Lake 将继续对事件数据存储产生存储成本。

数据删除

当您移除 Audit Manager 的委托管理员账户时，该账户的数据不会被删除。如果要删除委托管理员账户的资源数据，则必须先单独执行该任务，然后再移除账户。无论哪种方式，您都可以在 Audit

Manager 控制台中执行此操作。或者，您可以使用 Audit Manager 提供的删除 API 操作之一。有关可用删除操作的列表，请参阅删除 Audit Manager 数据。

目前，Audit Manager 不提供删除特定委托管理员的证据的选项。相反，当您的管理账户取消注册 Audit Manager 时，我们会在取消注册时对当前委托的管理员账户进行清理。

有关 Audit Manager 中常见的组织和委托管理员问题的解决方案，请参阅 委托管理员和 AWS Organizations 问题排查。

为 Audit Manager 管理您的委托管理员账户

您可以按如下方式查看和更改您的委托管理员账户设置。

添加委托管理员

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 添加委托管理员。

> **Note**
>
> 在 Audit Manager 设置中添加委托管理员后，您的管理账户将无法再在 Audit Manager 中创建其他评测。此外，对于管理账户创建的任何现有评测，证据收集将停止。Audit Manager 收集证据并将其附加到委托管理员账户，该账户是管理组织评测的主账户。

Audit Manager console

添加委托管理员（控制台）

1. 在常规设置”选项卡中，转到委托管理员部分。
2. 在委托管理员账户 ID 下，输入委托管理员的账户 ID。
3. 选择委托。

AWS CLI

添加委托管理员 (AWS CLI)

运行 register-organization-admin-account 命令并使用 `--admin-account-id` 参数指定委托管理员的账户 ID。

在以下示例中，将*#####*替换为您自己的信息。

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

添加当前的委托管理员 (API)

调用 RegisterOrganizationAdminAccount 操作并使用 adminAccountId 参数指定委托管理员的账户 ID。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

更改委托管理员

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更改委托管理员。

> **Warning**
>
> 更改委托管理员后，您可以继续访问之前在旧的委托管理员账户下收集的证据。但是，Audit Manager 会停止收集证据并将其附加到旧的委托管理员账户。

Audit Manager console

更改当前的委托管理员（控制台）

1. （可选）如果当前委托管理员（账户 A）启用了证据查找器，请执行以下清理任务：
   - 在将账户 B 分配为新的委托管理员之前，请确保账户 A 登录到 Audit Manager 并禁用证据查找器。

     禁用证据查找器会自动删除账户 A 启用证据查找器时创建的事件数据存储。如果您未完成此步骤，则账户 A 必须转到 CloudTrail Lake 并手动删除事件数据存储。否则，事件数据存储将保留在账户 A 中，并继续产生 CloudTrail Lake 存储费用。
2. 从常规设置选项卡中，转到委托管理员部分，然后选择移除。
3. 在出现的弹出窗口中，选择移除进行确认。

4. 在委托管理员账号 ID 下，输入新的委托管理员账号的 ID。
5. 选择委托。

AWS CLI

开始之前

如果当前委托管理员（账户 A）启用了证据查找器，请执行以下清理任务：

在将账户 B 分配为新的委托管理员之前，请确保账户 A 登录到 Audit Manager 并禁用证据查找器。

禁用证据查找器会自动删除账户 A 启用证据查找器时创建的事件数据存储。如果您未完成此步骤，则账户 A 必须转到 CloudTrail Lake 并手动删除事件数据存储。否则，事件数据存储将保留在账户 A 中，并继续产生 CloudTrail Lake 存储费用。

更改当前的委托管理员 (AWS CLI)

首先，使用 `--admin-account-id` 参数运行 deregister-organization-admin-account 命令来指定当前委托管理员的账户 ID。

在以下示例中，将*#####*替换为您自己的信息。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

然后，使用 `--admin-account-id` 参数运行 register-organization-admin-account 命令来指定新的委托管理员的账户 ID。

在以下示例中，将*#####*替换为您自己的信息。

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

开始之前

如果当前委托管理员（账户 A）启用了证据查找器，请执行以下清理任务：

在将账户 B 分配为新的委托管理员之前，请确保账户 A 登录到 Audit Manager 并禁用证据查找器。

禁用证据查找器会自动删除账户 A 启用证据查找器时创建的事件数据存储。如果您未完成此步骤，则账户 A 必须转到 CloudTrail Lake 并手动删除事件数据存储。否则，事件数据存储将保留在账户 A 中，并继续产生 CloudTrail Lake 存储费用。

更改当前的委托管理员 (API)

首先，调用 DeregisterOrganizationAdminAccount 操作并使用 adminAccountId 参数指定当前委托管理员的账户 ID。

然后，调用 RegisterOrganizationAdminAccount 操作并使用 adminAccountId 参数指定新的委托管理员的账户 ID。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

移除委托管理员

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 移除委托管理员。

> **Warning**
> 移除委托管理员后，您可以继续访问之前在该委托管理员账户下收集的证据。但是，Audit Manager 会停止收集证据并将其附加到旧的委托管理员账户。

Audit Manager console

移除当前的委托管理员（控制台）

1. （可选）如果当前委托管理员启用了证据查找器，请执行以下清理任务：
   - 确保当前委托管理员账户登录到 Audit Manager 并禁用证据查找器。

     禁用证据查找器会自动删除启用证据查找器时在其账户中创建的事件数据存储。如果此步骤未完成，则委托管理员账户必须使用 CloudTrail Lake 手动删除事件数据存储。否则，事件数据存储将保留在其账户中，并继续产生 CloudTrail Lake 存储费用。
2. 从常规设置选项卡中，转到委托管理员部分，然后选择移除。
3. 在出现的弹出窗口中，选择移除进行确认。

AWS CLI

开始之前

如果当前委托管理员启用了证据查找器，请执行以下清理任务：

确保当前委托管理员账户登录到 Audit Manager 并禁用证据查找器。

禁用证据查找器会自动删除启用证据查找器时在其账户中创建的事件数据存储。如果此步骤未完成，则委托管理员账户必须使用 CloudTrail Lake 手动删除事件数据存储。否则，事件数据存储将保留在其账户中，并继续产生 CloudTrail Lake 存储费用。

移除当前的委托管理员 (AWS CLI)

运行 deregister-organization-admin-account 命令并使用 `--admin-account-id` 参数指定委托管理员的账户 ID。

在以下示例中，将*#####*替换为您自己的信息。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

开始之前

如果当前委托管理员启用了证据查找器，请执行以下清理任务：

确保当前委托管理员账户登录到 Audit Manager 并禁用证据查找器。

禁用证据查找器会自动删除启用证据查找器时在其账户中创建的事件数据存储。如果此步骤未完成，则委托管理员账户必须使用 CloudTrail Lake 手动删除事件数据存储。否则，事件数据存储将保留在其账户中，并继续产生 CloudTrail Lake 存储费用。

移除当前的委托管理员 (API)

调用 DeregisterOrganizationAdminAccount 操作并使用 adminAccountId 参数指定委托管理员的账户 ID。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

AWS Config（可选）

您可以允许 Audit Manager 从 AWS Config 中收集调查发现。启用 AWS Config 后，Audit Manager 可以通过直接从 AWS Config 中报告规则检查结果，以捕获资源安全状况的快照。我们建议您在 Audit Manager 中启用 AWS Config，以获得最佳体验。

要启用 AWS Config，请选择启用 AWS Config 以转到该服务。有关如何启用 AWS Config 的说明，请参阅 AWS Config 开发人员指南中的设置 AWS Config。

Security Hub（可选）

您可以允许 Audit Manager 导入支持合规标准的 AWS Security Hub 调查发现。启用 Security Hub 后，Audit Manager 可以直接从 Security Hub 通过安全检查结果来捕获资源安全状态的快照。我们建议您启用 Security Hub，以便在 Audit Manager 中获得最佳体验。

要启用 Security Hub，请选择启用 Security Hub 以转到该服务。有关如何启用 Security Hub 的说明，请参阅 Security Hub 用户指南中的设置 Security HubAWS Security Hub。

禁用 AWS Audit Manager

如果不想再使用 Audit Manager，则可以禁用其服务。禁用 Audit Manager 后，您还可以选择删除所有数据。

默认情况下，当您禁用 Audit Manager 时，您的数据不会被删除。您的证据数据自创建之日起保留两年。您的其他 Audit Manager 资源（包括评测、自定义控件和自定义框架）将无限期保留，如果您将来重新启用 Audit Manager，则这些资源将可用。有关数据留存的更多信息，请参阅本指南中的数据保护。

如果您选择删除数据，Audit Manager 会删除所有证据数据以及您创建的所有 Audit Manager 资源（包括评测、自定义控件和自定义框架）。您的所有数据将在禁用 Audit Manager 后的七天内删除。

> **Warning**
>
> - 禁用 Audit Manager 后，您的访问权限将被撤销，并且该服务将不再收集任何现有评测的证据。除非重新启用 Audit Manager，否则您无法访问服务中的任何内容。
> - 删除所有数据是一项永久性操作。如果您决定将来重新启用 Audit Manager，则您的数据将无法恢复。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 禁用 Audit Manager。

Audit Manager console

禁用 Audit Manager（控制台）

1. 从常规设置选项卡中，转到禁用 AWS Audit Manager 部分。
2. 选择 Disable（禁用 Amazon Macie)。
3. 在弹出窗口中，查看您当前的数据留存设置。

   a. 要继续当前的选择，请选择禁用 Audit Manager。

   b. 要更改当前选择，请执行以下步骤：

      i. 选择取消以返回设置页面。

      ii. 要使用默认的数据留存设置，请关闭删除所有数据。此选择将证据数据自创建之日起保留两年，并无限期保留其他 Audit Manager 资源。

      iii. 要删除您的数据，请开启删除所有数据。

      iv. 选择禁用，然后选择禁用 Audit Manager 以确认您的选择。

AWS CLI

开始之前

在禁用 Audit Manager 之前，您可以运行 update-settings 命令来设置首选的数据留存策略。默认情况下，Audit Manager 会保留您的数据。如果您想请求删除数据，请使用 `--deregistration-policy` 参数并将 `deleteResources` 值设置为 `ALL`。

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

禁用 Audit Manager (AWS CLI)

当您准备好禁用 Audit Manager 时，运行 deregister-account 命令。

```
aws auditmanager deregister-account
```

Audit Manager API

开始之前

在禁用 Audit Manager 之前，您可以使用 UpdateSettings API 操作来设置首选的数据留存策略。默认情况下，Audit Manager 会保留您的数据。如果您想删除数据，可以使用 DeregistrationPolicy 属性来请求删除您的数据。

禁用 Audit Manager (API)

当您准备好禁用 Audit Manager 时，请调用 DeregisterAccount 操作。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括：如何在其中一个指定语言的 AWS 软件开发工具包中使用操作和参数的信息。

在禁用 Audit Manager 之后将其重新启用

转到 Audit Manager 服务主页并按照步骤将 Audit Manager 设置为新用户。有关更多信息，请参阅设置 AWS Audit Manager。

> **Tip**
>
> - 如果您在禁用 Audit Manager 时选择删除数据，则必须等到数据被删除后才能重新启用该服务。根据您拥有的数据量，这可能需要长达七天的时间。但是，在此之前，可以随时尝试重新启用 Audit Manager。在许多情况下，数据会在短短一小时内被删除。
> - 如果您在禁用 Audit Manager 时选择不删除数据，则您的现有评测将进入休眠状态并因此停止收集证据。如需重新开始为先前存在的评测收集证据，请编辑评测并选择保存，而不做任何更改。

评测设置

使用此选项卡查看和更新您的评测设置。

主题

- 默认审计负责人（可选）
- 评测报告目标（可选）
- 通知（可选）

默认审计负责人（可选）

您可以在 Audit Manager 中指定对您的评测拥有主要访问权限的默认审计负责人。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更新此设置。

Audit Manager console

您可以从表格中列出的 AWS 账户 中进行选择，也可以使用搜索栏查找其他 AWS 账户。

更新您的默认审计负责人设置（控制台）

1. 在评测设置选项卡中，转到默认审计负责人部分，然后选择编辑。
2. 要添加默认审计负责人，请选中审计负责人下面账户名称旁边的复选框。
3. 要移除默认审计负责人，请清除审计负责人下面账户名称旁边的复选框。
4. 完成操作后，选择保存。

AWS CLI

更新您的默认审计负责人设置 (AWS CLI)

运行 update-settings 命令并使用 `--default-process-owners` 参数指定审计负责人。

在以下示例中，将*#####*替换为您自己的信息。请注意，`roleType` 只能是 `PROCESS_OWNER`。

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

更新您的默认审计负责人设置 (API)

调用 UpdateSettings 操作并使用 defaultProcessOwners 参数指定默认审计负责人。请注意，`roleType` 只能是 `PROCESS_OWNER`。

有关审计负责人的更多信息，请参阅本指南概念和术语部分中的审计负责人。

评测报告目标（可选）

生成评测报告时，Audit Manager 会将报告发布到您选择的 S3 存储桶。此 S3 存储桶被称为评测报告目标。您可以选择 Audit Manager 用于存储评测报告的 Amazon S3 存储桶。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更新此设置。

Audit Manager console

更新您的评测报告目标设置（控制台）

1. 在评测设置选项卡中，转到评测报告目标部分。
2. 要使用现有的 Amazon S3 存储桶，请从下拉菜单中选择存储桶名称。
3. 要创建新的 Amazon S3 存储桶，请选择创建新的 S3 存储桶。
4. 完成操作后，选择保存。

AWS CLI

更新您的评测报告目标设置 (AWS CLI)

运行 update-settings 命令并使用 `--default-assessment-reports-destination` 参数指定 S3 存储桶。

在以下示例中，将*#####*替换为您自己的信息：

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

更新您的评测报告目标设置 (API)

调用 UpdateSettings 操作并使用 defaultAssessmentReportsDestination 参数指定 S3 存储桶。

有关如何创建 S3 存储桶的说明，请参阅 Amazon S3 用户指南中的创建存储桶。

评测报告目标的配置提示

为确保成功生成评测报告，我们建议您验证评测报告目标的以下配置。

同区域存储桶

建议您使用与评测在相同 AWS 区域 中的 S3 存储桶。当您使用同区域存储桶和评测时，您的评测报告最多可以包含 22,000 个证据项目。相反，当您使用跨区域存储桶和评测时，只能包含 3,500 个证据项目。

AWS 区域

您的客户托管密钥（如果您提供了密钥）的 AWS 区域 必须与您的评测区域和您的评测报告目标 S3 存储桶相匹配。有关如何更改 KMS 密钥的说明，请参阅 AWS Audit Manager 设置，数据加密。有关如何更改 S3 存储桶的说明，请参阅 AWS Audit Manager设置，评测报告目标。有关受支持的 Audit Manager 区域列表，请参阅 Amazon Web Services 一般参考中的 AWS Audit Manager 端点和限额。

S3 存储桶加密

如果您的评测报告目标的存储桶策略要求使用 SSE-KMS 进行服务器端加密（SSE），那么在该存储桶策略中使用的 KMS 密钥必须与您在 Audit Manager 数据加密设置中配置的 KMS 密钥匹配。如果您尚未在 Audit Manager 设置中配置 KMS 密钥，并且您的评测报告目标存储桶策略需要 SSE，请确保存储桶策略允许 SSE-S3。有关如何配置用于数据加密的 KMS 密钥的说明，请参阅数据加密设置。

跨账户 S3 存储桶

Audit Manager 控制台不支持使用跨账户 S3 存储桶作为评测报告目标。可以使用 AWS CLI 或其中一个 AWS SDK 将跨账户存储桶指定为评测报告目标，但为简单起见，我们建议您不要这样做。如果您确实选择使用跨账户 S3 存储桶作为评测报告目标，请考虑以下几点。

- 默认情况下，S3 对象（例如评测报告）归上传对象的 AWS 账户 所有。您可以使用 S3 对象所有权设置来更改此默认行为，以便由具有 `bucket-owner-full-control` 标准访问控制列表（ACL）的账户写入的任何新对象都会自动归存储桶所有者拥有。

  尽管这不是必需的，但我们建议您对跨账户存储桶设置进行以下更改。进行这些更改可确保存储桶所有者完全控制您发布到其存储桶的评测报告。

  - 将 S3 存储桶的对象所有权设置为首选存储桶所有者，而不是默认的对象写入者
  - 添加存储桶策略以确保上传到该存储桶的对象具有 `bucket-owner-full-control` ACL
- 要允许 Audit Manager 在跨账户 S3 存储桶中发布报告，您必须将以下 S3 存储桶策略添加到您的评测报告目标。将`#####`替换为您自己的信息。此策略中的 `Principal` 元素是负责评测并创建评测报告的用户或角色。`Resource` 指定发布报告的跨账户 S3 存储桶。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

通知（可选）

Audit Manager 可以向您在此设置中指定的 Amazon S主题发送通知。如果您订阅了该 SNS 主题，则在登录 Audit Manager 时会收到通知。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更新此设置。

Audit Manager console

更新您的通知设置（控制台）

1. 在评测设置选项卡中，转到通知部分。
2. 要使用现有 SNS 主题，请从下拉菜单中选择主题名称。
3. 要创建新 SNS 主题，请选择创建新主题。
4. 完成操作后，选择保存。

AWS CLI

更新您的通知设置 (AWS CLI)

运行 update-settings 命令并使用 `--sns-topic` 参数指定 SNS 主题。

在以下示例中，将*#####*替换为您自己的信息：

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

更新您的通知设置 (API)

调用 UpdateSettings 操作并使用 snsTopic 参数指定 SNS 主题。

> **Note**
>
> 您可以使用标准 SNS 主题，也可以使用 FIFO（先进先出）SNS 主题。尽管 Audit Manager 支持向 FIFO 主题发送通知，但不能保证消息的发送顺序。
> 如果您需要使用自己并不拥有的 Amazon SNS 主题，请为此配置您的 AWS Identity and Access Management IAM policy。更具体地说，您必须将其配置为允许从主题的 Amazon 资源名称（ARN）发布。有关 IAM 的更多信息，请参阅 AWS Audit Manager 的身份和访问管理。

要详细了解在 Audit Manager 中调用通知的操作列表，请参阅 AWS Audit Manager 中的通知。

有关如何创建 Amazon SNS 主题的信息，请参阅 Amazon SNS 用户指南中的创建 Amazon SNS 主题。

证据查找器设置

使用此选项卡查看和更新您的证据查找器设置。

主题

证据查找器（可选）

我们强烈建议您启用证据查找器。如果您想对证据进行搜索查询，则必须启用此功能。

请按照以下步骤启用、禁用或检查证据查找器的状态。

启用证据查找器

您必须在每个要搜索证据的 AWS 区域 启用证据查找器。如果您是 Audit Manager 的委托管理员，请启用证据查找器以搜索组织中所有成员账户的证据。

启用证据查找器所需的权限

要启用证据查找器，您需要在 CloudTrail Lake 中创建和管理事件数据存储的权限。要使用该功能，您需要具有执行 CloudTrail Lake 查询的权限。有关您可以使用的权限策略示例，请参阅允许完全管理员访问权限。

如果您需要权限方面的帮助，请联系您的 AWS 管理员。如果您是 AWS 管理员，则可以复制所需的权限声明并将其附加到 IAM policy 中。

请求启用证据查找器

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 来完成此任务。

Audit Manager console

请求启用证据查找器（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 从证据查找器设置选项卡中，转到证据查找器部分。
3. 选择所需权限策略，然后选择查看 CloudTrail Lake 权限以查看所需的证据查找器权限。如果您还没有这些权限，则可以复制此策略声明并将其附加到 IAM policy 中。
4. 请选择启用。
5. 在弹出窗口中，选择请求启用。

AWS CLI

请求启用证据查找器 (AWS CLI)

将 update-settings 命令与 `--evidence-finder-enabled` 参数一起运行。

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

请求启用证据查找器 (API)

调用 UpdateSettings 操作并使用 evidenceFinderEnabled 参数。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

确认证据查找器 的状态

提交请求后，启用证据查找器和创建事件数据存储最多需要 10 分钟。一旦创建了事件数据存储，所有新的证据就会被导入事件数据存储中。

启用证据查找器并创建事件数据存储后，我们会在新创建的事件数据存储中重新填充您过去两年的证据。此过程会自动进行，最多需要七天才能完成。

您可以使用 Audit Manager 控制台、AWS CLI、或 Audit Manager API 查看证据查找器的当前状态。

Audit Manager console

查看证据查找器的当前状态（控制台）

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在启用证据查找器 — 可选下，查看当前状态。

   每种状态的定义如下所示：

   - 证据查找器未启用 — 您尚未成功启用证据查找器。
   - 您已请求启用证据查找器 — 您的请求正在等待事件数据存储的创建。
   - 证据查找器已启用 — 事件数据存储已创建。您现在可以使用证据查找器。

根据您拥有的证据量，用您过去的证据数据回填新的事件数据存储最多需要七天。蓝色的信息面板表示数据回填正在进行中。在此期间，请随时开始浏览证据查找器。但是，请记住，在回填完成之前，并非所有数据都可用。

- 您已请求禁用证据查找器 — 您的请求正在等待删除事件数据存储。
- 证据查找器已被禁用 — 证据查找器已被永久禁用，事件数据存储已删除。

AWS CLI

查看证据查找器的当前状态 (AWS CLI)

调用 get-settings 命令，并将 `--attribute` 参数设置为 `EVIDENCE_FINDER_ENABLEMENT`。

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

这将返回以下信息：

enablementStatus

此属性显示证据查找器的当前状态。

- `ENABLE_IN_PROGRESS` — 您已请求启用证据查找器。目前正在创建事件数据存储以支持证据查找器查询。
- `ENABLED` — 已创建事件数据存储并启用了证据查找器。我们建议您等待 7 天，直到事件数据存储库中回填您过去的证据数据。在此期间，您可以使用证据查找器，但在回填完成之前，并非所有数据都可用。
- `DISABLE_IN_PROGRESS` — 您已请求禁用证据查找器，但您的请求正在等待删除事件数据存储。
- `DISABLED` — 您已永久禁用证据查找器，并且删除了事件数据存储。此后，您将无法重新启用证据查找器。

backfillStatus

此属性显示证据数据回填的当前状态。

- `NOT_STARTED` — 回填尚未开始。
- `IN_PROGRESS` — 回填正在进行中。这最多需要七天才能完成，具体取决于证据数据的数量。

- COMPLETED — 回填完成。您过去的所有证据现在都可以查询。

Audit Manager API

查看证据查找器的当前状态 (API)

调用 GetSettings 操作，并将 attribute 参数设置为 EVIDENCE_FINDER_ENABLEMENT。这将返回以下信息：

enablementStatus

此属性显示证据查找器的当前状态。

- ENABLE_IN_PROGRESS - 您已请求启用证据查找器。目前正在创建事件数据存储以支持证据查找器查询。
- ENABLED - 已创建事件数据存储并启用了证据查找器。我们建议您等待 7 天，直到事件数据存储库中回填您过去的证据数据。在此期间，您可以使用证据查找器，但在回填完成之前，并非所有数据都可用。
- DISABLE_IN_PROGRESS — 您已请求禁用证据查找器，但您的请求正在等待删除事件数据存储。
- DISABLED - 您已永久禁用证据查找器，并且删除了事件数据存储。此后，您将无法重新启用证据查找器。

backfillStatus

此属性显示证据数据回填的当前状态。

- NOT_STARTED 表示回填尚未开始。
- IN_PROGRESS 表示回填正在进行中。这最多需要七天才能完成，具体取决于证据数据的数量。
- COMPLETED 表示回填完成。您过去的所有证据现在都可以查询。

有关更多信息，请参阅 Audit Manager API 参考中的 evidenceFinderEnablement。

禁用证据查找器

如果您不再想使用证据查找器，可以随时禁用此功能。

> **Warning**
>
> 禁用证据查找器会删除 Audit Manager 创建的 CloudTrail Lake 事件数据存储。因此，您无法重新启用该功能。要在禁用证据查找器后重新使用它，您必须禁用 AWS Audit Manager，然后完全重新启用该服务。

禁用证据查找器所需的权限

要禁用证据查找器，您需要有删除 CloudTrail Lake 中的事件数据存储的权限。有关您可以使用的策略示例，请参阅禁用证据查找器的权限。

如果您需要权限方面的帮助，请联系您的 AWS 管理员。如果您是 AWS 管理员，则可以将所需的权限声明附加到 IAM policy 中。

禁用证据查找器

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 来完成此任务。

Audit Manager console

禁用证据查找器（控制台）

1. 在 Audit Manager 设置页面的证据查找器部分，选择禁用。
2. 在出现的弹出窗口中，输入 **Yes** 以确认您的决定。
3. 选择请求禁用。

AWS CLI

禁用证据查找器 (AWS CLI)

将 update-settings 命令与 `--no-evidence-finder-enabled` 参数一起运行。

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

禁用证据查找器 (API)

调用 UpdateSettings 操作并使用 evidenceFinderEnabled 参数。

如需了解更多信息，请选择前面的任一链接，在 Audit Manager API 参考中阅读更多内容。其中包括有关如何在特定于语言的 AWS SDK 中使用此操作和参数的信息。

导出目标（可选）

在证据查找器中运行查询时，可以将搜索结果导出到逗号分隔值 (CSV) 文件中。使用此设置选择 Audit Manager 用于保存导出文件的默认 S3 存储桶。

您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 或 Audit Manager API 更新此设置。

> **Important**
>
> 您的 S3 存储桶必须具有所需的权限策略，才能允许 CloudTrail 向其写入导出文件。更具体地说，存储桶策略必须包括 `s3:PutObject` 操作和存储桶 ARN，并将 CloudTrail 列为服务主体。我们提供了一个权限策略示例以供您使用。有关如何将此策略附加至 S3 存储桶的说明，请参阅使用 Amazon S3 控制台添加存储桶策略。
> 有关更多提示，请参阅本页面上的导出目标的配置提示。

Audit Manager console

更新您的导出目标设置（控制台）

1. 从证据查找器设置选项卡中，转到导出目标部分。
2. 请选择以下任一选项：
   - 如果要移除当前 S3 存储桶，请选择移除以清除您的设置。
   - 如果您想首次保存默认 S3 存储桶，请继续执行步骤 3。
3. 指定要用于存储导出文件的 S3 存储桶。
   - 选择浏览 S3，从您的存储桶列表中选择。
   - 或者，您可以输入以下格式的存储桶 URI：**`s3://bucketname/prefix`**

> **Tip**
>
> 要使目标存储桶井井有条，您可以为 CSV 导出创建一个可选文件夹。为此，请在资源 URI 框中的值前后附加一个斜杠 (**/**) 和一个前缀（例如 **/**

evidenceFinderCSVExports）。然后，Audit Manager 在将 CSV 文件添加至存储桶时会包含此前缀，而且 Amazon S3 会生成由该前缀指定的路径。有关 Amazon S3 中前缀的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的组织 Amazon S3 控制台中的对象。

4. 完成操作后，选择保存。

有关如何创建 S3 存储桶的说明，请参阅 Amazon S3 用户指南中的创建存储桶。

AWS CLI

更新您的导出目标设置 (AWS CLI)

运行 update-settings 命令并使用 `--default-export-destination` 参数指定 S3 存储桶。

在以下示例中，将*#####*替换为您自己的信息：

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

有关如何创建 S3 存储桶的说明，请参阅《AWS CLI 命令参考》中的 create-bucket。

Audit Manager API

更新您的导出目标设置 (API)

调用 UpdateSettings 操作并使用 defaultExportDestination 参数指定 S3 存储桶。

有关如何创建 S3 存储桶的说明，请参阅 Amazon S3 API 参考中的 CreateBucket。

导出目标的配置提示

为确保成功导出文件，我们建议您验证导出目标的以下配置。

AWS 区域

您的客户托管密钥（如果您提供了密钥）的 AWS 区域 必须与您的评测区域相匹配。有关如何更改 KMS 密钥的说明，请参阅 Audit Manager 数据加密设置。

跨账户 S3 存储桶

Audit Manager 控制台不支持使用跨账户 S3 存储桶作为导出目标。可以使用 AWS CLI 或其中一个 AWS SDK 指定跨账户存储桶，但为简单起见，我们建议您不要这样做。如果您确实选择使用跨账户 S3 存储桶作为导出目标，请考虑以下几点。

- 默认情况下，S3 对象（例如 CSV 导出）归上传对象的 AWS 账户 所有。您可以使用 S3 对象所有权设置来更改此默认行为，以便由具有 `bucket-owner-full-control` 标准访问控制列表（ACL）的账户写入的任何新对象都会自动归存储桶所有者拥有。

  尽管这不是必需的，但我们建议您对跨账户存储桶设置进行以下更改。进行这些更改可确保存储桶所有者完全控制您发布到其存储桶的导出文件。

  - 将 S3 存储桶的对象所有权设置为首选存储桶所有者，而不是默认的对象写入者
  - 添加存储桶策略以确保上传到该存储桶的对象具有 `bucket-owner-full-control` ACL

- 要允许 Audit Manager 将文件导出到跨账户 S3 存储桶，您必须将以下 S3 存储桶策略添加到您的导出目标存储桶。将*#####*替换为您自己的信息。此策略中的 `Principal` 元素是负责评测并导出文件的用户或角色。`Resource` 指定要将文件导出到的跨账户 S3 存储桶。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
```

```
    ]
}
```

AWS Audit Manager 中的通知

AWS Audit Manager 可以通过 Amazon Simple Notification Service (Amazon SNS) 通知您用户操作。

在发生下列事件之一时，Audit Manager 会发送通知：

- 审计负责人委托控制集进行审查。
- 委托人向审计负责人提交经过审核的控制集。
- 审计负责人完成对控制集的审查。

先决条件

在 Audit Manager 中设置 Amazon SNS 通知之前，请确保您已完成以下步骤。

1. 如果您还没有主题，请在 Amazon SNS 中创建一个主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的创建 Amazon SNS 主题。
2. 使用至少一个终端节点订阅主题。例如，如果您要通过文本消息接收通知，则为 SMS 端点订阅该主题。SMS 端点是一个移动电话号码。要通过电子邮件接收通知，使用电子邮件端点订阅主题。电子邮件端点是电子邮件地址。

   有关更多信息，请参阅 Amazon Simple Notification Service Developer Guide 中的入门。
3. （可选）如果您的主题使用 AWS Key Management Service (AWS KMS) 进行服务器端加密（SSE），则必须向 AWS KMS key 策略中添加权限。有关您可以使用的策略示例，请参阅附加到 SNS 主题的 KMS 密钥的权限。

在 AWS Audit Manager 中配置通知

按照这些步骤在 AWS Audit Manager 中配置通知。

在 AWS Audit Manager 中配置通知

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在通知 - 可选）下，指定要用于接收通知的 SNS 主题。

   - 要使用现有主题，请从下拉菜单中选择主题名称。

- 要创建新主题，请选择创建新主题。这会将您带到 Amazon SNS 控制台，您可以在其中创建主题。

4. 完成此操作后，选择保存。

> **注意**
>
> - 您可以使用标准 SNS 主题，也可以使用 FIFO（先进先出）SNS 主题。Audit Manager 支持向 FIFO 主题发送通知。但是，不能保证消息的发送顺序。
> - 如果您需要使用自己并不拥有的 Amazon SNS 主题，则必须配置您的 AWS Identity and Access Management IAM policy。更具体地说，您必须配置策略以允许从主题的 Amazon 资源名称（ARN）发布。有关更多信息，请参阅 AWS Audit Manager 的身份和访问权限管理。

故障排除

要查找常见问题和答案，请参阅本指南疑难解答部分中的解决通知问题。

在 AWS Audit Manager 中进行问题排查

您可以使用以下信息排查在使用 AWS Audit Manager 时遇到的问题。

如果以下信息未涵盖您遇到的问题，或者在您尝试解决问题后问题仍然存在，请联系 AWS Support。

主题

对评测和证据收集问题进行排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的评测和证据收集问题。

主题

- 我的评测创建失败
- 我禁用了 Audit Manager 然后又重新启用了 Audit Manager，现在，我以前的评测不再收集证据

我创建了评测，但我还看不到任何证据

如果您看不到任何证据，则很可能是距离您创建评测还不满 24 小时，或者存在配置错误。

建议您检查以下项目：

1. 确保距离您创建评测已满 24 小时。评测创建后 24 小时可获得自动证据。
2. 确保您使用的 Audit Manager 与您期望看到的证据所涉及 AWS 服务 处于同一 AWS 区域。
3. 如果您希望看到 AWS Config 和 AWS Security Hub 的合规检查证据，请确保 AWS Config 和 Security Hub 控制台都显示这些检查的结果。AWS Config 和 Security Hub 结果应显示在您使用 Audit Manager 的同一 AWS 区域。

如果您仍然无法在评测中看到证据，且并非上述某一问题导致，请查看本页上描述的其他潜在原因。

我的评测没有从 AWS Security Hub 中收集合规检查证据

如果您没有看到 AWS Security Hub 控件的合规检查证据，则可能是以下某一问题导致。

AWS Security Hub 中配置缺失

如果您在启用 AWS Security Hub 时遗漏了某些配置步骤，则可能会导致此问题。

请确保您已启用 Security Hub 并按如下方式配置您的设置。

确认单个 AWS 账户 的 Security Hub 设置

如果您使用单个 AWS 账户，请检查以下各项：

- 确认您已为账户启用 AWS Config 并配置资源记录。
- 确认您已为账户启用 PCI DSS 安全标准。
- 确认您在 Security Hub 中已打开合并控件调查发现设置。

确认一个组织的 Security Hub 设置

如果您使用 Organizations，请检查以下各项：

- 确认您已为组织启用 AWS Config 并配置资源记录。
- 确认您已为组织的每个成员账户启用 PCI DSS 安全标准。
- 确认您在 Security Hub 中已打开合并控件调查发现设置。
- 确认您在 Security Hub 中使用的委托管理员账户与您在 Audit Manager 中使用的委托管理员账户相同。
- 确认您已将您的组织账户启用为 Security Hub 成员账户。

您 **`ControlMappingSource`** 中输入的 Security Hub 控件名称不正确

使用 Audit Manager API 创建自定义控件时，可以将 Security Hub 控件指定为证据收集的数据来源映射。为此，请输入控件 ID 作为 `keywordValue`。

如果您没有看到 Security Hub 控件的合规检查证据，则可能您 `ControlMappingSource` 中输入的 `keywordValue` 不正确导致。`keywordValue` 区分大小写。如果输入不正确，Audit Manager 可能无法识别该规则。因此，您可能无法按预期收集该控件的合规检查证据。

如需解决此问题，请更新自定义控件并修改 `keywordValue`。Security Hub 关键字的正确格式不固定。为确保准确，请参考支持的 Security Hub 控件关键字列表。

`AuditManagerSecurityHubFindingsReceiver` Amazon EventBridge 规则缺失

启用 Audit Manager 后，名为 `AuditManagerSecurityHubFindingsReceiver` 的规则会自动在 Amazon EventBridge 中创建并启用。此规则允许 Audit Manager 收集 Security Hub 的调查发现作为证据。

如果在您使用 Security Hub 的 AWS 区域 中未列出并启用此规则，则 Audit Manager 将无法收集该区域的 Security Hub 调查发现。

如需解决此问题，请前往 EventBridge 控制台并确认 `AuditManagerSecurityHubFindingsReceiver` 规则存在于您的 AWS 账户 中。如果该规则不存在，我们建议您禁用 Audit Manager 后重新启用该服务。如果此操作不解决问题，或者无法禁用 Audit Manager，请联系 AWS Support 获取帮助。

由 Security Hub 创建的服务相关 AWS Config 规则

请注意 Audit Manager 不会从 Security Hub 创建的服务相关 AWS Config 规则收集证据。这是一种特定类型的托管 AWS Config 规则，由 Security Hub 服务启用和控制。即使已存在相同规则的其他实例，Security Hub 也会在您的 AWS 环境中创建这些服务相关规则的实例。因此，为防止证据重复，Audit Manager 不支持从服务相关规则中收集证据。

我的评测没有从 AWS Config 中收集合规检查证据

以下某一问题可能导致您看不到 AWS Config 规则的合规检查证据。

您 **ControlMappingSource** 中输入的规则标识符不正确

使用 Audit Manager API 创建自定义控件时，可以将 AWS Config 规则指定为证据收集的数据来源映射。您指定的 `keywordValue` 取决于规则的类型。

您 `ControlMappingSource` 中输入的 `keywordValue` 不正确可能导致您看不到 AWS Config 控件的合规检查证据。`keywordValue` 区分大小写。如果输入不正确，Audit Manager 可能无法识别规则。因此，您可能无法按预期收集该规则的合规检查证据。

如需解决此问题，请更新自定义控件并修改 `keywordValue`。

- 对于自定义规则，请确保 `keywordValue` 的 `Custom_` 前缀后跟自定义规则名称。自定义规则名称的格式不固定。为确保准确，请访问 AWS Config 控制台验证您的自定义规则名称。
- 对于托管规则，请确保 `keywordValue` 是 `ALL_CAPS_WITH_UNDERSCORES` 中的规则标识符。例如，`CLOUDWATCH_LOG_GROUP_ENCRYPTED`。为了确保准确，请参阅支持的托管规则关键字列表。

> **Note**
>
> 对于某些托管规则，规则标识符与规则名称不同。例如，restricted-ssh 的规则标识符是 `INCOMING_SSH_DISABLED`。确保使用规则标识符，而不是规则名称。如需查找规则标识符，请从托管规则列表中选择一条规则，然后查找其标识符值。

该规则是服务相关 AWS Config 规则

您可以使用托管规则和自定义规则作为证据收集的数据来源映射。但是，大多数服务相关规则都不是 Audit Manager 证据收集的来源。

Audit Manager 仅从两种类型的服务相关规则中收集证据：

- 一致性包中的服务相关规则
- 来自 AWS Organizations 的服务相关规则

Audit Manager 不会从其他服务相关规则中收集证据，特别是 Amazon 资源名称（ARN）包含前缀 `arn:aws:config:*:*:config-rule/aws-service-rule/...` 的任何规则：

Audit Manager 之所以不从大多数服务相关 AWS Config 规则中收集证据的原因是防止评测中出现重复的证据。服务相关的规则是一种独特类型的托管规则，可支持其他 AWS 服务 在您的账户中

创建 AWS Config 规则。例如，某些 Security Hub 控件使用 AWS Config 服务相关规则来运行安全检查。对于使用一个服务相关 AWS Config 规则的每个 Security Hub 控件，Security Hub 在您的 AWS 环境中创建所需的 AWS Config 规则实例。即使您的账户中已存在原始规则，也会发生这种情况。因此，为了避免两次从同一条规则中收集相同的证据，Audit Manager 会忽略服务相关规则，也不会从中收集证据。

AWS Config 未启用且未作为服务包含在范围内

AWS Config 必须在您的 AWS 账户 内启用。它还必须作为一项服务包含在您的评测范围内。以这种方式设置 AWS Config 后，每次评测 AWS Config 规则时，Audit Manager 都会收集证据。

首先，请确保已在 AWS 账户 中启用 AWS Config。有关说明，请参阅启用和设置 AWS Config。

接下来，请确保您将 AWS Config 作为一项服务包括在评测范围内。如需查看目前评测范围内的服务，请参阅查看评测，AWS 服务 选项卡。如需编辑评测范围内的服务列表，请参阅编辑范围内 AWS 服务。

在您设置评测之前，该 AWS Config 规则已评测资源配置

如果您的 AWS Config 规则设置为评测特定资源的配置更改，则可能会发现 AWS Config 中的评测与 Audit Manager 中的证据不匹配。如果您在 Audit Manager 评测中设置控件之前，已进行规则评测，则会发生这种情况。在这种情况下，在基础资源状态再次发生变更并触发对规则的重新评测之前，Audit Manager 不会生成证据。

您可以在 AWS Config 控制台中导航到该规则，然后手动重新评测该规则，以此作为一种变通方法。这将调用对该规则相关所有资源进行的新评测。

我的评测没有从 AWS CloudTrail 中收集用户活动证据

使用 Audit Manager API 创建自定义控件时，您可以将 CloudTrail 事件名称指定为证据收集的数据来源映射。为此，请输入事件名称作为 `keywordValue`。

如果您看不到某个 CloudTrail 事件的用户活动证据，则可能是您的 `ControlMappingSource` 中输入的 `keywordValue` 不正确。`keywordValue` 区分大小写。如果输入不正确，Audit Manager 可能无法识别事件名称。因此，您可能无法按预期收集该事件的用户活动证据。

如需解决此问题，请更新自定义控件并修改 `keywordValue`。确保事件写入为 `serviceprefix_ActionName`。例如，`cloudtrail_StartLogging`。为确保准确，请查看服务授权参考中的 AWS 服务 前缀和操作名称。

我的评测没有收集 AWS API 调用的配置数据证据

使用 Audit Manager API 创建自定义控件时，可以将 AWS API 调用指定为证据收集的数据来源映射。为此，您可以将 API 调用输入为 `keywordValue`。

您 `ControlMappingSource` 中输入的 `keywordValue` 不正确可能导致您看不到某个 AWS API 调用的配置数据证据。`keywordValue` 区分大小写。如果输入不正确，Audit Manager 可能无法识别 API 调用。因此，您可能无法按预期收集该 API 调用的配置数据证据。

如需解决此问题，请更新自定义控件并修改 `keywordValue`。确保 API 调用写入为 `serviceprefix_ActionName`。例如，`iam_ListGroups`。为确保准确，请参阅支持的 API 调用列表。

我的评测没有从另一 AWS 服务 中收集证据

如果 AWS 服务 未选定为评测范围内的服务，则 Audit Manager 不会从该服务相关资源中收集证据。如果未在自己的环境中启用选择的 AWS 服务，也会出现这种情况。

如果您使用自定义框架创建评测，您可以编辑评测范围内的服务。然后，您指定作为证据收集来源的其他 AWS 服务。添加这些服务 24 小时后即可获得证据。

> **Note**
>
> 如果您已根据标准框架创建评测，则范围内 AWS 服务 的列表为预先预定列表，无法编辑。这是因为当您根据标准框架创建评测时，Audit Manager 会自动为您映射和选择相关数据来源和服务。此选择基于标准框架要求。注意，对于仅包含手动控件的标准框架，AWS 服务 均不在范围内。
>
> 确保既可以编辑范围内 AWS 服务 又可以根据标准框架创建评测的变通方法是自定义标准框架。通过使用此变通方法，您可以使用您自定义的框架来创建新的评测。在此评测中，您可以指定范围内的 AWS 服务。

我的证据是在不同的时间间隔生成的，我不确定收集证据的频率

Audit Manager 评测中的控件映射至各类数据来源。数据来源的证据收集频率各异。因此，对于证据收集频率，没有一个放之四海而皆准的答案。有些数据来源评测合规性，而其他数据来源仅捕获资源状态并更改数据，而无需确定合规性。

以下是不同数据来源类型及其收集证据频率的摘要。

数据来源类型	描述	证据收集频率	当此控件在评测中处于活动状态时
AWS CloudTrail	跟踪特定的用户活动。	持续	Audit Manager 会根据您选择的关键字筛选您的 CloudTrail 日志。处理后的日志将作为用户活动证据导入。
AWS Security Hub	通过报告来自 Security Hub 的调查发现，捕获您资源安全状况的快照。	根据 Security Hub 检查的时间表 (通常每 12 小时左右检查一次)	Audit Manager 直接从 Security Hub 检索安全调查发现。调查发现作为合规检查证据导入。
AWS Config	通过报告来自 AWS Config 的调查发现，捕获您资源安全状况的快照。	基于 AWS Config 规则中定义的设置	Audit Manager 直接从 AWS Config 中检索规则评测。评测作为合规检查证据导入。
AWS API 调用	通过对指定 AWS 服务 的 API 调用，直接拍摄资源配置的快照。	每天、每周或每月。	Audit Manager 根据您指定的频率进行 API 调用。响应作为配置数据证据导入。

无论证据收集频率如何，只要评测处于活动状态，就会自动收集新的证据。如需更多信息，请参阅证据收集频率。

如需了解更多信息，请参阅自动证据支持的控件数据来源和更改控件的证据收集频率。

我从我的组织中移除一个范围内账户后会发生什么？

从您的组织中移除范围内的帐户后，Audit Manager 将不再为该账户收集证据。但是，该账户会继续在您的评测中的AWS 账户选项卡下显示。如需将该账户从范围内的账户列表中移除，请编辑评测。在编辑过程中，已移除的账户不再显示在列表中，该账户不在范围内不影响变更的保存。

我无法编辑评测的范围内服务

当您使用 Audit Manager 控制台从标准框架创建评测时，默认情况下会选择范围内 AWS 服务 的列表。此列表无法编辑。这是因为 Audit Manager 会自动为您映射和选择数据来源和服务。此选择基于标准框架要求。如果您选择的标准框架仅包含手动控件，则 AWS 服务 均不在评测范围内，并且您无法向评测添加任何服务。

如果您需要编辑范围内的服务列表，请使用 Audit Manager 提供的 UpdateAssessment API 操作。或者，您可以自定义标准框架，然后通过自定义框架创建评测。

范围内的服务和数据来源类型有什么区别？

范围内的服务是AWS 服务指定为评测部分的服务。当某项服务在范围内时，Audit Manager 会收集有关您使用该服务及其资源的证据。

数据来源类型表示证据的确切收集来源。如果您上传自己的证据，则数据来源类型为手动。Audit Manager 从以下 4 种数据来源之一收集证据。

1. AWS Security Hub — 通过报告来自 Security Hub 的调查发现，捕获您资源安全状况的快照。
2. AWS Config — 通过报告来自 AWS Config 的调查发现，捕获您资源安全状况的快照。
3. AWS CloudTrail — 跟踪资源的特定用户活动。
4. AWS API 调用 — 通过对特定 AWS 服务 的 API 调用，直接拍摄资源配置的快照。

以下是两个示例，用于说明范围内服务和数据来源类型之间的区别。

示例 1

假设您要为名为 4.1.2 — 不允许对 S3 桶的公开写入访问权限的控件收集证据。此控件会检查您的 S3 桶策略的访问级别。对于此控件，Audit Manager 使用特定 AWS Config 规则 (s3-bucket-public-write-prohibited) 查找 S3 桶的评测。在本示例中，以下为 true：

- 范围内服务是 Amazon S3
- 正在评测的资源是您的 S3 桶
- 数据来源的类型是 AWS Config。
- 数据来源映射是AWS Config一项特定规则 (`s3-bucket-public-write-prohibited`)

示例 2

假设您想为名为 164.308(a)(5)(ii)(C) 的 HIPAA 控件收集证据。此控件需要通过监控程序检测不当登录。对于此控件，Audit Manager 使用 CloudTrail 日志来查找所有 AWS 管理控制台登录事件。在本示例中，以下为 true：

- 范围内服务是 IAM
- 正在评测的资源是您的用户
- 数据来源类型为 CloudTrail
- 数据来源映射是一个特定的 CloudTrail 事件 (`ConsoleLogin`)

我的评测创建失败

如果您的评测创建失败，则可能是因为您选择包含在评测范围中的 AWS 账户 过多。如果您使用的是 AWS Organizations，在单个评测的范围内，Audit Manager 最多支持 150 个成员账户。如果超过此数量，评测创建可能会失败。作为一种变通办法，您可以运行多个评测，每个评测包含不同的账户。

我禁用了 Audit Manager 然后又重新启用了 Audit Manager，现在，我以前的评测不再收集证据

当您禁用 Audit Manager 并选择不删除数据时，您的现有评测将进入休眠状态并停止收集证据。这意味着，当您重新启用 Audit Manager 时，您之前创建的评测仍然可用。但是，他们不会自动恢复证据收集工作。

如需重新开始为先前存在的评测收集证据，请编辑评测并选择保存，而不做任何更改。

评测报告问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的评测报告问题。

主题

- 我的评测报告生成失败
- 我按照上述核对清单操作，但我的评测报告仍然无法生成
- 当我尝试生成报告时，出现拒绝访问的错误消息
- 我无法解压评测报告
- 我在报告中选择证据名称不会将我重定向到证据详情
- 我的评测报告生成一直处于进行中状态，我不确定这会对我的账单产生什么影响
- 另请参阅

我的评测报告生成失败

您的评测报告可能由于多种原因而无法生成。您可以通过检查最常见的原因进行问题排查。从以下核对清单入手：

1. 检查您的任何 AWS 区域 信息是否不匹配：
   a. 您的客户托管密钥 AWS 区域 是否与您的评测 AWS 区域 相符？

      如果您为 Audit Manager 数据加密提供了自己的 KMS 密钥，则该密钥必须与您的评测 AWS 区域 相同。如需解决此问题，请将 KMS 密钥更改为与您的评测位于同一区域的密钥。有关如何更改 KMS 密钥的说明，请参阅 AWS Audit Manager 设置，数据加密。

   b. 您的客户托管密钥 AWS 区域 与您的 S3 桶 AWS 区域 的密钥是否匹配？

      如果您为 Audit Manager 数据加密提供了自己的 KMS 密钥，则该密钥必须与您用作评测报告目的地的 S3 桶处于同一 AWS 区域。要解决此问题，您可以更改 KMS 密钥或 S3 桶，以便其与您的评测处于同一个区域。有关如何更改 KMS 密钥的说明，请参阅 AWS Audit Manager 设置，数据加密。有关如何更改 S3 存储桶的说明，请参阅 AWS Audit Manager设置，评测报告目标。
2. 检查您用作评测报告目的地的 S3 桶的权限：
   a. 生成评测报告的 IAM 实体是否拥有 S3 桶的必要权限？

      IAM 实体必须具有在该桶中发布报告所需的 S3 桶权限。我们提供了一个策略示例以供您使用。有关如何指定其他 S3 桶的说明，请参阅 AWS Audit Manager 设置，评测报告目的地。

   b. S3 桶是否有要求使用 SSE-KMS 进行服务器端加密 (SSE) 的桶策略？

      如果是，则该桶策略中使用的 KMS 密钥必须与 Audit Manager 数据加密设置中指定的 KMS 密钥相匹配。如果您没有在 Audit Manager 设置中配置 KMS 密钥，并且您的 S3 桶策略需要 SSE，请确保桶策略允许 SSE-S3。有关如何更改 KMS 密钥的说明，请参阅 AWS Audit Manager 设置，数据加密。有关如何更改 S3 存储桶的说明，请参阅 AWS Audit Manager设置，评测报告目标。

如果您仍然无法成功生成评测报告，请查看此页面上的以下问题。

我按照上述核对清单操作，但我的评测报告仍然无法生成

Audit Manager 限制了您可以向评测报告中添加的证据数量。该限制取决于您的评测 AWS 区域、用作评测报告目的地的 S3 桶的区域，以及您的评测是否使用客户托管 AWS KMS key。

1. 同区域报告的上限为 22,000 (S3 桶和评测处于同一 AWS 区域)

2. 跨区域报告的上限为 3,500 (S3 桶和评测处于不同 AWS 区域)

3. 如果评测使用客户托管 KMS 密钥，则限制为 3,500

如果您尝试生成包含更多证据的报告，该操作可能会失败。

作为一种变通方法，您可以生成多份评测报告，而不是生成一份较大的评测报告。通过这样做，您可以将评测中的证据导出为大小更易于管理的批次。

当我尝试生成报告时，出现拒绝访问的错误消息

如果您的评测由委托管理员账户创建，且您 Audit Manager 设置中指定的 KMS 密钥不属于该账户，则会收到 `access denied` 错误消息。为避免此错误，在为 Audit Manager 指定委托管理员时，请确保委托的管理员账户有权访问您在设置 Audit Manager 时提供的 KMS 密钥。

如果您对用作评测报告目的地的 S3 桶没有写入权限，也可能会收到 `access denied` 错误消息。

如果您遇到 `access denied` 错误，确保您满足以下要求：

- 您的 Audit Manager 设置中的 KMS 密钥向委托的管理员授予权限。您可以按照 AWS Key Management Service 开发人员指南中允许其他账户中的用户使用 KMS 密钥中的说明进行配置。有关如何在 Audit Manager 中审核和更改加密设置的说明，请参阅数据加密。
- 您的权限策略授予您对用作评测报告目的地的 S3 桶的写入权限。具体而言，您的权限策略包含一项 `s3:PutObject` 操作，指定 S3 桶的 ARN，并包括用于加密评测报告的 KMS 密钥。有关您可以使用的策略示例，请参阅 AWS Audit Manager 基于身份的策略示例。

> **Note**
>
> 如果您更改了 Audit Manager 数据加密设置，则这些更改将应用于您今后创建的新评测。这包括您根据新评测创建的任何评测报告。
> 这些更改不适用于您在更改加密设置之前已创建的评测。除现有评测报告外，这还包括您根据现有评测创建的新评测报告。现有评测及其评测报告继续使用旧的 KMS 密钥。如果生成评测报告的 IAM 身份无权使用旧 KMS 密钥，您可以授予密钥政策级权限。

我无法解压评测报告

如果您无法在 Windows 上解压评测报告，很可能因为其文件路径有多个嵌套的文件夹或长名称导致 Windows 资源管理器无法解压该报告。这是因为，在 Windows 文件命名系统下，文件夹路径、文件名和文件扩展名不能超过 259 个字符。否则，这会导致 `Destination Path Too Long` 错误。

要解决此问题，请尝试将 zip 文件移动到其当前位置的父文件夹。然后，您可以再次尝试在其中进行提取。或者，您也可以尝试缩短 zip 文件的名称或将其提取到文件路径较短的其他位置。

我在报告中选择证据名称不会将我重定向到证据详情

如果您在浏览器中与评测报告进行交互，或者使用操作系统上安装的默认 PDF 阅读器，则可能会出现此问题。某些浏览器和系统默认的 PDF 阅读器不允许打开对应的链接。这意味着，尽管在评测报告摘要 PDF 中超链接可能有用(例如目录中的超链接控件名称)，但当您尝试从评测摘要 PDF 导航到单独的证据详情 PDF 时，超链接将被忽略。

如果您遇到此问题，我们建议您使用专用 PDF 阅读器与评测报告进行交互。为了确保体验的可靠性，我们建议您安装和使用 Adobe Acrobat Reader，您可以在 Adobe 网站上下载该阅读器。其他 PDF 阅读器也可用，但事实证明，Adobe Acrobat Reader 可以持续可靠地处理 Audit Manager 评测报告。

我的评测报告生成一直处于进行中状态，我不确定这会对我的账单产生什么影响

评测报告的生成对计费没有影响。我们仅根据您评测收集的证据向您收费。有关定价的更多信息，请参阅 AWS Audit Manager 定价。

另请参阅

以下页面包含有关通过证据查找器生成评测报告的问题排查指南：

- 我无法根据搜索结果生成多份评测报告
- 我无法将个人搜索结果添加到评测报告中
- 部分证据查找器结果不包含在评测报告中
- 我想根据搜索结果生成评测报告，但是我的查询语句不起作用

控件和控制集问题排查

您可以使用此页面上的信息来解决 Audit Manager 中控件的常见问题。

一般性问题

- 我在评测中看不到任何控件或控制集
- 我无法上传手动证据至控件

AWS Config 集成问题

- 我需要使用多个 AWS Config 规则作为单个控件的数据来源
- 配置控件数据来源时，自定义规则选项不可用
- 自定义规则选项可用，但下拉列表中没有显示任何规则
- 部分自定义规则可用，但我看不到我想要使用的规则
- 我找不到我想要使用的托管规则
- 我想共享一个自定义框架，但该框架包含使用自定义 AWS Config 规则作为数据来源的控件。收件人能否为这些控件收集证据？
- 在 AWS Config 中更新自定义规则后会发生什么？ 我是否需要在 Audit Manager 中执行任何操作？

我在评测中看不到任何控件或控制集

简而言之，如需查看评测的控件，必须将您指定为该评测的审计负责人。此外，您需要必要的 IAM 权限才能查看和管理相关的 Audit Manager 资源。

如果您需要访问评测中的控件，请要求该评测的审计负责人之一将您指定为审计负责人。在创建或编辑评测时，您可以指定审计负责人。

此外，请确保您具备管理评测所需的权限。我们建议审计负责人使用 AWSAuditManagerAdministratorAccess 策略。如果您需要有关 IAM 权限的帮助，请联系您的管理员或 AWS Support。有关如何将策略附加到 IAM 身份的更多信息，请参阅 IAM 用户指南中的向用户添加权限以及添加和移除 IAM 身份权限。

我无法上传手动证据至控件

如果您无法手动将证据上传到控件，可能原因是因为该控件处于非活动状态。

如需上传手动证据至控件，您必须先将控件状态更改为正在审核或已审核。有关更多信息，请参阅更新控件状态。

> **Important**
>
> 每个 AWS 账户 每天最多只能将 100 个证据文件手动上传至一个控件。超过此每日配额，会导致该控件的任何其他手动上传失败。如果您需要将大量手动证据上传至单个控件，请在几天内分批上传证据。

我需要使用多个 AWS Config 规则作为单个控件的数据来源

您可以将托管规则和自定义规则组合用于单个控件。为此，请为控件设置多个数据来源，然后为每个数据来源选择首选的规则类型。您可以为单个自定义控件定义最多 10 个数据来源。

配置控件数据来源时，自定义规则选项不可用

这意味着您无权查看您 AWS 账户 或组织的自定义规则。具体而言，您无权在 Audit Manager 控制台中执行 DescribeConfigRules 操作。

要解决此问题，请联系您的 AWS 管理员获取帮助。如果您是 AWS 管理员，则可以通过管理 IAM policy 为您的用户或群组提供权限。

自定义规则选项可用，但下拉列表中没有显示任何规则

这意味着您 AWS 账户 或组织中没有可用的自定义规则。

如果您在 AWS Config 中还没有任何自定义规则，则可以创建一个。有关说明，请参阅 AWS Config 开发人员指南中的 AWS Config 自定义规则。

如果您希望看到自定义规则，请查看以下问题排查项目。

部分自定义规则可用，但我看不到我想要使用的规则

以下其中一个问题可导致您看不到希望找到的自定义规则。

您的账户已排除在规则之外

您正在使用的委托管理员账户可能排除在规则之外。

您所在组织的管理账户 (或其中一个 AWS Config 委托管理员账户) 可以使用 AWS Command Line Interface (AWS CLI) 创建自定义组织规则。创建时，他们可以指定需要从规则中排除的账户列表。如果您的账户在此列表中，则该规则在 Audit Manager 中不可用。

要解决此问题，请联系您的 AWS Config 管理员获取帮助。如果您是 AWS Config 管理员，则可以通过运行 put-organization-config-rule 命令来更新排除的帐户列表。

该规则在 AWS Config 中创建和启用失败

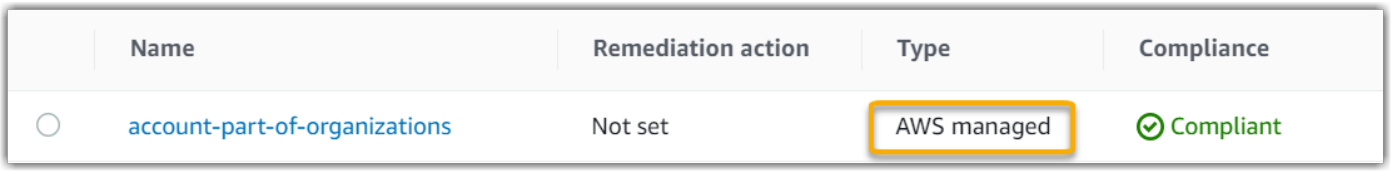
自定义规则也可能创建和启用失败。如果创建规则时出错，或者规则未启用，则该规则不会出现在 Audit Manager 的可用规则列表中。

我们建议您联系 AWS Config 获取有关该问题的帮助。

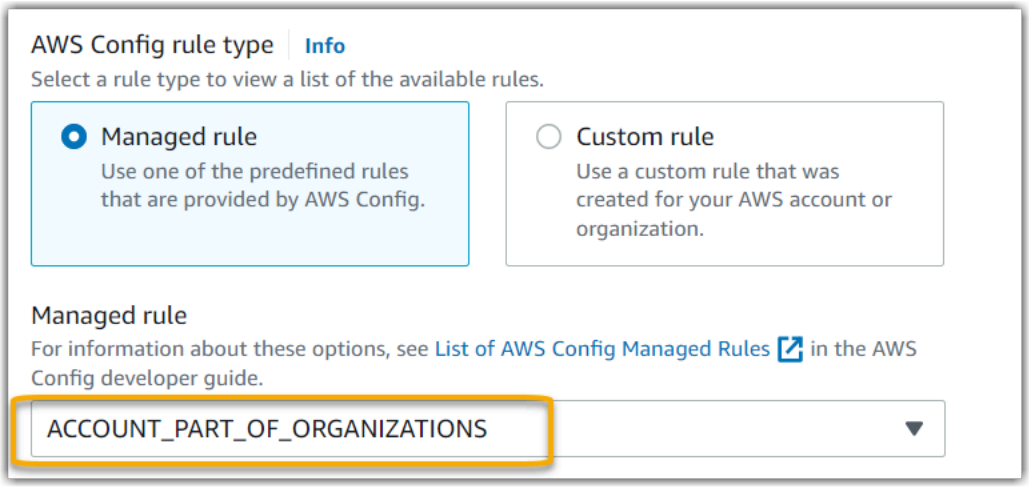
该规则属于托管规则

如果您在自定义规则的下拉列表中找不到要查找的规则，则该规则可能是托管规则。

您可以使用 AWS Config 控制台来验证规则是否为托管规则。为此，从左侧导航菜单中，选择规则，然后在表格中查找规则。如果是托管规则，则类型列显示 AWS 托管。

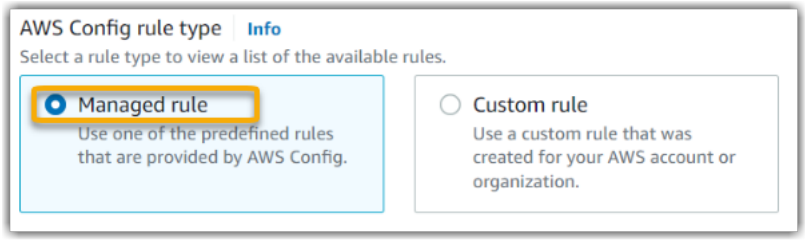


确认属于托管规则后，返回 Audit Manager 并选择托管规则作为规则类型。然后，在托管规则的下拉列表中查找托管规则标识符关键字。



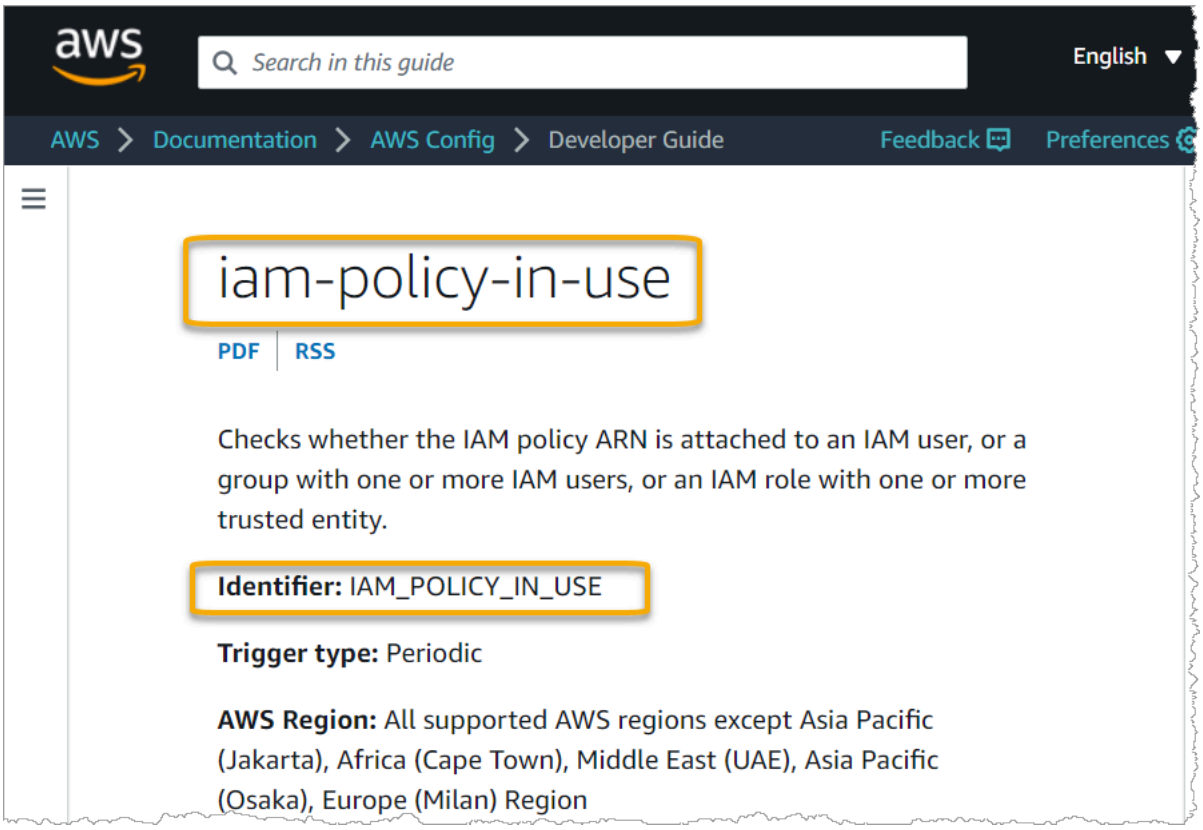
我找不到我想要使用的托管规则

在 Audit Manager 控制台的下拉列表中选择规则之前，请确保已选择托管规则作为规则类型。

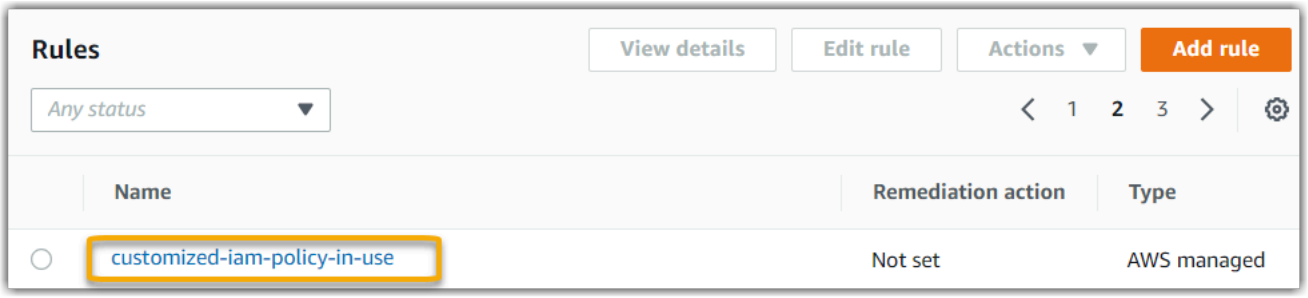


如果您仍然看不到期望找到的托管规则，有可能您查找的是规则名称。您必须查找规则标识符。

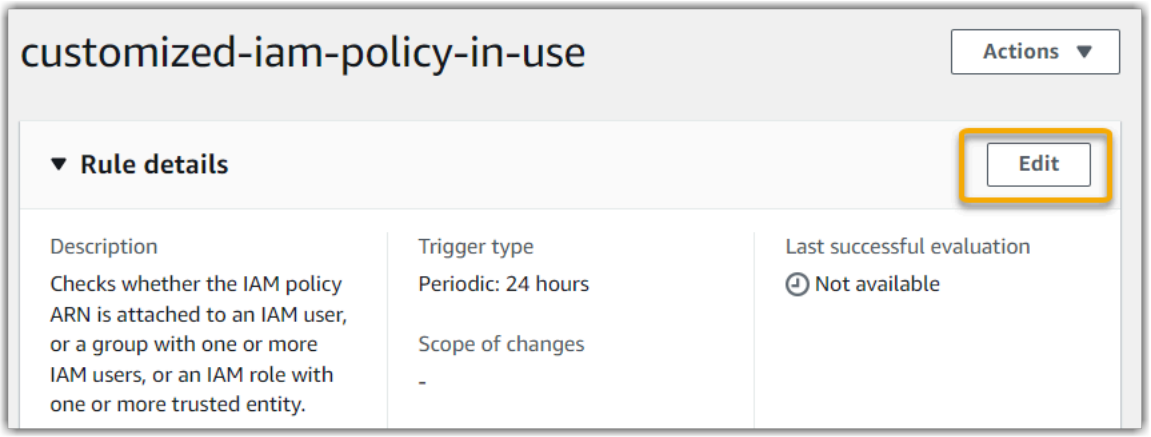
如果您使用的是默认托管规则，则名称和标识符相似。名称为小写并使用破折号 (例如，`iam-policy-in-use`)。标识符为大写并使用下划线 (例如，`IAM_POLICY_IN_USE`)。如需查找默认托管规则的标识符，请查看支持的 AWS Config 托管规则关键字列表，然后点击想要使用的规则的链接。该链接会将您带至该托管规则的 AWS Config 文档。您可以在文档中找到名称和标识符。在 Audit Manager 下拉列表中查找标识符关键字。



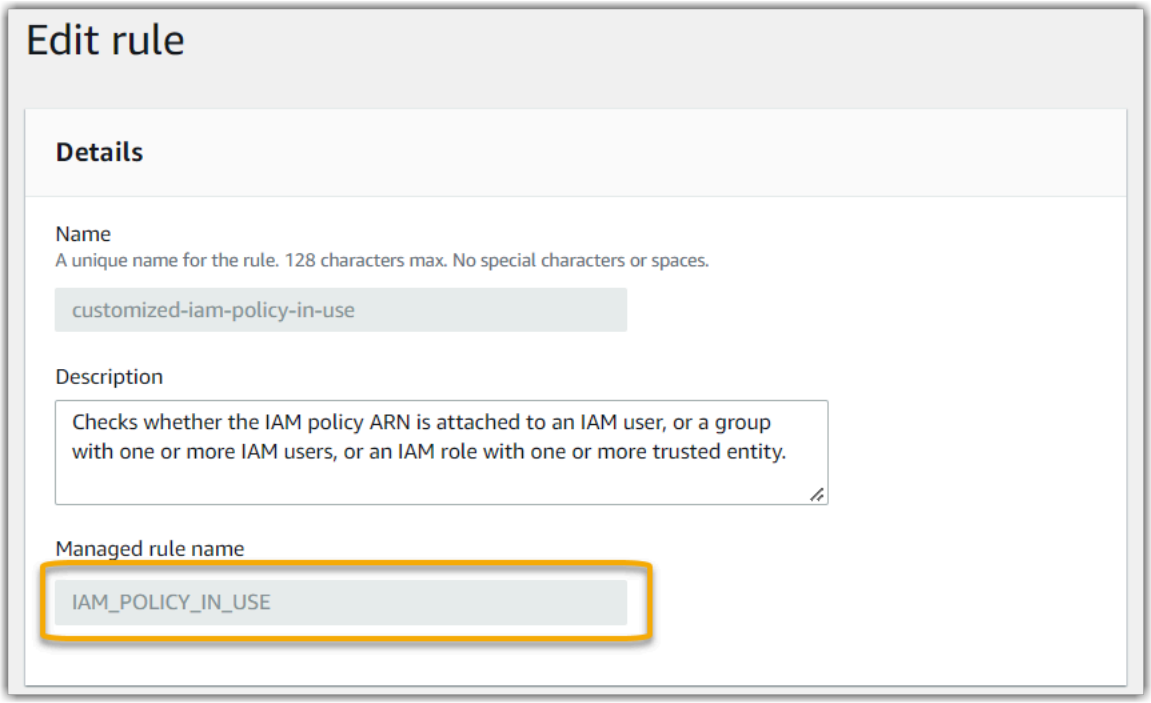
如果您使用的是自定义托管规则，则可以使用 AWS Config 控制台查找规则标识符。例如，假设您要使用名为 `customized-iam-policy-in-use` 的托管规则。如需查找此规则的标识符，请转到 AWS Config 控制台，在左侧导航菜单中选择规则，然后在表格中选择规则。



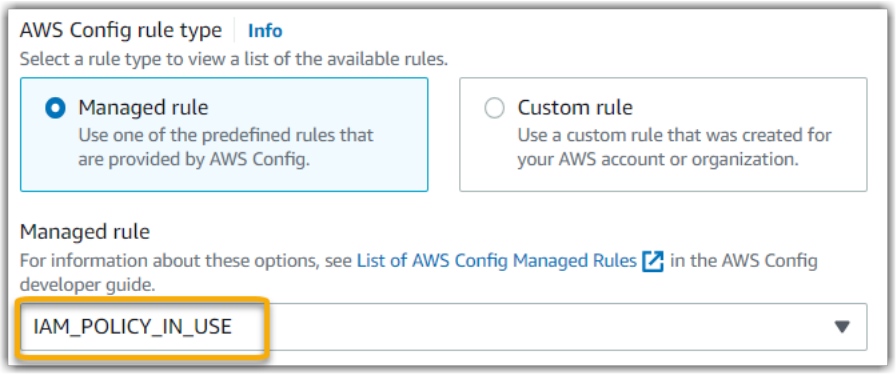
选择编辑 以打开有关托管规则的详细信息。



在详细信息部分，您可以找到创建托管规则依据的源标识符 (IAM_POLICY_IN_USE)。



现在，您可以返回 Audit Manager 控制台，从下拉列表中选择相同的标识符关键字。



我想共享一个自定义框架，但该框架包含使用自定义 AWS Config 规则作为数据来源的控件。收件人能否为这些控件收集证据？

是的，收件人可以为这些控件收集证据，但是在此之前需要采取一些步骤。

要让 Audit Manager 使用 AWS Config 规则作为数据来源映射收集证据，以下条件必须为 true。这适用于托管规则和自定义规则。

1. 该规则必须存在于收件人的 AWS 环境中
2. 该规则必须在收件人的 AWS 环境中启用

注意，收件人 AWS 环境中可能不存在您账户中的自定义 AWS Config 规则。此外，当收件人接受共享请求时，Audit Manager 不会在其账户中重新创建您的任何自定义规则。要让收件人使用您的自定义规则作为数据来源映射收集证据，他们必须在自己的 AWS Config 实例中创建相同的自定义规则。在收件人创建并启用规则后，Audit Manager 可以从该数据来源收集证据。

我们建议您与收件人沟通，告知他们是否需要在他们的 AWS Config 实例中创建任何自定义规则。

在 AWS Config 中更新自定义规则后会发生什么？ 我是否需要在 Audit Manager 中执行任何操作？

您 AWS 环境范围内的规则更新

如果您在 AWS 环境中更新自定义规则，则无需在 Audit Manager 中执行任何操作。Audit Manager 可检测并处理规则更新，如下表中所述。当检测到规则更新时，Audit Manager 不会通知您。

情况	Audit Manager 会做什么	您需要了解的内容
您的 AWS Config 实例中的自定义规则已更新。	Audit Manager 继续使用更新的规则定义报告该规则的调查发现。	无需任何操作。
您的 AWS Config 实例中的自定义规则已删除。	Audit Manager 停止报告已删除规则的调查发现。	无需任何操作。 如果需要，您可以编辑使用已删除规则作为数据来源映射的自定义控件。这样做有助于通过移除已删除的规则来清除数据来源设置。否则，已删除的规则名称将保留为未使用的数据来源映射。

您 AWS 环境范围外的规则更新

如果在您的 AWS 环境范围外更新了自定义规则，则 Audit Manager 不会检测到规则更新。如果您使用共享的自定义框架，则需要考虑这一点。这是因为，在这种情况下，发件人和收件人各自在不同的 AWS 环境中工作。下表提供了针对此场景建议进行的操作。

您的角色	情况	建议的操作
发件人	• 您共享了一个使用自定义规则作为数据来源映射的框架。 • 共享框架后，您在 AWS Config 中更新或删除了其中一项规则。	让收件人知道您的更新。这样，他们就可以应用相同的更新并与最新的规则定义保持同步。
收件人	• 您接受了使用自定义规则作为数据来源映射的共享框架。 • 在您的 AWS Config 实例中重新创建自定义规则后，发件人更新或删除了其中一项规则。	在您自己的 AWS Config 实例中更新相应的规则。

控制面板问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的控制面板问题。

主题

我的控制面板上没有任何数据

如果每日快照小组件中的数字显示连字符 (-)，则表示没有可用数据。您必须至少有一个活动的评测才能在控制面板中查看数据。要开始使用，请创建评测。24 小时后，您的评测数据开始显示在控制面板中。

> **Note**
>
> 如果每日快照小部件中的数字显示为零 (0)，则表示您的活动中评测 (或所选评测) 没有不合规的证据。

CSV 下载选项不可用

此选项仅适用于个人评测。请确保已对控制面板应用 the section called “评测筛选器”，然后重试。请记住，一次只能下载一个 CSV 文件。

我在尝试下载 CSV 文件时看不到下载的文件

如果控制域包含大量控件，则 Audit Manager 生成 CSV 文件时可能会有短暂的延迟。文件生成后即自动下载。

如果您仍然看不到下载的文件，请确保您的互联网连接正常并且您使用的是最新版本的网络浏览器。此外，请查看您的最近下载文件夹。文件会下载到浏览器决定的默认位置。如果问题未解决，请尝试使用其他浏览器下载文件。

控制面板中缺少特定的控件或控制域

这可能意味着您的活动评测 (或指定的评测) 没有该控件或控制域的任何相关数据。

仅当同时满足以下两个条件时，控制域才会显示在控制面板上：

- 您的活动中评测 (或指定的评测) 至少包含一个与该域相关的控件
- 该域中至少有一个控件在控制面板顶部的日期收集了证据

仅当控件在控制面板顶部日期收集了证据时，才会在域中显示该控件。

每日快照显示每天不同数量的证据。是否正常？

部分证据并非每天收集。Audit Manager 评测中的控件映射至各类数据来源，每个数据来源的证据收集时间表不必相同。因此，预计每日快照会显示每天不同数量的证据。如需有关证据收集频率的更多信息，请参阅 AWS Audit Manager 如何收集证据。

委托管理员和 AWS Organizations 问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的委托管理员问题。

主题

我无法使用我的委派管理员账户设置 Audit Manager

尽管 AWS Organizations 中支持多个委托管理员，但 Audit Manager 只允许指定一个委托管理员。如果您尝试在 Audit Manager 中指定多个委托管理员，则会收到以下错误消息：

- 控制台：`You have exceeded the allowed number of delegated administrators for the delegated service`

- CLI：`An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

在 Audit Manager 中选择一个要用作委托管理员的个人账户。请务必先在 Organizations 中注册委托管理员帐户，然后在 Audit Manager 中将该账户添加为委托管理员。

当我创建评测时，我无法在范围内的账户下看到我所在组织的账户

如果您希望 Audit Manager 评测包含您所在组织的多个帐户，则必须指定委托管理员。

请确保为 Audit Manager 配置了委托管理员账户。有关说明，请参阅设置 — 委托管理员。

请记住以下事项：

- 您不能在 Audit Manager 中以委托管理员的身份使用您的 AWS Organizations 管理账户。
- 如果要在多个 AWS 区域 中启用 Audit Manager，则必须在每个区域中分别指定一个委托管理员账户。在您的 Audit Manager 设置中，您应该在所有区域指定同一委托管理员账户。
- 在指定委托管理员时，请确保委托管理员账户有权访问您在设置 Audit Manager 时提供的 KMS 密钥。有关如何查看和更改加密设置，请参阅数据加密。

当我尝试使用我的委托管理员帐户生成评测报告时，出现拒绝访问的错误

如果您的评测由委托管理员账户创建，且您 Audit Manager 设置中指定的 KMS 密钥不属于该账户，则会收到 `access denied` 错误消息。为避免此错误，在为 Audit Manager 指定委托管理员时，请确保委托的管理员账户有权访问您在设置 Audit Manager 时提供的 KMS 密钥。

如果您对用作评测报告目的地的 S3 桶没有写入权限，也可能会收到 `access denied` 错误消息。

如果您遇到 `access denied` 错误，确保您满足以下要求：

- 您的 Audit Manager 设置中的 KMS 密钥向委托的管理员授予权限。您可以按照 AWS Key Management Service 开发人员指南中允许其他账户中的用户使用 KMS 密钥中的说明进行配置。有关如何在 Audit Manager 中审核和更改加密设置的说明，请参阅数据加密。
- 您的权限策略授予您对评测报告目的地的写入权限。具体而言，您的权限策略包含一项 `s3:PutObject` 操作，指定 S3 桶的 ARN，并包括用于加密评测报告的 KMS 密钥。有关您可以使用的策略示例，请参阅 AWS Audit Manager 基于身份的策略示例。

> **Note**
>
> 如果您更改了 Audit Manager 数据加密设置，则这些更改将应用于您今后创建的新评测。这包括您根据新评测创建的任何评测报告。
>
> 这些更改不适用于您在更改加密设置之前已创建的评测。除现有评测报告外，这还包括您根据现有评测创建的新评测报告。现有评测及其评测报告继续使用旧的 KMS 密钥。如果生成评测报告的 IAM 身份无权使用旧 KMS 密钥，您可以授予密钥政策级权限。

如果我取消成员账户与我的组织的关联，在 Audit Manager 中会发生什么？

当您取消成员账户与组织的关联时，Audit Manager 会收到相关通知。然后，Audit Manager 会自动将该 AWS 账户 从现有评测的范围内的账户列表中移除。当您指定之后新评测的范围时，未关联的账户将不再出现在符合条件的 AWS 账户 列表中。

当 Audit Manager 从您评测的范围内账户列表中移除未关联的成员账户时，您不会收到有关此更改的通知。此外，未关联的成员账户不会收到告知其账户已不再启用 Audit Manager 的通知。

我将成员账户重新关联到我的组织后会发生什么？

当您将成员账户重新关联到您的组织时，该帐户不会自动添加到您的现有 Audit Manager 评测范围中。但是，当您指定评测的范围内账户时，重新关联的成员账户现在显示为符合资格的 AWS 账户。

- 对于现有评测，您可以手动编辑评测范围，从而添加重新关联的成员账户。相关说明请参阅编辑范围内 AWS 账户。
- 对于新的评测，您可以在评测设置期间添加重新关联的账户。相关说明请参阅指定范围内 AWS 账户。

我将成员账户从一个组织迁移到另一个组织后会发生什么？

如果成员账户在组织 1 中启用了 Audit Manager，然后迁移到组织 2，则无法为组织 2 启用 Audit Manager。

证据查找器问题排查

使用此页面上的信息来解决 Audit Manager 中常见的证据查找器问题。

一般证据查找器问题

- 我无法启用证据查找器
- 我启用了证据查找器，但在搜索结果中看不到过去的证据
- 我无法禁用证据查找器
- 我的搜索查询失败

证据查找器评测报告问题

- 我无法根据搜索结果生成多份评测报告
- 我无法在搜索结果中加入具体证据
- 部分证据查找器结果不包含在评测报告中
- 我想根据搜索结果生成评测报告，但是我的查询语句不起作用
- 更多资源

证据查找器 CSV 导出问题

- 我的 CSV 导出失败
- 我无法汇出搜索结果的特定证据
- 我无法同时导出多个 CSV 文件

我无法启用证据查找器

无法启用证据查找器的常见原因包括以下情况：

您缺少权限

如果您首次尝试启用证据查找器，请确保您拥有所需的权限。这些权限允许您在 CloudTrail Lake 中创建和管理事件数据存储，这对支持证据查找器搜索查询具有必要性。这些权限还允许您在证据查找器中运行搜索查询。

如果您需要权限方面的帮助，请联系您的 AWS 管理员。如果您是 AWS 管理员，则可以复制所需的权限声明并将其附加到 IAM policy 中。

您正在使用您的 Organizations 管理账户

请记住，您不能使用管理账户启用证据查找器。请使用委托管理员账户登录，然后重试。

您之前禁用了证据查找器

当前不支持重新启用证据查找器。如果您之前禁用了证据查找器，则无法再次启用该功能。

我启用了证据查找器，但在搜索结果中看不到过去的证据

启用证据查找器后，您过去的所有证据数据最多需要 7 天才能变为可用。

在这 7 天的时间内，事件数据存储中将回填您过去两年的证据数据。这意味着，如果您在启用证据查找器后立即使用它，则在回填完成之前，部分结果不可用。

有关如何检查数据回填状态的说明，请参阅确认证据查找器的状态。

我无法禁用证据查找器

这可能因下列原因之一导致。

您缺少权限

如果您尝试禁用证据查找器，请确保您拥有所需的权限。这些权限允许您在 CloudTrail Lake 中更新和删除事件数据存储，这对禁用证据查找器具有必要性。

如果您需要权限方面的帮助，请联系您的 AWS 管理员。如果您是 AWS 管理员，则可以复制所需的权限声明并将其附加到 IAM policy 中。

启用证据查找器的请求仍在进行中

当您请求启用证据查找器时，我们会创建一个事件数据存储来支持证据查找器查询。创建事件数据存储时，您无法禁用证据查找器。

请等待事件数据存储创建完成，然后重试以继续。如需详细信息，请参阅确认证据查找器的状态。

您已经请求禁用证据查找器

当您请求禁用证据查找器时，我们会删除用于证据查找器查询的事件数据存储。如果在删除事件数据存储时再次尝试禁用证据查找器，则会收到一条错误消息。

在这种情况下，无需采取任何行动。等待删除事件数据存储。完成后，证据查找器随即禁用。如需详细信息，请参阅确认证据查找器的状态。

我的搜索查询失败

搜索查询失败可能因下列原因之一导致。

您缺少权限

验证用户是否具有运行搜索查询和访问搜索结果所需的权限。具体而言，您需要获得以下 CloudTrail 操作的权限：

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

如果您需要权限方面的帮助，请联系您的 AWS 管理员。如果您是 AWS 管理员，则可以复制所需的权限声明并将其附加到 IAM policy 中。

您运行的查询次数已达到最大值

一次最多运行 5 次查询。如果您运行的并发查询数量达到最大值，则会导致 `MaxConcurrentQueriesException` 错误。如果您收到此错误消息，请等待查询完成，然后再次运行查询。

您的查询语句存在验证错误

如果您使用 API 或 CLI 执行 CloudTrail Lake StartQuery 操作，请确保您的 `queryStatement` 有效。查询语句存在验证错误、语法不正确或不支持关键字会导致 `InvalidQueryStatementException`。

有关编写查询的更多信息，请参阅 AWS CloudTrail用户指南中的创建或编辑查询。

有关有效语法的示例，请查看以下可用于查询 Audit Manager 事件数据存储的查询语句示例。

示例 1：调查证据及其合规状态

此示例在指定日期范围内查找账户中所有评测中处于任何合规状态的证据。

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

示例 2：确定空间的不合规证据

该示例查找指定的日期范围内的所有不合规证据 (针对特定评测和控件)。

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
```

```
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

示例 3：按姓名计算证据

此示例列出了指定日期范围内评测的全部证据，按名称分组并按证据数量排序。

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

示例 4：按数据来源和服务了解证据

此示例查找特定数据来源和服务在指定日期范围内的所有证据。

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

示例 5：按数据来源和控制域浏览合规证据

此示例查找特定控制域的合规证据，其中证据来自不属于 AWS Config 的数据来源。

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

其他 API 异常

StartQuery API 可能由于其他几个原因而失败。有关可能的错误和描述的完整列表，请参阅 AWS CloudTrail API 参考中的 StartQuery 错误。

我无法根据搜索结果生成多份评测报告

此错误因同时运行太多 CloudTrail Lake 查询导致。

如果您对搜索结果进行分组并尝试立即为分组结果中的每个行项目生成评测报告，则可能会发生此错误。当您获得搜索结果并生成评测报告时，每个操作都会调用一此查询。您一次最多只能运行 5 次查询。如果您运行的并发查询数量达到最大值，则会返回 `MaxConcurrentQueriesException` 错误。

为防止出现此错误，请确保不要同时生成太多评测报告。如果您运行的并发查询数量达到最大值，则会返回 `MaxConcurrentQueriesException` 错误。如果您收到此错误消息，请等待几分钟，等待正在进行的评测报告完成。

您可以从 Audit Manager 控制台的下载中心页面查看评测报告的状态。报告完成后，在证据查找器中返回分组结果。然后，您可以继续获取结果，并为每个行项目生成评测报告。

我无法在搜索结果中加入具体证据

您的所有搜索结果都包含在评测报告中。您不能从搜索结果集中有选择地添加行。

如果您只想在评测报告中包含特定的搜索结果，我们建议您编辑当前的搜索筛选条件。这样，您可以缩小结果范围，即仅针对要加入报告的证据。

部分证据查找器结果不包含在评测报告中

生成评测报告时，可以添加的证据数量有限。该限制取决于您的评测 AWS 区域、用作评测报告目的地的 S3 桶的区域，以及您的评测是否使用客户托管 AWS KMS key。

1. 同区域报告的上限为 22,000 (S3 桶和评测处于同一 AWS 区域)
2. 跨区域报告的上限为 3,500 (S3 桶和评测处于不同 AWS 区域)
3. 如果评测使用客户托管 KMS 密钥，则限制为 3,500

如果您超过此限制，仍会创建报告。但是，Audit Manager 只在报告中添加了前 3,500 或 22,000 个证据项目。

为防止出现此问题，我们建议您编辑当前的搜索筛选条件。这样，您可以通过定位较少数量的证据来减少搜索结果。如果需要，您可以重复此方法并生成多份评测报告，而不是生成一个较大的报告。

我想根据搜索结果生成评测报告，但是我的查询语句不起作用

如果您使用的是 CreateAssessmentReport API，并且您的查询语句返回了验证异常，请查看下表以获取有关如何修复该异常的指导。

> **Note**
>
> 即使查询语句在 CloudTrail 中起作用，同一查询也可能无法在 Audit Manager 中生成评测报告。这是因为这两个服务在查询验证方面存在一些差异。

子句	问题	解决方案	注意
SELECT	该 SELECT 子句包含列名	移除该 SELECT 子句并替换为 SELECT eventJson 。	仅支持 SELECT eventJson 。 此验证由 Audit Manager 处理。
FROM	该 FROM 子句包含无效的事件数据存储 ID 或 提供的事件数据存储 ID 与 Audit Manager 设置中的事件数据存储 ID 不匹配	移除 FROM 子句并替换为 FROM *edsID* ，其中 edsID 的值与 Audit Manager 设置中指定的事件数据存储 ID 相匹配。 您可以从 Audit Manager 设置中检索事件数据存储的 ARN。有关更多信息，请参阅 AWS Audit Manager API 参考中的 GetSettings。	此验证由 Audit Manager 处理。
GROUP BY	查询中存在一个 GROUP BY 子句	移除 GROUP BY 子句。	此验证由 Audit Manager 处理。
HAVING	查询中存在一个 HAVING 子句	移除 HAVING 子句。	此验证由 Audit Manager 处理。
LIMIT	该 LIMIT 子句包含的值超过了允许的最大限制	如果该 LIMIT 子句存在，请确保其值等于或小于支持的最大限制： • 对于同区域报告，上限为 22,000 • 对于跨区域报告，上限为 3,500 • 对于相关评测使用客户受管 AWS KMS key 的报告，上限为 3,500	在控制台中，不限制可以返回的证据结果数量。但是，在生成评测报告时，您可以包含在内的证据数量有限。 如果您的查询语句中未提供任何 LIMIT 值，则应用默认的最大限制。 此验证由 Audit Manager 处理。

子句	问题	解决方案	注意
ORDER BY	该 ORDER BY 子句包含 SELECT 子句中不存在的聚合函数或别名	确保该 ORDER BY 子句不包含任何聚合函数或别名条件。	此验证由 CloudTrail StartQuery API 处理。
WHERE	该 WHERE 子句包含不止一个 assessmentId 或 该 WHERE 子句包含与您 createAssessmentReport 请求中 assessmentId 不匹配的 assessmentId 或 该 WHERE 子句包含不支持的列名	确保只指定了一个 assessmentID，并且它与您在 createAssessmentReport API 请求中指定的 assessmentId 参数相符。 移除所有不支持的列名称。	此验证由 CloudTrail StartQuery API 处理。

示例

以下示例示范如何在调用 CreateAssessmentReport 操作时使用 queryStatement 参数。在使用这些查询之前，请将*#####*替换为您自己的 edsId 和 assessmentId 值。

示例 1：创建报告 (同区域限制适用)

此示例创建了一份报告，其中包含在 2022 年 1 月 22 日至 23 日之间创建的 S3 桶的结果。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

示例 1：创建报告 (跨区域限制适用)

此示例创建了一个报告，其中包含指定事件数据存储和评测的所有结果，但未指定日期范围。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

示例 3：创建报告 (低于默认限制)

此示例创建了一个报告，其中包含指定事件数据存储和评测的所有结果，其限制低于默认最大值。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

更多资源

以下页面包含有关评测报告的一般问题排查指南：

- 评测报告问题排查

我的 CSV 导出失败

您的 CSV 导出可能会因多种原因失败。您可以通过检查最常见的原因进行问题排查。

首先，确保满足使用 CSV 导出功能的先决条件：

您成功启用了证据查找器

如果您尚未启用证据查找器，则无法运行搜索查询和导出搜索结果。

您的事件数据存储回填已完成

如果您在启用证据查找器后立即使用它，并且证据回填仍在进行中，则部分结果可能不可用。如需检查数据回填状态，请参阅确认证据查找器的状态。

搜索查询成功

Audit Manager 无法导出失败查询的结果。如需失败查询进行问题排查，请参阅 我的搜索查询失败。

确认满足先决条件后，请使用以下清单检查是否存在潜在问题：

1. 检查搜索查询的状态：
   a. 查询是否已取消？ 证据查找器显示取消查询之前处理的部分结果。但是，Audit Manager 不会将部分结果导出到您的 S3 桶或下载中心。
   b. 查询是否已运行超过一小时？ 运行时间超过一小时的查询可能会超时。证据查找器显示查询超时之前处理的部分结果。但是，Audit Manager 不会导出部分结果。为避免超时，您可以通过编辑搜索查询指定较短的时间范围，从而限制扫描的证据数量。
2. 检查您的导出目的地 S3 桶的名称和 URI：
   a. 您指定的桶是否存在？ 如果您手动输入了桶 URI，请确保没有输入错误。当 Audit Manager 尝试将 CSV 文件导出到 Amazon S3 时，输入错误或 URI 不正确可能会导致 `RESOURCE_NOT_FOUND` 错误。
3. 检查您的导出目的地 S3 桶的权限：
   a. 您是否具有 S3 桶的写入权限？ 您必须对用作导出目的地的 S3 桶具有写入权限。具体而言，IAM 权限策略必须包括 `s3:PutObject` 操作和桶 ARN，并将 CloudTrail 列为服务主体。我们提供了一个策略示例以供您使用。有关如何使用其他 S3 桶的说明，请参阅导出目的地设置。
4. 检查您的任何 AWS 区域 信息是否不匹配：
   a. 您的客户托管密钥 AWS 区域 是否与您的评测 AWS 区域 相符？ 如果您提供了用于数据加密的客户受托密钥，则该密钥必须与您的评测处于相同 AWS 区域。有关如何更改 KMS 密钥的说明，请参阅数据加密设置。
5. 检查您的委托管理员账户的权限：
   a. 您的 Audit Manager 设置中的客户托管密钥是否向您的托管管理员授予权限？ 如果您使用的是委托管理员账户，并且指定了用于数据加密的客户托管密钥，请确保委托管理员有权访问该 KMS 密钥。有关说明，请参阅 AWS Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。如需在 Audit Manager 中审核和更改加密设置，请参阅数据加密。

> **Note**
>
> 如果您更改了 Audit Manager 数据加密设置，则这些更改将应用于您今后创建的新评测。这包括您从新评测中导出的任何 CSV 文件。
> 这些更改不适用于您在更改加密设置之前已创建的评测。除了现有的 CSV 导出之外，这还包括现有评测中的新 CSV 导出。现有评测及其所有 CSV 导出将继续使用旧的 KMS 密钥。如果导出 CSV 文件的 IAM 身份无权使用旧 KMS 密钥，您可以授予密钥政策级权限。

我无法汇出搜索结果的特定证据

您的所有搜索结果都包含在结果中。

如果您只想在 CSV 文件中包含特定证据，我们建议您编辑当前的搜索筛选条件。这样，您可以缩小结果范围，即仅针对要导出的证据。

我无法同时导出多个 CSV 文件

此错误因同时运行太多 CloudTrail Lake 查询导致。

如果您对搜索结果进行分组并尝试立即为分组结果中的每个行项目导出一个 CSV 文件，则可能会发生这种情况。当您获得搜索结果并导出 CSV 文件时，每个操作都会调用查询。您一次最多只能运行 5 次查询。如果您运行的并发查询数量达到最大值，则会返回 `MaxConcurrentQueriesException` 错误。

为防止出现此错误，请确保不要一次导出过多 CSV 文件。

如需解决此错误，请等待正在进行的 CSV 导出完成。导出一般需要几分钟时间。但是，如果您导出大量数据，则可能需要长达一个小时才能完成导出。在导出过程中，您可随意离开证据查找器。

您可以从 Audit Manager 控制台的下载中心查看导出状态。文件导出后，在证据查找器中返回分组结果。然后，您可以继续获取结果，并为每一个行项目导出一个 CSV 文件。

框架共享问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的框架共享问题。

主题

- 我已发送共享请求的状态显示为失败
- 我的共享请求旁边有一个蓝点。这意味着什么？
- 我的共享框架包含使用自定义 AWS Config 规则作为数据来源的控件。收件人能否为这些控件收集证据？
- 我更新了共享框架中使用的自定义规则。我需要采取措施吗？

我已发送共享请求的状态显示为失败

如果您尝试共享自定义框架但操作失败，我们建议您检查以下内容：

1. 确保在收件人 AWS 账户 和指定区域中启用了 Audit Manager。有关支持的 AWS Audit Manager 区域列表，请参阅 Amazon Web Services 一般参考中的 AWS Audit Manager 端点和限额。
2. 请确保在指定收件人账户时输入了正确的 AWS 账户 ID。
3. 确保您没有将 AWS Organizations 管理账户指定为收件人。您可以与委托管理员共享自定义框架，但是如果您尝试与管理账户共享自定义框架，则操作将失败。
4. 如果您使用客户托管密钥来加密您的 Audit Manager 数据，请确保您的 KMS 密钥已启用。如果您的 KMS 密钥已禁用，而您尝试共享自定义框架，则操作将失败。有关如何启用已禁用的 KMS 密钥的说明，请参阅AWS Key Management Service开发人员指南中的启用和禁用密钥。

我的共享请求旁边有一个蓝点。这意味着什么？

蓝点通知指示需要您注意的共享请求。

发件人的蓝点通知

在发送的处于即将到期状态的请求旁边会出现一个蓝色的通知点。Audit Manager 会显示蓝点通知，这样您就可以提醒收件人在共享请求到期之前对其采取行动。

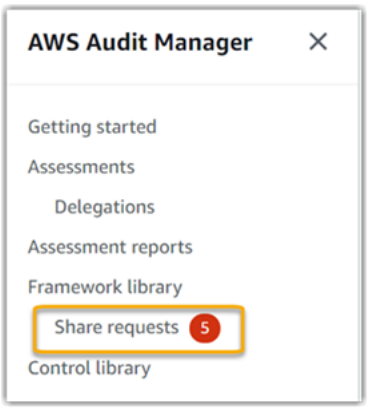
要使蓝色通知点消失，收件人必须接受或拒绝请求。如果您撤销共享请求，蓝点也会消失。

您可以使用以下步骤来检查是否有任何即将到期的共享请求，并向收件人发送提醒 (可选)，提醒其采取行动。

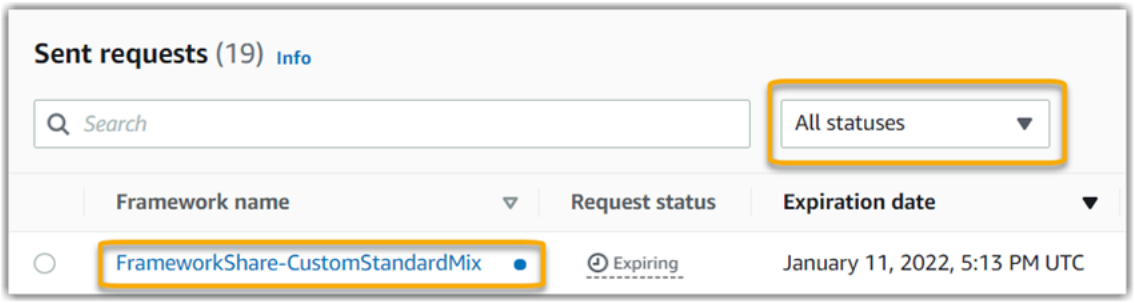
查看已发送请求的通知

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 如果您收到共享请求通知，Audit Manager 会在导航菜单图标旁边显示红点。

3. 展开导航窗格并查看 共享请求 旁边的内容。通知徽章指示需要注意的共享请求数量。



4. 选择共享请求，然后选择已发送请求选项卡。
5. 查找蓝点以识别在未来 30 天内到期的共享请求。或者，您也可以通过从所有状态筛选条件下拉列表中选择即将到期来查看即将到期的共享请求。



6. (可选) 提醒收件人他们需要在共享请求到期之前对其采取行动。此步骤为可选项，因为 Audit Manager 会在控制台中发送通知，通知收件人共享请求处于有效状态或即将到期的时间。但是，您也可以使用首选沟通渠道向收件人发送自己的提醒。

收件人蓝点通知

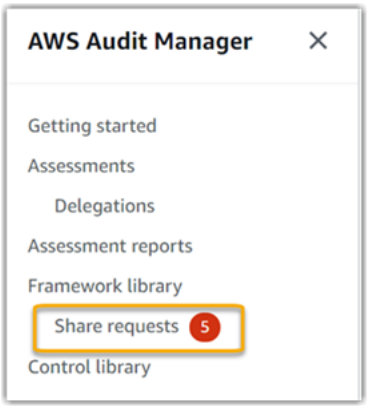
在收到的处于有效或即将到期状态的共享请求旁边会出现一个蓝色的通知点。Audit Manager 会显示蓝点通知，提醒您在共享请求到期之前对其采取行动。要使蓝色通知点消失，您必须接受或拒绝请求。如果发件人撤销共享请求，蓝点也会消失。

您可以使用以下过程检查是否存在有效和即将到期的共享请求。

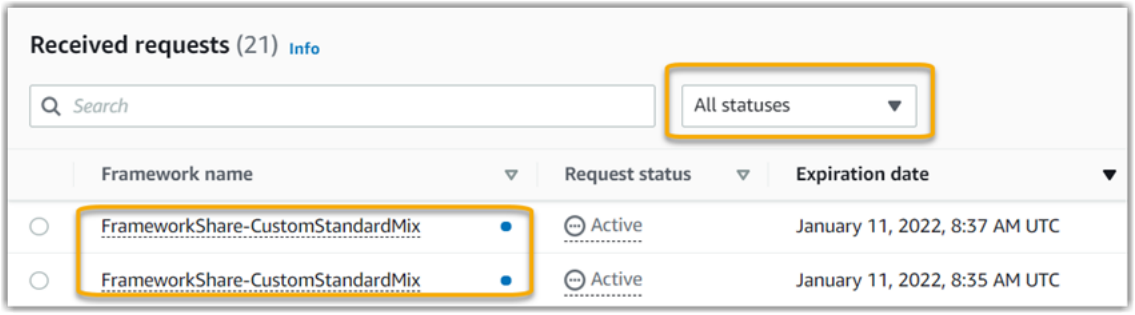
如需查看已收到请求的通知

1. 在 https://console.aws.amazon.com/auditmanager/home 处打开 AWS Audit Manager 控制台。
2. 如果您收到共享请求通知，Audit Manager 会在导航菜单图标旁边显示红点。

3. 展开导航窗格并查看 共享请求 旁边的内容。通知徽章指示需要您注意的共享请求数量。



4. 选择 共享请求。默认情况下，此页面在已收到的请求 选项卡中打开。
5. 通过查找带有蓝点的项目，识别需要您采取行动的共享请求。



6. (可选) 如仅需查看在未来 30 天内到期的请求，请找到所有状态下拉列表并选择即将到期。

我的共享框架包含使用自定义 AWS Config 规则作为数据来源的控件。收件人能否为这些控件收集证据？

是的，收件人可以为这些控件收集证据，但是在此之前需要采取一些步骤。

要让 Audit Manager 使用 AWS Config 规则作为数据来源映射收集证据，以下条件必须为 true。这些标准适用于托管规则和自定义规则。

- 规则必须存在于收件人的 AWS 环境中
- 规则必须在收件人的 AWS 环境中启用

注意，收件人 AWS 环境中可能不存在您账户中的 AWS Config 规则。此外，当收件人接受共享请求时，Audit Manager 不会在其账户中重新创建您的任何自定义规则。要让收件人使用您的自定义规则作为数据来源映射收集证据，他们必须在自己的 AWS Config 实例中创建相同的自定义规则。接收者在 AWS Config 中创建并启用规则后，Audit Manager 可以从该数据来源收集证据。

我们建议您与收件人沟通，告知他们是否需要在他们的 AWS Config 实例中创建任何自定义 AWS Config 规则。

我更新了共享框架中使用的自定义规则。我需要采取措施吗？

您 AWS 环境范围内的规则更新

如果您在 AWS 环境中更新自定义规则，则无需在 Audit Manager 中执行任何操作。Audit Manager 按下表所述方式检测并处理规则更新。当检测到规则更新时，Audit Manager 不会通知您。

情况	Audit Manager 会做什么	您需要了解的内容
您的 AWS Config 实例中的自定义规则已更新。	Audit Manager 继续使用更新的规则定义报告该规则的调查发现。	无需任何操作。
您的 AWS Config 实例中的自定义规则已删除。	Audit Manager 停止报告已删除规则的调查发现。	无需任何操作。 如果需要，您可以编辑使用已删除规则作为数据来源映射的自定义控件。然后，您可以移除已删除的规则，以清理控件的数据来源设置。否则，已删除的规则名称将保留为未使用的数据来源映射。

您 AWS 环境范围外的规则更新

在收件人的 AWS 环境中，Audit Manager 不会检测到规则更新。这是因为，发件人和收件人各自在不同的 AWS 环境中工作。下表提供了针对此场景建议进行的操作。

您的角色	情况	建议的操作
发件人	• 您共享了一个使用自定义规则作为数据来源映射的框架。 • 共享框架后，您在 AWS Config 中更新或删除了其中一项规则。	请联系收件人，告知他们更新情况。这样，他们就可以进行相同的更新并与最新的规则定义保持同步。

您的角色	情况	建议的操作
收件人	• 您接受了使用自定义规则作为数据来源映射的共享框架。 • 在您的 AWS Config 实例中重新创建自定义规则后，发件人更新或删除了其中一项规则。	在您自己的 AWS Config 实例中更新相应的规则。

通知问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的通知问题。

主题

我在 Audit Manager 中指定了一个 Amazon SNS 主题，但我没有收到任何通知

如果您的 Amazon SNS 主题使用 AWS KMS 进行服务器端加密 (SSE)，您可能缺少 AWS KMS 密钥政策所需的权限。如果您没有为主题订阅端点，也可能无法收到通知。

如果您没有收到通知，请确保执行以下操作：

- 您已将所需的权限策略附加至 KMS 密钥。本指南的通知页面上提供了示例政策。
- 您为发送通知的主题订阅了端点节点。当您使用电子邮件端点节点订阅主题时，您会收到一封电子邮件，要求您确认订阅。您必须确认订阅，才能开始接收电子邮件通知。有关更多信息，请参阅 Amazon SNS 开发人员指南中的入门。

我指定了 FIFO 主题，但我没有按预期顺序收到通知

Audit Manager 支持向 FIFO SNS 主题发送通知。但是，Audit Manager 向您的 FIFO 主题发送通知的顺序无法保证。

权限和访问问题排查

您可以使用此页面上的信息来解决 Audit Manager 中常见的权限问题。

主题

我遵循了 Audit Manager 的设置程序，但我没有足够的 IAM 权限

用于访问 Audit Manager 的用户、角色或组必须具有所需的权限。此外，您基于身份的策略不应过于严格。否则，控制台将无法按预期运行。本指南中的设置程序提供了一种策略，该策略授予设置 Audit Manager 所需的最低权限。根据使用案例，您可能需要更广泛、限制性更低的权限。例如，我们建议审计所有者拥有管理员访问权。以便修改 Audit Manager 设置并管理评测、框架、控件和评测报告等资源。其他用户 (例如委托人员) 可能只需要管理权或只读访问权。

请务必为您的用户、角色或组添加相应的权限。我们建议审计负责人使用 AWSAuditManagerAdministratorAccess 策略。委托人员可以使用 IAM policy 示例页面上提供的此示例。您可以基于这些示例策略，根据需要进行更改以满足您的要求。

我们建议您花点时间自定义权限，使其满足您的特定需求。如果您需要有关 IAM 权限的帮助，请联系您的管理员或 AWS Support。

我指定某人为审计负责人，但他们仍然没有评测的完全访问权。这是为什么？

仅将某人指定为审计负责人并不会授予对评测的完全访问权。审计所有者还必须拥有必要的 IAM 权限才能访问和管理 Audit Manager 资源。换而言之，除了将用户指定为审计负责任外，您还必须将必要的 IAM policy 附加至该用户。其原因在于，通过这两项要求，Audit Manager 可以确保您完全控制每次评测的所有细节。

> **Note**
>
> 我们建议审计负责人使用 AWSAuditManagerAdministratorAccess 策略。有关更多信息，请参阅针对 Audit Manager 中用户角色的推荐策略。

我无法在 Audit Manager 中执行操作

如果您没有使用 AWS Audit Manager 控制台或 Audit Manager API 操作所需的权限，则可能会遇到 `AccessDeniedException` 错误。

要解决此问题，务必联系管理员获取帮助。管理员是向您提供登录凭证的人。

我希望允许我 AWS 账户 以外的人员访问我的 Audit Manager 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，可以代入该角色。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：

- 如需了解 Audit Manager 是否支持这些功能，请参阅 如何 AWS Audit Manager 与 IAM 配合使用。
- 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。
- 要了解如何通过身份联合验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户 (身份联合验证) 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存取之间的差别，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。

另请参阅

以下页面包含权限缺失可能导致的其他问题的排查指南：

- 我在评测中看不到任何控件或控制集
- 配置控件数据来源时，自定义规则选项不可用

- 尝试生成评测报告时出现拒绝访问错误
- 当我尝试使用我的委托管理员账户生成评测报告时，出现拒绝访问的错误
- 我无法启用证据查找器
- 我无法禁用证据查找器
- 证据查找器中搜索查询失败
- 我在 Audit Manager 中指定了一个 Amazon SNS 主题，但我没有收到任何通知

AWS Audit Manager 的限额和限制

对于每项 AWS 服务，您的 AWS 账户 都具有默认限额（以前被称为限制）。除非另有说明，否则，每个配额是区域特定的。您可以请求增加某些限额，但其他一些限额无法增加。

大多数 Audit Manager（但不是全部）都列在服务限额控制台中的 AWS Audit Manager 命名空间下。若要了解如何请求提高限额，请参阅 管理您的 Audit Manager 限额。

Audit Manager 默认限额

下面是每个 AWS 账户 在每个区域的 AWS Audit Manager 限额。

评测

- 每个账户的有效评测数量：100

评测报告

- 可以添加至评测报告的证据项目数：
  - 对于同区域报告（其中评测和评测报告目标 S3 桶在同一 AWS 区域 中）：22,000
  - 对于跨区域报告（其中评测和评测报告目标 S3 桶在不同 AWS 区域 中）：3,500
  - 对于相关评测使用客户托管 AWS KMS key 的报告：3,500

控件

- 每个账户的自定义控件数：500

证据

- 单个手动证据文件的最大大小：100 MB
- 每个控件每天手动上传证据的次数：100

> **Tip**
>
> 如果您需要将大量手动证据上传至单个控件，我们建议您在几天内分批上传证据。

框架

- 每个账户的自定义框架数量：100

> **Note**
>
> 框架限额适用于您框架库中的所有共享自定义框架，与框架创建者无关。

共享自定义框架收件人

- 活跃收件人账户数量：100

API 访问

- 所有 API 每秒可处理事务数 (TPS)：20 TPS

管理您的 Audit Manager 限额

AWS Audit Manager 已与服务限额集成，AWS 服务 可让您从中心位置查看和管理您的限额。有关更多信息，请参阅《服务限额用户指南》中的什么是服务限额？。使用服务限额，可使用轻松查找 Audit Manager 限额的值。

若要使用控制台查看 Audit Manager 服务限额

1. 访问 https://console.aws.amazon.com/servicequotas/，打开 Service Quotas 控制台。
2. 在导航窗格中，选择 AWS 服务。
3. 从 AWS 服务 列表中，搜索并选择 AWS Audit Manager。
4. 在服务限额列表中，您可以查看服务限额名称、应用的限额值（如果该值可用）、AWS 默认限额值以及限额值是否可调整。
5. 要查看有关服务配额的其他信息 (如描述)，请选择配额名称。
6. （可选）要请求增加配额，请选择要增加的配额，选择 Request quota increase（请求增加配额），输入或选择所需信息，然后选择 Request（请求）。

有关更多信息，请参阅 Service Quotas 用户指南 中的请求增加配额。

安全性 AWS Audit Manager

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS Audit Manager，请参阅按合规计划划分的范围内的 AWSAWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，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。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Audit Manager。以下主题说明如何配置 Audit Manager 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Audit Manager 资源。

主题

中的数据保护 AWS Audit Manager

分 AWS 担责任模型适用于中的数据保护 AWS Audit Manager。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。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解答。有关欧洲数据保护的信息，请参阅AWS 安全性博客上的 AWS 责任共担模式和 GDPR 博客文章。

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) 设置个人用户。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 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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 AWS 通过命令行界面或 API 进行访问时需要经过 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）。这包括您 AWS 服务 使用控制台、API 或软件开发工具包与 Au AWS dit Manager 或其他人合作时。 AWS CLI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，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。

除了上述建议外，我们还特别建议 Audit Manager 客户在创建评测、自定义控件、自定义框架和委托注释时，不要在自由格式字段中包含敏感的识别信息。

删除 Audit Manager 数据

删除 Audit Manager 数据的方法有多种。

禁用 Audit Manager 时删除数据

禁用 Audit Manager 后，您可以决定是否要删除所有的 Audit Manager 数据。如果您选择删除数据，则会在禁用 Audit Manager 后的 7 天内将其删除。数据删除后，将无法恢复。

自动删除数据

某些 Audit Manager 数据会在特定时间段后自动删除。Audit Manager 按如下方式保留客户数据。

数据类型	数据留存期	注意事项
证据	数据自创建之时起保留 2 年	包括自动证据和手动证据
客户创建的资源	数据会无限期保留	包括评测、评测报告、自定义控件和自定义框架

手动删除数据

您可以随时删除单个 Audit Manager 资源。有关说明，请参阅：

- 删除评测
  - 另请参阅：DeleteAssessment在 AWS Audit Manager API 参考中
- 删除自定义框架
  - 另请参阅：DeleteAssessmentFramework在 AWS Audit Manager API 参考中
- 删除共享请求
  - 另请参阅：DeleteAssessmentFrameworkShare在 AWS Audit Manager API 参考中
- 删除评测报告
  - 另请参阅：DeleteAssessmentReport在 AWS Audit Manager API 参考中
- 删除自定义控件
  - 另请参阅：DeleteControl在 AWS Audit Manager API 参考中

要删除您在使用 Audit Manager 时可能创建的其他资源数据，请参阅以下内容：

- AWS CloudTrail 用户指南中的删除事件数据存储
- Amazon Simple Storage Service (Amazon S3) 用户指南中的删除存储桶

静态加密

为了加密静态数据，Audit Manager 对其所有数据存储和日志使用服务器端加密。 AWS 托管式密钥

您的数据使用客户管理的密钥或进行加密 AWS 拥有的密钥，具体取决于您选择的设置。如果您不提供客户托管密钥，Audit Manager AWS 拥有的密钥 会使用加密您的内容。DynamoDB 和 Amazon S3 中的所有服务元数据在 Audit Manager 中都使用 AWS 拥有的密钥进行加密。

Audit Manager 按如下方式对数据进行加密：

- 存储在 Amazon S3 中的服务元数据 AWS 拥有的密钥 使用 SSE-KMS 进行加密。
- 存储在 DynamoDB 中的服务元数据使用 KMS 和 AWS 拥有的密钥进行服务器端加密。
- 您存储在 DynamoDB 中的内容将使用客户托管密钥或 AWS 拥有的密钥进行客户端加密。KMS 密钥基于您选择的设置。
- 存储在 Amazon S3 中的内容在 Audit Manager 中使用 SSE-KMS 进行加密。KMS 密钥基于您的选择，可以是客户托管密钥或 AWS 拥有的密钥。
- 发布到您的 S3 存储桶的评测报告按以下方式进行加密：
  - 如果您提供了客户托管密钥，则您的数据将使用 SSE-KMS 进行加密。
  - 如果您使用了 AWS 拥有的密钥，则您的数据将使用 SSE-S3 进行加密。

传输中加密

Audit Manager 为传输中数据的加密提供安全的私有端点。安全和私有端点 AWS 允许保护向 Audit Manager 发出的 API 请求的完整性。

服务间中转

默认情况下，所有服务间通信都将通过传输层安全性协议（TLS）加密来进行保护。

密钥管理

Audit Manager 同时 AWS 拥有的密钥 支持客户托管密钥，用于加密所有 Audit Manager 资源（评估、控制、框架、证据和评估报告，保存到您账户的 S3 存储桶中的评估报告）。

建议使用客户托管密钥。这样，您就可以查看和管理保护数据的加密密钥，包括查看其在 AWS CloudTrail中的使用日志。当您选择客户托管密钥时，Audit Manager 会创建 KMS 密钥的授权，以便您可以使用此密钥加密您的内容。

> **Warning**
>
> 删除或禁用用于对 Audit Manager 资源进行加密的 KMS 密钥后，您不能再解密用该 KMS 密钥加密的资源，这意味着该数据将无法恢复。
> 删除 AWS Key Management Service (AWS KMS) 中的 KMS 密钥具有破坏性和潜在危险。有关删除 KMS 密钥的更多信息，请参阅 AWS Key Management Service 用户指南中的删除 AWS KMS keys。

在启用 Audit Manager 时，你可以使用 AWS Management Console、Audit Manager API 或 AWS Command Line Interface (AWS CLI) 来指定加密设置。有关说明，请参阅启用了 AWS Audit Manager。

您可以随时查看和更改您的加密设置。有关说明，请参阅数据加密。

有关如何设置客户托管密钥的更多信息，请参阅 AWS Key Management Service 用户指南中的创建密钥。

的身份和访问管理 AWS Audit Manager

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。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 Audit Manager 资源的人员。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Audit Manager 中所做的工作。

服务用户 – 如果使用 Audit Manager 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 Audit Manager 功能来完成工作时，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 Audit Manager 中的功能，请参阅对 AWS Audit Manager 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Audit Manager 资源，则您可能具有 Audit Manager 的完全访问权限。您有责任确定您的服务用户应访问哪些 Audit Manager 功能和资源。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 Audit Manager 搭配使用的更多信息，请参阅如何 AWS Audit Manager 与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解有关如何编写策略以管理对 Audit Manager 的访问权限的详细信息。要查看您可在 IAM 中使用的 Audit Manager 基于身份的策略示例，请参阅基于身份的策略示例 AWS Audit Manager。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。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。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。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 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议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

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

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您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。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

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。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，如果有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。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 组是一个用于指定一组 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

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。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。
- 跨账户访问——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，对于某些资源 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代理）。要了解用于跨账户访问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 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。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 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当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 请求时的策略详情，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分派的 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-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以担任代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 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证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该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

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档

的 AWS 形式存储在中。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 策略概述。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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，并且用户可以代入角色。

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。拥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 策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、群组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式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。委托人可以包括账户、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 IAM 中的 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 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF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) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。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` 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，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您在组织内启用了特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关组织和 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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Audit Manager 与 IAM 配合使用

在使用 IAM 管理对 Audit Manager 的访问权限之前，您应该了解哪些 IAM 功能可与Audit Manager 搭配使用。

您可以搭配使用的 IAM 功能 AWS Audit Manager

IAM 功能	Audit Manager 支持
基于身份的策略	是
基于资源的策略	否

IAM 功能	Audit Manager 支持
策略操作	是
策略资源	是
策略条件密钥	部分
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
服务相关角色	是

要全面了解 AWS Audit Manager 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 AWS Audit Manager

支持基于身份的策略	是

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。

AWS Audit Manager 创建名为 Audit Manager 管理员`AWSAuditManagerAdministratorAccess`的托管策略。此策略授予 Audit Manager 中的完全管理权限。管理员可以将此策略附加到任何现有角色或用户，也可以使用此策略创建新角色。

中针对用户角色的推荐策略 AWS Audit Manager

AWS Audit Manager 使您能够使用不同的 IAM 策略在不同用户之间保持职责分工，并进行不同的审计。Audit Manager 中的两个角色及其推荐的策略定义如下。

角色	描述和推荐的策略
审计负责人	• 此角色必须具有必要的权限才能在中管理评估。 AWS Audit Manager • 此角色的推荐策略是名AWSAuditManagerAdministratorAccess为的托管策略。您可以使用此策略作为起点，根据您的要求缩小这些权限的范围。
委托人	• 此角色可以访问评测中的委托控件集。他们可以更新控件状态、添加注释、提交控制集以供审查，以及向评测报告中添加证据。 • 为此角色推荐使用的策略是以下示例策略：允许用户拥有对 AWS Audit Manager的全部管理员访问权限 。您可以将此策略作为起点，并根据需要进行更改以满足您的要求。

基于身份的策略示例 AWS Audit Manager

要查看 Audit Manager 基于身份的策略示例，请参阅基于身份的策略示例 AWS Audit Manager。

内部基于资源的政策 AWS Audit Manager

支持基于资源的策略	否

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。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，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。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。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。

的政策行动 AWS Audit Manager

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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。

要查看 AWS Audit Manager 操作列表，请参阅《服务授权参考》中的 AWS Audit Manager 定义的操作。

正在执行的策略操作在操作前 AWS Audit Manager 使用以下前缀。

```
auditmanager
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Get` 开头的所有操作，请包括以下操作。

```
"Action": "auditmanager:Get*"
```

要查看 Audit Manager 基于身份的策略示例，请参阅基于身份的策略示例 AWS Audit Manager。

的政策资源 AWS Audit Manager

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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。作为最佳实操，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": "*"
```

要查看 AWS Audit Manager 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 AWS Audit Manager 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Audit Manager 定义的操作。

Audit Manager 评测具有以下 Amazon 资源名称（ARN）格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Audit Manager 控件集具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Audit Manager 控件具有以下 ARN 格式：

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

有关 ARN 格式的更多信息，请参阅 Amazon 资源名称（ARN）。

例如，要在语句中指定 `i-1234567890abcdef0` 评测，请使用以下 ARN。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

要指定属于特定账户的所有实例，请使用通配符 (*)。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

无法对特定资源执行某些 Audit Manager 操作，例如，用于创建资源的操作。在这些情况下，您必须使用通配符 （ *)。

```
"Resource": "*"
```

许多 Audit Manager API 操作涉及多种资源。例如，`ListAssessments`返回当前登录用户可以访问的评估元数据列表 AWS 账户。因此，用户必须具有查看评测的权限。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
```

要查看 Audit Manager 资源类型及其 ARN 的列表，请参阅 IAM 用户指南中的 AWS Audit Manager定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Audit Manager定义的操作。

某些 Audit Manager API 操作支持多个资源。例如，`GetChangeLogs` 访问 `assessmentID`、`controlID` 和 `controlSetId`，因此主体必须具有访问这些资源的权限。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

的策略条件密钥 AWS Audit Manager

支持特定于服务的策略条件密钥	部分

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

策略语句中的主体是 AWS 服务主体时，我们强烈建议您在策略中使用 aws:SourceArn 或 aws:SourceAccount 全局条件键。您可以使用这些全局条件上下文键来帮助防止出现混淆代理场景。以下记录策略演示如何使用 Audit Manager 中的 aws:SourceArn 和 aws:SourceAccount 全局条件上下文键来防范混淆代理问题。

- 用于 Audit Manager 通知的 SNS 主题的策略示例
- 用于 SNS 主题的 KMS 密钥的策略示例

您也可以在指定条件时使用占位符变量。例如，仅当用户使用其用户名进行标记时，您才可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 策略 元素：变量和标签。

Audit Manager 不提供任何特定于服务的条件键，但支持使用某些全局条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

AWS Audit Manager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。

基于属性的访问控制 (ABAC) AWS Audit Manager

支持 ABAC（策略中的标签）	是

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。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。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密钥，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密钥，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）。

有关为 AWS Audit Manager 资源添加标签的更多信息，请参阅为 AWS Audit Manager 资源添加标签。

将临时凭证与配合使用 AWS Audit Manager

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。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 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，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。

转发访问会话 AWS Audit Manager

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当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 请求时的策略详细信息，请参阅转发访问会话。

AWS Audit Manager的服务角色

支持服务角色	否

服务角色是由一项服务代入、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。

> **Warning**
>
> 更改服务角色的权限可能会破坏 AWS Audit Manager 的功能。仅当 Audit Manager 提供相关指导时才编辑服务角色。

的服务相关角色 AWS Audit Manager

支持服务相关角色	是

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以担任代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关服务相关角色的详细信息 AWS Audit Manager，请参阅将服务相关角色用于 AWS Audit Manager。

基于身份的策略示例 AWS Audit Manager

默认情况下，用户和角色没有创建或修改 Audit Manager 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 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

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 AWS Audit Manager 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 AWS Audit Manager 的操作、资源和条件键。

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 Audit Manager 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：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管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。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。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 策略，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 策略语言 (JSON) 和 IAM 最佳实操。IAM

Access Analyzer 提供 100 多项策略检查和可操作的建议，有助于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 Access Analyzer 策略验证。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

允许启用 Audit Manager 所需的最低权限

此示例显示如何允许不具有管理员角色的账户启用 AWS Audit Manager。

> **Note**
>
> 我们在此处提供的是一项基本策略，它授予启用 Audit Manager 所需的最低权限。以下策略中的所有权限都是必需的。如果省略此策略的任何部分，则无法启用 Audit Manager。
> 我们建议您花点时间自定义权限，使其满足您的特定需求。如果您需要帮助，请联系您的管理员或 AWS Support。

要授予启用 Audit Manager 所需的最低访问权限，请使用以下权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                   ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户拥有对 AWS Audit Manager的全部管理员访问权限

以下示例策略授予对的完全管理员访问权限 AWS Audit Manager。

- 示例 1（托管式策略，AWSAuditManagerAdministratorAccess）
- 示例 2（评测报告目标权限）
- 示例 3（导出目标权限）
- 示例 4（启用证据查找器的权限）
- 示例 5（禁用证据查找器的权限）

示例 1（托管式策略，**AWSAuditManagerAdministratorAccess**）

此策略与 AWSAuditManagerAdministratorAccess 托管式策略相同。此策略包括启用和禁用 Audit Manager、更改 Audit Manager 设置以及管理所有 Audit Manager 资源（例如评测、框架、控件和评测报告）的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
```

```
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

示例 2（评测报告目标权限）

此策略授予您访问特定 S3 存储桶以及向其中添加文件和从中删除文件的权限。这允许您在 Audit Manager 中使用指定的存储桶作为评测报告目标。

将*#####*替换为您自己的信息。包括您用作评测报告目标的 S3 存储桶和用于加密评测报告的 KMS 密钥。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
```

```
}
```

示例 3（导出目标权限）

以下策略允许 CloudTrail 将证据查找器查询结果传送到指定的 S3 存储桶。作为安全最佳实践，IAM 全局条件密钥`aws:SourceArn`有助于确保仅针对事件数据存储 CloudTrail 写入 S3 存储桶。

用您自己的信息替换*#####*，如下所示：

- 将 *DOC-EXAMPLE-DESTINATION-BUCKEL* 替换为用作导出目标的 S3 存储桶。
- 将*myQueryRunning##*替换 AWS 区域 为适合您的配置的区域。
- 将 *myAccountID* 替换为所用的 AWS 账户 ID。 CloudTrail这可能与 S3 存储桶的 AWS 账户 ID 不同。如果这是组织事件数据存储，则必须将 AWS 账户 用于管理账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

示例 4（启用证据查找器的权限）

如果要启用和使用证据查找器功能，则需要以下权限策略。本政策声明允许 Audit Manager 创建 CloudTrail Lake 事件数据存储并运行搜索查询。

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

```
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

示例 5（禁用证据查找器的权限）

此示例策略授予在 Audit Manager 中禁用证据查找器功能的权限。这包括删除首次启用该功能时创建的事件数据存储。

在您使用此策略前，请将*#####*替换为您自己的信息。您应该指定启用证据查找器时创建的事件数据存储的 UUID。您可以从 Audit Manager 设置中检索事件数据存储的 ARN。有关更多信息，请参阅《AWS Audit Manager API 参考》中的 GetSettings。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
```

```
}
```

允许对 AWS Audit Manager的用户管理访问权限

此示例显示了如何允许对 AWS Audit Manager的非管理员管理访问权限。

此策略允许管理所有 Audit Manager 资源（评测、框架和控件），但不允许启用或禁用 Audit Manager 或修改 Audit Manager 设置。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

允许用户只读访问 AWS Audit Manager

此策略授予对评估、框架和控件等 AWS Audit Manager 资源的只读访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

允许用户查看他们自己的权限

该示例说明了如何创建策略，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或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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": "*"
        }
    ]
}
```

AWS Audit Manager 允许向 Amazon SNS 主题发送通知

此示例中的策略授予 Audit Manager 向现有 Amazon SNS 主题发送通知的权限。

- 示例 1 - 如果您想接收来自 Audit Manager 的通知，请使用此示例向您的 SNS 主题访问策略添加权限。
- 示例 2-如果您的 SNS 主题使用 AWS Key Management Service (AWS KMS) 进行服务器端加密 (SSE)，请使用此示例向 KMS 密钥访问策略添加权限。

在以下策略中，获得权限的主体是 Audit Manager 服务主体，它是 `auditmanager.amazonaws.com`。策略语句中的主体是 AWS 服务主体时，我们强烈建议您在策略

中使用 aws:SourceArn 或 aws:SourceAccount 全局条件键。您可以使用这些全局条件上下文键来帮助防止出现混淆代理场景。

示例 1（SNS 主题的权限）

此策略声明允许 Audit Manager 将事件发布到指定的 SNS 主题。任何发布到指定 SNS 主题的请求都必须满足策略条件。

在使用此策略前，请将*#####*替换为您自己的信息。记录以下内容：

- 如果您在此策略中使用 aws:SourceArn 条件键，则该值必须是通知来自的 Audit Manager 资源的 ARN。在下面的示例中，aws:SourceArn 使用通配符 (*) 作为资源 ID。这允许来自 Audit Manager 的对所有 Audit Manager 资源的所有请求。使用 aws:SourceArn 全局条件键，您可以使用 StringLike 或 ArnLike 条件运算符。作为最佳实践，我们建议您使用 ArnLike。
- 如果使用 aws:SourceAccount 条件键，则可以使用 StringEquals 或 StringLike 条件运算符。作为最佳实践，我们建议您使用 StringEquals 实现最低权限。
- 如果使用 aws:SourceAccount 和 aws:SourceArn，则账户值必须显示相同的账户 ID。

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

以下替代示例仅使用 aws:SourceArn 条件键和 StringLike 条件运算符：

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

以下替代示例仅使用 aws:SourceAccount 条件键和 StringLike 条件运算符：

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

示例 2（附加到 SNS 主题的 KMS 密钥的权限）

本策略语句允许 Audit Manager 使用 KMS 密钥来生成数据密钥用来加密 SNS 主题。使用 KMS 密钥进行指定操作的任何请求都必须满足策略条件。

在使用此策略前，请将#####替换为您自己的信息。记录以下内容：

- 如果您在此策略中使用 aws:SourceArn 条件键，则该值必须是正在加密的资源的 ARN。例如，在本例中，这是您账户中的 SNS 主题。将值设置为 ARN 或带通配符 (*) 的 ARN 模式。您可以将 StringLike 或 ArnLike 条件运算符与 aws:SourceArn 条件键一起使用。作为最佳实践，我们建议您使用 ArnLike。
- 如果使用 aws:SourceAccount 条件键，则可以使用 StringEquals 或 StringLike 条件运算符。作为最佳实践，我们建议您使用 StringEquals 实现最低权限。如果您不知道 SNS 主题的 ARN，则可以使用 aws:SourceAccount。
- 如果使用 aws:SourceAccount 和 aws:SourceArn，则账户值必须显示相同的账户 ID。

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
```

```
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:region:accountID:key/*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

以下替代示例仅使用 aws:SourceArn 条件键和 StringLike 条件运算符：

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

以下替代示例仅使用 aws:SourceAccount 条件键和 StringLike 条件运算符：

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

允许用户在证据查找器中运行搜索查询

以下策略授予对 CloudTrail Lake 事件数据存储执行查询的权限。如果要使用证据查找器功能，则需要使用此权限策略。

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

```
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

防止跨服务混淆座席

混淆座席问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（调用服务）调用另一项服务（被调用服务)时，可能会发生跨服务模拟。可以操纵调用服务来使用其权限，以对另一个客户的资源进行操作（当它不具有权限来这么做时）。为了防止这种情况，Amazon Web Services 提供可帮助您保护所有服务的服务主体数据的工具，这些服务主体有权限访问账户中的资源。

我们建议在资源策略中使用aws:SourceArn和aws:SourceAccount全局条件上下文密钥来限制授 AWS Audit Manager 予其他服务访问您的资源的权限。

- 如果您只希望将一个资源与跨服务访问相关联，请使用 aws:SourceArn。如果要指定多个资源，也可以将 aws:SourceArn 与通配符 (*) 一起使用。

  例如，您可以使用 Amazon SNS 主题从 Audit Manager 接收活动通知。在本例中，在您的 SNS 主题访问策略中，aws:SourceArn 的 ARN 值是通知来自的 Audit Manager 资源。由于您可能有多个 Audit Manager 资源，因此我们建议您将 aws:SourceArn 与通配符一起使用。这使您能够在 SNS 主题访问策略中指定所有 Audit Manager 资源。
- 如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 aws:SourceAccount。
- 如果 aws:SourceArn 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文密钥来限制权限。
- 如果您同时使用了这两个条件，并且如果 aws:SourceArn 值包含账户 ID，则 aws:SourceAccount 值和 aws:SourceArn 值中的账户在同一策略语句中使用时，必须显示相同的账户 ID。

- 防范混淆代理问题最有效的方法是使用 aws:SourceArn 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 Amazon 资源名称（ARN），或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符字符 (*) 的 aws:SourceArn 全局上下文条件键。例如，arn:aws:*servicename*:*:*123456789012*:*。

Audit Manager 混淆代理支持

在以下情况下，Audit Manager 会提供混淆代理支持。这些策略示例说明如何使用 aws:SourceArn 和 aws:SourceAccount 条件键来防范混淆代理问题。

- 策略示例：您用来接收 Audit Manager 通知的 SNS 主题
- 策略示例：您用于加密您的 SNS 主题的 KMS 密钥

Audit Manager 不会为您在 Audit Manager 数据加密 设置中提供的客户托管密钥提供混淆代理支持。如果您提供了自己的客户托管密钥，则不能在该 KMS 密钥政策中使用 aws:SourceAccount 或 aws:SourceArn 条件。

AWS 的托管策略 AWS Audit Manager

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管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 托管策略可能不会为您的特定用例授予最低权限权限，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 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

主题

- AWS 托管策略： AWSAuditManagerAdministratorAccess
- AWS 托管策略： AWSAuditManagerServiceRolePolicy
- AWS Audit ManagerAWS 托管策略的更新

AWS 托管策略： AWSAuditManagerAdministratorAccess

您可以将 AWSAuditManagerAdministratorAccess 策略附加到 IAM 身份。

此策略授予管理权限，允许对的完全管理权限 AWS Audit Manager。此访问权限包括启用和禁用 AWS Audit Manager、更改设置和管理所有 Audit Manager 资源（例如评估、框架、控制和评估报告）的功能。 AWS Audit Manager

AWS Audit Manager 需要跨多个 AWS 服务的广泛权限。这是因为与多种 AWS 服务 AWS Audit Manager 集成，可以自动从评估范围内的 AWS 账户 和服务中收集证据。

权限详细信息

该策略包含以下权限：

- Audit Manager - 允许主体拥有对 AWS Audit Manager 资源的完全权限。
- Organizations - 允许主体列出账户和组织单位，以及注册或注销委派的管理员。这是必需的，这样您才能启用多账户支持，并允许 AWS Audit Manager 对多个账户进行评估并将证据整合到委托管理员账户中。
- iam - 允许主体在 IAM 中获取和列出用户并创建服务相关角色。这是必需的，这样您才能为评测指定审计负责人和委托人。此策略还允许主体删除服务相关角色并检索删除状态。这是必需的，这样当您在中选择禁用服务时， AWS Audit Manager 可以清理资源并删除服务相关角色。 AWS Management Console
- s3 - 允许主体列出可用的 Amazon Simple Storage Service (Amazon S3) 存储桶。此功能是必需的，这样您才能指定要在其中存储证据报告或上传手动证据的 S3 存储桶。
- kms - 允许主体列出和描述密钥、列出别名和创建授权。这是必需的，这样您才能选择客户托管密钥进行数据加密。
- sns - 允许主体在 Amazon SNS 中列出订阅主题。这是必需的，这样您才能指定要 AWS Audit Manager 向哪个 SNS 主题发送通知。
- events— 允许委托人列出和管理来自 AWS Security Hub的支票。这是必需的，这样 AWS Audit Manager 才能自动收集所监控 AWS 服务的 AWS Security Hub 调查结果 AWS Security Hub。然后，它可以将这些数据转换为证据，以包含在您的 AWS Audit Manager 评测中。
- tag - 允许主体检索已标记的资源。这是必需的，这样您就可以在 AWS Audit Manager中浏览框架、控件和评测时使用标签作为搜索过滤器。

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

```
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略： AWSAuditManagerServiceRolePolicy

您不能将 AWSAuditManagerServiceRolePolicy 附加到自己的 IAM 实体。此策略附加到服务相关角色AWSServiceRoleForAuditManager， AWS Audit Manager 允许您代表您执行操作。有关更多信息，请参阅为 AWS Audit Manager使用服务相关角色。

角色权限策略 AWSAuditManagerServiceRolePolicy 允许 AWS Audit Manager 通过代表您执行以下操作来收集自动证据：

- 从以下数据来源收集数据：
  - 管理活动来自 AWS CloudTrail
  - 合规性检查来自 AWS Config 规则
  - 合规性检查来自 AWS Security Hub
- 使用 API 调用来描述您以下 AWS 服务的资源配置。

> **Tip**
>
> 有关 Audit Manager 用于从这些服务收集证据的 API 调用的更多信息，请参阅本指南中的 支持自定义控件数据来源的 API 调用。

- AWS Certificate Manager
- AWS Backup
- Amazon Bedrock
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch 日志
- Amazon Cognito 用户群体
- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda

- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

权限详细信息

`AWSAuditManagerServiceRolePolicy` AWS Audit Manager 允许对指定资源完成以下操作：

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`

- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections

- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams

- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration

- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - 此 API 操作 AWS 账户 在可用的范围内运行。 service-linked-role 但无法访问跨账户存储桶策略。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- securityhub:DescribeStandards
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups

- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
```

```
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
```

```
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
```

```
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit ManagerAWS 托管策略的更新

查看 AWS Audit Manager 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “ AWS Audit Manager 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWSAuditManagerServiceRolePolicy – 对现有策略的更新	服务相关角色现在 AWS Audit Manager 允许执行`s3:GetBucketPolicy` 操作。 此 API 操作是支持 AWS 生成式人工智能最佳实践框架 v1 所必需的。该操作允许 Audit Manager 自动收集有关生成式人工智能模型数据训练数据集的策略限制证据。 该`GetBucketPolicy` 操作在可用的范围内运行。 AWS 账户 service-linked-role 但无法访问跨账户存储桶策略。	2023 年 6 月 12 日
AWSAuditManagerServiceRolePolicy	我们在中添加了以下权限`AWSAuditManagerServiceRolePolicy` 。 AWS	11/06/2023

更改	描述	日期
– 对现有策略的更新	Audit Manager 现在可以执行以下操作来收集有关您的资源的自动证据 AWS 账户。 • acm:GetAccountConfiguration • acm:ListCertificates • backup:ListRecoveryPointsBy Resource • bedrock:GetCustomModel • bedrock:GetFoundationModel • bedrock:GetModelCustomizati onJob • bedrock:GetModelInvocationL oggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizat ionJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsFo rMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirec tConnectGateways • directconnect:DescribeVirtu alGateways • dynamodb:ListBackups • dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways	

更改	描述	日期
	• ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers • elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups	

更改	描述	日期
	• elasticmapreduce:ListClusters • elasticmapreduce:ListSecuri tyConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParame terGroups • rds:DescribeDbClusters	

更改	描述	日期
	• rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – 对现有策略的更新	我们向 AWSAuditManagerServiceRolePolicy 中添加了以下权限： • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

更改	描述	日期
AWSAuditManagerServiceRolePolicy – 更新了现有策略	服务相关角色现在 AWS Audit Manager 允许执行`organizations:DescribeOrganization` 操作。 我们还利用通配符 (*) 将 `CreateEventsAccess` 资源的范围从缩小到特定类型的资源 (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`)。 最后，我们为 `events:source` 条件键添加了一个 `Null` 条件运算符，以确认源值存在且其值不为空。	05/20/2022
AWSAuditManagerAdministratorAccess – 更新了现有策略	我们更新了 `events:source` 的关键条件策略，以反映这是一个多值键。	04/29/2022
AWSAuditManagerServiceRolePolicy – 更新了现有策略	我们更新了 `events:source` 的关键条件策略，以反映这是一个多值键。	03/16/2022
AWS Audit Manager 已开始跟踪更改	AWS Audit Manager 开始跟踪其 AWS 托管策略的更改。	05/06/2021

对 AWS Audit Manager 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Audit Manager 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 AWS Audit Manager
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 AWS Audit Manager 资源

我无权在以下位置执行操作 AWS Audit Manager

当用户无权使用 AWS Audit Manager 或 Audit Manager API 操作时，就会出现`AccessDeniedException`错误。

在这种情况下，您的管理员必须更新策略以允许用户访问。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Audit Manager。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Audit Manager 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AWS Audit Manager 资源

您可以创建一个角色，以便其他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，可以代入角色。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 Audit Manager 是否支持这些功能，请参阅 如何 AWS Audit Manager 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户

- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）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存取之间的差别，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。

将服务相关角色用于 AWS Audit Manager

AWS Audit Manager 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Audit Manager 直接关联的独特类型的 IAM 角色。服务相关角色由 Audit Manager 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Audit Manager 更加容易，因为您不必手动添加必要的权限。Audit Manager 定义其服务相关角色的权限，除非另外定义，否则只有 Audit Manager 可以代入该角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

有关支持服务相关角色的其他服务的信息，请参阅可与 IAM 搭配使用的AWS 服务，并查找服务相关角色列中为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

的服务相关角色权限 AWS Audit Manager

Audit Manager 使用名为的服务相关角色**`AWSServiceRoleForAuditManager`**，该角色允许访问使用或管理的 AWS Audit ManagerAWS 服务和资源。

`AWSServiceRoleForAuditManager` 服务相关角色信任 `auditmanager.amazonaws.com` 服务来代入角色。

角色权限策略允许 Au `AWSAuditManagerServiceRolePolicy`dit Manager 自动收集有关您的 AWS 使用情况的证据。更具体地说，它可以代表您执行以下操作。

- Audit Manager 可以 AWS Security Hub 用来收集合规性检查证据。在这种情况下，Audit Manager 使用以下权限直接从中报告安全检查结果 AWS Security Hub。然后，它将结果作为证据附加到您的相关评测控件中。
  - `securityhub:DescribeStandards`

> **Note**
>
> 有关 Audit Manager 可以描述哪些特定 Security Hub 控件的更多信息，请参阅 AWS Audit Manager支持的AWS Security Hub 控件。

- Audit Manager 可以 AWS Config 用来收集合规性检查证据。在这种情况下，Audit Manager 使用以下权限直接从中报告 AWS Config 规则评估结果 AWS Config。然后，它将结果作为证据附加到您的相关评测控件中。
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > 有关 Audit Manager 可以描述哪些特定 AWS Config 规则的更多信息，请参阅 Audit Manager 支持的AWS Config 规则 AWS Audit Manager。

- Audit Manager 可以 AWS CloudTrail 用来收集用户活动证据。在这种情况下，Audit Manager 使用以下权限从 CloudTrail 日志中捕获用户活动。然后，它将该活动作为证据附加到您的相关评测控件中。
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > 有关 Audit Manager 可以描述哪些特定 CloudTrail AWS CloudTrail 事件的更多信息，请参阅支持的事件名称 AWS Audit Manager。

- Audit Manager 可以使用 AWS API 调用来收集资源配置证据。在这种情况下，Audit Manager 使用以下权限为以下 AWS 服务调用描述资源配置的只读 API。然后，它会将 API 响应作为证据附加到您的相关评测控件中。
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`

- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints

- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams

- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations

- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - 此 API 操作 AWS 账户 在可用的范围内运行。 service-linked-role 但无法访问跨账户存储桶策略。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups

- waf-regional:ListSubscribedRuleGroups

- `waf-regional:ListWebACLs`
- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> 有关 Audit Manager 可以描述的特定 API 调用的更多信息，请参阅 支持自定义控件数据来源的 API 调用。

要查看服务相关角色的完整权限详细信息`AWSServiceRoleForAuditManager`，请参阅AWSAuditManagerServiceRolePolicy《AWS 托管策略参考指南》。

您必须配置权限，允许 IAM 实体（如用户、组或角色）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。

创建 AWS Audit Manager 服务相关角色

您无需手动创建服务相关角色。启用后 AWS Audit Manager，该服务会自动为您创建服务相关角色。您可以从的入门页面启用 Audit Manager AWS Management Console，也可以通过 API 或 AWS CLI启用。有关更多信息，请参阅本用户指南中的 启用了 AWS Audit Manager。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。

编辑 AWS Audit Manager 服务相关角色

AWS Audit Manager 不允许您编辑`AWSServiceRoleForAuditManager`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。

允许 IAM 实体编辑 **`AWSServiceRoleForAuditManager`** 服务相关角色的描述

将以下语句添加到需要编辑服务相关角色的描述的 IAM 实体的权限策略。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
```

```
}
```

删除 AWS Audit Manager 服务相关角色

如果您不再使用 Audit Manager，我们建议您删除 `AWSServiceRoleForAuditManager` 服务相关角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色，然后才能将其删除。

清除 服务相关角色

必须先确认服务相关角色没有活动会话并移除该角色使用的任何资源，然后才能使用 IAM 删除 Audit Manager 服务相关角色。为此，请确保将 Audit Manager 全部 AWS 区域注销。取消注册后，Audit Manager 将不再使用服务相关角色。

有关如何取消注册 Audit Manager 的说明，请参阅以下资源：

- 本指南中的禁用 AWS Audit Manager
- 《AWS Audit Manager API 参考》中的 DeregisterAccount
- 在 “参考资料” 中注销账户AWS CLI AWS Audit Manager

有关如何手动删除 Audit Manager 资源的说明，请参阅本指南中的删除 Audit Manager 数据。

删除 服务相关角色

您可以使用 IAM 控制台、 AWS Command Line Interface (AWS CLI) 或 IAM API 删除服务相关角色。

IAM console

请按照以下步骤在 IAM 控制台中删除服务相关角色。

删除服务相关角色 (控制台)

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色。然后选中 `AWSServiceRoleForAuditManager` 旁边的复选框，而不是选择名称或行本身。
3. 在页面顶部的角色操作下方，选择删除。
4. 在确认对话框中，查看上次访问的信息，该信息显示每个选定角色上次访问 AWS 服务的时间。这样可帮助您确认角色当前是否处于活动状态。如果要继续，请在文本输入字段中输入 **`AWSServiceRoleForAuditManager`**，然后选择删除以提交服务相关角色进行删除。

5. 监视 IAM 控制台通知，以监控服务相关角色的删除进度。由于 IAM 服务相关角色删除是异步的，因此，在您提交角色进行删除后，删除任务可能成功，也可能失败。如果任务成功，则角色将从列表中移除，并会在页面顶部显示成功消息。

AWS CLI

您可以使用中的 IAM 命令 AWS CLI 删除服务相关角色。

删除服务相关角色 (AWS CLI)

1. 输入以下命令以列出您账户中的角色：

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. 如果服务相关角色正被使用或具有关联的资源，则无法删除它，因此您必须提交删除请求。如果不满足这些条件，该请求可能会被拒绝。您必须从响应中捕获 `deletion-task-id` 以检查删除任务的状态。

   键入以下命令以提交服务相关角色的删除请求：

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. 使用以下命令以检查删除任务的状态：

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   删除任务的状态可能是 `NOT_STARTED`、`IN_PROGRESS`、`SUCCEEDED` 或 `FAILED`。如果删除失败，则调用会返回失败的原因，以便您进行问题排查。

IAM API

您可以使用 IAM API 删除服务相关角色。

删除服务相关角色（API）

1. GetRole致电列出您账户中的角色。在请求中，指定 `AWSServiceRoleForAuditManager` 作为 `RoleName`。

2. 如果服务相关角色正被使用或具有关联的资源，则无法删除它，因此您必须提交删除请求。如果不满足这些条件，该请求可能会被拒绝。您必须从响应中捕获 `DeletionTaskId` 以检查删除任务的状态。

   要提交服务相关角色的删除请求，请调用 DeleteServiceLinkedRole。在请求中，指定 `AWSServiceRoleForAuditManager` 作为 `RoleName`。

3. 要检查删除的状态，请调用 GetServiceLinkedRoleDeletionStatus。在请求中，指定 `DeletionTaskId`。

   删除任务的状态可能是 `NOT_STARTED`、`IN_PROGRESS`、`SUCCEEDED` 或 `FAILED`。如果删除失败，则调用会返回失败的原因，以便您进行问题排查。

> **Tip**
>
> 如果 Audit Manager 服务正在使用该角色或具有关联的资源，则删除失败。只有当您仍在一个或多个 AWS 区域注册了 Audit Manager 时，才会发生这种情况。取消注册后，Audit Manager 将停止使用服务相关角色。
> 要解决删除失败的问题，请先确保在所有使用该服务 AWS 区域 的地方注销 Audit Manager。然后，重新尝试按照之前过程中的步骤操作。

AWS Audit Manager 服务相关角色支持的区域

AWS Audit Manager 支持在所有提供服务 AWS 区域 的地方使用与服务相关的角色。有关更多信息，请参阅AWS 服务端点。

合规性验证 AWS Audit Manager

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全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，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- 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的最佳实践， AWS 服务并将指南映射到跨多个框架（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)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。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践。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— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Audit Manager

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。

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失效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。

中的基础设施安全 AWS Audit Manager

作为一项托管服务，AWS Audit Manager 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 AWS Audit Manager。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（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 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 主体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。

您可以从任何网络位置调用这些 API 操作， AWS Audit Manager 但支持基于资源的访问策略，其中可能包括基于源 IP 地址的限制。您还可以使用 Audit Manager 策略来控制来自特定 Amazon Virtual Private Cloud (Amazon VPC) 端点或特定 VPC 的访问。实际上，这可以将对给定 Audit Manager 资源的网络访问与 AWS 网络中的特定 VPC 隔离开来。

AWS Audit Manager 和接口 VPC 终端节点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您 AWS Audit Manager 的 VPC 和之间建立私有连接。接口端点由 AWS PrivateLink 提供支持，该技术支持您通过私密方式访问 Audit Manager API，而无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与 Audit Manager API 进行通信。您的 VPC 和 VPC 之间的流量 AWS Audit Manager 不会离开 AWS 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》中的接口 VPC 端点 (AWS PrivateLink)。

AWS Audit Manager VPC 终端节点的注意事项

在为设置接口 VPC 终端节点之前 AWS Audit Manager，请务必查看 Amazon VPC 用户指南中的接口终端节点属性和限制。

AWS Audit Manager 支持从您的 VPC 调用其所有 API 操作。

为 AWS Audit Manager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 AWS Audit Manager 服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建接口端点。

AWS Audit Manager 使用以下服务名称创建 VPC 终端节点：

- com.amazonaws.*region*.auditmanager

例如，如果您为终端节点启用私有 DNS，则可以使用该终端节点的默认 DNS 名称向 AWS Audit Manager 发出 API 请求auditmanager.us-east-1.amazonaws.com。

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口端点访问服务。

为创建 VPC 终端节点策略 AWS Audit Manager

您可以为 VPC 端点附加控制对 AWS Audit Manager的访问的端点策略。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

示例：用于 AWS Audit Manager 操作的 VPC 终端节点策略

以下是的终端节点策略示例 AWS Audit Manager。当附加到端点时，此策略会向所有资源上的所有主体授予对列出的 Audit Manager 操作的访问权限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

登录和监控 AWS Audit Manager

监控是维护 Audit Manager 和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS 提供了以下监视工具，用于监视 Audit Manager，在出现问题时进行报告，并在适当时自动采取措施：

- AWS CloudTrail 捕获由您的 AWS 账户 或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 桶。您可以标识哪些用户和账户调用了 AWS、发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅AWS CloudTrail 《用户指南》。
- Amazon EventBridge 是一项无服务器事件总线服务，可以轻松地将您的应用程序与来自各种来源的数据连接起来。 EventBridge 提供来自您自己的应用程序、S oftware-as-a-Service (SaaS) 应用程序和 AWS 服务的实时数据流，并将这些数据路由到 Lambda 等目标。这使您能够监控服务中发生的事件，并构建事件驱动的架构。有关更多信息，请参阅 Amazon EventBridge 用户指南。

AWS Audit Manager 使用 Amazon 进行监控 EventBridge

Amazon EventBridge 可帮助您自动处理 AWS 服务 并自动响应系统事件，例如应用程序可用性问题或资源更改。

您可以使用 EventBridge规则来检测和响应 Audit Manager 事件。根据您创建的规则，当事件与您在规则中指定的值匹配时， EventBridge 调用一个或多个目标操作。根据事件类型，您可能想要发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。

例如，每当您的账户中发生以下 Audit Manager 事件时，您都可以检测到：

- 审计负责人创建、更新或删除评测
- 审计负责人委托控件集进行审核
- 委托人完成审核并将已审核的控件集提交给审计负责人
- 审计负责人更新评测控制的状态

可自动触发的操作包括：

- 使用 AWS Lambda 函数将通知传递给 Slack 频道。
- 将有关检查的数据推送到 Amazon Kinesis Data Streams 流，以支持全面、实时的状态监控。
- 将 Amazon Simple Notification Service (Amazon SNS) 主题发送到您的电子邮件。
- 获取 Amazon CloudWatch 警报操作的通知。

> **Note**
>
> Audit Manager 持久传送事件。这意味着 Audit Manager 将成功地尝试将事件传送到 EventBridge 至少一次。如果由于 EventBridge 服务中断而无法交付事件，Audit Manager 稍后将再次重试这些事件，最长可达 24 小时。

EventBridge Audit Manager 的示例格式

以下 JSON 代码显示了 Audit Manager 中创建评测事件的示例。有关此事件中任何字段的信息，请参阅事件结构参考。

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

创建 EventBridge 规则的先决条件

在为 Audit Manager 事件创建规则之前，建议执行以下操作：

- 熟悉中的事件、规则和目标。 EventBridge有关更多信息，请参阅什么是亚马逊 EventBridge？ 在《亚马逊 EventBridge 用户指南》中。
- 创建要在您的事件规则中使用的目标。例如，您可以创建 Amazon SNS 主题，以便每当完成控件集审核时，您都会收到短信或电子邮件。有关更多信息，请参阅EventBridge 目标。

为 Audi EventBridge t Manager 创建规则

按照以下步骤创建一条在 Audit Manager 发出的事件上触发的 EventBridge 规则。尽最大努力发出事件。

为 Audi EventBridge t Manager 创建规则

1. 打开亚马逊 EventBridge 控制台，网址为 https://console.aws.amazon.com/events/。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 在定义规则详细信息页面上，输入规则名称和描述。
5. 对于 事件总线和 规则类型，保留默认值，然后选择下一步。
6. 在构建事件模式页面上，为事件源选择AWS 事件或 EventBridge 合作伙伴事件。
7. 对于创建方法，选择自定义模式（JSON 编辑器）。
8. 在事件模式下，用 JSON 编写事件模式并指定要用于匹配的字段。

   要匹配 Audit Manager 事件，您可以使用以下简单模式：

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   将##替换为以下支持的值之一：

   a. 输入 `Assessment Created` 以在创建评测时收到通知。

   b. 输入 `Assessment Updated` 以在更新评测时收到通知。

   c. 输入 `Assessment Deleted` 以在删除评测时收到通知。

   d. 输入 `Assessment ControlSet Delegation Created` 以在委托控件集进行审核时收到通知。

   e. 输入 `Assessment ControlSet Reviewed` 以在审核评测控件集时收到通知。

f. 输入 `Assessment Control Reviewed` 以在审核评测控件时收到通知。

> **Tip**
>
> 根据需要向事件模式添加更多字段。有关可用字段的更多信息，请参阅 Amazon EventBridge 事件模式。

9. 选择下一步。
10. 在选择目标页面上，选择您为此规则创建的目标，然后配置该类型所需的任何其他选项。例如，如果您选择 Amazon SNS，请确保正确配置 SNS 主题，以便通过电子邮件或短信通知您。

> **Tip**
>
> 显示的字段因所选服务而异。有关可用目标的更多信息，请参阅 EventBridge 控制台中的可用目标。

11. 对于许多目标类型， EventBridge 需要向目标发送事件的权限。在这些情况下， EventBridge 可以创建规则运行所需的 IAM 角色。

    a. 若要自动创建 IAM 角色，请选择 Create a new role for this specific resource (为此特定资源创建新角色)。

    b. 要使用您之前创建的 IAM 角色，请选择 Use existing role (使用现有角色)。

12. （可选）选择 Add another target（添加其他目标），以为此规则添加其他目标。
13. 选择下一步。
14. （可选）在 Configure tags（配置标签）页面上，添加任意标签，然后选择 Next（下一步）。
15. 在 Review and create（审查并创建）页面上，审查您的规则设置并确保其符合您的事件监控要求。
16. 选择 创建规则。您的规则现在将监控 Audit Manager 事件，然后将它们发送到您指定的目标。

使用记录 AWS Audit Manager API 调用 CloudTrail

Audit Manager 与 CloudTrail一项服务集成，该服务提供用户、角色或 Audit Manager AWS 服务 中执行的操作的记录。 CloudTrail 将 Audit Manager 的所有 API 调用捕获为事件。捕获的调用包括来自 Audit Manager 控制台的调用和对 Audit Manager API 操作的代码调用。

如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Audit Manager 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。

使用收集的信息 CloudTrail，您可以确定向 Audit Manager 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

中的 Audit Manager 信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Audit Manager 中发生活动时，该活动会与其他 CloudTrail 事件一起记录在 AWS 服务 事件历史记录中。

您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录您的事件 AWS 账户，包括 Audit Manager 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。

此外，您可以配置其他 AWS 服务 ，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有 Audit Manager 操作都由 API 参考记录 CloudTrail 并记录在 AWS Audit Manager API 参考中。例如，对`DeleteControl`和 `UpdateAssessmentTemplate` API 操作的`CreateCustomControl`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。身份信息有助于您确定以下内容：

- 请求是否使用根用户凭证发出。
- 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 CloudTrail userIdentity 元素。

了解 Audit Manager 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该CreateAssessment操作的 CloudTrail 日志条目。

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
```

```
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

中的配置和漏洞分析 AWS Audit Manager

配置和 IT 控制由您（我们的客户）共同 AWS 负责。有关更多信息，请参阅责任 AWS 共担模型。

为 AWS Audit Manager 资源添加标签

标签是您或 AWS 为 AWS 资源分配的元数据标记。每个标签均包含一个键和一个值。对于您分配的标签，需要定义键和值。例如，您可以将键定义为 `stage`，将一个资源的值定义为 `test`。

标签可帮助您：

- 轻松找到您的 Audit Manager 资源。浏览框架库和控件库时，您可以使用标签作为搜索条件。
- 将您的资源与合规性类型相关联。您可以使用合规性专用标签来标记多个资源，以将这些资源与特定框架相关联。
- 标识和整理您的 AWS 资源。许多 AWS 服务都支持添加标签，因此，您可以将同一标签分配给来自不同服务的资源，以表明这些资源相互之间存在关系。
- 跟踪您的 AWS 成本。您可以在 AWS Billing and Cost Management 控制面板上激活这些标签。AWS 使用标签对您的成本进行分类，并向您提供每月成本分配报告。有关更多信息，请参阅《AWS Billing and Cost Management 用户指南》中的使用成本分配标签。

以下各部分提供有关 AWS Audit Manager 的标签的更多信息。

Audit Manager 中支持的资源

以下 Audit Manager 资源支持标记：

- 评测
- 控件
- 框架

标签限制

以下基本限制适用于 Audit Manager 资源上的标签：

- 您可以分配给资源的最大标签数量 — 50
- 最大密钥长度 — 128 个 Unicode 字符
- 最大值长度 — 256 个 Unicode 字符
- 键和值的有效字符 — a-z、A-Z、0-9、空格和以下字符：_ . : / = + - 和 @

- 键和值区分大小写
- 请不要使用 `aws:` 作为键的前缀；它保留为供 AWS 使用

管理标签

在创建评测、框架或控件时，可以将标签设置为属性。您可以使用 Audit Manager 控制台、AWS Command Line Interface (AWS CLI) 和 Audit Manager API 添加、编辑和删除标签。有关更多信息，请参阅以下链接。

- 对于评测：
  - 本指南评测部分中的 创建评测 和 编辑评测
  - 本指南审查评测部分中的 标签选项卡
  - AWS Audit Manager API 参考中的 CreateAssessment 和 UpdateAssessment
  - AWS Audit Manager API 参考中的 TagResource 和 UntagResource
- 对于框架：
  - 本指南框架库部分中的 创建自定义框架 和 编辑自定义框架
  - 本指南查看框架详细信息部分中的标签选项卡
  - AWS Audit Manager API 参考中的 CreateAssessmentFramework 和 UpdateAssessmentFramework
  - AWS Audit Manager API 参考中的 TagResource 和 UntagResource
- 对于控件：
  - 本指南控件库部分中的 创建自定义控件 和 编辑自定义控件
  - 本指南查看控件详细信息部分中的标签选项卡
  - AWS Audit Manager API 参考中的 CreateControl 和 UpdateControl
  - AWS Audit Manager API 参考中的 TagResource 和 UntagResource

使用 AWS CloudFormation 创建 AWS Audit Manager 资源

AWS Audit Manager 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（例如评测），AWS CloudFormation 将为您预调配和配置这些资源。

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 Audit Manager 资源。仅描述您的资源一次，然后在多个AWS账户和区域中反复配置相同的资源。

Audit Manager 和 AWS CloudFormation 模板

要为 Audit Manager 和相关服务预调配和配置资源，您必须了解 AWS CloudFormation 模板模板。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，可以在 AWS CloudFormation Designer 的帮助下开始使用 AWS CloudFormation 模板。有关更多信息，请参阅 AWS CloudFormation 用户指南中的什么是 AWS CloudFormation Designer？。

Audit Manager 支持在 AWS CloudFormation 中创建评测。有关更多信息（包括这些评测的 JSON 和 YAML 模板示例），请参阅 AWS CloudFormation 用户指南中的 AWS Audit Manager 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

AWS Audit Manager 用户指南的文档历史记录

下表介绍了 2020 年 12 月 8 日之后 AWS Audit Manager 用户指南每一版中的重要更改。

变更	说明	日期
支持的新框架：PCI DSS V4.0	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 PCI DSS V4.0。	2023 年 12 月 19 日
支持其他 AWS API 调用	现在，您可以在 Audit Manager 中将其他 AWS API 调用作为自定义控件的数据来源。有关更多信息，请参阅 VPC 支持的数据来源。	2023 年 12 月 7 日
更新了 AWS 托管式策略	AWS Audit Manager 已更新 AWSAuditManagerServiceRolePolicy。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2023 年 12 月 6 日
支持 AWS Security Hub 整合的控件检查结果	Audit Manager 现在支持 AWS Security Hub 中整合控件。有关更多信息，请参阅 AWS Audit Manager 支持的 AWS Security Hub 控件。	2023 年 11 月 16 日
与 MetricStream 集成	现在，您可以将来自 Audit Manager 的证据提取至 MetricStream 中。有关更多信息，请参阅与第三方 GRC 产品集成。	2023 年 11 月 14 日
新的支持框架：AWS生成式人工智能最佳实践	新的预构建框架现已在 AWS Audit Manager 中推出。有关	2023 年 11 月 8 日

	更多信息，请参阅 AWS生成式人工智能最佳实践框架 v1。	
更新了 AWS 托管式策略	AWS Audit Manager 已更新 AWSAuditManagerServiceRolePolicy。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2023 年 11 月 6 日
与 Amazon EventBridge 集成	现在，您可以监控 AWS Audit Manager 中发生的事件，并将这些事件用作事件驱动架构的一部分。有关更多信息，请参阅使用 Amazon EventBridge 监控 AWS Audit Manager。	2023 年 8 月 18 日
支持风险评测和新的手动举证选项	现在，您可以使用自定义控件创建工作流程支持风险评测。控件现在可以代表风险评测问题，您可以通过上传文件或输入文本，以手动举证提供答案。有关更多信息，请参阅 创建自定义控件和手动添加证据。	2023 年 6 月 12 日
支持用 CSV 格式导出	现在可以用 CSV 格式导出证据查找器搜索结果。有关更多信息，请参阅导出搜索结果。	2023 年 6 月 9 日
新支持框架：澳大利亚网络安全中心 (ACSC) 信息安全手册	新的预构建框架现已在 AWS Audit Manager 中推出。若要了解更多信息，请参阅澳大利亚网络安全中心 (ACSC) 信息安全手册。	2023 年 3 月 24 日

改进评测报告	我们改进了 Audit Manager 评测报告的格式和内容。有关如何浏览和理解评测报告的更多信息，请参阅评测报告。	2023 年 3 月 23 日
支持分页 API 调用	AWS Audit Manager 现在支持将分页 API 调用作为证据收集数据来源。有关更多信息，请参阅 分页 API 调用。	2023 年 3 月 8 日
新支持框架：2013 年 HIPAA 最终综合安全规则	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 2013 年 HIPAA 最终综合安全规则。为了区分起见，以前存在的 HIPAA 框架（以前在框架库内的名称为 HIPAA）现在被命名为 2003 年 HIPAA 安全规则。	2023 年 3 月 8 日
支持其他 AWS API 调用	现在，您可以在 Audit Manager 中使用另外九个 AWS API 调用作为自定义控件的数据来源。有关更多信息，请参阅 VPC 支持的数据来源。	2023 年 3 月 3 日
更新了指南，使其符合 IAM 最佳实践	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 1 月 6 日
新数据留存设置	现在，当您禁用 Audit Manager 时，可指定是否要删除所有数据。有关更多信息，请参阅禁用 AWS Audit Manager 和删除 Audit Manager 数据。	2023 年 1 月 6 日

证据查找器支持	现在，您可使用证据查找器对证据数据进行搜索查询。有关更多信息，请参阅证据查找器。	2022 年 11 月 18 日
新支持框架：澳大利亚网络安全中心 (ACSC) 八大要素	新的预构建框架现已在 AWS Audit Manager 中推出。若要了解更多信息，请参阅澳大利亚网络安全中心 (ACSC) 八大要素。	2022 年 8 月 24 日
更新了 AWS 托管式策略	AWS Audit Manager 已更新 AWSAuditManagerServiceRolePolicy。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2022 年 7 月 7 日
更新了 AWS 托管式策略	AWS Audit Manager 已更新 AWSAuditManagerServiceRolePolicy。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2022 年 5 月 20 日
新支持框架：加拿大网络安全中心中型云控制配置文件	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅加拿大网络安全中心中型云控制配置文件。	2022 年 5 月 6 日
更新了 AWS 托管式策略	AWS Audit Manager 已更新了 AWSAuditManagerAdministratorAccess 策略。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2022 年 4 月 29 日

支持其他 AWS Config 托管规则	现在，您可以在 Audit Manager 中使用另外 91 个 AWS Config 托管规则作为自定义控件的数据来源。有关更多信息，请参阅通过 AWS Audit Manager 使用 AWS Config 托管规则。	2022 年 4 月 27 日
支持 AWS Config 自定义规则	现在您可用 AWS Config 自定义规则作为 Audit Manager 自定义控件的数据来源。有关更多信息，请参阅通过 AWS Audit Manager 使用 AWS Config 自定义规则。	2022 年 4 月 27 日
新支持框架：ISO/IEC 27001:2013 附录 A	新的预构建框架现已在 AWS Audit Manager 中推出。欲了解更多信息，请参阅 ISO/IEC 27001:2013 附录 A。	2022 年 4 月 7 日
更新了 AWS 托管式策略	AWS Audit Manager 已更新 AWSAuditManagerServiceRolePolicy。有关更多信息，请参阅 适用于 AWS Audit Manager 的 AWS 托管策略。	2022 年 3 月 16 日
新支持框架：CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4	两个新的预建框架现已推出，即 AWS Audit Manager: CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4 1 级 以及 CIS Amazon Web Services 基金会基准的 CIS 基准，v1.4 1 级和 2 级。有关更多信息，请参阅 CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0。	2022 年 3 月 2 日

新支持框架：CIS Controls v8 IG1	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 CIS 控件 v8 IG1。	2022 年 3 月 2 日
AWS Audit Manager 控制面板	现在，您可以使用 Audit Manager 控制面板监控活动评测，并快速识别不合规证据。有关更多信息，请参阅使用 Audit Manager 控制面板。	2021 年 11 月 18 日
自定义框架共享	现在，您可以与其他 AWS 账户 共享您的自定义 Audit Manager 框架，也可将其复制到您自有账户下的其他 AWS 区域。有关更多信息，请参阅共享自定义框架。	2021 年 10 月 22 日
新的 AWS Audit Manager 控件示例	现在，您可以查看控件示例，了解 Audit Manager 如何帮助您将 AWS 环境与其要求保持一致。有关更多信息，请参阅AWS Audit Manager 控件示例。	2021 年 9 月 21 日
新支持框架：Gramm-Leach-Bliley 法案 (GLBA)	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 Gramm-Leach-Bliley 法案 (GLBA)。	2021 年 9 月 2 日
新故障排除章节	现在提供新故障排除章节。有关更多信息，请参阅 AWS Audit Manager 中的故障排除。	2021 年 8 月 23 日

新的委托章节与教程	我们在新的章节中介绍委托文件。有关更多信息，请参阅 AWS Audit Manager 中的委托。我们还在 AWS Audit Manager 中为首次审阅控件设置的委托人添加了新教程。有关更多信息，请参阅委托人教程：审阅控件设置。	2021 年 6 月 25 日
新支持框架：NIST SP 800-171 Rev. 2	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 NIST SP 800-171 Rev. 2。	2021 年 6 月 17 日
改进评测报告	我们改进了 AWS Audit Manager 评测报告的格式和内容。有关如何浏览和理解新评测报告的更多信息，请参阅评测报告。	2021 年 6 月 8 日
新的 AWS 托管式策略页面	AWS Audit Manager 为其托管式策略开启了跟踪更改。有关更多信息，请参阅适用于 AWS Audit Manager 的 AWS 托管式策略。	2021 年 5 月 6 日
新支持框架：NIST 网络安全框架 1.1 版	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 NIST 网络安全框架 1.1 版。	2021 年 5 月 5 日
新支持框架：AWS Well-Architected	新的预构建框架现已在 AWS Audit Manager 中推出。欲了解更多信息，请参阅 AWS Well-Architected。	2021 年 5 月 5 日

新支持框架：AWS 基础安全防御最佳实践	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 AWS 基础安全防御最佳实践。	2021 年 5 月 5 日
新支持框架：GxP EU 附录 11	新的预构建框架现已在 AWS Audit Manager 中推出。欲了解更多信息，请参阅 GxP EU 附录 11。	2021 年 4 月 28 日
新支持框架：NIST 800-53（Rev. 5）Low-Moderate-High	新的预构建框架现已在 AWS Audit Manager 中推出。有关更多信息，请参阅 NIST 800-53（Rev. 5）Low-Moderate-High。	2021 年 3 月 25 日
新支持框架：CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3	AWS Audit Manager现已推出两个新预置框架，即：CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0 1 级 和 CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0 1 级和 2 级。有关更多信息，请参阅 CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0。	2021 年 3 月 22 日
初始版本	首次发布 AWS Audit Manager 用户指南和 API 参考。	2020 年 12 月 8 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。