



入门指南

AWS 管理控制台



版本 1.0

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 管理控制台: 入门指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

那是什么 AWS 管理控制台？	1
的特点 AWS 管理控制台	1
个性化 AWS 服务控制台	2
访问 AWS 管理控制台	2
使用移动设备访问 AWS 管理控制台	2
开始使用服务	3
统一导航	4
访问“服务”菜单	4
搜索产品、服务、特征等	5
搜索 AWS 产品	6
缩小搜索范围	6
查看服务的特征	6
正在启动 AWS CloudShell	7
访问 AWS 通知和 Health 事件	7
获取支持	8
正在配置 AWS 管理控制台	8
配置统一设置	9
配置可见区域和服务	11
选择您的区域	13
Favorites	14
更改密码	18
更改的语言 AWS 管理控制台	20
访问您的 AWS 信息	22
访问账户信息	23
访问组织信息	23
访问服务配额信息	24
访问账单信息	24
登录多个账户	24
使用建议的操作	25
AWS 建议的操作的功能	26
使用建议的操作	26
使用 CloudTrail 日志进行监控	26
AWS Console Home	29
查看所有 AWS 服务	29

使用小组件	29
管理小组件	29
myApplications	31
myApplications 的特征	31
相关服务	32
访问 myApplications	32
定价	33
支持的区域 :	33
应用程序	34
资源	41
myApplications 控制面板	44
与 Amazon Q 聊天	48
开始使用 Amazon Q	48
问题示例	48
AWS 管理控制台 私密访问权限	49
支持 AWS 区域、服务控制台和功能	49
AWS 管理控制台 私人访问安全控制概述	55
AWS 管理控制台 来自您的网络的账号限制	55
从您的网络到互联网的连接	55
所需的 VPC 端点和 DNS 配置	55
DNS 配置	56
VPC 终端节点和 AWS 服务DNS配置	58
实施服务控制策略和 VPC 端点策略	59
服务控制策略	59
VPC 端点策略	60
实施基于身份的策略和其他策略类型	61
支持的 AWS 全局条件上下文密钥	61
AWS 管理控制台 私有访问权限如何与 aws 配合使用 : SourceVpc	62
不同的网络路径如何反映在 CloudTrail	63
试试 AWS 管理控制台 私密访问	63
使用 Amazon EC2 测试设置	63
使用 Amazon 测试设置 WorkSpaces	78
使用 IAM 策略测试 VPC 设置	94
参考架构	96
AWS 用户体验定制	97
开始使用	97

先决条件	98
在中访问 UXC 设置 AWS 管理控制台	98
以编程方式访问 UXC 设置	99
API 参考	99
使用 CloudTrail 日志进行监控	99
UXC 管理活动位于 CloudTrail	99
UXC 事件示例	27
安全性	101
身份和访问管理	101
AWS 托管策略	110
AWSManagementConsoleBasicUserAccess	110
AWSManagementConsoleAdministratorAccess	111
策略更新	112
Markdown 在 AWS	114
段落、行间距和水平线	114
标题	115
文本格式设置	115
链接	115
列表	115
表格和按钮 (CloudWatch 仪表板)	116
问题排查	118
页面未正确加载	118
我的浏览器在连接时显示“访问被拒绝”错误 AWS 管理控制台	119
我的浏览器在连接时显示超时错误 AWS 管理控制台	119
我想更改的语言，AWS 管理控制台但在页面底部找不到语言选择菜单	120
文档历史记录	121
.....	CXXIV

那是什么 AWS 管理控制台？

[AWS 管理控制台](#) 是一个基于 Web 的应用程序，包含所有单独的 AWS 服务控制台并提供对这些控制台的集中访问。您可以使用中的 Unified Navigation AWS 管理控制台 来搜索服务、查看通知 AWS CloudShell、访问权限、访问账户和账单信息，以及自定义您的常规控制台设置。的主页 AWS 管理控制台 被称为 AWS Console Home。您可以从中 AWS Console Home 管理您的 AWS 应用程序并访问所有其他单独的服务控制台。您还可以使用小组件进行自定义，AWS Console Home 以显示有关 AWS 您的资源的其他有用信息。您可以添加、删除和重新排列小组件，例如最近访问、AWS Health 等。

主题

- [的特点 AWS 管理控制台](#)
- [中的各个 AWS 服务控制台 AWS 管理控制台](#)
- [访问 AWS 管理控制台](#)
- [使用移动设备访问 AWS 管理控制台](#)

的特点 AWS 管理控制台

的重要功能 AWS 管理控制台 包括以下内容：

- 导航到 AWS 服务控制台-您可以使用 Unified Navigation 访问最近访问过的服务控制台、查看服务并将其添加到“收藏夹”列表、访问您的控制台设置以及进行访问 AWS 用户通知服务。
- 搜索 AWS 服务和其他 AWS 信息-使用统一搜索来搜索 AWS 服务和功能以及 AWS 商城产品。
- 自定义控制台 — 可以使用“统一设置”来自定义 AWS 管理控制台的各个方面，包括语言、默认区域等。
- 运行 CLI 命令 — AWS CloudShell 可直接从控制台访问。您可以使用 CloudShell 对自己喜欢的服务运行 AWS CLI 命令。
- 访问所有 AWS 事件通知-您可以使用 AWS 管理控制台 访问 AWS 用户通知服务 和的通知 AWS Health。
- 自定义 AWS Console Home — 您可以使用小部件完全自定义您的 AWS Console Home 体验。
- 创建和管理 AWS 应用程序 — 使用中的 AWS Console Home MyApplications 管理和监控应用程序的成本、运行状况、安全状况和性能。
- 与 Amazon Q 聊天 — 您可以直接从控制台获得生成式人工智能 (AI) 助手支持的 AWS 服务 问题答案。您还可以联系实时座席以获取更多支持。

- 控制网络中的 AWS 账户访问权限-当流量来自您的网络内部时，您可以使用 AWS 管理控制台 私有 AWS 管理控制台 访问权限将访问权限限制为一组指定的已知 AWS 帐户。

中的各个 AWS 服务控制台 AWS 管理控制台

每项 AWS 服务都有自己的独立服务控制台，您可以在中访问该控制台 AWS 管理控制台。您在统一设置中选择的 AWS 管理控制台设置（例如视觉模式和默认语言）将应用于所有单独的主 AWS 机。AWS 服务控制台提供各种云计算工具，以及有关您的帐户和[账单](#)的信息。如果您想进一步了解特定服务及其控制台（例如 Amazon Elastic Compute Cloud），请使用 AWS 管理控制台 导航栏中的统一搜索导航到其控制台，然后从 EC2 文档[网站访问亚马逊AWS 文档](#)。

当您导航到单个 AWS 服务的控制台时，您仍然可以使用控制台顶部的统一导航访问的功能。AWS 管理控制台 您可以通过导航到一项服务的控制台并在页面页脚中选择反馈来为该控制台留下反馈。

访问 AWS 管理控制台

您可以访问 a AWS 管理控制台 t <https://console.aws.amazon.com/>。

使用移动设备访问 AWS 管理控制台

[AWS 管理控制台](#) 适合在平板电脑以及其他种类的移动设备上工作：

- 水平和垂直空间最大化，可在屏幕上显示更多内容。
- 按钮和选择器更大，可获得更好的触控体验。

要在移动设备上访问 AWS 管理控制台，必须使用 AWS Console Mobile Application。此应用适用于 Android 和 iOS。控制台移动应用程序提供移动相关任务，是完整 Web 体验的好搭档。例如，您可以通过手机轻松地查看和管理现有 Amazon EC2 实例和 Amazon CloudWatch 警报。有关更多信息，请参阅《AWS Console Mobile Application 用户指南》中的[什么是 AWS Console Mobile Application ?](#)。

可以从 [Amazon Appstore](#)、[Google Play](#) 或 [iOS 应用商店](#) 下载控制台移动应用程序。

在 AWS 管理控制台中开始使用服务

[AWS 管理控制台](#)提供多种方式来导航到各个服务控制台。

要打开某项服务的控制台

请执行以下操作之一：

- 在导航栏上的搜索框中，输入服务的全部或部分名称。在 Services (服务) 下方，从搜索结果列表中选择您需要的服务。有关更多信息，请参阅 [使用统一搜索搜索产品、服务、功能等 AWS 管理控制台](#)。
- 在最新访问的服务小组件中，选择一个服务名称。
- 在最新访问的服务小组件中，选择查看所有 AWS 服务。然后，在所有 AWS 服务页面上，选择一个服务名称。
- 在导航栏中，选择 Services (服务) 可打开完整的服务列表。然后在最新访问或所有服务的下方选择服务。

通过统一导航使用 AWS 管理控制台导航栏

本主题介绍如何使用统一导航。统一导航是指充当控制台页眉和页脚的导航栏。使用统一导航可以执行以下操作：

- 搜索和访问 AWS 服务、特征、产品等。
- 启动 AWS Cloudshell。
- 访问 AWS 通知和 AWS Health 事件。
- 从各种 AWS 知识来源获得支持。
- 通过选择默认语言、视觉模式、区域等，对 AWS 管理控制台进行配置。
- 访问账户、组织、服务配额和账单信息。

主题

- [访问 AWS 管理控制台中的“服务”菜单](#)
- [使用统一搜索搜索产品、服务、功能等 AWS 管理控制台](#)
- [AWS CloudShell 从中的导航栏启动 AWS 管理控制台](#)
- [访问 AWS 通知和 Health 事件](#)
- [获取支持](#)
- [AWS 管理控制台 使用统一设置进行配置](#)
- [访问您的 AWS 账户、组织、服务配额和账单信息 AWS 管理控制台](#)
- [登录多个账户](#)
- [AWS 管理控制台中 AWS 建议的操作](#)

访问 AWS 管理控制台中的“服务”菜单

可以使用搜索栏旁边的“服务”菜单来访问最近访问的服务，查看收藏夹列表，以及查看所有 AWS 服务。还可以通过选择服务类型（如分析或应用程序集成）来按类型查看服务。

以下过程将介绍如何访问服务菜单。

访问“服务”菜单

1. 登录到 [AWS 管理控制台](#)。

2. 在导航栏中，选择服务 (⋮)。
3. (可选) 选择最近访问以查看您最近与之交互的服务和应用程序。
4. (可选) 选择收藏夹以查看收藏夹列表。
5. (可选) 选择所有应用程序以查看 myApplications 应用程序。
6. (可选) 选择所有服务以查看按字母顺序排列的所有 AWS 服务的列表。
7. (可选) 选择一种服务类型以按类型查看 AWS 服务。

使用统一搜索搜索搜索产品、服务、功能等 AWS 管理控制台

导航栏中的搜索框提供了一个统一的搜索工具，用于查找 AWS 服务和功能、服务文档、AWS Marketplace 产品等。只需输入几个字符或一个问题，即可开始生成各种可用内容类型的结果。输入的每个单词都会进一步优化您的结果。可用的内容类型包括：

- Services
- 功能
- 文档
- 博客
- 知识文章
- Events
- 教程
- Marketplace
- 资源

Note

可以通过执行有针对性的搜索对搜索结果进行筛选，以仅显示资源。要执行有针对性的搜索，请在搜索栏中的查询开头输入 `/Resources`，然后从下拉菜单中选择 `/Resources`。然后输入查询的其余部分。

主题

- [在中搜索 AWS 产品 AWS 管理控制台](#)
- [在中完善您的搜索 AWS 管理控制台](#)

- [在中查看服务的功能 AWS 管理控制台](#)

在中搜索 AWS 产品 AWS 管理控制台

以下步骤详细介绍了如何使用搜索工具搜索 AWS 产品。

搜索服务、功能、文档或 AWS Marketplace 产品

1. 在 [AWS 管理控制台](#) 导航栏的搜索框中，输入您的查询。
2. 选择任意链接以导航到预期目的地。

Tip

您还可以使用键盘快速导航到顶部搜索结果。首先，按 Alt+S (Windows) 或 Option+s (macOS) 访问搜索栏。然后开始输入您的搜索词。当预期的结果显示在列表顶部时，按 Enter。例如，要快速导航到 Amazon EC2 控制台，请输入 ec2，然后按 Enter。

在中完善您的搜索 AWS 管理控制台

可以按内容类型来缩小搜索范围，并查看有关搜索结果的其他信息。

将搜索范围缩小到特定的内容类型

1. 在 [AWS 管理控制台](#) 导航栏的搜索框中，输入您的查询。
2. 选择搜索结果旁边的内容类型之一。
3. (可选) 要查看特定类别的所有结果，请执行以下操作：
 - 选择显示更多。此时将打开一个显示结果的新选项卡。
4. (可选) 要查看有关搜索结果的其他信息，请执行以下操作：
 - a. 在搜索结果中，将光标悬停在其中一个搜索结果上。
 - b. 查看可用的其他信息。

在中查看服务的功能 AWS 管理控制台

可以在搜索结果中查看服务的特征。

查看服务的特征

1. 在 [AWS 管理控制台](#) 导航栏的搜索框中，输入您的查询。
2. 在搜索结果中，将光标悬停在服务中的一项服务上。
3. 在主要功能中选择一个链接。

AWS CloudShell 从中的导航栏启动 AWS 管理控制台

AWS CloudShell 是一个基于浏览器、经过预先验证的 shell，您可以直接从导航栏启动。AWS 管理控制台 您可以使用首选外壳 (Bash PowerShell、或 Z shell) 对服务运行 AWS CLI 命令。

您可以使用以下两种 AWS 管理控制台 方法之一 CloudShell 从启动：

- 选择控制台页脚中的 CloudShell 图标。
- 选择控制台导航栏上的 CloudShell 图标。

有关此服务的更多信息，请参阅 [AWS CloudShell 用户指南](#)。

有关 AWS 区域 在何 AWS CloudShell 处可用的信息，请参阅[AWS 区域服务列表](#)。控制台区域的选择与该 CloudShell 区域同步。如果在所选地区 CloudShell 不可用，则 CloudShell 将在最近的地区运行。

访问 AWS 通知和 Health 事件

可以从导航栏访问部分 AWS 通知以及查看运行状况事件。还可以从导航栏访问 AWS 用户通知服务 以查看所有 AWS 通知和 AWS Health 控制面板。

有关更多信息，请参阅《AWS 用户通知服务 用户指南》中的[什么是 AWS 用户通知服务？](#)，以及《AWS Health 用户指南》中的[什么是 AWS Health？](#)

以下过程将介绍如何访问 AWS 事件信息。

访问 AWS 事件信息

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择铃铛图标。
3. 查看通知和运行状况事件。
4. (可选) 选择查看所有通知以导航到 用户通知服务 控制台。

5. (可选) 选择查看所有运行状况事件以导航到 AWS Health 控制台。

获取支持

可以通过选择导航栏中的问号图标来获取支持。在支持菜单中，可以选择：

- 导航到支持中心服务控制台
- 从 AWS IQ 获取专家帮助
- 在 AWS re:Post 上查看来自社区文章和知识中心的精选知识
- 转到 AWS 文档
- 导航到 AWS 培训
- 导航到 AWS 入门资源中心
- 为当前正在访问的任何服务控制台留下反馈

Note

也可以通过选择控制台页脚中的反馈来提供反馈。打开的模式标题显示了您当前正为哪个控制台留下反馈

您还可以随时在控制台中获得帮助，与实时座席取得联系，并通过与 AWS Q 聊天来询问任何关于 AWS 的问题。有关更多信息，请参阅[???](#)。

AWS 管理控制台 使用统一设置进行配置

本主题介绍如何 AWS 管理控制台 使用统一设置页面进行配置，以设置适用于所有服务控制台的默认值。

主题

- [在中配置统一设置 AWS 管理控制台](#)
- [在中配置可见的区域和服务 AWS 管理控制台](#)
- [选择您的区域](#)
- [中的最爱 AWS 管理控制台](#)
- [在中更改您的密码 AWS 管理控制台](#)
- [更改的语言 AWS 管理控制台](#)

在中配置统一设置 AWS 管理控制台

您可以从“AWS 管理控制台 统一设置”页面配置设置和默认值，例如显示屏、语言和区域。可以通过统一导航中的导航栏访问统一设置。视觉模式和默认语言也可以直接从导航栏进行设置。这些更改应用于所有服务控制台。

Important

为确保您的设置、常用服务和最近访问的服务在全球范围内持续存在，这些数据将存储在所有区域 AWS 区域，包括默认禁用的区域。这些区域是非洲（开普敦）、亚太地区（香港）、亚太地区（海得拉巴）、亚太地区（雅加达）、欧洲（米兰）、欧洲（西班牙）、欧洲（苏黎世）、中东（巴林）和中东（阿联酋）。您还需要[手动启用区域](#)以访问它，并在该区域中创建和管理资源。如果您不想全部存储这些数据 AWS 区域，请选择“全部重置”以清除您的设置，然后在“设置”管理中选择不记住最近访问过的服务。

主题

- [在中访问统一设置 AWS 管理控制台](#)
- [在中重置统一设置 AWS 管理控制台](#)
- [在中编辑统一设置 AWS 管理控制台](#)
- [更改的视觉模式 AWS 管理控制台](#)

在中访问统一设置 AWS 管理控制台

以下过程介绍了如何访问统一设置。

访问统一设置

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标（#）。
3. 要打开统一设置页面，请选择查看所有用户设置。

在中重置统一设置 AWS 管理控制台

重置统一设置可删除所有“统一设置”配置并恢复默认设置。

Note

这会影响到多个区域 AWS，包括导航和“服务”菜单中的收藏服务、控制台主页小部件和中最近访问过的服务，以及适用于所有服务的设置，例如默认语言、默认区域和视觉模式。AWS Console Mobile Application

重置所有统一设置

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 选择查看所有用户设置打开统一设置页面。
4. 选择全部重置。

在中编辑统一设置 AWS 管理控制台

以下过程介绍了如何编辑首选设置。

编辑统一设置

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 选择查看所有用户设置打开统一设置页面。
4. 选择首选设置旁的编辑：
 - 本地化和区域设置：
 - 语言可让您为控制台文本选择默认语言。
 - 默认区域可让您选择每次登录时应用的默认区域。您可为您的账户选择任何可用区域。还可以选择上次使用的区域作为默认区域。

要了解 [AWS 管理控制台](#) 中的区域路由的更多信息，请参阅 [选择区域](#)。

- 显示：
 - 视觉模式允许您将控制台设置为浅色模式、深色模式或浏览器的默认显示模式。

深色模式是一项测试版特征，可能不适用于所有 AWS 服务控制台。

- 收藏夹栏显示在带有图标的完整服务名称或仅服务图标之间切换收藏夹栏显示。

- 使用收藏夹栏图标大小可以将收藏夹栏显示上服务图标的大小在小 (16x16 像素) 和大 (24x24 像素) 之间切换。
- 设置管理：
 - 记住最近访问过的服务允许你选择是否 AWS 管理控制台 记住你最近访问过的服务。关闭此功能还会删除您最近访问的服务历史记录，因此您将无法再在“服务”菜单或 Console Home 小组件中看到最近访问过的服务。AWS Console Mobile Application

5. 选择保存更改。

更改的视觉模式 AWS 管理控制台

视觉模式可将控制台设置为浅色模式、深色模式或浏览器的默认显示模式。

从导航栏更改视觉模式

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 对于视觉模式，选择浅色表示浅色模式，选择深色表示深色模式，选择浏览器默认模式表示浏览器的默认显示模式。

在中配置可见的区域和服务 AWS 管理控制台

账户管理员可以控制哪些 AWS 区域 和哪些 AWS 服务在 AWS 管理控制台 导航中可见。这些账户级别设置可在统一设置页面的账户设置选项卡中找到。当您隐藏某个区域时，该区域将从该账户中所有用户的区域选择器中删除。当您隐藏某项服务时，该服务将在账户中所有用户的“服务”菜单的单独部分中显示为不可用。在统一搜索结果以及控制台主页上的“最近访问过”和“收藏夹”小部件中，隐藏的服务也会显示为灰色。

如果用户通过网址直接导航到隐藏的区域或服务，他们会看到一个叠加层，告知他们该地区或服务已在账户级别隐藏。

Note

可以随时导航到“统一设置”页面，因此管理员无法将自己锁定在这些设置之外。如果用户没有所需的权限，或者 AWS 用户体验定制服务不可用，则默认情况下，所有区域和服务均可见。

主题

- [配置可见区域和服务的先决条件](#)
- [在中配置可见区域 AWS 管理控制台](#)
- [在中配置可见服务 AWS 管理控制台](#)

配置可见区域和服务的先决条件

要查看和更改可见的区域和服务设置，您需要特定的 IAM 权限。

- 要查看设置，您需要 `uxc:GetAccountCustomizations` 权限。
- 要更改设置，您需要 `uxc:UpdateAccountCustomizations` 权限。

AWS 托管策

略 `AWManagementConsoleBasicUserAccess` 和 `AWManagementConsoleAdministratorAccess` 包括这些权限。

有关更多信息，请参阅 [???](#)。

在中配置可见区域 AWS 管理控制台

您可以为账户中的所有用户选择在区域选择器中 AWS 区域 显示哪些用户。

配置可见区域

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 选择“查看所有用户设置”以打开“统一设置”页面。
4. 选择账户设置选项卡。
5. 对于可见区域，选中要显示的区域的复选框，或者清除要隐藏的区域复选框。
6. 选择保存更改。

保存后，账户中所有用户的隐藏区域将从区域选择器中移除。

在中配置可见服务 AWS 管理控制台

您可以为账户中的所有用户选择在“服务”菜单中显示哪些 AWS 服务。

配置可见服务

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 选择“查看所有用户设置”以打开“统一设置”页面。
4. 选择账户设置选项卡。
5. 对于 Visible 服务，选中要显示的服务的复选框，或者清除要隐藏的服务的复选框。
6. 选择保存更改。

保存后，隐藏的服务在账户中所有用户的“服务”菜单的单独部分中显示为不可用。在统一搜索结果以及控制台主页上的“最近访问过”和“收藏夹”小部件中，隐藏的服务也会显示为灰色。

选择您的区域

对于许多服务，您可以选择一个 AWS 区域 来指定资源管理位置。区域是位于同一地理区域的一组 AWS 资源。您无需为 [AWS 管理控制台](#) 或某些服务选择区域，例如 AWS Identity and Access Management。要了解有关 AWS 区域的更多信息，请参阅《AWS 一般参考》中的 [管理 AWS 区域](#)。

Note

如果您已创建 AWS 资源，但在控制台中看不到这些资源，则控制台可能会显示来自其他地区的资源。某些资源（如 Amazon EC2 实例）特定于在其中创建它们的区域。

主题

- [从导航栏中选择区域 AWS 管理控制台](#)
- [在中设置默认区域 AWS 管理控制台](#)

从导航栏中选择区域 AWS 管理控制台

以下过程详细介绍了如何在导航栏中更改您的区域。

从导航栏中选择区域

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择当前所显示区域的名称。
3. 选择要切换到的区域。

在中设置默认区域 AWS 管理控制台

以下过程详细介绍了如何在“统一设置”页面中更改默认区域。

设置默认区域

1. 在导航栏中，选择齿轮图标 (#)。
2. 选择查看所有用户设置以导航到统一设置页面。
3. 选择本地化和默认区域旁边的编辑。
4. 在默认区域中，选择一个区域。

Note

如果您未选择默认区域，则控制台将使用您上次访问的区域。如果您使用 IAM 身份中心登录，请选择特定的默认区域。上次访问的区域不会在 IAM 身份中心会话中持续存在。

5. 选择保存设置。
6. (可选) 选择转到新的默认区域以立即转到新的默认区域。

中的最爱 AWS 管理控制台

要更快地访问常用服务和应用程序，您可以将其服务控制台保存到收藏夹列表中。可以使用 AWS 管理控制台添加和删除收藏夹。将服务或应用程序添加到收藏夹后，它会显示在收藏夹快捷栏上。

主题

- [在中添加收藏夹 AWS 管理控制台](#)
- [在中访问收藏夹 AWS 管理控制台](#)
- [在中移除收藏夹 AWS 管理控制台](#)

在中添加收藏夹 AWS 管理控制台

您可以从服务菜单和最近访问菜单中将服务和应用程序添加到收藏夹。还可以使用搜索框中的搜索结果页面将服务添加到收藏夹。添加到收藏夹的服务和应用程序将显示在收藏夹快捷栏中。

主题

- [里面的“收藏夹”快捷栏 AWS 管理控制台](#)
- [在中将服务添加到您的收藏夹 AWS 管理控制台](#)

- [在中将应用程序添加到您的收藏夹 AWS 管理控制台](#)

里面的“收藏夹”快捷栏 AWS 管理控制台

当您的收藏夹中至少添加了一个 AWS 服务或应用程序时，就会出现收藏夹快捷栏。收藏夹快捷栏位于导航栏的下方，可在所有 AWS 服务控制台中看到，因此您可以快速访问自己喜欢的服务和应用程序。可以通过向左或向右拖动服务或应用程序来重新排列收藏夹快捷栏中服务和应用程序的顺序。

在中将服务添加到您的收藏夹 AWS 管理控制台

可以从服务菜单或搜索框中的搜索结果页面将服务添加到收藏夹。

Services menu

从“服务”菜单添加收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务 (⋮)。
3. (可选) 将最近访问的一项服务添加到收藏夹：
 - a. 在最近访问中，将光标悬停在一项服务上。
 - b. 选择该服务名称旁边的星号。
4. 选择所有服务。
5. 将光标悬停在所选服务上。
6. 选择该服务名称旁边的星号。

Search box

从搜索框中添加收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在搜索框中输入一项服务的名称。
3. 在搜索结果页面中，选择该服务名称旁边的星号。

Note

向收藏夹添加一项服务后，该服务将添加到导航栏下方的收藏夹快捷栏中。

在中将应用程序添加到您的收藏夹 AWS 管理控制台

您可以从服务菜单中将应用程序添加到收藏夹。

从“服务”菜单添加收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务 (⋮)。
3. (可选) 将最近访问的应用程序添加到收藏夹：
 - a. 在最近访问中，将光标悬停在应用程序上。
 - b. 选择该应用程序名称旁边的星号。
4. 选择应用程序。
5. 将光标悬停在所选应用程序上。
6. 选择该应用程序名称旁边的星号。

Note

向收藏夹添加应用程序后，该应用程序将添加到导航栏下方的收藏夹快捷栏中。

在中访问收藏夹 AWS 管理控制台

可以从服务菜单、收藏夹快捷栏和收藏夹小组件访问您添加到收藏夹的服务和应用程序。

Services menu

从服务菜单访问收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务 (⋮)。
3. 选择收藏夹。
4. 查看添加到收藏夹的服务和应用程序。
5. (可选) 查看应用程序资源：
 - a. 选择应用程序。
 - b. (可选) 选择[视图](#)。

- c. 查看资源。
- d. (可选) 选择筛选条件。您可以按属性或标签筛选资源。有关更多信息，请参阅《AWS 资源探索器 用户指南》中的[资源探索器的搜索查询语法参考](#)。
- e. (可选) 选择一个资源以在相关的服务控制台中查看该资源。

 Tip

您可以通过选择服务 (:::) 继续从中断处浏览资源。您应用的搜索筛选条件也将保留。

Favorites quickbar

从收藏夹快捷栏访问服务

1. 打开 [AWS 管理控制台](#)。
2. 在收藏夹快捷栏中查看服务和应用程序。

Favorites widget

从“收藏夹”小组件访问收藏项

1. 打开 [AWS 管理控制台](#)。
2. (可选) 添加收藏夹小组件 (如果没有的话) :
 - a. 在控制台主页上选择 +添加小组件按钮。
 - b. 在添加小组件菜单中，使用 :: 图标将收藏夹小组件拖放至控制台主页。
3. 在收藏夹小组件中查看服务和应用程序。

有关小组件的更多信息，请参阅[the section called “使用小组件”](#)。

在中移除收藏夹 AWS 管理控制台

您可以使用服务菜单从收藏夹中移除服务和应用程序。还可以使用搜索栏中的搜索结果页面移除服务。

Services menu

从“服务”菜单中删除收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务。
3. 选择收藏夹。
4. 取消选择服务或应用程序旁边的星号。

Search box

Note

目前，您只能使用搜索栏中的搜索结果页面移除服务。

从搜索框中删除收藏夹

1. 打开 [AWS 管理控制台](#)。
2. 在搜索框中输入一项服务的名称。
3. 在搜索结果页面中，取消选择该服务名称旁边的星号。

在中更改您的密码 AWS 管理控制台

可以根据用户类型和您的权限，从 [AWS 管理控制台](#) 中更改密码。以下主题介绍了如何针对每种用户类型更改密码。

主题

- [中的 root 用户 AWS 管理控制台](#)
- [IAM 用户位于 AWS 管理控制台](#)
- [IAM 身份中心用户位于 AWS 管理控制台](#)
- [中的联邦身份 AWS 管理控制台](#)

中的 root 用户 AWS 管理控制台

根用户可以直接从 AWS 管理控制台中更改密码。Root 用户是拥有所有 AWS 服务和资源的完全访问权限的账户所有者。如果您创建了 AWS 账户，并且使用根用户电子邮件和密码登录，则您是 root 用户。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[根用户](#)。

以根用户身份更改密码

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择您的账户名称。
3. 选择安全凭证。
4. 显示的选项将因您的 AWS 账户类型而异。请按照控制台中显示的说明更改密码。
5. 输入一次您的当前密码，再输入两次新密码。

新密码长度必须至少为 8 个字符，且必须包含以下内容：

- 至少有一个符号
 - 至少有一个数字
 - 至少有一个大写字母
 - 至少有一个小写字母
6. 选择更改密码或保存更改。

IAM 用户位于 AWS 管理控制台

IAM 用户可以 AWS 管理控制台 根据自己的权限从中更改密码。否则，他们必须使用 AWS 访问门户。IAM 用户是您的 AWS 账户中被授予特定自定义权限的身份。如果您没有创建账户，并且您的管理员或帮助台员工向您提供了包括 AWS 账户 ID 或账户别名、IAM 用户名和密码的登录证书，则您就是 IAM 用户。AWS 有关更多信息，请参阅《AWS 登录 用户指南》中的[IAM 用户](#)。

如果您具有以下策略的权限：[AWS：允许 IAM 用户在“安全凭证”页面上更改自己的控制台密码](#)，则可以从控制台更改密码。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的[IAM 用户如何更改自己的密码](#)。

如果您没有更改密码的必要权限，AWS 管理控制台 请参阅《用户指南》中的“[重置 AWS IAM Identity Center 用户密码](#)”AWS IAM Identity Center。

IAM 身份中心用户位于 AWS 管理控制台

AWS IAM Identity Center 用户必须通过 AWS 访问门户更改密码。有关更多信息，请参阅《[AWS IAM Identity Center 用户指南](#)》中的[重置AWS IAM Identity Center 用户密码](#)。

IAM Identity Center 用户是其 AWS 账户的一部分，通过 AWS 访问门户使用唯一 URL 登录的 AWS Organizations 用户。可以直接在 IAM Identity Center 的用户中创建这些用户，也可以在 Active Directory 或其他外部身份提供者中创建这些用户。有关更多信息，请参阅《AWS 登录 用户指南》中的[AWS IAM Identity Center 用户](#)。

中的联邦身份 AWS 管理控制台

联合身份用户必须 AWS 通过访问门户更改密码。有关更多信息，请参阅《[AWS IAM Identity Center 用户指南](#)》中的[重置AWS IAM Identity Center 用户密码](#)。

联合身份用户使用外部身份提供者 (IdP) 登录。如果您符合以下任何一种情况，则您就是联合身份：

- 使用第三方凭证 (例如 Login with Amazon、Facebook 或 Google) 访问您的 AWS 账户或资源。
- 使用相同的凭据登录公司系统和 AWS 服务，然后使用自定义的公司门户进行 AWS 登录。

有关更多信息，请参阅《AWS 登录 用户指南》中的[联合身份](#)。

更改的语言 AWS 管理控制台

该 AWS Console Home 体验包括统一设置页面，您可以在其中更改中 AWS 服务的默认语言 AWS 管理控制台。也可以从导航栏的设置菜单中快速更改默认语言。

Note

以下过程会更改所有 AWS 服务控制台的语言，但不会更改 AWS 文档的语言。要更改文档所用的语言，请使用任何文档页面右上角的语言菜单。

主题

- [支持的语言](#)
- [从导航栏中更改默认语言 AWS 管理控制台](#)
- [通过中的统一设置更改默认语言 AWS 管理控制台](#)

支持的语言

AWS 管理控制台 目前支持以下语言：

- 英语 (美国)
- 英语 (英国)
- 印度尼西亚语
- 德语
- 西班牙语
- 法语
- 日语
- 意大利语
- 葡萄牙语
- 韩语
- 中文 (简体)
- 中文 (繁体)
- 土耳其语

从导航栏中更改默认语言 AWS 管理控制台

以下过程详细介绍了如何直接从导航栏更改默认语言。

从导航栏更改默认语言

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择齿轮图标 (#)。
3. 对于语言，请选择浏览器默认值，或者从下拉列表中选择首选语言。

通过中的统一设置更改默认语言 AWS 管理控制台

以下过程详细介绍了如何从“统一设置”页面更改默认语言。

在“统一设置”中更改默认语言

1. 登录到 [AWS 管理控制台](#)。

2. 在导航栏中，选择齿轮图标 (#)。
3. 要打开统一设置页面，请选择查看所有用户设置。
4. 在统一设置中，选择本地化和默认区域旁边的编辑。
5. 要为控制台选择所需的语言，请选择以下选项之一：
 - 从下拉列表中选择浏览器默认样式，然后选择保存设置。

所有 AWS 服务的控制台文本均以您在浏览器设置中设置的首选语言显示。

Note

浏览器默认仅支持 AWS 管理控制台支持的语言。

- 从下拉列表中选择首选的语言，然后选择保存设置。

所有 AWS 服务的控制台文本均以您的首选语言显示。

访问您的 AWS 账户、组织、服务配额和账单信息 AWS 管理控制台

如果您拥有必要的权限，则可以从控制台访问有关您的 AWS 账户、服务配额、组织和账单信息的信息。

Note

AWS 管理控制台 仅提供对账户、组织、服务配额和账单信息的访问权限。这些服务各有自己的控制台。有关更多信息，请参阅下列内容：

- 在 AWS 账户管理 参考指南中 [@@ 管理您的 AWS 账户](#)。
- [什么是 AWS Organizations ?](#) 在《AWS Organizations 用户指南》中。
- 《服务配额用户指南》中的 [什么是服务配额 ?](#)。
- [使用《AWS 账单用户指南》中的 AWS 账单与成本管理 主页](#)。

Tip

您还可以通过询问 Amazon Q 来获取有关上述任何主题的更多信息。有关更多信息，请参阅 [与 Amazon Q 开发者版聊天](#)。

主题

- [访问中的账户信息 AWS 管理控制台](#)
- [访问中的组织信息 AWS 管理控制台](#)
- [访问中的服务配额信息 AWS 管理控制台](#)
- [访问中的账单信息 AWS 管理控制台](#)

访问中的账户信息 AWS 管理控制台

如果您拥有必要的权限，则可以从控制台访问有关您的 AWS 账户的信息。

访问账户信息

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏上，选择您的账户名称。
3. 选择账户。
4. 查看您的账户信息。

Note

如果您想关闭 AWS 账户，请参阅 [AWS 账户管理 参考指南中的关闭 AWS 账户](#)。

访问中的组织信息 AWS 管理控制台

如果您拥有必要的权限，则可以从控制台访问有关您的 AWS 组织的信息。

访问组织信息

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏上，选择您的账户名称。
3. 选择组织。
4. 查看您的组织信息。

访问中的服务配额信息 AWS 管理控制台

如果您拥有必要的权限，则可以通过控制台访问服务配额信息。

访问服务配额信息

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏上，选择您的账户名称。
3. 选择服务配额。
4. 查看和管理服务配额信息。

访问中的账单信息 AWS 管理控制台

如果您拥有必要的权限，则可以从控制台访问有关您的 AWS 费用的信息。

访问账单信息

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏上，选择您的账户名称。
3. 选择账单和成本管理。
4. 使用 AWS 账单与成本管理 控制面板查找每月支出的摘要和明细。

登录多个账户

在 AWS 管理控制台中的单个 Web 浏览器中，您最多可以同时登录五个不同的身份。这些身份可以是不同账户或同一个账户中的根角色、IAM 角色或联合角色的任意组合。您登录的每个身份都会在新的选项卡中打开其自己的 AWS 管理控制台实例。

启用多会话支持时，控制台 URL 将包含一个子域（例如 <https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1>）。请务必更新书签和控制台链接。

Note

您必须选择加入多会话支持，方法是在 AWS 管理控制台的账户菜单中选择开启多会话，或在 <https://console.aws.amazon.com/> 上选择启用多会话。您可以随时选择退出多会话，方法是在

<https://console.aws.amazon.com/> 上选择禁用多会话，或者清除浏览器 Cookie。选择加入特定于浏览器。

登录多个身份

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏中，选择您的账户名称。
3. 选择添加会话，然后选择登录。将打开一个新的选项卡供您登录。

Note

有关以根用户或 IAM 用户身份登录的更多信息，请参阅《AWS 登录用户指南》中的 [登录到 AWS 管理控制台](#)。

4. 输入您的凭证。
5. 选择登录。AWS 管理控制台将以您选择的 AWS 身份加载到此选项卡中。
6. (可选) 与其它角色一起进行联合身份验证
 - a. 在 AWS IAM Identity Center 访问门户或单点登录 (SSO) 门户中，登录其它角色。
 - b. 在 AWS 管理控制台中，选择您的账户名称。
 - c. 查看您可以选择的其它会话。

AWS 管理控制台中 AWS 建议的操作

AWS 建议的操作通过为完成任务和实施最佳实践提供上下文建议，协助您在 AWS 管理控制台中提高工作效率。当有相关建议可用时，会出现一个动态按钮，您可以使用该按钮根据这些建议快速采取行动。

Note

AWS 建议的操作会分析资源状态以提供建议，但不处理用户数据。

主题

- [AWS 建议的操作的功能](#)

- [使用建议的操作](#)
- [使用记录 AWS 推荐的操作 API 调用 AWS CloudTrail](#)

AWS 建议的操作的功能

- 操作建议：根据资源状态、最佳实践和常见使用模式获取相关建议
- 一键操作：直接从成功消息或资源视图中完成建议的操作
- 集成的右侧面板：访问集成的侧面板，在不中断工作流程的情况下实施建议
- 多服务支持：获取跨多项 AWS 服务的建议

使用建议的操作

使用建议的操作

1. 登录 [AWS 管理控制台](#)。
2. 查找 # 建议的操作按钮。

Note

“建议的操作”按钮可以出现在 AWS 管理控制台中的任何位置，并且只有在建议的操作可用时才可访问。

3. 选择该按钮可查看可用的操作。
4. 直接或通过侧面板运行建议。

使用记录 AWS 推荐的操作 API 调用 AWS CloudTrail

AWS 推荐操作与 [AWS CloudTrail](#) 一项服务集成，该服务提供用户、角色或用户所采取的操作的记录 AWS 服务。CloudTrail 将 AWS 推荐操作的所有 API 调用捕获为事件。捕获的调用包括来自的调用 AWS 管理控制台 以及对 AWS 推荐操作 API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向 AWS 推荐操作发出的请求、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的“[使用 CloudTrail 事件历史记录](#)”。查看活动历史记录不 CloudTrail 收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 [CloudTrailLake](#) 事件数据存储。

AWS 中的推荐操作管理事件 CloudTrail

[管理事件](#) 提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下，CloudTrail 记录管理事件。

AWS 推荐操作将所有 AWS 推荐操作控制平面操作记录为管理事件。

AWS 推荐操作事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 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，因此事件不会按任何特定顺序出现。

以下示例显示了一个演示该操作 CloudTrail 的事件。

```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIAZRZDBEXAMPLE",
    "sessionContext": {
```

```
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROARZDBHEXAMPLE",
      "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
      "accountId": "12345678909",
      "userName": "EXAMPLE"
    },
    "attributes": {
      "creationDate": "2025-09-03T03:52:00Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "action-recommendations.amazonaws.com"
}
```

有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的[CloudTrail 录制内容](#)。

AWS Console Home 在 AWS 管理控制台

本主题介绍如何使用 AWS Console Home，包括如何自定义您的控制台主页。控制台主页是 AWS 管理控制台的主页。首次登录控制台时，您将进入控制台主页。您可以使用小组件和应用程序自定义控制台主页。小组件允许您添加自定义组件，以跟踪有关您的 AWS 服务和资源的信息。应用程序允许您对 AWS 资源和元数据进行分组。您可以使用 myApplications 来管理应用程序。您也可以使用 Console Home 查看所有 AWS 服务的列表并与 Amazon Q 聊天。

主题

- [查看中的所有 AWS 服务 AWS Console Home](#)
- [在中使用小部件 AWS Console Home](#)
- [我的应用程序在 AWS Console Home 做什么？](#)
- [在 AWS Console Home 中与 Amazon Q 开发者版聊天](#)

查看中的所有 AWS 服务 AWS Console Home

您可以从 Console Home 查看所有 AWS 服务的列表并访问其控制台。

访问完整的 AWS 服务列表

1. 登录到 [AWS 管理控制台](#)。
2. 选择汉堡包图标 (☰)，展开控制台主页菜单。
3. 选择所有服务。
4. 选择一项 AWS 服务以导航到其控制台。

在中使用小部件 AWS Console Home

Console Home 控制面板包含一些小部件，用于显示有关您的 AWS 环境的重要信息并提供服务的快捷方式。您可以通过添加和删除小组件、重新排列它们或更改它们的大小来自定义体验。

管理小组件

您可以通过添加和删除小组件、重新排列它们以及调整它们的大小来管理小组件。可以移除默认小组件，然后重新添加。也可以将控制台主页重置为默认布局并请求新的小组件。

添加小组件

1. 在控制台主页控制面板的右上角或右下角，选择 +添加小组件按钮。
2. 选择拖动指示器 [由小组件标题栏左上角的六个垂直点 (⋮) 表示]，然后将其拖到控制台主页控制面板上。

删除小组件

1. 选择省略号 [由小组件标题栏右上角的三个垂直点 (⋮) 表示]。
2. 选择删除小组件。

重新排列小组件

- 选择拖动指示器 [由小组件标题栏左上角的六个垂直点 (⋮) 表示]，然后将小组件拖到控制台主页控制面板上的新位置。

调整小组件大小

- 选择小组件右下角的调整大小图标，然后拖动以调整小组件的大小。

如果您想重新组织和设置小组件，可以将控制台主页控制面板重置为默认布局。这将撤消对控制台主页控制面板布局的更改，并将所有小组件还原为其默认位置和大小。

将页面重置为默认布局

1. 在页面的右上角，选择重置为默认布局按钮。
2. 要确认，请选择重置。

Note

这将撤消您对控制台主页控制面板布局的所有更改。

在控制台主页控制面板中请求新的小组件

1. 从控制台主页控制面板的左下角，选择想要有更多的小组件？那就告诉我们吧！

描述您希望看到的在控制台主页控制面板中添加的小组件。

2. 选择提交。

Note

您的建议会定期受到审查，并可能在将来对 AWS 管理控制台的更新中添加新的小组件。

我的应用程序在 AWS Console Home 做什么？

myApplications 是控制台主页的一个扩展，可帮助您在 AWS 上管理和监控应用程序的成本、运行状况、安全状况和性能。应用程序可让您对资源和元数据进行分组。您可以通过一个视图访问账户中的所有应用程序、所有应用程序的关键指标，以及来自多个服务控制台的成本、安全性和运营指标的概述以及见解 AWS 管理控制台。myApplications 包括以下内容：

- 控制台主页上的应用程序小组件
- 可用于查看应用程序资源成本和安全性调查发现的 myApplications
- 提供成本、性能和安全性调查发现等关键应用程序指标视图的 myApplications 控制面板

主题

- [myApplications 的特征](#)
- [相关服务](#)
- [访问 myApplications](#)
- [定价](#)
- [myApplications 支持的区域](#)
- [myApplications 中的应用程序](#)
- [myApplications 中的资源](#)
- [中的“我的应用程序”控制面板 AWS Console Home](#)

myApplications 的特征

- 创建应用程序 – 创建新应用程序并组织其资源。您的应用程序会自动显示在 MyApplications 中，因此您可以在 AWS 管理控制台、APIs、CLI 和 SDKs 中执行操作。基础设施即代码 (IaC) 是在您

创建应用程序时生成的，可从 myApplications 控制面板进行访问。IaC 可用于 IaC 工具，包括 AWS CloudFormation 和 Terraform。

- 访问您的应用程序 – 通过从 myApplications 小组件进行选择即可快速访问您的任何应用程序。
- 访问您的资源：您可以从“服务”菜单中，通过选择应用程序来快速查看应用程序资源。选择资源后，您将直接进入相关的服务控制台。您在资源表中的位置已保存，因此您可以随时从“服务”菜单继续浏览。
- 比较应用程序指标 – 使用 myApplications 比较应用程序的关键指标，例如多个应用程序的应用程序资源成本和关键安全性调查发现的数量。
- 监控和管理应用程序 — 使用警报、金丝雀和服务级别目标、调查结果和成本趋势 Amazon CloudWatch，评估应用程序的运行状况和性能。AWS Security Hub CSPM AWS Cost Explorer Service您还可以从 AWS Systems Manager中找到计算指标摘要和优化，并管理资源合规性和配置状态。

相关服务

myApplications 使用以下服务：

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS 资源探索器
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- 标签

访问 myApplications

您可以通过在 [AWS 管理控制台](#) 的左侧边栏中选择 myApplications 来访问 myApplications。

定价

MyApplic AWS ations on 不收取额外费用。没有安装费或预先承诺。myApplication 控制面板汇总的底层资源和服务的使用费仍按这些资源的公布费率收取。

myApplications 支持的区域

MyApplications 有以下 AWS 区域版本：

- 美国东部 (俄亥俄州)
- 美国东部 (弗吉尼亚州北部)
- 美国西部 (北加利福尼亚)
- 美国西部 (俄勒冈州)
- 亚太地区 (孟买)
- 亚太地区 (大阪)
- 亚太地区 (首尔)
- 亚太地区 (新加坡)
- 亚太地区 (悉尼)
- 亚太地区 (东京)
- 加拿大 (中部)
- 欧洲地区 (法兰克福)
- 欧洲地区 (爱尔兰)
- 欧洲地区 (伦敦)
- 欧洲地区 (巴黎)
- 欧洲地区 (斯德哥尔摩)
- 南美洲 (圣保罗)

选择加入的区域

默认情况下未启用选择加入区域。您必须手动启用这些区域才能对这些区域使用 myApplications。有关的更多信息 AWS 区域，请参阅[管理 AWS 区域](#)。支持以下选择加入区域：

- 非洲 (开普敦)
- 亚太地区 (香港)

- 亚太地区 (海得拉巴)
- 亚太地区 (雅加达)
- 亚太地区 (墨尔本)
- 欧洲地区 (米兰)
- 欧洲 (西班牙)
- 欧洲 (苏黎世)
- 中东 (巴林)
- 中东 (阿联酋)
- 以色列 (特拉维夫)

myApplications 中的应用程序

应用程序可让您对资源和元数据进行分组。您可以通过创建、载入、查看、编辑或删除应用程序来管理应用程序。还可以创建代码段，以自动向应用程序添加新资源。

Note

您还可以将应用程序添加到收藏夹，以更便于访问。有关更多信息，请参阅 [???](#)。

主题

- [在 myApplications 中创建应用程序](#)
- [在“我的 AppRegistry 应用程序”中载入现有应用程序](#)
- [在 myApplications 中查看应用程序](#)
- [在 myApplications 中编辑应用程序](#)
- [在 myApplications 中删除应用程序](#)
- [在 myApplications 中创建代码段](#)

在 myApplications 中创建应用程序

您可以创建新应用程序，也可以[the section called “载入应用程序”](#)（2023 年 11 月 8 日之前创建），以开始使用 myApplications。创建新应用程序时可以添加资源（通过搜索和选择资源，或通过使用现有标签）。

创建新应用程序

1. 登录到 [AWS 管理控制台](#)。
2. 展开左侧边栏并选择 myApplications。
3. 选择创建应用程序。
4. 输入应用程序的名称。
5. (可选) 输入应用程序的描述。
6. (可选) 添加[标签](#)。标签是应用于资源的键值对，用于保存有关该资源的元数据。

Note

AWS 应用程序标签会自动应用于新创建的应用程序。有关更多信息，请参阅 [《AWS Service Catalog AppRegistry 管理员指南》](#) 中的 [AWS 应用程序标签](#)。

7. (可选) 添加[属性组](#)。您可以使用属性组来存储应用程序元数据。
8. 选择下一步。
9. (可选) 添加资源：

Search and select resources

Note

要搜索和添加资源，必须开启 AWS 资源探索器。有关更多信息，请参阅 [入门 AWS 资源探索器](#)。

所有添加的资源都使用 AWS 应用程序标签进行标记。

使用搜索功能添加资源

1. 选择搜索和选择资源。
2. 选择选择资源。
3. (可选) 选择[视图](#)。
4. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

Note

如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的[资源探索器搜索问题排查](#)。

5. 选中要添加的资源旁的复选框。
6. 选择添加。
7. 选择下一步。
8. 查看您的选择。

Automatically add resources using tags

创建应用程序时，可以通过指定现有的标签键值对来批量载入资源。使用此方法，AWS 会自动将awsApplication标签应用于所有使用指定键值对标记的资源，并在默认情况下为应用程序的资源创建标签同步。启用标签同步后，任何使用指定标签键值对标记的资源都将自动添加到应用程序中。有关解决标签同步错误的信息，请参阅[the section called “在 myApplications 中解决标签同步错误”](#)。

Note

使用标签向应用程序添加资源需要创建 AppRegistry 应用程序、对资源进行分组和取消分组以及标记和取消标记资源的权限。您可以添加 Resource Groups [ResourceGroupsTaggingAPITagUntagSupportedResources](#) AWS 托管策略，也可以创建和维护自己的自定义策略。必须在 IAM 中将以下权限添加到用户的策略声明中。

- servicecatalog:CreateApplication
- resource-groups:GroupResources
- resource-groups:UngroupResources
- tag:TagResources
- tag:UntagResources

使用现有标签添加资源

1. 选择使用标签自动添加资源。
2. 选择现有的标签键和值：
 - a. 选择用于标记资源的角色。有关更多信息，请参阅《S AWS ervice Catalog AppRegistry 管理员 [指南](#)》中的[标签同步所需权限](#)。
 - b. 选择一个标签键。
 - c. 选择一个标签值。
 - d. （可选）选择预览资源以预览使用该标签键值对标记的资源。
 - e. 查看并接受我确认将启用“组生命周期事件”以创建标签同步通知。GLE AWS 允许注意到用您的键值对标记的资源的更改。
3. 选择下一步。
4. 查看您的应用程序详细信息、选定的标签键值对，以及将添加到应用程序中的资源的预览。

Note

默认情况下，使用现有标签键值对创建应用程序会创建标签同步。设置完成后，标签同步还会持续管理应用程序的资源，添加或删除已使用指定键值对标记或取消标记的资源。您可以从应用程序的“管理资源”页面管理标签同步。

10. 如果要关联堆 CloudFormation 栈，请选中页面底部的复选框。

Note

向应用程序添加 CloudFormation 堆栈需要更新堆栈，因为添加到应用程序的所有资源都标有 AWS 应用程序标签。在此更新后，堆栈上次更新后执行的手动配置可能不会反映出来。这可能会导致停机或其他应用程序问题。有关更多信息，请参阅《CloudFormation 用户指南》中的[堆栈资源的更新行为](#)。

11. 选择创建应用程序。

在“我的 AppRegistry 应用程序”中载入现有应用程序

您可以载入在 2023 年 11 月 8 日之前创建的现有 AppRegistry 应用程序，开始使用 MyApplications。

载入现有 AppRegistry 应用程序

1. 登录到 [AWS 管理控制台](#)。
2. 在左侧边栏中，选择 myApplications。
3. 使用搜索栏查找应用程序。
4. 选择您的应用程序。
5. 选择“登机” **application name**。
6. 如果要关联 CloudFormation 堆栈，请选中警报框中的复选框。
7. 选择载入应用程序。

在 myApplications 中查看应用程序

您可以从 myApplications 或“服务”菜单中查看您的应用程序。如果从 MyApplications 查看应用程序，则可以在卡片 AWS 区域 或表格视图中查看全部或特定应用程序 AWS 区域 及其相关信息。

Note

您还可以从“收藏夹”菜单中查看添加到收藏夹的应用程序。有关更多信息，请参阅 [中的最爱 AWS 管理控制台](#)。

myApplications

在 myApplications 中查看应用程序

1. 打开 [AWS 管理控制台](#)。
2. 在左侧边栏中，选择 myApplications。
3. 在区域中，选择当前区域或支持的区域。
4. 要查找特定应用程序，请在搜索栏中输入其名称、关键字或描述。
5. （可选）默认视图是卡片视图。要自定义您的应用程序页面，请执行以下操作：
 - a. 选择齿轮图标。
 - b. （可选）选择页面大小。

- c. (可选) 选择卡片视图或表格视图。
- d. (可选) 选择页面大小。
- e. (可选) 如果使用表格视图，请选择表格视图的属性。
- f. (可选) 切换哪些应用程序属性可见及其显示顺序。
- g. 选择确认。

Services menu

从“服务”菜单中查看应用程序

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务 (⋮)。
3. 选择所有应用程序。
4. 选择应用程序。
5. (可选) 选择[视图](#)。
6. (可选) 选择筛选条件。您可以按属性或标签筛选资源。有关更多信息，请参阅《AWS 资源探索器 用户指南》中的[资源探索器的搜索查询语法参考](#)。
7. (可选) 选择一个资源以在相关的服务控制台中查看该资源。

Tip

您可以通过选择服务 (⋮) 继续从中断处浏览资源。您应用的搜索筛选条件也将保留。


在 myApplications 中编辑应用程序

将打开编辑您的应用程序 AppRegistry，以便您可以更新其描述。您还可以 AppRegistry 使用编辑应用程序的标签和属性组。

编辑应用程序

1. 打开 [AWS 管理控制台](#)。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 选择要编辑的应用程序。
4. 在 myApplication 控制面板上，选择操作，然后选择编辑应用程序。

5. 在编辑应用程序中，对应用程序的描述、标签和属性组进行所需的更改。


 Note

有关管理标签和属性组的更多信息，请参阅《AWS Service Catalog AppRegistry 管理员指南》中的[管理标签](#)和[编辑属性组](#)。

6. 选择更新。

在 myApplications 中删除应用程序

您可以删除不再需要的应用程序。在删除应用程序之前，请确保移除并非由 AWS 服务创建的所有关联资源共享和属性组。

 Note

删除应用程序不会影响您的资源。标有 AWS 应用程序标签的资源将保持标记状态。

删除 应用程序

1. 打开 [AWS 管理控制台](#)。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 选择要删除的应用程序。
4. 在 myApplication 控制面板上，选择操作。
5. 选择删除应用程序。
6. 选择删除角色，然后确认删除。

在 myApplications 中创建代码段

myApplications 会为您的所有应用程序创建代码段。您可以使用代码段，通过基础设施即代码 (IaC) 工具将新创建的资源自动添加到应用程序中。所有添加的资源都使用 AWS 应用程序标签进行标记，以将其与您的应用程序关联。

为应用程序创建代码段

1. 打开 [AWS 管理控制台](#)。

2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择操作。
5. 选择获取代码段。
6. 选择代码段类型。
7. 选择复制将代码复制到剪贴板。
8. 将代码粘贴到 IaC 工具中。

myApplications 中的资源

在中 AWS，资源是您可以使用的实体。示例包括 Amazon EC2 实例、AWS CloudFormation 堆栈或 Amazon S3 存储桶。您可以在 myApplications 中管理资源（通过在应用程序中添加和删除资源）。

主题

- [在 myApplications 中添加资源](#)
- [在 myApplications 中移除资源](#)
- [在 myApplications 中查看资源](#)

在 myApplications 中添加资源

向应用程序添加资源使您能够对它们进行分组并管理其安全性、性能和合规性。您可以通过搜索和选择资源，或通过使用现有标签并执行标签同步，向现有应用程序添加资源。

Search and select resources

搜索和选择资源

1. 打开 [AWS 管理控制台](#)。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择管理资源。
5. 选择添加资源。
6. （可选）选择[视图](#)。
7. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

Note

如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的[资源探索器搜索问题排查](#)。

8. 选中要添加的资源旁的复选框。
9. 选择添加。

Automatically add resources using tags

创建应用程序时，可以通过指定现有的标签键值对来批量载入资源。使用此方法，AWS 会自动将awsApplication标签应用于所有资源，并在默认情况下为应用程序的资源创建标签同步。启用标签同步后，任何使用指定标签键值对标记的资源都将自动添加到应用程序中。

使用现有标签添加资源

1. 打开 [AWS 管理控制台](#)。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 选择管理资源。
4. 选择创建标签同步。
5. 选择现有的标签键和值：
 - a. 选择用于标记资源的角色。有关更多信息，请参阅《S AWS ervice Catalog AppRegistry 管理员指南》中的[标签同步任务所需权限](#)。
 - b. 选择一个标签键。
 - c. 选择一个标签值。
 - d. 查看并接受我确认将启用“组生命周期事件”以创建标签同步通知。GLE AWS 允许注意到用您的键值对标记的资源的更改。
6. 选择创建标签同步。

在 myApplications 中解决标签同步错误

本节介绍常见的标签同步错误以及如何解决这些错误。尝试解决错误后，您可以重试失败的标签同步任务。

- 权限不足 — 您不具有启动、更新或取消标签同步所需的最低权限。有关更多信息，请查看[标签同步所需权限](#)。确保指定用于执行标签同步的角色具有所需的最低权限后，请重试失败的标签同步任务。
- 已存在 — 应用程序已存在带有此标签键值对的任务。一个应用程序可以支持多个标签同步，但是每个标签同步必须具有不同的标签键值对。指定不同的标签键值对后，请重试失败的标签同步任务。
- 已达到最大限制 — 您已达到每个账户 100 个标签同步任务的上限（所有应用程序）。

在 myApplications 中移除资源

您可以移除资源以取消它们与应用程序的关联。

移除资源

1. 打开 [AWS 管理控制台](#)。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择管理资源。
5. （可选）选择[视图](#)。
6. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

Note

如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的[资源探索器搜索问题排查](#)。

7. 选择移除。
8. 通过选择移除资源，确认您要移除该资源。

在 myApplications 中查看资源

您可以从 myApplications 和服务菜单中查看您的应用程序资源。

myApplications

在 myApplications 中查看您的资源

1. 打开 [AWS 管理控制台](#)。
2. 展开左侧边栏并选择 myApplications。

3. 选择应用程序。
4. 在资源小组件中，查看您的资源。

Services menu

从“服务”菜单中查看应用程序

1. 打开 [AWS 管理控制台](#)。
2. 在导航栏中，选择服务 (⋮)。
3. 选择所有应用程序。
4. 选择应用程序。
5. (可选) 选择[视图](#)。
6. (可选) 选择筛选条件。您可以按属性或标签筛选资源。有关更多信息，请参阅《AWS 资源探索器 用户指南》中的[资源探索器的搜索查询语法参考](#)。
7. (可选) 选择一个资源以在相关的服务控制台中查看该资源。

Tip

您可以通过选择服务 (⋮) 继续从中断处浏览资源。您应用的搜索筛选条件也将保留。

中的“我的应用程序”控制面板 AWS Console Home

您创建或载入的每个应用程序都有自己的 myApplications 控制面板。MyApplications 仪表板包含成本、安全和操作小部件，可显示来自多个 AWS 服务的见解。您可以对每个小组件执行收藏、重新排序、移除或调整大小操作。有关更多信息，请参阅 [在中使用小部件 AWS Console Home](#)。

主题

- [应用程序控制面板设置小组件](#)
- [应用程序摘要小组件](#)
- [计算小组件](#)
- [成本和使用情况小组件](#)
- [AWS 安全控件](#)
- [AWS 弹性控件](#)
- [资源小组件](#)

- [DevOps 小部件](#)
- [监控和运维小组件](#)
- [标签小组件](#)

应用程序控制面板设置小组件

此小组件包含建议的入门活动列表，您可以使用这些活动来帮助您 AWS 服务 进行配置以管理应用程序资源。

应用程序摘要小组件

此小组件显示应用程序的名称、描述和 [AWS 应用程序标签](#)。您可以在基础设施即代码 (IAC) 中访问和复制应用程序标签以手动标记资源。

计算小组件

此小组件显示您添加到应用程序中的计算资源的信息和指标。这包括警报总数和计算资源类型总数。该小组件还显示了 Amazon EC2 实例 CPU 利用率和 Lambda 调 Amazon CloudWatch 用的资源性能指标趋势图。

配置计算小组件

要在计算小组件中填充数据，请为您的应用程序设置至少一个 Amazon EC2 实例或一个 Lambda 函数。有关更多信息，请参阅 [Amazon Elastic Compute Cloud 文档](#)和《AWS Lambda 开发人员指南》中的 [Lambda 入门](#)。

成本和使用情况小组件

此小组件显示您的应用程序资源 AWS 的成本和使用情况数据。您可以使用这些数据来比较每月成本并按 AWS 服务查看成本明细。此小组件仅汇总标有 AWS 应用程序标签的资源成本，不包括税费、费用和其他与资源没有直接关联的共享成本。显示的费用未混合，至少每 24 小时更新一次。For 更多信息，请参阅《AWS Cost Management 用户指南》AWS 资源探索器中的“使用 [分析成本](#)”。

配置成本和使用情况小组件

要配置“成本和使用情况”微件，请 AWS Cost Explorer Service 为您的应用程序和账户启用。这项服务不收取额外费用，也没有安装费或预先承诺。有关更多信息，请参阅《AWS Cost Management User Guide》中的 [Enabling Cost Explorer](#)。

AWS 安全控件

此小组件显示来自应用程序 AWS 安全性的安全调查结果。AWS Security 为您的应用程序提供了全面的安全发现视图 AWS。您可以按严重性访问最近的高优先级调查发现，监控其安全状况，访问最近的关键或高严重性调查发现，并深入了解后续步骤。有关更多信息，请参阅 [AWS Security Hub CSPM](#)。

配置“AWS 安全”微件

要配置“AWS 安全”小组件，请 AWS Security Hub CSPM 为您的应用程序和帐户进行设置。有关更多信息，请参阅[什么是 AWS Security Hub CSPM ?](#) 在《AWS Security Hub CSPM 用户指南》中。有关定价信息，请参阅《AWS Security Hub CSPM User Guide》中的 [AWS Security Hub CSPM free trial, usage, and pricing](#)。

AWS Security Hub CSPM 需要您配置 AWS Config 录制。该服务提供与您的 AWS 账户关联的资源 的详细视图。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 [AWS Systems Manager](#)。

AWS 弹性控件

此控件显示来自 Resilience Hub 的应用程序 AWS 弹性详细信息。启动评估后，R AWS esiliency Hub 会根据预定义的弹性策略评估应用程序的资源，从而分析应用程序的弹性状况。您可以访问韧性得分、策略违规、策略偏移、资源偏移以及韧性得分历史记录等指标。系统每天都会对应用程序进行评测以增强跟踪，但可以随时禁用此功能。有关更多信息，请参阅 [AWS Resilience Hub](#)。有关定价信息，请参阅 [AWS Resilience Hub 定价](#)。

配置“AWS 弹性”微件

要配置“AWS 弹性”微件，请添加应用程序。有关更多信息，请参阅[什么是 AWS Resilience Hub ?](#) 在《AWS Resilience Hub 用户指南》中。

资源小组件

此控件使用 AWS 资源管理器在视图中显示您已添加到应用程序中的资源。您还可以使用此小组件，使用资源元数据（如名称、标签和）来搜索或筛选资源 IDs。有关更多信息，请参阅 [AWS 资源探索器](#)。

配置资源小组件

要配置资源小组件，请使用资源探索器载入。有关更多信息，请参阅《AWS 资源探索器用户指南》中的[资源探索器入门](#)。

DevOps 小部件

此小组件显示运维洞察，使您可以评估合规性并对应用程序采取行动。这些洞察包括：

- 实例集管理
- 状态管理
- 补丁管理
- 配置和 OpsItems 管理

配置 DevOps 小部件

要配置 DevOps 微件，请 AWS Systems Manager OpsCenter 为您的应用程序和帐户启用。有关更多信息，请参阅 [Systems Manager Explorer 入门](#) 和 [OpsCenter](#) 《AWS Systems Manager 用户指南》。启用 OpsCenter AWS Systems Manager Explorer 允许配置 AWS Config 和 Amazon CloudWatch 以便 OpsItems 根据常用的规则和事件自动创建其事件。有关更多信息，请参阅《AWS Systems Manager 用户指南》OpsCenter 中的 [设置](#)。

您可以将实例配置为让 Systems Manager 代理运行并应用权限以启用补丁扫描。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 [AWS Systems Manager Quick Setup](#)。

您还可以通过设置补丁管理器为您的应用程序设置自动修补 Amazon EC2 实例。AWS Systems Manager 有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 [使用 Quick Setup 补丁策略](#)。

有关定价信息，请参阅 [AWS Systems Manager 定价](#)。

监控和运维小组件

此小组件显示：

- 与应用程序关联的资源的警报和提醒
- 应用程序服务级别目标 (SLOs) 和指标
- 可用 AWS 应用程序信号指标

配置监控和运维小组件

要配置“监控和操作”微件，请在您的 AWS 帐户中创建 CloudWatch 警报和金丝雀。有关更多信息，请参阅《[亚马逊 CloudWatch 用户指南](#)》中的“[使用亚马逊 CloudWatch 警报](#)”和“[创建金丝雀](#)”。有关

CloudWatch 警报和合成金丝雀定价，请分别参阅 [Amazon CloudWatch 定价](#) 和 [AWS 云运营和迁移博客](#)。

有关 CloudWatch 应用程序信号的更多信息，请参阅《[亚马逊 CloudWatch 用户指南](#)》中的“[启用亚马逊 CloudWatch 应用程序信号](#)”。

标签小组件

此小组件显示与您的应用程序关联的所有标签。您可以使用此小组件来跟踪和管理应用程序元数据（重要程度、环境、成本中心）。有关更多信息，请参阅[什么是标签？](#)在《[标记 AWS 资源的最佳实践](#)》AWS 白皮书中。

在 AWS Console Home 中与 Amazon Q 开发者版聊天

Amazon Q 开发者版是一款由生成式人工智能（AI）提供支持的对话式助手，可为您理解、构建、扩展和操作 AWS 应用程序提供帮助。您可以向 Amazon Q 询问任何有关 AWS 的问题，包括 AWS 架构、您的 AWS 资源、最佳实践、文档等方面的问题。还可以创建支持案例并获得实时座席的帮助。有关更多信息，请参阅《[Amazon Q 开发者版指南](#)》中的[什么是 Amazon Q？](#)。

开始使用 Amazon Q

可以在 AWS 管理控制台、AWS 文档网站、AWS 网站或 AWS 控制台移动应用程序中通过选择六角形 Amazon Q 图标开始与 Amazon Q 聊天。有关更多信息，请参阅《[Amazon Q 开发者版用户指南](#)》中的[开始使用 Amazon Q 开发者版](#)。

问题示例

以下是可以询问 Amazon Q 的一些示例问题：

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

AWS 管理控制台 私密访问权限

AWS 管理控制台 私人访问是一项高级安全功能，用于控制对您的访问 AWS 管理控制台。控制台私有访问可用于防止用户从您的网络中登录到意外的 AWS 账户。使用此功能，当流量来自您的网络内部 AWS 账户时，您可以将访问权限限制为 AWS 管理控制台 仅限于一组已知的指定人群。如果您要确保所有来自的呼叫都来自您的网络内部和 AWS 管理控制台 允许 AWS 服务 的帐户，则控制台私有访问也非常有用。

主题

- [支持的 AWS 区域、服务控制台和私有访问功能](#)
- [AWS 管理控制台 私人访问安全控制概述](#)
- [所需的 VPC 端点和 DNS 配置](#)
- [实施服务控制策略和 VPC 端点策略](#)
- [实施基于身份的策略和其他策略类型](#)
- [试试 AWS 管理控制台 私密访问](#)
- [参考架构](#)

支持的 AWS 区域、服务控制台和私有访问功能

AWS 管理控制台 私有访问仅支持部分区域和 AWS 服务。不受支持的服务控制台在 AWS 管理控制台中将处于非活动状态。此外，在使用 AWS 管理控制台 私有访问权限时，某些 AWS 管理控制台 功能可能会被禁用，例如，统一设置中的[默认区域](#)选择。

支持以下区域和服务控制台。

支持的区域：

- 美国东部 (俄亥俄州)
- 美国东部 (弗吉尼亚州北部)
- 美国西部 (北加利福尼亚)
- 美国西部 (俄勒冈州)
- 亚太地区 (海得拉巴)
- 亚太地区 (孟买)

- 亚太地区 (首尔)
- 亚太地区 (大阪)
- 亚太地区 (新加坡)
- 亚太地区 (悉尼)
- 亚太地区 (马来西亚)
- 亚太地区 (泰国)
- 亚太地区 (东京)
- 加拿大 (中部)
- 欧洲地区 (法兰克福)
- 欧洲地区 (爱尔兰)
- 欧洲地区 (伦敦)
- 欧洲地区 (巴黎)
- 欧洲地区 (斯德哥尔摩)
- 南美洲 (圣保罗)
- 非洲 (开普敦)
- 亚太地区 (香港)
- 亚太地区 (雅加达)
- 亚太地区 (墨尔本)
- 加拿大西部 (卡尔加里)
- 墨西哥 (中部)
- 欧洲地区 (米兰)
- 欧洲 (西班牙)
- 欧洲 (苏黎世)
- 中东 (巴林)
- 中东 (阿联酋)
- 以色列 (特拉维夫)

支持的服务控制台

- Amazon API Gateway

- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS 账单与成本管理
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Control Tower
- Amazon DataZone

- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 全局视图
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS 弹性灾难恢复
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- 亚马逊 GameLift 服务器
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS IAM Identity Center

- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- 适用于 Apache Flink 的亚马逊托管服务
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- AWS Migration Hub 策略建议
- Amazon MQ
- 网络访问分析器
- AWS Network Firewall
- AWS Network Manager
- 亚马逊 OpenSearch 服务
- AWS Organizations
- AWS 私有证书颁发机构
- Public Health Dashboard
- Amazon Rekognition
- Amazon Relational Database Service

- AWS Resource Access Manager
- AWS Resource Groups 和标签编辑器
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver 域名防火墙
- Amazon S3 on Outposts
- Amazon SageMaker
- 亚马逊 SageMaker Runtime
- 亚马逊 SageMaker AI 合成数据
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- 服务配额
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- 支持
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- 统一设置
- Amazon VPC IP 地址管理器
- Amazon Virtual Private Cloud

- Amazon WorkSpaces 瘦客户端

AWS 管理控制台 私人访问安全控制概述

AWS 管理控制台 来自您的网络的账号限制

AWS 管理控制台 当您希望将 AWS 管理控制台 来自网络的访问权限限制为组织中已知 AWS 账户 的指定集合时，私有访问非常有用。这样，您可以防止用户从您的网络内登录到意外的 AWS 账户。您可以使用 AWS 管理控制台 VPC 端点策略实现这些控制。有关更多信息，请参阅 [实施服务控制策略和 VPC 端点策略](#)。

从您的网络到互联网的连接

要访问使用的资产，例如静态内容（、CSS AWS 管理控制台 JavaScript、图像）以及所有 AWS 服务 未由启用的资产，仍需要您的网络连接[AWS PrivateLink](#)。有关使用的顶级域的列表 AWS 管理控制台，请参阅[问题排查](#)。

Note

目前，AWS 管理控制台 私有访问不支持 `status.aws.amazon.com`、`health.aws.amazon.com`、和等端点 `docs.aws.amazon.com`。您需要将这些域路由到公共互联网。

所需的 VPC 端点和 DNS 配置

AWS 管理控制台 私有访问每个区域需要以下两个 VPC 终端节点。*region* 替换为您自己的地区信息。

1. `com.amazonaws.region.console` 为 AWS 管理控制台
2. `com.amazonaws.region.sign` for AWS 登录

Note

始终为美国东部（弗吉尼亚州北部）（`us-east-1`）区域预调配基础设施和网络连接，而与用于 AWS 管理控制台的其他区域无关。您可以使用 AWS Transit Gateway 设置美国东部（弗

吉尼亚州北部) 与每个其它区域之间的连接。有关更多信息, 请参阅《Amazon VPC Transit Gateway 指南》中的[开始使用中转网关](#)。您也可以使用 Amazon VPC 对等连接。有关更多信息, 请参阅《Amazon VPC 对等连接指南》中的[什么是 VPC 对等连接](#)。要比较这些选项, 请参阅《[亚马逊虚拟私 VPC-to-AWS 有云连接选项](#)》白皮书中的 Amazon VPC 连接选项。

主题

- [DNS AWS 管理控制台 和的配置 AWS 登录](#)
- [VPC 终端节点和 AWS 服务DNS配置 AWS 管理控制台](#)

DNS AWS 管理控制台 和的配置 AWS 登录

要将您的网络流量路由到相应的 VPC 端点, 请在您的用户将从中访问 AWS 管理控制台的网络中配置 DNS 记录。这些 DNS 记录会将您的用户浏览器流量引导至您创建的 VPC 端点。

您可以创建单个托管区。但是, 诸如 `health.aws.amazon.com` 和 `docs.aws.amazon.com` 之类的端点将无法访问, 因为它们没有 VPC 端点。您需要将这些域路由到公共互联网。我们建议您为每个区域创建两个私有托管区 (一个用于 `signin.aws.amazon.com`, 一个用于 `console.aws.amazon.com`) 以及以下 CNAME 记录:

- 登录
 - `region.signin.aws.amazon.com` 指向登录区域中的 AWS 登录 VPC 终端节点, DNS 其中是所需的区域 `region`
 - `signin.aws.amazon.com` 指向美国东部 (弗吉尼亚北部) 的 AWS 登录 VPC 终端节点 (us-east-1)
- 控制台
 - `region.console.aws.amazon.com` 指向 DNS 控制台区域中的 AWS 管理控制台 VPC 终端节点, 其中是所需的区域 `region`
 - *. `region.console.aws.amazon.com` 指向 DNS 控制台区域中的 AWS 管理控制台 VPC 终端节点, 其中是所需的区域 `region`
 - *. `region.console.aws.amazon.com` 指向控制台区域中的 AWS 管理控制台 VPC 终端节点 DNS
 - 仅针对美国东部 (弗吉尼亚州北部) 区域的无区域 CNAME 记录。您必须始终设置美国东部 (弗吉尼亚州北部) 区域。
 - `signin.aws.amazon.com` 指向美国东部 (弗吉尼亚北部) 的 VP AWS 登录 C 终端节点 (us-east-1)

- *.console.aws.amazon.com 指向美国东部 (弗吉尼亚北部) AWS 管理控制台的 VPC 终端节点 (us-east-1)

有关创建 CNAME 记录的说明，请参阅《Amazon Route 53 开发人员指南》中的[处理记录](#)。

一些 AWS 游戏机 (包括 Amazon S3) 的 DNS 名称使用不同的模式。下面是两个示例：

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

为了能够将此流量定向到您的 AWS 管理控制台 VPC 终端节点，您需要单独添加这些名称。我们建议您为所有端点配置路由，以获得完全私密的体验。但是，使用 AWS 管理控制台私有访问权限并不是必需的。

以下 json 文件包含要按区域配置的 AWS 服务完整列表和控制台终端节点。使用 com.amazonaws.*region*.console 端点下方的 PrivateIpv4DnsNames 字段作为 DNS 名称。

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ilcentral-1.config.json>

Note

随着我们向 AWS 管理控制台私有访问的范围中添加其他端点，此列表每月都会更新。要保持更新您的私有托管区，请定期提取前面的文件列表。

如果你使用 Route 53 来配置你的 DNS，请前往 <https://console.aws.amazon.com/route53/v2/hostedzones#验证设置>。DNS 对于 Route 53 中的每个私有托管区，验证是否存在以下记录集。

- console.aws.amazon.com
- signin.aws.amazon.com
- *。*region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *。*region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- 先前列出的 JSON 文件中存在的其他记录

VPC 终端节点和 AWS 服务 DNS 配置 AWS 管理控制台

AWS 服务 通过直接浏览器请求和由 Web 服务器代理的请求组合进行的 AWS 管理控制台 调用。要将此流量定向到您的 AWS 管理控制台 VPC 终端节点，您必须添加 VPC 终端节点 DNS 并为每项依赖 AWS 服务进行配置。

以下 json 文件列出了可供您 AWS 服务 使用的 AWS PrivateLink 支持文件。如果服务未与集成 AWS PrivateLink，则不会将其包含在这些文件中。

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>

- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ilcentral-1.config.json>

对于要添加到 VPC 的相应服务的 VPC 端点使用 `ServiceName` 字段。

Note

随着我们增加对更多服务控制台的 AWS 管理控制台 私有访问的支持，我们每个月都会更新此列表。为了保持最新状态，请定期提取前面的文件列表并更新您的 VPC 端点。

实施服务控制策略和 VPC 端点策略

您可以使用服务控制策略 (SCPs) 和 VPC 终端节点策略进行 AWS 管理控制台 私有访问，以限制允许 AWS 管理控制台 从您的 VPC 及其连接的本地网络中使用的一组账户。

主题

- [将 AWS 管理控制台 私有访问权限与 AWS Organizations 服务控制策略配合使用](#)
- [仅允许 AWS 管理控制台 用于预期的账户和组织 \(可信身份\)](#)

将 AWS 管理控制台 私有访问权限与 AWS Organizations 服务控制策略配合使用

如果您的 AWS 组织正在使用允许特定服务的服务控制策略 (SCP)，则必须添加 `signin:*` 允许的操作。之所以需要此权限，是因为 AWS 管理控制台 通过私有访问 VPC 终端节点登录会执行 IAM 授权，SCP 会在未经许可的情况下阻止该授权。例如，以下服务控制策略允许在组织中使用 Amazon EC2 和 CloudWatch 服务，包括使用 AWS 管理控制台 私有访问终端节点访问它们的时间。

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  ],
  "Resource": "*"
}
```

```
}
```

有关的更多信息 SCPs，请参阅《AWS Organizations 用户指南》中的[服务控制策略 \(SCPs\)](#)。

仅允许 AWS 管理控制台 用于预期的账户和组织 (可信身份)

AWS 管理控制台 并 AWS 登录 支持专门控制登录账户身份的 VPC 终端节点策略。

与其它 VPC 端点策略不同，该策略在身份验证之前进行评估。因此，它专门控制登录和使用经过身份验证的会话，而不控制会话采取的任何 AWS 特定于服务的操作。例如，当会话访问 AWS 服务控制台（例如 Amazon EC2 控制台）时，将不会根据为显示该页面而采取的 Amazon EC2 操作来评估这些 VPC 终端节点策略。相反，您可以使用与已登录的 IAM 委托人关联的 IAM 策略来控制其服务操作权限。AWS

Note

AWS 管理控制台 和 VPC 终端节点的 SignIn VPC 终端节点策略仅支持有限的策略公式子集。每个 Principal 和 Resource 均应设置为 *，而 Action 应设置为 * 或 signin:*。您可以使用 aws:PrincipalOrgId 和 aws:PrincipalAccount 条件键控制对 VPC 端点的访问。

建议对控制台和 SignIn VPC 终端节点使用以下策略。

此 VPC 终端节点策略允许 AWS 账户 在指定 AWS 组织中登录并阻止登录任何其他账户。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxxx"
        }
      }
    }
  ]
}
```

```
    }
  }
]
}
```

此 VPC 终端节点策略将登录限制为特定账户，AWS 账户 并禁止登录任何其他账户。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

在登录时会对限制 AWS 账户 或组织使用 AWS 管理控制台 和登录 VPC 终端节点的策略进行评估，并定期针对现有会话进行重新评估。

实施基于身份的策略和其他策略类型

您可以 AWS 通过创建策略并将其附加到 IAM 身份（用户、用户组或角色）或 AWS 资源来管理中的访问权限。本页介绍策略与 AWS 管理控制台 私有访问权限配合使用时的工作原理。

支持的 AWS 全局条件上下文密钥

AWS 管理控制台 私有访问不支持 `aws:SourceVpce` 和 `aws:VpcSourceIp` AWS 全局条件上下文密钥。在使用 AWS 管理控制台 私有访问时，您可以在策略中改用 `aws:SourceVpc` IAM 条件。

AWS 管理控制台 私有访问权限如何与 aws 配合使用：SourceVpc

本节介绍由您生成的请求 AWS 管理控制台 可以进入的各种网络路径 AWS 服务。通常，AWS 服务控制台是通过直接浏览器请求和由 AWS 管理控制台 Web 服务器代理的请求混合实现的。AWS 服务这些实现可能会发生变化，恕不另行通知。如果您的安全要求包括 AWS 服务使用 VPC 终端节点进行访问，我们建议您为打算从 VPC 使用的所有服务（无论是直接使用还是通过 AWS 管理控制台 私有访问）配置 VPC 终端节点。此外，您必须在 `aws:SourceVpc` 策略中使用 IAM 条件，而不是在 AWS 管理控制台 私有访问权限功能中使用特定 `aws:SourceVpc` 值。本节提供有关不同网络路径的工作原理的详细信息。

用户登录后 AWS 管理控制台，他们 AWS 服务 通过直接浏览器请求和由 AWS 管理控制台 Web 服务器代理到服务器的请求的组合向 AWS 发出请求。例如，CloudWatch 图形数据请求是从浏览器发出的。而某些 AWS 服务控制台请求（例如 Amazon S3）则由 Web 服务器代理到 Amazon S3。

对于直接的浏览器请求，使用 AWS 管理控制台 私有访问权限不会有任何改变。与以前一样，请求通过 VPC 已配置为到达 `monitoring.region.amazonaws.com` 的任何网络路径到达服务。如果 VPC 配置了 VPC 终端节点 `com.amazonaws.region.monitoring`，则请求将 CloudWatch 通过该 CloudWatch VPC 终端节点到达。如果没有 VPC 终端节点 CloudWatch，则请求将通过 VPC CloudWatch 上的 Internet Gateway 到达其公有终端节点。CloudWatch 通过 CloudWatch VPC 终端节点到达的请求将具有 IAM 条件 `aws:SourceVpc` 并 `aws:SourceVpc` 设置为各自的值。那些 CloudWatch 通过其公共端点到达的用户将 `aws:SourceIp` 设置为请求的源 IP 地址。有关这些 IAM 条件键的更多信息，请参阅《IAM 用户指南》中的 [全局条件键](#)。

对于由 AWS 管理控制台 Web 服务器代理的请求，例如 Amazon S3 控制台在您访问 Amazon S3 控制台时发出的列出您的存储桶的请求，则网络路径会有所不同。这些请求不是从您的 VPC 发起的，因此不使用您可能已在 VPC 上为该服务配置的 VPC 端点。在这种情况下，即使您具有用于 Amazon S3 的 VPC 端点，您的会话向 Amazon S3 发出的旨在列出存储桶的请求也不会使用 Amazon S3 VPC 端点。但是，当您对支持的服务使用 AWS 管理控制台 私有访问权限时，这些请求（例如，对 Amazon S3 的请求）将在其请求上下文中包含 `aws:SourceVpc` 条件密钥。`aws:SourceVpc` 条件密钥将设置为部署用于登录和控制台的 AWS 管理控制台 私有访问终端节点的 VPC ID。因此，如果您在基于身份的策略中使用 `aws:SourceVpc` 限制，则必须添加用于托管 AWS 管理控制台 私有访问登录和控制台端点的此 VPC 的 VPC ID。`aws:SourceVpc` 条件将设置为相应的登录或控制台 VPC 终端节点 IDs。

Note

如果您的用户要求访问 AWS 管理控制台 私有访问不支持的服务控制台，则必须在用户的基于身份的策略中使用 `aws:SourceIP` 条件键包括预期公有网络地址的列表（例如本地网络范围）。

不同的网络路径如何反映在 CloudTrail

您生成的请求使用的不同网络路径 AWS 管理控制台 会反映在您的 CloudTrail 事件历史记录中。

对于直接的浏览器请求，使用 AWS 管理控制台 私有访问权限不会有任何改变。CloudTrail 事件将包括有关连接的详细信息，例如用于调用服务 API 的 VPC 终端节点 ID。

对于由 AWS 管理控制台 Web 服务器代理的请求，CloudTrail 事件将不包含任何与 VPC 相关的详细信息。但是，建立浏览器会话所需的初始请求（例如 `AwsConsoleSignIn` 事件类型）将在事件详细信息中包含 AWS 登录 VPC 终端节点 ID。AWS 登录

试试 AWS 管理控制台 私密访问

本节介绍如何在新账户中设置和测试 AWS 管理控制台 私有访问权限。

AWS 管理控制台 Private Access 是一项高级安全功能，需要具备网络和设置方面的先验知识 VPCs。本主题介绍如何在没有全面基础设施的情况下试用 AWS 管理控制台 私有访问。

主题

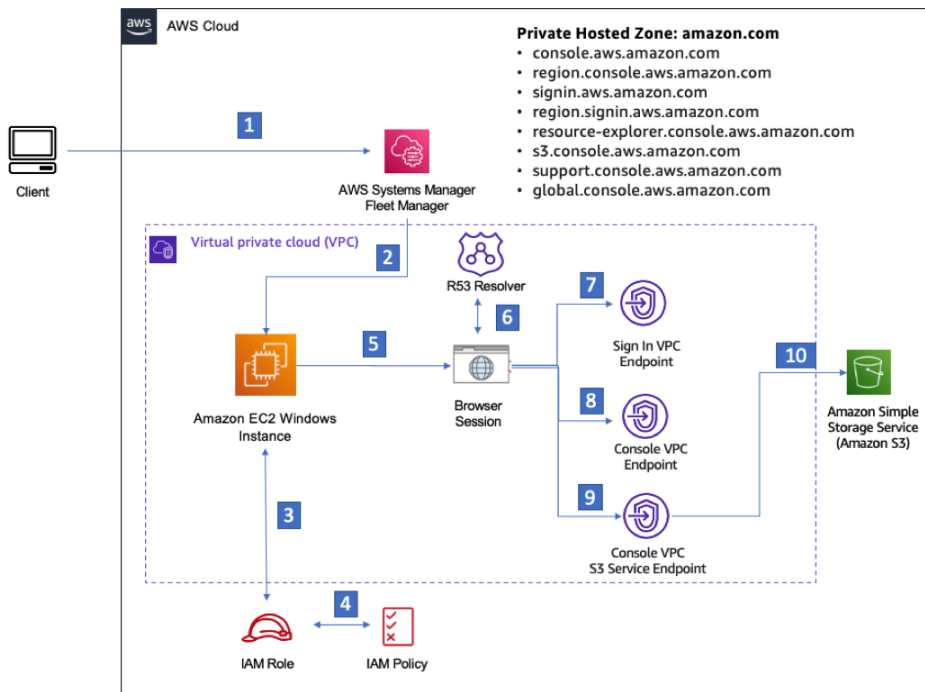
- [使用 Amazon EC2 测试设置](#)
- [使用 Amazon 测试设置 WorkSpaces](#)
- [使用 IAM 策略测试 VPC 设置](#)

使用 Amazon EC2 测试设置

[Amazon Elastic Compute Cloud](#) (Amazon EC2) 在 Amazon Web Services 云中提供可扩展的计算容量。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。在此设置中，我们使用 [Fleet Manager](#)（AWS Systems Manager 的一项功能），通过远程桌面协议（RDP）连接到 Amazon EC2 Windows 实例。

本指南演示了一个测试环境，用于设置和体验从 Amazon EC2 实例到亚马逊简单存储服务的 AWS 管理控制台 私有访问连接。本教程 CloudFormation 用于创建和配置 Amazon EC2 用于可视化此功能的网络设置。

下图描述了使用 Amazon EC2 访问 AWS 管理控制台 私有访问设置的工作流程。它显示了用户如何使用私有端点连接到 Amazon S3。



- 1 Client connects to the Fleet manager using Key pair.
- 2 Authenticated session connection to Windows Server using the Remote Desktop Protocol (RDP).
- 3 EC2 instance confirms credentials for IAM role in use as instance profile.
- 4 EC2 instance profile role permissions check.
- 5 Initiate browser session in EC2 instance.
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint.
- 8 Private Console endpoint.
- 9 S3 service private endpoint.
- 10 Connected to S3 service via private endpoint.

复制以下 CloudFormation 模板并将其保存到您将在设置网络过程的第三步中使用的文件中。

Note

此 CloudFormation 模板使用的配置目前在以色列（特拉维夫）地区不受支持。

AWS 管理控制台 私有访问环境 Amazon EC2 CloudFormation 模板

Description: |

AWS Management Console Private Access.

Parameters:

VpcCIDR:

Type: String

Default: 172.16.0.0/16

Description: CIDR range for VPC

Ec2KeyPair:

Type: AWS::EC2::KeyPair::KeyName

Description: The EC2 KeyPair to use to connect to the Windows instance

```
PublicSubnet1CIDR:
  Type: String
  Default: 172.16.1.0/24
  Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:
  Type: String
  Default: 172.16.0.0/24
  Description: CIDR range for Public Subnet B

PublicSubnet3CIDR:
  Type: String
  Default: 172.16.2.0/24
  Description: CIDR range for Public Subnet C

PrivateSubnet1CIDR:
  Type: String
  Default: 172.16.4.0/24
  Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:
  Type: String
  Default: 172.16.5.0/24
  Description: CIDR range for Private Subnet B

PrivateSubnet3CIDR:
  Type: String
  Default: 172.16.3.0/24
  Description: CIDR range for Private Subnet C

LatestWindowsAmiId:
  Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
  Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

InstanceTypeParameter:
  Type: String
  Default: 't3.medium'

Resources:

#####
# VPC AND SUBNETS
#####
```

```
AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""

PublicSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet3CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""

PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
```

Properties:

```
VpcId: !Ref AppVPC
CidrBlock: !Ref PrivateSubnet1CIDR
AvailabilityZone:
  Fn::Select:
    - 0
    - Fn::GetAZs: ""
```

PrivateSubnetB:

```
Type: 'AWS::EC2::Subnet'
Properties:
  VpcId: !Ref AppVPC
  CidrBlock: !Ref PrivateSubnet2CIDR
  AvailabilityZone:
    Fn::Select:
      - 1
      - Fn::GetAZs: ""
```

PrivateSubnetC:

```
Type: 'AWS::EC2::Subnet'
Properties:
  VpcId: !Ref AppVPC
  CidrBlock: !Ref PrivateSubnet3CIDR
  AvailabilityZone:
    Fn::Select:
      - 2
      - Fn::GetAZs: ""
```

InternetGateway:

```
Type: AWS::EC2::InternetGateway
```

InternetGatewayAttachment:

```
Type: AWS::EC2::VPCEGatewayAttachment
Properties:
  InternetGatewayId: !Ref InternetGateway
  VpcId: !Ref AppVPC
```

NatGatewayEIP:

```
Type: AWS::EC2::EIP
DependsOn: InternetGatewayAttachment
```

NatGateway:

```
Type: AWS::EC2::NatGateway
Properties:
```

```
    AllocationId: !GetAtt NatGatewayEIP.AllocationId
    SubnetId: !Ref PublicSubnetA

#####
# Route Tables
#####

PrivateRouteTable:
  Type: 'AWS::EC2::RouteTable'
  Properties:
    VpcId: !Ref AppVPC

DefaultPrivateRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway

PrivateSubnetRouteTableAssociation1:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetA

PrivateSubnetRouteTableAssociation2:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetB

PrivateSubnetRouteTableAssociation3:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetC

PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref AppVPC

DefaultPublicRoute:
  Type: AWS::EC2::Route
```

```
DependsOn: InternetGatewayAttachment
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
DestinationCidrBlock: 0.0.0.0/0
```

```
GatewayId: !Ref InternetGateway
```

```
PublicSubnetARouteTableAssociation1:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetA
```

```
PublicSubnetBRouteTableAssociation2:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetB
```

```
PublicSubnetBRouteTableAssociation3:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetC
```

```
#####
```

```
# SECURITY GROUPS
```

```
#####
```

```
VPCEndpointSecurityGroup:
```

```
Type: 'AWS::EC2::SecurityGroup'
```

```
Properties:
```

```
GroupDescription: Allow TLS for VPC Endpoint
```

```
VpcId: !Ref AppVPC
```

```
SecurityGroupIngress:
```

```
- IpProtocol: tcp
```

```
FromPort: 443
```

```
ToPort: 443
```

```
CidrIp: !GetAtt AppVPC.CidrBlock
```

```
EC2SecurityGroup:
```

```
Type: 'AWS::EC2::SecurityGroup'
```

```
Properties:
```

```
GroupDescription: Default EC2 Instance SG
```

```
VpcId: !Ref AppVPC

#####
# VPC ENDPOINTS
#####

VPCendpointGatewayS3:
  Type: 'AWS::EC2::VPCendpoint'
  Properties:
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
    VpcEndpointType: Gateway
    VpcId: !Ref AppVPC
    RouteTableIds:
      - !Ref PrivateRouteTable

VPCendpointInterfaceSSM:
  Type: 'AWS::EC2::VPCendpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
    SecurityGroupIds:
      - !Ref VPCendpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
    VpcId: !Ref AppVPC

VPCendpointInterfaceEc2messages:
  Type: 'AWS::EC2::VPCendpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCendpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
    VpcId: !Ref AppVPC

VPCendpointInterfaceSsmmessages:
  Type: 'AWS::EC2::VPCendpoint'
```

Properties:

VpcEndpointType: Interface

PrivateDnsEnabled: false

SubnetIds:

- !Ref PrivateSubnetA

- !Ref PrivateSubnetB

- !Ref PrivateSubnetC

SecurityGroupIds:

- !Ref VPCEndpointSecurityGroup

ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.ssmmessages'

VpcId: !Ref AppVPC

VPCEndpointInterfaceSignin:

Type: 'AWS::EC2::VPCEndpoint'

Properties:

VpcEndpointType: Interface

PrivateDnsEnabled: false

SubnetIds:

- !Ref PrivateSubnetA

- !Ref PrivateSubnetB

- !Ref PrivateSubnetC

SecurityGroupIds:

- !Ref VPCEndpointSecurityGroup

ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.signin'

VpcId: !Ref AppVPC

VPCEndpointInterfaceConsole:

Type: 'AWS::EC2::VPCEndpoint'

Properties:

VpcEndpointType: Interface

PrivateDnsEnabled: false

SubnetIds:

- !Ref PrivateSubnetA

- !Ref PrivateSubnetB

- !Ref PrivateSubnetC

SecurityGroupIds:

- !Ref VPCEndpointSecurityGroup

ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.console'

VpcId: !Ref AppVPC

#####

ROUTE53 RESOURCES

#####

```
ConsoleHostedZone:
  Type: "AWS::Route53::HostedZone"
  Properties:
    HostedZoneConfig:
      Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
    VPCs:
      -
        VPCId: !Ref AppVPC
        VPCRegion: !Ref "AWS::Region"

ConsoleRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 'console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

GlobalConsoleRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 'global.console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleS3ProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 's3.console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
        HostedZoneId: !Ref 'ConsoleHostedZone'
        Name: "support.console.aws.amazon.com"
        AliasTarget:
            DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
            HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
            Type: A

ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
        HostedZoneId: !Ref 'ConsoleHostedZone'
        Name: "resource-explorer.console.aws.amazon.com"
        AliasTarget:
            DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
            HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
            Type: A

WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
        HostedZoneId: !Ref 'ConsoleHostedZone'
        Name: "*.widget.console.aws.amazon.com"
        AliasTarget:
            DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
            HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
            Type: A

ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
        HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
Name: !Sub "${AWS::Region}.console.aws.amazon.com"
AliasTarget:
  DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
Type: A

ConsoleRecordRegionalMultiSession:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: !Sub ".*${AWS::Region}.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
Type: A

SigninHostedZone:
Type: "AWS::Route53::HostedZone"
Properties:
  HostedZoneConfig:
    Comment: 'Signin VPC Endpoint Hosted Zone'
  Name: 'signin.aws.amazon.com'
  VPCs:
    -
      VPCId: !Ref AppVPC
      VPCRegion: !Ref "AWS::Region"

SigninRecordGlobal:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'SigninHostedZone'
  Name: 'signin.aws.amazon.com'
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
Type: A

SigninRecordRegional:
```

```
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'SigninHostedZone'
  Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
  Type: A
```

```
#####
```

```
# EC2 INSTANCE
```

```
#####
```

```
Ec2InstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        -
          Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

```
Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
      - !Ref Ec2InstanceRole
```

```
EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:
    ImageId: !Ref LatestWindowsAmiId
    IamInstanceProfile: !Ref Ec2InstanceProfile
```

```
KeyName: !Ref Ec2KeyPair
InstanceType:
  Ref: InstanceTypeParameter
SubnetId: !Ref PrivateSubnetA
SecurityGroupIds:
  - Ref: EC2SecurityGroup
BlockDeviceMappings:
  - DeviceName: /dev/sda1
    Ebs:
      VolumeSize: 50
Tags:
  - Key: "Name"
    Value: "Console VPCE test instance"
```

设置网络

1. 登录您所在组织的管理账户并打开 [CloudFormation 控制台](#)。
2. 选择创建堆栈。
3. 选择使用新资源 (标准)。上传您之前创建的 CloudFormation 模板文件，然后选择下一步。
4. 输入堆栈的名称 (例如 **PrivateConsoleNetworkForS3**)，然后选择下一步。
5. 对于 VPC 和子网，输入您的首选 IP CIDR 范围，或使用提供的默认值。如果您使用默认值，请确认它们不与您的现有 VPC 资源重叠 AWS 账户。
6. 对于 E KeyPair c 2 参数，请从您账户中的现有 Amazon EC2 密钥对中选择一个。如果您没有现有的 Amazon EC2 密钥对，必须先创建一个密钥对，然后转至下一步。有关更多信息，请参阅《Amazon EC2 用户指南》中的[使用 Amazon EC2 创建密钥对](#)。
7. 选择创建堆栈。
8. 创建堆栈后，选择资源选项卡以查看已创建的资源。

连接到 Amazon EC2 实例

1. 登录您所在组织的管理账户并打开 [Amazon EC2 控制台](#)。
2. 在导航窗格中，选择 Instances (实例)。
3. 在实例页面上，选择由模板创建的控制台 VPCE 测试实例。CloudFormation 然后选择连接。

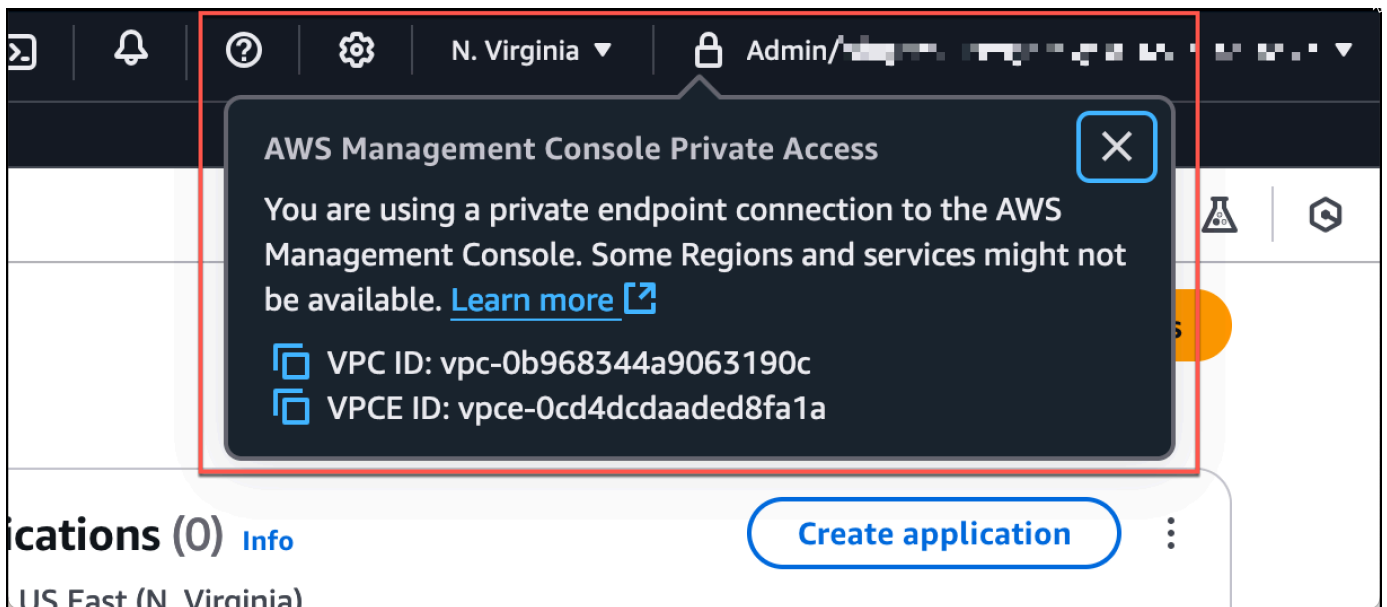
Note

此示例使用队列管理器（一种功能）连接到您的 Windows 服务器。AWS Systems Manager Explorer 可能需要几分钟才能开始连接。

4. 在连接到实例页面上，选择 RDP 客户端，然后使用 Fleet Manager 进行连接。
5. 选择 Fleet Manager 远程桌面。
6. 要获取 Amazon EC2 实例的管理密码并使用网页界面访问 Windows 桌面，请使用与您在创建 CloudFormation 模板时使用的 Amazon EC2 密钥对关联的私钥。
7. 在 Amazon EC2 Windows 实例中，AWS 管理控制台 在浏览器中打开。
8. 使用 AWS 凭证登录后，打开 [Amazon S3 控制台](#) 并确认您已使用 AWS 管理控制台 私有访问权限进行连接。

测试 AWS 管理控制台 私有访问设置

1. 登录您所在组织的管理账户并打开 [Amazon S3 控制台](#)。
2. 在导航栏中选择锁定私有图标，以查看所使用的 VPC 端点。以下屏幕截图显示了锁定私有图标的位置和 VPC 信息。



使用 Amazon 测试设置 WorkSpaces

亚马逊 WorkSpaces 允许您为用户配置虚拟的、基于云的 Windows、Amazon Linux 或 Ubuntu Linux 桌面，即。WorkSpaces 您可以根据需求的变更，快速添加或删除用户。用户可以从多个设备或 Web 浏览器访问自己的虚拟桌面。要了解更多信息 WorkSpaces，请参阅 [《Amazon WorkSpaces 管理指南》](#)。

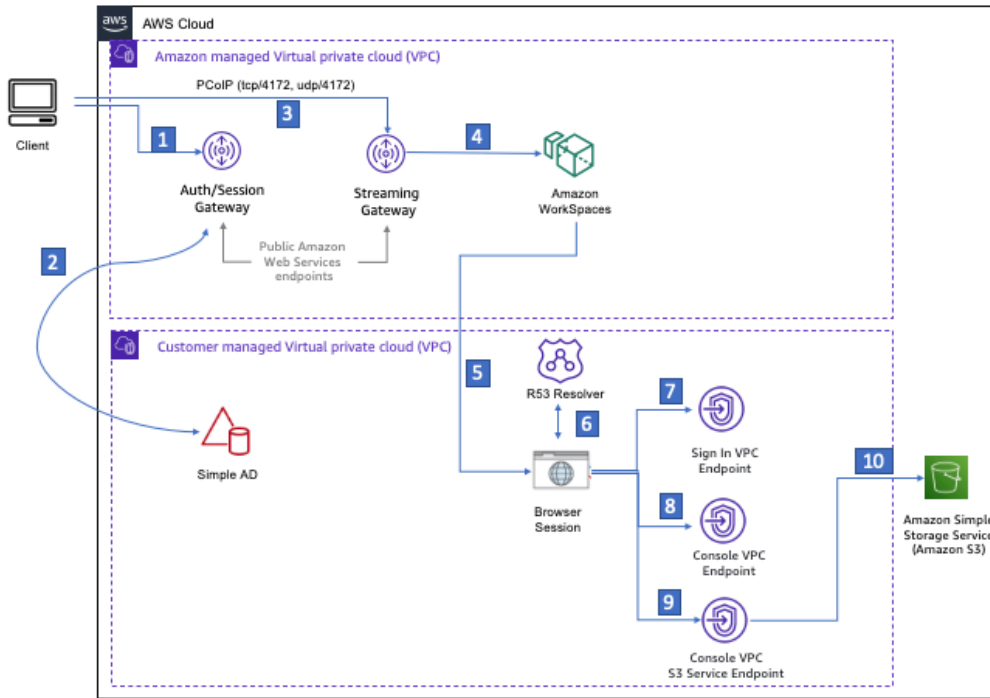
本节中的示例描述了一个测试环境，在该环境中，用户环境使用在上运行的 Web 浏览器登录 P AWS 管理控制台 ri Workspace vate Access。然后，用户访问 Amazon Simple Storage Service 控制台。Workspace 这旨在模拟企业用户在连接到 VPC 的网络上使用笔记本电脑，通过浏览器访问 AWS 管理控制台的体验。

本教程用于创建和配置网络设置和要使用的简单 Active Directory，WorkSpaces 以及 Workspace 使用设置的分步说明 AWS 管理控制台。AWS CloudFormation

下图描述了使用测试 AWS 管理控制台 私有 Workspace 访问设置的工作流程。它显示了客户端 Workspace、Amazon 托管 VPC 和客户托管 VPC 之间的关系。

Private Hosted Zone: amazon.com

- console.aws.amazon.com
- region.console.aws.amazon.com
- signin.aws.amazon.com
- region.signin.aws.amazon.com
- resource-explorer.console.aws.amazon.com
- s3.console.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com



- 1 Login information sent to authentication gateway
- 2 Authentication against Simple AD
- 3 Streaming Traffic to Streaming gateway
- 4 Each Workspace is connected to two networks simultaneously, Amazon-managed VPC for streaming traffic and Customer managed VPC handling all other traffic.
- 5 Initiate browser session
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint
- 8 Private Console endpoint
- 9 S3 service private endpoint
- 10 Connected to S3 service via private endpoint

复制以下 CloudFormation 模板并将其保存到一个文件中，您将在步骤的第 3 步中使用该文件来设置网络。

AWS 管理控制台 私有访问环境 CloudFormation 模板

Description: |
AWS Management Console Private Access.

Parameters:

VpcCIDR:

Type: String

Default: 172.16.0.0/16

Description: CIDR range for VPC

PublicSubnet1CIDR:

Type: String

Default: 172.16.1.0/24

```
Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:
  Type: String
  Default: 172.16.0.0/24
  Description: CIDR range for Public Subnet B

PrivateSubnet1CIDR:
  Type: String
  Default: 172.16.4.0/24
  Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:
  Type: String
  Default: 172.16.5.0/24
  Description: CIDR range for Private Subnet B

DSAdminPasswordResourceName:
  Type: String
  Default: ADAdminSecret
  Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
# supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
```

```
    az2: apse1-az2
ap-southeast-2:
    az1: apse2-az1
    az2: apse2-az3
ap-northeast-1:
    az1: apne1-az1
    az2: apne1-az4
ca-central-1:
    az1: cac1-az1
    az2: cac1-az2
eu-central-1:
    az1: euc1-az2
    az2: euc1-az3
eu-west-1:
    az1: euw1-az1
    az2: euw1-az2
eu-west-2:
    az1: euw2-az2
    az2: euw2-az3
sa-east-1:
    az1: sae1-az1
    az2: sae1-az3
```

Resources:

```
iamLambdaExecutionRole:
```

```
  Type: AWS::IAM::Role
```

```
  Properties:
```

```
    AssumeRolePolicyDocument:
```

```
      Version: 2012-10-17
```

```
      Statement:
```

```
        - Effect: Allow
```

```
          Principal:
```

```
            Service:
```

```
              - lambda.amazonaws.com
```

```
          Action:
```

```
            - 'sts:AssumeRole'
```

```
    ManagedPolicyArns:
```

```
      - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

```
    Policies:
```

```
      - PolicyName: describe-ec2-az
```

```
        PolicyDocument:
```

```
          Version: "2012-10-17"
```

```
          Statement:
```

```
- Effect: Allow
  Action:
    - 'ec2:DescribeAvailabilityZones'
  Resource: '*'
MaxSessionDuration: 3600
Path: /service-role/

fnZoneIdtoZoneName:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: python3.8
    Handler: index.lambda_handler
    Code:
      ZipFile: |
        import boto3
        import cfnresponse

        def zoneId_to_zoneName(event, context):
            responseData = {}
            ec2 = boto3.client('ec2')
            describe_az = ec2.describe_availability_zones()
            for az in describe_az['AvailabilityZones']:
                if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                    responseData['ZoneName'] = az['ZoneName']
                    cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

            def no_op(event, context):
                print(event)
                responseData = {}
                cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

            def lambda_handler(event, context):
                if event['RequestType'] == ('Create' or 'Update'):
                    zoneId_to_zoneName(event, context)
                else:
                    no_op(event, context)
  Role: !GetAtt iamLambdaExecutionRole.Arn

getAZ1:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
```

```
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
getAZ2:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#####
# VPC AND SUBNETS
#####

AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone: !GetAtt getAZ1.ZoneName

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone: !GetAtt getAZ2.ZoneName

PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet1CIDR
    AvailabilityZone: !GetAtt getAZ1.ZoneName

PrivateSubnetB:
  Type: 'AWS::EC2::Subnet'
```

```
Properties:
  VpcId: !Ref AppVPC
  CidrBlock: !Ref PrivateSubnet2CIDR
  AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
InternetGateway:
  Type: AWS::EC2::InternetGateway
```

```
InternetGatewayAttachment:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    InternetGatewayId: !Ref InternetGateway
    VpcId: !Ref AppVPC
```

```
NatGatewayEIP:
  Type: AWS::EC2::EIP
  DependsOn: InternetGatewayAttachment
```

```
NatGateway:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt NatGatewayEIP.AllocationId
    SubnetId: !Ref PublicSubnetA
```

```
#####
# Route Tables
#####
```

```
PrivateRouteTable:
  Type: 'AWS::EC2::RouteTable'
  Properties:
    VpcId: !Ref AppVPC
```

```
DefaultPrivateRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway
```

```
PrivateSubnetRouteTableAssociation1:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
```

```
    SubnetId: !Ref PrivateSubnetA

PrivateSubnetRouteTableAssociation2:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetB

PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref AppVPC

DefaultPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway

PublicSubnetARouteTableAssociation1:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetA

PublicSubnetBRouteTableAssociation2:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetB

#####
# SECURITY GROUPS
#####

VPCEndpointSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Allow TLS for VPC Endpoint
    VpcId: !Ref AppVPC
    SecurityGroupIngress:
```

```
- IpProtocol: tcp
  FromPort: 443
  ToPort: 443
  CidrIp: !GetAtt AppVPC.CidrBlock
```

```
#####
```

```
# VPC ENDPOINTS
```

```
#####
```

```
VPCEndpointGatewayS3:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
```

```
    VpcEndpointType: Gateway
```

```
    VpcId: !Ref AppVPC
```

```
    RouteTableIds:
```

```
      - !Ref PrivateRouteTable
```

```
VPCEndpointInterfaceSignin:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    VpcEndpointType: Interface
```

```
    PrivateDnsEnabled: false
```

```
    SubnetIds:
```

```
      - !Ref PrivateSubnetA
```

```
      - !Ref PrivateSubnetB
```

```
    SecurityGroupIds:
```

```
      - !Ref VPCEndpointSecurityGroup
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
```

```
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceConsole:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    VpcEndpointType: Interface
```

```
    PrivateDnsEnabled: false
```

```
    SubnetIds:
```

```
      - !Ref PrivateSubnetA
```

```
      - !Ref PrivateSubnetB
```

```
    SecurityGroupIds:
```

```
      - !Ref VPCEndpointSecurityGroup
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
```

```
    VpcId: !Ref AppVPC
```

```
#####  
# ROUTE53 RESOURCES  
#####  
  
ConsoleHostedZone:  
  Type: "AWS::Route53::HostedZone"  
  Properties:  
    HostedZoneConfig:  
      Comment: 'Console VPC Endpoint Hosted Zone'  
      Name: 'console.aws.amazon.com'  
      VPCs:  
        -  
          VPCId: !Ref AppVPC  
          VPCRegion: !Ref "AWS::Region"  
  
ConsoleRecordGlobal:  
  Type: AWS::Route53::RecordSet  
  Properties:  
    HostedZoneId: !Ref 'ConsoleHostedZone'  
    Name: 'console.aws.amazon.com'  
    AliasTarget:  
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]  
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]  
    Type: A  
  
GlobalConsoleRecord:  
  Type: AWS::Route53::RecordSet  
  Properties:  
    HostedZoneId: !Ref 'ConsoleHostedZone'  
    Name: 'global.console.aws.amazon.com'  
    AliasTarget:  
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]  
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]  
    Type: A  
  
ConsoleS3ProxyRecordGlobal:  
  Type: AWS::Route53::RecordSet  
  Properties:  
    HostedZoneId: !Ref 'ConsoleHostedZone'  
    Name: 's3.console.aws.amazon.com'
```

```
AliasTarget:
  DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

ConsoleSupportProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "support.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

ExplorerProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "resource-explorer.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

WidgetProxyRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref "ConsoleHostedZone"
    Name: "*.widget.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

ConsoleRecordRegional:
```

```
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: !Sub "${AWS::Region}.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

ConsoleRecordRegionalMultiSession:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: !Sub ".*${AWS::Region}.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

SigninHostedZone:
Type: "AWS::Route53::HostedZone"
Properties:
  HostedZoneConfig:
    Comment: 'Signin VPC Endpoint Hosted Zone'
    Name: 'signin.aws.amazon.com'
  VPCs:
    -
      VPCId: !Ref AppVPC
      VPCRegion: !Ref "AWS::Region"

SigninRecordGlobal:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'SigninHostedZone'
  Name: 'signin.aws.amazon.com'
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
```

```

    Type: A

SigninRecordRegional:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'SigninHostedZone'
    Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    Type: A

#####
# WORKSPACE RESOURCES
#####
ADAdminSecret:
  Type: AWS::SecretsManager::Secret
  Properties:
    Name: !Ref DSAdminPasswordResourceName
    Description: "Password for directory services admin"
    GenerateSecretString:
      SecretStringTemplate: '{"username": "Admin"}'
      GenerateStringKey: password
      PasswordLength: 30
      ExcludeCharacters: '@/\`

WorkspaceSimpleDirectory:
  Type: AWS::DirectoryService::SimpleAD
  DependsOn: AppVPC
  Properties:
    Name: "corp.awsconsole.com"
    Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
    Size: "Small"
    VpcSettings:
      SubnetIds:
        - Ref: PrivateSubnetA
        - Ref: PrivateSubnetB

    VpcId:
      Ref: AppVPC

```

Outputs:**PrivateSubnetA:**

Description: Private Subnet A

Value: !Ref PrivateSubnetA

PrivateSubnetB:

Description: Private Subnet B

Value: !Ref PrivateSubnetB

WorkspaceSimpleDirectory:


Description: Directory to be used for Workspaces

Value: !Ref WorkspaceSimpleDirectory

WorkspacesAdminPassword:

Description : "The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value."

Value: !Ref ADAdminSecret

 **Note**

此测试设置设计为在美国东部（弗吉尼亚州北部）（us-east-1）区域中运行。

设置网络

1. 登录您所在组织的管理账户并打开 [CloudFormation 控制台](#)。
2. 选择创建堆栈。
3. 选择使用新资源（标准）。上传您之前创建的 CloudFormation 模板文件，然后选择下一步。
4. 输入堆栈的名称（例如 **PrivateConsoleNetworkForS3**），然后选择下一步。
5. 对于 VPC 和子网，输入您的首选 IP CIDR 范围，或使用提供的默认值。如果您使用默认值，请确认它们不与您的现有 VPC 资源重叠 AWS 账户。
6. 选择创建堆栈。
7. 创建堆栈后，选择资源选项卡以查看已创建的资源。
8. 选择输出选项卡，以查看私有子网和工作区简单目录的值。请记住这些值，因为您将在下一个创建和配置过程的第四步中使用它们 WorkSpace。

以下屏幕截图显示了输出选项卡的视图，其中显示了私有子网和工作区简单目录的值。

PrivateConsoleNetworkForS3

[- updated] Resources **Outputs** Parameters Template Change sets Git sync

Delete Update Stack actions Create stack

Search outputs

Key	Value	Description	Export name
PrivateSubnetA	subnet-0aea1291fe9eb1b47	Private Subnet A	-
PrivateSubnetB	subnet-04f6adc31f08a09b6	Private Subnet B	-
WorkspacesAdminPassword	arn:aws:secretsmanager:us-east-1:851725487077:secret:ADAdminSecret-GAwM8i	The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value.	-
WorkspaceSimpleDirectory	d-9067f40091	Directory to be used for Workspaces	-

现在您已经创建了网络，请按照以下步骤创建和访问网络 WorkSpace。

要创建 WorkSpace

1. 打开 [WorkSpaces 控制台](#)。
2. 在导航窗格中，选择目录。
3. 在目录页面上，验证目录状态是否为活动。以下屏幕截图显示了具有一个活动的目录的目录页面。

Directories (1) Info

View details Actions Create directory

Directory ID	Workspace Type	Directory name	Organization n...	Identity source	Status
d-9067f40091	Personal	corp.awsconsole.com	d-9067f40091	AWS Directory Service	Registered

4. 要使用中的目录 WorkSpaces，必须对其进行注册。在导航窗格中，选择 WorkSpaces，然后选择创建 WorkSpaces。
5. 对于选择目录，选择 CloudFormation 在前面的过程中创建的目录。在操作菜单上，选择注册。

6. 要选择子网，请选择前述过程的步骤 9 中记下的两个私有子网。
7. 选择启用自助服务权限，然后选择注册。
8. 注册目录后，继续创建 WorkSpace。选择注册的目录，然后选择下一步。
9. 在创建用户页面上，选择创建其他用户。输入您的姓名和电子邮件以使您能够使用 WorkSpace。验证电子邮件地址是否有效，因为 WorkSpace 登录信息已发送到该电子邮件地址。
10. 选择下一步。
11. 在标识用户页面上，选择您在步骤 9 中创建的用户，然后选择下一步。
12. 在选择服务包页面上，选择 Amazon Linux 2 标准版，然后选择下一步。
13. 对于运行模式和用户自定义使用默认值，然后选择创建工作区。WorkSpace 开始进入 Pending 状态，然后在大约 20 分钟 Available 内过渡到状态。
14. 可用 WorkSpace 时，您将通过您在步骤九中提供的电子邮件地址收到一封包含访问说明的电子邮件。

登录后 WorkSpace，您可以测试自己是否正在使用 AWS 管理控制台 私有访问权限对其进行访问。

要访问 WorkSpace

1. 打开您在前述过程的步骤 14 中收到的电子邮件。
2. 在电子邮件中，选择提供的唯一链接来设置您的个人资料并下载 WorkSpaces 客户端。
3. 设置您的密码。
4. 下载您选择的客户端。
5. 安装并启动客户端。输入电子邮件中提供的注册码，然后选择注册。
6. WorkSpaces 使用您在第三步中创建的凭证登录 Amazon。

测试 AWS 管理控制台 私有访问设置

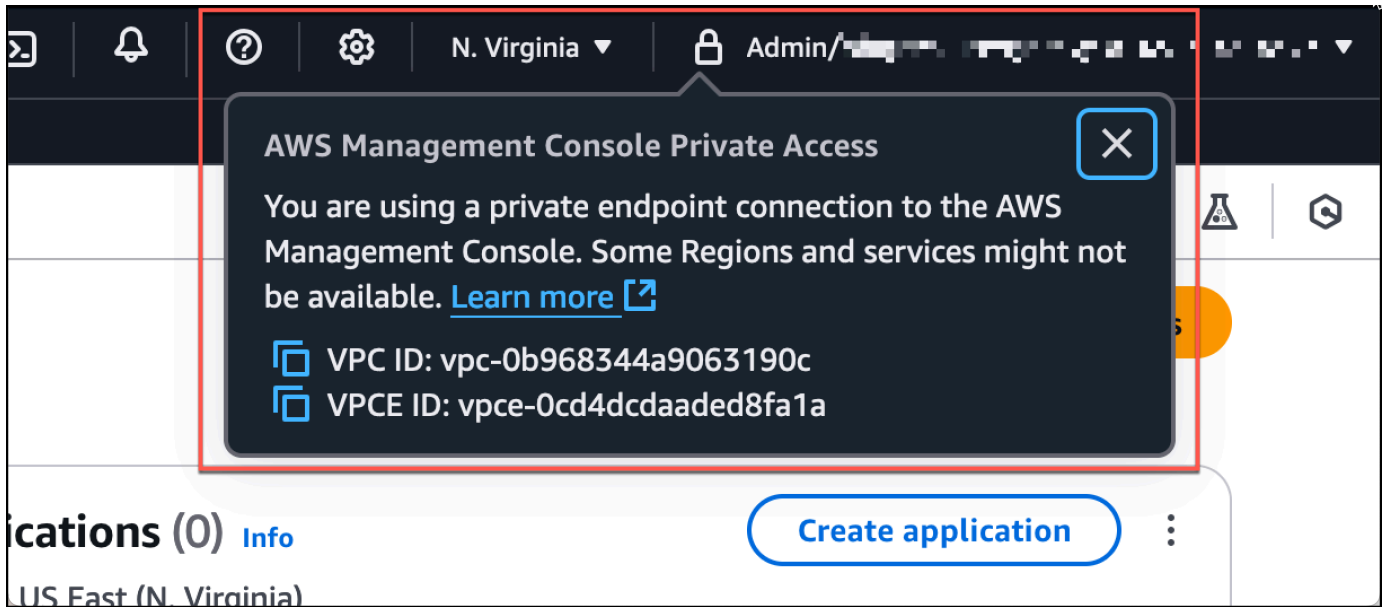
1. 从您的 WorkSpace，打开浏览器。然后，导航到 [AWS 管理控制台](#) 并使用您的凭证登录。

Note

如果您使用 Firefox 作为浏览器，请验证浏览器设置中的通过 HTTPS 启用 DNS 选项已关闭。

2. 打开 [Amazon S3 控制台](#)，您可以在其中验证您是否已使用 AWS 管理控制台 私有访问进行连接。

3. 在导航栏上选择锁定私有图标，以查看所使用的 VPC 和 VPC 端点。以下屏幕截图显示了锁定私有图标的位置和 VPC 信息。



使用 IAM 策略测试 VPC 设置

您可以进一步测试您通过 Amazon EC2 或部署限制访问 WorkSpaces 的 IAM 策略设置的 VPC。

除非 Amazon S3 使用您指定的 VPC，否则以下策略将拒绝对 Amazon S3 的访问。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "S3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": "vpc-12345678"
        },
        "Bool": {
          "aws:ViaAwsService": "false"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

以下策略使用登录端点的 AWS 管理控制台 私有访问策略将登录限制为选定 AWS 账户 IDs 用户。

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "*",  
      "Resource": "*",  
      "Condition": {  
        "StringEquals": {  
          "aws:PrincipalAccount": [  
            "AWSAccountID"  
          ]  
        }  
      }  
    }  
  ]  
}
```

如果您进行连接时所用的身份不属于您的账户，则会显示以下错误页面。



Your account doesn't have permission to use AWS Management Console Private Access

Your corporate network uses AWS Management Console Private Access, which only allows sign-ins from specific authorized accounts.

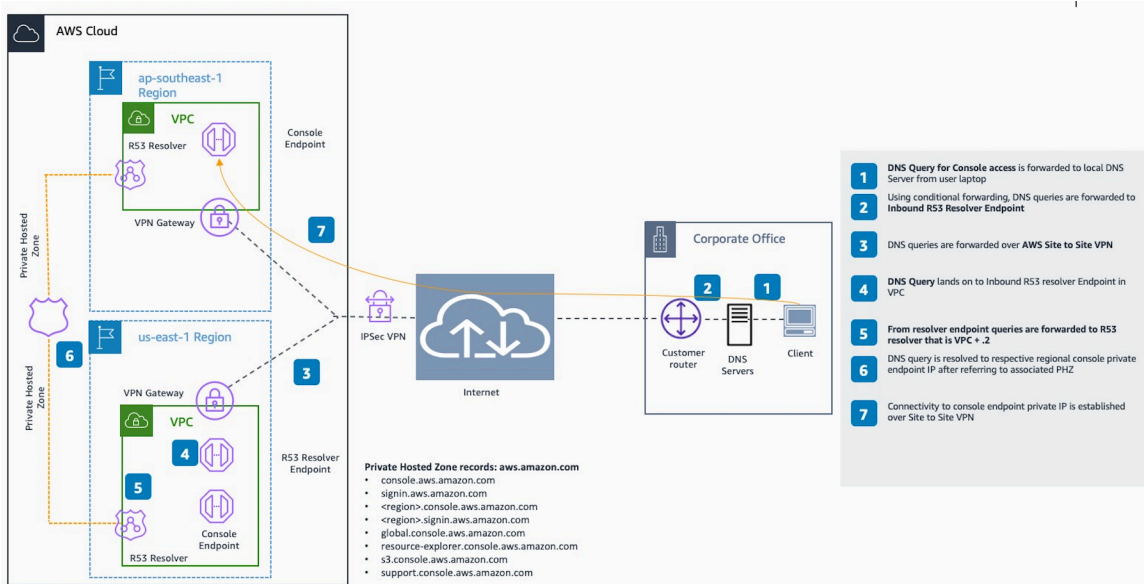
To access this account, sign in from a different network, or contact your administrator for more information.

Logout

参考架构

要通过本地网络私密连接到私 AWS 管理控制台 有访问权限，可以利用 AWS Site-to-Site VPN 到 AWS 虚拟专用网关 (VGW) 连接选项。AWS Site-to-Site VPN 通过创建连接并配置路由以通过连接传递流量，允许从 VPC 访问您的远程网络。有关更多信息，请参阅《VPN 用户 AWS 指南》中的[什么是点对点 VPN](#)。AWS Site-to-Site AWS 虚拟专用网关 (VGW) 是一项高度可用的区域服务，充当 VPC 和本地网络之间的网关。

AWS Site-to-Site VPN 到 AWS 虚拟专用网关 (VGW)



本参考架构设计中的一个重要组件是 Amazon Route 53 Resolver，特别是入站解析器。当您在创建 AWS 管理控制台 私有访问终端节点的 VPC 中进行设置时，将在指定的子网中创建解析器终端节点（网络接口）。然后，可以在本地 DNS 服务器上的条件转发器中引用解析器端点的 IP 地址，以允许查询私有托管区中的记录。当本地客户端连接到时 AWS 管理控制台，它们会被路由到私有访问端点的 AWS 管理控制台 私有访问终端节点。IPs

在设置与 AWS 管理控制台 私有访问终端节点的连接之前，请完成先决条件步骤，即 AWS 管理控制台 在您要访问的所有区域以及美国东部（弗吉尼亚北部）地区设置私有访问终端节点，并配置私有托管区域。AWS 管理控制台

AWS 用户体验定制 (UXC)

AWS 用户体验自定义 (UXC) 是一个实用程序，允许账户管理员自定义的视觉外观，AWS 管理控制台并在账户级别管理这些设置。

使用 UXC，您可以自定义以下设置：

- **账户颜色** — 您可以为账户设置一种颜色，以便在视觉上区分它们。例如，您可以将绿色用于开发帐户，黄色用于测试帐户，红色用于生产帐户。
- **服务可见性**-您可以控制控制台导航中显示哪些 AWS 服务。服务可见性 AWS 管理控制台 简化了仅显示与您的账户相关的 AWS 服务。
- **区域可见性**-您可以控制在 AWS 区域选择器中显示哪些区域。区域可见性 AWS 管理控制台 简化了仅显示与您的账户相关的区域。

如果您尚未配置设置，则默认行为适用：所有服务和区域均可见，并且未设置任何账户颜色。您可以通过将该值设置为，将账户颜色重置为其默认值"none"。您可以通过将可见服务和区域的值设置为，将其重置为默认值null。

Note

`visibleServices`和`visibleRegions`设置仅控制服务和区域在中的外观 AWS 管理控制台。它们不限制通过 AWS Command Line Interface SDKs、或其他方式进行访问 APIs。

主题

- [AWS 用户体验定制入门](#)
- [UXC API 参考](#)
- [使用记录 AWS 用户体验自定义 API 调用 AWS CloudTrail](#)
- [AWS 用户体验定制中的安全性](#)

AWS 用户体验定制入门

使用 UXC，账户管理员可以为配置账户自定义。AWS 管理控制台

先决条件

在开始之前，您需要：

- 一个 AWS 账户
- 适用于 UXC 的 AWS Identity and Access Management (IAM) 权限。有关更多信息，请参阅[AWS 用户体验自定义如何与 IAM 配合使用](#)以及[的AWS 托管策略 AWS 管理控制台](#)。

在中访问 UXC 设置 AWS 管理控制台

要访问中的账户颜色 AWS 管理控制台，请参阅[中的访问账户信息 AWS 管理控制台](#)。要访问中的服务可见性和区域可见性 AWS 管理控制台，请参阅[AWS 管理控制台 使用统一设置进行配置](#)。

在控制台中设置账户颜色

1. 登录到 [AWS 管理控制台](#)。
2. 在导航栏上，选择您的账户名称。
3. 选择账户。
4. 在账户显示设置中，选择颜色。
5. 选择更新。

在控制台中设置可见区域

1. 登录到 [AWS 管理控制台](#)。
2. 打开 [“统一设置”](#)。
3. 在“可见区域”部分中选择“编辑”。
4. 将您的可见区域设置为所有可用区域或选择区域并配置您的列表。
5. 选择保存更改。

在控制台中设置可见服务

1. 登录到 [AWS 管理控制台](#)。
2. 打开 [“统一设置”](#)。
3. 在“可见服务”部分中选择“编辑”。
4. 将您的可见服务设置为“所有服务”或“选择服务”，然后配置您的列表。

5. 选择保存更改。

以编程方式访问 UXC 设置

您还可以通过编程方式管理账户自定义设置，也可以将其作为基础架构即代码进行管理。有关更多信息，请参阅[AWS 用户体验自定义 API 参考](#)和[AWS::UXC::AccountCustomization](#) CloudFormation 模板参考。

UXC API 参考

《[AWS 用户体验自定义 API 参考](#)》包含 UXC 支持的操作的完整列表。

使用记录 AWS 用户体验自定义 API 调用 AWS CloudTrail

AWS 用户体验定制与[AWS CloudTrail](#)一项服务集成，该服务提供用户、角色或用户所采取的操作的记录 AWS 服务。CloudTrail 将 UXC 的所有 API 调用捕获为事件。捕获的调用包含来自 UXC 控制台的调用和对 UXC API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向 UXC 发出的请求、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

CloudTrail 在您创建账户 AWS 账户时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。AWS 区域有关更多信息，请参阅《[AWS CloudTrail 用户指南](#)》中的“[使用 CloudTrail 事件历史记录](#)”。查看活动历史记录不 CloudTrail 收取任何费用。

要持续记录 AWS 账户过去 90 天内的事件，请创建跟踪或 [CloudTrailLake](#) 事件数据存储。

UXC 管理活动位于 CloudTrail

[管理事件](#)提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下，CloudTrail 记录管理事件。

AWS 用户体验定制将所有 UXC 控制平面操作记录为管理事件。有关 UXC 登录到的 AWS 用户体验自定义控制平面操作的列表 CloudTrail，请参阅《[AWS 用户体验自定义 API 参考](#)》。

UXC 事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 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，因此事件不会按任何特定顺序出现。

以下示例显示了一个演示该GetAccountCustomizations操作 CloudTrail 的事件。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn": "arn:aws:sts::111122223333:assumed-role/MyRole/jdoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/MyRole",
        "accountId": "111122223333",
        "userName": "MyRole"
      },
      "attributes": {
        "creationDate": "2026-03-06T15:15:16Z",
        "mfaAuthenticated": "false"
      }
    },
    "attributes": {
      "creationDate": "2026-03-06T15:15:16Z",
      "mfaAuthenticated": "false"
    }
  },
  "eventTime": "2026-03-06T15:36:13Z",
  "eventSource": "uxc.amazonaws.com",
  "eventName": "GetAccountCustomizations",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-sdk-java/2.41.27",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID": "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::UXC::AccountCustomization",
      "ARN": "arn:aws:uxc::111122223333:account-customizations"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
```

```
"recipientAccountId": "111122223333",  
"eventCategory": "Data"  
}
```

有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的[CloudTrail 录制内容](#)。

AWS 用户体验定制中的安全性

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](#)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 AWS 用户体验定制的合规性计划，请参阅按合规计划划分的[范围内的 AWS 服务按合规计划](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的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 UXC 时如何应用分担责任模型。以下主题向您介绍如何配置 UXC 以满足您的安全和合规性目标。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 UXC 资源。

主题

- [用于 AWS 用户体验定制的 Identity and Access Management](#)

用于 AWS 用户体验定制的 Identity and Access Management

AWS 用户体验定制 (UXC) 使用 IAM 策略来管理对 UXC API 操作的访问权限。

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 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用用户体验自定义资源。您可以使用 IAM AWS 服务，无需支付额外费用。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)

- [AWS 用户体验自定义如何与 IAM 配合使用](#)
- [AWS 用户体验自定义的基于身份的策略示例](#)

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[AWS 用户体验疑难解答自定义身份和访问权限](#)）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅[AWS 用户体验自定义如何与 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[AWS 用户体验自定义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。有关要求根用户凭证的任务，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

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](#)。

AWS 用户体验自定义如何与 IAM 配合使用

AWS 用户体验定制 (UXC) 与 IAM 策略配合使用，以管理对 UXC API 操作的访问权限。

在使用 IAM 管理 AWS 用户体验自定义 (用户体验自定义) 的访问权限之前，请先了解有哪些 IAM 功能可用于用户体验定制。我们建议您通过 AWS 托管策略与用户体验自定义集成，有关更多信息，请参阅 [AWS 托管策略 AWS 管理控制台](#)。

在使用 IAM 管理对用户体验自定义的访问权限之前，请先了解有哪些 IAM 功能可用于用户体验定制。

IAM 功能	用户体验定制支持
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	否
策略条件密钥	否
临时凭证	是
跨服务主体权限	否

IAM 功能	用户体验定制支持
服务关联角色	否
服务角色	否

要全面了解用户体验定制和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM [配合使用的AWS 服务](#)。

用于用户体验定制的基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户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](#)。

要查看用户体验自定义基于身份的策略示例，请参阅用户体验自定义的[基于身份的策略示例](#)。 [AWS](#)

用户体验自定义的策略操作

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。

要查看所有用户体验自定义操作，请参阅 [API 参考](#)。

用户体验自定义中的策略操作在操作前使用 `uxc:` 前缀（例如 `uxc:GetAccountCustomizations`）。

要在单个语句中指定多项操作，请使用逗号将它们隔开：

```
"Action": [
  "uxc:GetAccountCustomizations",
  "uxc:ListServices"
]
```

要查看用户体验自定义基于身份的策略示例，请参阅用户体验自定义的[基于身份的策略示例](#)。AWS

用户体验定制的政策资源

用户体验自定义不支持策略资源。

使用临时凭证进行用户体验自定义

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 用户体验疑难解答自定义身份和访问权限

使用以下信息来帮助您诊断和修复在使用用户体验自定义和 IAM 时可能遇到的常见问题。

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 `uxc: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:
  uxc:GetWidget on resource: my-example-widget because no identity-based policy allows
  the GetWidget action
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 `uxc: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。

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 AKIAIOSFODNN7EXAMPLE）和秘密访问密钥（例如 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

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。通过这样做，您可以授予他人永久访问您的权限 AWS 账户。

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。如果丢失了您的秘密访问密钥，您必须为 IAM 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](#)。

要允许其他人访问用户体验自定义，您必须向需要访问的人员或应用程序授予权限。如果使用 AWS IAM Identity Center 管理人员和应用程序，则可以向用户或组分配权限集来定义其访问权限级别。权限集会自动创建 IAM 策略并将其分配给与人员或应用程序关联的 IAM 角色。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。

如果未使用 IAM Identity Center，则必须为需要访问的人员或应用程序创建 IAM 实体（用户或角色）。然后，您必须将策略附加到该实体，以便在用户体验自定义中向他们授予正确权限。授予权限后，向用户或应用程序开发人员提供凭证。他们将使用这些凭证访问 AWS。要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅《IAM 用户指南》中的[IAM 身份](#)和[IAM 中的策略和权限](#)。

AWS 用户体验自定义的基于身份的策略示例

默认情况下，用户和角色无权获取或修改 UXC 资源。要向用户授予对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）](#)。

主题

- [策略最佳实践](#)
- [对 UXC 账户自定义项的只读访问权限](#)
- [对 UXC 账户自定义的完全访问权限](#)

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、访问或删除用户体验自定义资源。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 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

对 UXC 账户自定义项的只读访问权限

以下示例说明如何创建允许对 UXC 账户自定义项进行只读访问的策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "uxc:GetAccountCustomizations",
        "uxc:ListServices"
      ],
      "Resource": "*"
    }
  ]
}
```

对 UXC 账户自定义的完全访问权限

以下示例说明如何创建允许完全访问 UXC 账户自定义项的策略：

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

```
    "Effect": "Allow",
    "Action": [
      "uxc:*"
    ],
    "Resource": "*"
  }
]
```

AWS 的托管策略 AWS 管理控制台

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的[客户管理型策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)。

AWS 托管策略：AWSManagementConsoleBasicUserAccess

您可以将 AWSManagementConsoleBasicUserAccess 附加到您的用户、组和角色。

此策略向 AWS 管理控制台的非管理员用户授予必要的权限。这包括资源发现、通知、基于浏览器的 Shell 访问和自定义导航等功能。

权限详细信息

此 AWSManagementConsoleBasicUserAccess 分组为以下权限集：

- `cloudshell`— 允许委托人完全访问各种 AWS CloudShell 功能，包括环境创建、会话管理和命令执行。
- `ec2`：支持主体描述在[统一导航](#)中为该账户启用的区域。
- `notifications`— 允许委托人从中获取事件。AWS 用户通知服务
- `q`：支持主体与 Amazon Q 开发者版聊天。
- `resource-explorer-2`— 允许委托人使用[统一搜索](#)搜索和发现 AWS 资源。

- `uxc`— 允许委托人读取 AWS 用户体验自定义设置。
- `action-recommendations`— 允许委托人接收上下文操作建议。
- `account`— 允许委托人检索有关指定账户的信息，包括其账户名、账户 ID 以及账户创建日期和时间。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 [AWSManagementConsoleBasicUserAccess](#)。

AWS 托管策略：AWSManagementConsoleAdministratorAccess

您可以将 `AWSManagementConsoleAdministratorAccess` 附加到您的用户、组和角色。

此策略授予配置和自定义 AWS 管理控制台的完全访问权限。它可让管理员设置账户颜色、启用用户通知和配置资源发现。它还包括来自 `AWSManagementConsoleBasicUserAccess` 托管式策略的权限，这些权限对于 AWS 管理控制台的非管理员用户来说是必不可少的。

权限详细信息

此 `AWSManagementConsoleAdministratorAccess` 分组为以下权限集：

- `cloudshell`— 允许委托人完全访问各种 AWS CloudShell 功能，包括环境创建、会话管理和命令执行。
- `ec2`：支持主体描述在[统一导航](#)中为该账户启用的区域。
- `notifications`：支持主体访问和更新通知配置、事件和功能选择加入状态。
- `q`：支持主体与 Amazon Q 开发者版聊天，以获得 AI 辅助支持。
- `resource-explorer-2`— 允许委托人使用[统一](#)搜索搜索和发现 AWS 资源。
- `uxc`— 允许委托人完全访问 AWS 用户体验自定义设置。
- `action-recommendations`— 允许委托人接收上下文操作建议。
- `account`— 允许委托人检索有关指定账户的信息，包括其账户名、账户 ID 以及账户创建日期和时间。

要查看此策略的权限，请参阅《AWS 托管策略参考》中的 [AWSManagementConsoleAdministratorAccess](#)。

AWS 管理控制台 AWS 托管策略的更新

查看有关 AWS 管理控制台 自该服务开始跟踪这些更改以来的 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅“AWS 管理控制台 文档历史记录”页面上的 RSS feed。

更改	描述	日期
AWSManagementConsoleBasicUserAccess - 更新的策略	添加了 <code>uxc:GetAccountCustomizations</code> 和 <code>uxc:ListServices</code> 权限。	2026 年 3 月 26 日
AWSManagementConsoleAdministratorAccess - 更新的策略	添加了 <code>uxc:GetAccountCustomizations</code> 、 <code>uxc:UpdateAccountCustomizations</code> 和 <code>uxc:ListServices</code> 权限。	2026 年 3 月 26 日
AWSManagementConsoleBasicUserAccess - 更新的策略	更新了策略，添加了权限，允许用户在浏览账户时查看账户信息并接收操作建议。AWS 管理控制台	2025 年 12 月 9 日
AWSManagementConsoleAdministratorAccess - 更新的策略	更新了策略，添加了权限，允许用户在浏览账户时查看账户信息并接收操作建议。AWS 管理控制台	2025 年 12 月 9 日
AWSManagementConsoleBasicUserAccess : 新策略	添加了一个新的 AWS 托管策略，该策略授予基本 AWS 管理控制台 导航、账户颜色查看和资源发现所需的权限。	2025 年 8 月 14 日

更改	描述	日期
AWSManagementConso leAdministratorAccess : 新策略	添加了一个新的 AWS 托管策略，该策略提供配置和自定义的完全访问权限 AWS 管理控制台。	2025 年 8 月 14 日
AWS 管理控制台 开始跟踪更改	AWS 管理控制台 开始跟踪其 AWS 托管策略的更改。	2025 年 8 月 14 日

在控制台中使用 Markdown

中的某些服务 AWS 管理控制台，例如亚马逊 CloudWatch，支持在某些领域使用 [Markdown](#)。本主题说明控制台中支持的 Markdown 格式的类型。

内容

- [段落、行间距和水平线](#)
- [标题](#)
- [文本格式设置](#)
- [链接](#)
- [列表](#)
- [表格和按钮 \(CloudWatch 仪表板 \)](#)

段落、行间距和水平线

段落由空白行分隔。为了确保段落之间的空白行在转换为 HTML 时呈现，请添加一个带有不间断空格 () 的新行，然后添加一个空白行。重复这两行，依次插入多个空白行，如下例所示：

```
&nbsp;
&nbsp;
```

要创建分隔段落的水平规则，请添加一个连续包含三个连字符的新行：---

```
Previous paragraph.
---
Next paragraph.
```

要创建具有等宽类型的文本块，请添加一个带有三个反引号 (``) 的行。输入要以等宽类型显示的文本。然后，添加另一个包含三个反引号的新行。以下示例演示了在显示时格式将设置为等宽类型的文本：

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

标题

要创建标题，请使用井号 (#)。单个井号和空格表示顶级标题。两个井号将创建一个二级标题，三个井号将创建一个三级标题。以下示例显示了顶级、二级和三级标题：

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

文本格式设置

要将文本的格式设置为斜体，请在文本的两端各使用一个下划线 (_) 或星号 (*) 以将其括起。

```
*This text appears in italics.*
```

要将文本的格式设置为粗体，请在文本的两端各使用两个下划线或星号以将其括起。

```
**This text appears in bold.**
```

要将文本的格式设置为带删除线，请在文本的两端各使用两个波浪线 (~) 以将其括起。

```
~~This text appears in strikethrough.~~
```

链接

要添加文本超链接，请输入用方括号 ([]) 括起来的链接文本，后跟放入括号 (()) 中的完整 URL，如下示例所示：

```
Choose [link_text](http://my.example.com).
```

列表

要将行的格式设置为项目符号列表的一部分，请将它们添加到以一个星号 (*) 后跟一个空格开头的单独行上，如下示例所示：

Here is a bulleted list:

- * Ant
- * Bug
- * Caterpillar

要将行的格式设置为编号列表的一部分，请将它们添加到以一个数字、句点 (.) 和一个空格开头的单独行上，如以下示例所示：

Here is a numbered list:

1. Do the first step
2. Do the next step
3. Do the final step

表格和按钮 (CloudWatch 仪表板)

CloudWatch 仪表板文本控件支持 Markdown 表格和按钮。

要创建表，请使用竖线 (|) 分隔列并使用新行分隔行。要使第一行成为标题行，请在标题行和第一行值之间插入一行。然后，为表中的每一列添加至少三个连字符 (-)。使用竖线分隔各列。以下示例显示包含两列、一个标题行和两个数据行的表的 Markdown：

```
Table | Header
----|-----
Amazon Web Services | AWS
1 | 2
```

上一个示例中的 Markdown 文本创建了下表：

表	标题
Amazon Web Services	AWS
1	2

在 CloudWatch 仪表板文本控件中，您还可以设置超链接的格式，使其显示为按钮。要创建按钮，请使用 [button:*Button text*]，后跟放入括号 (()) 中的完整 URL，如以下示例所示：

```
[button:Go to AWS](http://my.example.com)
```

```
[button:primary:This button stands out even more](http://my.example.com)
```

问题排查

请参阅本节以查找常见问题的解决方案 AWS 管理控制台。

您还可以使用 Amazon Q Developer 诊断和解决某些 AWS 服务的常见错误。有关更多信息，请参阅《Amazon Q 开发者版用户指南》中的[使用 Amazon Q 开发者版诊断控制台中的常见错误](#)。

主题

- [页面未正确加载](#)
- [我的浏览器在连接时显示“访问被拒绝”错误 AWS 管理控制台](#)
- [我的浏览器在连接时显示超时错误 AWS 管理控制台](#)
- [我想更改的语言，AWS 管理控制台 但在页面底部找不到语言选择菜单](#)

页面未正确加载

- 如果此问题只是偶尔出现，请检查您的互联网连接。尝试通过其他网络进行连接，或者使用或不使用 VPN 进行连接，或者尝试使用不同的 Web 浏览器。
- 如果所有受影响的用户都来自同一个团队，则可能是隐私浏览器扩展程序或安全防火墙问题。隐私浏览器扩展程序和安全防火墙可能会阻止访问由 AWS 管理控制台使用的域。尝试关闭这些扩展程序或调整防火墙设置。要验证您的连接问题，请打开浏览器开发工具（[Chrome](#)、[Firefox](#)），并在控制台选项卡中检查错误。AWS 管理控制台 使用域名的后缀，包括以下列表。此列表并不详尽，可能会随着时间而变化。这些域的后缀并非专供 AWS 使用。
 - .a2z.com
 - .amazon.com
 - .amazonaws.com
 - .aws
 - .aws.com
 - .aws.dev
 - .awscloud.com
 - .awsplayer.com
 - .awsstatic.com
 - .cloudfront.net
 - .live-video.net

⚠ Warning

自 2022 年 7 月 31 日起，AWS 不再支持 Internet Explorer 11。我们建议您将与其他支持的浏览器 AWS 管理控制台 一起使用。有关更多信息，请参阅 [AWS 新闻博客](#)。

我的浏览器在连接时显示“访问被拒绝”错误 AWS 管理控制台

如果满足以下所有条件，最近对控制台所做的更改可能会影响您的访问权限：

- 您可以 AWS 管理控制台 从配置为通过 VPC 终端节点访问 AWS 服务终端节点的网络进行访问。
- 您可以通过在 IAM 策略中使用 `aws:SourceIp` 或 `aws:SourceVpc` 全局条件密钥来限制对 AWS 服务的访问。

我们建议您查看包含 `aws:SourceIp` 或 `aws:SourceVpc` 全局条件键的 IAM 策略。在适用的情况下同时应用 `aws:SourceIp` 和 `aws:SourceVpc`。

某些 AWS 管理控制台 功能使用同时支持 IPv4 和 IPv6 连接的双栈域。如果您的 IAM 策略限制仅使用 IPv4 CIDR 块 `aws:SourceIp` 进行访问，则当您的操作系统首选 IPv6 连接时，请求可能会失败（反之亦然）。为避免这种情况，请在您的 `aws:SourceIp` 状况中同时包含两者 IPv4 和 IPv6 CIDR 块。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》SourceIp 中的 [aws](#)。

您还可以使用 AWS 管理控制台 私有访问功能，AWS 管理控制台 通过 VPC 终端节点进行访问，并在策略中使用 `aws:SourceVpc` 条件。有关更多信息，请参阅下列内容：

- [AWS 管理控制台 私密访问权限](#)
- [the section called “AWS 管理控制台 私有访问权限如何与 aws 配合使用 : SourceVpc”](#)
- [the section called “支持的 AWS 全局条件上下文密钥”](#)

我的浏览器在连接时显示超时错误 AWS 管理控制台

如果您的默认服务中断 AWS 区域，则您的浏览器在尝试连接时可能会显示 504 网关超时错误。AWS 管理控制台 要 AWS 管理控制台 从其他区域登录，请在 URL 中指定备用区域终端节点。例如，如果 `us-west-1`（加利福尼亚北部）区域发生中断，要访问 `us-west-2`（俄勒冈）区域，请使用以下模板：

```
https://region.console.aws.amazon.com
```

有关更多信息，请参阅《AWS 一般参考》中的 [AWS 管理控制台 服务端点](#)。

要查看所有 AWS 服务内容（包括）的状态 AWS 管理控制台，请参阅 [AWS Health Dashboard](#)。

我想更改的语言，AWS 管理控制台 但在页面底部找不到语言选择菜单

语言选择菜单已移至新的 Unified Settings（统一设置）页面。要更改的语言 AWS 管理控制台，[请导航至“统一设置”页面](#)，然后选择控制台的语言。

有关更多信息，请参阅 [更改 AWS 管理控制台的语言](#)。

文档历史记录

下表介绍了自 2021 年 3 月起对《AWS 管理控制台 入门指南》的一些重要更改。

更改	描述	日期
更新了 AWS 托管策略	使用新的 UXC 权限更新了 AWSManagementConsoleAdministratorAccess 和 AWSManagementConsoleBasicUserAccess 政策。有关更多信息，请参阅 ??? 。	2026 年 3 月 26 日
添加了页面	添加了新页面，以解释建议的操作。有关更多信息，请参阅 ??? 。	2025 年 10 月 15 日
新的 AWS 托管策略	<p>添加了两个新策略，以确定使用、配置和自定义 AWS 管理控制台的权限范围。</p> <ul style="list-style-type: none"> • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess 	2025 年 8 月 14 日
用户体验自定义 (UXC)	新服务可用。	2025 年 8 月 14 日
页面已更新	现在，您可以通过“服务”菜单在 myApplications 中查看您的应用程序。有关更多信息，请参阅 ??? 。	2025 年 7 月 29 日
添加了页面	添加了新页面来解释多会话功能。有关更多信息，请参阅 ??? 。	2024 年 12 月 6 日

更改	描述	日期
页面已更新	更改密码页面已更新。有关更多信息，请参阅 ??? 。	2024 年 6 月 18 日
添加了新页面	添加了新页面，描述了如何访问服务菜单和 AWS 事件通知。有关更多信息，请参阅 ??? 和 ??? 。	2024 年 6 月 18 日
页面已更新	那是什么 AWS 管理控制台？页面已更新。有关更多信息，请参阅 ??? 。	2024 年 6 月 18 日
获取支持	添加了一个新页面以介绍如何获取支持。有关更多信息，请参阅 ??? 。	2024 年 6 月 18 日
统一导航和 AWS Console Home	添加了新页面以介绍如何使用控制台。有关更多信息，请参阅 ??? 和 ??? 。	2024 年 6 月 18 日
与 Amazon Q 聊天	一个新的设置页面，详细说明了用户如何向 Amazon Q 开发者 AWS 提问。有关更多信息，请参阅 与 Amazon Q 开发者版聊天 。	2024 年 5 月 29 日
myApplications	一个介绍 myApplications 的新页面。有关更多信息，请参阅 MyApplications 在 AWS 做什么？ 。	2023 年 11 月 29 日
配置统一设置	一个新的设置页面，用于配置应用于当前用户的设置和原定设置，包括语言和区域。有关更多信息，请参阅 配置统一设置 。	2022 年 4 月 6 日

更改	描述	日期
全新 AWS Console Home 用户界面	新的 AWS Console Home 用户界面，包括用于显示重要使用信息的小部件和 AWS 服务快捷方式。有关更多信息，请参阅 使用小组件 。	2022 年 2 月 25 日
更改控制台语言	为 AWS 管理控制台选择不同的语言。有关更多信息，请参阅 更改 AWS 管理控制台的语言 。	2021 年 4 月 1 日
正在启动 CloudShell	AWS CloudShell 从中打开 AWS 管理控制台 并运行 AWS CLI 命令。有关更多信息，请参阅 启动 AWS CloudShell 。	2021 年 3 月 22 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。