aws

安全信息

AWS 控制目录

AWS 控制目录: 安全信息

Table of Contents

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。它是一个合并的 AWS 控件目录。您无需进行设置 AWS Control Tower 即可使用控制目录。

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 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 CSPM 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。

对控制目录的访问权限

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。要了解适用于 Control Catalog 的合规性计划，请参阅按合规计划划分的范围AWS 服务 内的AWS 服务划分）。
- 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 Control Catalog; 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

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》https://aws.amazon.com/compliance/fips/。

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 URL，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 Cont AWS rol Catalog 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

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅控制目录身份和访问权限疑难解答）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅控制目录如何与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（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 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center （例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，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，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，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 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。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。

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。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。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。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。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。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。您必须在基于资源的策略中指定主体。

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。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，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)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在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。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 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	否
ABAC（策略中的标签）	否
临时凭证	是
主体权限	否
服务角色	否
服务关联角色	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。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。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。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 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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，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。

Condition 元素根据定义的条件指定语句何时执行。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。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

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

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

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。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 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

AWS 控制目录的跨服务委托人权限

支持转发访问会话（FAS）：否

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。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关联角色的权限。

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。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。

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

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 托管策略或工作职能的AWS 托管策略。
- 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 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 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。

JSON

```
{
"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。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

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 提供多个物理分隔和隔离的可用区，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、容错能力和可扩展性。

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 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。

使用日志控制目录 API 调用 AWS CloudTrail

作为 AWS Control Tower 控制目录的一部分 AWS CloudTrail，与一项服务集成，该服务提供用户、角色或 AWS 服务所执行操作的记录。 CloudTrail 将控制目录的所有 API 调用捕获为事件。捕获的调用包括直接来自 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，则可以将 CloudTrail 事件持续传输到 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 Control Catalog 发出的请求（通过 AWS Control Tower）、发出请求的 IP 地址、谁发出了请求、何时发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。

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。当活动发生在控制目录中时，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，包括控制目录的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，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

- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 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 userIdentity 元素。

了解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 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

下表描述了控制目录的文档版本。

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。