管理员指南

# Amazon Nimble Studio

# Amazon Nimble Studio: 管理员指南

# Table of Contents

# 什么是 Amazon Nimble Studio？

Nimble Studio 为一套应用程序和服务提供基础设施和集中化管理，艺术家可以使用这些应用程序和服务在云端制作视觉效果、动画和游戏内容。

借助 Nimble Studio，您可以获得用户和群组管理使用的必备工具。您还可以添加和管理应用程序，包括 AWS Thinkbox 和 Nimble Studio 文件传输功能。

Nimble Studio 拥有统一的界面，可将所有工作室资源集中在一个地方。您可以加入用户、分配应用程序以及为其工作职能附加特定权限。Nimble Studio 不要求拥有任何 AWS 经验，您可以在大约五分钟内完成设置。

目录



## 特征和优点

以下是您使用 Nimble Studio 时可以获得的一些特征和优点：

- 免费使用 Nimble Studio；只需为应用程序使用的工作室资源付费。
- 集中化管理工作室，检查工作室状态并获取对其操作的高级见解。
- 添加和管理 Nimble Studio 应用程序、用户和群组，并附加权限。
- 使用 AWS Identity and Access Management (IAM) 策略和角色安全地管理访问工作室资源的权限。
- 使用 AWS IAM Identity Center (IAM Identity Center) 管理工作室用户和外部身份提供商的安全登录。
- 使用工作室资源的标签整理和轻松查找工作室资源。

## 相关应用程序

Nimble Studio 为数字内容创作者提供应用程序，用于操作制作视觉效果 (VFX)、动画和交互式内容的基于云的工作室。

您可以使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例将这些应用程序安装到您的本地计算机或云端。您也可以使用 Amazon Simple Storage Service (Amazon S3) 安全地传输和存储数字媒体资产。这表示您可以使用 Nimble Studio 来降低物理基础设施、设备和技术员工的成本。

Nimble Studio 目前提供以下应用程序：

- AWS Thinkbox：Thinkbox 软件包括渲染农场管理器 Thinkbox Deadline 和 3D 插件 Thinkbox Krakatoa。您可以使用 Thinkbox 软件来提高本地、使用 Amazon EC2 的云端或两者组合的工作室创意产出。有关更多信息，请参阅 AWS Thinkbox 产品。
- Nimble Studio File Transfer：File Transfer 会增加 Amazon S3 的媒体资产传输速度。File Transfer 提供了一个图形用户界面，使用此界面您可以快速移动成千上万的大型媒体文件。有关更多信息，请参阅什么是 Nimble Studio File Transfer？页面。

# Nimble Studio 定价

您可以免费设置 Nimble Studio 并用它来管理您的工作室基础设施、用户、安全和服务。

但是，如果您在工作室中设置服务和应用程序，则可能需要为存储和其他工作室资源付费。有关 Nimble Studio 应用程序定价的更多信息，请参阅各个应用程序的定价页面。

有关管理 AWS 成本的信息，请参阅 AWS Cost Explorer Service 和 AWS Budgets。

# 开始使用 Nimble Studio

Nimble Studio 大约需要五分钟的设置和部署时间。

熟悉 Nimble Studio 概念和术语后，请参阅开始使用 Amazon Nimble Studio。其中有关于如何部署工作室的逐步指示。

# Amazon Nimble Studio 的概念和术语

为了帮助您开始使用 Amazon Nimble Studio 并了解其工作原理，您可以参考本指南中的关键概念和术语。

## 主要特征

Amazon Nimble Studio

Amazon Nimble Studio 是一项 AWS 服务，允许创意工作室完全在云中制作从故事情节到最终交付内容的视觉效果、动画和交互内容。

Amazon Nimble Studio 控制台

Nimble Studio 控制台是 AWS Management Console 中我们管理员 IT 客户专用的一部分。管理员可以在此控制台上创建自己的云工作室并管理许多设置。例如，工作室管理器页面允许您添加或删除资源、添加应用程序以及向用户和群组授予权限。

Amazon Nimble Studio 门户网站

Nimble Studio 门户网站提供了一个与 Nimble Studio 应用程序和服务进行日常交互的用户界面。用户使用其用户名和密码直接登录门户，无需与 AWS Management Console 进行交互。

Nimble Studio File Transfer

File Transfer 会增加 Amazon Simple Storage Service (Amazon S3) 的数字媒体资产的传输速度。File Transfer 提供了一个图形用户界面，您可以使用此界面快速移动成千上万的大型媒体文件。有关更多信息，请参阅什么是 Nimble Studio File Transfer？页面。

AWS Thinkbox

Thinkbox 软件包括渲染农场管理器 Thinkbox Deadline 和 3D 插件 Thinkbox Krakatoa。您可以使用 Thinkbox 软件来提高本地、使用 Amazon EC2 的云端或两者组合的工作室创意产出。有关更多信息，请参阅 AWS Thinkbox 产品。

## 关键概念和术语

AWS 托管策略

AWS 托管策略是由 AWS 创建和管理的独立策略。独立策略意味着策略有自身的 Amazon 资源名称 (ARN)，其中包含策略名称。例如，arn:aws:iam::aws:policy/IAMReadOnlyAccess 是一个 AWS 托管策略。有关 ARN 的更多信息，请参阅 IAM ARN。

AWS 托管策略可用于授予对常见工作职能的权限。在推出新的服务和 API 操作时，AWS 会对工作职能策略进行维护和更新。例如，AdministratorAccess 工作职能提供对 AWS 中的每个服务和资源的完全访问权限和权限委派。而 AmazonMobileAnalyticsWriteOnlyAccess 和 AmazonEC2ReadOnlyAccess 等部分访问的 AWS 托管策略可以在不允许完全访问的情况下提供对 AWS 服务 的特定级别访问权限。要了解访问策略的更多信息，请参阅了解策略摘要内的访问级别摘要。

AWS Management Console

AWS Management Console 是一款 Web 应用程序，其提供了多种用于管理 AWS 服务 的服务控制台的权限。

各项服务还包括其自身的控制台。这些控制台提供了多种云计算工具。甚至还有一项有助于管理账单和成本的服务。

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center 是一项 AWS 服务，可让您轻松地集中管理多个 AWS 账户和业务应用程序的访问权限。使用 IAM Identity Center，您可以为用户提供从一个位置，访问其所有分配账户和应用程序的单点登录权限。您还可以集中管理 AWS Organizations 中所有账户的多账户访问权限和用户权限。有关更多信息，请访问 AWS IAM Identity Center FAQ。

AWSPrivateLink

AWS PrivateLink 在 VPC、AWS 服务 和您的本地网络之间提供私有连接，而不会将您的流量暴露给公共网络。AWS PrivateLink 可以轻松地跨不同账户和 VPC 连接服务。AWS PrivateLink 按月收费，由您的 AWS 账户 支付。

数字内容创作 (DCC)

数字内容创作 (DCC) 是指用于制作创意内容的应用程序类别，包括 Blender、Nuke、Maya 和 Houdini。

区域

Nimble Studio 提供了 11 种部署工作室的可选 AWS 区域。区域是存在基本工作室基础设施（例如您的数据和应用程序）的地方。

该区域的位置应离您的工作室最近。这样可以减少滞后并提高数据传输速度。

Studio

工作室是其他 Nimble Studio 相关资源的顶级容器。云工作室可以管理 Nimble Studio Web 门户以及与 AWS 账户 中基本资源的连接，例如 VPC、用户目录和存储加密密钥。

Studio 应用程序

工作室组件是客户 Nimble Studio 中的配置，该组件会告诉服务如何访问 AWS 账户 中的文件系统、许可证服务器和渲染农场等资源。

Nimble Studio 包含工作室组件的许多子类型，其中包括共享文件系统、计算场、Active Directory 和许可组件。这些子类型描述了您希望工作室使用的资源。

工作室资源

工作室资源是一个术语，其概括了工作室在日常操作中需要的资源。在描述资源如何应用于云工作室的基础设施时，它们也可能被称为工作室组件。

标签

标签是为 AWS 资源分配的标记。每个标签都包含您所定义的一个键和可选值。

标签可让您按不同方式对 AWS 资源进行分类。例如，您可以为账户中的 Amazon Elastic Compute Cloud (Amazon EC2) 实例定义一组标签，以跟踪每个实例的所有者和堆栈级别。标签还能允许您将贵组织的共享文件系统和渲染农场与 Nimble Studio 集成，从而在将工作人员转移到云端的同时保持工作流程不间断。

借助标签，您可以按用途、所有者或环境对 AWS 资源进行分类。这在您具有相同类型的很多资源时会很有用—您可以根据分配给特定资源的标签快速识别该资源。

# 设置 Nimble Studio

本教程适用于想要设置 Amazon Nimble Studio 的管理员用户。

以下各节将指导您完成在 Nimble Studio 中部署工作室之前需要完成的步骤。

内容



# 设置 IAM

开始之前，请查看以下 AWS Identity and Access Management (IAM) 文档。

- IAM 安全最佳实操
- 以管理员用户 AWS 账户 身份登录以完成剩余的设置。

## 注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 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。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。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，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后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。

# 创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。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. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

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《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 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。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

# 相关资源

- IAM 安全最佳实践
- AWS 服务 配额- AWS 一般参考

# 开始使用 Amazon Nimble Studio

本章介绍如何使用 Nimble Studio 控制台创建工作室的基础设施、确认 AWS 区域、查看设置以及创建工作室。您还可以使用其他设置来自定义您的设置。

对于首次使用的 AWS 客户，请参阅 设置 Nimble Studio 教程。

主题



# 设置 Nimble Studio

本指南说明如何配置基础设施、查看设置和创建工作室。您也可以使用 其他工作室设置 自定义工作室。

## 步骤 1：配置工作室基础设施

您的工作室基础设施包括以下组件：

- 工作室显示名称：工作室显示名称用于识别工作室 - 例如 AnyCompany Studio。工作室的名称还决定了您的工作室门户 URL。完成设置后，您可以随时更改工作室显示名称。
- 工作室门户 URL：您可以使用工作室门户 URL 访问您的工作室。URL 基于工作室显示名称 - 例如 https://anycompanystudio.awsapps.com。完成设置后，您可以随时更改工作室门户 URL。
- AWS 区域：AWS 区域 是 AWS 数据中心收集数据的物理位置。当您设置工作室时，该区域默认为离您最近的位置。您应该更改此区域，使其位于离您的用户最近的位置。这样可以减少滞后并提高数据传输速度。

> **Important**
>
> 设置完 Nimble Studio 后，您无法更改自己的区域。

完整本章节所述任务，以便配置您的工作室基础设施。

配置工作室基础设施

1. 登录 AWS Management Console 并打开 Nimble Studio 控制台。
2. 选择设置 Nimble Studio，然后选择下一步。
3. 输入工作室显示名称 — 例如 **AnyCompany Studio**。
4. （可选）要更改工作室门户名称，请选择编辑 URL。
5. （可选）要更改 AWS 区域 使其离您的工作室用户最近，请选择更改区域。
   a. 选择离您的大多数用户最近的区域。
   b. 选择应用区域。
6. （可选）要进一步自定义工作室设置，请选择 其他工作室设置。
7. 要在创建工作室之前查看设置，请选择下一步。

## 步骤 2：查看并创建工作室

配置工作室基础设施后，您可以查看、更改和创建工作室。

查看和创建工作室

1. 在查看并创建页面上，查看工作室基础设施。
2. 确认 AWS 区域 离您的工作室用户最近。
3. （可选）选择编辑以更改工作室设置。
4. 当您准备好后，选择创建工作室。

# 其他工作室设置

Nimble Studio 设置包括其他工作室设置。使用这些设置，您可以查看 Nimble Studio 设置功能对 AWS 账户 所做的更改、配置工作室用户角色和更改加密密钥类型。您还可以为工作室资源添加可选标签。

## 配置工作室用户角色

AWS 服务是一个代入以代表您执行操作的服务角色。Nimble Studio 需要工作室用户角色，才能允许用户访问工作室中的资源。

您可以将 AWS Identity and Access Management (IAM) 托管策略附加到工作室用户角色。这些策略允许用户执行某些操作，例如在特定的 Nimble Studio 应用程序中创建作业。由于此应用程序依赖于托管策略中的特定条件，所以如果您不使用托管策略，则此应用程序可能无法按预期运行。

完成设置后，您可以随时更改工作室用户角色。有关用户角色的更多信息，请参阅 IAM 角色。

以下选项卡包含两种不同用例的说明。要创建和使用新的服务角色，请选择新服务角色选项卡。要使用现有的服务角色，请选择现有服务角色选项卡。

New service role

创建和使用新的服务角色

1. 选择创建和使用新服务角色
2. （可选）输入服务用户角色名称。
3. 选择查看权限详细信息以了解有关该角色的更多信息。

Existing service role

使用现有服务角色

1. 选择使用现有服务角色。
2. 打开下拉列表，选择一个现有服务角色。
3. （可选）选择在 IAM 控制台中查看以了解有关该角色的更多信息。

## AWS IAM Identity Center

AWS IAM Identity Center 是一项基于云的单点登录服务，用于管理用户和群组。IAM Identity Center 还可以与企业单点登录（SSO）提供商集成，以便用户能够使用其公司账户登录。

默认情况下，Nimble Studio 会启用 IAM Identity Center，IAM Identity Center 需要设置和使用 Nimble Studio。有关更多信息，请参阅什么是 AWS IAM Identity Center。

## 配置 AWS KMS 加密密钥

AWS Key Management Service(AWS KMS) 密钥是 KMS 密钥的主要类型，可用于加密、解密和重新加密数据。

Nimble Studio 包括以下 AWS KMS 加密密钥类型：

- AWS 拥有的密钥：AWS 拥有的密钥都 KMS 密钥，此类密钥由 AWS 服务 拥有并对其在多个 AWS 账户 中的使用进行管理。 AWS 拥有的密钥不在您的 AWS 账户 中，但是 Nimble Studio 可以使用 AWS 拥有的密钥来保护您账户中的资源。

要使用 AWS KMS，您就不必创建或维护该密钥或其密钥策略。使用 AWS 拥有的密钥不收取任何费用，其费用也不会计入您 AWS 账户 的配额 AWS KMS 中。

- 客户托管 AWS KMS 密钥：客户托管密钥是一个您在 AWS 账户 中创建、拥有和管理的 KMS 密钥。

  您拥有 KMS 密钥的完全控制权。客户托管密钥会产生月费。他们还会为向 AWS KMS 发出的超出免费套餐的每个 API 请求收取费用。有关 AWS KMS 定价的更多信息，请参阅 AWS Key Management Service 定价。

完成设置后，无法更改加密密钥类型。有关 AWS KMS 和加密密钥类型的更多信息，请参阅 AWS KMS 文档。

选择其他加密密钥类型

1. 选择选择其他 AWS KMS 密钥（高级）。
2. 选择 AWS KMS 密钥或输入 Amazon 资源编号 (ARN)。
3. 选择创建 AWS KMS 密钥。

## 配置标签

此标签充当组织 Nimble Studio 资源使用的标签。您可以添加 50 个标签，用于识别、管理、筛选和搜索资源。

每个标签包含由您定义的两个部分：一个标签键和一个可选标签值 - 例如，键：`domain` 和值：`anycompanystudio.com`。

完成设置后，您可以随时添加或删除标签。有关标记的更多信息，请参阅标记您的 AWS 资源。

为工作室资源添加标签

1. 选择添加新标签。
2. 输入标签键。
3. （可选）输入标签值。

# 删除工作室

如果您不再需要某一工作室，则可将其删除。删除工作室时，只会删除工作室基础设施。您的其他 AWS 资源（例如用户角色、策略和应用程序数据）保持不变。

> **Important**
>
> 您无法在删除后恢复它。

删除您的工作室

1. 登录 AWS Management Console 并打开 Nimble Studio 控制台。
2. 选择工作室概述。
3. 选择操作，然后选择删除工作室。
4. 输入 **`delete`**，然后选择删除。

# Amazon Nimble Studio 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 负责保护在云中运行 AWS 服务的基础架构 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 Amazon Nimble Studio 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 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。

> **Important**
>
> 强烈建议你阅读并熟悉安全支柱——Well-Architected Framewor AWS k。本文包含保护 AWS 基础架构的关键原则。

此文档将帮助您了解如何在使用 Nimble Studio 时应用责任共担模型。以下主题说明如何配置 Nimble Studio 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 Nimble Studio资源。

## 更多信息

- 安全支柱——Well-Arch AWS itected 框架
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) 的安全性
- Amazon Virtual Private Cloud 中的安全性
- AWS 安全凭证
- Amazon EC2 中的安全性
  - Linux
  - Windows

# 设置 AWS 账户 安全性

本指南介绍如何将您的设置 AWS 账户 为在资源受损时接收通知，以及如何允许特定 AWS 账户 用户访问通知。要保护您的资源 AWS 账户 并跟踪您的资源，请完成以下步骤。

内容



## 删除账户的访问密钥

您可以允许通过 AWS Command Line Interface (AWS CLI) 或 AWS API 以编程方式访问您的 AWS 资源。但是， AWS 建议您不要创建或使用与根账户关联的访问密钥进行编程访问。

如果您还有访问密钥，建议您删除这些密钥并创建一个用户。然后，仅向该用户授予您计划调用的 API 需要的权限。您可以使用此用户来颁发访问密钥。

有关更多信息，请参阅《AWS 一般参考 指南》中的管理 AWS 账户的访问密钥。

## 启用多重身份验证

多重身份验证 (MFA) 是一项安全功能，除用户名和密码外，此功能还可以提供一层身份验证保护。

MFA 的工作方式如下所示：使用用户名和密码登录后，您还必须提供只有您才能实际访问的一条额外信息。此信息可能来自一台专用 MFA 硬件设备，也可以来自手机上的应用程序。

您必须从支持的 MFA 设备列表中选择要使用的 MFA 设备类型。对于硬件设备，请将 MFA 设备保存到安全的地方。

如果您使用虚拟 MFA 设备（例如手机应用程序），请考虑如果您的手机丢失或损坏会发生什么。其中可选择的一种方法是将您使用的虚拟 MFA 设备保存在安全的地方。另一个选择是同时激活多台设备，或者使用虚拟 MFA 选项恢复设备密钥。

要了解有关 MFA 的更多信息，请参阅启用虚拟多重身份验证 (MFA) 设备。

### 相关资源

- 开始使用多重身份验证

- AWS 使用 MFA 保护访问权限

## 全部启用 CloudTrail AWS 区域

您可以使用跟踪 AWS 资源中的所有活动AWS CloudTrail。我们建议你 CloudTrail 立即开启。这可以帮助 AWS Support 您的 AWS 解决方案架构师稍后解决安全或配置问题。

要启用全部 CloudTrail 登录 AWS 区域，请参阅AWS CloudTrail 更新-在所有区域开启和使用多条路径。

要了解更多信息 CloudTrail，请参阅开启 CloudTrail：在你的 API 活动中记录 API 活动 AWS 账户。要了解如何 CloudTrail监控 Nimble Studio，请参阅使用记录 Nimble Studio 通话 AWS CloudTrail。

## 设置 Amazon GuardDuty 和通知

Amazon GuardDuty 是一项持续的安全监控服务，可分析和处理以下内容：

- 数据源
- Amazon VPC 流日志
- AWS CloudTrail 管理事件日志
- CloudTrail S3 数据事件日志
- DNS 日志

Amazon 会在您的 AWS 环境中 GuardDuty 识别出意外的、可能未经授权的恶意活动。恶意活动包括特权升级、使用遭暴露的凭证或者与恶意 IP 地址或域通信等问题。要识别这些活动，请 GuardDuty 使用威胁情报源，例如恶意 IP 地址和域名列表以及机器学习。例如， GuardDuty 可以检测提供恶意软件或挖矿比特币的已入侵的 Amazon EC2 实例。

GuardDuty 还会监控 AWS 账户 访问行为是否存在泄露迹象。这包括未经授权的基础设施部署，例如在从未使用过 AWS 区域 的中部署的实例。它还包括异常 API 调用，例如更改密码策略以降低密码强度。

GuardDuty 通过生成安全调查结果来告知您 AWS 环境的状态。您可以在 GuardDuty 控制台或通过 Amazon CloudWatch 事件查看这些发现。

### 设置 Amazon SNS 主题和端点

遵照设置 Amazon SNS 主题和端点教程中的说明。

## 为 GuardDuty 调查结果设置 EventBridge 活动

为创建规则 EventBridge ，为 GuardDuty 生成的所有发现发送事件。

为 GuardDuty 调查结果创建 EventBridge 事件

1. 登录亚马逊 EventBridge 控制台：https://console.aws.amazon.com/events/
2. 在导航窗格中，选择规则。然后，选择创建规则。
3. 为新规则输入名称和描述。然后选择下一步。
4. 将AWS 事件源选为事件或 EventBridge 合作伙伴事件。
5. 在事件模式中，为事件源选择 AWS 服务。然后GuardDuty是AWS 服务，然后是GuardDuty 查找事件类型。这是您在 设置 Amazon SNS 主题和端点 中创建的主题。
6. 选择下一步。
7. 对于目标 1，选择 AWS 服务。在选择目标下拉列表中选择 SNS 主题。然后选择你的 GuardDuty_to_email 主题。
8. 在其他设置部分：使用配置目标输入下拉列表，选择输入转换器。选择配置输入转换器。
9. 在目标输入转换器部分的输入路径字段中输入以下代码。

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. 要格式化电子邮件，请在模板字段中输入以下代码。

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. 选择创建。然后选择下一步。
12. （可选）如果您使用标签来跟踪 AWS 资源，请添加标签。

13. 选择下一步。
14. 检查您的规则。然后，选择创建规则。

现在，您已经设置了 AWS 账户 安全性，可以向特定用户授予访问权限，并在资源受到威胁时收到通知。

# Amazon Nimble Studio 中的数据保护

分 AWS 担责任模型适用于中的数据保护Amazon Nimble Studio。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。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）。这包括您使用Nimble Studio或 AWS 服务 使用控制台 AWS CLI、API 或 AWS SDK 时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，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。

分 AWS 担责任模式适用于亚马逊 Nimble Studio 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设施上的内容的控制。此内容包括您 AWS 服务 使用的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。有关欧盟数据保护的更多信息，请访问一般数据保护条例 (GDPR) 中心。

## 静态加密

Nimble Studio 使用 AWS Key Management Service (AWS KMS) 中存储的加密密钥对敏感工作室数据进行静态加密。所有可用 Nimble Studio AWS 区域 的地方都可以使用静态加密。加密的工作室数据包括所有资源类型的名称和描述，以及工作室组件脚本、脚本参数、挂载点、共享名称和其他数据。

加密数据表示任何无有效密钥的用户或应用程序都无法读取保存在磁盘上的敏感数据。加密数据可以安全地静态存储，并且只能由有托管密钥访问权一方解密。

有关 Nimble Studio 如何使用 AWS KMS 加密静态数据的信息，请参阅。Amazon Nimble Studio 的密钥管理

### 使用带有 AWS KMS 密钥的授权

赠款是一种政策工具，允许AWS 委托人在加密操作中使用 AWS KMS 密钥。它还可以允许其使用命令 `DescribeKey` 查看 KMS 密钥，以及创建和管理授权。

与集成的 Gran AWS 服务 ts 通常使用赠款 AWS KMS 来加密您的静态数据。该服务代表账户中的用户创建授权，使用其权限，并在其任务完成后立即停用授权。

Nimble Studio 创建工作室时，会为 Nimble Studio 门户网站用户提供两个角色：用户角色和管理员角色。Nimble Studio 为这些角色创建客户托管密钥的授权，为其提供访问工作室加密数据的权限。

> **Important**
>
> 如果您删除授权，则在管理员创建新授权之前，用户将无法使用 Nimble Studio 门户网站。

有关如何 AWS 服务 使用授权的详细信息，请参阅服务用户指南AWS KMS 或开发者指南中的如何 AWS 服务 使用或静态加密主题。

## 传输中加密

下表提供了有关如何加密传输中数据的信息。若适用，还列出了其他适用于 Nimble Studio 的数据保护方法。

| 数据 | 网络路径 | 保护 |
| --- | --- | --- |

| | | |
|---|---|---|
| Web 资产，例如图像和 JavaScript 文件 | 网络路径是 Nimble Studio 用户和 Nimble Studio 之间路径。 | 数据加密使用 TLS 1.2 或更高版本。 |
| 像素和相关的流式传输流量 | 网络路径是 Nimble Studio 用户和 Nimble Studio 之间路径。 | 使用 256 位高级加密标准 (AES-256) 加密，使用 TLS 1.2 或更高版本进行传输。 |
| API 流量 | 这条路径是 Nimble Studio 用户和 Nimble Studio 之间的路径。 | 使用 TLS 1.2 或更高版本加密。创建连接的请求使用 SigV4 签名。 |

# Amazon Nimble Studio 的密钥管理

创建新工作室时，可以选择以下密钥来加密工作室数据：

- AWS 拥有的 KMS 密钥-默认加密类型。此密钥归 Nimble Studio 拥有（不另外收费）。
- 客户管理的 KMS 密钥：此密钥存储在您的账户中，由您创建、拥有和管理。你可以完全控制钥匙。AWS KMS 需收费。

删除 AWS Key Management Service (AWS KMS) 中客户管理的 KMS 密钥具有破坏性，并且具有潜在的危险。这将删除密钥材料以及与此密钥关联的所有元数据，并且不可撤销。删除客户托管 KMS 密钥后，您不能再解密用该此密钥加密的数据。这表示无法恢复此数据。

这就是为什么客户 AWS KMS 在删除密钥之前有长达 30 天的等待期。默认的等待期限为 30 天。

## 关于等待期限

因为删除客户托管 KMS 密钥具有破坏性且存在潜在危险，所以要求您将等待期限设置为 7-30 天。默认的等待期限为 30 天。

但是，实际等待期限可能最多比您计划的时间长 24 小时。要获取删除密钥的实际日期和时间，请使用DescribeKey操作。您还可以在 AWS KMS 控制台中的密钥详细信息页面的常规配置部分中参阅密钥计划删除日期。注意时区。

在等待期限内，客户托管密钥状态和密钥状态为等待删除。

- 待删除的客户托管 KMS 密钥不能用于任何加密操作。

- AWS KMS 不会轮换待删除的客户托管 AWS KMS 密钥的备用密钥。

有关删除客户托管 AWS KMS 密钥的更多信息，请参阅删除客户主密钥。

## 数据安全措施

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置个人账户。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 建议使用 TLS 1.2 或更高版本。
- 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。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将敏感的可识别信息（例如客户的账号）放入自由格式字段（例如名称字段）。这包括当你 AWS 服务 使用控制台、API 或软件开发工具包与 Amazon Nimble Stu AWS dio 或其他人合作时。 AWS CLI您输入到 Amazon Nimble Studio 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

## 诊断数据和指标

在部署和删除期间 StudioBuilder，Amazon Nimble Studio 会收集某些指标，我们使用这些指标来诊断问题并改进 Nimble Studio 的功能和用户体验。

### 收集指标的类型

- 使用方法信息：运行的通用命令和子命令。
- 错误和诊断信息：运行命令的状态和持续时间，包括退出代码、内部异常名称和故障。
- 系统和环境信息-Python 版本WindowsLinux、操作系统（、或macOS）以及运行环境。StudioBuilder

# 适用于 Amazon Nimble Studio 的 Identity and Access Management

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（具有权限）来使用 Amazon Nimble Studio 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题



## 受众

你的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于你在 Nimble Studio 中所做的工作。

服务用户：如果您使用 Nimble Studio 服务来完成作业，您就是服务用户。在这种情况下，您的管理员会为您提供访问分配资源时需要的凭证和权限。当您使用更多 Nimble Studio 特征来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Nimble Studio 中的特征，请参阅 Amazon Nimble Studio 身份和访问问题排查。

服务管理员：如果您在公司负责管理 Nimble Studio 资源，则您可能具有 Nimble Studio 的完全访问权限。您有责任确定您的员工应访问哪些 Nimble Studio 特征和资源。然后向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。要了解有关贵公司如何将 IAM 与 Nimble Studio 搭配使用的更多信息，请参阅 Amazon Nimble Studio 如何与 IAM 协同工作。

## 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。有关使用登录的更多信息 AWS Management Console，请参阅 IAM 用户指南中的以 IAM 用户或根用户身份登录。 AWS Management Console

您需要以 AWS 账户 根用户、用户身份或通过担任 IAM 角色进行身份验证（登录 AWS）。您还可以使用贵公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。当你 AWS 使用另一家公司的凭证进行访问时，你是在间接担任角色。

要直接登录到 AWS Management Console，请将密码与根用户电子邮件地址或用户名一起使用。您可以使用根用户或用户访问密钥以编程方式访问 AWS 。

AWS 提供 SDK 和命令行工具，可使用您的凭证对请求进行加密签名。如果您不使用 AWS 工具，请自己签署请求。使用签名版本 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅 AWS 一般参考 中的签名版本 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。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《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

首次创建时 AWS 账户，您首先需要一个单一登录身份，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。我们强烈建议您不要使用根用户来执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

## 用户和组

用户是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。用户可以拥有长期凭证或一组访问密钥。要了解如何生成访问密钥，请参阅《IAM 用户指南》中的管理 IAM 用户的访问密钥。为用户生成访问密钥时，请查看并安全保存密钥对。您以后无法找回秘密访问密钥。而是必须生成新的访问密钥对。

IAM 组是指定一个用户集合的身份。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。它类似于用户，但未与特定人员关联。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：

- 临时用户权限：用户可代入 IAM 角色，暂时获得针对特定任务的不同权限。
- 联合用户访问权限-您可以使用来自 AWS Directory Service企业用户目录或 Web 身份提供商的现有身份，而不是创建用户。这些用户称为联合用户。在通过身份提供者请求访问权限时， AWS 将为联合用户分配角色。有关联合身份用户的更多信息，请参阅《IAM 用户指南》中的联合身份用户和角色。
  - 成员资格：Nimble Studio 使用一个名为 '成员资格' 的概念来为用户提供访问特定启动配置文件的权限。成员资格允许工作室管理员将资源访问权限委托给用户，而无需写入或理解 IAM 策略。Nimble Studio 管理员在启动配置文件中为用户创建成员资格时，该用户有权执行使用启动配置文件所需的 IAM 操作，例如查看其属性和使用该启动配置文件启动流会话。
  - 服务角色：服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。服务角色只在您的账户内提供访问权限，不能用于为访问其它账户中的服务授权。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。Nimble Studio 不支持服务相关角色。
- 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 IAM 身份或 AWS 资源来控制访问权限。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。您可以通过根用户或用户身份登录，也可以代入 IAM 角色。然后，当您提出请求时， AWS 会评估相关的基于身份或基于资源的策略。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。

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，预设情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

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 policy。

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 Simple Storage Service（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。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。

## Nimble Studio 中的访问控制列表 (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）概览。

### 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（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的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 是指定 Organizations 中的组织或组织单位 (OU) 的最大权限的 JSON 策略。Organizations 是一个服务，用于对您的企业拥有的多个 AWS 账户 进行分组和集中管理。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个 AWS 账户 root 用户。有关 Organizations 和 SCP 的更多信息，请参阅《 AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

### 多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解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。

## Amazon Nimble Studio 如何与 IAM 协同工作

在使用 IAM 管理对 Nimble Studio 的访问之前，您应该了解哪些 IAM 特征可用于 Nimble Studio。

可与 Amazon Nimble Studio 一起使用的 IAM 特征

| IAM 功能 | Nimble Studio 支持 |
| --- | --- |
| Nimble Studio 的策略操作 | 支持 |
| Nimble Studio 的策略资源 | 是 |
| Amazon Nimble Studio 的策略条件密钥 | 是 |

| IAM 功能 | Nimble Studio 支持 |
| --- | --- |
| Nimble Studio 中的访问控制列表 (ACL) | 否 |
| 使用 Nimble Studio 的基于属性的访问控制 (ABAC) | 是 |
| 将临时凭证用于 Nimble Studio | 是 |
| Nimble Studio 的跨服务主体权限 | 是 |
| Nimble Studio 的服务角色 | 是 |
| Nimble Studio 的服务相关角色 | 不支持 |

要全面了解 Nimble Studio 和其他 AWS 服务 功能如何与大多数 IAM 功能配合使用 AWS 服务 ，请参阅 IAM 用户指南中的如何与 I AM 配合使用。

## 适用于 Nimble Studio 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 policy。

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。

适用于 Amazon Nimble Studio 的基于身份的策略示例

要查看 Nimble Studio 基于身份的策略的示例，请参阅 适用于 Amazon Nimble Studio 的基于身份的策略示例。

## Nimble Studio 内基于资源的策略

| 支持基于资源的策略 | 否 |
| --- | --- |

Nimble Studio 不支持基于资源的策略或跨账户存取。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 Simple Storage Service（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。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。

## Nimble Studio 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。

如查看 Nimble Studio 操作的列表，请参阅《服务授权参考》中 Amazon Nimble Studio 定义的操作。

Nimble Studio 中的策略操作在操作前使用以下前缀：

```
nimble
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

要查看 Nimble Studio 基于身份的策略的示例，请参阅 适用于 Amazon Nimble Studio 的基于身份的策略示例。

## Nimble Studio 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 Nimble Studio 基于身份的策略的示例，请参阅 适用于 Amazon Nimble Studio 的基于身份的策略示例。

## Amazon Nimble Studio 的策略条件密钥

| | |
|---|---|
| 支持策略条件密钥 | 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（或 Condition`**block**）lets you specify conditions in which a statement is in effect. The `Condition 元素）是可选项。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 AWS 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。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 policy 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 全局条件上下文键。

要查看 Nimble Studio 基于身份的策略的示例，请参阅 适用于 Amazon Nimble Studio 的基于身份的策略示例。

## Nimble Studio 中的访问控制列表 (ACL)

| | |
|---|---|
| 支持 ACL | 否 |

Nimble Studio 不支持访问控制列表 (ACL)。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。

## 使用 Nimble Studio 的基于属性的访问控制 (ABAC)

| | |
|---|---|
| 支持 ABAC（策略中的标签） | 是 |

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。

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。

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控制 (ABAC)。

## 将临时凭证用于 Nimble Studio

| | |
|---|---|
| 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。

### Nimble Studio 的跨服务主体权限

| | |
|---|---|
| 支持主体权限 | 是 |

### Nimble Studio 的服务角色

| | |
|---|---|
| 支持服务角色 | 是 |

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。服务角色只在您的账户内提供访问权限，不能用于为访问其它账户中的服务授权。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 Nimble Studio 的功能。仅当 Nimble Studio 提供相关指导时才编辑服务角色。

### Nimble Studio 的服务相关角色

| | |
|---|---|
| 支持服务相关角色 | 否 |

Nimble Studio 不支持服务相关角色。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。服务相关角色显示在您的 IAM 账户中，并归该服务所有。 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，请参阅使用 IAM 的AWS 服务。在表中查找服务相关角色列中包含 Yes 额表。选择是链接以查看该服务的服务相关角色文档。

## 适用于 Amazon Nimble Studio 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Nimble Studio 资源的权限。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。管理员必须创建 IAM policy，以便为用户和角色授予权限，以对所需资源执行操作。然后，管理员必须将这些策略附加到需要这些权限的用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践

### 策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 Nimble Studio 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 — 要快速开始使用 Nimble Studio，请使用 AWS 托管策略为员工提供所需的权限。这些策略已在您的账户中提供，并由 AWS维护和更新。有关更多信息，请参阅 IAM 用户指南中的使用 AWS 托管策略的权限入门。
- 授予最低权限：创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其它权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅 IAM 用户指南 中的授予最低权限。
- 为敏感操作启用 MFA：为增强安全性，要求用户使用多重身份验证 (MFA) 来访问敏感资源或 API 操作。要了解更多信息，请参阅《IAM 用户指南》中的在 AWS中使用多重身份验证 (MFA)。
- 使用策略条件来增强安全性：在切实可行的范围内，定义基于身份的策略允许访问资源的条件。例如，您可编写条件来指定请求必须来自允许的 IP 地址范围。您也可以编写条件，以便仅允许指定日期或时间范围内的请求，或者要求使用 SSL 或 MFA。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

## AWS 亚马逊 Nimble Studio 的托管政策

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的适用于工作职能的AWS 托管策略。

您的最终用户将主要使用 Nimble Studio 门户网站访问 Amazon Nimble Studio。使用 StudioBuilder 或 Nimble Studio 控制台创建工作室时，会为每个工作室角色创建一个 IAM 角色：工作室管理员和工作室用户。每个角色都附加了各自的 IAM 托管策略。Nimble Studio 门户提供的体验是，用户只能列出和使用他们有权访问的资源。

Nimble Studio 门户提供的体验是，用户只能列出和使用他们有权访问的资源，并且门户的正常操作须依赖于这些策略的内容。Nimble Studio 的最终用户将使用该门户访问他们的云工作室。因此，当管理员使用创建工作室时 StudioBuilder，会为需要访问工作室的每个人创建一个 IAM 角色。这包括工作室管理员和工作室用户，他们都附加了各自的 IAM 托管策略。

有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的适用于工作职能的AWS 托管策略。

## AWS 托管策略：**AmazonNimbleStudio-LaunchProfileWorker**

您可以将 AmazonNimbleStudio-LaunchProfileWorker 策略附加到 IAM 身份。

将此策略附加到 Nimble Studio Builder 创建的 EC2 实例，以授予 Nimble Studio 启动配置文件工作人员对所需资源的访问权限。

权限详细信息

该策略包含以下权限。

- ds-允许 LaunchProfile 工作人员发现 AWS Managed Microsoft AD 与关联的的连接信息 LaunchProfile。
- ec2-允许 LaunchProfile 工作人员发现用于连接的安全组和子网信息 LaunchProfile。
- fsx-允许 LaunchProfile 工作人员发现与关联的 Amazon FSx 卷的连接信息。 LaunchProfile

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

## AWS 托管策略：**AmazonNimbleStudio-StudioAdmin**

您可以将 AmazonNimbleStudio-StudioAdmin 策略附加到 IAM 身份。

将此策略附加到与工作室关联的管理员角色，以授予访问权限以访问与工作室管理员关联的 Amazon Nimble Studio 资源以及其他服务中的相关工作室资源。

权限详细信息

该策略包含以下权限。

- 灵活-允许 Studio 用户访问委托给他们的 Nimble 资源。 StudioAdmins
- sso：允许工作室用户查看工作室中其他用户的姓名。
- identitystore：允许工作室用户查看工作室中其他用户的姓名。
- ds-允许 Nimble Studio 向与工作室 AWS Managed Microsoft AD 关联的虚拟工作站添加虚拟工作站。
- ec2：允许 Nimble Studio 将虚拟工作站附加到您配置的 VPC。
- fsx：允许 Nimble Studio 将虚拟工作站连接到您配置的 Amazon FSx 卷。
- cloudwatch-允许 Nimble Studio 检索指标 CloudWatch 。

```
{
  "Statement": [
    {
```

```
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
```

```
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

## AWS 托管策略：**AmazonNimbleStudio-StudioUser**

您可以将 AmazonNimbleStudio-StudioUser 策略附加到 IAM 身份。

将此策略附加到与工作室关联的用户角色，授予访问权限以访问与工作室用户关联的 Amazon Nimble Studio 资源以及其他服务中的相关工作室资源。

权限详细信息

该策略包含以下权限。

- 灵活-允许 Studio 用户访问委托给他们的 Nimble 资源。 StudioAdmins
- sso：允许工作室用户查看工作室中其他用户的姓名。
- identitystore：允许工作室用户查看工作室中其他用户的姓名。
- ds-允许 Nimble Studio 向与工作室 AWS Managed Microsoft AD 关联的虚拟工作站添加虚拟工作站。
- ec2：允许 Nimble Studio 将虚拟工作站附加到您配置的 VPC。
- fsx：允许 Nimble Studio 将虚拟工作站连接到您配置的 Amazon FSx 卷。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
```

```
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

## Nimble Studio 更新了 AWS 托管策略

查看有关 Amazon Nimble Studio AWS 托管政策自该服务开始跟踪这些变更以来这些更新的详细信息。

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：更新策略 | Amazon Nimble Studio 更新了使用最新版身份存储服务的策略。 | 2023 年 9 月 22 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioAdmin：更新策略 | Amazon Nimble Studio 更新了使用最新版身份存储服务的策略。 | 2023 年 9 月 22 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：更新策略 | Amazon Nimble Studio 更新策略以允许工作室用户查看其工作站备份。 | 2022 年 12 月 20 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioAdmin：更新策略 | Amazon Nimble Studio 更新策略以允许工作室管理员查看其工作站备份。 | 2022 年 12 月 20 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：更新策略 | Amazon Nimble Studio 更新了一项政策，允许工作室管理员检索 CloudWatch指标。 | 2021 年 11 月 11 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：更新策略 | Amazon Nimble Studio 更新策略以允许工作室用户启动和停止工作站。 | 2021 年 11 月 1 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioAdmin：更新策略 | Amazon Nimble Studio 更新策略以允许工作室管理员启动和停止工作站。 | 2021 年 11 月 1 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：更新策略 | Amazon Nimble Studio 更新策略，以便有条件地允许访问基于 `nimble:ownedBy` 而非 `nimble:createdBy` 的流会话资源。 | 2021 年 8 月 16 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioUser：新策略 | Amazon Nimble Studio 添加了一项新策略，此策略允许访问与工作室用户相关的资源以及其他服务中的相关工作室资源。 | 2021 年 4 月 28 日 |
| AWS 托管策略：AmazonNimbleStudio-StudioAdmin：新策略 | Amazon Nimble Studio 添加了一项新策略，此策略允许访问与工作室管理员相关的资源以及其他服务中的相关工作室资源。 | 2021 年 4 月 28 日 |
| AWS 托管策略：AmazonNimbleStudio-LaunchProfileWorker：新策略 | Amazon Nimble Studio 添加了一项新策略，此策略允许访问 Nimble Studio 启动配置文件工作人员所需的资源。 | 2021 年 4 月 28 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon Nimble Studio 开始跟踪变更 | Amazon Nimble Studio 开始跟踪其 AWS 托管政策的变更。 | 2021 年 4 月 28 日 |

## 防止跨服务混淆代理

混淆代理问题是一个安全问题，即没有执行操作权限的实体可能会迫使更具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（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务以使用其权限对另一个客户的资源进行操作，否则该服务不应有访问权限。为防止这种情况， AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议使用资源策略中的 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键，限制 Identity and Access Management (IAM) 向 Amazon Nimble Studio 提供的资源访问权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，`aws:SourceAccount` 值和 `aws:SourceArn` 值中的账户必须使用相同的账户 ID。

`aws:SourceArn` 值必须是工作室的 ARN，并且 `aws:SourceAccount` 必须是您的账户 ID。在工作室创建之前，您不会知道工作室 ID，因为此 ID 是由 Nimble Studio 生成的。创建工作室后，您可以更新信任策略，并将最终的工作室 ID 设置为 `aws:SourceArn`。

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。如果您不知道资源的完整 ARN，或正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (*) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:nimble::123456789012:*`。

当您的最终用户登录 Nimble Studio 门户网站时，他们将担任您的工作室角色。创建工作室时， AWS 配置角色并评估策略。 AWS 之后每当您的一个用户登录 Nimble Studio 门户时，都会评估该策略。您在创建工作室时不能修改 `aws:SourceArn`。创建完工作室后，您可以为 `aws:SourceArn` 使用 studioArn。

以下示例是一项担任角色策略，其演示如何使用 Nimble Studio 中的 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键来防范混淆代理问题。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

# Amazon Nimble Studio 身份和访问问题排查

使用以下信息可帮助您诊断和修复在使用 Nimble Studio 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Nimble Studio 中执行操作
- 我无权执行 iam:PassRole.
- 我想要查看我的访问密钥。
- 我是管理员并希望允许其他人访问 Nimble Studio。
- 我想允许我以外的人访问我 AWS 账户 的 Nimble Studio 资源。

## 我无权在 Nimble Studio 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 `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 `nimble:`*`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:
 nimble: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 nimble:*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，则必须联系您的管理员寻求帮助。请求管理员更新您的策略，以便允许您将角色传递给 Nimble Studio。

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与服务相关的角色。为此，您必须具有将角色传递到服务的权限。

当名为 johndoe 的用户尝试使用控制台在 Nimble Studio 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操作。John 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/johndoe is not authorized to perform: iam:PassRole
```

在这种情况下，John 可以请求管理员更新其策略，以授予其执行 iam:PassRole 操作的权限。

### 我想要查看我的访问密钥。

Amazon Nimble Studio 不提供访问密钥。要了解有关秘密访问密钥的信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey中的管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果您丢失了秘密访问密钥，则必须向您的用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅《IAM 用户指南》中的管理访问密钥。

### 我是管理员并希望允许其他人访问 Nimble Studio。

要允许其他人访问 Nimble Studio，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 AWS。然后，将策略附加到实体，以便向其授予正确的权限。

Nimble Studio 为您提供了 AWS Management Console中的 `AmazonNimbleStudio-StudioUser`。管理控制台的 IT 管理员使用此策略向其他人授予工作室访问权限。

有关使用管理员策略的教程，请查看 设置 Nimble Studio 指南。要了解如何将现有策略（例如用户策略和启动配置文件策略）附加到用户，请参阅创建 IAM 用户（控制台）。

有关导入策略的信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-delegated-user.html中的创建您的第一个 IAM 委托用户和委托组。

### 我想允许我以外的人访问我 AWS 账户 的 Nimble Studio 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（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 Nimble Studio 是否支持这些特征，请参阅 Amazon Nimble Studio 如何与 IAM 协同工作。
- 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。

## 使用 Nimble Studio 记录和监控安全事件

监控是维护 Amazon Nimble Studio 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。从 AWS 解决方案的所有部分收集监控数据，以便在出现多点故障时可以更轻松地对其进行调试。

AWS 和 Nimble Studio 提供了用于监控您的资源和应对潜在事件的工具，包括使用记录 Nimble Studio 通话 AWS CloudTrail和《AWS CloudFormation 用户指南》。

有关 Amazon Nimble Studio 如何使用的更多信息 AWS CloudFormation，包括 JSON 和 YAML 模板的示例，请参阅用户指南中的 A mazon Nimble Studio 资源和属性参考。 AWS CloudFormation 要了解如何使用 CloudFormation模板，请参阅AWS CloudFormation 概念。

主题



# 使用记录 Nimble Studio 通话 AWS CloudTrail

Amazon Nimble Studio 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或用户 AWS 服务 在 Nimble Studio 中采取的操作的记录。 CloudTrail 将 Nimble Studio 的所有 API 调用捕获为事件。捕获的调用中包括来自 Nimble Studio 控制台的调用以及对 Amazon Nimble Studio 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 Nimble Studio 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 Nimble Studio 发出的请求、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。

## Nimble Studio 中的信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Nimble Studio 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，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录你中的事件 AWS 账户，包括 Nimble Studio 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

接收来自多个账户的 CloudTrail 日志文件

Nimble Studio 的操作由亚马逊 Nimble Studio API 参考记录 CloudTrail 并记录在案。例如，调用 GetStudio 和 DeleteStudio 操作会在 CloudTrail 日志文件中生成条目。 CreateStudio

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。
- 请求是否由其它 服务发出。

有关更多信息，请参阅CloudTrail 用户身份元素。

## 理解 Nimble Studio 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。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。

这个 JSON 示例显示了三个操作：

- ACTION_1: CreateStudio
- ACTION_2: GetStudio
- ACTION_3: DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
```

```
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
```

```
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
```

```
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
```

```
    "recipientAccountId": "111122223333"
}
```

在示例中，您会注意到事件显示了区域、IP 地址和其他 “请求参数”，例如 “” userRoleArn 和 “adminRoleArn”，它们将帮助您识别事件。您可以在 "creationDate" 中看到时间和日期，以及请求的来源，此来源标记为 "eventSource": "nimble.amazonaws.com"。

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 IAM 或 AWS STS 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。

AWS CloudTrail 将 IAM 和 AWS Security Token Service (AWS STS) 的所有 API 调用捕获为事件，包括来自控制台的调用和 API 调用。要了解有关 CloudTrail 与 IAM 和一起使用的更多信息 AWS STS，请参阅使用记录 IAM 和 AWS STS API 调用 AWS CloudTrail。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

有关亚马逊提供的其他监控服务的信息，请参阅亚马逊 CloudWatch 用户指南。

# Amazon Nimble Studio 的合规性验证

Amazon Nimble Studio 遵循责任共担模式，合规由我们的客户共同 AWS 承担。

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、行业指导方针和法规。
- 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件的列表，请参阅 Security Hub 控件参考。
- 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。

# Amazon Nimble Studio 中的基础设施安全性

作为一项托管服务，Amazon Nimble Studio 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 Nimble Studio。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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

# Nimble Studio 的安全最佳实践

Amazon Nimble Studio 提供了在您开发和实施自己的安全策略时需要考虑的大量安全特征。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

## 监控

监控是维护 Nimble Studio 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。有关监控和响应事件的详细信息，请参阅 使用 Nimble Studio 记录和监控安全事件。

## 数据保护

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置个人账户。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 建议使用 TLS 1.2 或更高版本。
- 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 中的个人数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅美国联邦信息处理标准（FIPS）第 140-2 版。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如名称字段）。这包括当你 AWS 服务 使用控制台、API 或软件开发工具包与 Amazon Nimble Stu AWS dio 或其他人合作时。 AWS CLI您输入到 Amazon Nimble Studio 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

## 权限

使用用户、IAM 角色以及向用户授予最低权限来管理对 AWS 资源的访问权限。制定用于创建、分发、轮换和撤消 AWS 访问凭证的凭证管理策略和程序。有关更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实践。

# Nimble Studio 的支持

本节提供了 Nimble Studio 的支持选项，例如如何在部署或使用服务及其相关应用程序时获得帮助。

目录



## Nimble Studio 论坛

如果您对 Nimble Studio 有疑问，请访问 Nimble Studio 论坛。在这里，您可以从社区和 AWS 论坛版主那里获得有关 Nimble Studio 特征、技术问题和故障排除帮助的答案。

## 应用程序支持

Nimble Studio 为以下应用程序提供了其他文档。

### AWSThinkboxDeadline

如需有关渲染农场的帮助或要了解 Deadline 的工作原理，请参阅 AWSThinkboxDeadline 文档。

### Nimble Studio File Transfer

要了解文件传输功能的工作原理，请参阅 Nimble Studio 文件传输功能用户指南。

## AWS Support Center

AWS Support Center 是创建和管理支持案例的中心。它提供访问各种资源的权限，包括账单和技术解决方案、Knowledge Center、Knowledge Center 视频、AWS 文档以及培训和认证。

## AWS Support 计划

AWS Support 计划可帮助您优化性能、保持安全、避免停机和控制成本。有关不同 AWS Support 计划的更多信息，请参阅比较 AWS Support 计划。

有关 AWS 如何为您提供支持的更多信息，请访问联系我们页面。

# 文档历史记录

- API 版本：最新
- 最近文档更新时间：2023 年 9 月 22 日。

下表描述《Nimble Studio 管理员指南》每次发布时进行的重要更改。

| 更改 | 说明 | |
|---|---|---|
| 新服务和指南 | 这是 Amazon Nimble Studio 和《Amazon Nimble Studio 管理员指南》的初始版本。 | 2023 年 6 月 19 日 |
| AWS 托管策略更新 | 更新 `AmazonNimbleStudio-StudioUser` 和 `AmazonNimbleStudio-StudioAdmin` 策略以使用最新版本的 AWS IAM Identity Center 服务。 | 2023 年 9 月 22 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。