安全信息

AWS控制目录

AWS控制目录: 安全信息

Table of Contents

什么是AWS控制目录？ 1
本体论概述 1
对AWS控制目录的访问权限 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
Identity and Access Management 5
受众 5
使用身份进行身份验证 5
使用策略管理访问 8
AWS控制目录的工作原理 IAM 10
基于身份的策略示例 17
故障排除 19
合规性验证 21
弹性 22
基础架构安全性 22
配置和脆弱性 22
监控 23
CloudTrail 日志 23
AWS 控制目录信息位于 CloudTrail 23
了解 AWS 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AWS控制目录？

欢迎阅读AWS控制目录安全信息指南。控制目录是其中的一部分 AWS Control Tower，其中列出了几个控件 AWS 服务的支持。它是以下内容的合并目录 AWS 控件。您无需设置 AWS Control Tower 以使用控制目录。

使用控制目录，您可以根据常见用例（包括安全性、成本、耐久性和操作）查看控件。

在本文档中，您可以找到在使用 Cont AWS rol 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。此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PCIHIPAA、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一的父控制目标。
- 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，它可以代表中的特定控制实现 AWS，例如，一个 AWS Control Tower 控制，一个 AWS Security Hub 支票，一个 AWS Config 规则等等，

或者外部的非技术实现 AWS，例如过程指导。单独的控制证据 (L7) 概念表示可用作控制证据的数据源 AWS Audit Manager、第三方工具或客户本人。这些证据来源可能是 AWS 来源，例如 AWS CloudTrail 事件、API通话记录和 AWS Config 规则评估结果。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。

这个本体是由一个人设计的 AWS 由注册审计师组成的团队，基于他们与数百家客户合作进行合规审计的经验。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被使用。它们符合常见的行业模式和NIST建议。其余三层 (L5-L7) 是在现有基础上设计的 AWS 概念，例如资源类型和托管控件。

对AWS控制目录的访问权限

AWS控制目录可通过控制台和AWS控制目录应用程序编程接口 (API) 获得。这API提供了一种编程方式来识别和筛选常用控件和相关元数据，这些控件和相关元数据可用作为 AWS 客户。有关更多信息，请参阅《AWS控制目录API参考》。

AWS控制目录中的安全性

云安全位于 AWS 是最高优先级。作为 AWS 客户，您将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。

安全是双方的共同责任 AWS 还有你。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 负责保护运行的基础架构 AWS 服务 在 AWS Cloud. AWS 还为您提供可以安全使用的服务。作为安全措施的一部分，第三方审计师定期测试和验证我们安全的有效性 AWS 合规计划 。要了解适用于AWS控制目录的合规性计划，请参阅 AWS 按合规计划划分的范围内的服务 。
- 云端安全 — 您的责任由 AWS 服务 你用的。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AWS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AWS控制目录以满足您的安全和合规性目标。你还会学习如何使用其他 AWS 服务 可帮助您监控和保护您的AWS控制目录资源。

主题

- AWS控制目录中的数据保护
- AWS控制目录的身份和访问管理
- AWS控制目录的合规性验证
- 韧性在 AWS 控制目录
- AWS控制目录中的基础设施安全

AWS控制目录中的数据保护

这些区域有： AWS 分担责任模型适用于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设施 AWS Cloud。 您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，请参阅数据隐私 FAQ。 有关欧洲数据保护的信息，请参阅 AWS 责任共担模型和GDPR博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您进行保护 AWS 账户 凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。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与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。 有关使用 CloudTrail 轨迹进行捕获的信息 AWS 活动，请参阅使用中的 CloudTrail 轨迹 AWS CloudTrail 用户指南。
- 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。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当你使用AWS控制目录或其他控制目录时 AWS 服务 使用控制台，API，AWS CLI，或 AWS SDKs。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URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

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。因为不保留或保留任何客户数据 AWS 控制目录，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。因为不交换或保留任何敏感数据 AWS 控制目录，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。

AWS控制目录的身份和访问管理

AWS Identity and Access Management (IAM) 是一个 AWS 服务 可帮助管理员安全地控制对以下内容的访问权限 AWS 资源的费用。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。IAM是一个 AWS 服务 无需支付额外费用即可使用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS控制目录的工作原理 IAM
- 控制目录的基于身份的AWS策略示例
- AWS控制目录身份和访问权限疑难解答

受众

你怎么用 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控制目录服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多的AWS控制目录功能来完成工作时，你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AWS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管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM使用AWS控制目录，请参阅AWS控制目录的工作原理 IAM。

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对AWS控制目录的访问权限。要查看可在中使用的基于身份的AWS控制目录策略示例IAM，请参阅。控制目录的基于身份的AWS策略示例

使用身份进行身份验证

身份验证是您登录的方式 AWS 使用您的身份凭证。您必须经过身份验证（登录到 AWS) 作为 AWS 账户根用户、以IAM用户身份或通过担任IAM角色来完成。

你可以登录 AWS 使用通过身份源提供的凭证作为联合身份。 AWS IAM Identity Center （IAM身份中心）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，您的管理员之前使用IAM角色设置了联合身份。当你访问时 AWS 通过使用联合，您就是在间接担任角色。

根据您的用户类型，您可以登录 AWS Management Console 或者 AWS 访问门户。有关登录的更多信息 AWS，请参阅如何登录您的 AWS 账户中的 AWS 登录 用户指南。

如果你访问 AWS 以编程方式， AWS 提供了一个软件开发套件 (SDK) 和一个命令行界面 (CLI)，用于使用您的凭证对您的请求进行加密签名。如果你不使用 AWS 工具，你必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅签名 AWS APIIAM用户指南中的请求。

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) 来提高帐户的安全性。要了解更多信息，请参阅中的多重身份验证 AWS IAM Identity Center 《用户指南》和《使用多因素身份验证》(MFA) AWS（在 IAM 用户指南中）。

AWS 账户 根用户

当你创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 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。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。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM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进行访问 AWS 服务 通过使用临时证书。

联合身份是企业用户目录中的用户、Web 身份提供商、 AWS Directory Service、身份中心目录或任何访问的用户 AWS 服务 通过使用通过身份源提供的凭证。当联合身份访问时 AWS 账户，他们扮演角色，角色提供临时证书。

要进行集中访问管理，我们建议您使用 AWS IAM Identity Center。 您可以在 Ident IAM ity 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，以便在您的所有用户和群组中使用 AWS 账户 和应用程序。有关IAM身份中心的信息，请参阅什么是IAM身份中心？ 在 AWS IAM Identity Center 用户指南。

IAM 用户和组

IAM用户是你内部的身份 AWS 账户 对个人或应用程序具有特定权限。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的定期轮换需要长期凭证的用例的访问密钥。

IAM群组是指定IAM用户集合的身份。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组，IAMAdmins并授予该组管理IAM资源的权限。

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》中的何时创建IAM用户（而不是角色）。

IAM角色

IAM角色是你内在的身份 AWS 账户 具有特定权限的。它与IAM用户类似，但与特定人员无关。你可以暂时扮IAM演一个角色 AWS Management Console 通过切换角色。你可以通过调用来扮演角色 AWS CLI 或者 AWS API操作或使用自定义URL。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。

IAM具有临时证书的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。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅中的权限集 AWS IAM Identity Center 用户指南。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，有些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 一些 AWS 服务 使用其他功能 AWS 服务。 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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。
- 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。
- 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。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色来管理在EC2实例上运行并制作的应用程序的临时证书 AWS CLI 或者 AWS API请求。这比在EC2实例中存储访问密钥更可取。要分配 AWS 在EC2实例中扮演角色并使其可供其所有应用程序使用，则可以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 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用IAM角色还是使用IAM用户，请参阅《用户指南》中的何时创建IAM角色（而不是IAM用户）。

使用策略管理访问

您可以控制访问权限 AWS 通过创建策略并将其附加到 AWS 身份或资源。策略是中的一个对象 AWS 当与身份或资源关联时，它定义了他们的权限。 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。大多数策略存储在 AWS 作为JSON文件。有关JSON策略文档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用于指定谁有权访问什么的策略。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。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。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中获取角色信息 AWS Management Console，AWS CLI，或者 AWS API.

基于身份的策略

基于身份的策略是可以附加到身份（例如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。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到您的多个用户、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。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。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。你不能用 AWS 基于资源的策略IAM中的托管策略。

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。

亚马逊 S3， AWS WAF，Amazon VPC 就是支持的服务示例ACLs。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-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向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 是指定组织或组织单位 (OU) 的最大权限的JSON策略 AWS Organizations. AWS Organizations 是一项用于对多个进行分组和集中管理的服务 AWS 账户 你的企

业拥有的。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限制了成员账户中实体的权限，包括每个 AWS 账户根用户。 有关 Organization SCPs s 和的更多信息，请参阅中的服务控制策略 AWS Organizations 用户指南。

- 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。要了解如何 AWS 决定在涉及多种策略类型时是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

AWS控制目录的工作原理 IAM

在使用管理IAM对AWS控制目录的访问之前，请先了解哪些IAM功能可用于AWS控制目录。

IAM可以与 “AWS控制目录” 一起使用的功能

IAM功能	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	不支持
ABAC（策略中的标签）	否
临时凭证	是
主体权限	否

IAM功能	AWS控制目录支持
服务角色	否
服务相关角色	否

要全面了解如何AWS控制目录和其他 AWS 服务适用于大多数IAM功能，请参阅 AWS IAM在《IAM用户指南》中使用的服务。

控制目录的基于身份的AWS策略

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如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。

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。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

控制目录的基于身份的AWS策略示例

要查看基于身份的AWS控制目录策略的示例，请参阅。控制目录的基于身份的AWS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JSON策略是您附加到资源的策略文档。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另一个账户中的IAM实体指定为基于资源的策略中的委托人。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状态时 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》IAM中的跨账户资源访问权限。

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用于指定谁有权访问什么的策略。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Action元素描述了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同名 AWS API操作。也有一些例外，例如没有匹配API操作的仅限权限的操作。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 开头的所有操作，请包括以下操作。

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

要查看基于身份的AWS控制目录策略的示例，请参阅。控制目录的基于身份的AWS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用于指定谁有权访问什么的策略。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。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 Amazon 资源名称 (ARN) 来指定资源。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ARN种资源，请参阅AWS控制目录定义的操作。

AWS控制目录域名采用以下 Amazon 资源名称 (ARN) 格式：

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

AWS控制目录目标的ARN格式如下：

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

AWS控制目录常用控件的ARN格式如下：

```
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，请使用以下命令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"
```

要查看基于身份的AWS控制目录策略的示例，请参阅。控制目录的基于身份的AWS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用于指定谁有权访问什么的策略。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。

如果您在一条语句中指定多个Condition元素，或者在单个Condition元素中指定多个键， AWS 使用逻辑AND运算对其进行评估。如果您为单个条件键指定多个值， AWS 使用逻辑OR运算评估条件。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，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。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键。要查看全部 AWS 全局条件键，请参见 AWS 《IAM用户指南》中的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AWS控制目录的条件键。要了解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。

要查看基于身份的AWS控制目录策略的示例，请参阅。控制目录的基于身份的AWS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。

ABAC使用AWS控制目录

支持ABAC（策略中的标签）：否

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。In AWS，这些属性称为标签。您可以将标签附加到IAM实体（用户或角色）和许多实体 AWS 资源的费用。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

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。

有关的更多信息ABAC，请参阅什么是ABAC？ 在《IAM用户指南》中。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的使用基于属性的访问控制 (ABAC)。

在AWS控制目录中使用临时证书

支持临时凭证：是

一段时间 AWS 服务 使用临时凭证登录时不起作用。欲了解更多信息，包括哪个 AWS 服务 使用临时证书，请参阅 AWS 服务 可以IAM在《IAM用户指南》中使用。

如果您登录，则使用的是临时证书 AWS Management Console 使用除用户名和密码之外的任何方法。例如，当您访问时 AWS 使用贵公司的单点登录 (SSO) 链接，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》中的切换到角色（控制台）。

您可以使用手动创建临时证书 AWS CLI 或者 AWS API。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，请参阅中的临时安全证书IAM。

AWS控制目录的跨服务主体权限

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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，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IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。

> **Warning**
>
> 更改服务角色的权限可能会中断AWS控制目录的功能。只有当AWS控制目录提供相关指导时，才能编辑服务角色。

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与服务相关联的服务角色 AWS 服务。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。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 AWS 与之配合使用的服务IAM。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AWS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。他们也无法使用来执行任务 AWS Management Console, AWS Command Line Interface (AWS CLI)，或 AWS API。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的创建IAM策略。

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了某人是否可以在您的账户中创建、访问或删除AWS控制目录资源。这些操作可能会使您付出代价 AWS 账户。 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 AWS 为许多常见用例授予权限的托管策略。它们在你的 AWS 账户。 我们建议您通过定义来进一步减少权限 AWS 特定于您的用例的客户托管政策。有关更多信息，请参阅 AWS 托管策略或 AWS 《IAM用户指南》 中工作职能的托管策略。
- 应用最低权限权限-使用IAM策略设置权限时，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。有关使用应用权限IAM的更多信息，请参阅IAM用户指南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-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果通过特定条件使用服务操作，则也可以使用条件来授予对服务操作的访问权限 AWS 服务之外的压缩算法（例如 AWS CloudFormation。 有关更多信息，请参阅《IAM用户指南》中的IAMJSON策略元素：条件。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实

践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 IAMAccess Analyzer 策略验证。

- 需要多因素身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的配置MFA受保护的API访问权限。

有关中最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM中的安全最佳实践。

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括通过控制台或以编程方式使用控制台完成此操作的权限 AWS CLI 或者 AWS API.

```
{
    "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": "*"
        }
    ]
}
```

AWS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控制目录和时可能遇到的常见问题IAM。

主题

- 我无权在AWS控制目录中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人进入 AWS 账户 访问我的AWS控制目录资源

我无权在AWS控制目录中执行操作

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

当mateojacksonIAM用户尝试使用控制台查看虚构*my-example-widget*资源的详细信息但没有虚构权限时，就会出现以下示例错误。controlcatalog:*GetWidget*

```
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

如果您收到错误消息，提示您无权执行iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Cont AWS rol Catalog。

一段时间 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 Contro AWS l Catalog 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。

我想允许我以外的人进入 AWS 账户 访问我的AWS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，可以担任角色。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AWS控制目录的工作原理 IAM。
- 要了解如何提供对您的资源的访问权限 AWS 账户 您拥有的，请参阅向其他IAM用户提供访问权限 AWS 账户 您在《IAM用户指南》中拥有的。

- 了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅提供访问权限 AWS 账户IAM用户指南中归第三方所有。
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的向经过外部身份验证的用户提供访问权限（联合身份验证）。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。

AWS控制目录的合规性验证

要了解是否 AWS 服务 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 划分的范围” 中，选择您感兴趣的合规计划。有关一般信息，请参见 AWS 合规计划 。

您可以使用以下方式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 AWS Artifact.

您在使用时的合规责任 AWS 服务 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，并提供了在上部署基准环境的步骤 AWS 以安全性和合规性为重点。
- 在 Amazon Web Services 上进行HIPAA安全与合规架构设计 — 本白皮书描述了各公司如何使用 AWS 创建HIPAA符合条件的应用程序。

> **Note**
>
> 不是全部 AWS 服务 符合HIPAA资格。有关更多信息，请参阅《HIPAA合格服务参考》。

- AWS 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地。
- 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所 (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。
- 使用规则评估资源 AWS Config 开发者指南 — 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— 这个 AWS 服务 提供您的安全状态的全面视图 AWS。 Security Hub 使用安全控制来评估你的 AWS 资源，并检查您是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。

- 亚马逊 GuardDuty — 这个 AWS 服务 检测您面临的潜在威胁 AWS 账户、工作负载、容器和数据，监控您的环境中是否存在可疑和恶意活动。 GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- AWS Audit Manager— 这个 AWS 服务 帮助您持续审核您的 AWS 用于简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS 控制目录

这些区域有： AWS 全球基础设施是围绕着建立的 AWS 区域 和可用区。 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，请参阅 AWS 全球基础设施。

AWS控制目录中的基础设施安全

作为一项托管服务，AWS控制目录受以下内容的保护 AWS 《Amazon Web Services：安全流程概述》白皮书中描述的全球网络安全程序。

你用 AWS 已发布通过网络访问AWS控制目录的API呼叫。客户端必须支持传输层安全 (TLS) 1.0 或更高版本。我们建议使用 TLS 1.2 或更高版本。客户还必须支持具有完全向前保密性的密码套件 ()，例如（Ephemeral Diffie-HellmanPFS）或（Elliptic Cur DHE ve Ephemeral Diffie-Hellman）。ECDHE大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与IAM委托人关联的私有访问密钥对请求进行签名。或者你可以使用 AWS Security Token Service (AWS STS) 生成用于签署请求的临时安全证书。

中的配置和漏洞分析 AWS 控制目录

配置和 IT 控制由两者共同负责 AWS 还有你，我们的客户。有关更多信息，请参阅 AWS 分担责任模型。

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 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账户拨打了电话 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 AWS 控制目录 API 调用 AWS CloudTrail

AWS Control Catalog 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 AWS 控制目录中采取的操作的记录。 CloudTrail 将 AWS 控制目录的所有 API 调用捕获为事件。捕获的调用包括来自 AWS 控制目录控制台的调用和对 AWS 控制目录 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 AWS 控制目录的事件。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 AWS Control Control Catalog 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》。

AWS 控制目录信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当活动发生在 AWS Control Control Catalog 中时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。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，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的事件 AWS 账户，包括 AWS 控制目录中的事件，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：

- 创建跟踪记录概述
- 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 AWS 控制目录操作均由 AWS 控制目录 API 参考记录 CloudTrail 并记录在 AWS 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：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 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 用户身份元素。

了解 AWS 控制目录日志文件条目

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`ListDomains`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:"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 AWS 控制目录 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您的VPC和 AWS 控制目录之间创建私有连接。无需使用 Internet 网关、NAT设备VPC、连接或VPN AWS Direct Connect 连接，即可像访问 AWS 控制目录一样访问控制目录。您中的实例VPC不需要公有 IP 地址即可访问 AWS 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 AWS 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 直通访问。

AWS 控制目录的注意事项

在为 AWS 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。

AWS 控制目录支持通过接口端点调用其所有API操作。

为 AWS 控制目录创建接口端点

您可以使用 Amazon AWS 控制台或 AWS Command Line Interface (AWS CLI) 为VPC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 AWS 控制目录创建接口端点：

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

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

为 VPC 端点创建端点策略

终端节点策略是您可以附加到接口终端节点的IAM资源。默认端点策略允许通过接口端点对 AWS 控制目录进行完全访问权限。要控制允许您访问 AWS 控制目录的权限VPC，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：

- 可以执行操作的委托人（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： AWS 控制目录操作的VPC端点策略

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ListControlsAPI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。不支持其他 AWS Control Tower API操作 AWS PrivateLink。

AWS 控制目录安全信息指南的文档历史记录

下表描述了 AWS 控制目录的文档版本。

变更	说明	日期
初始版本	AWS 控制目录 API 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。