

用户指南

AWS CloudShell



AWS CloudShell: 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 AWS CloudShell ?	1
AWS CloudShell的特征	1
AWS Command Line Interface	2
Shell 和开发工具	2
持久性存储	2
CloudShell VPC环境	3
安全性	3
自定义选项	3
会话恢复	3
如何开始 AWS CloudShell ?	4
的定价 AWS CloudShell	7
关键 AWS CloudShell 话题	7
FAQs	7
我该如何开始使用 AWS CloudShell ?	8
我需要访问什么 AWS CloudShell ?	8
AWS CloudShell 上面有什么 Console Toolbar?	8
我该如何 AWS CloudShell 在 Console Toolbar?	9
哪些 AWS 区域 版本 AWS CloudShell 可用 ?	9
当您在 CloudShell 上启动时，AWS 区域 如果 AWS CloudShell 在选定区域中不可用，则会分配该选项 Console Toolbar?	9
我可以在 AWS CloudShell中使用哪些类型的 Shell ?	9
我可以使用的 Web 浏览器 AWS CloudShell ?	9
如何创建和管理我的 AWS CloudShell 环境 ?	9
当我在 AWS CloudShell 上启动时，我可以使用的 Web 浏览器 Console Toolbar?	10
我可以从中下载文件 AWS CloudShell吗 ?	10
Shell 环境中预装了什么软件 ?	10
我能否安装在 Shell 环境中不可用的软件 ?	10
我能否限制用户在 AWS CloudShell中可以执行的操作 ?	11
如果我想更改我的使用 AWS 区域 位置，如何从我的主目录中移动数据 AWS CloudShell ? ...	11
我能否增加 AWS CloudShell 因用户不活动而超时的限制 ?	11
我可以 AWS Console Mobile Application 从主屏幕访问 AWS CloudShell 吗 ?	11
我怎样才能 AWS CloudShell 在 AWS Console Mobile Application ?	11
在 iOS 和 Android 键盘 AWS CloudShell 中使用修改键时，我能否使用修饰键 ? AWS Console Mobile Application	12

我能否将 AWS CloudShell 选项卡显示分成多个选项卡 AWS Console Mobile Application ? ...	12
我可以访问 AWS CloudShell 吗 Console Toolbar 在移动设备上 ?	12
我的亚马逊费用 CloudShell 是VPC多少 ?	12
我可以为每个IAM委托人创建两个以上的VPC环境吗 ?	12
开始使用	13
先决条件	13
内容	14
第 1 步 : 登录 AWS Management Console	14
第 2 步 : 选择区域 AWS CloudShell , 启动并选择外壳	17
第 3 步 : 从中下载文件 AWS CloudShell	19
第 4 步 : 将文件上传到 AWS CloudShell	21
第 5 步 : 从中移除文件 AWS CloudShell	22
步骤 6 : 创建主目录备份	22
步骤 7 : 重新启动 Shell 会话	24
步骤 8 : 删除 Shell 会话主目录	24
步骤 9 : 编辑文件代码并使用命令行运行	26
步骤 10 : 使用将文件作为对象添加 AWS CLI 到 Amazon S3 存储桶中	27
相关 主题	28
教程	29
教程 : 复制多个文件	29
使用 Amazon S3 上传和下载多个文件	29
使用压缩文件夹上传和下载多个文件	33
教程 : 使用 CodeCommit	34
先决条件	34
步骤 1 : 创建和克隆存储 CodeCommit 库	34
第 2 步 : 暂存并提交文件 , 然后再将其推送到存储 CodeCommit 库	35
教程 : 创建预签名 URLs	36
先决条件	36
步骤 1 : 创建IAM角色以授予对 Amazon S3 存储桶的访问权限	37
生成预签名 URL	38
教程 : 在里面构建 Docker 容器 AWS CloudShell 并推送到亚马逊 ECR	39
先决条件	40
教程程序	40
清理	42
教程 : 使用部署 Lambda 函数 AWS CDK	42
先决条件	42

教程程序	42
清理	45
与 AWS CloudShell	46
浏览界面 AWS CloudShell	46
.....	46
在 AWS 区域	47
指定您的默认 AWS 区域 值 AWS CLI	48
处理文件和存储	49
使用 Docker	50
辅助功能	51
键盘导航 CloudShell	51
CloudShell 终端无障碍功能	51
在中选择字体大小和界面主题 CloudShell	51
使用 AWS 服务	52
AWS CLI 所选 AWS 服务的命令行示例	52
DynamoDB	52
AWS Cloud9	53
Amazon EC2	53
S3 Glacier	53
AWS Elastic Beanstalk CLI	54
Amazon ECS CLI	54
AWS SAM CLI	54
正在定制 AWS CloudShell	56
将命令行显示拆分成多个标签页	56
更改字体大小	56
更改界面主题	57
对多行文本使用安全粘贴	57
使用 tmux 到会话恢复	58
AWS CloudShell 在亚马逊 Virtual Private Cloud (亚马逊VPC) 中使用	59
操作限制	59
创建 CloudShell VPC环境	60
创建和使用 CloudShell VPC环境所需的IAM权限	61
IAM策略授予完全 CloudShell 访问权限，包括访问权限 VPC	62
为VPC环境使用IAM条件键	64
带有VPC设置条件键的策略示例	65
安全性	3

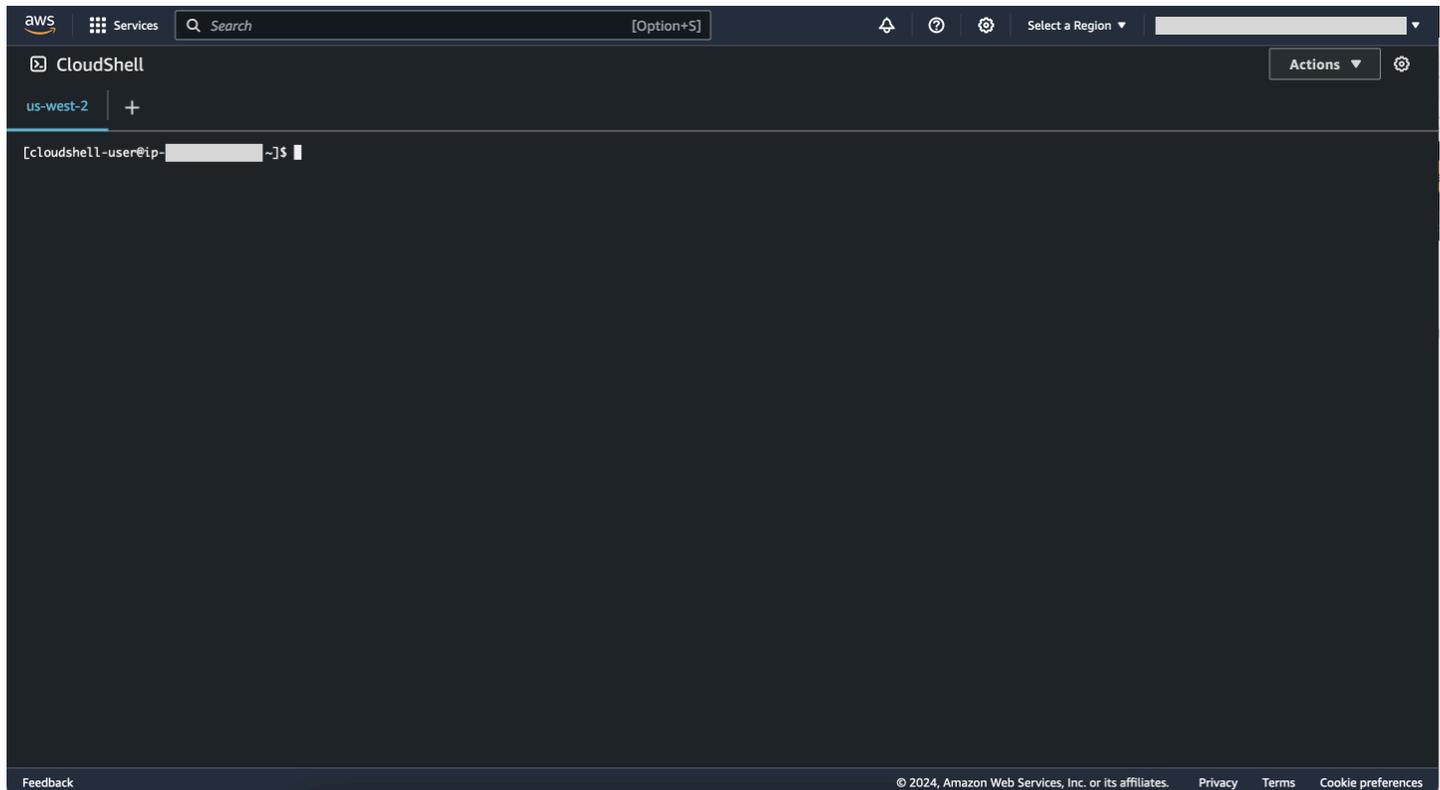
数据保护	70
数据加密	71
Identity and Access Management	72
受众	72
使用身份进行身份验证	73
使用策略管理访问	75
AWS CloudShell 如何使用 IAM	77
基于身份的策略示例	82
故障排除	85
使用IAM策略管理 AWS CloudShell 访问和使用情况	86
日记账记录和监控	99
使用监控活动 CloudTrail	100
AWS CloudShell 在 CloudTrail	100
合规性验证	102
弹性	107
基础设施安全性	107
安全最佳实操	108
安全 FAQs	108
启动和启动 shell 会话时使用了哪些 AWS 流程 CloudShell 和技术？	108
是否可以将网络访问限制为 CloudShell？	109
我可以自定义我的 CloudShell 环境吗？	109
我的 \$HOME 目录实际上存储在 AWS Cloud 中的什么地方？	109
可以加密我的 \$HOME 目录吗？	109
我能否对我的 \$HOME 目录进行病毒扫描？	109
我能否限制我的数据入口或出口？ CloudShell	110
AWS CloudShell 计算环境	111
计算环境资源	111
CloudShell 网络要求	111
预安装的软件	112
Shell	112
AWS 命令行界面 (CLI)	113
运行时和 AWSSDKs : Node.js 和 Python 3	116
开发工具和 Shell 实用程序	117
安装 AWS CLI 到你的主目录	122
在 Shell 环境中安装第三方软件	123
使用脚本修改 Shell	123

从 Amazon Linux 2 迁移到 Amazon Linux 2023	124
AWS CloudShell 迁移 FAQs	125
故障排除	127
纠正错误	127
错误：“无法启动环境。要重试，请刷新浏览器或通过选择“操作，重新启动”来重新启动 AWS CloudShell	128
错误：“无法启动环境。您没有所需的权限。请您的IAM管理员授予对 AWS CloudShell”的访 问权限	128
无法访问 AWS CloudShell 命令行	128
无法 ping 外部 IP 地址	128
准备您的终端时遇到了一些问题	129
箭头键在中无法正常工作 PowerShell	129
不支持的 Web 套接字会导致无法启动 CloudShell 会话	130
无法导入 AWSPowerShell.NetCore 模块	131
使用 Docker 时未运行 AWS CloudShell	132
Docker 的磁盘空间已经用完了	132
docker push正在超时并且一直在重试	132
无法VPC从我的 AWS CloudShell VPC环境中访问其中的资源	133
ENI AWS CloudShell 用于我的VPC环境的未清理干净	133
仅CreateEnvironment有权访问VPC环境的用户也可以访问公共 AWS CloudShell 环境 ...	133
证书在中不起作用 CloudShell	134
支持的区域	135
GovCloud 区域	136
服务限额和限制	137
持久性存储	137
每月使用量	138
命令大小	138
并发 Shell	139
Shell 会话	139
网络访问和数据传输	139
对系统文件和页面重新加载的限制	139
文档历史记录	140
.....	cxliii

什么是 AWS CloudShell ?

AWS CloudShell 是一个基于浏览器、经过预先验证的 shell，您可以直接从启动。AWS Management Console 您可以通过 AWS Management Console 几种不同的方式导航到。CloudShell 有关更多信息，请参阅[如何开始使用 AWS CloudShell ?](#)。

您可以使用首选的 shell 运行 AWS CLI 命令，例如 Bash PowerShell、或 Z shell。而且，您无需下载或安装命令行工具即可执行此操作。



启动时 AWS CloudShell，将创建一个基于亚马逊 Linux 2023 的[计算环境](#)。在此环境中，您可以访问[大量预安装的开发工具](#)、用于[上传](#)和[下载](#)文件的选项，以及在[会话之间保存的文件存储](#)。

(现在就试试吧：[入门 AWS CloudShell](#))

AWS CloudShell的特征

AWS CloudShell 提供以下功能：

AWS Command Line Interface

您可以从启动 AWS CloudShell 启动 AWS Management Console。您用于登录控制台的 AWS 凭据将在新的 shell 会话中自动可用。由于 AWS CloudShell 用户已通过预先身份验证，因此在 AWS 服务使用 AWS CLI 版本 2 进行交互时，您无需配置凭证。AWS CLI 已预先安装在外壳的计算环境中。

有关 AWS 服务使用命令行界面与进行交互的更多信息，请参阅[使用中的 AWS 服务 AWS CloudShell](#)。

Shell 和开发工具

使用为 AWS CloudShell 会话创建的 shell，您可以在首选的命令行 shell 之间无缝切换。更具体地说，您可以在两者之间切换 Bash PowerShell、和 Z shell。您还可以访问预先安装的工具和实用程序。这些包括 git, make, pip, sudo, tar, tmux, vim, wget，以及 zip。

shell 环境已预先配置为支持几种主要软件语言，例如 Node.js 以及 Python。这意味着，例如，你可以运行 Node.js 以及 Python 无需先执行运行时安装的项目。PowerShell 用户可以使用 .NET Core 运行时间。

您可以先提交在本地存储库中创建或上传 AWS CloudShell 到本地存储库的文件，然后再将这些文件推送到由管理的远程存储库 AWS CodeCommit。

有关更多信息，请参阅[AWS CloudShell 计算环境：规格和软件](#)。

持久性存储

使用 AWS CloudShell，您可以免费使用每种 AWS 区域存储空间中最多 1 GB 的永久存储空间。持久性存储位于您的主目录 (\$HOME) 中，对您而言是私有的。与每个 Shell 会话结束后回收的临时环境资源不同的是，主目录中的数据会在不同会话之间保留。

有关在持久性存储中保留数据的更多信息，请参阅[持久性存储](#)。

Note

CloudShell VPC 环境没有永久存储。当您的 VPC 环境超时（20-30 分钟处于非活动状态之后），或者当您删除或重新启动环境时，\$ HOME 目录将被删除。

CloudShell VPC环境

AWS CloudShell 虚拟私有云 (VPC) 使您能够在自己的 CloudShell 环境中创建环境VPC。对于每个 VPC环境，您可以分配VPC、添加子网以及关联一个或多个安全组。AWS CloudShell 继承的网络配置，使您能够在VPC与中的其他资源相同的子网中 AWS CloudShell 安全地使用。VPC

安全性

AWS CloudShell 环境及其用户受到特定安全功能的保护。这包括IAM权限管理、shell 会话限制和用于文本输入的安全粘贴等功能。

使用权限管理 IAM

作为管理员，您可以使用IAM策略向 AWS CloudShell 用户授予和拒绝权限。您还可以创建策略来指定用户可以在 Shell 环境中执行的特定操作。有关更多信息，请参阅 [使用IAM策略管理 AWS CloudShell 访问和使用情况](#)。

Shell 会话管理

非活动和长时间运行的会话将自动停止和回收。有关更多信息，请参阅 [Shell 会话](#)。

用于文本输入的安全粘贴

默认情况下，“安全粘贴”处于启用状态。此安全功能要求您确认要粘贴到 Shell 中的多行文本不包含恶意脚本。有关更多信息，请参阅 [对多行文本使用安全粘贴](#)。

自定义选项

您可以根据自己的确切偏好自定义 AWS CloudShell 体验。例如，您可以更改屏幕布局（多个标签页）、显示的文本大小，以及在浅色和深色界面主题之间切换。有关更多信息，请参阅 [定制您的体验 AWS CloudShell](#)。

您还可以通过[安装自己的软件](#)并使用[脚本修改外壳来扩展外壳](#)环境。

会话恢复

会话恢复功能可以恢复您在 CloudShell 终端的单个或多个浏览器选项卡上运行的会话。如果您刷新或重新打开最近关闭的浏览器标签页，则此功能会恢复会话，直到 Shell 因会话处于非活动状态而停止。要继续使用您的 CloudShell 会话，请在终端窗口中按任意键。有关 Shell 会话的更多信息，请参阅 [Shell 会话](#)。

会话恢复还可以在每个终端标签页中恢复最新的终端输出和正在运行的进程。

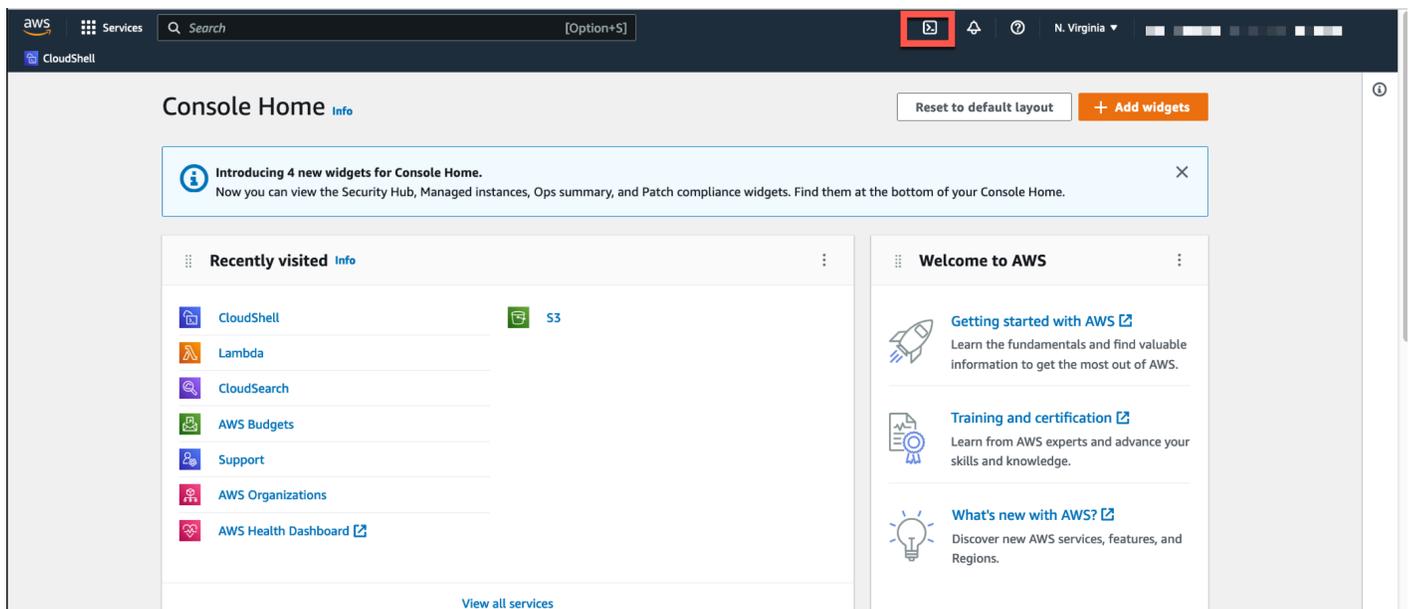
Note

会话恢复功能在移动应用程序中不可用。

如何开始 AWS CloudShell ?

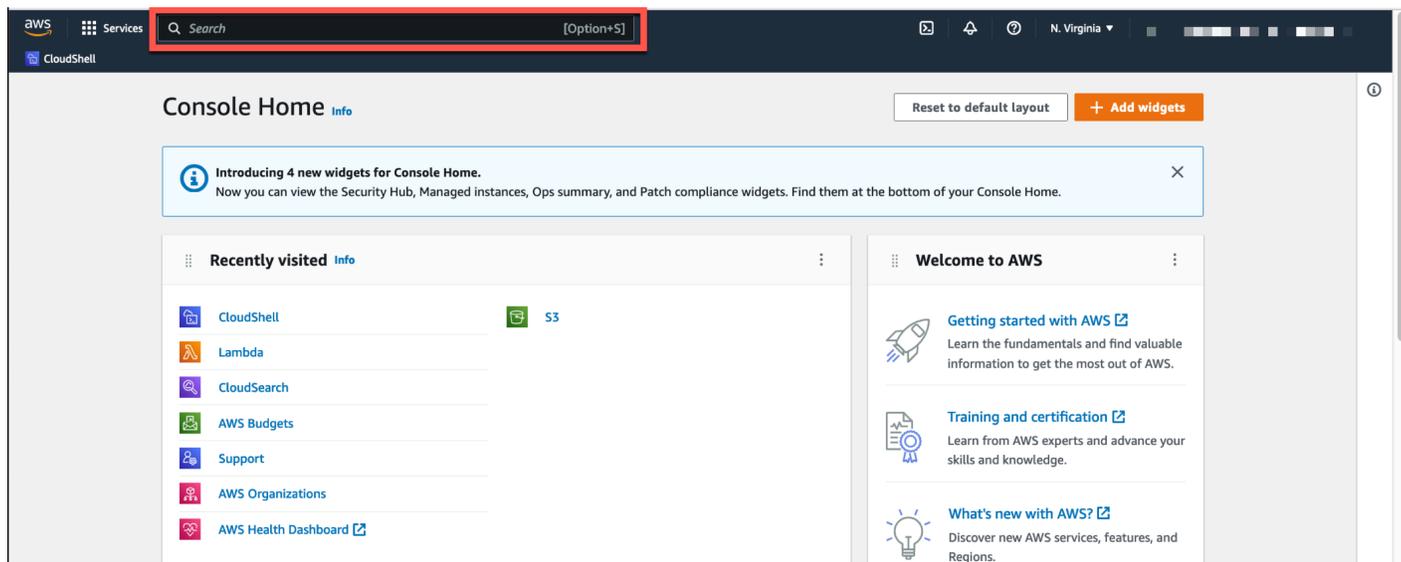
要开始使用外壳，请登录 AWS Management Console 并选择以下选项之一：

- 在导航栏上，选择图CloudShell标。



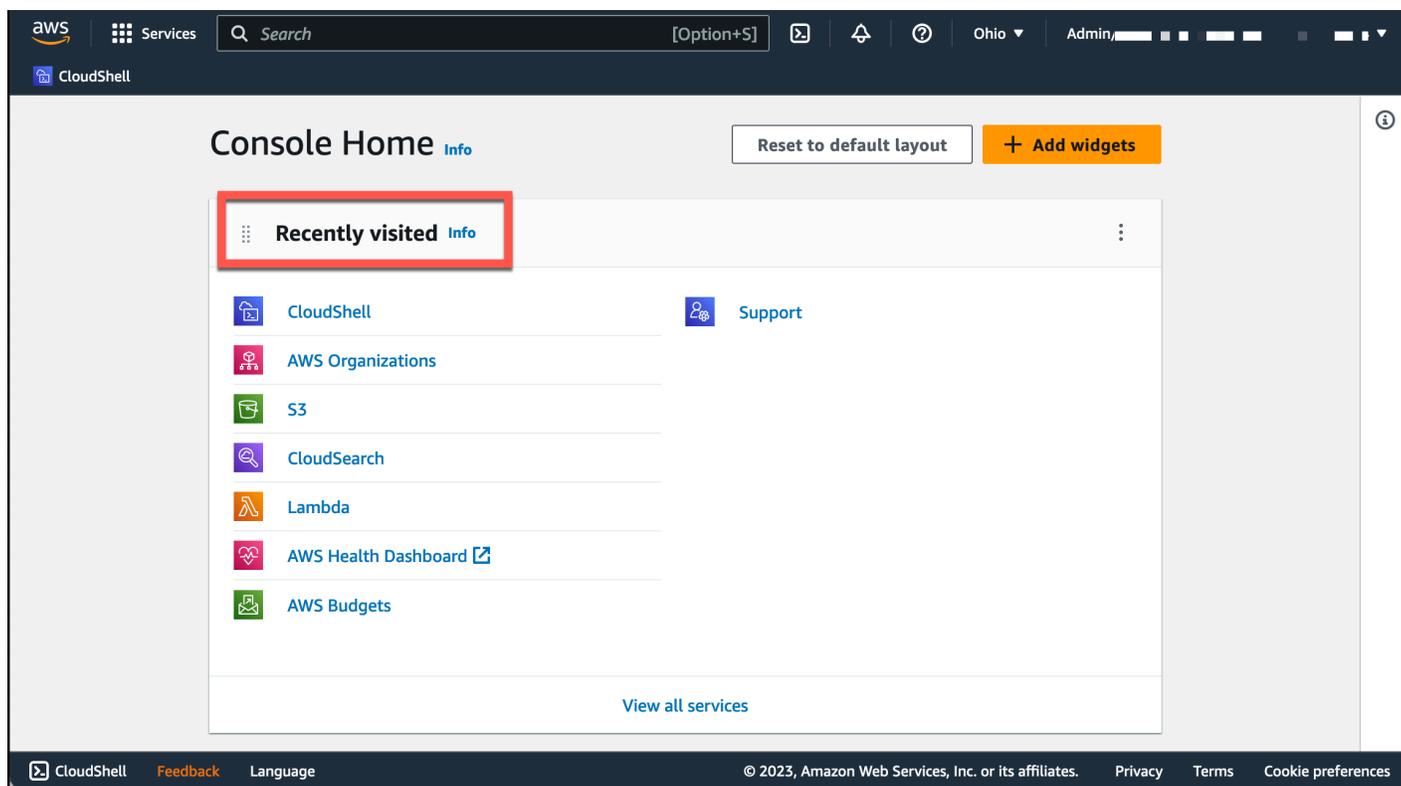
- 在“搜索”框中，键入“CloudShell”，然后选择CloudShell。

此步骤将您的 CloudShell 会话以全屏模式打开。

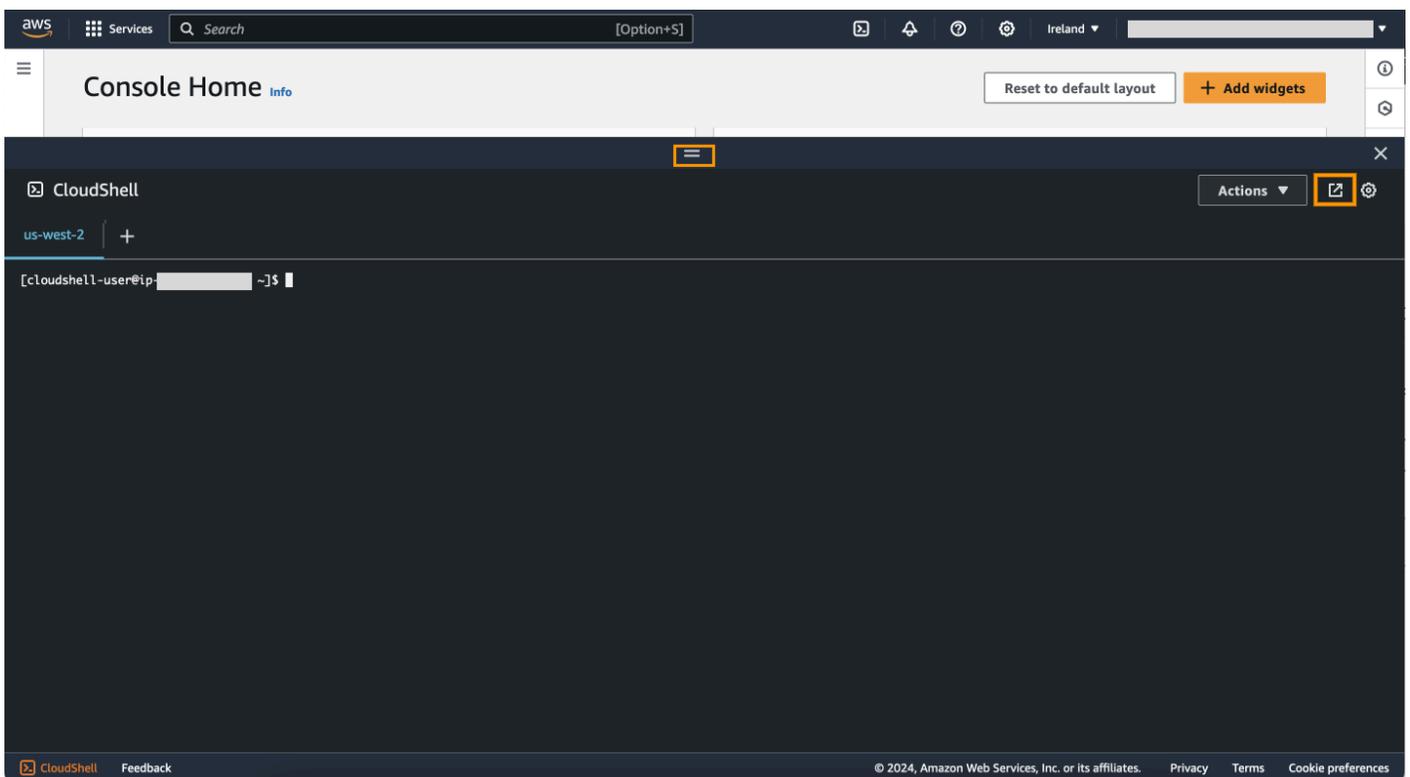
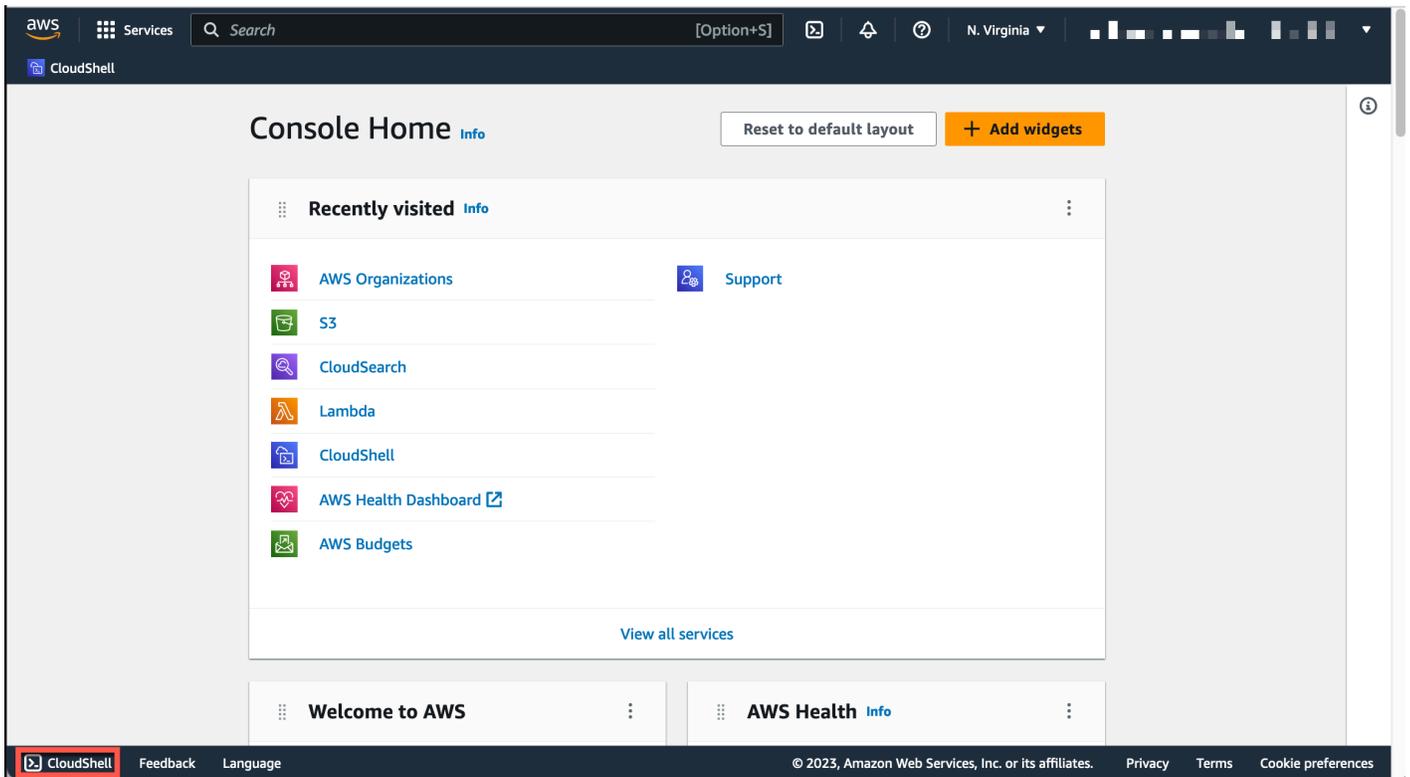


- 在“最近访问过”控件中，选择CloudShell。

此步骤将您的 CloudShell 会话以全屏模式打开。



- CloudShell在 Console Toolbar，位于控制台的左下角。您可以通过拖动来调整 CloudShell 会话的高度=。



您也可以通过单击“在新浏览器选项卡中打开”将 CloudShell 会话切换到全屏模式。

有关如何登录 AWS Management Console 和使用执行关键任务的说明 AWS CloudShell，请参阅[入门 AWS CloudShell](#)。

的定价 AWS CloudShell

AWS CloudShell AWS 服务 是免费提供的。但是，您需要为运行的其他 AWS 资源付费 AWS CloudShell。此外，[标准数据传输费用](#)也适用。有关更多信息，请参阅[AWS CloudShell 定价](#)。

有关更多信息，请参阅 [的服务配额和限制 AWS CloudShell](#)。

关键 AWS CloudShell 话题

- [入门 AWS CloudShell](#)
- [与 AWS CloudShell](#)
- [使用中的 AWS 服务 AWS CloudShell](#)
- [定制您的体验 AWS CloudShell](#)
- [AWS CloudShell 计算环境：规格和软件](#)

AWS CloudShell FAQs

以下是有关的一些常见问题的答案 AWS CloudShell。

有关安全FAQs性的更多内容，请参阅[AWS CloudShell 安全 FAQs](#)。

- [我该如何开始使用 AWS CloudShell？](#)
- [我需要访问什么 AWS CloudShell？](#)
- [AWS CloudShell 上面有什么 Console Toolbar？](#)
- [我该如何 AWS CloudShell 在 Console Toolbar？](#)
- [如何创建和管理我的 AWS CloudShell 环境？](#)
- [哪些 AWS 区域 版本 AWS CloudShell 可用？](#)
- [当您在 CloudShell 上启动时，AWS 区域 如果 AWS CloudShell 在选定区域中不可用，则会分配该选项 Console Toolbar？](#)
- [我可以在 AWS CloudShell中使用哪些类型的 Shell？](#)

- [我可以使用的哪些 Web 浏览器 AWS CloudShell ?](#)
- [当我在 AWS CloudShell 上启动时，我可以使用的哪些 Web 浏览器 Console Toolbar?](#)
- [我可以在 AWS CloudShell 上启动时下载文件吗 Console Toolbar?](#)
- [Shell 环境中预装了什么软件？](#)
- [我能否安装在 Shell 环境中不可用的软件？](#)
- [我能否限制用户在 AWS CloudShell 中可以执行的操作？](#)
- [如果我想更改我的使用 AWS 区域 位置，如何从我的主目录中移动数据 AWS CloudShell ?](#)
- [我能否增加 AWS CloudShell 因用户不活动而超时的限制？](#)
- [我可以 AWS Console Mobile Application 从主屏幕访问 AWS CloudShell 吗？](#)
- [我怎样才能 AWS CloudShell 在 AWS Console Mobile Application ?](#)
- [在我 iOS 和 Android 键盘中使用修改键时，我能否 AWS CloudShell 在键盘上使用修饰键？ AWS Console Mobile Application](#)
- [我能否将 AWS CloudShell 选项卡显示分成多个选项卡 AWS Console Mobile Application ?](#)
- [我可以在移动设备 AWS CloudShell 上访问控制台工具栏吗？](#)
- [我的亚马逊费用 CloudShell 是 VPC 多少？](#)
- [我可以为每个 IAM 委托人创建两个以上的 VPC 环境吗？](#)

我该如何开始使用 AWS CloudShell ?

只需几个步骤即可开始启动 AWS CloudShell AWS Management Console。为此，请在家中使用的您的 AWS 账户 或 IAM 凭据登录 <https://console.aws.amazon.com/console/> 主机。

有关更多信息，请参阅 [AWS CloudShell 入门](#)。

我需要访问什么 AWS CloudShell ?

由于您可以 AWS CloudShell 从进行访问 AWS Management Console，因此您必须是 IAM 能够提供有效账户别名或 ID、用户名和密码的用户。

要在控制台 AWS CloudShell 上启动，您需要附加的策略提供的 IAM 权限。有关更多信息，请参阅 [使用 IAM 策略管理 AWS CloudShell 访问和使用情况](#)。

AWS CloudShell 上面有什么 Console Toolbar?

左下角的 CloudShell 图标 AWS Management Console。

我该如何 AWS CloudShell 在 Console Toolbar?

你可以在 AWS CloudShell 上启动 Console Toolbar 通过选择控制台左下角的CloudShell图标。

哪些 AWS 区域 版本 AWS CloudShell 可用？

有关支持的服务终端节点 AWS 区域 和相关服务端点的列表，请参阅中的[AWS CloudShell 页面Amazon Web Services 一般参考](#)。

当您在 CloudShell 上启动时，AWS 区域 如果 AWS CloudShell 在选定区域中不可用，则会分配该选项 Console Toolbar?

默认区域分配给最接近选定区域的区域。有关更多信息，请参阅[选择区域 AWS CloudShell、启动和选择外壳](#)。

您可以运行该命令，该命令提供在与默认区域不同的区域中管理资源的权限。有关更多信息，请参阅[在中工作 AWS 区域](#)。

我可以在 AWS CloudShell中使用哪些类型的 Shell？

在中 AWS CloudShell，你可以使用运行命令 Bash shell PowerShell，或者 Z shell。要切换 shell，请在命令提示符下使用以下格式输入要使用的外壳名称：

- bash: 使用 Bash shell
- pwsh: 使用 PowerShell
- zsh: 使用 Z shell

我可以使用的 Web 浏览器 AWS CloudShell？

AWS CloudShell 支持最新版本的谷歌浏览器、Mozilla Firefox、Microsoft Edge 和苹果 Safari 浏览器。

如何创建和管理我的 AWS CloudShell 环境？

您的 AWS CloudShell 环境是按每个区域的IAM用户 ID 创建和管理的。你可以UserId通过运行来检查aws sts get-caller-identity。该环境归该特定区域的IAM用户 ID 所有。如果您更改IAMUserId或区域，则可以访问其他 AWS CloudShell 环境。

当我在 AWS CloudShell 上启动时，我可以使用的哪些 Web 浏览器 Console Toolbar?

你可以在 CloudShell 上启动 Console Toolbar 使用最新版本的谷歌浏览器、微软 Edge、Mozilla Firefox 和 Apple Safari 浏览器。

我可以从中下载文件 AWS CloudShell 吗？

是的，您可以在 CloudShell 上启动时下载文件 Console Toolbar 或者使用浏览器从 CloudShell 控制台页面上访问。你可以使用最新版本的谷歌浏览器和微软 Edge 浏览器下载文件。

目前，你无法使用 Mozilla Firefox 和 Apple Safari 浏览器下载文件。

Note

文件下载选项不适用于 AWS CloudShell VPC 环境。

Shell 环境中预装了什么软件？

使用为 AWS CloudShell 会话创建的 shell，您可以在首选的命令行 shell 之间无缝切换 (Bash PowerShell、和 Z shell)。您还可以访问预先安装的工具和实用程序，例如 Make, pip, sudo, tar, tmux, Vim, Wget 以及 Zip.

Shell 环境已预先配置为支持大多数主要软件语言。例如，你可以用它来运行 Node.js 以及 Python 无需先执行运行时安装的项目。PowerShell 用户可以使用 .NET Core 运行时间。

您可以将使用 shell 创建的文件或通过 shell 接口上传的文件添加到使用预安装版本管理的版本控制存储库中 git.

有关更多信息，请参阅 [预安装的软件](#)。

我能否安装在 Shell 环境中不可用的软件？

是的，AWS CloudShell 用户有 sudo 权限，并且可以从命令行安装软件。有关更多信息，请参阅 [在 Shell 环境中安装第三方软件](#)。

我能否限制用户在 AWS CloudShell中可以执行的操作？

可以，您可以控制用户在 AWS CloudShell中可执行的操作。例如，您可以允许用户访问 AWS CloudShell 但禁止他们在 shell 环境中上传或下载文件。或者，您可以完全阻止用户访问 AWS CloudShell。有关更多信息，请参阅 [使用IAM策略管理 AWS CloudShell 访问和使用情况](#)。

如果我想更改我的使用 AWS 区域 位置，如何从我的主目录中移动数据 AWS CloudShell？

要将 AWS CloudShell 数据从一个区域移动 AWS 区域 到另一个区域，请先将一个区域的主目录的内容下载到本地计算机，然后从该区域上传到另一个区域的主目录。有关更多信息，请参阅 [???](#)。

Note

上传和下载选项不适用于 AWS CloudShell VPC环境。

我能否增加 AWS CloudShell 因用户不活动而超时的限制？

如果您不 AWS CloudShell 使用键盘或指针进行交互，则外壳会话将在大约 20-30 分钟后自动结束。正在运行的进程不算作交互。由于专 CloudShell 为有针对性、基于任务的活动而设计，因此目前没有计划增加此[超时](#)限制。

如果您想使用更灵活的超时时间来执行基于终端 AWS 服务 的任务，我们建议您使用基于云IDE的或启动并[连接到 Amazon 实例](#)。 [AWS Cloud9EC2](#)

我可以 AWS Console Mobile Application 从主屏幕访问 AWS CloudShell 吗？

是的，您可以 AWS Console Mobile Application 通过登录 Console Mobile Application 进行访问 AWS CloudShell 。有关更多信息，请参阅 [《AWS Console Mobile Application 用户指南》](#)。

我怎样才能 AWS CloudShell 在 AWS Console Mobile Application ？

您可以使用以下方法之一启动 AWS CloudShell ：

1. 选择导航栏底部的 AWS CloudShell 图标。
2. 在服务菜单上选择 AWS CloudShell。

Note

目前，您无法在中创建或启动VPC环境 AWS Console Mobile Application。

在 iOS 和 Android 键盘 AWS CloudShell 中使用修改键时，我能否使用修饰键？ AWS Console Mobile Application

是的，您可以在 iOS 和 Android 键盘上使用修饰键。有关更多信息，请参阅 [AWSConsole Mobile Application 用户指南](#)。

我能否将 AWS CloudShell 选项卡显示分成多个选项卡 AWS Console Mobile Application？

不，目前您无法在移动应用程序上运行多个 AWS CloudShell 选项卡。

我可以访问 AWS CloudShell 吗 Console Toolbar 在移动设备上？

不，目前您无法访问 AWS CloudShell Console Toolbar 在您的移动设备上。

我的亚马逊费用 CloudShell 是VPC多少？

连接到您的私有设备VPC并访问其中的资源是免费的。Private VPC 内部的数据传输已包含在您的VPC账单中，您VPCs之间的数据传输费用与您当前的费用相同 CloudShell。 CloudShell

我可以为每个IAM委托人创建两个以上的VPC环境吗？

不是。您最多只能创建两个VPC环境。

入门 AWS CloudShell

本入门教程向您展示如何使用 shell 命令行界面启动 AWS CloudShell 和执行关键任务。

首先，您登录 AWS Management Console 并选择一个 AWS 区域。然后，您可以在新的浏览器窗口 CloudShell 中启动，并选择要使用的外壳类型。

接下来，在主目录中创建一个新文件夹，然后从本地计算机上传一个文件到该文件夹。在从命令行将该文件作为程序运行之前，您可以使用预安装的编辑器处理文件。最后，您调用 AWS CLI 命令创建 Amazon S3 存储桶，并将您的文件作为对象添加到该存储桶。

先决条件

IAM权限

您可以 AWS CloudShell 通过将以下 AWS 托管策略附加到您的IAM身份（例如用户、角色或组）来获取权限：

- `AWSCloudShellFullAccess`：为用户提供对 AWS CloudShell 及其功能的完全访问权限。

在本教程中，您还可以与之互动 AWS 服务。更具体地说，您可以通过创建 S3 存储桶并向该存储桶添加对象来与 Amazon S3 进行交互。您的IAM身份需要一个至少授予 `s3:CreateBucket` 和 `s3:PutObject` 权限的策略。

有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 [Amazon S3 操作](#)。

练习文件

此练习还包括上传和编辑一个文件，然后在命令行界面中将该文件作为程序运行。在本地计算机上打开文本编辑器并添加以下代码段。

```
import sys
x=int(sys.argv[1])
y=int(sys.argv[2])
sum=x+y
print("The sum is",sum)
```

使用文件名 `add_prog.py` 保存该文件。

内容

- [第 1 步：登录 AWS Management Console](#)
- [第 2 步：选择区域 AWS CloudShell，启动并选择外壳](#)
- [第 3 步：从中下载文件 AWS CloudShell](#)
- [第 4 步：将文件上传到 AWS CloudShell](#)
- [第 5 步：从中移除文件 AWS CloudShell](#)
- [步骤 6：创建主目录备份](#)
- [步骤 7：重新启动 Shell 会话](#)
- [步骤 8：删除 Shell 会话主目录](#)
- [步骤 9：编辑文件代码并从命令行运行](#)
- [步骤 10：使用将文件作为对象添加 AWS CLI 到 Amazon S3 存储桶中](#)

第 1 步：登录 AWS Management Console

此步骤包括输入您的IAM用户信息以访问 AWS Management Console。如果您已经在控制台中，请跳至[步骤 2](#)。

- 您可以使用IAM用户登录URL或转到主登录页面来访问。AWS Management Console

IAM user sign-in URL

- 打开浏览器并输入以下登录URL信息。将 `account_alias_or_id` 替换为管理员提供的账户别名或账户 ID。

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

- 输入您的IAM登录凭据，然后选择登录。

Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Password

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Main sign-in page

- 打开<https://aws.amazon.com/console/>。
- 如果您之前没有使用此浏览器登录过，则会显示主登录页面。选择IAM用户，输入账户别名或账户 ID，然后选择下一步。

Sign in

Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user

User within an account that performs daily tasks. [Learn more](#)

Account ID (12 digits) or account alias

Next

- 如果您之前已经以IAM用户身份登录。浏览器可能会记住 AWS 账户的账户别名或账户 ID。如果是，请输入您的IAM登录凭据并选择登录。

Sign in as IAM user

Account ID (12 digits) or account alias

account_alias_or_id

IAM user name

Password

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Note

您也可以以[根用户](#)身份登录。此身份可以完全访问账户中的所有资源 AWS 服务和资源。但是，我们强烈建议您不要使用根用户来执行日常任务，即使是管理任务。相反，请遵循仅使用 root 用户来创建您的第一个 IAM 用户的最佳实践。

第 2 步：选择区域 AWS CloudShell，启动并选择外壳

在此步骤中，您将 AWS CloudShell 从控制台界面启动，选择可用的 shell AWS 区域，然后切换到您的首选 shell，例如 Bash PowerShell、或 Z shell。

1. 要选择 AWS 区域 要工作的区域，请前往“选择区域”菜单，然后选择要使用的[支持 AWS 区域](#)。（可用区域突出显示。）

Important

如果您切换区域，则界面会刷新，所选 AWS 区域 的名称将显示在命令行文本的上方。您添加到持久性存储空间的所有文件都仅在同一 AWS 区域可用。如果您更改区域，则可以访问不同的存储空间和文件。

Important

当您在 CloudShell 上启动时，如果 CloudShell 在选定区域中不可用 Console Toolbar，在控制台的左下角，默认区域设置为最接近所选区域的区域。您可以运行该命令，该命令提供在与默认区域不同的区域中管理资源的权限。有关更多信息，请参阅[在中工作 AWS 区域](#)。

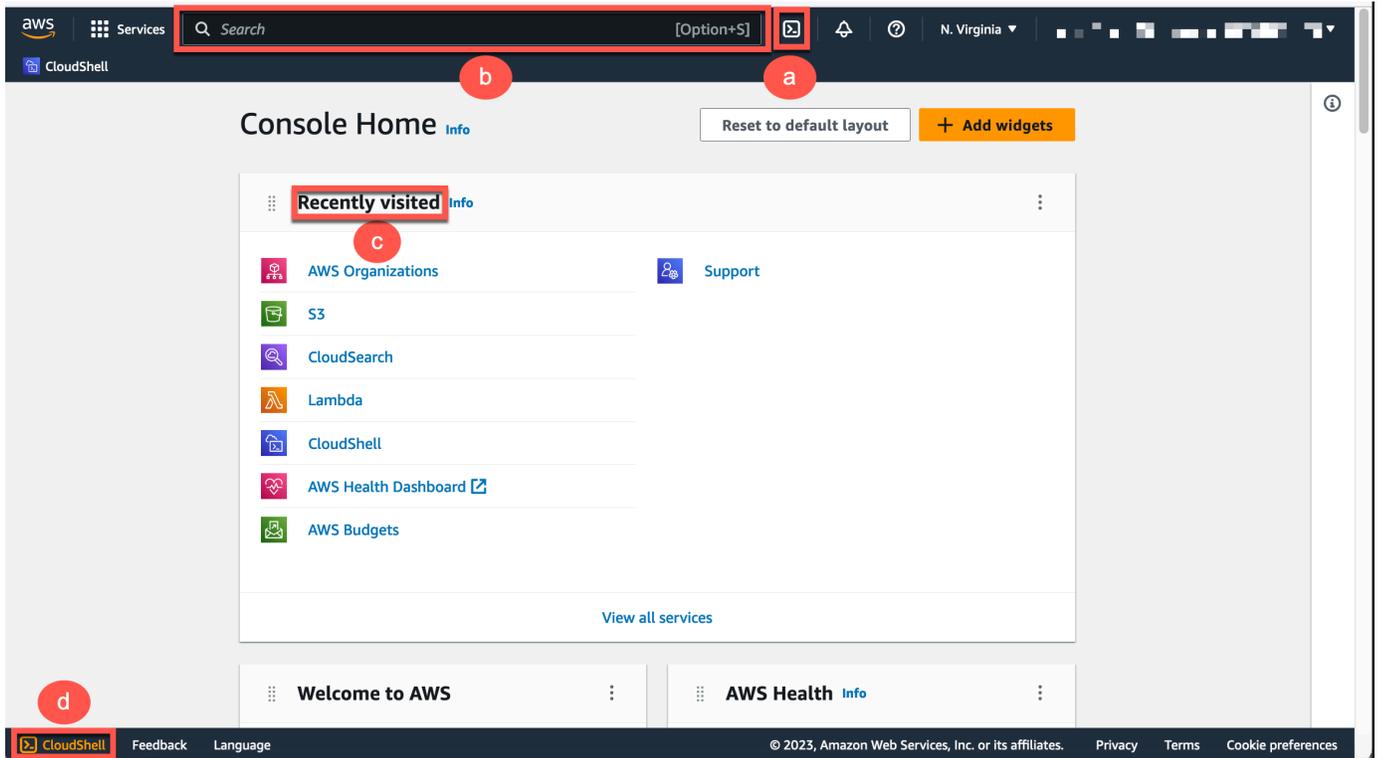
Example**示例**

如果你选择欧洲（西班牙）eu-south-2 但在欧洲（西班牙）CloudShell 不可用 eu-south-2，则默认区域设置为欧洲（爱尔兰）eu-west-1，它离欧洲最近（西班牙）eu-south-2。

您将使用默认区域欧洲（爱尔兰）的服务配额 eu-west-1 并且将在所有地区恢复相同的会话 CloudShell 话。默认区域可能会更改，CloudShell 浏览器窗口中将通知您。

2. 从中 AWS Management Console，您可以 CloudShell 通过选择以下选项之一来启动：

1. 在导航栏上，选择图CloudShell标。
2. 在“搜索”框中，键入“CloudShell”，然后选择CloudShell。
3. 在“最近访问过”控件中，选择CloudShell。
4. 在“CloudShell上选择” Console Toolbar，位于控制台的左下角。
 - 要调整会话 CloudShell 话的高度，请拖动=。
 - 要将您的 CloudShell 会话切换到全屏模式，请单击“在新浏览器选项卡中打开”图标。



当系统显示命令提示符时，表示 shell 已经准备就绪，可以进行交互。

Note

如果您遇到阻碍您成功启动或与之交互的问题 AWS CloudShell，请在中查看信息以识别和解决这些问题[故障排除 AWS CloudShell](#)。

3. 要选择要使用的预安装 Shell，请在命令行提示栏中输入以下程序名称之一：

Bash

bash

如果你切换到 Bash，命令提示符处的符号将更新为\$。

Note

Bash 是你启动时正在运行的默认 shell AWS CloudShell。

PowerShell

pwsh

如果切换到 PowerShell，则命令提示符处的符号将更新为PS>。

Z shell

zsh

如果你切换到 Z shell，命令提示符处的符号将更新为%。

有关 shell 环境中预安装的版本的信息，请参阅[AWS CloudShell 计算环境](#)部分的 [shell 表](#)。

第 3 步：从中下载文件 AWS CloudShell

Note

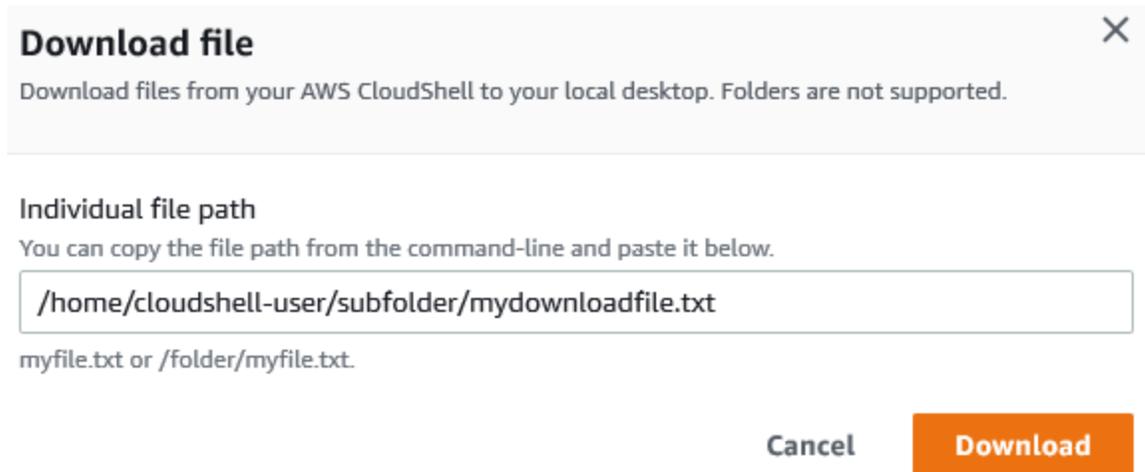
此选项不适用于VPC环境。

此步骤指导您完成下载文件的过程。

1. 要下载文件，请转到操作，然后从菜单中选择下载文件。

将显示下载文件对话框。

2. 在下载文件对话框中，输入要下载的文件的路径。



Note

指定要下载的文件时，可以使用绝对路径或相对路径。对于相对路径名，默认情况下 /home/cloudshell-user/ 会自动添加到开头。因此，要下载名为 mydownload-file 的文件，以下两个路径都是有效的路径：

- 绝对路径：/home/cloudshell-user/subfolder/mydownloadfile.txt
- 相对路径：subfolder/mydownloadfile.txt

3. 选择下载。

如果文件路径正确，则会显示一个对话框。您可以使用此对话框通过默认应用程序打开文件。或者，您可以将文件保存到本地计算机上的某个文件夹。

Note

当您在 CloudShell 上启动时，“下载”选项不可用 Console Toolbar。您可以从 CloudShell 控制台或使用 Chrome 网络浏览器下载文件。有关如何下载文件的更多信息，请参阅[步骤 3：从下载文件 AWS CloudShell](#)。

第 4 步：将文件上传到 AWS CloudShell

Note

此选项不适用于VPC环境。

此步骤介绍如何上传文件，然后将其移至主目录中的新目录。

1. 要检查当前的工作目录，请在提示符下输入以下命令：

```
pwd
```

当您按 Enter 键时，Shell 会返回您当前的工作目录（例如，`/home/cloudshell-user`）。

2. 要将文件上传到该目录，请转至操作并从菜单中选择上传文件。

将显示上传文件对话框。

3. 选择 Browse。
4. 在系统的文件上传对话框中，选择您为本教程（`add_prog.py`）创建的文本文件，然后选择打开。
5. 在上传对话框里，选择添加文件。

进度条会跟踪上传情况。如果上传成功，则会显示一条消息，确认 `add_prog.py` 已添加到主目录的根目录中。

6. 要为文件创建目录，请输入 `make directories` 命令：`mkdir mysub_dir`。
7. 要将上传的文件从主目录的根目录移动到新目录，请使用 `mv` 命令：

```
mv add_prog.py mysub_dir.
```

8. 要将工作目录更改为新目录，请输入 `cd mysub_dir`。

命令提示符会更新以表明您已更改工作目录。

9. 要查看当前目录 `mysub_dir` 的内容，请输入 `ls` 命令。

列出工作目录的内容。这包括您刚刚上传的文件。

第 5 步：从中移除文件 AWS CloudShell

此步骤介绍如何从中删除文件 AWS CloudShell。

1. 要从中删除文件 AWS CloudShell，请使用标准 shell 命令，例如 `rm`（删除）。

```
rm my-file-for-removal
```

2. 要移除多个符合指定条件的文件，请运行 `find` 命令。

以下示例删除了名称中包含后缀“.pdf”的所有文件。

```
find -type f -name '*.pdf' -delete
```

Note

假设您停止 AWS CloudShell 在特定环境中使用 AWS 区域。然后，该区域的持续性存储中的数据将在指定时间段后自动删除。更多信息，请参阅[持久性存储](#)。

步骤 6：创建主目录备份

此步骤介绍如何创建主目录备份。

1. 创建备份文件

在主目录之外创建一个临时文件夹。

```
HOME_BACKUP_DIR=$(mktemp --directory)
```

您可以使用以下方法之一创建备份：

- a. 使用 `tar` 创建备份文件

要使用 `tar` 创建备份文件，请输入以下命令：

```
tar \  
  --create \  
  --gzip \  
  --verbose \  
  ...
```

```
--file=${HOME_BACKUP_DIR}/home.tar.gz \  
[--exclude ${HOME}/.cache] \ // Optional  
${HOME}/  
echo "Home directory backed up to this file: ${HOME_BACKUP_DIR}/home.tar.gz"
```

b. 使用 zip 创建备份文件

要使用 zip 创建备份文件，请输入以下命令：

```
zip \  
--recurse-paths \  
${HOME_BACKUP_DIR}/home.zip \  
${HOME} \  
[--exclude ${HOME}/.cache/\*] // Optional  
echo "Home directory backed up to this file: ${HOME_BACKUP_DIR}/home.zip"
```

2. 将备份文件传输到外面 CloudShell

您可以使用以下选项之一将备份文件传输到外部 CloudShell：

a. 将备份文件下载到本地计算机上

您可以下载在先前步骤中创建的文件。有关如何从中下载文件的更多信息 CloudShell，请参阅[从下载文件 AWS CloudShell](#)。

在“下载文件”对话框中，输入要下载的文件的路径（例如，`/tmp/tmp.iA99tD9L98/home.tar.gz`）。

b. 将备份文件传输到 S3

要生成存储桶，请输入以下命令：

```
aws s3 mb s3://${BUCKET_NAME}
```

用于AWSCLI将文件复制到 S3 存储桶：

```
aws s3 cp ${HOME_BACKUP_DIR}/home.tar.gz s3://${BUCKET_NAME}
```

Note

可能会收取数据传输费用。

3. 直接备份到 S3 存储桶

要直接备份到 S3 存储桶，请输入以下命令：

```
aws s3 cp \  
  ${HOME}/ \  
  s3://${BUCKET_NAME} \  
  --recursive \  
  [--exclude .cache/\^*] // Optional
```

步骤 7：重新启动 Shell 会话

此步骤介绍如何重新启动 shell 会话。

Note

作为一项安全措施，如果您长时间不使用键盘或指针与 Shell 进行交互，则会话会自动停止。长时间运行的会话也会自动停止。有关更多信息，请参阅 [Shell 会话](#)。

1. 要重新启动 Shell 会话，请选择操作、重新启动。

系统会通知您，重新启动会 AWS CloudShell 停止当前 AWS 区域的所有活动会话。

2. 要确认，请选择重新启动。

接口显示一条消息，表示 CloudShell 计算环境正在停止。环境停止并重新启动后，您可以开始在新会话中使用命令行。

Note

在某些情况下，环境重新启动可能需要几分钟时间。

步骤 8：删除 Shell 会话主目录

此步骤介绍如何删除 shell 会话。

Note

此选项不适用于VPC环境。重新启动VPC环境时，其主目录将被删除。

Warning

删除主目录是一项不可逆的操作，即存储在主目录中的所有数据将被永久删除。但是，在以下情况下，您可以考虑使用此选项：

- 您错误地修改了文件并且无法访问 AWS CloudShell 计算环境。删除您的主目录会 AWS CloudShell 恢复其默认设置。
- 您想 AWS CloudShell 立即从中删除所有数据。如果您停止 AWS CloudShell 在某个 AWS 区域中使用，则永久存储将在[保留期结束时自动删除](#)，除非您在该地区 AWS CloudShell 重新启动。

如果您需要长期存储文件，请考虑使用诸如 Amazon S3 或之类的服务 CodeCommit。

1. 要删除 shell 会话，请选择操作、删除。

系统会通知您，删除 AWS CloudShell 主目录会删除当前存储在您的 AWS CloudShell 环境中的所有数据。

Note

您不能撤消此操作。

2. 要确认删除操作，请在文本输入字段中输入位置名称，然后选择 删除。

AWS CloudShell 停止当前所有活动会话 AWS 区域 并立即创建新环境。

手动退出 Shell 会话

使用命令行，您可以退出 Shell 会话并使用 `exit` 命令进行注销。然后，您可以按任意键重新连接并继续使用 AWS CloudShell。

步骤 9：编辑文件代码并使用命令行运行

此步骤演示如何使用预安装的 Vim 编辑器来处理文件。然后，您可以从命令行将该文件作为程序运行。

1. 要编辑您在上一步骤中上传的文件，请输入以下命令：

```
vim add_prog.py
```

shell 界面将刷新以显示 Vim 编辑。

2. 要在中编辑文件 Vim，按 I 键。现在编辑内容，让程序将三个数字而不是两个数字相加。

```
import sys
x=int(sys.argv[1])
y=int(sys.argv[2])
z=int(sys.argv[3])
sum=x+y+z
print("The sum is",sum)
```

Note

如果您将文本粘贴到编辑器中并启用了[安全粘贴功能](#)，则会显示一条警告。复制的多行文本可能包含恶意脚本。使用“安全粘贴”功能，您可以在粘贴之前验证完整的文本。如果您对文本安全感到满意，请选粘贴。

3. 编辑程序后，按键 Esc 进入 Vim 命令模式。然后，输入 :wq 命令保存文件，并退出编辑器。

Note

如果你是新手 Vim 命令模式，您最初可能会发现很难在命令模式和插入模式之间切换。保存文件和退出应用程序时使用命令模式。插入新文本时使用插入模式。要进入插入模式，请按 I；要进入命令模式，请按 Esc。有关 Vim 以及中提供的其他工具 AWS CloudShell，请参阅[开发工具和 Shell 实用程序](#)。

4. 在主命令行界面上，运行以下程序并指定要输入的三个数字。语法如下所示。

```
python3 add_prog.py 4 5 6
```

命令行显示程序输出：The sum is 15。

步骤 10：使用将文件作为对象添加 AWS CLI 到 Amazon S3 存储桶中

在此步骤中，您将创建一个 Amazon S3 存储桶，然后使用 PutObject 方法将您的代码文件作为对象添加到该存储桶中。

Note

在大多数情况下，您可以将软件文件提交 [CodeCommit 在中使用 AWS CloudShell](#) 到版本控制的存储库中。本教程介绍如何使用 AWS CLI 在 AWS CloudShell 与其他 AWS 服务进行交互。使用此方法时，无需下载或安装任何其他资源。此外，由于已经在 Shell 中进行了身份验证，因此在调用之前无需配置凭证。

1. 要在指定的存储桶中创建存储桶 AWS 区域，请输入以下命令：

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

Note

如果您要在 us-east-1 区域之外创建存储桶，请使用 LocationConstraint 参数添加 create-bucket-configuration 以指定区域。以下是示例语法。

```
$ aws s3api create-bucket --bucket my-bucket --region eu-west-1 --create-bucket-configuration LocationConstraint=eu-west-1
```

如果调用成功，命令行将显示来自服务的响应，输出与以下类似。

```
{
  "Location": "/insert-unique-bucket-name-here"
}
```

Note

如果您不遵守[命名存储桶的规则](#)，则会显示以下错误：调用 CreateBucket操作时出现错误 (InvalidBucketName)：指定的存储桶无效。

- 要上传文件并将该文件作为对象添加到您刚创建的存储桶，请调用 PutObject 方法。

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body add_prog.py
```

将对象上传到 Amazon S3 存储桶后，命令行将显示来自服务的响应，类似于以下输出：

```
{"ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebee56\""} 
```

ETag 是存储的对象的哈希值。您可以使用此哈希值来[检查上传到 Amazon S3 的对象的完整性](#)。

相关主题

- [使用中的 AWS 服务 AWS CloudShell](#)
- [在本地计算机之间复制多个文件和 CloudShell](#)
- [CodeCommit 在中使用 AWS CloudShell](#)
- [与 AWS CloudShell](#)
- [定制您的体验 AWS CloudShell](#)

AWS CloudShell 教程

以下教程向您展示了在使用时如何进行实验和测试不同的功能和集成。AWS CloudShell

教程概述	了解更多
正在复制多个文件	the section called “教程：复制多个文件”
使用 CodeCommit	???
创建预签名 URLs	???
在里面建一个 Docker 容器AWS CloudShell 然后推送到亚马逊 ECR	???
使用部署 Lambda 函数 AWS CDK	???

在本地计算机之间复制多个文件和 CloudShell

本教程介绍如何在本地计算机和之间复制多个文件 CloudShell。

使用该 AWS CloudShell 接口，您可以一次在本地计算机和 shell 环境之间上传或下载单个文件。要同时在本本地计算机 CloudShell 之间复制多个文件，请使用以下选项之一：

- Amazon S3：在本地计算机和 CloudShell之间复制文件时，使用 S3 存储桶作为中介。
- 压缩文件：将多个文件压缩到一个压缩文件夹中，可以使用该 CloudShell 界面上传或下载这些文件。

Note

由于 CloudShell 不允许传入的互联网流量，因此目前无法使用scp或rsync之类的命令在本地计算机和 CloudShell 计算环境之间复制多个文件。

使用 Amazon S3 上传和下载多个文件

此步骤介绍如何使用 Amazon S3 上传和下载多个文件。

先决条件

要使用存储桶和对象，您需要一个IAM策略来授予执行以下 Amazon S3 API 操作的权限：

- `s3:CreateBucket`
- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

有关 Amazon S3 操作的完整列表，请参阅《亚马逊简单存储服务API参考》中的[操作](#)。

AWS CloudShell 使用 Amazon S3 将多个文件上传到

此步骤介绍如何使用 Amazon S3 上传多个文件。

1. 在中 AWS CloudShell，通过运行以下s3命令创建 S3 存储桶：

```
aws s3api create-bucket --bucket your-bucket-name --region us-east-1
```

如果调用成功，命令行将显示来自 S3 服务的响应：

```
{
  "Location": "/your-bucket-name"
}
```

2. 将目录中的文件从本地计算机上传到存储桶。请选择以下选项之一来上传文件：

- AWS Management Console：用于 drag-and-drop 将文件和文件夹上传到存储桶。
- AWS CLI：在本地计算机上安装该版本版本的工具后，使用命令行将文件和文件夹上传到存储桶。

Using the console

- 打开 Amazon S3 控制台，网址为<https://s3.console.aws.amazon.com/s3/>。

(如果您正在使用 AWS CloudShell，则应该已经登录到控制台。)

- 在 桶列表中，请选择要将文件夹和文件上传到的桶的名称。您也可以通过选择创建存储桶来创建自己选择的存储桶。

- 要将文件上传到文件夹，请选择要上传的文件，然后选择 上传。然后，将您选择的文件和文件夹拖放到列出目标存储桶中的对象的控制台窗口，或者选择添加文件或添加文件夹。

Upload (上传) 页面上将列出所选文件。

- 选中复选框以指示要添加的文件。
- 要将所选文件添加到存储桶，请选择上传。

Note

有关更多信息，请参阅 Amazon Simple Storage Service 控制台用户指南中的[如何将文件和文件夹上传到 S3 存储桶](#)。

Using AWS CLI

Note

对于此选项，您需要在本地计算机上安装该 AWS CLI 工具，并配置用于调用 AWS 服务的凭据。有关更多信息，请参阅 [用户指南。AWS Command Line Interface](#)

- 启动该 AWS CLI 工具并运行以下 `aws s3` 命令，将指定的存储桶与本地计算机上当前目录的内容同步：

```
aws s3 sync folder-path s3://your-bucket-name
```

如果同步成功，则会显示添加到存储桶的每个对象的上传消息。

3. 返回 CloudShell 命令行并输入以下命令，将 shell 环境中的目录与 S3 存储桶的内容同步：

```
aws s3 sync s3://your-bucket-name folder-path
```

Note

您还可以将 `--exclude "<value>"` 和 `--include "<value>"` 参数添加至 `sync` 命令来执行模式匹配以排除或包含特定文件或对象。

有关更多信息，请参阅AWS CLI 命令参考中的[使用 Exclude 和 Include 筛选条件](#)。

如果同步成功，则会显示从存储桶下载到目录的每个文件的下载消息。

Note

应用同步命令时，仅以递归方式将源目录中的新文件和更新过的文件复制到目标位置。

AWS CloudShell 使用 Amazon S3 下载多个文件

此步骤介绍如何使用 Amazon S3 下载多个文件。

1. 使用 AWS CloudShell 命令行输入以下 `aws s3` 命令，将 S3 存储桶与 shell 环境中当前目录的内容同步：

```
aws s3 sync folder-path s3://your-bucket-name
```

Note

您还可以将 `--exclude "<value>"` 和 `--include "<value>"` 参数添加至 `sync` 命令来执行模式匹配以排除或包含特定文件或对象。

有关更多信息，请参阅AWS CLI 命令参考中的[使用 Exclude 和 Include 筛选条件](#)。

如果同步成功，则会显示添加到存储桶的每个对象的上传消息。

2. 将桶内容下载到本地计算机上。由于 Amazon S3 控制台不支持下载多个对象，因此您需要使用安装在本地计算机上的 AWS CLI 工具。

在该 AWS CLI 工具的命令行中，运行以下命令：

```
aws s3 sync s3://your-bucket-name folder-path
```

如果同步成功，命令行将显示在目标目录中更新或添加的每个文件的下载消息。

Note

对于此选项，您需要在本地计算机上安装该 AWS CLI 工具，并配置用于调用 AWS 服务的凭据。有关更多信息，请参阅 [用户指南。AWS Command Line Interface](#)

使用压缩文件夹上传和下载多个文件

此步骤介绍如何使用压缩文件夹上传和下载多个文件。

使用 zip/unzip 实用程序，您可以压缩存档中的多个文件，这些文件可以视为单个文件。这些实用程序已预先安装在 CloudShell 计算环境中。

有关预安装工具的更多信息，请参阅 [开发工具和 Shell 实用程序](#)。

AWS CloudShell 使用压缩文件夹将多个文件上传到

此步骤介绍如何使用压缩文件夹上传多个文件。

1. 在本地计算机上，将要上传的文件添加到压缩文件夹中。
2. 启动 CloudShell，然后选择操作，上传文件。
3. 在上传文件对话框中，选择选择文件，然后选择您刚创建的压缩文件夹。
4. 在上传文件对话框中，选择上传，将所选文件添加到 Shell 环境中。
5. 在 CloudShell 命令行中，运行以下命令将 zip 存档的内容解压缩到指定目录：

```
unzip zipped-files.zip -d my-unzipped-folder
```

AWS CloudShell 使用压缩文件夹下载多个文件

此步骤介绍如何使用压缩文件夹下载多个文件。

1. 在 CloudShell 命令行中，运行以下命令将当前目录中的所有文件添加到压缩文件夹：

```
zip -r zipped-archive.zip *
```

2. 选择操作、下载文件。
3. 在下载文件对话框中，输入压缩文件夹的路径（例如 `/home/cloudshell-user/zip-folder/zipped-archive.zip`），然后选择下载。

如果路径正确，浏览器对话框将提供打开压缩文件夹或将其保存到本地计算机的选项。

4. 现在，您可以在本地计算机上解压缩下载的压缩文件夹中的内容。

CodeCommit 在中使用 AWS CloudShell

CodeCommit 是一项安全、高度可扩展且托管的源代码控制服务，用于托管私有 Git 存储库。使用 AWS CloudShell，您可以使用该 `git-remote-codecommit` 实用程序在命令行 CodeCommit 上使用。此实用程序已预先安装在 AWS CloudShell 计算环境中，提供了一种从 CodeCommit 存储库中推送和提取代码的简单方法。该实用程序通过扩展 Git 来实现此目的。有关更多信息，请参阅 [用户指南。AWS CodeCommit](#)

本教程介绍如何创建 CodeCommit 存储库并将其克隆到您的 AWS CloudShell 计算环境。您还将学习如何将文件暂存并提交到克隆的存储库，然后再将其推送到在 CI AWS Cloud 中管理的远程存储库。

先决条件

有关 IAM 用户需要使用的权限的信息 AWS CloudShell，请参阅 [入门教程中的先决条件部分](#)。您还需要 [IAM 权限](#) 才能使用 CodeCommit。

此外，在开始之前，请确保具备以下条件：

- 对 Git 命令和版本控制概念的基本了解
- Shell 主目录中的文件，可以提交到本地和远程存储库。在本教程中，它被称为 `my-git-file`。

步骤 1：创建和克隆存储 CodeCommit 库

此步骤介绍如何创建和克隆 CodeCommit 存储库。

1. 在 CloudShell 命令行界面中，输入以下 `codecommit` 命令以创建名为 `MyDemoRepo` 的 CodeCommit 存储库 `MyDemoRepo`。

```
aws codecommit create-repository --repository-name MyDemoRepo --repository-  
description "My demonstration repository"
```

如果成功创建了存储库，则命令行会显示服务的响应。

```
{  
  "repositoryMetadata": {
```

```
"accountId": "111122223333",
"repositoryId": "0dcd29a8-941a-1111-1111-11111111111a",
"repositoryName": "MyDemoRepo",
"repositoryDescription": "My demonstration repository",
"lastModifiedDate": "2020-11-23T20:38:23.068000+00:00",
"creationDate": "2020-11-23T20:38:23.068000+00:00",
"cloneUrlHttp": "https://git-codecommit.eu-west-1.amazonaws.com/v1/repos/
MyDemoRepo",
"cloneUrlSsh": "ssh://git-codecommit.eu-west-1.amazonaws.com/v1/repos/
MyDemoRepo",
"Arn": "arn:aws:codecommit:eu-west-1:111111111111:MyDemoRepo"
}
)
```

2. 使用命令行，为本地存储库创建新目录，并将其设为工作目录。

```
mkdir my-shell-repo
cd my-shell-repo
```

3. 要克隆远程存储库，请使用 `git clone` 命令。（在使用时 `git-remote-codecommit`，请使用 HTTPS (GRC) URL 样式）。

```
git clone codecommit::eu-west-1://MyDemoRepo
```

如果成功克隆了存储库，则命令行会显示服务的响应。

```
Cloning into 'MyDemoRepo'...
warning: You appear to have cloned an empty repository.
```

4. 要导航到克隆存储库，请使用 `cd` 命令。

```
cd MyDemoRepo
```

第 2 步：暂存并提交文件，然后再将其推送到存储 CodeCommit 库

此步骤介绍如何在将文件推送到 CodeCommit 存储库之前暂存和提交文件。

1. 使用 Vim 编辑器或的文件上传功能将名 `my-git-file` 为的文件添加到该文件 `MyDemoRepo` 夹。AWS CloudShell 要了解如何将两者结合使用，请参阅 [入门教程](#)。
2. 要将文件暂存到存储库中，请运行 `git add` 命令。

```
git add my-git-file
```

3. 要检查文件是否已暂存并准备提交，请运行 `git status` 命令。

```
git status
```

`my-git-file` 作为新文件列出并以绿色文本显示，表示它已准备好提交。

4. 将此版本的暂存文件提交到存储库。

```
git commit -m "first commit to repo"
```

Note

如果系统要求您提供配置信息以完成提交，请使用以下格式。

```
$ git config --global user.name "Jane Doe"
$ git config --global user.email janedoe@example.com
```

5. 要将远程存储库与在本地存储库中所做的更改同步，请将更改推送到上游分支。

```
git push
```

使用为 Amazon URL S3 对象创建预签名 AWS CloudShell

本教程向您展示如何创建预签名URL以与其他人共享 Amazon S3 对象。由于对象所有者在共享时会指定自己的安全证书，因此任何收到预签名证书的人都URL可以在有限的时间内访问该对象。

先决条件

- 具有AWSCloudShellFullAccess策略提供的访问权限的IAM用户。
- 有关创建预签名所需的IAM权限URL，请参阅 Amazon 简单存储服务用户指南中的[与其他人共享对象](#)。

步骤 1：创建IAM角色以授予对 Amazon S3 存储桶的访问权限

此步骤介绍如何创建IAM角色以授予对 Amazon S3 存储桶的访问权限。

1. 要获取可以共享的IAM详细信息，请从中调用`get-caller-identity`命令 AWS CloudShell。

```
aws sts get-caller-identity
```

如果调用成功，命令行将显示类似如下内容的响应：

```
{
  "Account": "123456789012",
  "UserId": "AROAXX0ZUU0TTWDCVIDZ2:redirect_session",
  "Arn": "arn:aws:sts::531421766567:assumed-role/Feder08/redirect_session"
}
```

2. 获取您在上一步中获得的用户信息，并将其添加到 AWS CloudFormation 模板中。此模板创建了一个IAM角色。该角色向您的合作者授予对共享资源的最低权限。

```
Resources:
  CollaboratorRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS: "arn:aws:iam::531421766567:role/Feder08"
            Action: "sts:AssumeRole"
      Description: Role used by my collaborators
      MaxSessionDuration: 7200
  CollaboratorPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - 's3:*'
            Resource: 'arn:aws:s3:::<YOUR_BUCKET_FOR_FILE_TRANSFER>'
```

```

        Condition:
          StringEquals:
            s3:prefix:
              - "myfolder/*"
        PolicyName: S3ReadSpecificFolder
        Roles:
          - !Ref CollaboratorRole
    Outputs:
      CollaboratorRoleArn:
        Description: Arn for the Collaborator's Role
        Value: !GetAtt CollaboratorRole.Arn

```

3. 将 AWS CloudFormation 模板保存在名为的文件中 `template.yaml`。
4. 使用模板部署堆栈并通过调用 `deploy` 命令创建 IAM 角色。

```

aws cloudformation deploy --template-file ./template.yaml --stack-name
CollaboratorRole --capabilities CAPABILITY_IAM

```

生成预签名 URL

此步骤介绍如何生成预签名 URL。

1. 在中使用您的编辑器 AWS CloudShell，添加以下代码。此代码创建了一个 URL，为联合用户提供直接访问的权限 AWS Management Console。

```

import urllib, json, sys
import requests
import boto3
import os

def main():
    sts_client = boto3.client('sts')
    assume_role_response = sts_client.assume_role(
        RoleArn=os.environ.get('ROLE_ARN'),
        RoleSessionName="collaborator-session"
    )
    credentials = assume_role_response['Credentials']
    url_credentials = {}
    url_credentials['sessionId'] = credentials.get('AccessKeyId')
    url_credentials['sessionKey'] = credentials.get('SecretAccessKey')
    url_credentials['sessionToken'] = credentials.get('SessionToken')

```

```

json_string_with_temp_credentials = json.dumps(url_credentials)
print(f"json string {json_string_with_temp_credentials}")

request_parameters = f"?
Action=getSignInToken&Session={urllib.parse.quote(json_string_with_temp_credentials)}"
request_url = "https://signin.aws.amazon.com/federation" + request_parameters
r = requests.get(request_url)
signin_token = json.loads(r.text)
request_parameters = "?Action=login"
request_parameters += "&Issuer=Example.org"
request_parameters += "&Destination=" + urllib.parse.quote("https://us-
west-2.console.aws.amazon.com/cloudshell")
request_parameters += "&SignInToken=" + signin_token["SignInToken"]
request_url = "https://signin.aws.amazon.com/federation" + request_parameters

# Send final URL to stdout
print (request_url)

if __name__ == "__main__":
    main()

```

2. 将代码保存在名为 `share.py` 的文件中。
3. 从命令行运行以下命令，从中检索IAM角色的 Amazon 资源名称 (ARN) AWS CloudFormation。然后，将其用于 Python 获取临时安全证书脚本。

```

ROLE_ARN=$(aws cloudformation describe-stacks --stack-name CollaboratorRole --query
"Stacks[*].Outputs[?OutputKey=='CollaboratorRoleArn'].OutputValue" --output text)
python3 ./share.py

```

该脚本会返回一个URL，合作者可以点击该脚本将其带 AWS CloudShell 进 AWS Management Console去。在接下来的 3600 秒（1 小时）内，合作者可以完全控制在 Amazon S3 存储桶中的 `myfolder/` 文件夹。凭证在 1 小时后到期。在此时间之后，合作者将无法再访问该存储桶。

在里面构建 Docker 容器 CloudShell并将其推送到亚马逊存储库 ECR

本教程向您展示如何定义和构建 Docker 容器 AWS CloudShell 并将其推送到 Amazon ECR 存储库。

先决条件

- 您必须拥有必要的权限才能创建和推送到 Amazon ECR 存储库。有关亚马逊存储库的更多信息 ECR，请参阅《[亚马逊ECR用户指南](#)》中的[亚马逊ECR私有存储库](#)。有关通过亚马逊推送图片所需权限的更多信息 ECR，请参阅《[亚马逊ECR用户指南](#)》中的[推送图片所需的IAM权限](#)。

教程程序

以下教程概述了如何使用该 CloudShell 接口构建 Docker 容器并将其推送到 Amazon ECR 存储库。

1. 在您的主目录中创建一个新文件夹。

```
mkdir ~/docker-cli-tutorial
```

2. 导航到您创建的文件夹。

```
cd ~/docker-cli-tutorial
```

3. 创建一个空的 Dockerfile。

```
touch Dockerfile
```

4. 例如 nano Dockerfile，使用文本编辑器打开文件并将以下内容粘贴到其中。

```
# Dockerfile

# Base this container on the latest Amazon Linux version
FROM public.ecr.aws/amazonlinux/amazonlinux:latest

# Install the cowsay binary
RUN dnf install --assumeyes cowsay

# Default entrypoint binary
ENTRYPOINT [ "cowsay" ]

# Default argument for the cowsay entrypoint
CMD [ "Hello, World!" ]
```

5. Dockerfile 现已准备好构建。通过运行来构建容器 docker build。用 easy-to-type 名称标记容器，以便在 future 命令中使用。

```
docker build --tag test-container .
```

请务必包括最后时段 (.)。

6. 现在，您可以测试容器以检查其是否正常运行 AWS CloudShell。

```
docker container run test-container
```

7. 既然你已经有了正常运行的 Docker 容器，您需要将其推送到 Amazon ECR 存储库。如果您已有 Amazon ECR 存储库，则可以跳过此步骤。

运行以下命令为本教程创建 Amazon ECR 存储库。

```
ECR_REPO_NAME=docker-tutorial-repo  
aws ecr create-repository --repository-name ${ECR_REPO_NAME}
```

8. 创建 Amazon ECR 存储库后，您可以将 Docker 容器推送到该存储库中。

运行以下命令获取 Docker 的亚马逊 ECR 登录凭证。

```
AWS_ACCOUNT_ID=$(aws sts get-caller-identity --query "Account" --output text)  
ECR_URL=${AWS_ACCOUNT_ID}.dkr.ecr.${AWS_REGION}.amazonaws.com  
aws ecr get-login-password | docker login --username AWS --password-stdin  
${ECR_URL}
```

Note

如果未在您的 AWS_REGION 环境变量中设置环境变量，CloudShell 或者您想与其他环境中的资源进行交互 AWS 区域，请运行以下命令：

```
AWS_REGION=<your-desired-region>
```

9. 使用目标 Amazon ECR 存储库标记图像，然后将其推送到该存储库。

```
docker tag test-container ${ECR_URL}/${ECR_REPO_NAME}  
docker push ${ECR_URL}/${ECR_REPO_NAME}
```

如果您在尝试完成本教程时遇到错误或遇到问题，请参阅本指南的“[疑难解答](#)”部分以获取帮助。

清理

现在，您已成功将您的 Docker 容器部署到您的亚马逊 ECR 存储库。要从您的 AWS CloudShell 环境中删除您在本教程中创建的文件，请运行以下命令。

- ```
cd ~
rm -rf ~/docker-cli-tutorial
```

- 删除 Amazon ECR 存储库。

```
aws ecr delete-repository --force --repository-name ${ECR_REPO_NAME}
```

## 使用中的部署 Lambda 函数 AWS CDK AWS CloudShell

本教程向您展示如何使用中的将 Lambda 函数部署到您的账户。AWS Cloud Development Kit (AWS CDK) CloudShell

### 先决条件

- 引导您的帐户以用于. AWS CDK有关使用引导的信息 AWS CDK，请参阅 v2 开发者指南中的[AWS CDK 引导](#)。如果你还没有引导账户，你可以跑`cdk bootstrap`进去。CloudShell
- 确保您拥有将资源部署到您的账户的相应权限。建议使用管理员权限。

## 教程程序

以下教程概述了如何使用中的部署基于 Docker 容器的 Lambda 函数。AWS CDK CloudShell

1. 在您的主目录中创建一个新文件夹。

```
mkdir ~/docker-cdk-tutorial
```

2. 导航到您创建的文件夹。

```
cd ~/docker-cdk-tutorial
```

3. 在本地安装 AWS CDK 依赖项。

```
npm install aws-cdk aws-cdk-lib
```

4. 在您创建的文件夹中创建一个基本 AWS CDK 项目。

```
touch cdk.json
mkdir lib
touch lib/docker-tutorial.js lib/Dockerfile lib/hello.js
```

5. 例如 `nano cdk.json`，使用文本编辑器打开文件并将以下内容粘贴到其中。

```
{
 "app": "node lib/docker-tutorial.js"
}
```

6. 打开 `lib/docker-tutorial.js` 文件并将以下内容粘贴到其中。

```
// this file defines the CDK constructs we want to deploy

const { App, Stack } = require('aws-cdk-lib');
const { DockerImageFunction, DockerImageCode } = require('aws-cdk-lib/aws-lambda');
const path = require('path');

// create an application
const app = new App();

// define stack
class DockerTutorialStack extends Stack {
 constructor(scope, id, props) {
 super(scope, id, props);

 // define lambda that uses a Docker container
 const dockerfileDir = path.join(__dirname);
 new DockerImageFunction(this, 'DockerTutorialFunction', {
 code: DockerImageCode.fromImageAsset(dockerfileDir),
 functionName: 'DockerTutorialFunction',
 });
 }
}
```

```
}

// instantiate stack
new DockerTutorialStack(app, 'DockerTutorialStack');
```

7. 打开lib/Dockerfile并将以下内容粘贴到其中。

```
Use a NodeJS 20.x runtime
FROM public.ecr.aws/lambda/nodejs:20

Copy the function code to the LAMBDA_TASK_ROOT directory
This environment variable is provided by the lambda base image
COPY hello.js ${LAMBDA_TASK_ROOT}

Set the CMD to the function handler
CMD ["hello.handler"]
```

8. 打开lib/hello.js文件并将以下内容粘贴到其中。

```
// define the handler
exports.handler = async (event) => {
 // simply return a friendly success response
 const response = {
 statusCode: 200,
 body: JSON.stringify('Hello, World!'),
 };
 return response;
};
```

9. 使用 AWS CDK CLI来合成项目并部署资源。您必须启动您的帐户。

```
npx cdk synth
npx cdk deploy --require-approval never
```

10. 调用 Lambda 函数进行确认和验证。

```
aws lambda invoke --function-name DockerTutorialFunction out.json
jq . out.json
```

现在，您已经使用成功部署了基于 Docker 容器的 Lambda 函数。AWS CDK有关的更多信息 AWS CDK，请参阅 [AWS CDK v2 开发者指南](#)。如果您在尝试完成本教程时遇到错误或遇到问题，请参阅本指南的“[疑难解答](#)”部分寻求帮助。

## 清理

现在，您已经使用成功部署了基于 Docker 容器的 Lambda 函数。AWS CDK在 AWS CDK 项目内部，运行以下命令以删除关联的资源。系统将提示您确认删除。

- ```
npx cdk destroy DockerTutorialStack
```
- 要将您在本教程中创建的文件和资源从您的 AWS CloudShell 环境中删除，请运行以下命令。

```
cd ~  
rm -rf ~/docker-cli-tutorial
```

与 AWS CloudShell

本节介绍如何与支持的应用程序交互 AWS CloudShell 并执行特定操作。

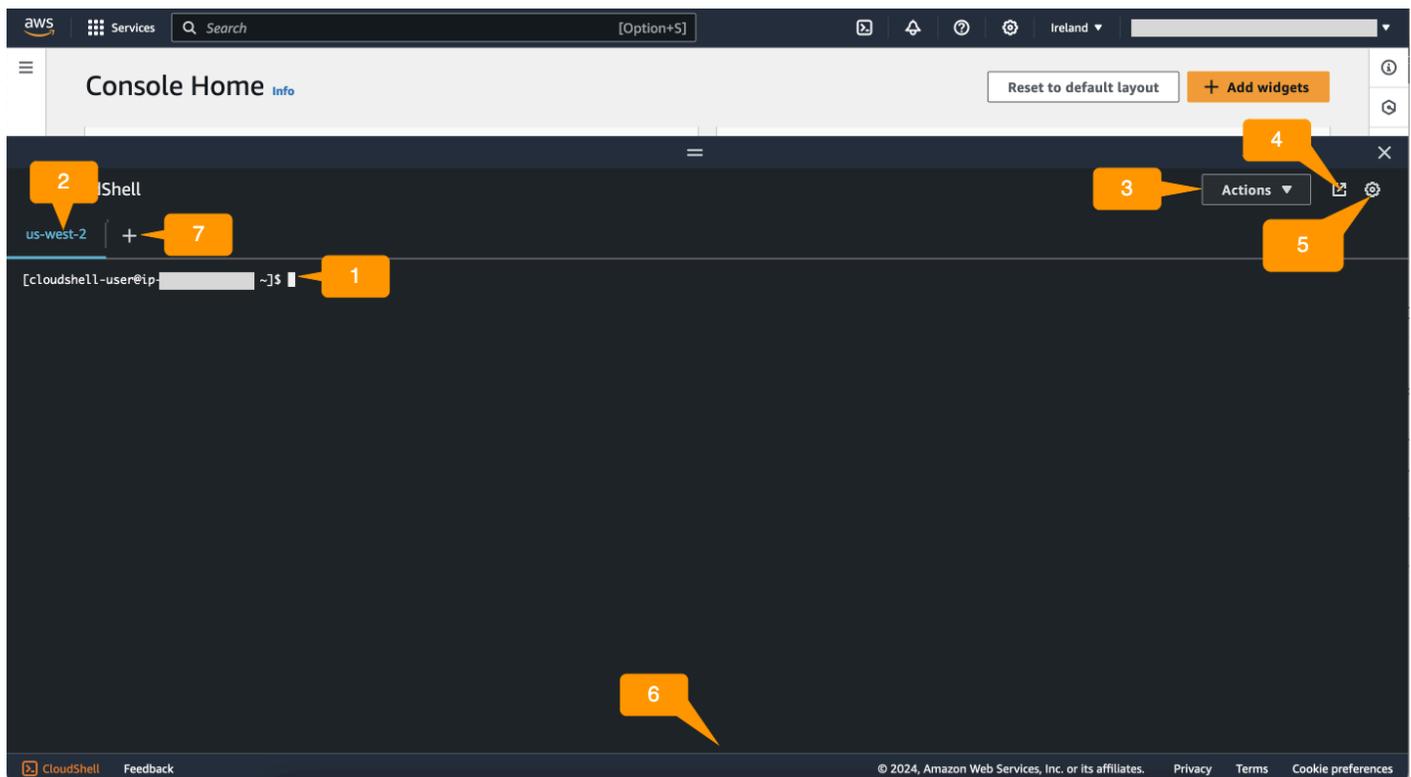
主题

- [浏览界面 AWS CloudShell](#)
- [在 AWS 区域](#)
- [处理文件和存储](#)
- [使用 Docker](#)

浏览界面 AWS CloudShell

您可以从 AWS Management Console 和中浏览 CloudShell 界面功能 Console Toolbar。

以下屏幕截图显示了几个关键的 AWS CloudShell 界面功能。



1. AWS CloudShell 命令行界面，用于使用[首选 shell](#) 运行命令。当前 Shell 类型由命令提示符指示。
2. 终端选项卡，它使用当前 AWS CloudShell 的运行 AWS 区域 位置。

- 操作菜单，提供[更改屏幕布局](#)、[下载和上传文件](#)、[重启 AWS CloudShell](#)和[删除 AWS CloudShell 主目录](#)的选项。

 Note

当你在 CloudShell 上启动时，“下载”选项不可用 Console Toolbar.

- 在新浏览器中打开选项卡，提供全屏访问 CloudShell 会话的选项。
- 首选项选项，可用于[自定义 Shell 体验](#)。
- 底部栏提供以下选项：
 - CloudShell 从 CloudShell 图标启动。
 - 通过反馈图标提供反馈。选择您要提交的反馈类型，添加您的评论，然后选择提交。
 - 要提交反馈 CloudShell，请选择以下选项之一：
 - 从控制台启动 CloudShell 并选择“反馈”。添加您的评论，然后选择提交。
 - 在“CloudShell 上选择” Console Toolbar，在控制台的左下角，然后选择“在新浏览器选项卡中打开”图标“反馈”。添加您的评论，然后选择提交。

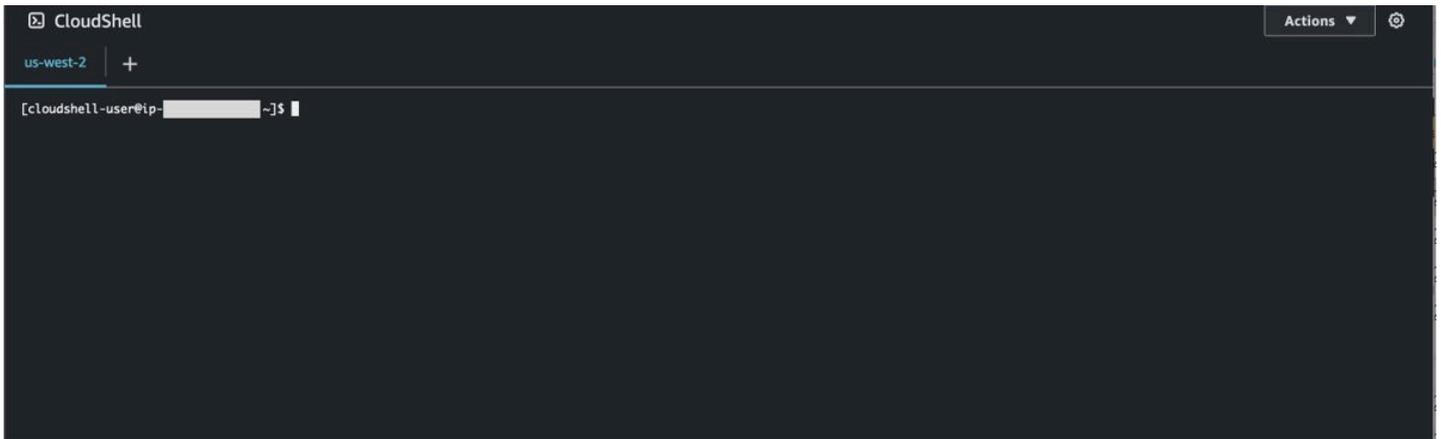
 Note

当你在 CloudShell 上启动时，“反馈”选项不可用 Console Toolbar.

- 了解我们的隐私政策和使用条款，并自定义 Cookie 首选项。
- + 图标是一个下拉菜单，包括创建、重启和删除环境的选项。

在 AWS 区域

您 AWS 区域正在运行的当前显示为选项卡。



您可以通过使用区域选择器选择特定区域来选择 AWS 区域 要处理的区域。更改区域后，当您的 Shell 会话连接到在选定区域中运行的不同计算环境时，界面会刷新。

Important

- 每个存储空间最多可使用 1 GB 的永久存储空间 AWS 区域。持久性存储保存在您的主目录 (\$HOME) 中。这意味着存储在您的主目录中的任何个人文件、目录、程序或脚本都位于同一个 AWS 区域中。此外，它们与位于主目录中但存储在不同区域中的那些文件不同。

文件在持久性存储中的长期保留也是按区域管理的。有关更多信息，请参阅 [持久性存储](#)。

- 永久存储不适用于 AWS CloudShell VPC 环境。

指定您的默认 AWS 区域 值 AWS CLI

您可以使用 [环境变量](#) 来指定访问 AWS 服务 所需的配置选项和凭据 AWS CLI。当您从中的特定区域启动时，或者在区域选择器 AWS CloudShell 中选择一个选项时，将在中设置 AWS 区域 用于指定 shell 会话默认值的环境变量。AWS Management Console

[环境变量优先于由更新的 AWS CLI 凭据文件](#) `aws configure`。因此，您无法运行 `aws configure` 命令来更改由环境变量指定的区域。相反，要更改 AWS CLI 命令的默认区域，请为 `AWS_REGION` 环境变量赋值。在以下示例中，将 `us-east-1` 替换为您所在的区域。

Bash or Zsh

```
$ export AWS_REGION=us-east-1
```

设置环境变量会更改使用的值，直到 Shell 会话结束或当您将该变量设置为其他值时。通过在 Shell 的启动脚本中设置变量，可使变量在未来的会话中继续有效。

PowerShell

```
PS C:\> $Env:AWS_REGION="us-east-1"
```

如果在 PowerShell 提示符处设置环境变量，则环境变量仅在当前会话的持续时间内保存该值。或者，您可以通过将变量添加到您的 PowerShell 个人资料中来为所有未来 PowerShell 会话设置该变量。有关存储环境变量的更多信息，请参阅[PowerShell 文档](#)。

要确认您已更改默认区域，请运行 `aws configure list` 命令以显示当前的 AWS CLI 配置数据。

Note

对于特定 AWS CLI 命令，您可以使用命令行选项覆盖默认区域 `--region`。有关更多信息，请参阅 AWS Command Line Interface 用户指南中的 [Command line options](#)。

处理文件和存储

使用 AWS CloudShell 的界面，您可以将文件上传到 shell 环境，也可以从 shell 环境中下载文件。有关下载和上传文件的更多信息，请参阅[入门 AWS CloudShell](#)。

为了确保您添加的任何文件在会话结束后仍然可用，您应该知道持久性存储和临时存储之间的区别。

- 永久存储：每种存储空间都有 1 GB AWS 区域。持久性存储在您的主目录中。
- 临时存储：临时存储空间在会话结束时被回收。临时存储位于主目录之外的目录中。

Important

确保将要保留并用于将来的 Shell 会话的文件保存在您的主目录中。例如，假设您通过运行 `mv` 命令将某个文件移出主目录。然后，当前 Shell 会话结束时，该文件将被回收。

使用 Docker

AWS CloudShell 无需安装或配置即可完全支持 Docker。您可以在里面 AWS CloudShell 定义、构建和运行 Docker 容器。您可以通过 AWS CDK 工具包部署基于 Docker 的资源，例如基于 Docker 容器的 Lambda 函数，也可以构建 Docker 容器并将其通过 Docker 推送到亚马逊存储库。ECR CLI 有关如何运行这两个部署的详细步骤，请参阅以下教程：

- [教程：使用部署 Lambda 函数 AWS CDK](#)
- [教程：在里面构建 Docker 容器 AWS CloudShell 并将其推送到亚马逊存储库 ECR](#)

通过以下方式使用 Docker 有 AWS CloudShell 某些限制和限制：

- Docker 在环境中的空间有限。如果您的单个映像较大，或者预先存在的 Docker 映像过多，则可能会导致无法拉取、构建或运行其他映像的问题。有关 Docker 的更多信息，请参阅 [Docker 文档指南](#)。
- 除了 AWS GovCloud（美国）AWS 地区外，Docker 在所有地区都可用。有关可用 Docker 的区域列表，请参阅 [支持的 AWS 区域。AWS CloudShell](#)
- 如果您在使用 Docker 时遇到问题 AWS CloudShell，请参阅本指南的“[疑难解答](#)”部分，了解如何解决这些问题。

的无障碍功能 AWS CloudShell

本主题介绍如何使用无障碍功能 CloudShell。您可以使用键盘浏览页面上的可聚焦元素。您还可以自定义的外观 CloudShell，包括字体大小和界面主题。

键盘导航 CloudShell

要浏览页面上的可聚焦元素，请按 Tab。

CloudShell 终端无障碍功能

您可以通过以下方式使用 Tab 键：

- 终端模式（默认）——在此模式下，终端会捕获您的 Tab 密钥输入。将焦点放在终端上后，按下 Tab 即可仅访问终端的功能。
- 导航模式——在此模式下，终端不会捕获您的 Tab 密钥输入。按下 Tab 可浏览页面上的可聚焦元素。

要在终端模式和导航模式之间切换，请按 Ctrl+M。切换回去后，标题中会出现 Tab：导航，您可以使用 Tab 键在页面中导航。

要返回终端模式，请按 Ctrl+M。或者，选择 Tab：导航旁边的 X。

Note

目前，CloudShell 终端无障碍功能在移动设备上不可用。

在中选择字体大小和界面主题 CloudShell

您可以自定义的外观 CloudShell 以适应您的视觉偏好。

- 字体大小——在终端中从最小、小、中、大和最大字体大小中进行选择。有关更改字体大小的更多信息，请参阅 [the section called “更改字体大小”](#)。
- 主题——在浅色和深色界面主题之间进行选择。有关更改界面主题的更多信息，请参阅 [the section called “更改界面主题”](#)。

使用中的 AWS 服务 AWS CloudShell

的一个主要好处 AWS CloudShell 是，您可以使用它从命令行界面管理您的 AWS 服务。这意味着您不需要事先下载和安装工具或在本地配置您的凭证。启动时 AWS CloudShell，将创建一个已安装以下 AWS 命令行工具的计算环境：

- [AWS CLI](#)
- [AWS Elastic Beanstalk CLI](#)
- [Amazon ECS CLI](#)
- [AWS SAM](#)

而且，由于您已经登录 AWS，因此无需在使用服务之前在本地配置证书。您用于登录 AWS Management Console 的凭证会被转发到 AWS CloudShell。

如果要更改使用的默认 AWS 区域 AWS CLI，则可以更改分配给 AWS_REGION 环境变量的值。（有关更多信息，请参阅 [指定您的默认 AWS 区域值 AWS CLI](#)。）

本主题的其余部分演示如何开始使用 AWS CloudShell 命令行与所选 AWS 服务进行交互。

AWS CLI 所选 AWS 服务的命令行示例

以下示例仅代表您可以使用 AWS CLI 版本 2 中提供的命令使用的众多 AWS 服务中的一部分。有关完整列表，请参阅 [AWS CLI 命令参考](#)。

- [DynamoDB](#)
- [AWS Cloud9](#)
- [Amazon EC2](#)
- [S3 Glacier](#)

DynamoDB

DynamoDB 是一项完全托管的 SQL 无数据库服务，可提供快速且可预测的性能以及无缝的可扩展性。此服务的“否”SQL 模式实现支持键值和文档数据结构。

以下 create-table 命令创建在您的 AWS 账户 MusicCollection 中命名的 No SQL 样式表。

```
aws dynamodb create-table \
```

```
--table-name MusicCollection \  
--attribute-definitions AttributeName=Artist,AttributeType=S  
AttributeName=SongTitle,AttributeType=S \  
--key-schema AttributeName=Artist,KeyType=HASH  
AttributeName=SongTitle,KeyType=RANGE \  
--provisioned-throughput ReadCapacityUnits=5,WriteCapacityUnits=5 \  
--tags Key=Owner,Value=blueTeam
```

有关更多信息，请参阅 AWS Command Line Interface 用户指南中的[通过 AWS CLI使用 DynamoDB](#)。

AWS Cloud9

AWS Cloud9 是一个基于云的集成开发环境 (IDE)，可用于在浏览器窗口中编写、运行和调试代码。该环境包含代码编辑器、调试器和终端。

以下 `create-environment-ec2` 命令使用指定设置创建 AWS Cloud9 EC2 开发环境。它启动一个 Amazon EC2 实例，然后从该实例连接到环境。

```
aws cloud9 create-environment-ec2 --name my-demo-env --description "My demonstration  
development environment." --instance-type t2.micro --subnet-id subnet-1fab8aEX --  
automatic-stop-time-minutes 60 --owner-arn arn:aws:iam::123456789012:user/MyDemoUser
```

有关更多信息，请参阅 [AWS Cloud9 命令行参考](#)。

Amazon EC2

Amazon Elastic Compute Cloud (AmazonEC2) 是一项网络服务，可在云中提供安全且可调整大小的计算容量。该服务旨在降低网络规模级云计算的难度，并且更易访问。

以下 `run-instances` 命令在的指定子网中启动 t2.micro 实例：VPC

```
aws ec2 run-instances --image-id ami-xxxxxxxx --count 1 --instance-type t2.micro --key-  
name MyKeyPair --security-group-ids sg-903004f8 --subnet-id subnet-6e7f829e
```

有关更多信息，请参阅《AWS Command Line Interface 用户指南》AWS CLI 中的[“EC2使用 Amazon”](#)。

S3 Glacier

S3 Glacier 和 S3 Glacier Deep Archive 是一种安全、持久且成本极低的 Amazon S3 云存储类别，用于数据存档和长期备份。

以下 `create-vault` 命令创建一个文件库，即用于存储档案的容器：

```
aws glacier create-vault --vault-name my-vault --account-id -
```

更多信息，请参阅 AWS Command Line Interface 用户指南中的[通过 AWS CLI 使用 Amazon S3 Glacier](#)。

AWS Elastic Beanstalk CLI

AWS Elastic Beanstalk CLI 提供了一个命令行界面，用于简化从本地存储库创建、更新和监控环境的过程。在这种情况下，环境是指运行应用程序版本的 AWS 资源集合。

以下 `create` 命令在自定义 Amazon Virtual Private Cloud (VPC) 中创建新环境。

```
$ eb create dev-vpc --vpc.id vpc-0ce8dd99 --vpc.elbsubnets subnet-  
b356d7c6,subnet-02f74b0c --vpc.ec2subnets subnet-0bb7f0cd,subnet-3b6697c1 --  
vpc.securitygroup sg-70cff265
```

有关更多信息，请参阅《AWS Elastic Beanstalk 开发人员指南》中的[EB CLI 命令参考](#)。

Amazon ECS CLI

亚马逊弹性容器服务 (Amazon ECS) 命令行界面 (CLI) 提供了几个高级命令。这些命令旨在简化从本地开发环境创建、更新和监视集群和任务的过程。（Amazon ECS 集群是任务或服务的逻辑分组。）

以下 `configure` 命令将 Amazon 配置 ECS CLI 为创建名为 `ecs-cli-demo` 的集群配置。此集群配置使用 FARGATE 作为 `us-east-1` region 中 `ecs-cli-demo` 集群的默认启动类型。

```
ecs-cli configure --region us-east-1 --cluster ecs-cli-demo --default-launch-type  
FARGATE --config-name ecs-cli-demo
```

有关更多信息，请参阅《[亚马逊弹性容器服务开发者指南](#)》中的[亚马逊 ECS 命令行参考](#)。

AWS SAM CLI

AWS SAM CLI 是一种对 AWS Serverless Application Model 模板和应用程序代码进行操作的命令行工具。您可以使用它执行多项任务。其中包括在本地调用 Lambda 函数、为无服务器应用程序创建部署包以及将您的无服务器应用程序部署到云端。AWS

以下init命令使用作为参数传递的必需参数来初始化一个新SAM项目：

```
sam init --runtime python3.7 --dependency-manager pip --app-template hello-world --name  
sam-app
```

有关更多信息，请参阅《AWS Serverless Application Model 开发人员指南》中的[AWS SAM CLI命令参考](#)。

定制您的体验 AWS CloudShell

您可以自定义 AWS CloudShell 体验的以下方面：

- [标签页布局](#)：将命令行界面拆分为多列和多行。
- [字体大小](#)：调整命令行文本的大小。
- [颜色主题](#)：在浅色和深色主题之间切换。
- [安全粘贴](#)：开启或关闭一项要求您在粘贴多行文本之前对其进行验证的功能。
- [Tmux 到会话恢复](#)：使用 tmux 可以恢复会话，直到会话变为非活动状态。

您还可以通过[安装自己的软件](#)并使用[脚本修改外壳来扩展外壳](#)环境。

将命令行显示拆分成多个标签页

通过将命令行界面拆分为多个窗格来运行多个命令。

Note

打开多个标签页后，您可以通过单击所选窗格中的任意位置来选择一个要处理的标签页。您可以通过选择区域名称旁边的 x 符号来关闭标签页。

- 从标签页布局中选择操作和以下选项之一：
 - 新建标签页：在当前活动标签页旁边添加一个新标签页。
 - 拆分成行：在当前活动标签页下方的行中添加一个新标签页。
 - 拆分为列：在当前活动标签页旁边的列中添加一个新标签页。

如果空间不足，无法完全显示每个标签页，请滚动查看整个标签页。您也可以选择分隔窗格的分隔条，然后使用指针拖动分隔条来增加或减小窗格大小。

更改字体大小

增大或减小命令行界面中显示的文本的大小。

1. 要更改 AWS CloudShell 终端设置，请前往“设置”、“首选项”。
2. 选择文本大小。选项有最小、小、中、大和最大。

更改界面主题

在命令行界面的浅色和深色主题之间切换。

1. 要更改 AWS CloudShell 主题，请前往“设置”、“偏好设置”。
2. 选择浅色或深色。

对多行文本使用安全粘贴

“安全粘贴”是一项安全功能，可提示您验证要粘贴到 Shell 中的多行文本是否包含恶意脚本。从第三方网站复制的文本可能包含隐藏代码，这些代码会在您的 Shell 环境中触发意外行为。

“安全粘贴”对话框显示您复制到剪贴板的完整文本。如果您对不存在安全风险感到满意，请选择粘贴。

Warning: Pasting multiline text into AWS CloudShell



Text that's copied from external sources can contain malicious scripts. Verify the text below before pasting.

```
import sys
x=int(sys.argv[1])
y=int(sys.argv[2])
z=int(sys.argv[3])
total=x+y+z
print("The total is",total)
```

Always ask before pasting multiline code

Cancel

Paste

我们建议您启用“安全粘贴”以捕获脚本中的潜在安全风险。您可以通过选择首选项、启用安全粘贴和禁用安全粘贴来打开或关闭此功能。

使用 tmux 到会话恢复

AWS CloudShell 使用 tmux 在单个或多个浏览器选项卡上恢复会话。如果您刷新浏览器标签页，它会恢复您的会话，直到会话变为非活动状态。有关更多信息，请参阅[会话恢复](#)。

AWS CloudShell 在 Amazon 中使用 VPC

AWS CloudShell 虚拟私有云 (VPC) 使您能够在自己的 CloudShell 环境中创建环境 VPC。对于每个 VPC 环境，您可以分配一个 VPC、添加子网以及关联最多五个安全组。AWS CloudShell 继承的网络配置，使您能够在 VPC 中的其他资源相同的子网中 AWS CloudShell 安全使用 VPC 并连接到这些资源。

借助 Amazon VPC，您可以在您定义的逻辑隔离的虚拟网络中启动 AWS 资源。这个虚拟网络与您在数据中心中运行的传统网络极其相似，并会为您提供使用 AWS 的可扩展基础设施的优势。有关更多信息 VPC，请参阅[亚马逊 Virtual Private Cloud](#)。

操作限制

AWS CloudShell VPC 环境有以下限制：

- 每个 IAM 主体最多可以创建两个 VPC 环境。
- 您最多可以为一个 VPC 环境分配五个安全组。
- 您不能使用 VPC 环境的“操作”菜单中的 CloudShell 上传和下载选项。

Note

可以从可通过其他工具访问互联网入口/出口的 VPC 环境中上传或下载文件。CLI

- VPC 环境不支持永久存储。存储是短暂的。活动环境会话结束后，数据和主目录将被删除。
- 只有在私有子网中，您的 AWS CloudShell 环境才能连接到互联网 VPC 网。

Note

默认情况下，不会将公有 IP 地址分配给 CloudShell VPC 环境。VPC 在公共子网中创建的环境如果路由表配置为将所有流量路由到 Internet Gateway，则无法访问公共 Internet，但配置了网络地址转换 (NAT) 的私有子网可以访问公共互联网。VPC 在此类私有子网中创建的环境将可以访问公共 Internet。

- 要为您的账户提供托管 CloudShell 环境，AWS 可以为底层计算主机配置对以下服务的网络访问权限：
 - Amazon S3

- VPC端点
 - com.amazonaws。 <region>.ssmmessages
 - com.amazonaws。 <region>.logs
 - com.amazonaws。 <region>.kms
 - com.amazonaws。 <region>.execute-api
 - com.amazonaws。 <region>.ecs-telemetry
 - com.amazonaws。 <region>.ecs-agent
 - com.amazonaws。 <region>.ecs
 - com.amazonaws。 <region>.ecr.dkr
 - com.amazonaws。 <region>.ecr.api
 - com.amazonaws。 <region>.codetalytst.packages
 - com.amazonaws。 <region>.codecatalyst.git
 - aws.api.global.codecat

您不能通过修改VPC配置来限制对这些端点的访问。

CloudShellVPC在除了 AWS GovCloud (美国) AWS 地区之外的所有地区都可用。有关可用区域的 CloudShell VPC列表，请参阅[支持的 AWS 区域 AWS CloudShell](#)。

创建 CloudShell VPC环境

本主题将引导您完成在中创建VPC环境的步骤 CloudShell。

先决条件

您的管理员必须提供必要的IAM权限才能创建VPC环境。有关启用 CloudShell VPC环境创建权限的更多信息，请参阅[the section called “创建和使用 CloudShell VPC环境所需的IAM权限”](#)。

创建 CloudShell VPC环境

1. 在 CloudShell 控制台页面上，选择 + 图标，然后从下拉菜单中选择创建VPC环境。
2. 在创建VPC环境页面上，在名称框中输入VPC环境的名称。
3. 从虚拟私有云 (VPC) 下拉列表中，选择一个VPC。
4. 从“子网”下拉列表中，选择一个子网。
5. 从安全组下拉列表中，选择要分配给VPC环境的一个或多个安全组。

Note

您最多可以选择五个安全组。

6. 选择“创建”来创建您的VPC环境。
7. （可选）选择“操作”，然后选择“查看详细信息”以查看新创建的VPC环境的详细信息。您的VPC环境的IP地址显示在命令行提示符中。

有关使用VPC环境的信息，请参阅[开始使用](#)。

创建和使用 CloudShell VPC环境所需的IAM权限

要创建和使用 CloudShell VPC环境，IAM管理员必须允许访问VPC特定 Amazon EC2 权限。本节列出了创建和使用VPC环境所需的 Amazon EC2 权限。

要创建VPC环境，分配给您的角色的IAM策略必须包含以下 Amazon EC2 权限：

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeNetworkInterfaces`

- `ec2:CreateTags`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`

我们建议包括：

- `ec2>DeleteNetworkInterface`

Note

此权限不是强制性的，但这是清理由 CloudShell 其创建的ENI资源（为 CloudShell VPC环境 ENIs创建的带有ManagedByCloudShell密钥标记）所必需的。如果未启用此权限，则必须在每次使用 CloudShell VPC环境后手动清理ENI资源。

IAM策略授予完全 CloudShell 访问权限，包括访问权限 VPC

以下示例显示了如何启用对以下内容的完全权限，包括对以下内容的VPC访问权限 CloudShell：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudShellOperations",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowDescribeVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowCreateTagWithCloudShellKey",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
```

```

    "StringEquals": {
      "ec2:CreateAction": "CreateNetworkInterface"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": "ManagedByCloudShell"
    }
  }
},
{
  "Sid": "AllowCreateNetworkInterfaceWithSubnetsAndSG",
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterface"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Sid": "AllowCreateNetworkInterfaceWithCloudShellTag",
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterface"
  ],
  "Resource": "arn:aws:ec2:*:*:network-interface/*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": "ManagedByCloudShell"
    }
  }
},
{
  "Sid": "AllowCreateNetworkInterfacePermissionWithCloudShellTag",
  "Effect": "Allow",
  "Action": [
    "ec2:CreateNetworkInterfacePermission"
  ],
  "Resource": "arn:aws:ec2:*:*:network-interface/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/ManagedByCloudShell": ""
    }
  }
}

```

```
    },
    {
      "Sid": "AllowDeleteNetworkInterfaceWithCloudShellTag",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ManagedByCloudShell": ""
        }
      }
    }
  ]
}
```

为VPC环境使用IAM条件键

您可以使用 CloudShell 特定条件键进行 VPC 设置，为您的 VPC 环境提供额外的权限控制。您还可以指定 VPC 环境可以使用和不能使用的子网和安全组。

CloudShell 在 IAM 策略中支持以下条件键：

- CloudShell:VpcIds— 允许或拒绝一个或多个 VPCs
- CloudShell:SubnetIds— 允许或拒绝一个或多个子网
- CloudShell:SecurityGroupIds— 允许或拒绝一个或多个安全组

Note

如果修改了有权访问公共 CloudShell 环境的用户的权限以增加对 `cloudshell:createEnvironment` 操作的限制，他们仍然可以访问其现有的公共环境。但是，如果您想修改具有此限制的 IAM 策略并禁用他们对现有公共环境的访问权限，则必须先使用该限制更新 IAM 策略，然后确保您账户中的每个 CloudShell 用户都使用 CloudShell Web 用户界面（操作 → 删除环境）手动删除现有的公共 CloudShell 环境。

带有VPC设置条件键的策略示例

以下示例演示如何使用条件键进行VPC设置。创建具有所需限制的策略语句后，为目标用户或角色附加策略语句。

确保用户仅创建VPC环境并拒绝创建公共环境

为确保用户只能创建VPC环境，请使用拒绝权限，如以下示例所示：

```
{
  "Statement": [
    {
      "Sid": "DenyCloudShellNonVpcEnvironments",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudshell:VpcIds": "true"
        }
      }
    }
  ]
}
```

拒绝用户访问特定VPCs、子网或安全组

要拒绝用户访问特定的VPCs内容，StringEquals请使用检查cloudshell:VpcIds条件的值。以下示例拒绝用户访问vpc-1和vpc-2：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",

```

```

    "Condition": {
      "StringEquals": {
        "cloudshell:VpcIds": [
          "vpc-1",
          "vpc-2"
        ]
      }
    }
  ]
}

```

要拒绝用户访问特定的VPCs内容，StringEquals请使用检查cloudshell:SubnetIds条件的值。以下示例拒绝用户访问subnet-1和subnet-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}

```

要拒绝用户访问特定的VPCs内容，StringEquals请使用检查cloudshell:SecurityGroupIds条件的值。以下示例拒绝用户访问sg-1和sg-2：

```

{
  "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Sid": "EnforceOutOfSecurityGroups",
    "Action": [
      "cloudshell:CreateEnvironment"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "cloudshell:SecurityGroupIds": [
          "sg-1",
          "sg-2"
        ]
      }
    }
  }
]
}

```

允许用户创建具有特定VPC配置的环境

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:VpcIds条件的值。以下示例允许用户访问vpc-1和vpc-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}

```

```

    }
  ]
}

```

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:SubnetIds条件的值。以下示例允许用户访问subnet-1和subnet-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SubnetIds": [
            "subnet-1",
            "subnet-2"
          ]
        }
      }
    }
  ]
}

```

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:SecurityGroupIds条件的值。以下示例允许用户访问sg-1和sg-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSecurityGroup",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",

```

```
    "Condition": {
      "ForAllValues:StringEquals": {
        "cloudshell:SecurityGroupIds": [
          "sg-1",
          "sg-2"
        ]
      }
    }
  ]
}
```

的安全性 AWS CloudShell

云安全性一直是 Amazon Web Services (AWS) 的重中之重。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 负责保护运行 AWS 云中提供的所有服务的基础架构，并为您提供可以安全使用的服务。我们的安全责任是重中之重 AWS，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。

云端安全 — 您的责任由您使用的 AWS 服务以及其他因素决定，包括数据的敏感性、组织的要求以及适用的法律和法规。

AWS CloudShell 通过其支持的特定 AWS 服务遵循[分担责任模式](#)。有关 AWS 服务安全信息，请参阅[AWS 服务安全文档页面](#)和[合规计划合 AWS 规工作范围内的AWS 服务](#)。

以下主题向您介绍如何进行配置 AWS CloudShell 以满足您的安全和合规性目标。

主题

- [中的数据保护 AWS CloudShell](#)
- [适用于 Identity and Access Managem AWS CloudShell](#)
- [登录和监控 AWS CloudShell](#)
- [合规性验证 AWS CloudShell](#)
- [韧性在 AWS CloudShell](#)
- [中的基础设施安全 AWS CloudShell](#)
- [以下方面的安全最佳实践 AWS CloudShell](#)
- [AWS CloudShell 安全 FAQs](#)

中的数据保护 AWS CloudShell

分 AWS [担责任模型](#)适用于中的数据保护 AWS CloudShell。如本模型所述 AWS，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私FAQ](#)。有关欧洲数据保护的信息，请参阅[责任AWS 共担模型和AWS安全GDPR](#)博客上的博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭据并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用SSL/TLS与 AWS 资源通信。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用跟 CloudTrail 踪](#)。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或访问时需要 FIPS 140-3 经过验证的加密模块API，请使用端点。FIPS有关可用FIPS端点的更多信息，请参阅[联邦信息处理标准 \(FIPS\) 140-3](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用 AWS CloudShell 或以其他 AWS 服务方式使用控制台时API、AWS CLI、或 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

数据加密

数据加密是指在数据处于静止状态时，AWS CloudShell 以及数据在与服务端点 AWS CloudShell 之间传输时保护数据。

使用静态加密 AWS KMS

静态加密是指通过对存储数据进行加密来保护您的数据免受未经授权的访问。使用时 AWS CloudShell，您可以免费获得每个 AWS 区域 1 GB 的永久存储空间。持久性存储位于您的主目录 (\$HOME) 中，对您而言是私有的。与每个 Shell 会话结束后回收的临时环境资源不同的是，主目录中的数据会保留。

存储在中的数据加密 AWS CloudShell 是使用 AWS Key Management Service (AWS KMS) 提供的加密密钥实现的。这是一项托管 AWS 服务，用于创建和控制客户主密钥 (CMKs)，即用于加密存储在 AWS CloudShell 环境中的客户数据的加密密钥。AWS CloudShell 代表客户生成和管理用于加密数据的加密密钥。

传输中加密

传输中加密是指在通信终端节点之间移动数据时，保护您的数据免遭拦截。

默认情况下，客户端的 Web 浏览器计算机与基于云 AWS CloudShell 的计算机之间的所有数据通信都通过 HTTPS/TLS 连接发送所有数据进行加密。

您无需执行任何操作即可使用 HTTPS/TLS 进行通信。

适用于 Identity and Access Management AWS CloudShell

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 CloudShell 资源。IAM 无需支付额外费用即可使用。AWS 服务

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [AWS CloudShell 如何使用 IAM](#)
- [基于身份的策略示例 AWS CloudShell](#)
- [对 AWS CloudShell 身份和访问进行故障排除](#)
- [使用 IAM 策略管理 AWS CloudShell 访问和使用情况](#)

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你所做的工作 CloudShell。

服务用户-如果您使用该 CloudShell 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多 CloudShell 功能来完成工作时，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问中的功能 CloudShell，请参阅[对 AWS CloudShell 身份和访问进行故障排除](#)。

服务管理员-如果您负责公司的 CloudShell 资源，则可能拥有完全访问权限 CloudShell。您的工作是确定您的服务用户应访问哪些 CloudShell 功能和资源。然后，您必须向 IAM 管理员提交更改服务用

户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM与配合使用CloudShell，请参阅[AWS CloudShell 如何使用 IAM](#)。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写用于管理访问权限的策略 CloudShell。要查看可在中使用的 CloudShell 基于身份的策略示例IAM，请参阅。[基于身份的策略示例 AWS CloudShell](#)

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 AWS 账户根用户、IAM用户身份或通过担任IAM角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。AWS IAM Identity Center（IAM身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用IAM角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的[如何登录到您 AWS 账户的](#)。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅[《IAM用户指南》中的对 AWS API请求进行签名](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的[多重身份验证](#)和AWS IAM Identity Center 用户指南 AWS中的[使用多因素身份验证 \(MFA\)](#)。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的[“需要根用户凭证的IAM任务”](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity Center 目录中的用户，或者任何使用 AWS 服务通过身份源提供的凭据进行访问的用户。AWS Directory Service 当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM 身份中心的信息，请参阅[什么是 IAM 身份中心？](#) 在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

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

[IAM 群组](#)是指定 IAM 用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins 并授予该群组管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《[IAM 用户指南](#)》中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

[IAM 角色](#)是您内部具有特定权限 AWS 账户的身份。它与 IAM 用户类似，但与特定人员无关。您可以通过[切换 IAM 角色 AWS Management Console 来临时担任中的角色](#)。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义操作来代入角色 URL。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的[使用 IAM 角色](#)。

IAM 具有临时证书的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集关联到中的 IAM 角色。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。
- 临时 IAM 用户权限-IAM 用户或角色可以代入一个 IAM 角色，为特定任务临时获得不同的权限。

- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
 - 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。
 - 服务角色-服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。
 - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 AWS CLI 或 AWS API请求的应用程序的临时证书。这比在EC2实例中存储访问密钥更可取。要为EC2实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在EC2实例上运行的程序获得临时证书。有关更多信息，请参阅IAM用户指南中的[使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

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

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以JSON文档的 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅 [《IAM用户指南》中的JSON策略概述](#)。

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

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

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

基于资源的策略

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

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 AWS 托管策略。

访问控制列表 (ACLs)

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

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的[访问控制列表 \(ACL\) 概述](#)。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体（IAM用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限

边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的[IAM实体的权限边界](#)。

- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。对成员账户中的实体（包括每个实体）的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的[策略评估逻辑](#)。

AWS CloudShell 如何使用 IAM

在使用管理IAM访问权限之前 CloudShell，请先了解哪些IAM功能可供使用 CloudShell。

IAM你可以使用的功能 AWS CloudShell

IAM特征	CloudShell 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否

IAM特征	CloudShell 支持
ABAC (策略中的标签)	否
临时凭证	是
转发访问会话 (FAS)	否
服务角色	否
服务相关角色	否

要全面了解大多数IAM功能 CloudShell 以及其他 AWS 服务是如何使用的，请参阅《IAM用户指南》IAM中[与之配合使用的AWS 服务](#)。

基于身份的策略 CloudShell

支持基于身份的策略：是

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

使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

基于身份的策略示例 CloudShell

要查看 CloudShell 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS CloudShell](#)

内部基于资源的政策 CloudShell

支持基于资源的策略：否

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

要启用跨账户访问权限，您可以将整个账户或另一个账户中的IAM实体指定为基于资源的策略中的委托人。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的IAM管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM用户指南》IAM中的[跨账户资源访问权限](#)。

的政策行动 CloudShell

支持策略操作：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 CloudShell 操作列表，请参阅《服务授权参考》AWS CloudShell中[定义的操作](#)。有些操作可能不止一个API。

正在执行的策略操作在操作前 CloudShell 使用以下前缀：

```
cloudshell
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 CloudShell 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS CloudShell](#)

的政策资源 CloudShell

支持策略资源：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 [Amazon 资源名称 \(ARN\)](#) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

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

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

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

要查看 CloudShell 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS CloudShell](#)

的策略条件密钥 CloudShell

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。有关更多信息，请参阅《IAM用户指南》中的[IAM策略元素：变量和标签](#)。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的[AWS 全局条件上下文密钥](#)。

要查看 CloudShell 条件密钥列表，请参阅《服务授权参考》AWS CloudShell中的[条件密钥](#)。要了解可以使用条件键的操作和资源，请参阅[由定义的操作AWS CloudShell](#)。

要查看 CloudShell 基于身份的策略的示例，请参阅 [基于身份的策略示例 AWS CloudShell](#)

ACLs在 CloudShell

支持ACLs：否

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

ABAC与 CloudShell

支持ABAC（策略中的标签）：否

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

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

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

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

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

将临时证书与 CloudShell

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关其他信息，包括哪些 AWS 服务 适用于临时证书 [AWS 服务](#)，请参阅《IAM用户指南》IAM中的“适用于临时证书”。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM用户指南》中的[切换到角色（控制台）](#)。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅[中的临时安全证书IAM](#)。

当你切换角色时，你将使用不同的环境。您不能在同一个 AWS CloudShell 环境中切换角色。

转发访问会话 CloudShell

支持转发访问会话 (FAS)：否

当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。

CloudShell 的服务角色

支持服务角色：否

服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。

Warning

更改服务角色的权限可能会中断 CloudShell 功能。只有在 CloudShell 提供操作指导时才编辑服务角色。

的服务相关角色 CloudShell

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

基于身份的策略示例 AWS CloudShell

默认情况下，用户和角色无权创建或修改 CloudShell资源。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或执行任务 AWS API。要授予用户对其所需资

源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入角色。

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

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

主题

- [策略最佳实践](#)
- [使用控制 CloudShell台](#)
- [允许用户查看他们自己的权限](#)

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 CloudShell 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托管策略](#)。
- 应用最低权限权限-使用IAM策略设置权限时，仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限IAM的更多信息，请参阅《IAM用户指南》IAM[中的策略和权限](#)。
- 使用IAM策略中的条件进一步限制访问权限-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 [IAMAccess Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的[配置MFA受保护的API访问权限](#)。

有关最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM[中的安全最佳实践](#)。

使用控制 CloudShell 台

要访问AWS CloudShell 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的CloudShell 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

您无需为仅拨打 AWS CLI 或的用户设置最低控制台权限 AWS API。相反，只允许访问与他们尝试执行的API操作相匹配的操作。

为确保用户和角色仍然可以使用 CloudShell 控制台，还需要将 CloudShell *ConsoleAccess*或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《[用户指南](#)》中的[向IAM用户添加权限](#)。

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用或以编程方式完成此操作的 AWS CLI 权限。 AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
```

```
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

对AWS CloudShell 身份和访问进行故障排除

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

主题

- [我无权在以下位置执行操作 CloudShell](#)
- [我无权执行 iam : PassRole](#)
- [我想允许我以外的人 AWS 账户 访问我的 CloudShell 资源](#)

我无权在以下位置执行操作 CloudShell

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

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

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

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

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam : PassRole

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

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的IAM用户marymajor尝试使用控制台在中执行操作时，会出现以下示例错误 CloudShell。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 CloudShell 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 CloudShell 支持这些功能，请参阅[AWS CloudShell 如何使用 IAM](#)。
- 要了解如何提供对您拥有的资源的[访问权限](#)，请参阅《IAM用户指南》中的[AWS 账户 向其他IAM用户提供访问权限](#)。AWS 账户
- 要了解如何向第三方提供对您的资源的[访问权限 AWS 账户](#)，请参阅IAM用户指南中的[向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的[向经过外部身份验证的用户提供访问权限 \(联合身份验证 \)](#)。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。

使用IAM策略管理 AWS CloudShell 访问和使用情况

通过提供的访问管理资源 AWS Identity and Access Management，管理员可以向IAM用户授予权限。这样，这些用户就可以访问 AWS CloudShell 和使用环境的功能。管理员还可以创建策略，在精细级别上指定这些用户可以在 Shell 环境中执行哪些操作。

管理员向用户授予访问权限的最快方法是通过 AWS 托管策略。[AWS托管策略](#)是由创建和管理的独立策略 AWS。以下的 AWS 托管策略 AWS CloudShell 可以附加到IAM身份：

- **AWS CloudShellFullAccess**：授予使用权限，并 AWS CloudShell 具有对所有功能的完全访问权限。

该AWS CloudShellFullAccess策略使用通配符 (*) 来授予IAM身份 (用户、角色或群组) 对 CloudShell 和功能的完全访问权限。有关此策略的更多信息，请参阅[AWS CloudShellFullAccess](#) 《AWS 托管策略用户指南》。

Note

IAM也可以启动具有以下 AWS 托管策略的身份 CloudShell。但是，这些策略提供了广泛的权限。因此，我们建议您仅在这些政策对IAM用户的工作角色至关重要时才授予这些政策。

- **管理员**：为IAM用户提供完全访问权限，并允许他们向中的每项服务和资源委派权限 AWS。
- **开发者高级IAM用户**：使用户能够执行应用程序开发任务，创建和配置支持 AWS 感知型应用程序开发的资源和服务。

有关附加托管策略的更多信息，请参阅《IAM用户指南》中的[添加IAM身份权限 \(控制台 \)](#)。

AWS CloudShell 使用自定义策略管理允许的操作

要管理IAM用户可以执行的操作 CloudShell，请创建使用 CloudShellPolicy 托管策略作为模板的自定义策略。或者，编辑嵌入在相关IAM身份 (用户、组或角色) 中的[内联策略](#)。

例如，您可以允许IAM用户访问 CloudShell，但阻止他们转发用于登录的 CloudShell 环境凭证 AWS Management Console。

Important

要 AWS CloudShell 从启动 AWS Management Console，IAM用户需要具有执行以下操作的权限：

- CreateEnvironment
- CreateSession
- GetEnvironmentStatus

- StartEnvironment

如果附加的策略未明确允许其中一项操作，则在您尝试启动时会返回IAM权限错误 CloudShell。

AWS CloudShell 权限

名称	对已授予权限的描述	需要启动 CloudShell吗？
cloudshell:CreateEnvironment	创建 CloudShell 环境，在会话 CloudShell 话开始时检索布局，并将来自 Web 应用程序的当前布局保存在后端。此权限的期望*值仅Resource为中概述的值 the section called “的 IAM政策示例 CloudShell” 。	是
cloudshell:CreateSession	从连接到 CloudShell 环境 AWS Management Console。	是
cloudshell:GetEnvironmentStatus	读取 CloudShell 环境的状态。	是
cloudshell>DeleteEnvironment	删除 CloudShell 环境。	否
cloudshell:GetFileDownloadURLs	生成预签名URLs 的 Amazon S3，用于 CloudShell 通过 CloudShell 网络界面下载文件。这不适用于VPC环境。	否

名称	对已授予权限的描述	需要启动 CloudShell 吗？
cloudshell:GetFileUploadUrls	生成预签名URLs 的 Amazon S3，用于 CloudShell 通过 CloudShell 网络界面上传文件。这不适用于VPC环境。	否
cloudshell:DescribeEnvironments	描述环境。	否
cloudshell:PutCredentials	将用于登录的凭据转发 AWS Management Console 到。 CloudShell	否
cloudshell:StartEnvironment	启动已停止的 CloudShell 环境。	是
cloudshell:StopEnvironment	停止正在运行的 CloudShell 环境。	否

的IAM政策示例 CloudShell

以下示例说明如何创建策略来限制谁可以访问 CloudShell。这些示例还显示可在 Shell 环境中执行的操作。

以下政策强制完全拒绝访问 CloudShell 及其功能。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyCloudShell",
    "Effect": "Deny",
    "Action": [
      "cloudshell:*"
    ],
    "Resource": "*"
  }]
}
```

```
}

```

以下策略允许IAM用户访问，CloudShell 但禁止他们生成URLs用于文件上传和下载的预签名。用户仍然可以将文件传入和传出环境，例如使用 `wget` 等客户端。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUsingCloudshell",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyUploadDownload",
      "Effect": "Deny",
      "Action": [
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls"
      ],
      "Resource": "*"
    }
  ]
}
```

以下策略允许IAM用户访问 CloudShell。但是，该策略禁止将您用于登录的凭据转发 AWS Management Console 到 CloudShell 环境。IAM使用此策略的用户需要在中手动配置其凭证 CloudShell。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUsingCloudshell",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },

```

```
{
  "Sid": "DenyCredentialForwarding",
  "Effect": "Deny",
  "Action": [
    "cloudshell:PutCredentials"
  ],
  "Resource": "*"
}]
}
```

以下策略允许IAM用户创建 AWS CloudShell 环境。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "CloudShellUser",
    "Effect": "Allow",
    "Action": [
      "cloudshell:CreateEnvironment",
      "cloudshell:CreateSession",
      "cloudshell:GetEnvironmentStatus",
      "cloudshell:StartEnvironment"
    ],
    "Resource": "*"
  }]
}
```

创建和使用 CloudShell VPC环境所需的IAM权限

要创建和使用 CloudShell VPC环境，IAM管理员必须允许访问VPC特定 Amazon EC2 权限。本节列出了创建和使用VPC环境所需的 Amazon EC2 权限。

要创建VPC环境，分配给您的角色的IAM策略必须包含以下 Amazon EC2 权限：

- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeDhcpOptions
- ec2:DescribeNetworkInterfaces

- ec2:CreateTags
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission

我们还建议包括：

- ec2:DeleteNetworkInterface

Note

此权限不是强制性的，但这是清理由 CloudShell 其创建的ENI资源（为 CloudShell VPC环境 ENIs创建的带有ManagedByCloudShell密钥标记）所必需的。如果未启用此权限，则必须在每次使用 CloudShell VPC环境后手动清理ENI资源。

IAM策略授予完全 CloudShell访问权限，包括访问权限 VPC

以下示例显示如何启用对以下内容的完全权限，包括对以下内容的VPC访问权限 CloudShell：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudShellOperations",
      "Effect": "Allow",
      "Action": [
        "cloudshell:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowDescribeVPC",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
    }
  ]
}
```

```

    "Resource": "*"
  },
  {
    "Sid": "AllowCreateTagWithCloudShellKey",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateNetworkInterface"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "ManagedByCloudShell"
      }
    }
  },
  {
    "Sid": "AllowCreateNetworkInterfaceWithSubnetsAndSG",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group*"
    ]
  },
  {
    "Sid": "AllowCreateNetworkInterfaceWithCloudShellTag",
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "ManagedByCloudShell"
      }
    }
  },
  {
    "Sid": "AllowCreateNetworkInterfacePermissionWithCloudShellTag",

```

```

    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterfacePermission"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/ManagedByCloudShell": ""
      }
    }
  },
  {
    "Sid": "AllowDeleteNetworkInterfaceWithCloudShellTag",
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/ManagedByCloudShell": ""
      }
    }
  }
]
}

```

为VPC环境使用IAM条件键

您可以使用 CloudShell 特定条件键进行 VPC 设置，为您的 VPC 环境提供额外的权限控制。您还可以指定 VPC 环境可以使用和不能使用的子网和安全组。

CloudShell 在 IAM 策略中支持以下条件键：

- CloudShell:VpcIds— 允许或拒绝一个或多个 VPCs
- CloudShell:SubnetIds— 允许或拒绝一个或多个子网
- CloudShell:SecurityGroupIds— 允许或拒绝一个或多个安全组

Note

如果修改了有权访问公共 CloudShell 环境的用户的权限以增加对 `cloudshell:createEnvironment` 操作的限制，他们仍然可以访问其现有的公共环境。但是，如果您想修改具有此限制的 IAM 策略并禁用他们对现有公共环境的访问权限，则必须先使用该限制更新 IAM 策略，然后确保您账户中的每个 CloudShell 用户都使用 CloudShell Web 用户界面（操作 → 删除环境）手动删除现有的公共 CloudShell 环境。

带有 VPC 设置条件键的策略示例

以下示例演示如何使用条件键进行 VPC 设置。创建具有所需限制的策略语句后，为目标用户或角色附加策略语句。

确保用户仅创建 VPC 环境并拒绝创建公共环境

为确保用户只能创建 VPC 环境，请使用拒绝权限，如以下示例所示：

```
{
  "Statement": [
    {
      "Sid": "DenyCloudShellNonVpcEnvironments",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudshell:VpcIds": "true"
        }
      }
    }
  ]
}
```

拒绝用户访问特定 VPCs、子网或安全组

要拒绝用户访问特定的 VPCs 内容，`StringEquals` 请使用检查 `cloudshell:VpcIds` 条件的值。以下示例拒绝用户访问 `vpc-1` 和 `vpc-2`：

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "EnforceOutOfVpc",
    "Action": [
      "cloudshell:CreateEnvironment"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudshell:VpcIds": [
          "vpc-1",
          "vpc-2"
        ]
      }
    }
  }
]
}

```

要拒绝用户访问特定的VPCs内容，StringEquals请使用检查cloudshell:SubnetIds条件的值。以下示例拒绝用户访问subnet-1和subnet-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudshell:VpcIds": [
            "vpc-1",
            "vpc-2"
          ]
        }
      }
    }
  ]
}

```

```
]
}
```

要拒绝用户访问特定的VPCs内容，StringEquals请使用检查cloudshell:SecurityGroupIds条件的值。以下示例拒绝用户访问sg-1和sg-2：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfSecurityGroups",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "cloudshell:SecurityGroupIds": [
            "sg-1",
            "sg-2"
          ]
        }
      }
    }
  ]
}
```

允许用户创建具有特定VPC配置的环境

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:VpcIds条件的值。以下示例允许用户访问vpc-1和vpc-2：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificVpc",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",

```

```

    "Condition": {
      "StringEquals": {
        "cloudshell:VpcIds": [
          "vpc-1",
          "vpc-2"
        ]
      }
    }
  ]
}

```

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:SubnetIds条件的值。以下示例允许用户访问subnet-1和subnet-2：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
        "cloudshell:CreateEnvironment"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "cloudshell:SubnetIds": [
            "subnet-1",
            "subnet-2"
          ]
        }
      }
    }
  ]
}

```

要允许用户访问特定的VPCs，StringEquals请使用检查cloudshell:SecurityGroupIds条件的值。以下示例允许用户访问sg-1和sg-2：

```

{
  "Version": "2012-10-17",

```

```
"Statement": [
  {
    "Sid": "EnforceStayInSpecificSecurityGroup",
    "Action": [
      "cloudshell:CreateEnvironment"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "cloudshell:SecurityGroupIds": [
          "sg-1",
          "sg-2"
        ]
      }
    }
  }
]
```

访问权限 AWS 服务

CloudShell 使用您用于登录的IAM凭据 AWS Management Console。

Note

要使用您登录时使用的IAM证书 AWS Management Console，您必须拥有cloudshell:PutCredentials权限。

的这种预身份验证功能 CloudShell 便于使用 AWS CLI。但是，对于从命令行调用的IAM用户 AWS 服务，用户仍然需要显式权限。

例如，假设IAM用户需要创建 Amazon S3 存储桶并将文件作为对象上传给他们。您可以创建明确允许这些操作的策略。IAM控制台提供了交互式[可视化编辑器](#)，可指导您完成构建JSON格式策略文档的过程。创建策略后，您可以将其附加到相关IAM身份（用户、组或角色）。

有关附加托管策略的更多信息，请参阅《IAM用户指南》中的[添加IAM身份权限（控制台）](#)。

登录和监控 AWS CloudShell

本主题介绍如何使用记录和监控 AWS CloudShell 活动和性能 CloudTrail。

使用监控活动 CloudTrail

AWS CloudShell 与 AWS CloudTrail 一项服务集成，该服务提供用户、角色或 AWS 服务 中的操作记录 AWS CloudShell。CloudTrail 将所有 API 呼叫捕获 AWS CloudShell 为事件。捕获的调用包括来自 AWS CloudShell 控制台的调用和对控制台的代码调用 AWS CloudShell API。

如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传送到亚马逊简单存储服务 (Amazon S3) 存储桶。这包括以下活动：AWS CloudShell。

如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集的信息 CloudTrail，您可以发现有关请求的各种信息。例如，您可以确定向哪个请求发出 AWS CloudShell，可以了解发出请求的 IP 地址、谁发出了请求以及何时发出请求。

AWS CloudShell 在 CloudTrail

下表列出了保存在 CloudTrail 日志文件中的 AWS CloudShell 事件。

Note

AWS CloudShell 活动包括：

- *表示这是一个非变异（只读）API 调用。
- 这个词 Environment 与托管 shell 体验的计算环境的生命周期有关。
- 这个词可以 Layout 恢复 CloudShell 终端中的所有浏览器选项卡。

CloudShell 中的活动 CloudTrail

事件名称	描述
createEnvironment	在创建 CloudShell 环境时发生。
createSession	当 CloudShell 环境从连接时发生 AWS Management Console。
deleteEnvironment	在删除 CloudShell 环境时发生。

事件名称	描述
deleteSession	在当前浏览器 CloudShell 选项卡中运行的选项卡中的会话被删除时发生。
getEnvironmentStatus*	在检索 CloudShell 环境状态时发生。
getFileDownloadUrls*	生成用于通过 CloudShell CloudShell 网络界面下载文件的预签名 Amazon S3 URLs 时发生。
getFileUploadUrls*	生成用于使用 CloudShell 网页界面上上传文件的预签名 Amazon S3 URLs 时发生。 CloudShell
cloudshell:DescribeEnvironments	描述环境。
getLayout*	在检索会话开始时的 CloudShell 布局时发生。
putCredentials	当用于登录到的凭据 CloudShell 被 AWS Management Console 转发时发生。
redeemCode*	在 CloudShell 环境中检索刷新令牌的工作流程开始时发生。您稍后可以在 putCredentials 命令中使用此令牌来访问 CloudShell 环境。
sendHeartBeat	用于确认会 CloudShell 话处于活动状态。
startEnvironment	在 CloudShell 环境启动时发生。
stopEnvironment	在运行 CloudShell 环境停止时发生。
updateLayout	保存后端 Web 应用程序的当前布局时发生。

包含“布局”一词的事件会恢复 CloudShell 终端中的所有浏览器选项卡。

EventBridge AWS CloudShell 行动规则

使用 EventBridge 规则，您可以指定在 EventBridge 收到与规则匹配的事件时要采取的目标操作。您可以定义一条规则，根据 CloudTrail 日志文件中记录为事件的 AWS CloudShell 操作来指定要采取的目标操作。

例如，您可以使用put-rule命令[创建 EventBridge 规则](#)。AWS CLI呼put-rule叫必须至少包含 EventPattern 或 ScheduleExpression。当观察到匹配的事件时，会触发带有 EventPatterns 的规则。EventPattern 对于 AWS CloudShell 活动：

```
{ "source": [ "aws.cloudshell" ], "detail-type": [ "AWS API Call via CloudTrail" ],
  "detail": { "eventSource": [ "cloudshell.amazonaws.com" ] } }
```

有关更多信息，请参阅 Amazon EventBridge 用户指南 [EventBridge中的事件和事件模式](#)。

合规性验证 AWS CloudShell

作为多个合规计划的一部分，第三方审计师对 AWS 服务的安全性和 AWS 合规性进行评估。

AWS CloudShell 符合以下合规计划：

SOC

AWS 系统和组织控制 (SOC) 报告是独立的第三方检查报告，用于展示如何 AWS 实现关键合规控制和目标。

服务	SDK	SOC1,2,3
AWS CloudShell	CloudShell	✓

PCI

支付卡行业数据安全标准 (PCIDSS) 是安全标准委员会管理的专有信息PCI安全标准，该委员会由美国运通、Discover Financial Services、In JCB ernational、Worldw MasterCard ide和Visa Inc.创立。

服务	SDK	PCI
AWS CloudShell	CloudShell	✓

ISO以及CSASTAR认证和服务

AWS 已获得符合ISO/

IEC27001:2013、27017:2015、27018:2019、27701:2019、22301:2019、9001:2015 和 v4.0 的合规认证。CSA STAR CCM

服务	SDK	ISO以及CSASTAR认证和服务
AWS CloudShell	CloudShell	✓

FedRamp

联邦风险和授权管理计划 (FedRAMP) 是一项美国政府范围的计划，它为云产品和服务的安全评估、授权和持续监控提供标准方法。

服务	SDK	美联储RAMP温和派 (东/西)	美联储RAMP高点 (GovCloud)
AWS CloudShell	CloudShell	✓	✓

国防部 CC SRG

国防部 (DoD) 云计算安全要求指南 (SRG) 为云服务提供商 (CSPs) 提供了标准化的评估和授权流程，以获得国防部的临时授权，以便他们能够为国防部客户提供服务。

通过国防部 CC SRG 评估和授权的服务将处于以下状态：

- 第三方评估组织 (3PAO) 评估：我们的第三方评估机构目前正在对这项服务进行评估。
- 联合授权委员会 (JAB) 审查：该服务目前正在接受JAB审查。
- 国防信息系统局 (DISA) 审查：该服务目前正在接受DISA审查。

服务	SDK	国防部 CC SRGIL2 (东/西)	国防部 CC SRG IL2 () GovCloud	国防部 CC SRG IL4 () GovCloud	国防部 CC SRG IL5 () GovCloud	国防部 CC SRGIL6 (AWS 秘密区域)
AWS CloudShell	CloudShell	3 PAO 评估	不适用	不适用	不适用	不适用

HIPAA BAA

1996年的《健康保险便携性和问责法》(HIPAA) 是一项联邦法律，要求制定国家标准，以保护敏感的患者健康信息不在患者同意或不知情的情况下被披露。

AWS 使受保实体及其业务伙伴HIPAA能够安全地处理、存储和传输受保护的健康信息 (PHI)。此外，自 2013 年 7 月起，AWS 为此类客户提供标准化的商业伙伴附录 (BAA)。

服务	SDK	HIPAA BAA
AWS CloudShell	CloudShell	✓

IRAP

信息安全注册评估员计划 (IRAP) 使澳大利亚政府客户能够验证适当的控制措施是否到位，并确定适当的责任模式，以满足澳大利亚网络安全中心 (ISM) 编写的《澳大利亚政府信息安全手册》() 的要求 (ACSC)。

服务	命名空间*	IRAP受保护的
AWS CloudShell	不适用	✓

*命名空间可帮助您识别环境中的服务。AWS 例如，在创建IAM策略时，使用 Amazon 资源名称 (ARNs) 并读取 AWS CloudTrail 日志。

MTCS

多层云安全 (MTCS) 是一项可操作的新加坡安全管理标准 (SPRINGSS 584)，基于 ISO 27001/02 信息安全管理系统 () 标准。ISMS

服务	SDK	美国东部 (俄亥俄州)	美国东部 (弗吉尼亚州北部)	美国西部 (俄勒冈州)	美国西部 (北加利福尼亚)	新加坡	首尔
AWS CloudShell	CloudShell	✓	✓	✓	不适用	不适用	不适用

C5

云计算合规控制目录 (C5) 是德国政府支持的认证计划，由联邦信息安全办公室 (BSI) 在德国推出，旨在帮助组织在德国政府的“云提供商安全建议”的背景下使用云服务时证明运营安全，抵御常见的网络攻击。

服务	SDK	C5
AWS CloudShell	CloudShell	✓

ENS高

ENS (Esquema Nacional de Seguridad) 认证计划由财政和公共管理部和CCN (国家密码学中心) 制定。这包括充分保护信息所必需的基本原则和最低要求。

服务	SDK	ENS高
AWS CloudShell	CloudShell	✓

FINMA

瑞士金融市场监管局 (FINMA) 是瑞士的独立金融市场监管机构。AWS与FINMA要求的一致性表明了我们对满足瑞士金融服务监管机构和客户对云服务提供商更高的期望的持续承诺。

服务	SDK	FINMA
AWS CloudShell	CloudShell	✓

PiTuKri

AWS 与 PiTuKri 需求保持一致表明了我们对满足芬兰交通和通信局Traficom对云服务提供商更高的期望的持续承诺。

服务	SDK	PiTuKri
AWS CloudShell	CloudShell	✓

有关特定合规计划范围内的 AWS 服务列表，请参阅合规计划[范围内的AWS服务按合规计划](#)划。有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅在 Artifact 中[下载报告在 AWS Ar](#)。

您在使用 AWS CloudShell 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#)讨论了架构注意事项，并提供了在上面部署以安全为重点和以合规为重点的基准环境的步骤。AWS
- [HIPAA安全与合规架构白皮书 — 本白皮书](#)描述了公司如何使用 AWS 来创建HIPAA符合要求的应用程序。
- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [使用AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- [AWS Security Hub](#)— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准 and 最佳实践。

韧性在 AWS CloudShell

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

除了 AWS 全球基础架构外，还 AWS CloudShell 支持以下功能来支持您的数据弹性和备份需求：

- 提交您创建并添加到的文件 AWS CodeCommit。这是一项 Amazon Web Services 托管的版本控制服务，可让您在云中私人化存储和管理资产。这些资产可包括文档、源代码和二进制文件。有关更多信息，请参阅 [CodeCommit 在中使用 AWS CloudShell](#)。
- 使用 AWS CLI 调用在中指定主目录中的 AWS CloudShell 文件，并将它们作为对象添加到 Amazon S3 存储桶中。有关示例，请参阅[入门 AWS CloudShell](#)。

中的基础设施安全 AWS CloudShell

作为一项托管服务 AWS CloudShell，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅[AWS 云安全](#)。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS security Pillar Well-Architected Framework 中的[基础设施保护](#)。

您可以使用 AWS 已发布的 API 呼叫 AWS CloudShell 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic Curve Diffie-Hellman)。ECDHE 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的私有访问密钥对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

Note

默认情况下，AWS CloudShell 自动为计算环境的系统包安装安全补丁。

以下方面的安全最佳实践 AWS CloudShell

以下最佳实践是一般指导原则，并不代表完整安全解决方案。由于这些最佳实践可能不适合或不足以适应您的环境，因此我们建议您将它们视为有用的注意事项而不是处方。

以下方面的一些安全最佳实践 AWS CloudShell

- 使用IAM权限和策略来控制访问权限，AWS CloudShell 并确保用户只能执行其角色要求的操作（例如，下载和上传文件）。有关更多信息，请参阅使用[IAM策略管理 AWS CloudShell 访问和使用情况](#)。
- 请勿在IAM实体中包含敏感数据，例如用户、角色或会话名称。
- 启用“保持安全粘贴”功能，以捕获从外部源复制的文本中的潜在安全风险。默认情况下，“安全粘贴”处于启用状态。有关对多行文本使用安全粘贴的更多信息，请参阅对多行文本[使用安全粘贴](#)。
- 如果您在的计算环境中安装第三方应用程序，请熟悉[共担安全责任模型](#) AWS CloudShell。
- 在编辑会影响用户 Shell 体验的 Shell 脚本之前，请准备好回滚机制。有关修改默认 shell 环境的更多信息，请参阅[使用脚本修改 shell](#)。
- 将您的代码安全地存储在版本控制系统中，如 [AWS CodeCommit](#)。

AWS CloudShell 安全 FAQs

以下是有关安全性的常见问题的答案 CloudShell。

- [启动和启动 shell 会话时使用了哪些 AWS 流程 CloudShell 和技术？](#)
- [是否可以将网络访问限制为 CloudShell？](#)
- [我可以自定义我的 CloudShell 环境吗？](#)
- [我的 \\$HOME 目录实际上存储在 AWS Cloud 中的什么地方？](#)
- [可以加密我的 \\$HOME 目录吗？](#)
- [我能否对我的 \\$HOME 目录进行病毒扫描？](#)

启动和启动 shell 会话时使用了哪些 AWS 流程 CloudShell 和技术？

登录时 AWS Management Console，您需要输入您的IAM用户凭据。而且，当您 CloudShell 从控制台界面启动时，这些凭据将用于调用 CloudShell API，从而为服务创建计算环境。然后为计算环境创建一个 AWS Systems Manager 会话，并 CloudShell 向该会话发送命令。

[返回安全清单 FAQs](#)

是否可以将网络访问限制为 CloudShell ？

对于公共环境，不可能限制网络访问。如果要限制网络访问，则必须启用仅创建VPC环境和拒绝创建公共环境的权限。

有关更多信息，请参阅[确保用户仅创建VPC环境并拒绝创建公共环境](#)。

对于 CloudShell VPC环境，网络设置继承自您的VPC。CloudShell 在中使用VPC可以控制 CloudShell VPC环境的网络访问权限。

[返回安全清单 FAQs](#)

我可以自定义我的 CloudShell 环境吗？

您可以为您的 CloudShell 环境下载和安装实用程序和其他第三方软件。只有安装在 \$HOME 目录中的软件才会在会话之间保留。

根据[AWS 责任共担模式](#)的定义，您负责对所安装的应用程序进行必要的配置和管理。

[返回安全清单 FAQs](#)

我的 \$HOME 目录实际上存储在 AWS Cloud中的什么地方？

对于公共环境，用于在中存储数据的基础设施由 Amazon S3 提供。\$HOME

对于VPC环境，当您的环境超时（20-30 分钟处于非活动状态之后），或者当您删除或重新启动VPC环境时，您的\$HOME目录将被删除。

[返回安全清单 FAQs](#)

可以加密我的 \$HOME 目录吗？

不可以，不可能用自己的密钥加密您的\$HOME目录。但是在将您的\$HOME目录内容存储在 Amazon S3 中时会对其 CloudShell 进行加密。

[返回安全清单 FAQs](#)

我能否对我的 \$HOME 目录进行病毒扫描？

目前，无法对您的 \$HOME 目录进行病毒扫描。对此功能的支持正在审核中。

[返回安全清单 FAQs](#)

我能否限制我的数据入口或出口？ CloudShell

要限制入口或出口，我们建议您使用环境。 CloudShell VPC当您的VPCVPC环境超时（20-30分钟处于非活动状态之后），或者当您删除或重新启动环境时，环境的\$HOME目录将被删除。在“操作”菜单中，上传和下载选项不适用于VPC环境。

[返回安全清单 FAQs](#)

AWS CloudShell 计算环境：规格和软件

启动时 AWS CloudShell，将创建一个基于 [Amazon Linux 2023](#) 的计算环境来托管 shell 体验。该环境配置了 [计算资源 \(vCPU 和内存\)](#)，并提供了大量可从命令行界面访问的 [预安装软件](#)。确保您在计算环境中安装的所有软件都已修补并处于最新状态。您还可以通过安装软件和修改 Shell 脚本来配置默认环境。

计算环境资源

每个 AWS CloudShell 计算环境都分配了以下资源CPU和内存资源：

- 1 vCPU (虚拟中央处理器)
- 2 GiB RAM

而且，为环境配置了以下存储配置：

- 1GB 持久性存储空间 (会话结束后存储空间仍保留)

有关更多信息，请参阅 [持久性存储](#)。

CloudShell 网络要求

WebSockets

CloudShell 取决于WebSocket 协议，该协议允许用户的 Web 浏览器和 AWS 云端 CloudShell 服务之间进行双向交互式通信。如果您在专用网络中使用浏览器，则代理服务器和防火墙可能有助于安全访问互联网。WebSocket 通信通常可以毫无问题地通过代理服务器。但是在某些情况下，代理服务器会 WebSockets 阻止正常工作。如果出现此问题，您的 CloudShell 接口将报告以下错误：Failed to open sessions : Timed out while opening the session。

如果此错误反复出现，请参阅代理服务器的文档，确保将其配置为允许 WebSockets。或者，您可以与网络的系统管理员联系。

Note

如果要通过特定许可名单来定义精细权限URLs，则可以添加 AWS Systems Manager 会话用来打开 WebSocket 连接以发送输入和接收输出的部分权限。URL（您的 AWS CloudShell 命令将发送到该 Systems Manager 会话。）

Systems Manager StreamUrl 使用的格式是 `wss://`

`ssmmessages.region.amazonaws.com/v1/data-channel/session-id?`

`stream=(input|output)`。

该区域表示所 AWS Systems Manager 支持的 AWS 区域（例如 `us-east-2` 美国东部（俄亥俄州）地区的区域标识符。

由于会话 ID 是在特定 Systems Manager 会话成功启动后创建的，因此您只能 `wss://ssmmessages.region.amazonaws.com` 在更新许可名单时指定。URL 有关更多信息，请参阅《AWS Systems Manager API 参考》中的 [StartSession](#) 操作。

预安装的软件

Note

由于 AWS CloudShell 开发环境会定期更新以提供对最新软件的访问权限，因此我们在本文档中不提供具体的版本号。相反，我们将介绍如何检查安装了哪个版本。要查看已安装的版本，请输入程序名称，然后选择 `--version` 选项（例如，`git --version`）。

Shell

预安装的 Shell

名称	描述	版本信息
Bash	Bash 外壳是的默认外壳应用程序。AWS CloudShell	<code>bash --version</code>
PowerShell (pwsh)	提供命令行界面和脚本语言支持，PowerShell 建立在 Microsoft 的基础上。NET 命令语言运行时。PowerShell 使用	<code>pwsh --version</code>

名称	描述	版本信息
Z Shell (zsh)	<p>名为接受和返回cmdlets的轻量级命令。NET物体。</p> <p>Z Shell，也被称为 zsh，是 Bourne Shell 的扩展版本，它为主题和插件提供了增强的自定义支持。</p>	zsh --version

AWS 命令行界面 (CLI)

CLI

名称	描述	版本信息
AWS CDK 工具包 CLI	<p>T AWS CDK toolkit (CLI命令) 是与您的 AWS CDK 应用程序交互的主要工具。cdk它执行您的应用程序，查询您定义的应用程序模型，并生成和部署由生成的 AWS CloudFormation 模板。AWS CDK</p> <p>有关更多信息，请参阅 AWS CDK 工具包。</p>	cdk --version
AWS CLI	<p>AWS CLI 是一个命令行界面，可用于从命令行管理多个 AWS 服务，并使用脚本自动执行这些服务。有关更多信息，请参阅 使用中的 AWS 服务 AWS CloudShell。</p> <p>有关如何确保使用最多的 up-to-date AWS CLI 版本 2 的信</p>	aws --version

名称	描述	版本信息
	息，请参阅 安装 AWS CLI 到你的主目录 。	
EB CLI	<p>AWS Elastic Beanstalk CLI 提供了命令行界面，可简化从本地存储库创建、更新和监控环境的过程。</p> <p>有关更多信息，请参阅《开发人员指南》中的“使用 Elastic Beanstalk 命令行接口 CLI (EB)”。AWS Elastic Beanstalk</p>	eb --version
Amazon ECS CLI	<p>亚马逊弹性容器服务 (AmazonECS) 命令行界面 (CLI) 提供高级命令来简化集群和任务的创建、更新和监控。</p> <p>有关更多信息，请参阅《亚马逊弹性容器服务开发者指南》中的使用亚马逊ECS命令行界面。</p>	ecs-cli --version

名称	描述	版本信息
AWS SAM CLI	<p>AWS SAM CLI是一个对 AWS Serverless Application Model 模板和应用程序代码进行操作的命令行工具。您可以执行多项任务。其中包括在本地调用 Lambda 函数、为无服务器应用程序创建部署包以及将您的无服务器应用程序部署到云端。AWS</p> <p>有关更多信息，请参阅《AWS Serverless Application Model 开发人员指南》中的AWS SAM CLI命令参考。</p>	<pre>sam --version</pre>
AWS Tools for PowerShell	<p>AWS Tools for PowerShell 这些 PowerShell 模块是在公开的功能基础上构建的 AWS SDK for .NET。使用 AWS Tools for PowerShell，您可以通过 PowerShell 命令行编写 AWS 资源操作脚本。</p> <p>AWS CloudShell 预安装的模块化版本 (AWS.Tools)。AWS Tools for PowerShell 有关更多信息，请参阅《AWS Tools for PowerShell 用户指南》 PowerShell中的使用AWS 工具。</p>	<pre>pwsh --Command ' Get-Module -ListAvailable -Name AWS.Tools .Common'</pre>

运行时和 AWSSDKs : Node.js 和 Python 3

运行时和 AWS SDKs

名称	描述	版本信息
Node.js (带 npm)	<p>Node.js 是一个 JavaScript 运行时，旨在简化异步编程技术的应用。有关更多信息，请参阅 Node.js 官方网站上的文档。</p> <p>npm 是一个包管理器，提供对 JavaScript 模块在线注册表的访问。有关更多信息，请参阅 npm 官方网站上的文档。</p>	<ul style="list-style-type: none"> Node.js: <code>node --version</code> npm : <code>npm --version</code>
SDK for JavaScript 在 Node.js 中	<p>软件开发套件 (SDK) 通过为包括亚马逊 S3、亚马逊、DynamoDB 和亚马逊在内的 AWS 服务提供 JavaScript 对象 EC2，帮助简化编码。SWF 有关更多信息，请参见 AWS SDK for JavaScript 开发人员指南。</p>	<pre>npm -g ls --depth 0 2>/dev/null grep aws-sdk</pre>
Python	<p>Python 3 已准备好在外壳环境中使用。Python 3 现在被认为是该编程语言的默认版本（对 Python 2 的支持已于 2020 年 1 月结束）。有关更多信息，请参阅 Python 官方网站上的文档。</p> <p>此外，预装的是 Pip，这是一款适用于 Python 的软件包安装程序。您可以使用此命令行程序从在线索引（例如 Python 程序包索引）中安装 Python 软件包。有关更多信息，请参阅</p>	<ul style="list-style-type: none"> Python 3: <code>python3 --version</code> pip: <code>pip3 --version</code>

名称	描述	版本信息
	Python 打包权威机构提供的文档 。	
SDK适用于 Python (Boto3)	<p>Boto 是 Python 开发人员用来创建、配置和管理的软件开发套件 (SDK) AWS 服务，例如亚马逊EC2和亚马逊 S3。SDK 提供了面向对象API的 easy-to-use访问权限和低级访问权限。AWS 服务</p> <p>更多信息，请参阅 Boto3 文档。</p>	<pre>pip3 list grep boto3</pre>

开发工具和 Shell 实用程序

开发工具和 Shell 实用程序

名称	描述	版本信息
bash-completion	<p>bash-completion 是一个 Shell 函数集合，允许通过按 Tab 键自动完成部分键入的命令或参数。您可以在 <code>/usr/share/bash-completion/completions</code> 中找到 bash-completion 支持的软件包。</p> <p>要为软件包的命令设置自动完成功能，必须获取该程序文件。例如，要为 Git 命令设置自动完成功能，请在 <code>.bashrc</code> 中添加以下一行，这样每当您的 AWS CloudShell 会话开始时，该功能都可用：</p>	<pre>dnf info bash-completion</pre>

名称	描述	版本信息
	<pre>source /usr/share/ bash-completion/ completions/git</pre> <p>如果要使用自定义完成脚本，请将它们添加到持久性主目录 (\$HOME) 中，然后直接从 .bashrc 中获取它们。</p> <p>有关更多信息，请参阅该项目的 README 页面 GitHub。</p>	
CodeCommit 适用于 Git 的实用工具	<p>git-remote-codecommit 是一个实用工具，它提供了一种通过扩展 Git 从 CodeCommit 存储库中推送和提取代码的简单方法。这是支持使用联合访问、身份提供程序和临时凭证建立连接的推荐方法。</p> <p>有关更多信息，请参阅《AWS CodeCommit 用户指南》git-remote-codecommit 中的 AWS CodeCommit 与 HTTPS 连接的安装步骤。</p>	<pre>pip3 list grep git- remote-codecommit</pre>
Git	<p>Git 是一个分布式版本控制系统，它通过分支工作流程和内容暂存支持现代软件开发实践。有关更多信息，请参阅 Git 官方网站上的文档页面。</p>	<pre>git --version</pre>
iputils	<p>iputils 软件包包含用于 Linux 联网的实用程序。有关所提供实用程序的更多信息，请参阅上的 iputils 存储库。GitHub</p>	<p>iputils 工具的示例：arping -V</p>

名称	描述	版本信息
jq	jq 实用程序解析JSON格式化数据以生成由命令行过滤器修改的输出。有关更多信息，请参阅 托管的 jq 手册 。 GitHub	jq --version
kubectl	kubectl 是一个命令行工具，用于使用 Kubernetes 与 Kubernetes 集群的控制平面进行通信。API	kubectl --version
make	make 实用程序使用 makefiles 自动执行任务集并组织代码编译。有关更多信息，请参阅 GNU Make 文档 。	make --version
man	man 命令提供命令行实用程序和工具的手册页。例如，man ls 返回列出目录内容的 ls 命令的手册页。更多信息，请参阅 Wikipedia 的 man 词条 。	man --version
nano	nano 是一款小型且用户友好的、基于文本界面的编辑器。有关更多信息，请参阅 GNU nano 文档 。	nano --version
procps	procps 是一个系统管理实用程序，可用于监控和停止当前正在运行的进程。有关更多信息，请参阅 列出可以使用 procps 运行的程序的README文件 。	ps --version

名称	描述	版本信息
SSH客户端	SSH客户端使用安全 shell 协议与远程计算机进行加密通信。Op SSH en 是预安装的 SSH 客户端。欲了解更多信息，请参阅 公开赛维护的公开SSH网站 BSD。	ssh -V
sudo	使用 sudo 实用程序，用户可以使用其他用户（通常是超级用户）的安全权限运行程序。当您需要以系统管理员身份安装应用程序时，Sudo 非常有用。有关更多信息，请参阅 Sudo 手册 。	sudo --version
tar	tar 是一个命令行实用程序，可用于将多个文件分组到单个存档文件（通常称为 tarball）中。有关更多信息，请参阅 GNUtar 文档 。	tar --version
tmux	tmux 是一个终端多路复用器，可用于在多个窗口中同时运行不同的程序。有关更多信息，请参阅 简要介绍 tmux 的博客 。	tmux -V
unzip	有关更多信息，请参阅 zip/unzip 。	
vim	Vim 是一个可自定义的编辑器，您可以通过基于文本的界面与之交互。更多信息，请参阅 vim.org 上提供的文档资源 。	vim --version

名称	描述	版本信息
wget	wget 是一种计算机程序，用于从命令行中的端点指定的 Web 服务器检索内容。有关更多信息，请参阅 GNUWget 文档 。	wget --version
zip/unzip	zip/unzip 实用程序使用存档文件格式，可在不丢失数据的情况下提供无损数据压缩。调用 zip 命令将文件分组并压缩到单个存档中。使用 unzip 将存档中的文件解压缩到指定目录中。	unzip --version zip --version
Docker	Docker 是一个用于开发、发布和运行应用程序的开放平台。Docker 使您可以将应用程序与基础架构分开，以便快速交付软件。它使你能够在内部构建 Dockerfile AWS CloudShell，并使用它来构建 Docker 资产。CDK有关 Docker 支持哪些 AWS 区域的信息，请参阅 支持的 AWS 区域 。 AWS CloudShell 你应该知道，Docker 在环境中的空间有限。如果您的单个镜像较大，或者预先存在的 Docker 镜像过多，则可能会导致问题。有关 Docker 的更多信息，请参阅 Docker 文档指南 。	docker --version

安装 AWS CLI 到你的主目录

与 CloudShell 环境中预安装的其余软件一样，该 AWS CLI 工具会自动更新定期升级和安全补丁。如果要确保拥有的最高 up-to-date 版本 AWS CLI，可以选择在外壳程序的主目录中手动安装该工具。

Important

您需要在主目录 AWS CLI 中手动安装副本，以便下次启动 CloudShell 会话时可用。之所以需要此安装，是因为在完成 Shell 会话后，添加到 \$HOME 之外的目录的文件将被删除。此外，安装此副本后 AWS CLI，它不会自动更新。换句话说，管理更新和安全补丁是您的责任。有关责任 AWS 共担模型的更多信息，请参阅[中的数据保护 AWS CloudShell](#)。

要安装 AWS CLI

1. 在 CloudShell 命令行中，使用 curl 命令将 AWS CLI 已安装的压缩副本传输到 shell：

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

2. 对压缩文件夹进行解压缩：

```
unzip awscliv2.zip
```

3. 要将工具添加到指定文件夹，请运行 AWS CLI 安装程序：

```
sudo ./aws/install --install-dir /home/cloudshell-user/usr/local/aws-cli --bin-dir /home/cloudshell-user/usr/local/bin
```

如果安装成功，命令行会显示以下消息：

```
You can now run: /home/cloudshell-user/usr/local/bin/aws --version
```

4. 为了方便起见，我们建议您同时更新 PATH 环境变量，这样在运行 aws 命令时就无需指定工具的安装路径：

```
export PATH=/home/cloudshell-user/usr/local/bin:$PATH
```

Note

如果撤消此更改PATH，则默认情况下，不包含指定路径的aws命令将使用预安装 AWS CLI 的版本。

在 Shell 环境中安装第三方软件

Note

我们建议您在向的计算环境安装任何第三方应用程序之前，先查看[安全责任共担模型](#)。AWS CloudShell

默认情况下，所有 AWS CloudShell 用户都具有 sudo 权限。因此，您可以使用 sudo 命令来安装 Shell 计算环境中尚不可用的软件。例如，您可以使用DNF软件包管理实用程序sudo进行安装cowsay，该实用程序会生成带有以下消息的奶牛的ASCII艺术图片：

```
sudo dnf install cowsay
```

然后，您可以通过键入 `echo "Welcome to AWS CloudShell" | cowsay` 来启动新安装的程序。

Important

Package 管理工具，例如 dnf 将程序安装在目录中（例如）`/usr/bin`，当你的 shell 会话结束时，这些程序会被回收。这意味着要在每个会话的基础上安装和使用其他软件。

使用脚本修改 Shell

如果您要修改默认的 Shell 环境，可以编辑每次启动 Shell 环境时都会运行的 Shell 脚本。每当默认 bash shell 启动时，`.bashrc` 脚本就会运行。

Warning

如果您错误地修改了 `.bashrc` 文件，则以后可能无法访问您的 Shell 环境。在编辑文件之前，最好先制作一份文件副本。您还可以在编辑 `.bashrc` 时通过打开两个 Shell 来降低风险。如果您在一个 Shell 中失去访问权限，则仍可以登录到另一个 Shell，并且可以回滚任何更改。

如果修改错误 `.bashrc` 或任何其他文件后确实失去了访问权限，则可以通过[删除主目录 AWS CloudShell](#)来恢复其默认设置。

在此过程中，您将修改 `.bashrc` 脚本，以便您的 Shell 环境自动切换到运行 Z shell。

1. 使用文本编辑器（例如 Vim）打开 `.bashrc`：

```
vim .bashrc
```

2. 在编辑器界面中，按 `I` 键开始编辑，然后添加以下内容：

```
zsh
```

3. 要退出并保存编辑后的 `.bashrc` 文件，请 `Esc` 进入 Vim 命令模式并输入以下内容：

```
:wq
```

4. 使用 `source` 命令重新加载 `.bashrc` 文件：

```
source .bashrc
```

当命令行界面再次可用时，提示符号已更改为 `%` 表示您现在正在使用 Z shell。

AWS CloudShell 从迁移AL2到 AL2 023

AWS CloudShell基于亚马逊 Linux 2 (AL2)，现已迁移到亚马逊 Linux 2023 (AL2023)。有关 AL2 023 的更多信息，请参阅[亚马逊 Linux 2023 用户指南中的什么是亚马逊 Linux 2023 \(AL2023\)](#)。

使用 AL2 023，您可以使用提供的所有工具继续访问现有 CloudShell 环境。CloudShell有关可用工具的更多信息，请参阅[预安装的软件](#)。

AL2023 对开发工具进行了多项改进，包括更新版本的软件包，例如 Node.js 18 和 Python 3.9。

Note

在 AL2 023 年，Python 2 已不再随您的 CloudShell 环境一起提供。

有关 AL2 和 AL2 023 之间主要区别的更多信息，请参阅《[亚马逊 Linux 2023 用户指南](#)》中的“[比较亚马逊 Linux 2 和亚马逊 Linux 2023](#)”。

如果您有任何疑问，请联系 [AWS Support](#)。您还可以在 [AWS re:Post](#) 上搜索答案和发布问题。当您进入时 AWS re:Post，您可能需要登录 AWS。

AWS CloudShell 迁移 FAQs

以下是有关从 023 迁移 AL2 到 AL2 023 的一些常见问题的答案。AWS CloudShell

- [此次迁移会影响我的任何其他 AWS 资源（例如运行的 Amazon EC2 实例）AL2 吗？](#)
- [迁移到 AL2 023 后会更改哪些软件包？](#)
- [我可以选择不迁移吗？](#)
- [我能否为我的 AWS CloudShell 环境创建备份？](#)

迁移到 AL2 023 会影响我的任何其他 AWS 资源（例如运行的 Amazon EC2 实例）吗？ AL2

除了您的 AWS CloudShell 环境之外，没有任何服务或资源受到此次迁移的影响。这包括您可能已在内部创建或访问的资源 AWS CloudShell。例如，如果您创建了一个在其上运行的 Amazon EC2 实例 AL2，则不会迁移到 AL2 023。

迁移到 AL2 023 后，有哪些软件包发生了变化？

AWS CloudShell 环境当前包括预安装的软件。要了解预安装软件的完整列表，请参阅[预安装](#)的软件。AWS CloudShell 将继续交付这些软件包，Python 2 除外。有关和 023 提供的软件包之间的完整区别，请参阅[比较 AL2 AL2 和 AL2 AL2 0 23](#)。对于在迁移到 AL2 023 之后将不再满足的特定软件包和版本要求的客户，我们建议您联系 Supp AWS ort 提交申请。

我可以选择不迁移吗？

不，您不能选择退出迁移。AWS CloudShell 环境由管理 AWS，因此，所有环境都已升级到 AL2 023。

我能否为我的 AWS CloudShell 环境创建备份？

AWS CloudShell 将继续保留用户的主目录。有关更多信息，请参阅 [AWS CloudShell 服务限额和限制](#)。如果您在主文件夹中存储了任何文件或配置，并且想要为其创建备份，请完成 [步骤 6：创建主目录备份](#)。

故障排除 AWS CloudShell

使用时 AWS CloudShell，您可能会遇到问题，例如使用 shell 命令行界面启动 CloudShell 或执行关键任务时。本章介绍的信息涵盖如何解决您可能遇到的一些常见问题。

有关各种问题的答案 CloudShell，请参阅[AWS CloudShell FAQs](#)。您还可以在[AWS CloudShell 论坛](#)上搜索答案和发布问题。当您进入此论坛时，可能会要求您登录 AWS。您也可以直接[联系我们](#)。

纠正错误

当您遇到以下任何索引错误时，可以使用以下解决方案来解决这些错误。

主题

- [错误：“无法启动环境。要重试，请刷新浏览器或通过选择“操作，重新启动”来重新启动 AWS CloudShell](#)
- [错误：“无法启动环境。您没有所需的权限。请您的IAM管理员授予对 AWS CloudShell”的访问权限](#)
- [无法访问 AWS CloudShell 命令行](#)
- [无法 ping 外部 IP 地址](#)
- [准备您的终端时遇到了一些问题](#)
- [箭头键在中无法正常工作 PowerShell](#)
- [不支持的 Web 套接字会导致无法启动 CloudShell 会话](#)
- [无法导入 AWSPowerShell.NetCore 模块](#)
- [使用 Docker 时未运行 AWS CloudShell](#)
- [Docker 的磁盘空间已经用完了](#)
- [docker push正在超时并且一直在重试](#)
- [无法VPC从我的 AWS CloudShell VPC环境中访问其中的资源](#)
- [ENI AWS CloudShell 用于我的VPC环境的未清理干净](#)
- [仅CreateEnvironment有权访问VPC环境的用户也可以访问公共 AWS CloudShell 环境](#)
- [证书在中不起作用 CloudShell](#)

错误：“无法启动环境。要重试，请刷新浏览器或通过选择“操作，重新启动”来重新启动 AWS CloudShell

问题：当您尝试 AWS CloudShell 从启动时 AWS Management Console，即使您已获得IAM管理员所需的权限，并且您已刷新浏览器或重新 CloudShell启动，您仍会被拒绝访问。

解决方案：联系 [AWS Support](#)。

([回到顶部](#))

错误：“无法启动环境。您没有所需的权限。请您的IAM管理员授予对 AWS CloudShell” 的访问权限

问题：当您尝试 AWS CloudShell 从启动时 AWS Management Console，系统会拒绝您访问并通知您没有所需的权限。

原因：您用于访问的IAM身份 AWS CloudShell 缺少必要的IAM权限。

解决方案：请求IAM管理员为您提供必要的权限。他们可以通过添加附加的 AWS 托管策略 (AWSCloudShellFullAccess) 或嵌入式内联策略来实现此目的。有关更多信息，请参阅 [使用IAM策略管理 AWS CloudShell 访问和使用情况](#)。

([回到顶部](#))

无法访问 AWS CloudShell 命令行

问题：修改计算环境使用的文件后，您无法在中访问命令行 AWS CloudShell。

解决方案：如果修改不当 `.bashrc` 或任何其他文件后失去访问权限，则可以通过 [删除主目录 AWS CloudShell](#) 来恢复其默认设置。

([回到顶部](#))

无法 ping 外部 IP 地址

问题：从命令行 (例如，`ping amazon.com`) 运行 `ping` 命令时，您会收到以下消息。

```
ping: socket: Operation not permitted
```

原因：ping 实用程序使用 Internet 控制消息协议 (ICMP) 向目标主机发送回应请求数据包。它会等待目标的回显回复。由于中未启用该ICMP协议 AWS CloudShell，因此 ping 实用程序无法在 shell 的计算环境中运行。

解决方案：由于中ICMP不支持 AWS CloudShell，您可以运行以下命令来安装 Netcat。Netcat 是一款计算机网络实用程序，用于使用TCP或UDP读取和写入网络连接。

```
sudo yum install nc
nc -zv www.amazon.com 443
```

([回到顶部](#))

准备您的终端时遇到了一些问题

问题：尝试 AWS CloudShell 使用 Microsoft Edge 浏览器进行访问时，你无法启动 shell 会话，并且浏览器会显示一条错误消息。

原因：与早期版本 AWS CloudShell 的 Microsoft Edge 不兼容。您可以使用支持的浏览器的最新四个主要版本进行访问 AWS CloudShell。

解决方案：从 [Microsoft 网站](#) 安装更新版本的 Edge 浏览器。

([回到顶部](#))

箭头键在中无法正常工作 PowerShell

问题：在正常操作中，您可以使用箭头键浏览命令行界面，并来回扫描命令历史记录。但是，在某些版本的 PowerShell on 中按箭头键时 AWS CloudShell，可能会错误地输出字母。

原因：在 Linux 上运行的 PowerShell 7.2.x 版本中，箭头键错误输出字母的情况是一个已知问题。

解决方案：要删除修改箭头键行为的转义序列，请编辑 PowerShell 配置文件并将 \$PSStyle 变量设置为 PlainText。

1. 在 AWS CloudShell 命令行中，输入以下命令以打开配置文件。

```
vim ~/.config/powershell/Microsoft.PowerShell_profile.ps1
```

Note

如果您已经在编辑器中 PowerShell，也可以使用以下命令在编辑器中打开配置文件。

```
vim $PROFILE
```

- 在编辑器中，转到文件现有文本的末尾，按 `i` 进入插入模式，然后添加以下语句。

```
$PSStyle.OutputRendering = 'PlainText'
```

- 编辑完成后，按下 `Esc` 进入命令模式。接下来，请输入以下命令保存文件，然后退出编辑器。

```
:wq
```

Note

您的更改将在下次开始时生效 PowerShell。

([回到顶部](#))

不支持的 Web 套接字会导致无法启动 CloudShell 会话

问题：尝试启动时 AWS CloudShell，您会反复收到以下消息：`Failed to open sessions : Timed out while opening the session.`

原因：CloudShell 取决于 WebSocket 协议，它允许在您的 Web 浏览器和之间进行双向交互式通信 AWS CloudShell。如果您在专用网络中使用浏览器，则代理服务器和防火墙可能有助于安全访问互联网。WebSocket 通信通常可以毫无问题地通过代理服务器。但是，在某些情况下，代理服务器 WebSockets 无法正常工作。如果出现此问题，则 CloudShell 无法启动 shell 会话，连接尝试最终会超时。

解决方案：连接超时可能是由不支持 WebSockets 以外的其他问题引起的。如果是这种情况，请先刷新 CloudShell 命令行界面所在的浏览器窗口。

如果刷新后仍然出现超时错误，请参阅代理服务器的文档。并且，请确保您的代理服务器已配置为允许 WebSocket。或者，请与您网络的系统管理员联系。

Note

假设您想通过特定许可名单来定义精细权限。URLs您可以添加 AWS Systems Manager 会话用来打开用于发送输入和接收输出的 WebSocket连接的一部分。URL您的 AWS CloudShell 命令将发送到该 Systems Manager 会话。

Systems Manager 使用的格式是 `wss://ssmmessages.region.amazonaws.com/v1/data-channel/session-id?stream=(input|output)`。StreamUrl 该区域表示支持的区域标 AWS 区域 标识符 AWS Systems Manager。例如，`us-east-2` 是美国东部（俄亥俄州）区域的区域标识符。

由于会话 ID 是在特定 Systems Manager 会话成功启动后创建的，因此您只能指定 `wss://ssmmessages.region.amazonaws.com` 何时更新许可名单。URL 有关更多信息，请参阅《AWS Systems Manager API 参考》中的 [StartSession](#) 操作。

([回到顶部](#))

无法导入 `AWSPowerShell.NetCore` 模块

问题：当您导入时 `AWSPowerShell.NetCore` 在 PowerShell 的模块中 `Import-Module -Name AWSPowerShell.NetCore`，您会收到以下错误消息：

导入模块：指定的模块 'AWSPowerShell.NetCore' 未加载，因为在任何模块目录中都找不到有效的模块文件。

原因：该 `AWSPowerShell.NetCore` 模块已被每个服务的 `AWS.Tools` 模块所取代。AWS CloudShell

解决方案：可能不再需要任何显式导入语句，或者需要将其更改为相关的每项服务 `AWS.Tools` 模块。

Example

Example

- 在大多数情况下，只要不使用 `.Net` 类型，就不需要任何显式导入语句。以下是导入语句的示例。
 - `Get-S3Bucket`
 - `(Get-EC2Instance).Instances`
- 如果使用 `.Net` 类型，请导入服务级别模块 (`AWS.Tools.<Service>`)。以下是示例语法。

```
Import-Module -Name AWS.Tools.EC2
$instanceTag = [Amazon.EC2.Model.Tag]::new("Environment","Dev")
```

```
Import-Module -Name AWS.Tools.S3
$lifecycleRule = [Amazon.S3.Model.LifecycleRule]::new()
```

有关更多信息，请参阅 AWS Tools for PowerShell的[版本 4 公告](#)。

([回到顶部](#))

使用 Docker 时未运行 AWS CloudShell

问题：使用 AWS CloudShell Docker 时无法正常运行。您会收到以下错误消息：`docker: Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?.`

解决方案：尝试重启您的环境。当您在不支持 Docker 的 GovCloud 区域 AWS CloudShell 中运行 Docker 时，可能会出现此错误消息。请确保您在支持的 AWS 区域中运行 Docker。有关可用 Docker 的区域列表，请参阅[支持的 AWS 区域 AWS CloudShell](#)

Docker 的磁盘空间已经用完了

问题：您收到以下错误消息：`ERROR: failed to solve: failed to register layer: write [...]: no space left on device.`

原因：Dockerfile 超出了中的可用磁盘空间。AWS CloudShell 这可能是由于单个镜像过大或预先存在的 Docker 镜像过多造成的。

解决方案：运行 `df -h` 以查找磁盘使用情况。运行 `sudo du -sh /folder/folder1` 来评估某些您认为可能很大的文件夹的大小，并考虑删除其他文件以释放空间。一种选择是考虑通过运行 `docker rmi` 来删除未使用的 Docker 镜像。你应该知道 Docker 在环境中的空间有限，有关 Docker 的更多信息，请参阅 [Docker 文档指南](#)。

docker push正在超时并且一直在重试

问题：当你运行时 `docker push`，它会超时，并且会继续重试，但没有成功。

原因：这可能是由于缺少权限、推送到错误的存储库或缺乏身份验证所致。

解决方案：要尝试解决此问题，请确保您推送到正确的存储库。运行 `docker login` 以正确进行身份验证。确保您拥有推送到 Amazon ECR 存储库所需的所有权限。

无法VPC从我的 AWS CloudShell VPC环境中访问其中的资源

问题：在使用我的 AWS CloudShell VPC环境VPC时无法访问资源。

原因：您的 AWS CloudShell VPC环境继承了您的VPC网络设置。

解决方案：要解决此问题，请确保VPC已正确设置您的资源访问权限。有关更多信息，请参阅VPC文档 [Connect 您的VPC连接到其他网络以及网络](#) 访问分析器文档 [Network Access Analyzer](#)。您可以通过在 AWS CloudShell VPC环境中的命令 `ip -a` 行提示符下或在VPC控制台页面上运行命令来找到环境正在使用IPv4的地址。

ENI AWS CloudShell 用于我的VPC环境的未清理干净

问题：无法清理我的VPC环境中ENI使用 AWS CloudShell 的。

原因：您的角色未启用 `ec2:DeleteNetworkInterface` 权限。

解决方案：要解决此问题，请确保您的角色已启用 `ec2:DeleteNetworkInterface` 权限，如以下示例脚本所示：

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteNetworkInterface"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/ManagedByCloudShell": ""
    }
  },
  "Resource": "arn:aws:ec2:*:*:network-interface/*"
}
```

仅 `CreateEnvironment` 有权访问VPC环境的用户也可以访问公共 AWS CloudShell 环境

问题：仅限VPC环境访问 `CreateEnvironment` 权限的用户也可以访问公共 AWS CloudShell 环境。

原因：当您仅限制创建VPC环境的CreateEnvironment权限并且已经创建了公共环境时，您将保留对现有公共 CloudShell环境的访问权限，直到使用 Web 用户界面删除该环境。但是，如果您 CloudShell 以前从未使用过，则将无法访问公共环境。

解决方案：要限制对公共 AWS CloudShell 环境的访问，IAM管理员必须先使用限制更新IAM策略，然后用户必须使用 AWS CloudShell Web 用户界面手动删除现有的公共环境。（操作 → 删除 CloudShell 环境）。

证书在中不起作用 CloudShell

问题：当你尝试从 AWS CLI 拨打电话时 CloudShell，你会收到错误消息“内部服务器错误”。

原因：以下是此问题的可能原因：

- 用于刷新凭据的putCredentialsAPI调 CloudShell 用失败。由于缺乏putCredentials操作IAM权限，API呼叫可能会失败。有关更多信息，请参阅 [???](#)。如果您已经拥有putCredentials操作IAM权限，则由于网络问题或操作问题，API呼叫可能会失败 CloudShell。
- 您的凭证已失效，因为 AWS 控制台会话已过期，但您的 CloudShell环境仍在运行。当您的凭证失效时，CloudShell无法拨打任何API电话。

解决方案：如果您已经拥有所需的putCredentials操作IAM权限，请尝试刷新网页。如果问题未得到解决，而您仍然收到错误，请联系 Su [AWS pport](#)。

支持的 AWS 区域 AWS CloudShell

本节介绍支持的 AWS 区域和可选区域列表。AWS CloudShell有关 AWS 服务终端节点和配额的列表 CloudShell，请参阅中的[AWS CloudShell 页面Amazon Web Services 一般参考](#)。

以下是 CloudShell、Docker 和 CloudShell VPC环境支持的 AWS 区域：

- 美国东部 (俄亥俄)
- 美国东部 (弗吉尼亚州北部)
- 美国西部 (加利福尼亚北部)
- 美国西部 (俄勒冈州)
- 非洲 (开普敦)
- Asia Pacific (Hong Kong)
- 亚太地区 (雅加达)
- 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 (米兰)
- 欧洲地区 (巴黎)
- 欧洲地区 (斯德哥尔摩)
- 中东 (巴林)
- 中东 (UAE)
- 南美洲 (圣保罗)

GovCloud 区域

以下是支持的 GovCloud 区域 CloudShell：

- AWS GovCloud（美国东部）
- AWS GovCloud（美国西部）

目前，Docker 和 CloudShell VPC环境在 GovCloud区域中不可用。

的服务配额和限制 AWS CloudShell

本页介绍适用于以下领域的服务限额和限制：

- [持久性存储](#)
- [月度使用情况](#)
- [命令大小](#)
- [并发 Shell](#)
- [Shell 会话](#)
- [网络访问和数据传输](#)
- [系统文件和页面重新加载](#)

持久性存储

使用 AWS CloudShell，您可以免费获得每个 AWS 区域 1 GB 的永久存储空间。永久存储位于您的主目录 (\$HOME) 中，对您来说是私有的。与每个 Shell 会话结束后回收的临时环境资源不同的是，主目录中的数据会在不同会话之间保留。

Note

CloudShell VPC环境没有永久存储。当您的VPC环境超时（20-30 分钟处于非活动状态之后）或删除环境时，\$ HOME 目录将被删除。

如果您停止 AWS CloudShell 在中使用 AWS 区域，则在上次会话结束后，数据将在该区域的永久存储中保留 120 天。120 天后，除非您采取措施，否则您的数据将自动从该地区的持久性存储中删除。您可以通过在 AWS 区域中再次启动 AWS CloudShell 来阻止删除。有关更多信息，请参阅[步骤 2：选择区域 AWS CloudShell、启动并选择外壳](#)。

Note

使用场景

Márcia 过去曾 AWS CloudShell 将文件存储在两个主目录中 AWS 区域：美国东部（弗吉尼亚北部）和欧洲（爱尔兰）。然后，她开始 AWS CloudShell 只在欧洲（爱尔兰）使用，并停止在美国东部（弗吉尼亚北部）推出空壳会议。

在美国东部（弗吉尼亚北部）删除数据的截止日期之前，Márcia 决定再次启动 AWS CloudShell 并选择美国东部（弗吉尼亚北部）区域，以防止其主目录被回收。由于她一直使用欧洲地区（爱尔兰）进行 Shell 会话，因此她在该地区的持久性存储不会受到影响。

每月使用量

你 AWS 区域中的每一个 AWS 账户都有每月的使用配额 AWS CloudShell。该配额汇总了该地区所有 CloudShell IAM 委托人的总使用时间。如果您在达到该区域的月度配额 CloudShell 后尝试访问，则会显示一条消息，解释无法启动 shell 环境的原因。

Note

如果您需要增加每月使用配额，请联系 [Support](#) 并提供以下信息：

- CloudShell 用法区域
- 您的用例。例如，AWS CLI 操作和 Linux 命令执行
- CloudShell 用户数量。例如，5-10
- 您在该地区使用 CloudShell 的最大估计时间
- CloudShell VPC 环境使用情况

我们可以批准将最长估计时间增加到每月 1000 小时，而不是现有的限制 200 小时。

命令大小

命令大小不能超过 65412 个字符。

Note

如果您打算执行超过 65412 个字符的命令，请使用您选择的语言创建脚本，然后从命令行界面执行该脚本。有关可从命令行界面访问的预安装软件范围的更多信息，请参阅 [预安装的软件](#)。要查看如何创建脚本然后从命令行界面执行脚本的示例，请参阅 [教程：AWS CloudShell 入门](#)。

并发 Shell

- 并发 shell：您最多可以为自己的账户在每个 AWS 区域 外壳中同时运行 10 个 shell。

Shell 会话

- 非活动会话：AWS CloudShell 是一个交互式外壳环境，如果您在 20-30 分钟内没有使用键盘或指针与之交互，则外壳会话将结束。正在运行的进程不算作交互。
- 长时间运行的会话：持续运行大约 12 小时的 Shell 会话会自动结束，即使用户在此期间定期与其交互。

网络访问和数据传输

以下限制适用于您的 AWS CloudShell 环境的入站和出站通信：

- 出站：您可以访问公共互联网。
- 入站：您无法访问入站端口。公共 IP 地址不可用。

Warning

通过访问公共互联网，某些用户可能会从 AWS CloudShell 环境中导出数据。我们建议 IAM 管理员通过 IAM 工具管理可信 AWS CloudShell 用户的允许列表。有关如何明确拒绝特定用户访问的信息，请参阅 [AWS CloudShell 使用自定义策略管理允许的操作](#)。

数据传输：对于大文件，上传和下载文件 AWS CloudShell 可能会很慢。或者，您可以使用 Shell 的命令行界面将文件从 Amazon S3 存储桶传输到您的环境。

对系统文件和页面重新加载的限制

- 系统文件：如果您错误地修改了计算环境所需的文件，则在访问或使用该 AWS CloudShell 环境时可能会遇到问题。如果发生这种情况，您可能需要[删除主目录](#)才能重新获得访问权限。
- 重新加载页面：要重新加载 AWS CloudShell 界面，请使用浏览器中的刷新按钮，而不是操作系统的默认快捷键序列。

《AWS CloudShell 用户指南》的文档历史记录

最近的更新

下表介绍了 AWS CloudShell 用户指南 的重要更改。

变更	说明	日期
亚马逊 AWS CloudShell 在某些地区VPC提供支持	增加了对在某些地区创建和使用 AWS CloudShell VPC环境的支持。	2024 年 6 月 13 日
新教程已添加到《AWS CloudShell 用户指南》	新增了两个教程，详细介绍了如何在内部 AWS CloudShell 构建 Docker 容器并将其推送到 Amazon ECR 存储库，以及如何通过部署 Lambda 函数。AWS CDK	2023 年 12 月 27 日
某些区域支持 Docker 容器 AWS CloudShell	某些区域 AWS CloudShell 已添加对 Docker 容器的支持。	2023 年 12 月 27 日
AWS CloudShell 已迁移到现在使用亚马逊 Linux 2023 (AL2023)	AWS CloudShell 现在使用 AL2023 并已从亚马逊 Linux 2 迁移。	2023 年 12 月 4 日
的新AWS区域 AWS CloudShell	AWS CloudShell 现已在以下 AWS 地区正式上市： <ul style="list-style-type: none"> • 美国西部 (加利福尼亚北部) • 非洲 (开普敦) • Asia Pacific (Hong Kong) • 亚太地区 (大阪) • 亚太地区 (首尔) • 亚太地区 (雅加达) • 亚太地区 (新加坡) 	2023 年 6 月 16 日

- 欧洲地区 (巴黎)
- Europe (Stockholm)
- Europe (Milan)
- Middle East (Bahrain)
- 中东 (UAE)

[AWS CloudShell 在 Console Toolbar](#)

CloudShell 在 Console
Toolbar，在控制台的左下角选
择 CloudShell。

2023 年 3 月 28 日

[的新 AWS 区域 AWS CloudShell](#)

AWS CloudShell 现已在以下
AWS 地区推出：

2022 年 10 月 6 日

- 加拿大 (中部)
- 欧洲地区 (伦敦)
- 南美洲 (圣保罗)

[AWS CloudShell 在美国支持 AWS GovCloud](#)

AWS CloudShell 现在在 AWS
GovCloud (美国) 地区支持。

2022 年 6 月 29 日

[安全 FAQs](#)

其他FAQs重点是安全问题。

2022 年 4 月 14 日

[Web 套接字](#)

在网络要求中添加了一节，解
释 CloudShell了该 WebSocket
协议的用法。

2022 年 3 月 21 日

[中的箭头键疑难解答 PowerShell](#)

按照步骤修复按下箭头键时错
误输出字母的问题。

2022 年 2 月 7 日

[Tab 键自动完成](#)

解释如何使用 bash-completion
的新文档，它允许通过按 Tab
键自动完成部分键入的命令或
参数。

2021 年 9 月 24 日

[指定 AWS 区域](#)

有关 AWS 区域 为 AWS CLI
命令指定默认值的文档。

2021 年 5 月 11 日

[格式化版本PDF和 Kindle 版本](#)

修复了表格单元格中的图像大小和文本。

2021 年 3 月 10 日

[AWS CloudShell 在选定 AWS 区域正式上市 \(GA\) 版本](#)

AWS CloudShell 现已在以下 AWS 地区正式上市：

2020 年 12 月 15 日

- 美国东部 (俄亥俄)
- 美国东部 (弗吉尼亚州北部)
- 美国西部 (俄勒冈)
- 亚太地区 (东京)
- 欧洲地区 (爱尔兰)
- 亚太地区 (孟买)
- 亚太地区 (悉尼)
- 欧洲地区 (法兰克福)

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。