



安全信息

AWS 控制目录



AWS 控制目录: 安全信息

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是控制目录？	1
本体论概述	1
Catalog	2
安全性	3
数据保护	3
数据加密	4
传输中加密	4
密钥管理	4
互联网络流量隐私	4
身份和访问管理	5
受众	5
使用身份进行身份验证	5
使用策略管理访问	8
控制目录如何与 IAM 配合使用	10
基于身份的策略示例	16
故障排除	19
合规性验证	21
恢复能力	21
基础设施安全性	22
配置和脆弱性	22
监控	23
CloudTrail 日志	23
控制中的目录信息 CloudTrail	23
了解控制目录日志文件条目	24
AWS PrivateLink	26
注意事项	26
创建接口端点	26
创建端点策略	26
文档历史记录	28
.....	xxix

什么是控制目录？

欢迎阅读控制目录安全信息指南。控制目录是其中的一部分 AWS Control Tower，它列出了多个 AWS 服务的控件。它是 AWS 控件的合并目录。如果出现上述情况 AWS Control Tower，则无需设置。

使用Control Catalog。

在本文档中，您可以找到在使用 Control Catalog 提供的安全与合规性信息时 APIs 需要了解的安全和合规性信息。

控制目录体现了控制本体论，这是控件的标准分类系统。

本体论概述

AWS 开发了标准分类系统，以帮助对控件进行分类、组织和创建映射。该本体可用于将控制与现有和新的监管标准（包括 24 个框架）以及监管标准（例如 PCI、HIPAA 等）对应起来。我们还映射到行业标准，例如NIST和ISO，以及亚马逊特定的框架，包括Well-Architected框架。

本体有四个核心方面

- 按控制域、控制目标和常用控制对控制进行分类。本体有助于将相关的控件组织和分组为三个级别

- L1：控制域，
- L2：控制目标，
- L3：通用控制。

这些级别具有严格的等级关系。也就是说，每个域都有多个控制目标，但每个控制目标必须有一个父域。每个控制目标都有多个常用控件，但每个常用控制目标都有一个单父目标。

- 映射到监管标准。本体有一个称为标准控制（L4）的概念，它代表了监管或行业标准中的特定要求。这些标准控件映射到有助于满足这些特定要求的常用控件。

例如，PCI- DSS v3.2.1。ID 4.1 在通过开放的公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，以及 NIST 800.53.r5 ID SC-16 安全和隐私属性的传输是两个标准控件，两者都映射到传输中的加密数据通用控件。

- 控制实施和控制证据。本体有一个控制实现（L6）的概念，它可以表示控件 AWS、AWS Security Hub 检查、AWS Config 规则等中的特定 AWS Control Tower 控制实现，也可以表示外部的非技术实现 AWS，例如过程指导。单独的控制证据（L7）概念表示可由 AWS Audit Manager第三方工具或

客户自己用作控制证据的数据源。这些证据 AWS 来源可能是 AWS CloudTrail 事件、API 调用日志和 AWS Config 规则评估结果等来源。或者，它们可能是外部来源，例如客户文档。

- 核心控件 (L5) 的概念。核心控件是一个映射层，它将所有控制实现 (L6)、相应的证据来源 (L7)、相关的标准控件 (L4) 和常用控件 (L3) 整合到一个整体对象中。核心控件与其说是一个控件本身，不如说是一个映射文档。它有助于回答向我展示与控件 X 相关的所有信息的问题。每个核心控制可以有多个控制实现 (L6) 和多个证据来源 (L7)。

总而言之，AWS 控制目录本体包含七层。三个是分层分类层（控制域、控制目标、通用控制）。另一层（标准控制）描述了监管或行业标准要求。映射层（核心控件）描述给定资源类型的控制结果。两层（控制实现、控制证据）描述了具体的控制实施和证据来源。

本体论是由一 AWS 组经过认证的审计师根据他们与数百家客户合作进行合规审计的经验设计的。控制域、控制目标、通用控制和标准控制 (L1-L4) 的概念在整个行业中都使用。它们符合常见的行业模式和 NIST 的建议。其余三个层 (L5-L7) 是根据现有 AWS 概念（例如资源类型和托管控件）设计的。

Catalog

控制目录可通过控制台和控制目录应用程序编程接口 (API) 获得。此 API 提供了一种编程方式来识别和筛选您作为 AWS 客户可用的常用控件和相关元数据。有关更多信息，请参阅 [Control Catalog API 参考](#)。

控制目录中的安全性

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 AWS 的共同责任。[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 负责保护在云 AWS 服务 中运行的基础架构 AWS Cloud。AWS 还为您提供可以安全使用的服务。作为[AWS 合规计划](#)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。要了解适用于控制目录的合规性计划，请参阅[按合规计划AWS 服务 划分的范围内的AWS 服务 \(按合规分\)](#)。
- 云端安全 — 您的责任由您 AWS 服务 使用的内容决定。您还需要对其他因素负责，包括您的数据的敏感性、您的要求以及适用的法律法规。

本文档可帮助您了解在使用控制目录时如何应用分担责任模型；以下主题向您介绍如何配置控制目录；以实现您的安全和合规性目标。您还将学习如何使用其他 AWS 服务 工具来监控和保护您的控制目录资源。

主题

- [控制目录中的数据保护](#)
- [控制目录的身份和访问管理](#)
- [控制目录的合规性验证](#)
- [控制目录中的弹性](#)
- [控制目录中的基础设施安全](#)

控制目录中的数据保护

分 AWS [担责任模型](#)适用于 AWS 控制目录中的数据保护。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结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题](#)。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 [AWS Shared Responsibility Model and 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。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)。
- 用于 SSL/TLS 与 AWS 资源通信。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。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用跟 CloudTrail 踪](#)。
- 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 140-3 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 140-3 版》](#)。

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）。这包括您使用控制台、API 或 AWS 服务使用 AWS 控制目录或其他方式时 AWS SDKs。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。

数据加密

AWS 控制目录不存储任何客户数据。

静态加密

AWS 控制目录不加密客户数据。由于 AWS 控制目录不会保留或保留任何客户数据，因此没有针对静态加密的具体指导方针。

传输中加密

AWS 控制目录不加密客户数据。由于 Cont AWS rol Catalog 不会交换或保存任何敏感数据，因此对于传输中的加密没有具体的指导方针。

密钥管理

加密密钥管理不适用于 AWS 控制目录。

互联网络流量隐私

网络间流量隐私不适用于 AWS 控制目录。

控制目录的身份和访问管理

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 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 AWS 控制目录资源。您可以使用 IAM AWS 服务，无需支付额外费用。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [控制目录如何与 IAM 配合使用](#)
- [控制目录的基于身份的策略示例](#)
- [控制目录身份和访问权限疑难解答](#)

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 AWS 控制目录中所做的工作。

服务用户 — 如果您使用 AWS Control Catalog 服务完成工作，则您的管理员会为您提供所需的证书和权限。当您使用更多的 AWS 控制目录功能来完成工作时，您可能需要额外的权限。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 AWS 控制目录中的功能，请参阅[控制目录身份和访问权限疑难解答](#)。

服务管理员 — 如果您负责公司的 AWS 控制目录资源，则可能拥有对 AWS 控制目录的完全访问权限。您的工作是确定您的服务用户应访问哪些 AWS 控制目录功能和资源。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。要详细了解贵公司如何将 IAM 与 AWS 控制目录结合使用，请参阅[控制目录如何与 IAM 配合使用](#)。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 AWS 控制目录的访问权限。要查看您可以在 IAM 中使用的 AWS 控制目录基于身份的策略示例，请参阅[控制目录的基于身份的策略示例](#)

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 用户身份或通过担任 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，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合访问 AWS 时，您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[用于签署 API 请求的 AWS 签名版本 4](#)。

无论使用何种身份验证方法，您可能都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[IAM 中的 AWS 多重身份验证](#)。

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，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，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 Center 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，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

IAM 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，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的用例，应在需要时更新访问密钥](#)。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。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，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。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[IAM 用户的使用案例](#)。

IAM 角色

IAM 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。要在中临时担任 IAM 角色 AWS Management Console，您可以[从用户切换到 IAM 角色（控制台）](#)。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[代入角色的方法](#)。

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。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的[针对第三方身份提供商创建角色（联合身份验证）](#)。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的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 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- **跨账户存取**：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。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 中的跨账户资源访问](#)。
- **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，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 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，然后此操作在其他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项操作的权限。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链接到的服务角色。AWS 服务服务可以代入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 上运行的应用程序 EC2 — 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。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 [IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限](#)。

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 策略概览](#)。

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。管理员随后可以向角色添加 IAM 策略，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，假设您有一个允许 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[使用客户托管策略定义自定义 IAM 权限](#)。

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、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 and 角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的[在托管策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。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 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs 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 就是支持的服务示例 ACLs。AWS WAF 要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》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向您授予的最大权限。

- **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 (SCPs)** — SCPs 是 JSON 策略，用于指定中组织或组织单位 (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。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。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 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份 (包括身份) 的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的[资源控制策略 \(RCPs\)](#)。
 - 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解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](#)。

控制目录如何与 IAM 配合使用

在使用 IAM 管理对 AWS 控制目录的访问权限之前，请先了解有哪些 IAM 功能可用于 AWS 控制目录。

可与控制目录配合使用的 IAM 功能

IAM 特征	AWS 控制目录支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否

IAM 特征	AWS 控制目录支持
ABAC (策略中的标签)	否
临时凭证	是
主体权限	否
服务角色	否
服务相关角色	否

要全面了解 AWS 控制目录和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM [配合使用的AWS 服务](#)。

AWS 控制目录的基于身份的策略

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[使用客户管理型策略定义自定义 IAM 权限](#)。

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 控制目录的基于身份的策略示例

要查看 AWS 控制目录基于身份的策略示例，请参阅。[控制目录的基于身份的策略示例](#)

AWS 控制目录中基于资源的策略

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 中的跨账户资源访问](#)。

AWS 控制目录的策略操作

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 控制目录操作列表，请参阅服务授权参考中的 [AWS 控制目录定义的操作](#)。

AWS 控制目录中的策略操作在操作前使用以下前缀：

```
controlcatalog
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
    "controlcatalog:ListCommonControls",
    "controlcatalog:ListDomains"
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 List 开头的操作，请包括以下操作。

```
"Action": "controlcatalog:List*"
```

要查看 AWS 控制目录基于身份的策略示例，请参阅。 [控制目录的基于身份的策略示例](#)

AWS 控制目录的策略资源

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。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*" 
```

要查看 AWS 控制目录资源类型及其列表 ARNs，请参阅《服务授权参考》中的 [AWS 控制目录定义的资源](#)。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 [AWS 控制目录定义的操作](#)。

AWS 控制目录域的亚马逊资源名称 (ARN) 格式如下：

```
arn:${Partition}:controlcatalog:::domain/${domainId}
```

AWS 控制目录目标采用以下 ARN 格式：

```
arn:${Partition}:controlcatalog:::objective/${objectiveId}
```

AWS 控制目录常用控件采用以下 ARN 格式：

```
arn:${Partition}:controlcatalog:::commonControl/${commonControlId}
```

有关格式的更多信息 ARNs，请参阅 [Amazon 资源名称 \(ARNs\)](#)。

例如，要在语句中指定 i-1234567890abcdef0 域，请使用以下 ARN。

```
"Resource": "arn:aws:controlcatalog:::domain/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:controlcatalog:::domain/*" 
```

某些 AWS 控制目录操作（例如用于创建资源的操作）无法对特定资源执行。在这些情况下，您必须使用通配符（*）。

```
"Resource": "*"
```

某些 AWS 控制目录 API 操作支持多种资源。例如，ListCommonControls 访问公共控件、目标和域，因此委托人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 ARNs 用逗号分隔。

```
"Resource": [  
    "commonControl",  
    "objective",  
    "domain"
```

要查看 AWS 控制目录基于身份的策略示例，请参阅 [控制目录的基于身份的策略示例](#)

AWS 控制目录的策略条件密钥

支持特定于服务的策略条件键：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。

在 Condition 元素（或 Condition 块）中，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。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，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。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 策略元素：变量和标签](#)。

AWS 支持全局条件密钥和特定于服务的条件密钥。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](#)。

要查看 AWS 控制目录条件键列表，请参阅服务授权参考中的 [AWS 控制目录的条件密钥](#)。要了解您可以使用条件键的操作和资源，请参阅 [AWS 控制目录定义的操作](#)。

要查看 AWS 控制目录基于身份的策略示例，请参阅 [控制目录的基于身份的策略示例](#)

ACLs 在 AWS 控制目录中

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人 (账户成员、用户或角色) 有权访问资源。ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带有 AWS 控制目录的 ABAC

支持 ABAC (策略中的标签)：否

基于属性的访问控制 (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，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的[条件元素](#)中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的[使用 ABAC 授权定义权限](#)。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 \(ABAC \)](#)。

在 AWS 控制目录中使用临时证书

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 IAM 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，您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[从用户切换到 IAM 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](#)。

AWS 控制目录的跨服务委托人权限

支持转发访问会话 (FAS) : 否

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，然后此操作在其他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项操作的权限。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

AWS 控制目录的服务角色

支持服务角色 : 否

服务角色是由一项服务担任、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的[创建向 AWS 服务委派权限的角色](#)。

Warning

更改服务角色的权限可能会中断 AWS 控制目录的功能。仅当 AWS 控制目录提供相关指导时，才可编辑服务角色。

AWS 控制目录的服务相关角色

支持服务相关角色 : 否

服务相关角色是一种链接到的服务角色。AWS 服务服务可以代入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。

有关创建或管理服务相关角色的详细信息，请参阅[能够与 IAM 搭配使用的AWS 服务](#)。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

控制目录的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 AWS 控制目录资源。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。管理员随后可以向角色添加 IAM 策略，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 策略（控制台）](#)。

有关 AWS 控制目录定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的[AWS 控制目录的操作、资源和条件键](#)。ARNs

主题

- [策略最佳实践](#)
- [允许用户查看他们自己的权限](#)
- [允许用户查看 AWS 控制目录中的资源](#)

策略最佳实践

基于身份的策略决定是否有人可以在您的账户中创建、访问或删除 AWS 控制目录资源。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，请遵循以下指南和建议：

- 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 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的[使用 IAM Access Analyzer 验证策略](#)。
- 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。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的[使用 MFA 保护 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 中的安全最佳实践](#)。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 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": "*"
    }
  ]
}
```

允许用户查看 AWS 控制目录中的资源

以下策略授予从 AWS 控制目录中列出域、目标和常用控件的权限。

```
{
```

```
"Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageControlCatalogAccess",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

控制目录身份和访问权限疑难解答

使用以下信息来帮助您诊断和修复在使用 AWS 控制目录和 IAM 时可能遇到的常见问题。

主题

- [我无权在控制目录中执行操作](#)
- [我无权执行 iam : PassRole](#)
- [我想让不在我之外的人 AWS 账户 访问我的控制目录资源](#)

我无权在控制目录中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 controlcatalog:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
controlcatalog:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 controlcatalog:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一条错误消息，指出您无权执行该iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 AWS Control Catalog。

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。

当名为的 IAM 用户marymajor尝试使用控制台在 AWS 控制目录中执行操作时，会出现以下示例错误。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。

我想让不在我之外的人 AWS 账户 访问我的控制目录资源

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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 AWS 控制目录是否支持这些功能，请参阅[控制目录如何与 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访问之间的差别，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

控制目录的合规性验证

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：

- [Security Compliance & Governance](#)：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- [符合 HIPAA 要求的服务参考](#)：列出符合 HIPAA 要求的服务。并非所有 AWS 服务 人都符合 HIPAA 资格。
- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [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 可以全面了解您的安全状态 AWS。Security Hub 通过安全控制措施评估您的 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措施的列表，请参阅 [Security Hub 控制措施参考](#)。
- [Amazon GuardDuty](#) — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- [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。

控制目录中的弹性

AWS 全球基础设施是围绕 AWS 区域 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连接。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结构相比，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](#)。

控制目录中的基础设施安全

作为一项托管服务，控制目录受到《[Amazon Web Services：安全流程概述](#)》白皮书中描述的 [AWS 全球网络安全](#) 程序的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问控制目录。客户端必须支持传输层安全性协议 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 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。

控制目录中的配置和漏洞分析

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](#)。

监控 AWS 控制目录

监控是维护 AWS Control Catalog 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 提供了以下监控工具，用于监视 AWS Control Catalog，在出现问题时进行报告，并在适当时自动采取措施：

- AWS CloudTrail 捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 [AWS CloudTrail 用户指南](#)。

使用记录 Control Catalog AWS CloudTrail

作为 AWS Control Tower 控制目录的一部分 AWS CloudTrail，后者作为一项服务，提供用户、角色或 AWS 服务所执行的操作的记录。CloudTrail 将控制目录的所有 API 调用作为事件捕获。捕获的调用包括直接从 AWS Control Tower 控制台的调用（例如启用或禁用控件的调用），以及对控制目录 API 操作的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括与控制目录中的控件有关的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history (事件历史记录) 中查看最新事件。使用收集的信息 CloudTrail，您可以确定向 Control Catalog 发出的请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。AWS Control Tower

要了解更多信息 CloudTrail，请参阅 [AWS CloudTrail 用户指南](#)。

控制中的目录信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当控制目录中发生活动时，该活动将记录在事件中，并与其他 AWS 服务 CloudTrail 事件一同保存在事件历史记录中。您可以在中查看、搜索和下载最新事件 AWS 账户。有关更多信息，请参阅 [使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您的 AWS 账户事件（包括 Control Catalog 的事件），请创建跟踪。通过跟踪 CloudTrail，您可以将日志文件传送至 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。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为配置 Amazon SNS 通知 CloudTrail](#)

- [从多个区域接收 CloudTrail 日志文件](#)和[从多个账户中接收 CloudTrail 日志文件](#)

所有控制目录操作均由《控制目录 API 参考》记录 CloudTrail 并记录在《[控制目录 API 参考](#)》中。。例如，对ListCommonControlsListObjectives、和ListDomains操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志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：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

了解控制目录日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了ListDomains操作。

```
{
  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:"controlcatalog.amazonaws.com",  
  eventName:"ListDomains",  
  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: null,  
  responseElements: null,  
  requestId:"0d950f8c-5211-40db-8c37-2ed38ffcc894",  
  eventId:"a782029a-959e-4549-81df-9f6596775cb0",  
  readOnly:false,  
  eventType:"AwsApiCall",  
  recipientAccountId:"recipientAccountId"  
}
```

使用接口端点访问控制目录 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您的 VPC 和控制目录之间创建私有连接。您可以像访问您的 VPC 一样访问 AWS 控制目录，无需使用互联网网关、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 地址即可访问控制目录。

您可以通过创建由 AWS PrivateLink 提供支持的接口端点来建立此私有连接。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者管理的网络接口，用作发往控制目录的流量的入口点。

有关更多信息，请参阅 AWS PrivateLink 指南 AWS PrivateLink 中的 [AWS 服务 通过访问](#)。

AWS 控制目录的注意事项

在为控制目录设置接口端点之前，请查看 AWS PrivateLink 指南中的 [注意事项](#)。

控制目录支持通过接口端点调用其所有 API 操作。

为控制目录创建接口端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为控制目录创建接口终端节点。有关更多信息，请参阅《AWS PrivateLink 指南》中的 [创建接口端点](#)。

使用以下服务名称为控制目录创建接口端点：

```
com.amazonaws.region.controlcatalog
```

如果您为接口终端节点启用私有 DNS，则可以使用控制目录的默认区域 DNS 名称向控制目录发出 API 请求。例如 `service-name.us-east-1.amazonaws.com`。

为 VPC 端点创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口端点。默认端点策略允许通过接口端点对控制目录进行完全访问权限。要控制允许从您的 VPC 访问控制目录，请将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可执行操作的主体 (AWS 账户、IAM 用户和 IAM 角色)。
- 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《AWS PrivateLink 指南》中的[使用端点策略控制对服务的访问权限](#)。

示例：控制目录操作的 VPC 终端节点策略

以下是自定义端点策略的示例。当您将此策略附加到接口终端节点时，它会向所有资源的所有委托人授予对列出的 AWS 控制目录操作的访问权限。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "controlcatalog:ListCommonControls"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

GetControl和 ListControls API 操作需要不同的权限，即默认的完全权限。有关示例，请参阅[默认终端节点策略](#)。

控制目录安全信息指南的文档历史记录

下表介绍了 Control Catalog 的文档版本。

变更	说明	日期
初始版本	控制目录 APIs 和安全信息指南的初始版本。	2024 年 4 月 8 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。