aws

用户指南

研究与工程工作室

研究与工程工作室: 用户指南

Table of Contents

概览

> **Important**
>
> 此版本的用户指南涵盖了 Research and Engineering Studio 的 2024.08 版本。 AWS有关当前版本，请参阅《AWS 用户指南》中的研究与工程工作室。

Research and Engineering Studio (RES) 是一款 AWS 受支持的开源产品，它使 IT 管理员能够为科学家和工程师提供一个用于运行技术计算工作负载的 Web 门户 AWS。RES 为用户提供单一管理平台，让用户可以启动安全的虚拟桌面，以进行科学研究、产品设计、工程模拟或数据分析工作负载。用户可以使用其现有的公司凭证连接到 RES 门户，并处理个人或协作项目。

管理员可以创建名为项目的虚拟协作空间，供一组特定的用户访问共享资源并进行协作。管理员可以构建自己的应用程序软件堆栈 (AMIs)，允许 RES 用户启动 Windows 或 Linux 虚拟桌面，并允许通过共享文件系统访问项目数据。管理员可以分配软件堆栈和文件系统，并限制只有这些项目用户才能访问。管理员可以使用内置的遥测来监控环境使用情况并对用户问题进行故障排除。他们还可以为单个项目设定预算，以防止过度消耗资源。由于该产品是开源的，因此客户还可以根据自己的需求自定义 RES 门户的用户体验。

RES 不收取额外费用，您只需为运行应用程序所需的 AWS 资源付费。

本指南概述了 Research and Engineering Studio 的参考架构和组件、部署规划注意事项以及将 RES 部署到 Amazon Web Services (AWS) 云的配置步骤。 AWS

功能和优势

上的研究与工程工作室 AWS 提供以下功能：

基于网络的用户界面

RES 提供了一个基于 Web 的门户，管理员、研究人员和工程师可以使用该门户访问和管理他们的研究和工程工作空间。科学家和工程师无需具备 AWS 账户 或云专业知识即可使用 RES。

基于项目的配置

使用项目为一组任务或活动定义访问权限、分配资源和管理预算。为项目分配特定的软件堆栈（操作系统和经批准的应用程序）和存储资源，以确保一致性和合规性。监控和管理每个项目的支出。

协作工具

科学家和工程师可以邀请其项目的其他成员与他们合作，设置他们希望这些同事拥有的权限级别。这些人可以登录 RES 以连接到这些桌面。

与现有身份管理基础设施集成

与您现有的身份管理和目录服务基础架构集成，使用用户的现有企业身份与 RES 门户建立连接，并使用现有用户和群组成员资格为项目分配权限。

永久存储和对共享数据的访问

要为用户提供跨虚拟桌面会话访问共享数据的权限，请连接到您现有的文件系统或在 RES 中创建新的文件系统。支持的存储服务包括适用于 Linux 桌面的亚马逊 Elastic File System 和 FSx 适用于 Windows 和 Linux 桌面的亚马逊 NetApp ONTAP 版。

监控和报告

使用分析仪表板监控实例类型、软件堆栈和操作系统类型的资源使用情况。控制面板还提供了按项目分列的资源使用情况细目以供报告。

预算和成本管理

链接 AWS Budgets 到您的 RES 项目以监控每个项目的成本。如果您超出预算，则可以限制 VDI 会话的启动。

概念和定义

本节介绍关键概念并定义了本产品特有的术语：

文件浏览器

文件浏览器是 RES 用户界面的一部分，当前登录的用户可以在其中查看其文件系统。

文件系统

文件系统充当项目数据（通常称为数据集）的容器。它提供了项目范围内的存储解决方案，并改善了协作和数据访问控制。

全局管理员

有权访问在 RES 环境中共享的 RES 资源的管理委托人。范围和权限跨越多个项目。他们可以创建或修改项目并分配项目所有者。他们可以向项目所有者和项目成员委派或分配权限。有时，同一个人担任 RES 管理员，具体取决于组织的规模。

Project

项目是应用程序中的一个逻辑分区，它充当数据和计算资源的独特边界，可确保对数据流的监管，并防止数据和 VDI 主机在项目之间共享。

基于项目的权限

基于项目的权限描述了在可能存在多个项目的系统中，数据和 VDI 主机的逻辑分区。用户对项目内数据和 VDI 主机的访问权限由其关联的角色决定。必须为用户分配他们需要访问的每个项目的访问权限（或项目成员资格）。否则，当用户未被授予成员资格 VDIs 时，他们将无法访问项目数据。

项目成员

RES 资源（VDI、存储等）的最终用户。范围和权限仅限于分配给他们的项目。他们不能委托或分配任何权限。

项目拥有者

对特定项目具有访问权限和所有权的行政代表。范围和权限仅限于他们拥有的项目。他们可以为其拥有的项目的项目成员分配权限。

软件堆栈

软件堆栈是亚马逊系统映像 (AMI)，其中包含基于用户选择为其 VDI 主机配置的任何操作系统的特定元数据。

VDI 主机

虚拟桌面实例 (VDI) 主机允许项目成员访问项目特定的数据和计算环境，从而确保工作空间的安全和隔离。

有关 AWS 术语的一般参考，请参阅《AWS 通用参考》中的AWS 词汇表。

架构概述

本节提供与此产品一起部署的组件的架构图。

架构图

使用默认参数部署此产品将在中部署以下组件。 AWS 账户

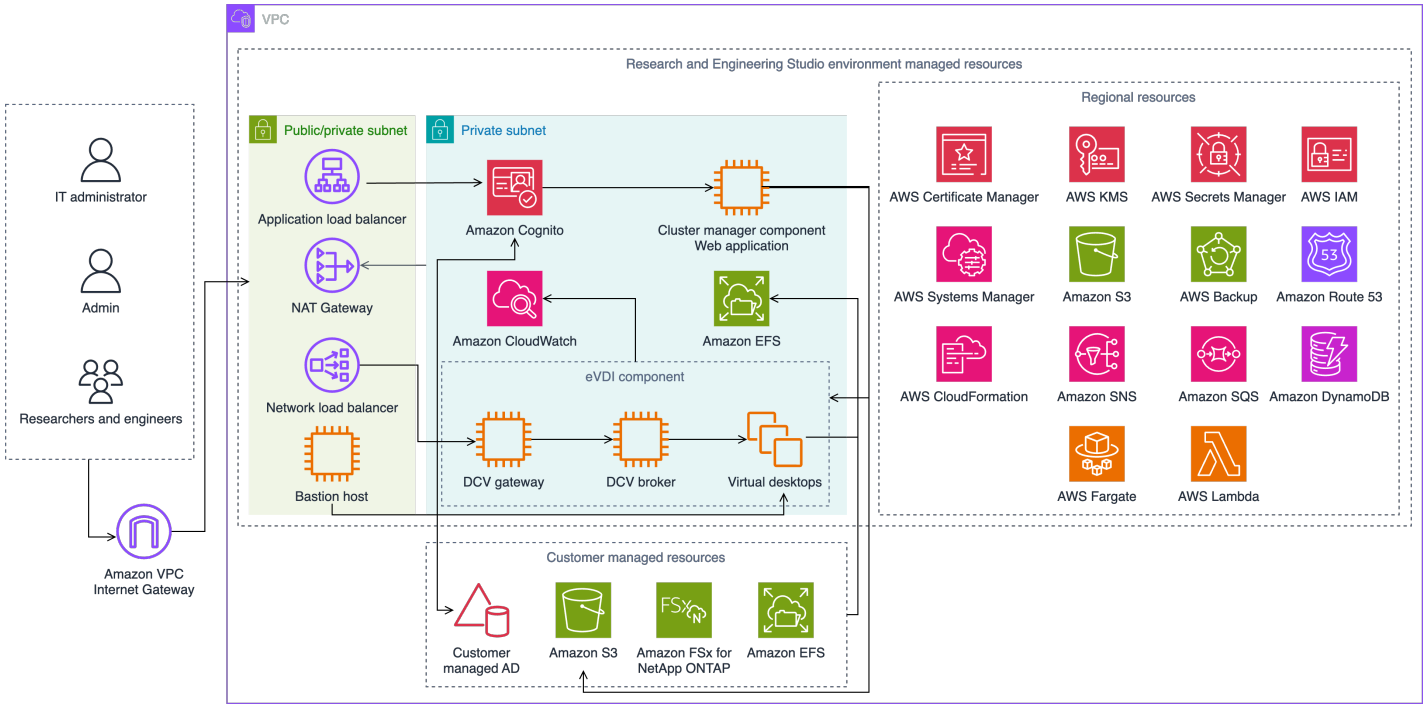


图 1： AWS 建筑研究与工程工作室

> **Note**
>
> AWS CloudFormation 资源是从 AWS Cloud Development Kit (AWS CDK) 构造中创建的。

使用 AWS CloudFormation 模板部署的产品组件的高级流程如下：

1. RES 为门户网站安装组件以及：
   a. 为交互式工作负载设计虚拟桌面 (eVDi) 组件
   b. 指标组件

      亚马逊从 eVDi 组件 CloudWatch 接收指标。

c. 堡垒主机组件

管理员可以使用 SSH 连接到堡垒主机组件来管理底层基础架构。

2. RES 在 NAT 网关后面的私有子网中安装组件。管理员通过 Application Load Balancer (ALB) 或 Bastion Host 组件访问私有子网。
3. 亚马逊 DynamoDB 存储环境配置。
4. AWS Certificate Manager (ACM) 为 Application Load Balancer (ALB) 生成并存储公共证书。

> **Note**
>
> 我们建议 AWS Certificate Manager 使用为您的域生成可信证书。

5. Amazon Elastic File System (EFS) 托管安装在所有适用的基础设施主机和 eVDi Linux 会话上的默认`/home`文件系统。
6. RES 使用 Amazon Cognito 在其中创建名为 clusteradmin 的初始引导用户，并将临时证书发送到安装期间提供的电子邮件地址。群集管理员必须在首次登录时更改密码。
7. Amazon Cognito 可与贵组织的活动目录和用户身份集成，用于权限管理。
8. 安全区域允许管理员根据权限限制对产品内特定组件的访问权限。

AWS 本产品中的服务

AWS 服务	描述
Amazon Elastic Compute Cloud	核心。提供底层计算服务，用他们选择的操作系统和软件堆栈创建虚拟桌面。
Elastic Load Balancing	核心。堡垒、集群管理器和 VDI 主机是在负载均衡器后面的 Auto Scaling 组中创建的。ELB 在 RES 主机上平衡来自门户网站的流量。
Amazon Virtual Private Cloud	核心。所有核心产品组件都是在您的 VPC 中创建的。

AWS 服务	描述
Amazon Cognito	核心。管理用户身份和身份验证。Active Directory 用户会映射到 Amazon Cognito 用户和群组，以验证访问级别。
Amazon Elastic File System	核心。为/home文件浏览器和 VDI 主机以及共享的外部文件系统提供文件系统。
Amazon DynamoDB	核心。存储配置数据，例如用户、群组、项目、文件系统和组件设置。
AWS Systems Manager (系统管理员)	核心。存储用于执行 VDI 会话管理命令的文档。
AWS Lambda	核心。支持产品功能，例如更新 DynamoDB 表中的设置、启动 Active Directory 同步工作流程和更新前缀列表。
Amazon CloudWatch	支持。为所有 Amazon EC2 主机和 Lambda 函数提供指标和活动日志。
Amazon Simple Storage Service	支持。存储用于主机引导和配置的应用程序二进制文件。
AWS Key Management Service	支持。用于对亚马逊 SQS 队列、DynamoDB 表和亚马逊 SNS 主题进行静态加密。
AWS Secrets Manager	支持。将服务帐户凭据存储在 Active Directory 中，并为 VDIs存储自签名证书
AWS CloudFormation	支持。为产品提供部署机制。
AWS Identity and Access Management	支持。限制主机的访问级别。
Amazon Route 53	支持。创建私有托管区域以解析内部负载均衡器和堡垒主机域名。
Amazon Simple Queue Service	支持。创建任务队列以支持异步执行。

AWS 服务	描述
Amazon Simple Notification Service	支持。支持 VDI 组件（例如控制器和主机）之间的发布订阅者模式。
AWS Fargate	支持。使用 Fargate 任务安装、更新和删除环境。
Amazon FSx 文件网关	可选。提供外部共享文件系统。
FSx 适用于 NetApp ONTAP 的亚马逊	可选。提供外部共享文件系统。
AWS Certificate Manager	可选。为您的自定义域生成可信证书。
AWS Backup	可选。为 Amazon EC2 主机、文件系统和 DynamoDB 提供备份功能。

创建演示环境

请按照本节中的步骤试用 Research and Engineering Studio AWS。此演示使用演AWS 示环境堆栈模板上的 Research and Engineering Studio 部署具有最少参数集的非生产环境。它使用 Keycloak 服务器进行 SSO。

请注意，部署堆栈后，必须按照部署后步骤以下步骤在环境中设置用户，然后才能登录。

创建一键演示堆栈

该 AWS CloudFormation 堆栈创建了研究与工程工作室所需的所有组件。

部署时间：大约 90 分钟

先决条件

主题

- AWS 账户 使用管理员用户创建
- 创建 Amazon EC2 SSH 密钥对
- 提高服务配额

AWS 账户 使用管理员用户创建

您必须 AWS 账户 拥有管理员用户：

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

创建 Amazon EC2 SSH 密钥对

如果您没有 Amazon EC2 SSH 密钥对，则需要创建一个密钥对。有关更多信息，请参阅亚马逊 EC2 用户指南 EC2中的使用亚马逊创建密钥对。

提高服务配额

我们建议增加以下各项的服务配额：

- 亚马逊 VPC
  - 将每个 NAT 网关的弹性 IP 地址配额从五个增加到八个
  - 将每个可用区的 NAT 网关从五个增加到十个
- Amazon EC2
  - 将 EC2-VPC 弹性 IPs 从五个增加到十个

您的 AWS 账户对每项 AWS 服务都有默认配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。有关更多信息，请参阅 the section called “本产品中的 AWS 服务配额”。

创建资源和输入参数

1. 登录 AWS Management Console 并在 https://console.aws.amazon.com/cloudformation 上打开 AWS CloudFormation 控制台。

   > **Note**
   >
   > 确保您使用的是管理员帐户。

2. 在控制台中启动模板。
3. 在“参数”下，查看此产品模板的参数并根据需要进行修改。

参数	默认值	描述
EnvironmentName	*<res-demo>*	以 res-开头且不超过 11 个字符的 RES 环境的唯一名称。
AdministratorEmail		完成产品设置的用户的电子邮件地址。如果 Active Directory 单点登录集成失败，则此用户还可以充当破碎玻璃用户。

参数	默认值	描述
KeyPair		用于连接基础架构主机的密钥 pair。
客户端 IPCidr	<0.0.0.0/0>	IP 地址过滤器，用于限制与系统的连接。您可以在部署 ClientIpCidr 后进行更新。
InboundPrefixList		（可选）提供托管前缀列表，IPs 允许直接访问 Web UI 和 SSH 进入堡垒主机。

部署后步骤

1. 重置用户密码 `AWS Directory Service` — 演示堆栈创建了四个用户，其用户名可供您使用：`admin1`、`user1admin2`、和`user2`。

   a. 前往 Directory Service 控制台。

   b. 为您的环境选择目录 ID。你可以从`<StackName>*DirectoryService*`堆栈的输出中获取目录 ID。

   c. 从右上角的 “操作” 下拉菜单中，选择 “重置用户密码”。

   d. 对于您要使用的所有用户，输入用户名并键入您想要的密码，然后选择 “重置密码”。

2. 重置用户密码后，您需要等待 Research and Engineering Studio 同步环境中的用户。Research and Engineering Studio 每小时在 xx.00 同步用户。您可以等待这种情况发生，也可以按照中已将用户添加到 Active Directory 中，但在列出的步骤立即同步用户。

您的部署现已准备就绪。使用 EnvironmentUrl 您在电子邮件中收到的访问界面，或者也可以从已部署堆栈的输出中获取相同的 URL。现在，您可以使用在 Active Directory 中重置密码的用户名和密码登录研究与工程工作室环境。

规划您的部署

费用

上 AWS 的 Research and Engineering Studio 不收取额外费用，您只需为运行应用程序所需的 AWS 资源付费。有关更多信息，请参阅 AWS 本产品中的服务。

> **Note**
>
> 运行本产品时使用的 AWS 服务费用由您承担。
> 我们建议通过创建预算AWS Cost Explorer来帮助管理成本。价格可能会发生变化。有关完整详情，请参阅本产品中使用的每项 AWS 服务的定价网页。

安全性

当您在 AWS 基础架构上构建系统时，安全责任由您和共同承担 AWS。这种分担责任模式减轻了您的 AWS 运营负担，因为您可以操作、管理和控制包括主机操作系统、虚拟化层和服务运行设施的物理安全在内的组件。有关 AWS 安全的更多信息，请访问AWS Cloud 安全。

IAM 角色

AWS Identity and Access Management (IAM) 角色允许客户向上的服务和用户分配精细的访问策略和权限。 AWS Cloud该产品创建 IAM 角色来授予产品的 AWS Lambda 功能和 Amazon EC2 实例创建区域资源的访问权限。

RES 支持 IAM 中基于身份的策略。部署后，RES 会创建策略来定义管理员的权限和访问权限。实施产品的管理员在与 RES 集成的现有客户 Active Directory 中创建和管理最终用户和项目负责人。有关更多信息，请参阅 Identity and A ccess Managem AWS ent 用户指南中的创建 IAM 策略。

贵组织的管理员可以使用活动目录管理用户访问权限。当最终用户访问 RES 用户界面时，RES 会使用 Amazon Cognito 进行身份验证。

安全组

在本产品中创建的安全组旨在控制和隔离 Lambda 函数、 EC2 实例、文件系统 CSR 实例和远程 VPN 终端节点之间的网络流量。我们建议您在部署产品后查看安全组并根据需要进一步限制访问权限。

数据加密

默认情况下，Research and Engineering Studio AWS （RES）使用RES拥有的密钥对静态和传输中的客户数据进行加密。部署 RES 时，可以指定 AWS KMS key。RES 使用您的证书授予密钥访问权限。如果您提供的是客户所有和管理的 AWS KMS key，则将使用该密钥对客户静态数据进行加密。

RES 使用 SSL/TLS 对传输中的客户数据进行加密。我们需要 TLS 1.2，但建议使用 TLS 1.3。

限额

服务限额（也称为限制）是 AWS 账户使用的服务资源或操作的最大数量。

本产品中的 AWS 服务配额

请确保您有足够的配额来使用本产品中实施的每项服务。有关更多信息，请参阅AWS 服务配额。

对于此产品，我们建议提高以下服务的配额：

- Amazon Virtual Private Cloud
- Amazon EC2

要请求提高配额，请参阅《Service Quotas 用户指南》中的请求提高配额。如果限额在服务限额中尚不可用，请使用提高限制表格。

AWS CloudFormation 配额

您 AWS 账户 有 AWS CloudFormation 配额，在该产品中启动堆栈时应注意这些配额。通过了解这些配额，您可以避免限制错误，从而使您无法成功部署此产品。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的AWS CloudFormation 配额。

规划恢复能力

该产品部署了默认基础设施，该基础设施具有最小数量和大小的 Amazon EC2 实例来运行系统。为了提高大规模生产环境的弹性，我们建议在基础架构的 Auto Scaling 组 (ASG) 中增加默认的最低容量设置。将值从一个实例增加到两个实例可以获得多个可用区 (AZ) 的好处，并缩短在数据意外丢失时恢复系统功能的时间。

ASG 设置可以在亚马逊 EC2 控制台中自定义，网址为。https://console.aws.amazon.com/ec2/ ASGs 默认情况下，产品会创建四个，每个名称都以`-asg`。您可以将最小值和所需值更改为适合您的生产

环境的数量。选择要修改的群组，然后选择操作和编辑。有关更多信息 ASGs，请参阅 Amazon Auto Scaling 用户指南中的扩展 A EC2 uto Scaling 组的大小。

支持 AWS 区域

本产品使用的服务目前并非全部可用 AWS 区域。您必须在所有服务都可用 AWS 区域 的地方启动此产品。有关按地区划分的最新 AWS 服务可用性，请参阅AWS 区域所有服务列表。

以下内容支持上 AWS 的 “研究与工程工作室” AWS 区域：

区域名称	区域	2024.06 及更早版本	2024.08 版本
美国东部（弗吉尼亚州北部）	us-east-1	是	是
美国东部（俄亥俄州）	us-east-2	是	是
美国西部（加利福尼亚北部）	us-west-1	是	是
美国西部（俄勒冈州）	us-west-2	是	是
亚太地区（东京）	ap-northeast-1	是	是
亚太地区（首尔）	ap-northeast-2	是	是
亚太地区（孟买）	ap-south-1	是	是
亚太地区（新加坡）	ap-southeast-1	是	是
亚太地区（悉尼）	ap-southeast-2	是	是
加拿大（中部）	ca-central-1	是	是
欧洲（法兰克福）	eu-central-1	是	是
欧洲（米兰）	eu-south-1	是	是
欧洲地区（爱尔兰）	eu-west-1	是	是

区域名称	区域	2024.06 及更早版本	2024.08 版本
欧洲地区（伦敦）	eu-west-2	是	是
欧洲（巴黎）	eu-west-3	是	是
欧洲地区（斯德哥尔摩）	eu-north-1	否	是
以色列（特拉维夫）	il-central-1	是	是
AWS GovCloud （美国西部）	us-gov-west-1	是	否

部署产品

> **Note**
>
> 该产品使用AWS CloudFormation 模板和堆栈来自动部署。这些 CloudFormation模板描述了本产品中包含的 AWS 资源及其属性。 CloudFormation 堆栈提供模板中描述的资源。

在发布产品之前，请查看本指南前面讨论的成本、架构、网络安全和其他注意事项。

主题

先决条件

主题

AWS 账户 使用管理员用户创建

您必须 AWS 账户 拥有管理员用户：

1. 打开https://portal.aws.amazon.com/billing/注册。

2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

创建 Amazon EC2 SSH 密钥对

如果您没有 Amazon EC2 SSH 密钥对，则需要创建一个密钥对。有关更多信息，请参阅亚马逊 EC2 用户指南 EC2中的使用亚马逊创建密钥对。

提高服务配额

我们建议增加以下各项的服务配额：

- Amazon VPC
  - 将每个 NAT 网关的弹性 IP 地址配额从五个增加到八个
  - 将每个可用区的 NAT 网关从五个增加到十个
- Amazon EC2
  - 将 EC2-VPC 弹性 IPs 从五增加到十

您的 AWS 账户对每项 AWS 服务都有默认配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。有关更多信息，请参阅 the section called “本产品中的 AWS 服务配额”。

创建公共领域（可选）

我们建议为产品使用自定义域名，以便获得用户友好的网址。您需要使用 Amazon Route 53 或其他提供商注册域名，然后使用为该域导入证书 AWS Certificate Manager。如果您已经拥有公共域名和证书，则可以跳过此步骤。

1. 按照说明在 Route 53 上注册域名。您应该会收到一封确认电子邮件。
2. 检索您的域的托管区域。这是由 Route53 自动创建的。

   a. 打开 Route53 控制台。

b. 从左侧导航栏中选择托管区域。

c. 打开为您的域名创建的托管区域，然后复制托管区域 ID。

3. 打开 AWS Certificate Manager 并按照以下步骤申请域证书。确保您位于计划部署解决方案的区域。
4. 从导航栏中选择 “列出证书”，然后找到您的证书申请。该请求应该处于待处理状态。
5. 选择您的证书 ID 以打开请求。
6. 从 “域” 部分中，选择 “在 Route53 中创建记录”。处理请求大约需要十分钟。
7. 证书颁发后，从证书状态部分复制 ARN。

创建域名（GovCloud 仅限）

如果您在 AWS GovCloud （美国西部）地区进行部署，则需要完成这些必备步骤。

1. 在创建公共托管域的商业分区 AWS 账户中部署证书 AWS CloudFormation 堆栈。
2. 从 “证书 CloudFormation 输出” 中，找到并记下`CertificateARN`和`PrivateKeySecretARN`。
3. 在 GovCloud 分区帐户中，使用`CertificateARN`输出值创建一个密钥。记下新的密钥 ARN，并在该密钥中添加两个标签，这样`vdc-gateway`就可以访问密钥值了：

   a. res: ModuleName = virtual-desktop-controller

   b. res: EnvironmentName = [环境名称]（这可能是 res-demo。）
4. 在 GovCloud 分区帐户中，使用`PrivateKeySecretArn`输出值创建一个密钥。记下新的密钥 ARN，并在该密钥中添加两个标签，这样`vdc-gateway`就可以访问密钥值了：

   a. res: ModuleName = virtual-desktop-controller

   b. res: EnvironmentName = [环境名称]（这可能是 res-demo。）

提供外部资源

Research and Engineering Studio 在部署时 AWS 预计会有以下外部资源。

- 网络（VPC、公有子网和私有子网）

  在这里，您将运行用于托管 RES 环境、Active Directory (AD) 和共享存储空间的 EC2 实例。
- 存储（亚马逊 EFS）

存储卷包含虚拟桌面基础架构 (VDI) 所需的文件和数据。

- 目录服务 (AWS Directory Service for Microsoft Active Directory)

  目录服务对 RES 环境的用户进行身份验证。

- 包含服务账号密码的密钥

  Research and Engineering Studio 使用AWS Secrets Manager访问你提供的机密，包括服务帐户密码。

> **Tip**
>
> 如果您正在部署演示环境，但没有这些外部资源可用，则可以使用 AWS 高性能计算配方来生成外部资源。要在您的账户中部署资源创建外部资源，请参阅以下部分。
> 要在 AWS GovCloud （美国西部）区域进行演示部署，您需要完成中的创建域名（GovCloud 仅限）必备步骤。

在您的环境中配置 LDAPS（可选）

如果您计划在您的环境中使用 LDAPS 通信，则必须完成以下步骤来创建证书并将其附加到 AWS Managed Microsoft AD (AD) 域控制器，以提供 AD 和 RES 之间的通信。

1. 按照如何为您启用服务器端 LDAPS 中提供的步骤进行操作。 AWS Managed Microsoft AD如果您已经启用 LDAPS，则可以跳过此步骤。
2. 确认已在 AD 上配置 LDAPS 后，导出 AD 证书：
   a. 前往您的活动目录服务器。
   b. 以管理员 PowerShell 身份打开。
   c. 运行`certmgr.msc`打开证书列表。
   d. 首先打开受信任的根证书颁发机构，然后打开证书，打开证书列表。
   e. 选择并按住（或右键单击）与 AD 服务器同名的证书，然后选择 “所有任务”，然后选择 “导出”。
   f. 选择 Base-64 编码的 X.509 (.C ER)，然后选择 “下一步”。
   g. 选择一个目录，然后选择 “下一步”。
3. 在以下位置创建密钥 AWS Secrets Manager：

在 Secrets Manager 中创建 Secret 时，在 secret type（密钥类型）下选择 Other type of secrets（其他类型密钥）并将 PEM 编码的凭证粘贴到 Plaintext（明文）字段中。

4. 记下创建的 ARN 并将其作为`DomainTLSCertificateSecretARN`参数输入。the section called “第 1 步：启动产品”

配置私有 VPC（可选）

在隔离的 VPC 中部署 Research and Engineering Studio 可增强安全性，以满足组织的合规和治理要求。但是，标准的 RES 部署依赖于互联网访问来安装依赖关系。要在私有 VPC 中安装 RES，您需要满足以下先决条件：

主题

准备 Amazon 机器映像 (AMIs)

1. 下载依赖关系。要在隔离的 VPC 中部署，RES 基础设施需要在没有公共互联网访问权限的情况下提供依赖关系。
2. 创建具有 Amazon S3 只读访问权限和可信身份的 IAM 角色，名为 Amazon EC2。
   a. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
   b. 在角色中，选择创建角色。
   c. 在选择可信实体页面：
      - 在 “可信实体类型” 下，选择 AWS 服务。
      - 对于 “服务” 或 “用例” 下的 “用例”，选择EC2并选择 “下一步”。
   d. 在 “添加权限” 上，选择以下权限策略，然后选择 “下一步”：
      - 亚马逊 3 ReadOnlyAccess
      - Amazon SSMManaged InstanceCore
      - EC2InstanceProfileForImageBuilder

e. 添加角色名称和描述，然后选择创建角色。

3. 创建 EC2 镜像生成器组件：

a. 打开 EC2 Image Builder 控制台，网址为https://console.aws.amazon.com/imagebuilder。

b. 在 “已保存的资源” 下，选择 “组件”，然后选择 “创建组件”。

c. 在创建组件页面上，输入以下详细信息：

- 对于组件类型，选择构建。
- 要了解组件详情，请选择：

参数	用户条目
镜像操作系统 (OS)	Linux
兼容的操作系统版本	Amazon Linux 2
组件名称	选择一个名字，例如：*<research-and-engineering-studio-infrastructure>*
组件版本	我们建议从 1.0.0 开始。
描述	可选的用户条目。

d. 在 “创建组件” 页面上，选择 “定义文档内容”。

i. 在输入定义文档内容之前，需要一个 tar.gz 文件的文件 URI。将 RES 提供的 tar.gz 文件上传到亚马逊 S3 存储桶，然后从存储桶属性中复制该文件的 URI。

ii. 输入以下信息：

> **Note**
>
> `AddEnvironmentVariables`是可选的，如果您不需要在基础架构主机中使用自定义环境变量，则可以将其删除。
> 如果您正在设置`http_proxy`和 `https_proxy`环境变量，则需要使用这些`no_proxy`参数来防止实例使用代理来查询本地主机、实例元数据 IP 地址和支持 VPC 终端节点的服务。

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may
 not use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
```

```
            commands:
                - 'cd /root/bootstrap/res_dependencies'
                - 'tar -xf res_dependencies.tar.gz'
                - 'cd all_dependencies'
                - '/bin/bash install.sh'
        - name: AddEnvironmentVariables
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                - |
                  echo -e "
                  http_proxy=http://<ip>:<port>
                  https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com
                  " > /etc/environment
```

e. 选择创建组件。

4. 创建 Image Builder 图片配方。

a. 在创建食谱页面上，输入以下内容：

Section	参数	用户条目
食谱详情	名称	输入适当的名称，例如 res-recipe-linux-x 86。
	版本	输入一个版本，通常从 1.0.0 开始。
	描述	添加可选描述。
基础图片	选择图片	选择托管映像。
	OS	Amazon Linux
	图像来源	快速入门（亚马逊管理）
	映像名称	亚马逊 Linux 2 x86
	自动版本控制选项	使用最新的可用操作系统版本。
实例配置	–	将所有内容保持在默认设置中，并确保未选中 “在管道执行后移除 SSM 代理”。
工作目录	工作目录路径	/root/bootstrap/res_依赖关系
组成部分	构建组件	搜索并选择以下内容： • 亚马逊管理：-2-linux aws-cli-version • 亚马逊管理： amazon-cloudwatch-agent-linux

Section	参数	用户条目
		• 归您所有：之前创建的 Amazon EC2 组件。在字段 AWS 区域 中输入您的 AWS 账户 身份证和当前身份。
	测试组件	搜索并选择： • 亚马逊管理： simple-boot-test-linux

b. 选择创建配方。

5. 创建 Image Builder 基础架构配置。

a. 在 “保存的资源” 下，选择基础架构配置。

b. 选择创建基础设施配置。

c. 在创建基础架构配置页面上，输入以下内容：

Section	参数	用户条目
一般性问题	名称	输入适当的名称，例如 res-infra-linux-x 86。
	描述	添加可选描述。
	IAM 角色	选择之前创建的 IAM 角色。
AWS 基础设施	实例类型	选择 t3.medium。
	VPC、子网和安全组	选择一个允许互联网访问和访问 Amazon S3 存储桶的选项。如果您需要创建安全组，则可以使用以下输入从 Amazon EC2 控制台创建一个安全组：

Section	参数	用户条目

		• VPC：选择用于基础设施配置的同一 VPC。此 VPC 必须可以访问互联网。
		• 入站规则：
		  • 类型：SSH
		  • Source：Custom
		  • CIDR 区块：0.0.0.0/0

d. 选择创建基础设施配置。

6. 创建新的 EC2 Image Builder 管道：

a. 转到图像管道，然后选择创建图像管道。

b. 在指定管道详细信息页面上，输入以下内容并选择下一步：

- 管道名称和可选描述
- 对于生成计划，请设置计划，或者如果您想手动启动 AMI 烘焙流程，请选择手动。

c. 在 “选择食谱” 页面上，选择 “使用现有食谱”，然后输入之前创建的食谱名称。选择下一步。

d. 在 “定义图像处理” 页面上，选择默认工作流程，然后选择 “下一步”。

e. 在定义基础架构配置页面上，选择使用现有基础设施配置，然后输入先前创建的基础架构配置的名称。选择下一步。

f. 在 “定义分发设置” 页面上，请考虑以下内容进行选择：

- 输出映像必须与已部署的 RES 环境位于同一区域，这样 RES 才能从中正确启动基础设施主机实例。使用服务默认值，将在使用 Image Builder 服务的区域创建输出 EC2图像。
- 如果要在多个区域部署 RES，可以选择创建新的分布设置并在那里添加更多区域。

g. 查看您的选择并选择创建管道。

7. 运行 EC2 Image Builder 管道：

a. 在图像管道中，找到并选择您创建的管道。

b. 选择 “操作”，然后选择 “运行管道”。

该管道可能需要大约 45 分钟到一个小时才能创建 AMI 映像。

8. 记下生成的 AMI 的 AMI ID，并将其用作中 InfrastructureHost AMI 参数的输入the section called “第 1 步：启动产品”。

设置 VPC 终端节点

要部署 RES 并启动虚拟桌面， AWS 服务 需要访问您的私有子网。您必须设置 VPC 终端节点以提供所需的访问权限，并且需要对每个终端节点重复这些步骤。

1. 如果之前未配置过终端节点，请按照AWS 服务 使用接口 VPC 终端节点访问中提供的说明进行操作。
2. 在两个可用区中各选择一个私有子网。

AWS 服务	服务名称
Application Auto Scaling	com.amazonaws。*region*. 应用程序自动缩放
AWS CloudFormation	com.amazonaws。*region*.cloudfor
Amazon CloudWatch	com.amazonaws。*region*. 监控
Amazon CloudWatch 日志	com.amazonaws。*region*.logs
Amazon DynamoDB	com.amazonaws。*region*.dynamodb（需要网关终端节点）
Amazon EC2	com.amazonaws。*region*.ec2
Amazon ECR	com.amazonaws。*region*.ecr.api
	com.amazonaws。*region*.ecr.dkr
Amazon Elastic File System	com.amazonaws。*region*.elasticfilesyste
Elastic Load Balancing	com.amazonaws。*region*.elasticload bal
Amazon EventBridge	com.amazonaws。*region*. 事件
Amazon FSx	com.amazonaws。*region*.fsx

AWS 服务	服务名称
AWS Key Management Service	com.amazonaws。 *region*.kms
Amazon Kinesis Data Streams	com.amazonaws。 *region*.kinesis-streams
Amazon S3	com.amazonaws。 *region*.s3（需要在 RES 中默认创建的网关终端节点。）
AWS Secrets Manager	com.amazonaws。 *region*.secretsManag
Amazon SES	com.amazonaws。 *region*.email-smtp（以下可用区不支持：use-1-az2、use1-az3、use1-az5、usw1-az2、usw2-az4、apne2-az4、cac1-az3 和 cac1-az4。）
AWS Security Token Service	com.amazonaws。 *region*.sts
Amazon SNS	com.amazonaws。 *region*.sns
Amazon SQS	com.amazonaws。 *region*.sqs
AWS Systems Manager	com.amazonaws。 *region*.ec2messages
	com.amazonaws。 *region*.ssm
	com.amazonaws。 *region*.ssmmessages

在没有 VPC 终端节点的情况下连接到服务

要与不支持 VPC 终端节点的服务集成，您可以在 VPC 的公有子网中设置代理服务器。使用 Identity Center 作为 AWS 身份提供商，按照以下步骤创建具有研究与工程工作室部署所需的最低访问权限的代理服务器。

1. 在您将用于 RES 部署的 VPC 的公有子网中启动一个 Linux 实例。

   - Linux 系列 — 亚马逊 Linux 2 或亚马逊 Linux 3
   - 架构 — x86
   - 实例类型 — t2.micro 或更高版本
   - 安全组 — 从 0.0.0.0/0 开始的端口 3128 上的 TCP

2. 连接到实例以设置代理服务器。

   a. 打开 http 连接。
   b. 允许从所有相关子网连接到以下域：

      - .amazonaws.com（适用于通用服务） AWS
      - .amazoncognito.com（适用于亚马逊 Cognito）
      - .awsapps.com（用于身份中心）
      - .signin.aws（用于身份中心）
      - 。 amazonaws-us-gov.com（适用于 Gov Cloud）

   c. 拒绝所有其他连接。
   d. 激活并启动代理服务器。
   e. 记下代理服务器监听的端口。
3. 配置您的路由表以允许访问代理服务器。

   a. 转到您的 VPC 控制台，确定您将用于基础设施主机和 VDI 主机的子网的路由表。
   b. 编辑路由表以允许所有传入连接转到在前面步骤中创建的代理服务器实例。
   c. 对要用于 Inf VDIs rastructure/ 的所有子网（无法访问互联网）的路由表执行此操作。
4. 修改代理服务器 EC2 实例的安全组，并确保它允许在代理服务器侦听的端口上进行入站 TCP 连接。

设置私有 VPC 部署参数

在中the section called “第 1 步：启动产品”，您需要在 AWS CloudFormation 模板中输入某些参数。请务必按照说明设置以下参数，以便成功部署到您刚刚配置的私有 VPC 中。

参数	输入
InfrastructureHostAMI	使用中创建的基础设施 AMI ID the section called “准备 Amazon 机器映像 (AMIs)”。
IsLoadBalancerInternetFacing	设置为 false。
LoadBalancerSubnets	选择无法访问互联网的私有子网。
InfrastructureHostSubnets	选择无法访问互联网的私有子网。

参数	输入
VdiSubnets	选择无法访问互联网的私有子网。
ClientIP	您可以选择您的 VPC CIDR 以允许所有 VPC IP 地址进行访问。

创建外部资源

此 CloudFormation 堆栈创建联网、存储、活动目录和域证书（ PortalDomainName 如果提供了 ）。您必须拥有这些外部资源才能部署产品。

您可以在部署之前下载配方模板。

部署时间：大约 40-90 分钟

1. 登录 AWS Management Console 并在 https://console.aws.amazon.com/cloudformation 上打开 AWS CloudFormation 控制台。

   > **Note**
   >
   > 确保您使用的是管理员帐户。

2. 在控制台中启动模板。

   如果您要在 AWS GovCloud （美国西部）地区进行部署，请在 GovCloud 分区账户中启动模板。

3. 输入模板参数：

参数	默认值	描述
DomainName	`corp.res.com`	用于活动目录的域。默认值是在设置引导用户的LDIF文件中提供的。如果您想使用默认用户，请将该值保留为默认值。要更改该值，请更新并提供一个单独的LDIF文件。这

参数	默认值	描述
		不需要与用于活动目录的域相匹配。
SubDomain （GovCloud 仅限）		对于商业区域，此参数是可选的，但对于 GovCloud 区域则是必需的。 如果您提供 SubDomain，则参数将以 DomainName 提供的参数为前缀。提供的 Active Directory 域名将成为子域名。
AdminPassword		活动目录管理员的密码（用户名`Admin`）。此用户是在初始引导阶段在活动目录中创建的，之后不使用。 重要：此字段的格式可以是 (1) 纯文本密码或 (2) 成对格式的 AWS 密钥的 ARN。key/value `{"password":"somepassword"}` 注意：此用户的密码必须满足 A ctive Directory 的密码复杂性要求。

参数	默认值	描述
ServiceAccountPassword		用于创建服务帐号的密码 (`ReadOnlyUser`)。此账户用于同步。 重要：此字段的格式可以是 (1) 纯文本密码或 (2) 成对格式的 AWS 密钥的 ARN。key/value `{"password":"somepassword"}` 注意：此用户的密码必须满足 A ctive Directory 的密码复杂性要求。
密钥对		使用 SSH 客户端连接管理实例。 注意：AWS Systems Manager 会话管理器还可用于连接实例。
LDIFS3路径	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	在活动目录设置的引导阶段导入的 LDIF 文件的 Amazon S3 路径。有关更多信息，请参阅 LDIF Supp ort。该参数预先填充一个文件，该文件可在活动目录中创建多个用户。 要查看该文件，请参阅中提供的 res.ldif 文件。 GitHub

参数	默认值	描述
ClientIpCidr		您将从中访问该网站的 IP 地址。例如，您可以选择自己的 IP 地址，然后使用仅[IPADDRESS]/32 允许主机进行访问。您可以在部署后更新此内容。
ClientPrefixList		输入前缀列表以提供对活动目录管理节点的访问权限。有关创建托管前缀列表的信息，请参阅使用客户管理的前缀列表。
EnvironmentName	res-*[environment name]*	如果提供PortalDomainName 了，则此参数用于为生成的密钥添加标签，以便可以在环境中使用它们。这将需要与创建 RES 堆栈时使用的EnvironmentName 参数相匹配。如果您要在账户中部署多个环境，则该环境必须是唯一的。
PortalDomainName		对于 GovCloud 部署，请勿输入此参数。证书和密钥是在先决条件期间手动创建的。该账户在 Amazon Route 53 中的域名。如果提供了这个，则会生成一个公共证书和密钥文件并将其上传到 AWS Secrets Manager。如果您有自己的域名和证书，则EnvironmentName 可以将此参数和留空。

4. 确认功能中的所有复选框，然后选择创建堆栈。

第 1 步：启动产品

按照本节中的 step-by-step说明配置产品并将其部署到您的账户。

部署时间：大约 60 分钟

您可以先下载该产品的 CloudFormation 模板，然后再进行部署。

如果您要在 AWS GovCloud （美国西部）部署，请使用此模板。

res-stack-使用此模板启动产品和所有关联组件。默认配置部署 RES 主堆栈和身份验证、前端和后端资源。

> **Note**
>
> AWS CloudFormation 资源是从 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 构造中创建的。

该 AWS CloudFormation 模板在 AWS 中部署了研究与工程工作室。 AWS Cloud在启动堆栈之前，您必须满足先决条件。

1. 登录 AWS Management Console 并在 https://console.aws.amazon.com/cloudformat ion 上打开 AWS CloudFormation 控制台。
2. 启动模板。

   要在 AWS GovCloud （美国西部）部署，请启动此模板。
3. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要以其他方式启动解决方案 AWS 区域，请使用控制台导航栏中的区域选择器。

   > **Note**
   >
   > 本产品使用 Amazon Cognito 服务，但目前并非所有服务都可用。 AWS 区域您必须在可用 Amazon Cognito AWS 区域 的地方发布此产品。有关按地区划分的最新可用性，请参阅AWS 区域所有服务列表。
4. 在 “参数” 下，查看此产品模板的参数并根据需要进行修改。如果您部署了自动外部资源，则可以在外部资源堆栈的输出选项卡中找到这些参数。

参数	默认值	描述
EnvironmentName	*<res-demo>*	以 res-开头且不超过 11 个字符的 RES 环境的唯一名称。
AdministratorEmail		完成产品设置的用户的电子邮件地址。如果集成失败时出现活动目录单点登录，则此用户还可以充当破碎玻璃用户。
InfrastructureHostAMI	ami-*[numbers or letters only]*	（可选）您可以提供用于所有基础设施主机的自定义 AMI ID。目前支持的基本操作系统是亚马逊 Linux 2。有关更多信息，请参阅 配置 RES-ready AMIs。
SSHKey配对		用于连接基础架构主机的密钥 pair。
ClientIP	*x.x.x*.0/24 或 .0/32 *x.x.x*	IP 地址过滤器，用于限制与系统的连接。您可以在部署 ClientIpCidr 后进行更新。
ClientPrefixList		（可选）提供托管前缀列表，IPs 允许直接访问 Web UI 和 SSH 进入堡垒主机。
IAMPermission边界		（可选）您可以提供托管策略 ARN，该策略将作为权限边界附加到在 RES 中创建的所有角色。有关更多信息，请参阅 设置自定义权限边界。
VpcId		将在其中启动实例的 VPC 的 IP。

参数	默认值	描述
IsLoadBalancerInternetFacing		选择 true 部署面向 Internet 的负载均衡器（负载均衡器需要公有子网）。对于需要限制互联网访问的部署，请选择 false。
LoadBalancerSubnets		在不同的可用区中选择至少两个子网，负载均衡器将在其中启动。对于需要受限互联网访问的部署，请选择私有子网。对于需要互联网访问的部署，请选择公有子网。如果外部网络堆栈创建了两个以上，请选择所有已创建的组件。
InfrastructureHostSubnets		在不同的可用区中选择至少两个私有子网，基础设施主机将在其中启动。如果外部网络堆栈创建了两个以上，请选择所有已创建的组件。
VdiSubnets		在不同的可用区中选择至少两个私有子网，VDI 实例将在其中启动。如果外部网络堆栈创建了两个以上，请选择所有已创建的组件。
ActiveDirectoryName	*corp.res.com*	活动目录的域。它不需要与门户域名相匹配。
ADShort名称	*corp*	活动目录的简称。这也被称为 NetBIOS 名称。
LDAP 基础	***DC=corp,DC=res,DC=com***	LDAP 层次结构中指向基础的 LDAP 路径。

参数	默认值	描述
LDAPConnectionURI		活动目录的主服务器可以访问的单个 ldap://路径。如果您使用默认 AD 域部署了自动外部资源，则可以使用 ldap: // corp.res.com。
ServiceAccountUserName	ServiceAccount	用于连接到 AD 的服务帐号的用户名。此帐户必须有权在 ComputerSOU 中创建计算机。
ServiceAccountPass wordSecretArn		提供一个秘密 ARN，其中包含的纯文本密码。 ServiceAc count
UsersOU		AD 中的组织单位，供将要同步的用户使用。
GroupSOU		AD 中用于将要同步的群组的组织单位。
sudoerSou		AD 内面向全球 sudoer 的组织单位。
SudoersGroupName	RESAdministrators	组名，包含安装时对实例具有 sudoer 访问权限和在 RES 上具有管理员访问权限的所有用户。
ComputersO		实例将加入的 AD 中的组织单位。
域名TLSCertificate秘书		（可选）提供域 TLS 证书密钥 ARN 以启用与 AD 的 TLS 通信。

参数	默认值	描述
EnableLdapIDMapping		确定 UID 和 GID 编号是由 SSSD 生成的，还是使用 AD 提供的数字。如果使用 SSSD 生成的 UID 和 GID，则设置为 True，如果使用 AD 提供的 UID 和 GID，则设置为 False。在大多数情况下，此参数应设置为 True。
禁用 ADJoin	False	要防止 Linux 主机加入目录域，请更改为 True。否则，请保留默认设置 False。
ServiceAccountUserDN		在“目录”中提供服务帐户用户的可分辨名称 (DN)。
SharedHomeFilesystem身份证		用于 Linux VDI 主机的共享主文件系统的 EFS ID。
CustomDomainNamefo rWebApp		（可选）Web 门户网站使用的子域名为系统的 Web 部分提供链接。
CustomDomainNameforVDI		（可选）Web 门户网站使用的子域名为系统的 VDI 部分提供链接。

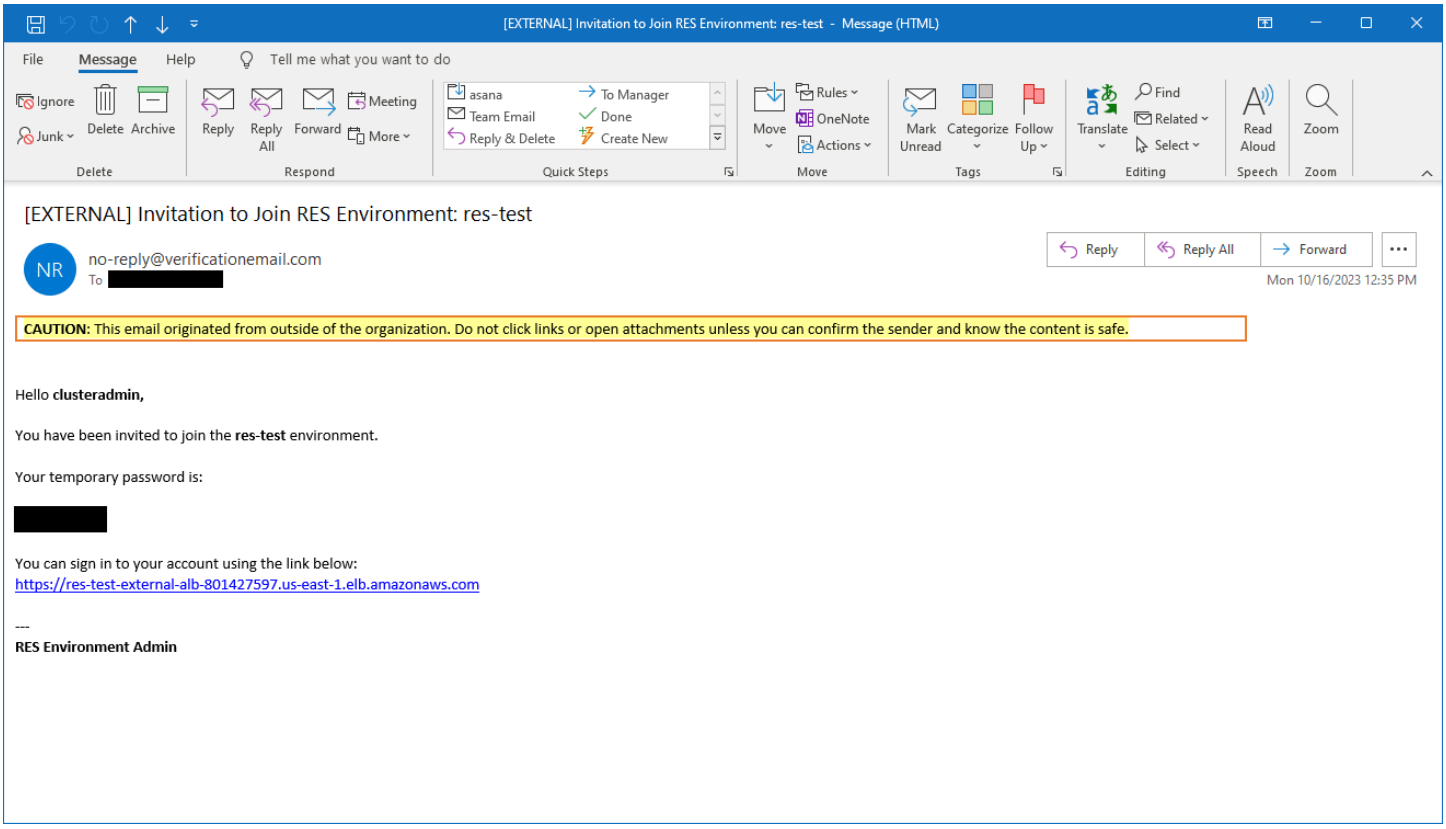
参数	默认值	描述
ACMCertificateARNforWebApp		（可选）使用默认配置时，产品将网络应用程序托管在 amazonaws.com 域下。您可以在自己的域名下托管产品服务。如果您部署了自动外部资源，则该资源是为您生成的，信息可以在 res-bi 堆栈的输出中找到。如果您需要为 Web 应用程序生成证书，请参阅配置指南。
CertificateSecretARNforVDI		（可选）此 ARN 密钥存储您的门户网站公共证书的公共证书。如果您为自动外部资源设置了门户域名，则可以在 res-bi 堆栈的 Outputs 选项卡下找到该值。
PrivateKeySecretARNforVDI		（可选）此 ARN 密钥存储您的门户网站证书的私钥。如果您为自动外部资源设置了门户域名，则可以在 res-bi 堆栈的 Outputs 选项卡下找到该值。

5. 选择 Create stack（创建堆栈）以部署堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。您将在大约 60 分钟后收到 “创建_完成” 状态。

第 2 步：首次登录

在您的账户中部署产品堆栈后，您将收到一封包含您的凭据的电子邮件。使用该 URL 登录您的账户并为其他用户配置工作空间。



首次登录后，您可以在 Web 门户中配置设置以连接到 SSO 提供商。有关部署后的配置信息，请参阅。配置指南请注意，`clusteradmin`这是一个 breakglass 帐户，你可以用它来创建项目并为这些项目分配用户或群组成员资格；它不能为自己分配软件堆栈或部署桌面。

更新产品

Research and Engineering Studio (RES) 有两种更新产品的方法，这取决于版本更新是主要更新还是次要更新。

RES 使用基于日期的版本控制方案。主要版本使用年份和月份，次要版本在必要时添加序列号。例如，版本 2024.01 于 2024 年 1 月作为主要版本发布；版本 2024.01.01 是该版本的次要版本更新。

主题

主要版本更新

Research and Engineering Studio 使用快照来支持从以前的 RES 环境迁移到最新版本，而不会丢失您的环境设置。在用户入职之前，您还可以使用此流程来测试和验证环境的更新。

要使用最新版本的 RES 更新您的环境，请执行以下操作：

1. 创建当前环境的快照。请参阅the section called “创建快照”。
2. 使用新版本重新部署 RES。请参阅the section called “第 1 步：启动产品”。
3. 将快照应用于更新的环境。请参阅the section called “应用快照”。
4. 验证所有数据已成功迁移到新环境。

次要版本更新

对于 RES 的次要版本更新，不需要重新安装。您可以通过更新现有的 RES 堆栈 AWS CloudFormation 模板来更新该堆栈。在部署更新之前，请在中检查当 AWS CloudFormation 前 RES 环境的版本。你可以在模板的开头找到版本号。

例如：`"Description": "RES_2024.1"`

要进行次要版本更新，请执行以下操作：

1. 在中下载最新的 AWS CloudFormation 模板the section called “第 1 步：启动产品”。
2. 在 https://console.aws.amazon.com/cloudformat ion 上打开 AWS CloudFormation 控制台。

3. 在堆栈中，找到并选择主堆栈。它应该显示为*<stack-name>*。
4. 选择更新。
5. 选择 “替换当前模板”。
6. 对于 Template source(模板来源)，选择 Upload a template file(上载模板文件)。
7. 选择选择文件并上传您下载的模板。
8. 在 “指定堆栈详细信息” 上，选择 “下一步”。您无需更新参数。
9. 在配置堆栈选项上，选择下一步。
10. 在 “查看<stack-name>” 中，选择 “提交”。

卸载产品

你可以使用 AWS Management Console 或卸载 AWS 产品上的 Research and Engineering Studio AWS Command Line Interface。您必须手动删除此产品创建的亚马逊简单存储服务 (Amazon S3) 存储桶。如果您存储了要保留的数据，本产品不会自动删除 < EnvironmentName >-shared-storage-security-group 。

使用 AWS Management Console

1. 登录 AWS CloudFormation 控制台。
2. 在堆栈页面上，选择此产品的安装堆栈。
3. 选择删除。

使用 AWS Command Line Interface

确定 AWS Command Line Interface (AWS CLI) 在您的环境中是否可用。有关安装说明，请参阅《AWS CLI 用户指南》 AWS Command Line Interface中的 “是什么”。确认产品部署所在区域的管理员帐户可用且已配置为管理员帐户后，运行以下命令。 AWS CLI

```
$ aws cloudformation delete-stack --stack-name
<RES-stack-name>
```

正在删除 shared-storage-security-group

> **Warning**
>
> 默认情况下，该产品会保留此文件系统，以防止数据意外丢失。如果您选择删除安全组和关联的文件系统，则保留在这些系统中的所有数据都将被永久删除。我们建议备份数据或将数据重新分配给新的安全组。

1. 登录 AWS Management Console 并打开 Amazon EFS 控制台，网址为 https://console.aws.amazon.com/efs/。
2. 删除与 *<RES-stack-name>*-关联的所有文件系统shared-storage-security-group。或者，您可以将这些文件系统重新分配给另一个安全组来维护数据。

3. 登录 AWS Management Console 并打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
4. 删除 *<RES-stack-name>*-shared-storage-security-group。

删除 Amazon S3 存储桶

如果您决定删除 AWS CloudFormation 堆栈以防止数据意外丢失，则该产品配置为保留产品创建的 Amazon S3 存储桶（用于在可选区域进行部署）。卸载产品后，如果您不需要保留数据，则可以手动删除此 S3 存储桶。按照以下步骤删除 Amazon S3 存储桶。

1. 登录 AWS Management Console 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
2. 在导航窗格中选择存储桶。
3. 找到 S `stack-name` 3 存储桶。
4. 选择每个 Amazon S3 存储桶，然后选择清空。您必须清空每个存储桶。
5. 选择 S3 存储桶，然后选择删除。

要使用删除 S3 存储桶 AWS CLI，请运行以下命令：

```
$ aws s3 rb s3://<bucket-name> --force
```

> **Note**
>
> 该`--force`命令会清空存储桶中的内容。

配置指南

本配置指南为技术受众提供了部署后指导，说明如何在 AWS 产品上进一步定制和与研究与工程工作室集成。

主题

管理用户和群组

研究与工程工作室可以使用任何符合 SAML 2.0 标准的身份提供商。如果您使用外部资源部署 RES 或计划使用 IAM 身份中心，请参阅使用 IAM 身份中心设置单点登录 (SSO)。如果您有自己的符合 SAML 2.0 标准的身份提供商，请参阅为单点登录 (SSO) 配置您的身份提供商。

主题

使用 IAM 身份中心设置单点登录 (SSO)

如果您尚未将身份中心连接到托管 Active Directory，请从开始步骤 1：设置身份中心。如果您已经将身份中心与托管的 Active Directory 连接在一起，请从开始步骤 2：Connect 连接到身份中心。

> **Note**
>
> 如果您要部署到 AWS GovCloud （美国西部）区域，请在部署 Research and Engineering Studio 的 AWS GovCloud (US) 分区账户中设置 SSO。

步骤 1：设置身份中心

启用 IAM Identity Center

1. 登录 AWS Identity and Access Management 控制台。
2. 打开身份中心。
3. 选择 启用。
4. 选择 “启用方式” AWS Organizations。
5. 选择继续。

> **Note**
>
> 确保您所在的区域与托管活动目录所在的区域相同。

将 IAM 身份中心连接到托管活动目录

启用 IAM Identity Center 后，请完成以下推荐的设置步骤：

1. 在导航窗格中，选择设置。
2. 在 “身份来源” 下，选择 “操作”，然后选择 “更改身份来源”。
3. 在 “现有目录” 下，选择您的目录。
4. 选择下一步。
5. 查看您的更改并在确认框**ACCEPT**中输入。
6. 选择更改身份源。

将用户和群组同步到身份中心

所做的更改完成后，将出现一个绿色的确认横幅。将 IAM 身份中心连接到托管活动目录

1. 在确认横幅中，选择启动引导式设置。
2. 在配置属性映射中，选择下一步。
3. 在 “用户” 部分下，输入要同步的用户。
4. 选择添加。

5. 选择下一步。
6. 查看您的更改，然后选择保存配置。
7. 同步过程可能需要几分钟。如果您收到有关用户未同步的警告消息，请选择恢复同步。

启用用户

1. 从菜单中选择 “用户”。
2. 选择要为其启用访问权限的用户。
3. 选择 “启用用户访问权限”。

步骤 2：Connect 连接到身份中心

在 IAM 身份中心设置应用程序

1. 打开 IAM Identity Center 控制台。
2. 选择 “应用程序”。
3. 选择 “添加应用程序”。
4. 在 “设置” 首选项下，选择 “我有要设置的应用程序”。
5. 在 “应用程序类型” 下，选择 SAML 2.0。
6. 选择下一步。
7. 输入您要使用的显示名称和描述。
8. 在 IAM 身份中心元数据下，复制 IAM 身份中心 SAML 元数据文件的链接。在使用 RES 门户配置 IAM 身份中心时，您将需要这个。
9. 在 “应用程序属性” 下，输入您的应用程序起始 URL。例如 `<your-portal-domain>/sso`。
10. 在 “应用程序 ACS URL” 下，输入来自 RES 门户的重定向 URL。要找到这个：

    a. 在 “环境管理” 下，选择 “常规设置”。

    b. 选择 Identity provider 选项卡。

    c. 在 “单点登录” 下，您将找到 SAML 重定向网址。
11. 在 “应用程序 SAML 受众” 下，输入 Amazon Cognito URN。

    要创建骨灰盒，请执行以下操作：

    a. 在 RES 门户中，打开 “常规设置”。

b. 在 “身份提供商” 选项卡下，找到用户池 ID。

c. 将用户池 ID 添加到以下字符串：

```
urn:amazon:cognito:sp:<user_pool_id>
```

12. 输入 Amazon Cognito URN 后，选择提交。

为应用程序配置属性映射

1. 在身份中心中，打开您创建的应用程序的详细信息。
2. 选择操作，然后选择编辑属性映射。
3. 在主题下，输入 **${user:email}**。
4. 在 “格式” 下，选择 “电子邮件地址”。
5. 选择 “添加新属性映射”。
6. 在应用程序的用户属性下，输入 “电子邮件”。
7. 在 IAM Identity Center 中映射到此字符串值或用户属性下，输入**${user:email}**。
8. 在 “格式” 下，输入 “未指定”。
9. 选择保存更改。

在 IAM 身份中心向应用程序添加用户

1. 在 Identity Center 中，为你创建的应用程序打开分配的用户，然后选择分配用户。
2. 选择要分配应用程序访问权限的用户。
3. 选择 “分配用户”。

在 RES 环境中设置 IAM 身份中心

1. 在 “研究与工程工作室” 环境中，在 “环境管理” 下，打开 “常规设置”。
2. 打开 “身份提供商” 选项卡。
3. 在 “单点登录” 下，选择 “编辑”（在 “状态” 旁边）。
4. 在表格中填写以下信息：

a. 选择 SAML。

b. 在 “提供者名称” 下，输入用户友好的名称。

c. 选择输入元数据文档端点 URL。

d. 输入您在期间复制的 URL 在 IAM 身份中心设置应用程序。

e. 在 “提供商电子邮件属性” 下，输入 “电子邮件”。

f. 选择提交。

5. 刷新页面并检查状态是否显示为已启用。

为单点登录 (SSO) 配置您的身份提供商

Research and Engineering Studio 与任何 SAML 2.0 身份提供商集成，以验证用户对 RES 门户 这些步骤提供了与您选择的 SAML 2.0 身份提供商集成的指导。如果您打算使用 IAM 身份中心，请参阅the section called “使用 IAM 身份中心设置 SSO”。

> **Note**
>
> 在 IDP SAML 断言和 Active Directory 中，用户的电子邮件地址必须匹配。您需要将您的身份提供商与 Active Directory 连接起来，并定期同步用户。

主题

配置您的身份提供商

本节提供了使用 RES Amazon Cognito 用户池中的信息配置身份提供商的步骤。

1. RES 假设您有一个 AD（AWS 托管 AD 或自配置 AD），其用户身份允许访问 RES 门户和项目。将您的 AD 连接到您的身份服务提供商并同步用户身份。请查看您的身份提供商的文档，了解如何连接您的 AD 和同步用户身份。例如，请参阅《AWS IAM Identity Center 用户指南》中的使用 Active Directory 作为身份源。
2. 在您的身份提供商 (IdP) 中为 RES 配置 SAML 2.0 应用程序。此配置需要以下参数：
   - SAML 重定向网址 — 您的 IdP 用来向服务提供商发送 SAML 2.0 响应的网址。

> **Note**
>
> 根据 IdP 的不同，SAML 重定向网址可能有不同的名称：
>
> - 应用程序 URL
> - 断言消费者服务 (ACS) 网址
> - ACS POST 绑定网址

要获取网址

1. 以管理员或集群管理员身份登录 RES。
2. 导航到 “环境管理” ⇒ “常规设置” ⇒ “身份提供者”。
3. 选择 SAML 重定向网址。

- SAML 受众 URI — 服务提供商方面 SAML 受众实体的唯一 ID。

> **Note**
>
> 根据 IdP 的不同，SAML 受众 URI 的名称可能有所不同：
>
> - ClientID
> - 应用程序 SAML 受众
> - SP 实体 ID

按以下格式提供输入。

```
urn:amazon:cognito:sp:user-pool-id
```

要查找您的 SAML 受众 URI

1. 以管理员或集群管理员身份登录 RES。
2. 导航到 “环境管理” ⇒ “常规设置” ⇒ “身份提供者”。
3. 选择用户池 ID。

3. 发布到 RES 的 SAML 断言必须将以下内容 fields/claims 设置为用户的电子邮件地址：
   - SAML 主题或姓名 ID
   - SAML 电子邮件
4. 根据配置，您的 IdP 会添加 fields/claims 到 SAML 断言中。RES 需要这些字段。默认情况下，大多数提供商会自动填写这些字段。如果必须对其进行配置，请参阅以下字段输入和值。

   - AudienceRestriction — 设置为 `urn:amazon:cognito:sp:`*`user-pool-id`*。*`user-pool-id`*替换为您的 Amazon Cognito 用户池的 ID。

     ```
     <saml:AudienceRestriction>
         <saml:Audience> urn:amazon:cognito:sp:user-pool-id
     </saml:AudienceRestriction>
     ```

   - 响应-设置`InResponseTo`为`https://`*`user-pool-domain`*`/saml2/idpresponse`。*`user-pool-domain`*替换为您的 Amazon Cognito 用户池的域名。

     ```
     <saml2p:Response
       Destination="http://user-pool-domain/saml2/idpresponse"
       ID="id123"
       InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
       IssueInstant="Date-time stamp"
       Version="2.0"
       xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">
     ```

   - SubjectConfirmationData— 设置`Recipient`为您的用户池`saml2/idpresponse`终端节点和`InResponseTo`原始 SAML 请求 ID。

     ```
     <saml2:SubjectConfirmationData
       InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
       NotOnOrAfter="Date-time stamp"
       Recipient="https://user-pool-domain/saml2/idpresponse"/>
     ```

   - AuthnStatement— 按以下方式进行配置：

     ```
     <saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
       SessionIndex="32413b2e54db89c764fb96ya2k"
      SessionNotOnOrAfter="2016-10-30T13:13:28">
         <saml2:SubjectLocality />
         <saml2:AuthnContext>
     ```

```
 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
```

5. 如果您的 SAML 应用程序有注销 URL 字段，请将其设置为:。<*domain-url*>/saml2/logout

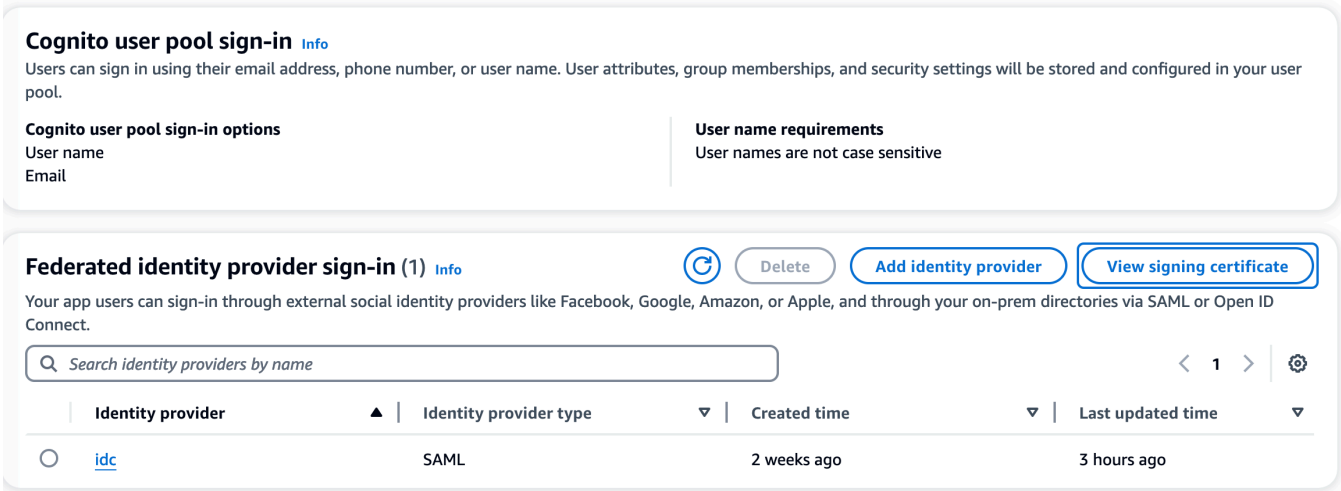
   获取域名网址

   1. 以管理员或集群管理员身份登录 RES。
   2. 导航到 “环境管理” ⇒ “常规设置” ⇒ “身份提供者”。
   3. 选择域名网址。

6. 如果您的 IdP 接受签名证书以建立与 Amazon Cognito 的信任，请下载亚马逊 Cognito 签名证书并将其上传到您的 IdP 中。

   获取签名证书

   1. 在 “入门” 中打开 Amazon Cognito 控制台 AWS Management Console
   2. 选择您的用户池。您的用户池应该是res-*<environment name>*-user-pool。
   3. 选择登录体验选项卡。
   4. 在联合身份提供商登录部分，选择查看签名证书。



您可以使用此证书在该信赖方上设置 Active Directory IDP `relying party trust`、添加和启用 SAML 支持。

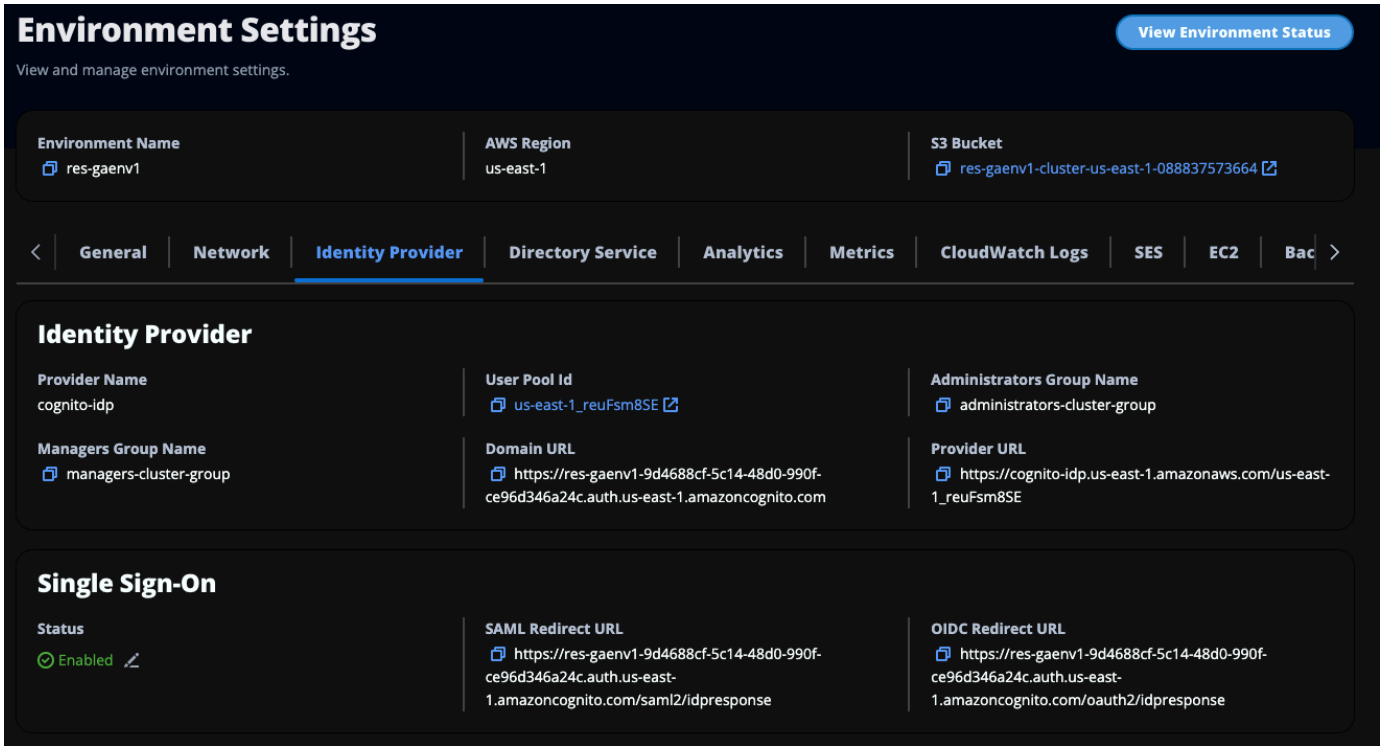
> **Note**
>
> 这不适用于 Keycloak 和 IDC。

5. 应用程序设置完成后，下载 SAML 2.0 应用程序元数据 XML 或 URL。你将在下一节中使用它。

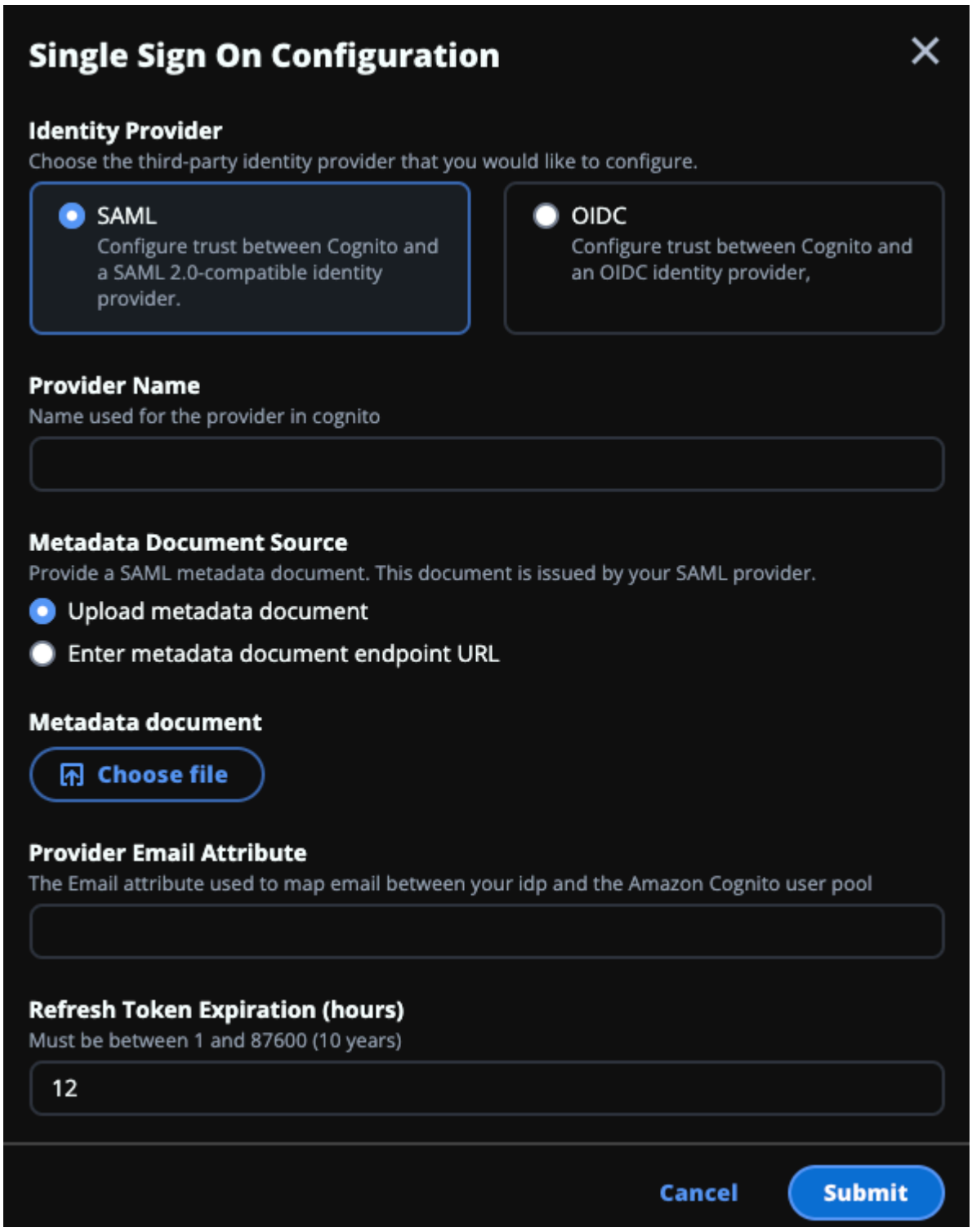
将 RES 配置为使用您的身份提供商

完成 RES 的单点登录设置

1. 以管理员或集群管理员身份登录 RES。
2. 导航到 “环境管理” ⇒ “常规设置” ⇒ “身份提供者”。



3. 在 “单点登录” 下，选择状态指示器旁边的编辑图标以打开 “单点登录配置” 页面。



a. 对于身份提供商，请选择 SAML。

b. 在提供商名称中，输入您的身份提供商的唯一名称。

> **Note**
>
> 不允许使用以下名称：
>
> - Cognito
> - IdentityCenter

c. 在 “元数据文档来源” 下，选择相应的选项并上传元数据 XML 文档或提供身份提供商提供的 URL。

d. 在 “提供商电子邮件属性” 中，输入文本值`email`。

e. 选择提交。

4. 重新加载环境设置页面。如果配置正确，则启用单点登录。

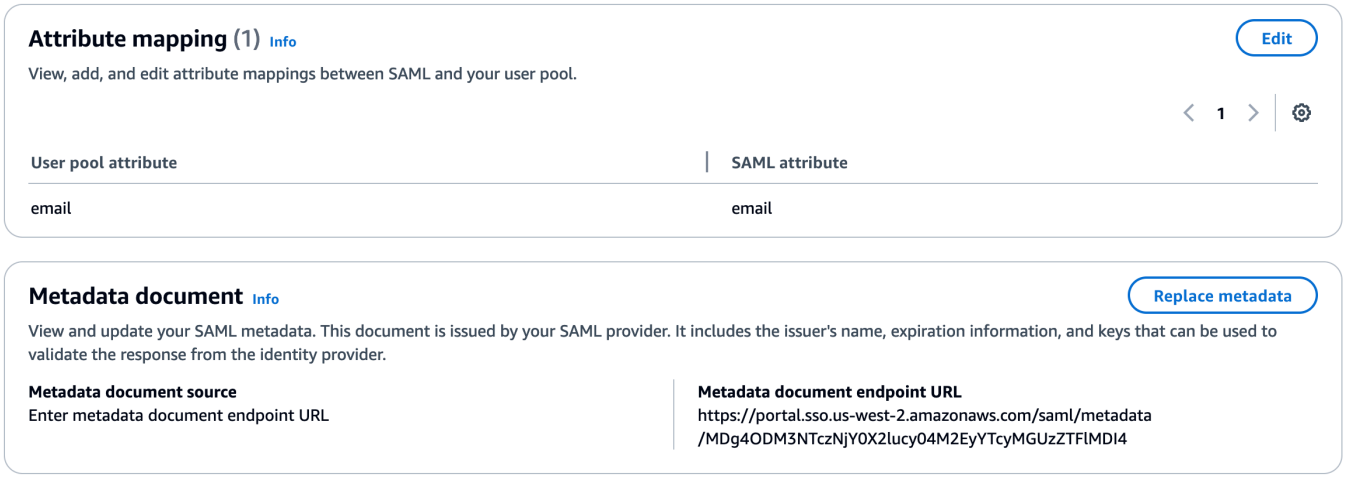
在非生产环境中配置您的身份提供商

如果您使用提供的外部资源创建了非生产 RES 环境，并将 IAM Identity Center 配置为身份提供商，则可能需要配置其他身份提供商，例如 Okta。RES SSO 启用表单要求提供三个配置参数：

1. 提供商名称-无法修改
2. 元数据文档或 URL-可以修改
3. 提供商电子邮件属性-可以修改

要修改元数据文档和提供者电子邮件属性，请执行以下操作：

1. 转到 Amazon Cognito 控制台。
2. 从导航栏中选择 “用户池”。
3. 选择您的用户池以查看用户池概述。
4. 在登录体验选项卡中，前往联合身份提供商登录，然后打开您配置的身份提供商。
5. 通常，您只需要更改元数据并保持属性映射不变。要更新属性映射，请选择编辑。要更新元数据文档，请选择替换元数据。



6. 如果您编辑了属性映射，则需要在 DynamoDB 中更新`<environment name>.cluster-settings`表。

   a. 打开 DynamoDB 控制台，然后从导航栏中选择 “表”。

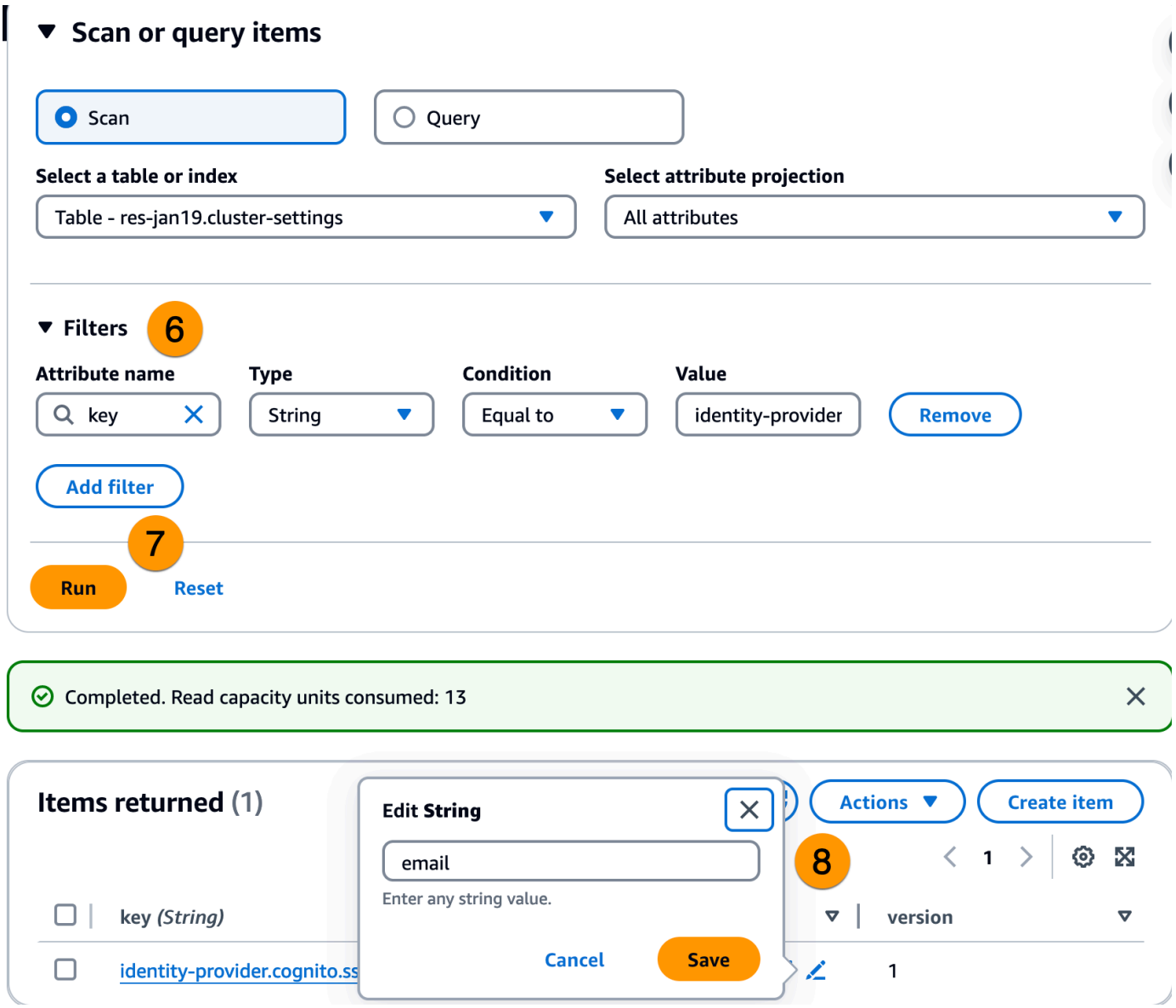
   b. 查找并选择`<environment name>.cluster-settings`表格，然后从 “操作” 菜单中选择 “浏览项目”。

   c. 在 “扫描或查询项目” 下，转至 “筛选” 并输入以下参数：

      - 属性名称 — `key`
      - 价值 — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. 选择运行。

7. 在 “已退回的商品” 下，找到该`identity-provider.cognito.sso_idp_provider_email_attribute`字符串并选择 “编辑”，修改字符串以匹配您在 Amazon Cognito 中所做的更改。



调试 SAML IdP 问题

SAML-tracer — 你可以在 Chrome 浏览器中使用这个扩展程序来跟踪 SAML 请求并检查 SAML 断言值。如需了解更多信息，请参阅 Chrome 网上应用店中的 SAML-Tracer。

SAML 开发人员工具 — OneLogin 提供可用于解码 SAML 编码值和检查 SAML 断言中必填字段的工具。有关更多信息，请参阅 OneLogin 网站上的 Base 64 Decode + Inflate。

Amazon CloudWatch 日志 — 您可以在 “日志” 中查看 RES CloudWatch 日志中是否有错误或警告。您的日志位于名称格式为的日志组中*res-environment-name*/cluster-manager。

Amazon Cognito 文档 — 有关 SAML 与 Amazon Cognito 集成的更多信息，请参阅《亚马逊 Cognito 开发者指南》中的将 SAML 身份提供商添加到用户池。

为用户设置密码

1. 在AWS Directory Service 控制台中，为创建的堆栈选择目录。
2. 在 “操作” 菜单下，选择 “重置用户密码”。
3. 选择用户并输入新密码。
4. 选择 “重置密码”。

创建子域名

如果您使用的是自定义域名，则需要设置子域名以支持门户的 Web 和 VDI 部分。

> **Note**
>
> 如果您要部署到 AWS GovCloud （美国西部）区域，请在托管域公共托管区域的商业分区账户中设置 Web 应用程序和 VDI 子域。

1. 打开 Route 53 控制台。
2. 找到您创建的域名，然后选择创建记录。
3. 输入 “web” 作为记录名称。
4. 选择 CNAME 作为记录类型。
5. 在 “值” 栏中，输入您在初始电子邮件中收到的链接。
6. 选择创建记录。
7. 要为 VDC 创建记录，请检索 NLB 地址。
    a. 打开 AWS CloudFormation 管理控制台。
    b. 选择 `<environment-name>-vdc`。
    c. 选择资源并打开`<environmentname>-vdc-external-nlb`。
    d. 从 NLB 中复制 DNS 名称。
8. 打开 Route 53 控制台。

9. 找到您的域名并选择创建记录。
10. 在 “记录名称” 下输入vdc。
11. 在记录类型下，选择 CNAME。
12. 对于 NLB，请输入 DNS。
13. 选择创建记录。

创建 ACM 证书

默认情况下，RES 使用域 amazonaws.com 将门户网站托管在应用程序负载均衡器下。要使用自己的域，您需要配置由您提供或请求自 AWS Certificate Manager (ACM) 的公共 SSL/TLS 证书。如果您使用 ACM，您将收到一个 AWS 资源名称，您需要将其作为参数提供，以加密客户端和 Web 服务主机之间的 SSL/TLS 通道。

> **Tip**
>
> 如果您要部署外部资源演示包，则需要在中部署外部资源堆栈PortalDomainName时在中输入您选择的域创建外部资源。

要为自定义域创建证书，请执行以下操作：

1. 在控制台中，打开AWS Certificate Manager以请求公共证书。如果您要在 AWS GovCloud （美国西部）进行部署，请在您的 GovCloud 分区账户中创建证书。
2. 选择 “申请公共证书”，然后选择 “下一步”。
3. 在 “域名” 下，为*.PortalDomainName和请求证书PortalDomainName。
4. 在 “验证方法” 下，选择 DNS 验证。
5. 选择请求。
6. 在证书列表中，打开您请求的证书。每个证书的状态都将为 “待验证”。

   > **Note**
   >
   > 如果您看不到您的证书，请刷新列表。

7. 请执行以下操作之一：
   - 商业部署：

从每个请求的证书的证书详细信息中，选择在 R oute 53 中创建记录。证书的状态应更改为“已签发”。

- GovCloud 部署：

  如果您要在 AWS GovCloud （美国西部）部署，请复制 CNAME 密钥和值。在商业分区账户中，使用这些值在公共托管区域中创建新记录。证书的状态应更改为 “已签发”。

8. 复制要输入的新证书 ARN 作为参数。`ACMCertificateARNforWebApp`

Amazon CloudWatch 日志

研究与工程工作室在安装 CloudWatch 过程中会创建以下日志组。有关默认保留的内容，请参见下表：

CloudWatch 日志组	保留
/aws/lambda/ < >-集群端点 installation-stack-name	永不过期
/aws/lambda/ < >-sync installation-stack-name cluster-manager-scheduled-ad	永不过期
/aws/lambda/ < >-集群设置 installation-stack-name	永不过期
/aws/lambda/ < >-oauth-credentials installation-stack-name	永不过期
/aws/lambda/ < >-installation-stack-name self-signed-certificate	永不过期
/aws/lambda/ < >-installation-stack-name update-cluster-prefix-list	永不过期
/aws/lambda/ < >-installation-stack-name vdc-scheduled-event-transformer	永不过期
/aws/lambda/ < >-client-scope installation-stack-name vdc-update-cluster-manager	永不过期

CloudWatch 日志组	保留
/< >/集群管理器 installation-stack-name	3 个月
/< >/vdc/con installation-stack-name troller	3 个月
/< >/vdc/dcv installation-stack-name-broker	3 个月
/< >/vdc/ installation-stack-name dcv-conne ction-gateway	3 个月

如果您想更改日志组的默认保留期，可以转到CloudWatch 控制台并按照更改日志中的 CloudWatch 日志数据保留期的说明进行操作。

设置自定义权限边界

从 2024.04 开始，您可以选择通过附加自定义权限边界来修改 RES 创建的角色。通过在 Boundary 参数中提供权限边界的 ARN，可以将自定义权限边界定义为 RES AWS CloudFormation 安装的一部分。IAMPermission如果将此参数留空，则不会对任何 RES 角色设置权限边界。以下是 RES 角色操作所需的操作列表。确保您计划使用的任何权限边界都明确允许执行以下操作：

```
[
    {
        "Effect": "Allow",
        "Resource": "*",
        "Sid": "ResRequiredActions",
        "Action": [
            "access-analyzer:*",
            "account:GetAccountInformation",
            "account:ListRegions",
            "acm:*",
            "airflow:*",
            "amplify:*",
            "amplifybackend:*",
            "amplifyuibuilder:*",
            "aoss:*",
            "apigateway:*",
            "appflow:*",
            "application-autoscaling:*",
            "appmesh:*",
```

```
            "apprunner:*",
            "aps:*",
            "athena:*",
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
```

```
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
            "ecr:*",
            "ecs:*",
            "eks:*",
            "elastic-inference:*",
            "elasticache:*",
            "elasticbeanstalk:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "elasticmapreduce:*",
            "elastictranscoder:*",
            "es:*",
            "events:*",
            "firehose:*",
            "fis:*",
            "fms:*",
            "forecast:*",
            "fsx:*",
            "geo:*",
            "glacier:*",
            "glue:*",
            "grafana:*",
            "guardduty:*",
            "health:*",
            "iam:*",
            "identitystore:*",
            "imagebuilder:*",
            "inspector2:*",
            "inspector:*",
            "internetmonitor:*",
            "iot:*",
            "iotanalytics:*",
            "kafka:*",
            "kafkaconnect:*",
            "kinesis:*",
            "kinesisanalytics:*",
            "kms:*",
            "lambda:*",
            "lightsail:*",
            "logs:*",
            "memorydb:*",
            "mgh:*",
```

```
            "mobiletargeting:*",
            "mq:*",
            "neptune-db:*",
            "organizations:DescribeOrganization",
            "osis:*",
            "personalize:*",
            "pi:*",
            "pipes:*",
            "polly:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
            "resource-groups:*",
            "route53:*",
            "route53domains:*",
            "route53resolver:*",
            "rum:*",
            "s3:*",
            "sagemaker:*",
            "scheduler:*",
            "schemas:*",
            "sdb:*",
            "secretsmanager:*",
            "securityhub:*",
            "serverlessrepo:*",
            "servicecatalog:*",
            "servicequotas:*",
            "ses:*",
            "signer:*",
            "sns:*",
            "sqs:*",
            "ssm:*",
            "ssmmessages:*",
            "states:*",
            "storagegateway:*",
            "sts:*",
            "support:*",
            "tag:GetResources",
```

```
            "tag:GetTagKeys",
            "tag:GetTagValues",
            "textract:*",
            "timestream:*",
            "transcribe:*",
            "transfer:*",
            "translate:*",
            "vpc-lattice:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*",
            "wisdom:*",
            "xray:*"
        ]
    }
]
```

配置 RES-ready AMIs

借助 RES-ready AMIs，您可以在自定义实例上预先安装虚拟桌面实例 (VDIs) 的 RES 依赖项。 AMIs 使用 RES-ready 可以 AMIs 缩短使用预烘焙映像的 VDI 实例的启动时间。使用 EC2 Image Builder，您可以构建自己的软件堆栈并将其注册 AMIs 为新的软件堆栈。有关 Image Builder 的更多信息，请参阅 Image Builder 用户指南。

在开始之前，必须部署最新版本的 RES。

主题

- 准备 IAM 角色以访问 RES 环境
- 创建 EC2 Image Builder 组件
- 准备好你的 EC2 Image Builder 配方
- 配置 EC2 Image Builder 基础架构
- 配置 Image Builder 图像管道
- 运行 Image Builder 图像管道
- 在 RES 中注册新的软件堆栈

准备 IAM 角色以访问 RES 环境

要从 I EC2 mage Builder 访问 RES 环境服务，您必须创建或修改名为 RES-的 IAM 角色 EC2InstanceProfileForImageBuilder。有关配置在 Image Builder 中使用的 IAM 角色的信息，请参阅 Imag e Builder 用户指南中的AWS Identity and Access Management (IAM)。

你的角色需要：

- 可信关系包括 Amazon EC2 服务
- 亚马逊SSMManagedInstanceCore 和 EC2InstanceProfileForImageBuilder 政策
- 自定义 RES 策略，对 DynamoDB 和 Amazon S3 对已部署的 RES 环境的访问权限有限

  （此政策可以是客户管理的策略文档，也可以是客户内联策略文档。）

可信关系实体：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
            "Action": "sts:AssumeRole"
        }
    ]
}
```

可再生能源政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
```

```
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-
Account-ID}/idea/vdc/res-ready-install-script-packages/*"
        }
    ]
}
```

创建 EC2 Image Builder 组件

按照《Image Builder 用户指南》中的说明使用 Image Builder 控制台创建组件。

输入您的组件详细信息：

1. 对于 “类型”，选择 “构建”。
2. 对于映像操作系统 (OS)，请选择 Linux 或 Windows。
3. 在 “组件名称” 中，输入一个有意义的名称，例如**research-and-engineering-studio-vdi-<operating-system>**。
4. 输入组件的版本号，并根据需要添加描述。
5. 在定义文档中，输入以下定义文件。如果您遇到任何错误，那么 YAML 文件对空间很敏感，这很可能是导致错误的原因。

   Linux

   ```
   #  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
   #
   #  Licensed under the Apache License, Version 2.0 (the "License"). You may not
    use this file except in compliance
   #  with the License. A copy of the License is located at
   #
   #      http://www.apache.org/licenses/LICENSE-2.0
   ```

```
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-linux
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
```

```
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
```

```
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-windows
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
```

```
              destination:
'{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
      - name: RunInstallScript
        action: ExecutePowerShell
        onFailure: Abort
        maxAttempts: 3
        inputs:
           commands:
               - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
               - 'Tar -xf
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
               - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
               - 'Install-WindowsEC2Instance'
      - name: Reboot
        action: Reboot
        onFailure: Abort
        maxAttempts: 3
        inputs:
           delaySeconds: 0
```

6. 创建任何可选标签，然后选择创建组件。

准备好你的 EC2 Image Builder 配方

EC2 Image Builder 配方定义了用作创建新图像的起点的基础图像，以及为自定义图像和验证一切是否按预期运行而添加的一组组组件。您必须创建或修改配方才能构造具有必要的 RES 软件依赖项的目标 AMI。有关食谱的更多信息，请参阅管理食谱。

RES 支持以下镜像操作系统：

- 亚马逊 Linux 2 (x86 和 ARM64)
- Ubuntu 22.04.3 (x86)
- Windows 2019、2022 (x86)

Create a new recipe

1. 打开 EC2 Image Builder 控制台，网址为https://console.aws.amazon.com/imagebuilder。
2. 在 “已保存的资源” 下，选择 “图像配方”。
3. 选择创建映像配方。

4. 输入唯一的名称和版本号。
5. 选择 RES 支持的基础镜像。
6. 在 “实例配置” 下，如果未预安装 SSM 代理，请安装。在用户数据和任何其他需要的用户数据中输入信息。

> **Note**
>
> 有关如何安装 SSM 代理的信息，请参阅：
>
> - 在 Linux 版 EC2 实例上手动安装 SSM 代理
> - 在 Windows 服务器 EC2 实例上手动安装和卸载 SSM 代理

7. 对于基于 Linux 的配方，请将亚马逊管理的`aws-cli-version-2-linux`构建组件添加到配方中。RES 安装脚本使用提供对 DynamoDB 集群设置配置值的 VDI 访问权限。 AWS CLI Windows 不需要这个组件。
8. 添加为您的 Linux 或 Windows 环境创建的 EC2 Image Builder 组件，然后输入任何必需的参数值。以下参数是必填输入： AWSAccountID、 RESEnv名称、 RESEnv地区和 RESEnvReleaseVersion。

> **Important**
>
> 对于 Linux 环境，必须按顺序添加这些组件，并先添加`aws-cli-version-2-linux`构建组件。

9. （推荐）添加亚马逊管理的`simple-boot-test-<linux-or-windows>`测试组件以验证 AMI 是否可以启动。这是最低限度的建议。您可以选择其他符合您要求的测试组件。
10. 如果需要，请完成所有可选部分，添加任何其他所需的组件，然后选择 “创建配方”。

Modify a recipe

如果您已有 I EC2 mage Builder 配方，则可以通过添加以下组件来使用它：

1. 对于基于 Linux 的配方，请将亚马逊管理的`aws-cli-version-2-linux`构建组件添加到配方中。RES 安装脚本使用提供对 DynamoDB 集群设置配置值的 VDI 访问权限。 AWS CLI Windows 不需要这个组件。

2. 添加为您的 Linux 或 Windows 环境创建的 EC2 Image Builder 组件，然后输入任何必需的参数值。以下参数是必填输入： AWSAccountID、 RESEnv名称、 RESEnv地区和 RESEnvReleaseVersion。

> **Important**
>
> 对于 Linux 环境，必须按顺序添加这些组件，并先添加`aws-cli-version-2-linux`构建组件。

3. 如果需要，请完成所有可选部分，添加任何其他所需的组件，然后选择 “创建配方”。

配置 EC2 Image Builder 基础架构

您可以使用基础设施配置来指定 Image Builder 用来构建和测试您的 Image Builder 映像的亚马逊 EC2 基础设施。要与 RES 配合使用，您可以选择创建新的基础架构配置，也可以选择使用现有基础架构配置。

- 要创建新的基础架构配置，请参阅创建基础架构配置。
- 要使用现有基础架构配置，请更新基础架构配置。

要配置 Image Builder 基础设施，请执行以下操作：

1. 对于 IAM 角色，请输入您之前在中配置的角色the section called “准备 IAM 角色以访问 RES 环境”。
2. 对于实例类型，请选择内存至少 4 GB 且支持所选基本 AMI 架构的类型。参见 Amazon EC2 实例类型。
3. 对于 VPC、子网和安全组，您必须允许互联网访问才能下载软件包。还必须允许访问 RES 环境的`cluster-settings` DynamoDB 表和 Amazon S3 集群存储桶。

配置 Image Builder 图像管道

Image Builder 映像管道汇集了基础映像、用于构建和测试的组件、基础架构配置和分发设置。要将图像管道配置为 RES-ready AMIs，您可以选择创建新管道或使用现有管道。有关更多信息，请参阅 Image Builder 用户指南中的创建和更新 AMI 图像管道。

Create a new Image Builder pipeline

1. 打开 Image Builder 控制台，网址为https://console.aws.amazon.com/imagebuilder。
2. 从导航栏中选择 “图像管道”。
3. 选择 “创建映像管道”。
4. 通过输入唯一的名称、可选描述、时间表和频率来指定您的管道详细信息。
5. 在 “选择食谱” 中，选择 “使用现有食谱”，然后选择在中创建的配方the section called “准备好你的 EC2 Image Builder 配方”。验证您的食谱详细信息是否正确。
6. 在 “定义图像创建流程” 中，根据用例选择默认或自定义工作流程。在大多数情况下，默认工作流程就足够了。有关更多信息，请参阅为 Image Builder 管道配置 EC2 图像工作流程。
7. 在定义基础架构配置中，选择选择现有基础架构配置，然后选择在中创建的基础架构配置the section called “配置 EC2 Image Builder 基础架构”。验证您的基础架构详细信息是否正确。
8. 在 “定义分发设置” 中，选择 “使用服务默认值创建分发设置”。输出图像必须与您的 RES 环境 AWS 区域 相同。使用服务默认值，将在使用 Image Builder 的区域创建图像。
9. 查看管道详细信息并选择创建管道。

Modify an existing Image Builder pipeline

1. 要使用现有管道，请修改详细信息以使用中创建的配方the section called “准备好你的 EC2 Image Builder 配方”。
2. 选择保存更改。

运行 Image Builder 图像管道

要生成配置的输出图像，必须启动图像管道。构建过程可能需要长达一个小时，具体取决于图像配方中组件的数量。

要运行图像管道，请执行以下操作：

1. 从图像管道中，选择在中创建的管道the section called “配置 Image Builder 图像管道”。
2. 从 “操作” 中选择 “运行管道”。

在 RES 中注册新的软件堆栈

1. 按照中的the section called “软件堆栈 () AMIs”说明注册软件堆栈。

2. 对于 AMI ID，请输入内置输出映像的 AMI ID the section called “运行 Image Builder 图像管道”。

管理员指南

本管理员指南为技术受众提供了有关如何进一步定制 AWS 产品并与研究与工程工作室集成的其他说明。

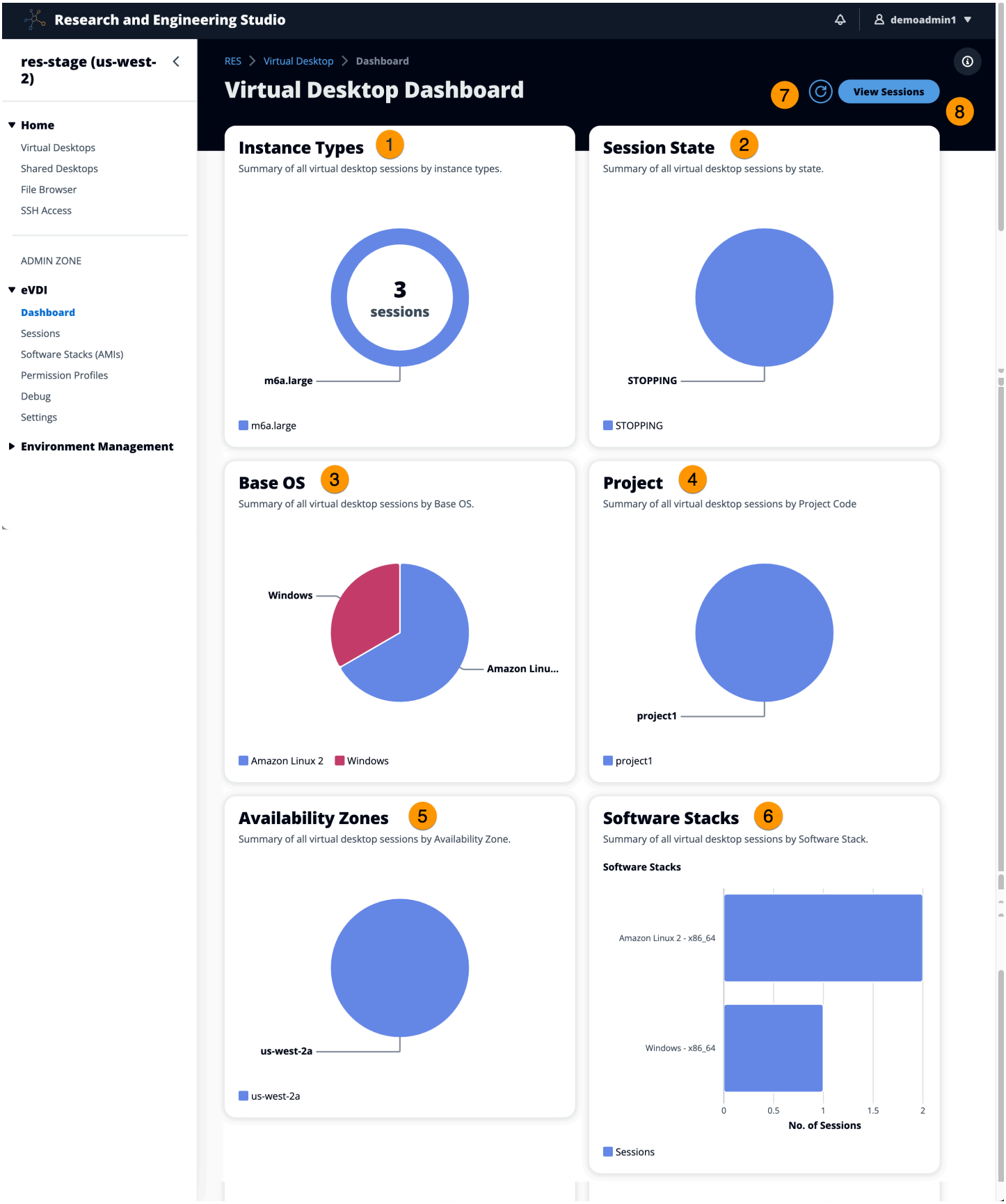
主题

会话管理

会话管理为开发和测试会话提供了灵活的交互式环境。作为管理用户，您可以允许用户在其项目环境中创建和管理交互式会话。

主题

控制面板


Research and Engineering Studio
demoadmin1
res-stage (us-west-2)
Home
Virtual Desktops
Shared Desktops
File Browser
SSH Access
ADMIN ZONE
eVDI
Dashboard
Sessions
Software Stacks (AMIs)
Permission Profiles
Debug
Settings
Environment Management
RES > Virtual Desktop > Dashboard
Virtual Desktop Dashboard
7
View Sessions
8
Instance Types
1
Summary of all virtual desktop sessions by instance types.
3
sessions
m6a.large
m6a.large
Session State
2
Summary of all virtual desktop sessions by state.
STOPPING
STOPPING
Base OS
3
Summary of all virtual desktop sessions by Base OS.
Windows
Amazon Linu...
Amazon Linux 2
Windows
Project
4
Summary of all virtual desktop sessions by Project Code
project1
project1
Availability Zones
5
Summary of all virtual desktop sessions by Availability Zone.
us-west-2a
us-west-2a
Software Stacks
6
Summary of all virtual desktop sessions by Software Stack.
Software Stacks
Amazon Linux 2 - x86_64
Windows - x86_64
0
0.5
1
1.5
2
No. of Sessions
Sessions

会话管理控制面板让管理员可以快速查看：

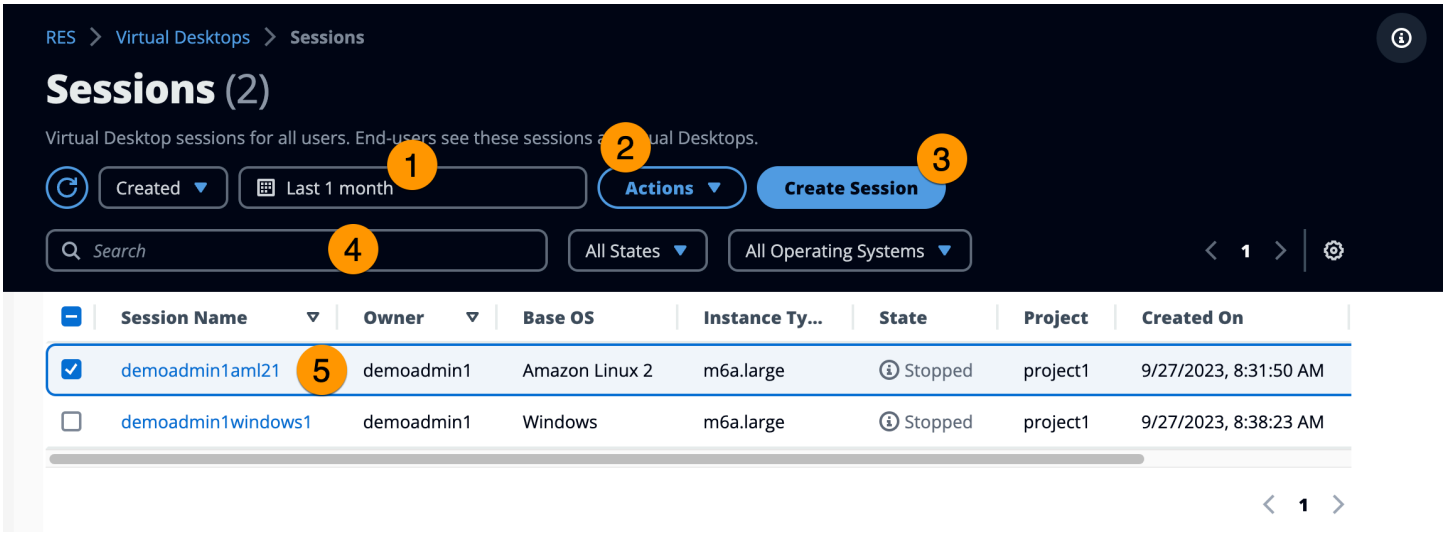
1. 实例类型
2. 会话状态
3. 基础操作系统
4. Projects
5. 可用区
6. 软件堆栈

此外，管理员还可以：

7. 刷新仪表板以更新信息。
8. 选择 “查看会话” 以导航到 “会话”。

会话

会话显示在研究与工程工作室中创建的所有虚拟桌面。在 “会话” 页面中，您可以筛选和查看会话信息或创建新会话。



1. 使用该菜单按在指定时间范围内创建或更新的会话筛选结果。
2. 选择一个会话，然后使用 “操作” 菜单执行以下操作：
   a. 恢复会话
   b. Stop/Hibernate 会话

c. 强制 Stop/Hibernate 会话

d. 终止会话

e. 强制终止会话

f. 会话 Health

g. 创建软件堆栈

3. 选择 “创建会话” 以创建新会话。
4. 按名称搜索会话，并按状态和操作系统进行筛选。
5. 选择会话名称以查看更多详细信息。

创建会话

1. 选择创建会话。“启动新虚拟桌面” 模式打开。
2. 输入新会话的详细信息。
3. （可选。）打开 “显示高级选项” 以提供更多详细信息，例如子网 ID 和 DCV 会话类型。
4. 选择提交。

Launch New Virtual Desktop

Session Name
Enter a name for the virtual desktop

Session Name is required. Use any characters and form a name of length between 3 and 24 characters, inclusive.

User
Select the user to create the session for

Project
Select the project under which the session will get created

Operating System
Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack
Select the software stack for your virtual desktop

Enable Instance Hibernation
Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

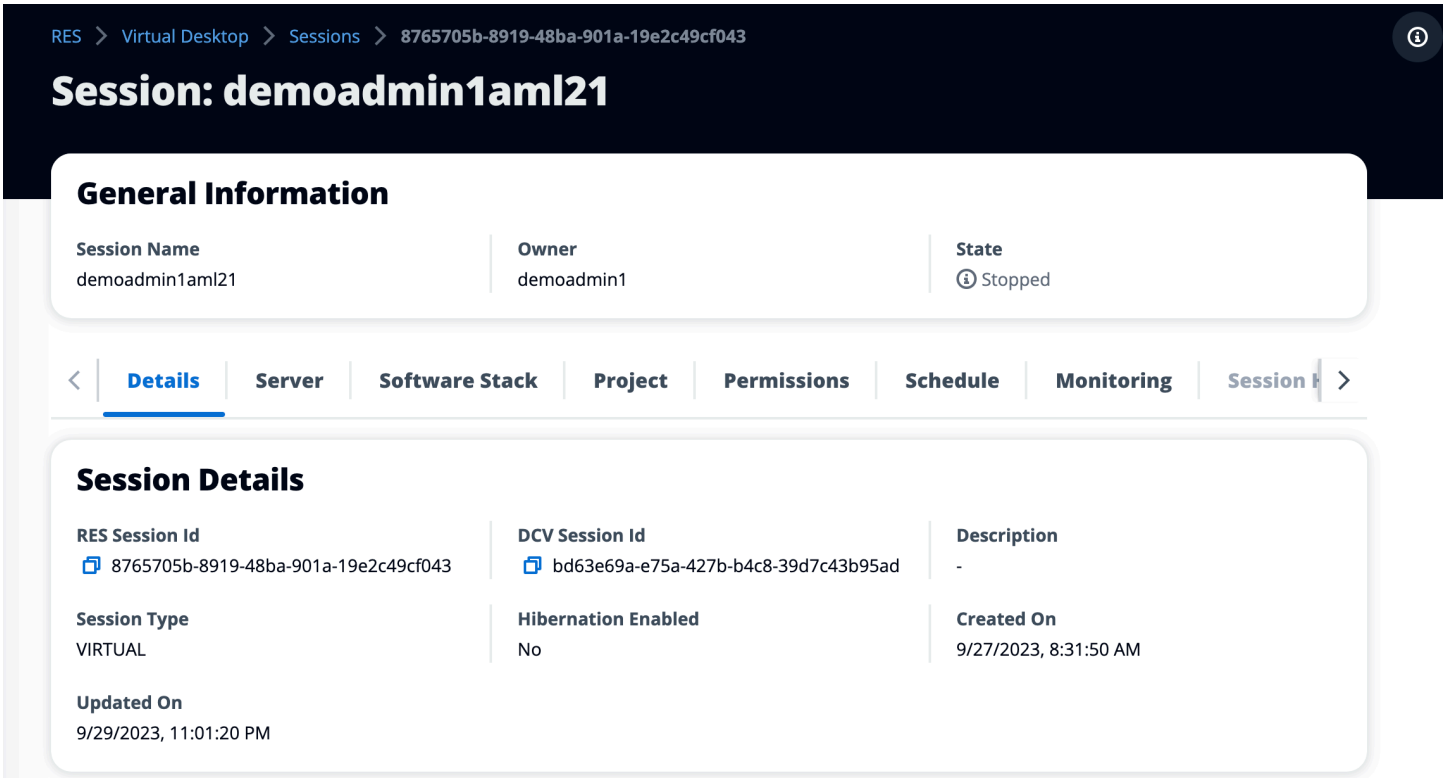
Virtual Desktop Size
Select a virtual desktop instance type

Storage Size (GB)
Enter the storage size for your virtual desktop in GBs

10

会话详情

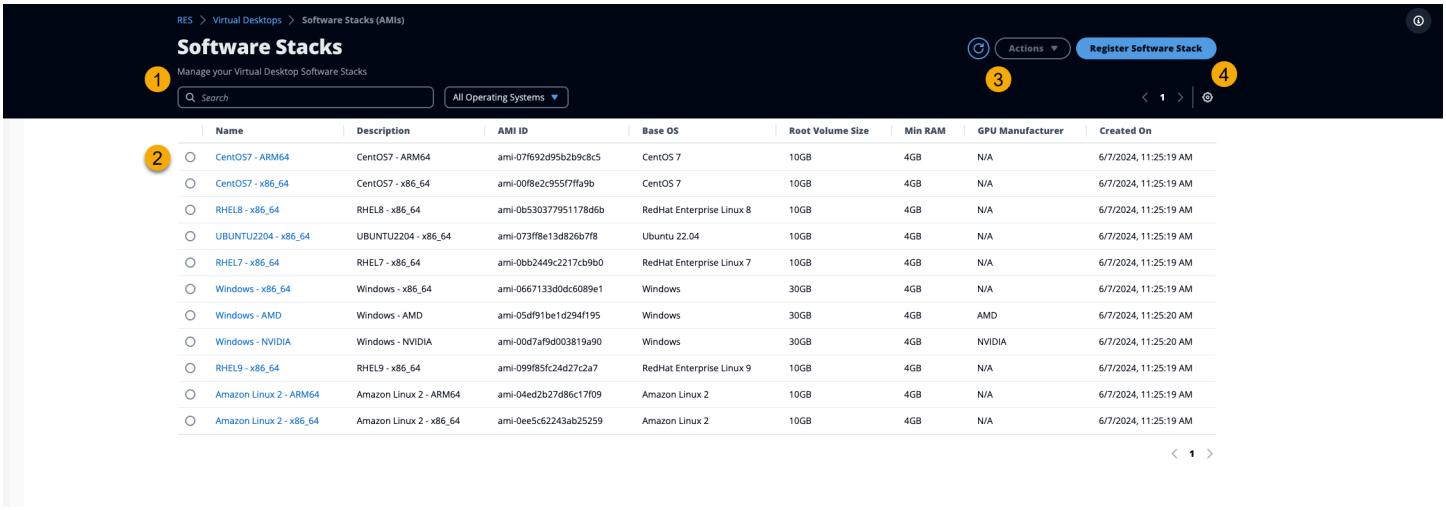
从 “会话” 列表中，选择会话名称以查看会话详细信息。



软件堆栈 () AMIs

> **Note**
>
> 要在中运行提供的 Cent SO7 软件堆栈 AWS GovCloud (US)，您需要 AWS Marketplace 使用关联的标准账户订阅其中的 AMI。

在软件堆栈页面上，您可以配置 Amazon 系统映像 (AMIs) 并管理现有 AMIs映像。



1. 要搜索现有的软件堆栈，请使用操作系统下拉列表按操作系统进行筛选。
2. 选择软件堆栈的名称以查看有关堆栈的详细信息。
3. 选择软件堆栈后，使用操作菜单编辑堆栈并将堆栈分配给项目。
4. 使用 “注册软件堆栈” 按钮可以创建新堆栈：
    1. 选择 “注册软件堆栈”。
    2. 输入新软件堆栈的详细信息。
    3. 选择提交。

Register new Software Stack

Name
Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description
Enter a user friendly description for the software stack

AMI Id
Enter the AMI Id

AMI Id must start with ami-xxx

Operating System
Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer
Select the GPU Manufacturer for the software stack

N/A

Min. Storage Size (GB)
Enter the min. storage size for your virtual desktop in GBs

10

Min. RAM (GB)
Enter the min. ram for your virtual desktop in GBs

10

Projects
Select applicable projects for the software stack

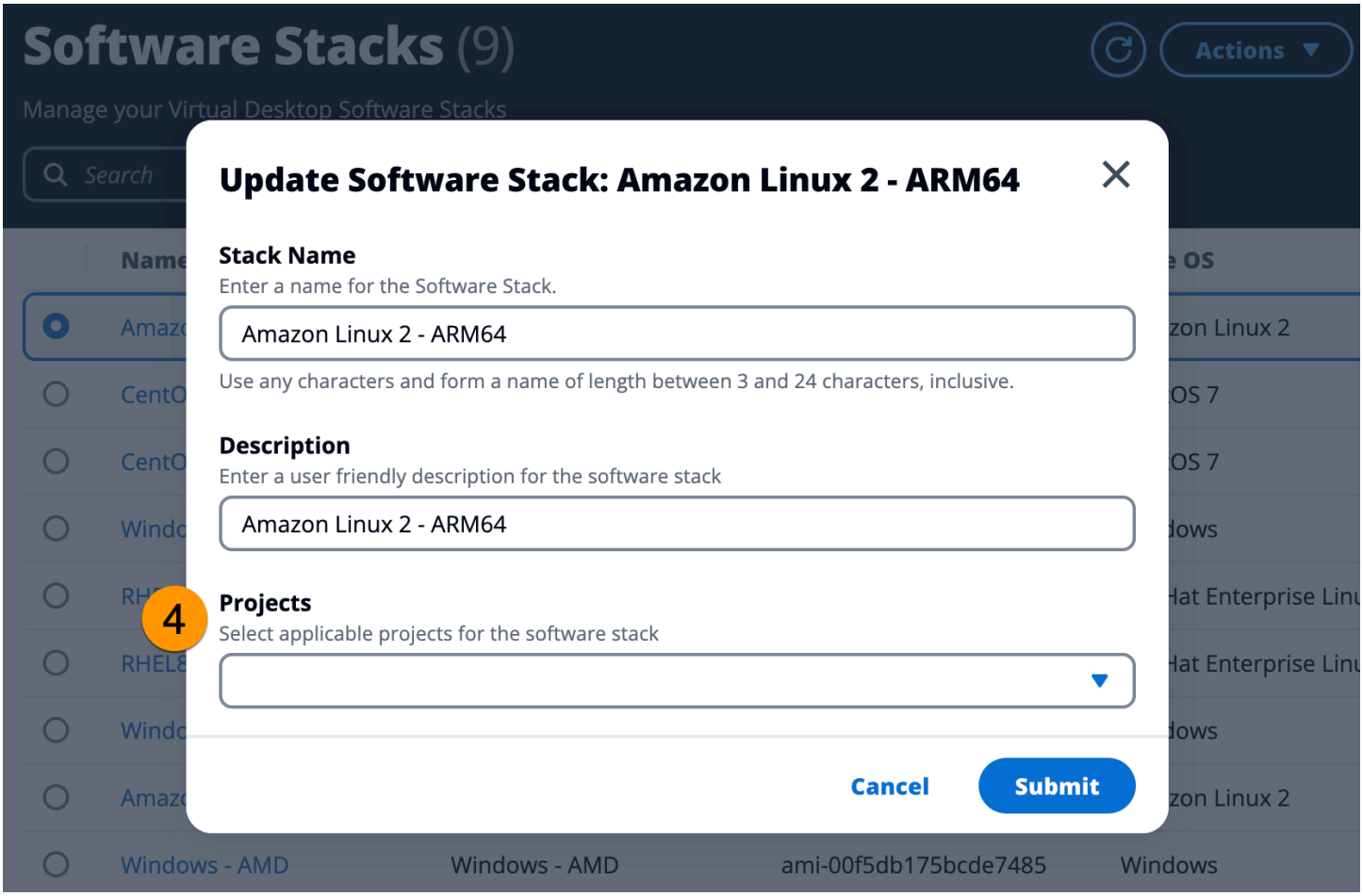
为项目分配软件堆栈

创建新的软件堆栈时，可以将堆栈分配给项目。如果您需要在初始创建后将堆栈添加到项目中，请执行以下操作：

> **Note**
>
> 您只能将软件堆栈分配给您所属的项目。

1. 从 “软件堆栈” 页面中选择需要添加到项目的软件堆栈。
2. 选择操作。
3. 选择编辑。
4. 使用 “项目” 下拉列表选择项目。
5. 选择提交。

您也可以从堆栈详细信息页面编辑软件堆栈。

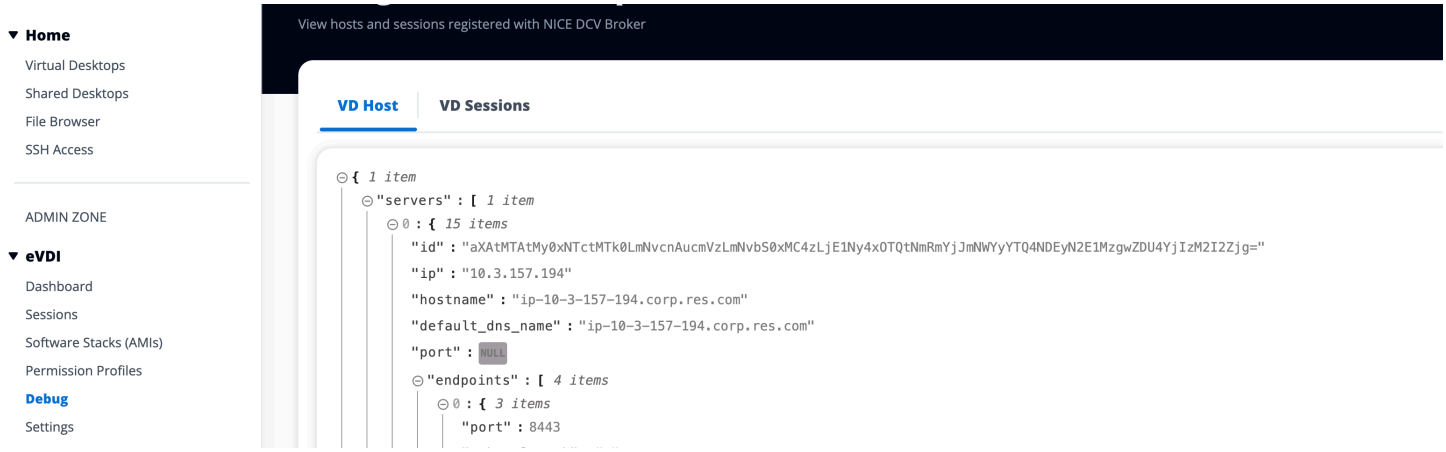


查看软件堆栈详细信息

从软件堆栈列表中，选择软件堆栈名称以查看详细信息。在详细信息页面中，您也可以选择编辑来编辑软件堆栈。

调试

调试面板显示与虚拟桌面相关的消息流量。您可以使用此面板来观察主机之间的活动。VD Host 选项卡显示特定于实例的活动，VD 会话选项卡显示正在进行的会话活动。



桌面设置

您可以使用 “桌面设置” 页面来配置与虚拟桌面关联的资源。通过 “服务器” 选项卡可以访问以下设置：

DCV 会话空闲超时

在此时间之后，DCV 会话将自动断开。这不会更改桌面会话的状态，只会从 DCV 客户端或 Web 浏览器关闭会话。

空闲超时警告

在此时间之后，将向客户端发出空闲警告。

CPU 利用率阈值

要视为空闲的 CPU 使用率。

每位用户允许的会话数

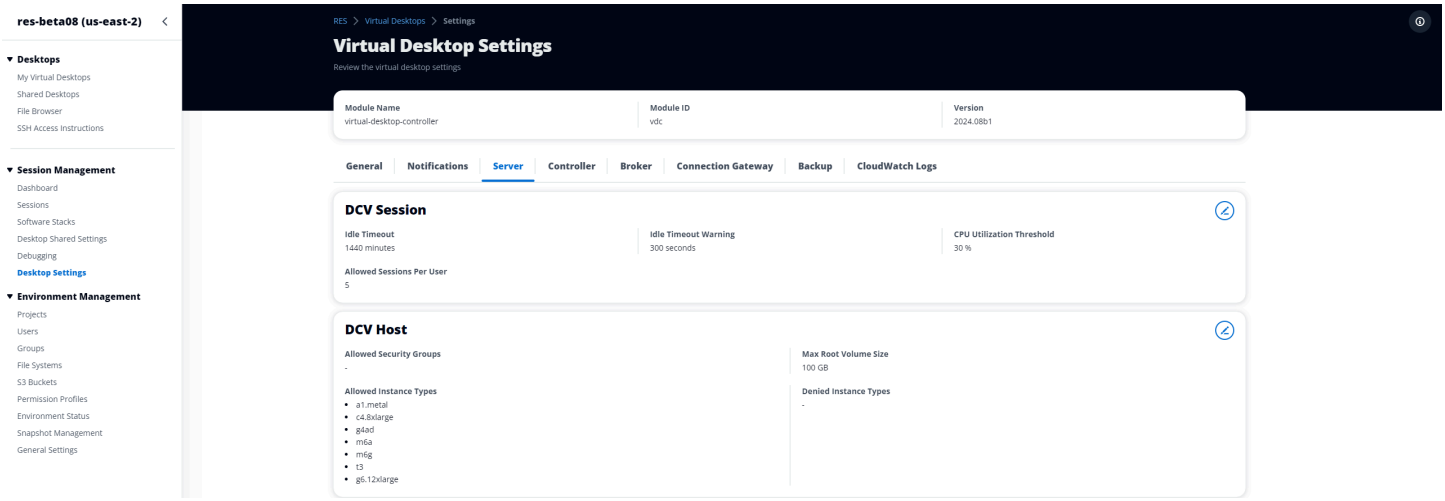
单个用户在给定时间可以进行的 VDI 会话数。如果用户达到或超过此值，则他们将无法从 “我的虚拟桌面” 页面启动新会话。通过 “会话” 页面启动会话的能力不受此值的影响。

最大根卷大小

虚拟桌面会话中根卷的默认大小。

允许的实例类型

可以为此 RES 环境启动的实例系列和大小列表。均接受实例系列和实例大小组合。例如，如果您指定 “m7a”，则所有大小的 m7a 系列都可作为 VDI 会话启动。如果您指定 “m7a.24xlarge”，则只有 m7a.24xlarge 可以作为 VDI 会话启动。此列表会影响环境中的所有项目。



环境管理

在 RES 的 “环境管理” 部分，管理用户可以为其研究和工程项目创建和管理隔离的环境。这些环境可以包括计算资源、存储和其他必要的组件，所有这些都位于安全的环境中。用户可以配置和自定义这些环境以满足其项目的特定要求，从而更轻松地对解决方案进行实验、测试和迭代，而不会影响其他项目或环境。

主题

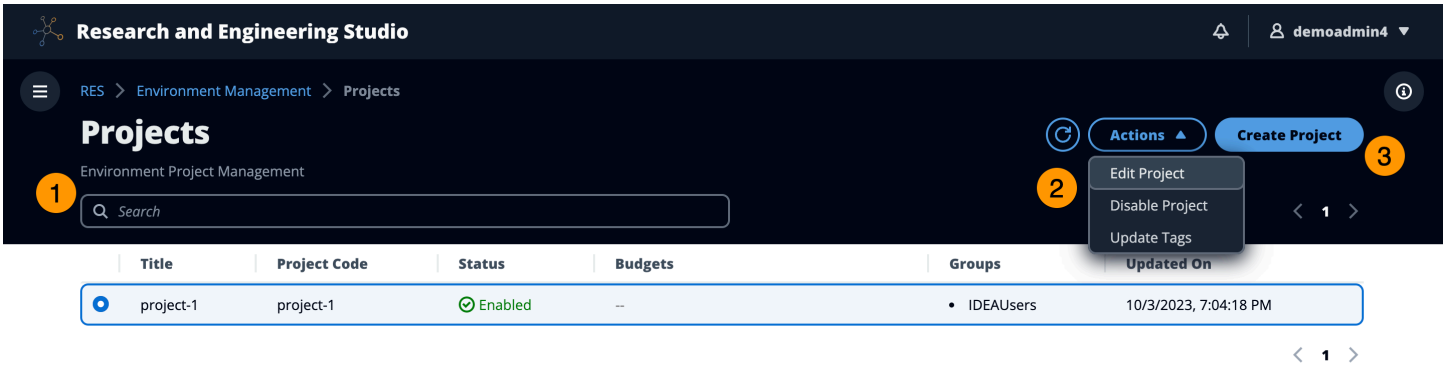
- Projects
- Users
- 组
- 权限配置文件
- 文件系统
- 环境状态
- 快照管理
- 环境设置
- Amazon S3 存储桶

Projects

项目构成了虚拟桌面、团队和预算的界限。创建项目时，需要定义其设置，例如名称、描述和环境配置。项目通常包括一个或多个环境，可以对其进行自定义以满足项目的特定要求，例如计算资源的类型和大小、软件堆栈和网络配置。

主题

查看项目



“项目” 仪表板提供了可供您使用的项目列表。在 “项目” 仪表板中，您可以：

1. 您可以使用搜索字段来查找项目。
2. 选择项目后，您可以使用 “操作” 菜单执行以下操作：
   a. 编辑项目
   b. 禁用或启用项目
   c. 更新项目标签
3. 您可以选择 “创建项目” 来创建新项目。

创建项目

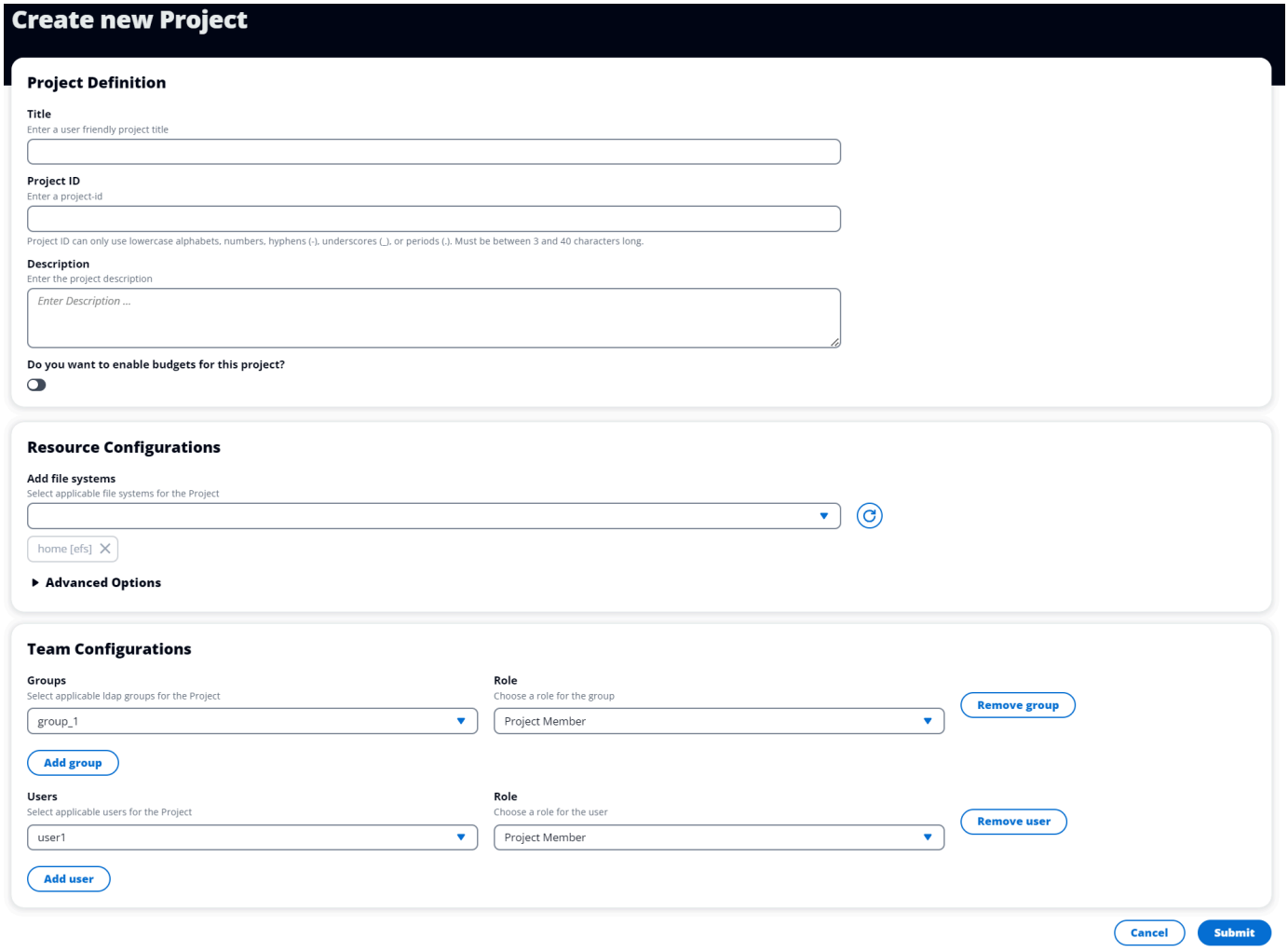
1. 选择创建项目。
2. 输入项目详细信息。

   项目 ID 是一个资源标签，可用于跟踪中的成本分配 AWS Cost Explorer Service。有关更多信息，请参阅激活用户定义的成本分配标签。

> **Important**
>
> 项目 ID 在创建后无法更改。

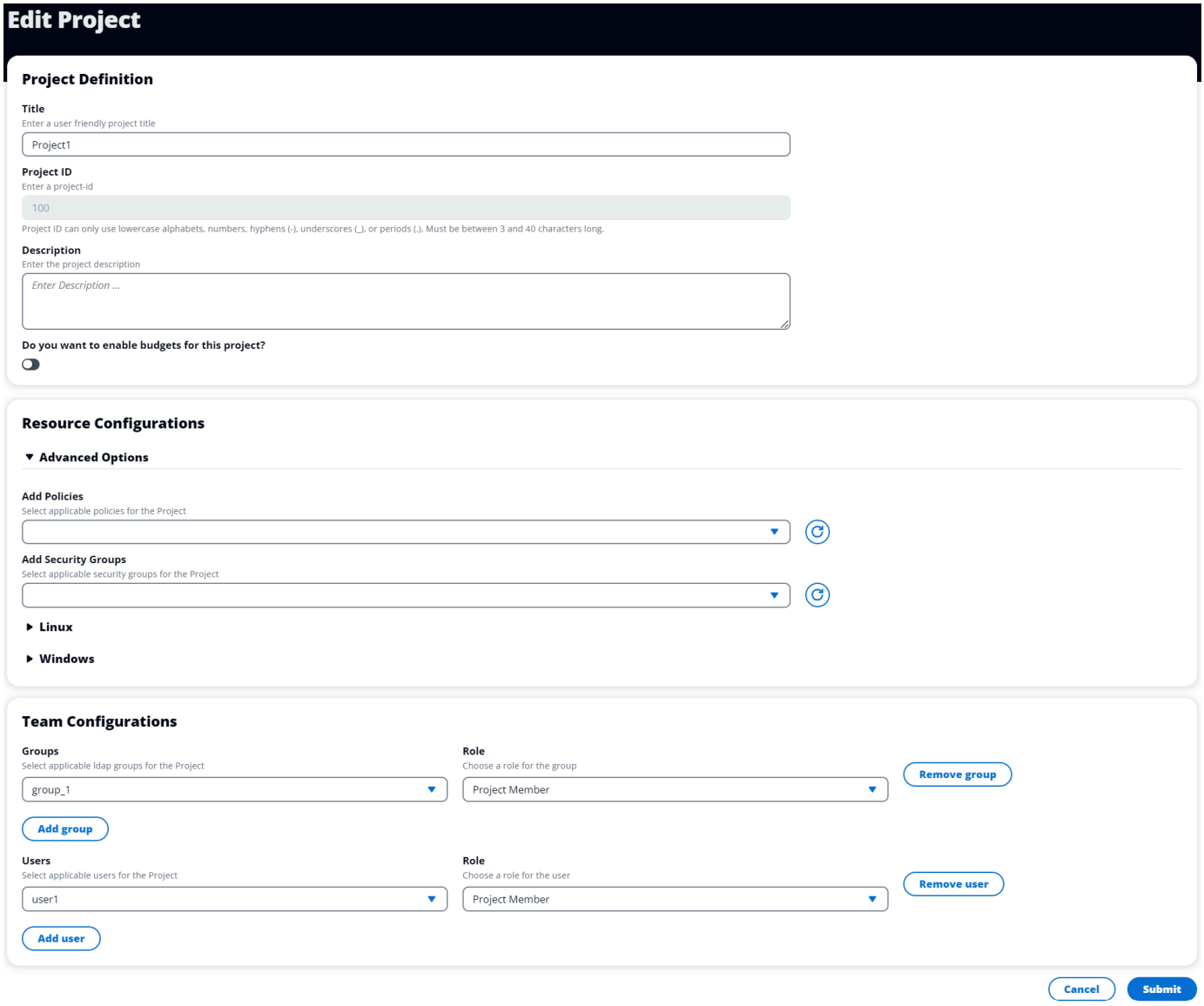
有关高级选项的信息，请参阅添加启动模板。

3. （可选）为项目开启预算。有关预算的更多信息，请参阅成本监测和控制。
4. 为用户 and/or 组分配相应的角色（“项目成员”或“项目所有者”）。默认权限配置文件有关每个角色可以采取的操作，请参阅。
5. 选择提交。



编辑项目

1. 在项目列表中选择一个项目。
2. 从 “操作” 菜单中选择 “编辑项目”。
3. 输入您的更新。如果您打算启用预算，请参阅，了解成本监测和控制更多信息。有关高级选项的信息，请参阅添加启动模板。
4. 选择提交。



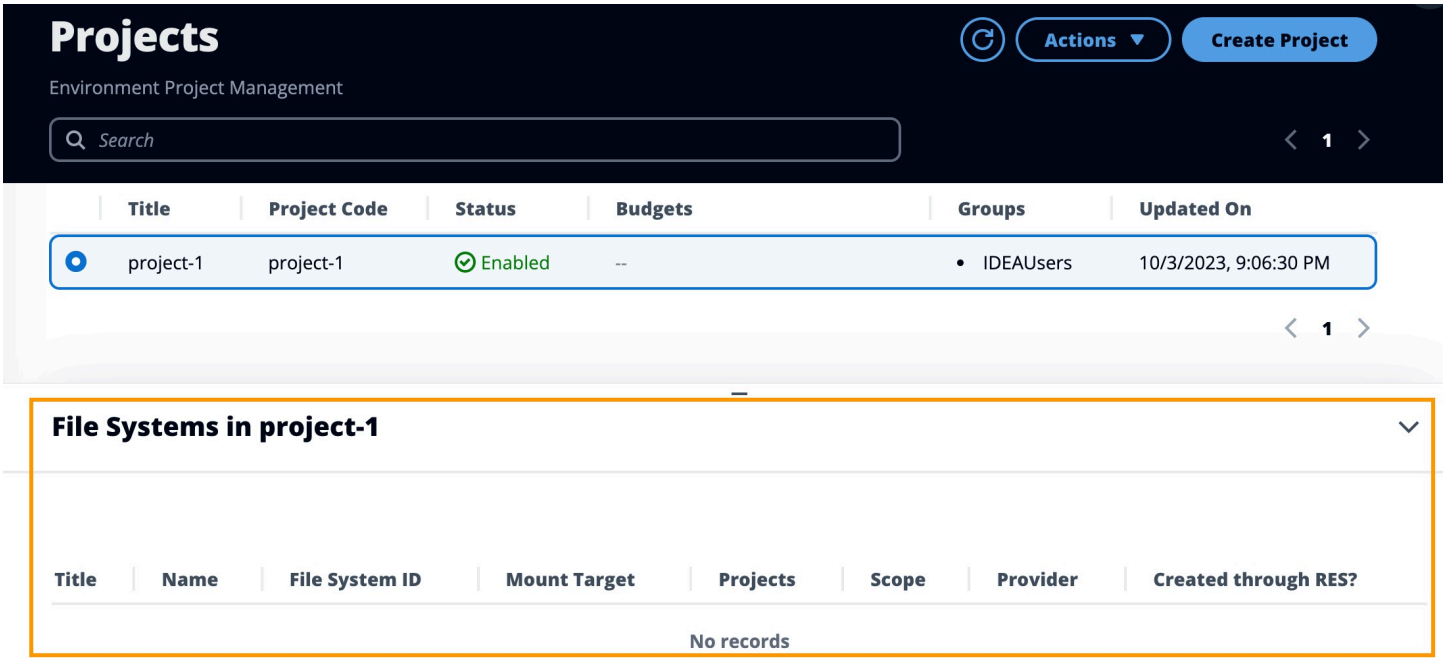
在项目中添加或移除标签

项目标签将为在该项目下创建的所有实例分配标签。

1. 在项目列表中选择一个项目。
2. 从 “操作” 菜单中选择 “更新标签”。
3. 选择 “添加标签”，然后为 Key 输入一个值。
4. 要移除标签，请选择要移除的标签旁边的 “移除”。

查看与项目关联的文件系统

选择项目后，您可以展开屏幕底部的 “文件系统” 窗格以查看与该项目关联的文件系统。



添加启动模板

创建或编辑项目时，您可以使用项目配置中的高级选项添加启动模板。启动模板为项目中的所有 VDI 实例提供了其他配置，例如安全组、IAM 策略和启动脚本。

添加策略

您可以添加 IAM 策略来控制在您的项目下部署的所有实例的 VDI 访问权限。要加入策略，请使用以下键值对标记该策略：

```
res:Resource/vdi-host-policy
```

有关 IAM 角色的更多信息，请参阅 I AM 中的策略和权限。

添加安全组

您可以添加安全组来控制项目下所有 VDI 实例的出口和入口数据。要加入安全组，请使用以下键值对标记该安全组：

```
res:Resource/vdi-security-group
```

有关安全组的更多信息，请参阅 Amazon VPC 用户指南中的使用安全组控制 AWS 资源流量。

添加启动脚本

您可以添加启动脚本，这些脚本将在项目中的所有 VDI 会话中启动。RES 支持 Linux 和 Windows 的脚本初始化。要启动脚本，您可以选择以下任一选项：

VDI 启动时运行脚本

在任何 RES 配置或安装运行之前，此选项在 VDI 实例的开头启动脚本。

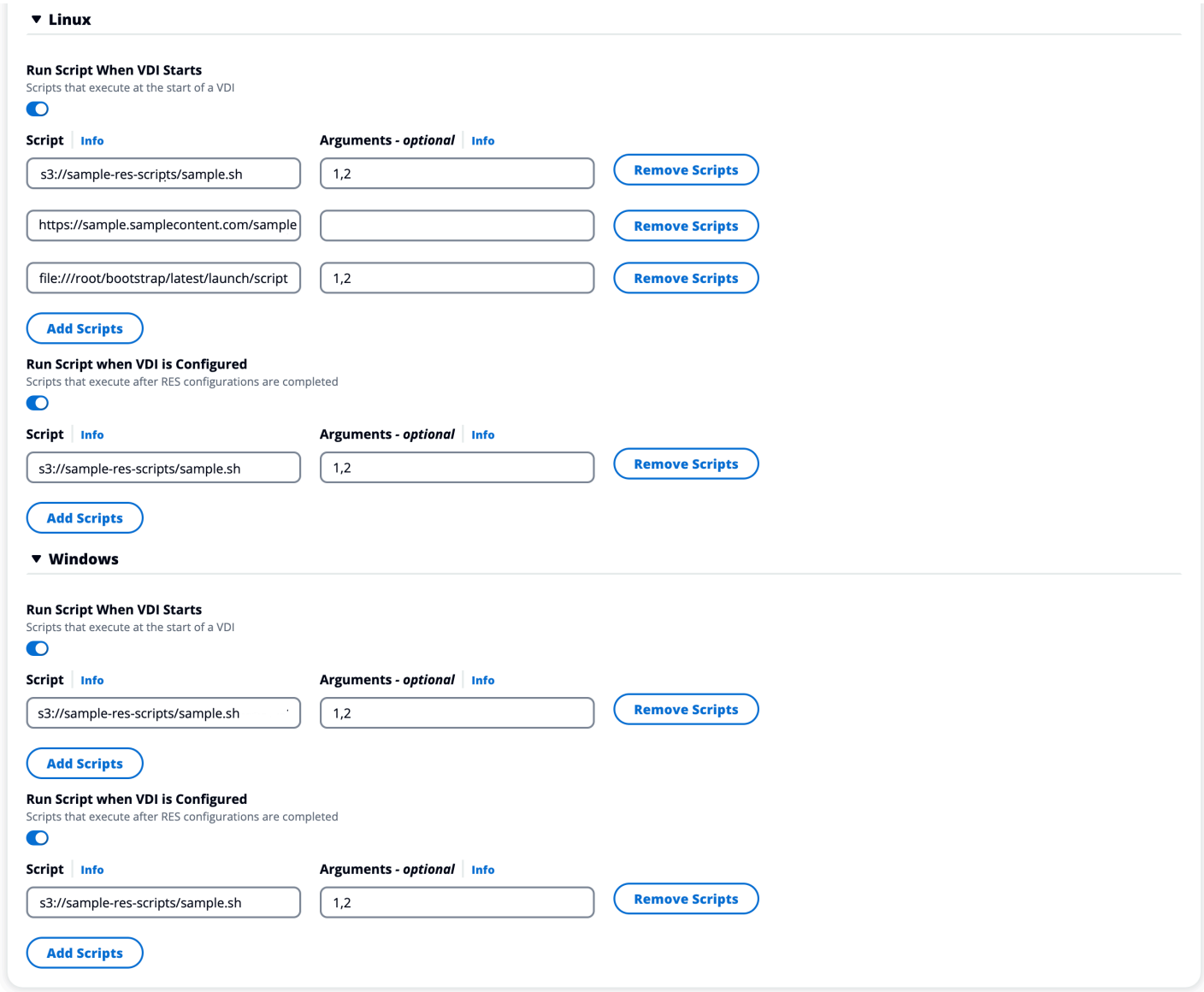
配置 VDI 后运行脚本

此选项在 RES 配置完成后启动脚本。

脚本支持以下选项：

脚本配置	示例
S3 URI	s3://bucketname/script.sh
HTTPS URL	https://sample.samplecontent.com/sample
本地文件	文件:///.sh user/scripts/example

对于参数，请提供用逗号分隔的所有参数。

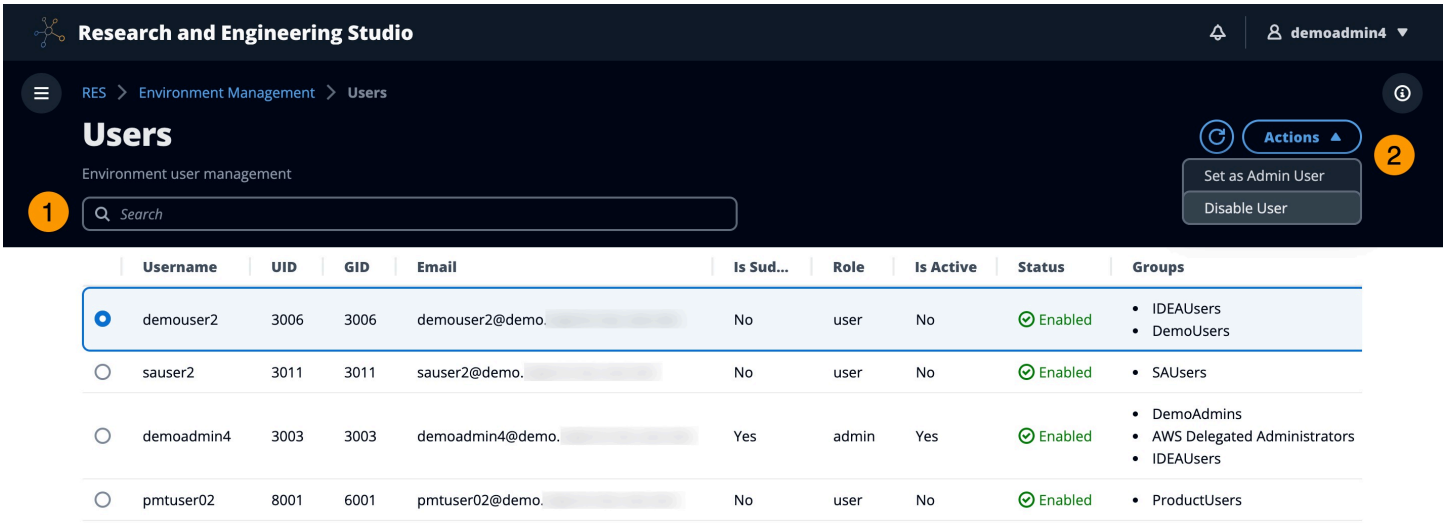


项目配置示例

Users

从您的活动目录同步的所有用户都将显示在 “用户” 页面上。在配置产品期间，用户由群集管理员用户同步。有关初始用户配置的更多信息，请参阅配置指南。

> **Note**
>
> 管理员只能为活跃用户创建会话。默认情况下，所有用户在登录产品环境之前都将处于非活动状态。如果用户处于非活动状态，请在为他们创建会话之前要求他们登录。

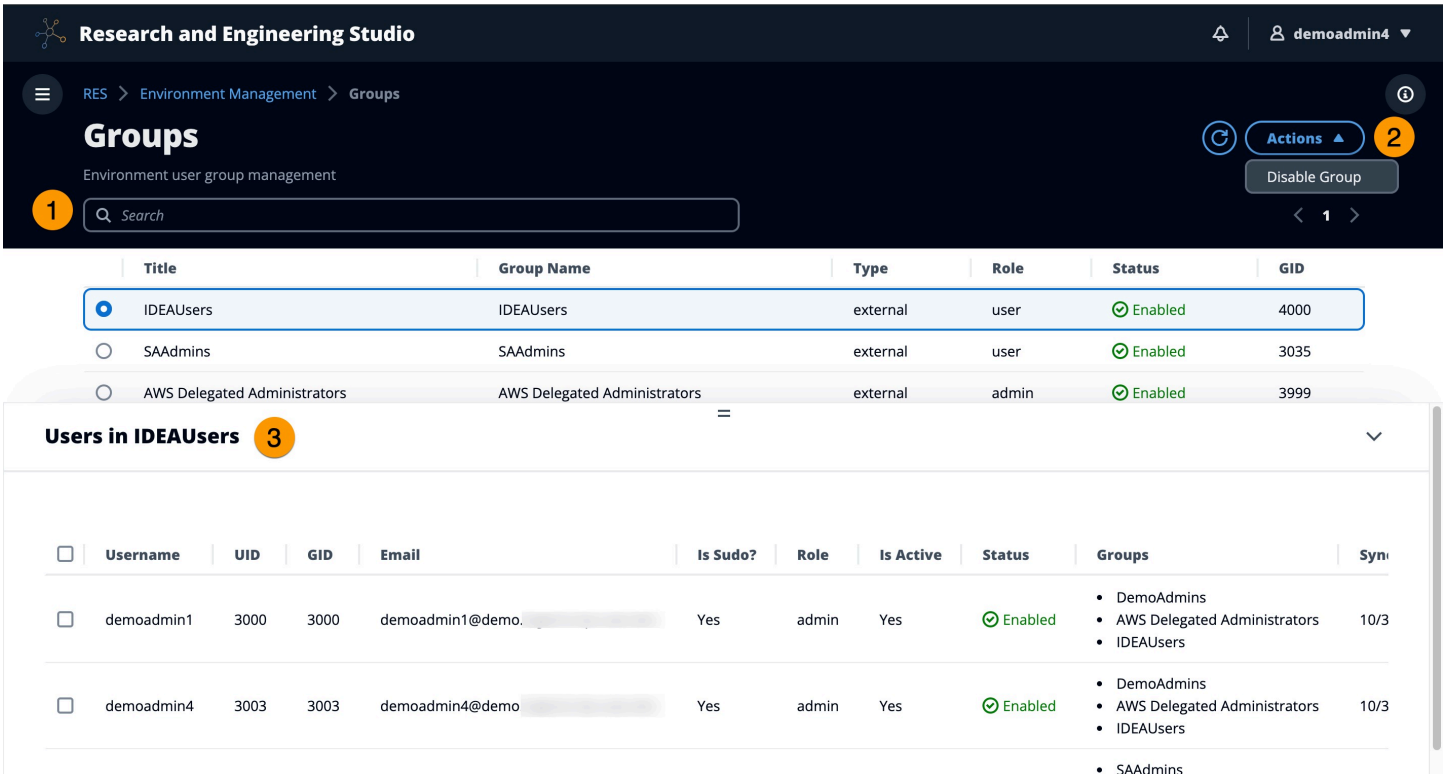


在 “用户” 页面上，您可以：

1. 搜索用户。
2. 选择用户名后，使用 “操作” 菜单可以：
   a. 设置为管理员用户
   b. 禁用用户

组

从活动目录同步的所有群组都显示在 “群组” 页面上。有关组配置和管理的更多信息，请参阅配置指南。



在“群组”页面上，您可以：

1. 搜索用户组。
2. 选择用户组后，使用“操作”菜单禁用或启用该群组。
3. 选择用户组后，您可以展开屏幕底部的“用户”窗格以查看该组中的用户。

权限配置文件

概览

Research and Engineering Studio (RES) 允许管理用户创建自定义权限配置文件，向选定的用户授予管理他们所参与的项目的额外权限。每个项目都有两个默认权限配置文件 —— “项目成员”和“项目所有者”，可以在部署后对其进行自定义。

目前，管理员可以使用权限配置文件授予两个权限集合：

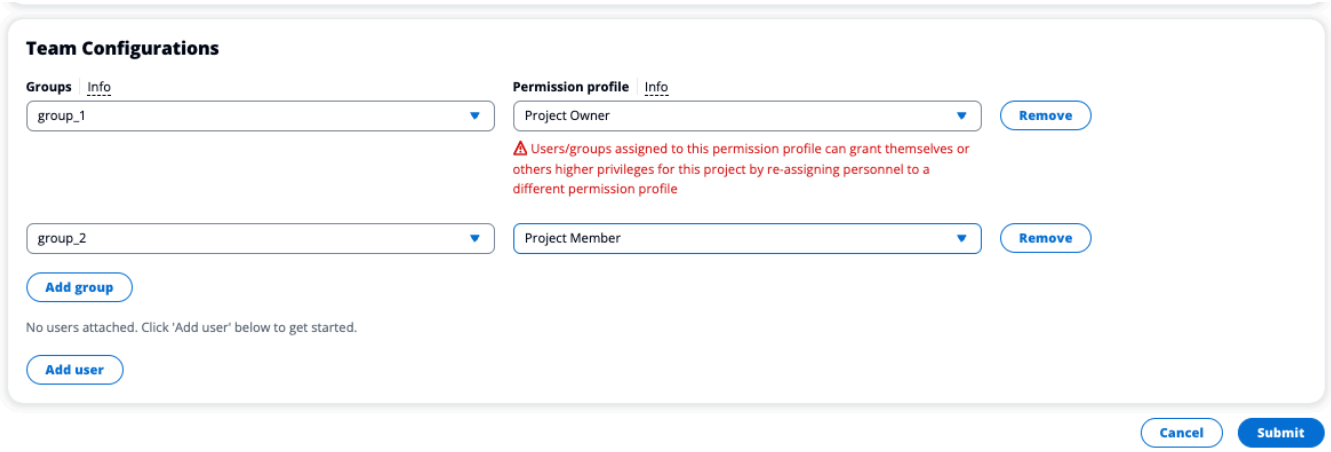
1. 项目管理权限，包括“更新项目成员资格”（允许指定用户将其他用户和组添加到项目或从项目中移除）和“更新项目状态”（允许指定用户启用或禁用项目）。
2. VDI 会话管理权限，包括“创建会话”（允许指定用户在其项目中创建 VDI 会话）和“创建/终止其他用户的会话”（允许指定用户在项目中创建或终止其他用户的会话）。

通过这种方式，管理员可以将基于项目的权限委派给其环境中的非管理员。

项目管理权限

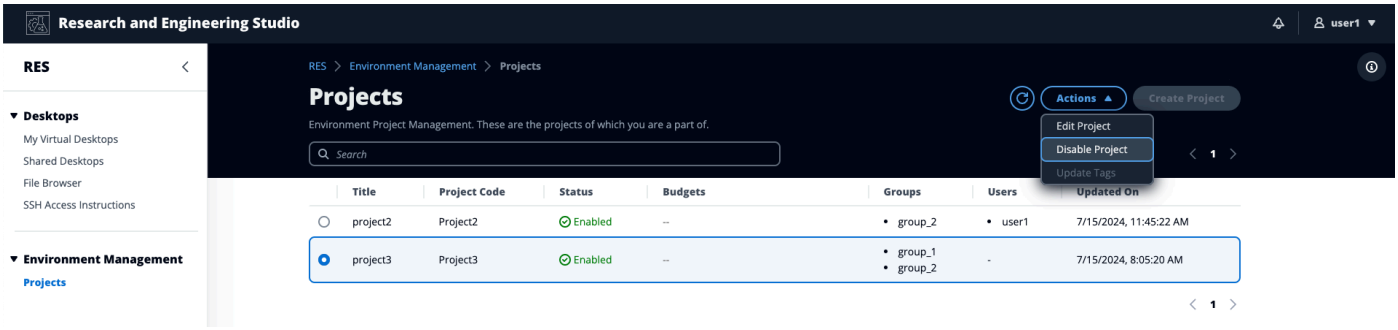
更新项目成员资格

此权限允许获得该权限的非管理员用户在项目中添加和删除用户或组。它还允许他们设置权限配置文件并决定该项目的所有其他用户和群组的访问级别。



更新项目状态

此权限允许获得该权限的非管理员用户使用 “项目” 页面上的 “操作” 按钮启用或禁用项目。

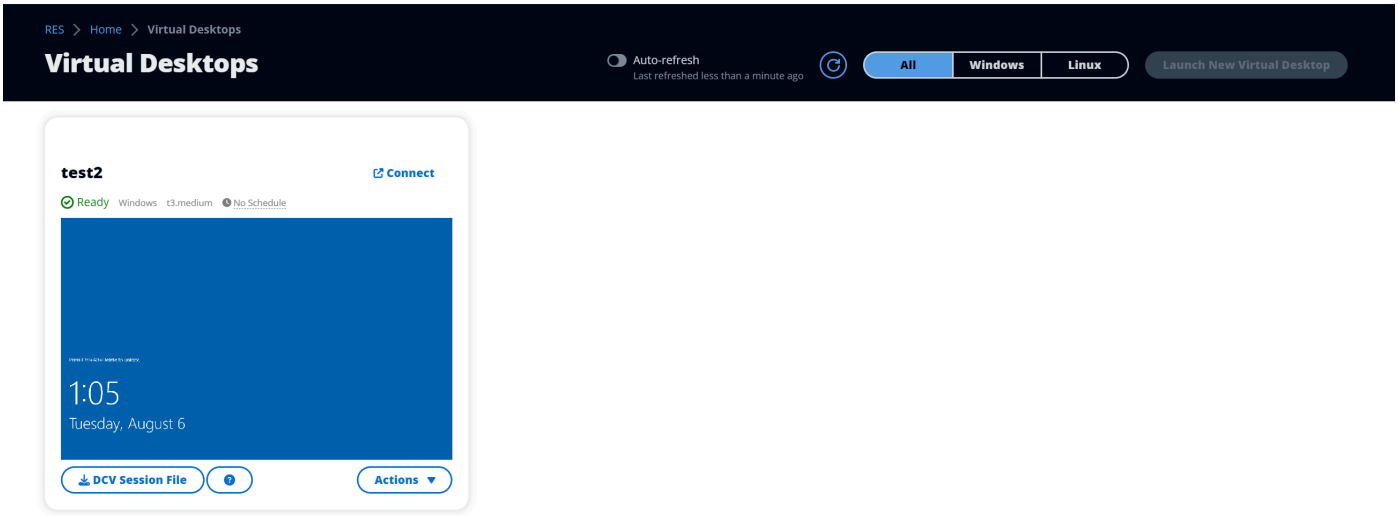


VDI 会话管理权限

创建会话

控制是否允许用户从 “我的虚拟桌面” 页面启动自己的 VDI 会话。禁用此选项可拒绝非管理员用户启动自己的 VDI 会话。用户可以随时停止和终止自己的 VDI 会话。

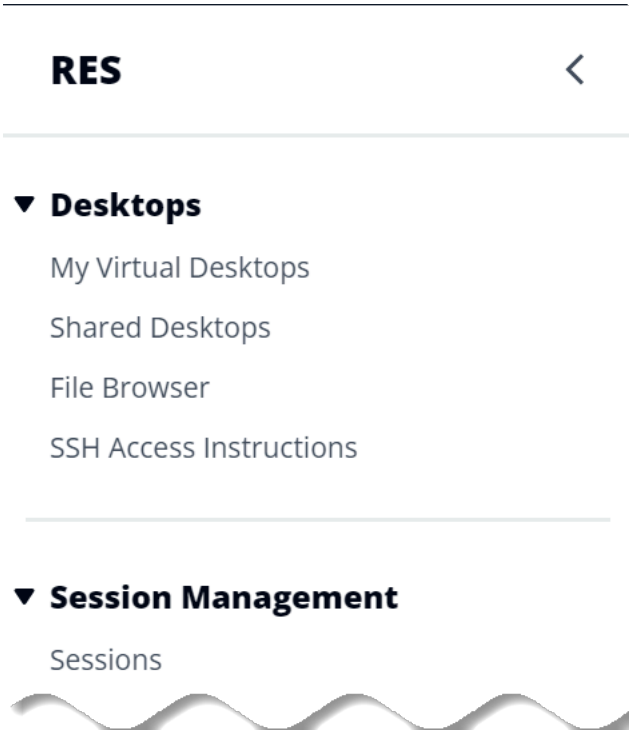
如果非管理员用户无权创建会话，则他们的 “启动新虚拟桌面” 按钮将被禁用，如下所示：



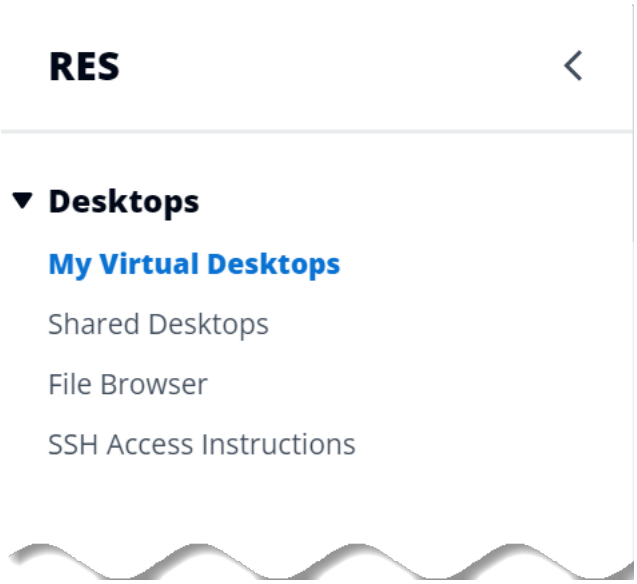
创建或终止其他人的会话

允许非管理员用户从左侧导航窗格访问 “会话” 页面。这些用户将能够在获得此权限的项目中为其他用户启动 VDI 会话。

如果非管理员用户有权为其他用户启动会话，则他们的左侧导航窗格将在会话管理下方显示会话链接，如下所示：



如果非管理员用户无权为其他人创建会话，则他们的左侧导航窗格将不会显示会话管理，如下所示：

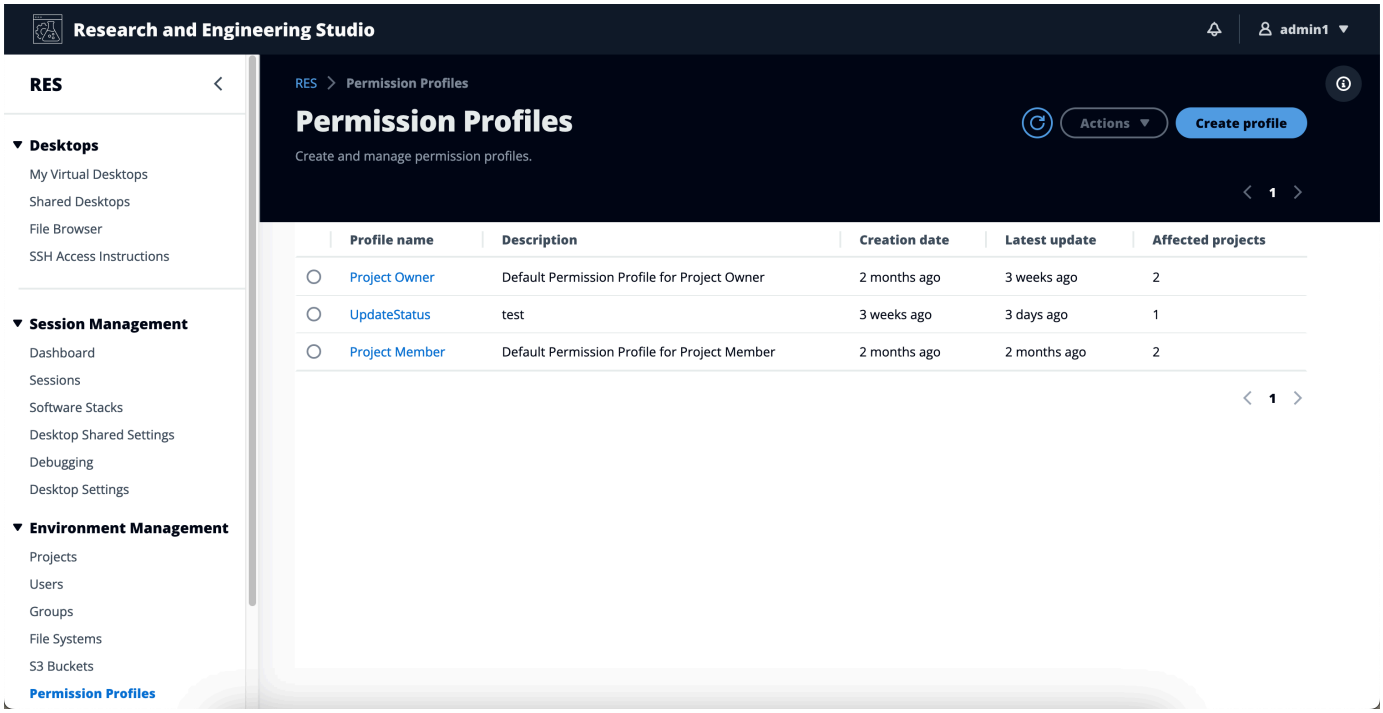


管理权限配置文件

作为 RES 管理员，您可以执行以下操作来管理权限配置文件。

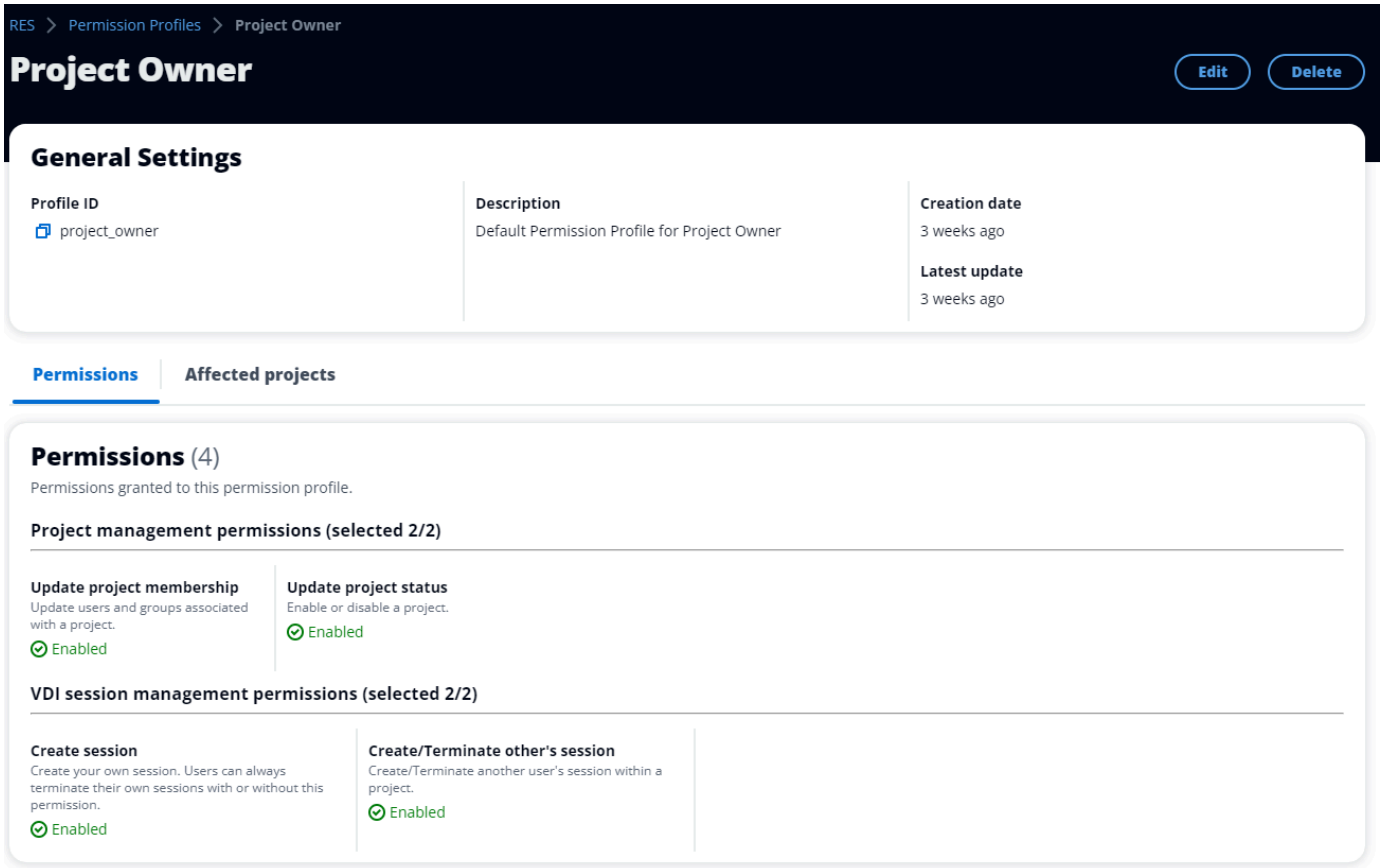
列出权限配置文件

- 在 Research and Engineering Studio 控制台页面上，选择左侧导航窗格中的权限配置文件。在此页面上，您可以创建、更新、列出、查看和删除权限配置文件。

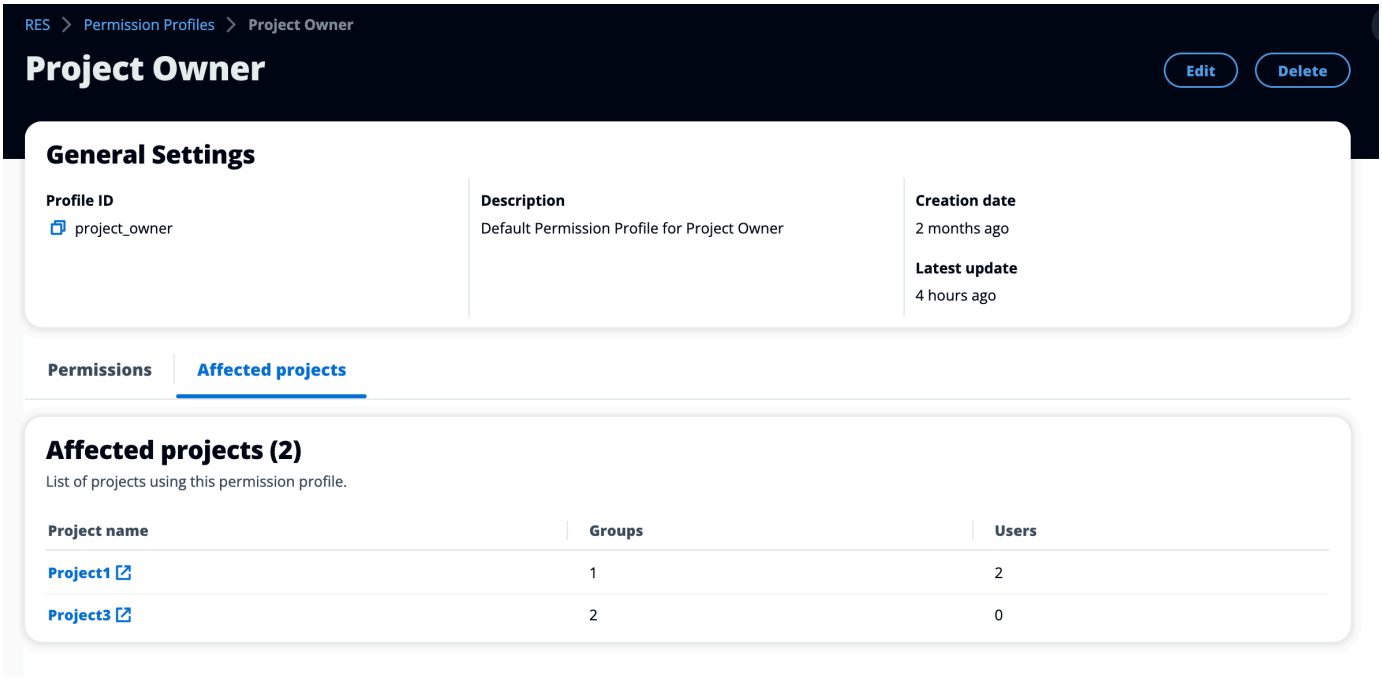


查看权限配置文件

1. 在 “权限配置文件” 主页面上，选择要查看的权限配置文件的名称。在此页面上，您可以编辑或删除选定的权限配置文件。

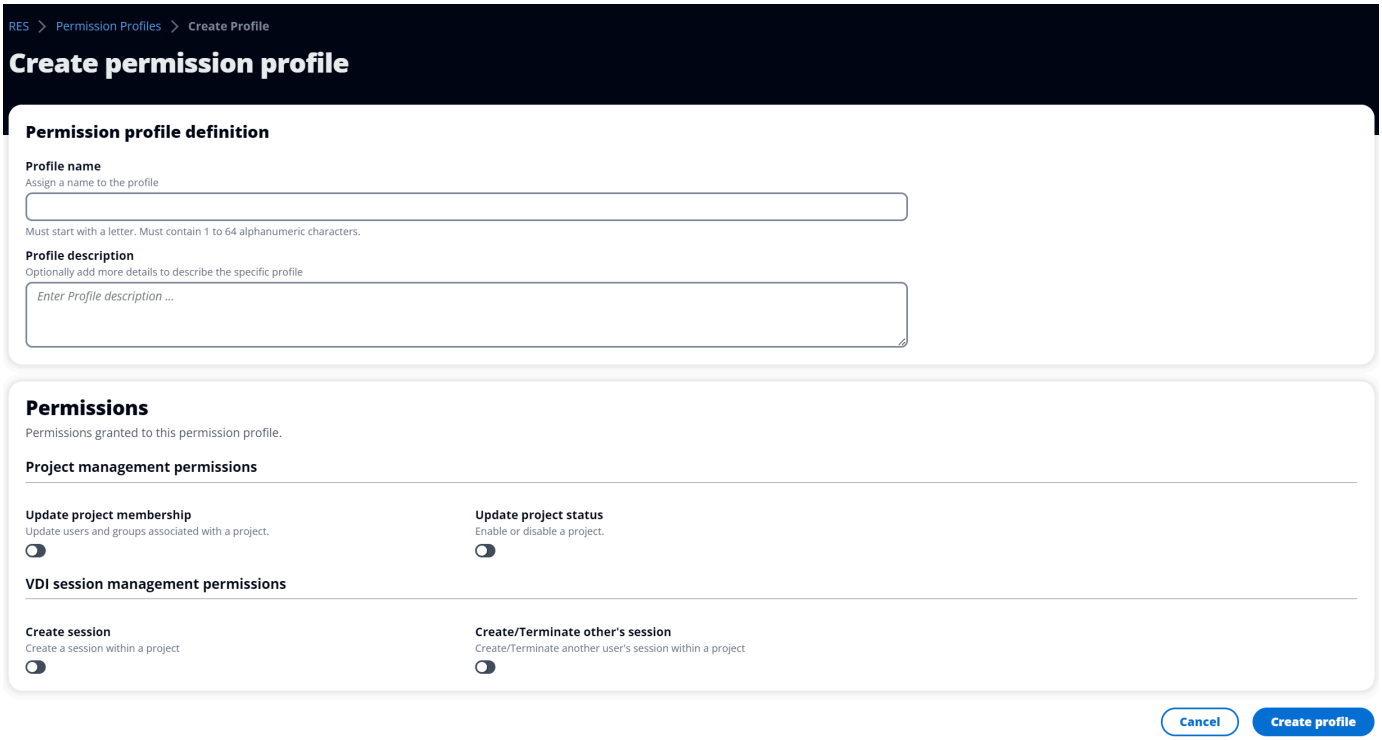


2. 选择 “受影响的项目” 选项卡，查看当前使用权限配置文件的项目。



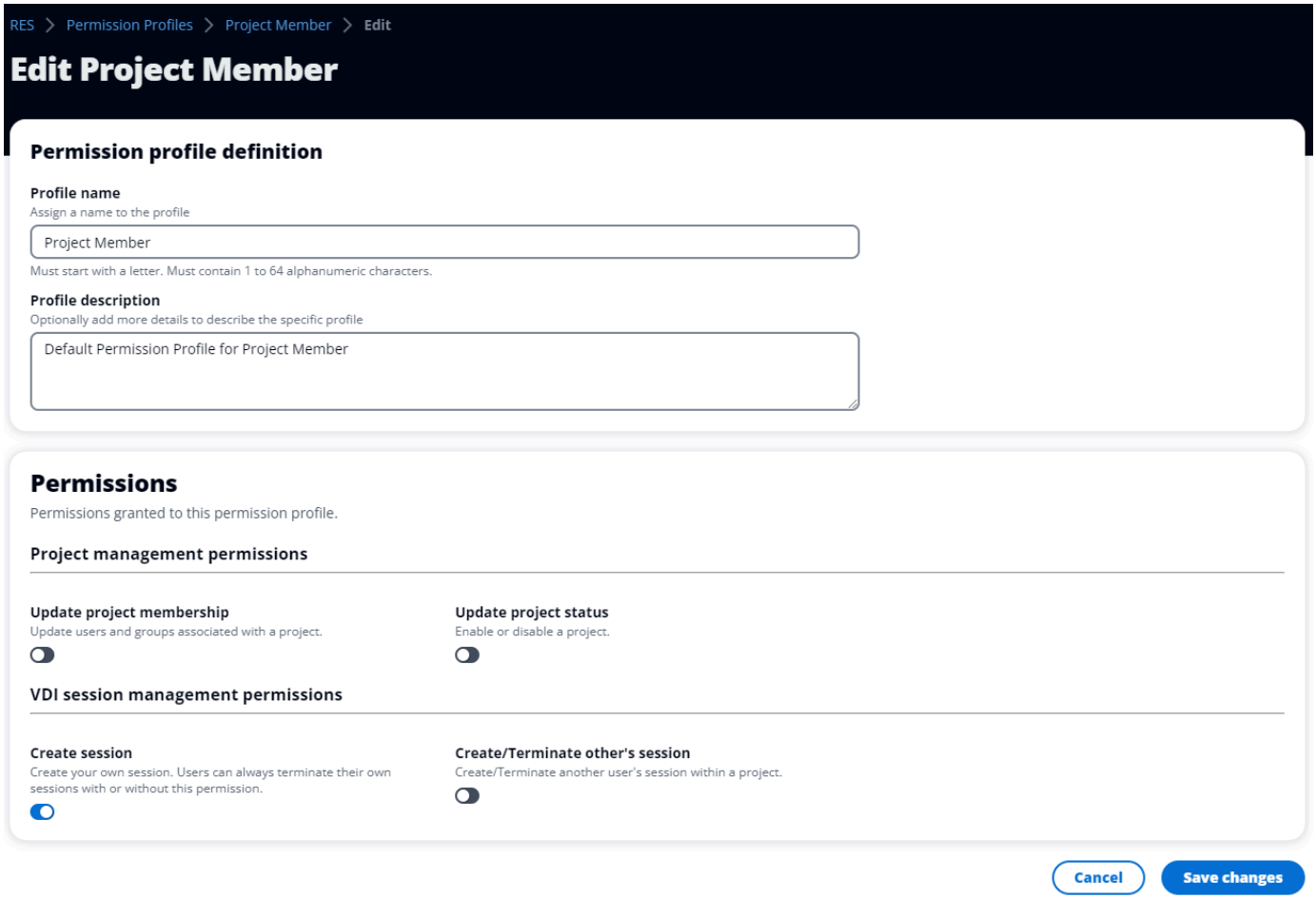
创建权限配置文件

1. 在权限配置文件主页面上，选择创建配置文件以创建权限配置文件。
2. 输入权限配置文件名称和描述，然后选择要向分配给该配置文件的用户或组授予的权限。



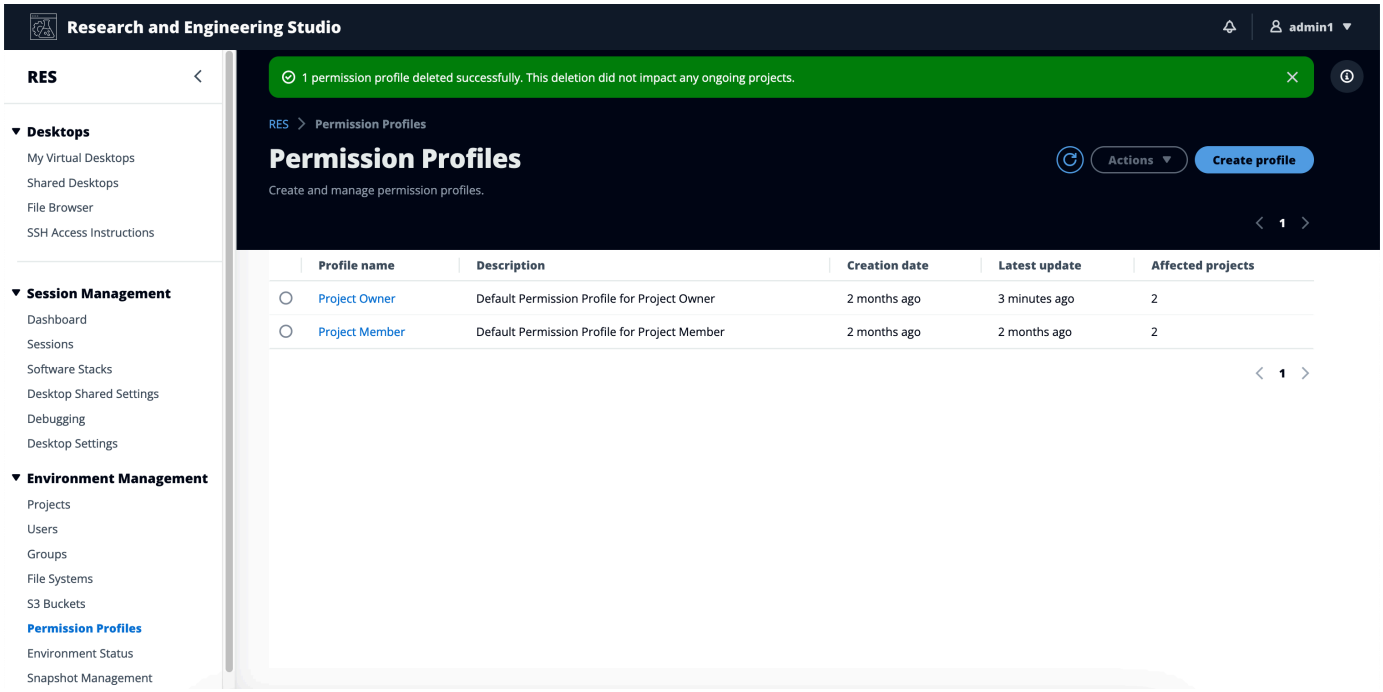
编辑权限配置文件

- 在权限配置文件主页面上，单击配置文件旁边的圆圈选择该配置文件，选择操作，然后选择编辑配置文件以更新该权限配置文件。



删除权限配置文件

- 在 “权限配置文件” 主页面上，单击配置文件旁边的圆圈选择该配置文件，选择操作，然后选择删除配置文件。您不能删除任何现有项目使用的权限配置文件。



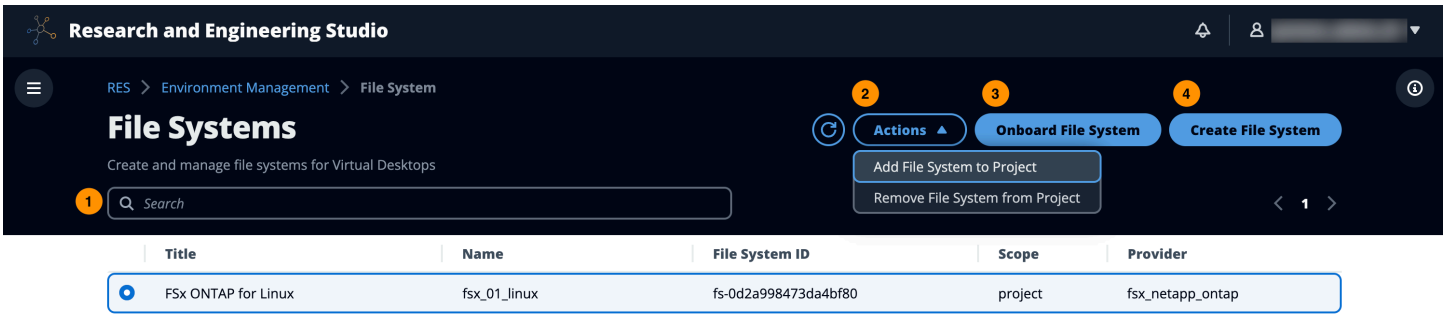
默认权限配置文件

每个 RES 项目都有两个默认权限配置文件，全局管理员可以对其进行配置。（此外，全局管理员可以为项目创建和修改新的权限配置文件。）下表显示了默认权限配置文件（“项目成员”和“项目所有者”）允许的权限。权限配置文件及其授予项目选定用户的权限仅适用于他们所属的项目；全局管理员是超级用户，他们在所有项目中拥有以下所有权限。

权限	描述	项目成员	项目所有者	
创建会话	创建自己的会话。无论是否拥有此权限，用户都可以随时停止和终止自己的会话。	X 形	X 形	
创建/终止其他人的会话	在项目中创建或终止其他用户的会话。		X 形	

权限	描述	项目成员	项目所有者	
更新项目成员资格	更新与项目关联的用户和群组。		X 形	
更新项目状态	启用或禁用项目。		X 形	

文件系统



在 “文件系统” 页面上，您可以：

1. 搜索文件系统。
2. 选择文件系统后，使用操作菜单执行以下操作：
   a. 将文件系统添加到项目中
   b. 从项目中移除文件系统
3. 载入新的文件系统。
4. 创建文件系统。
5. 选择文件系统后，您可以展开屏幕底部的窗格以查看文件系统的详细信息。

创建文件系统

1. 选择创建文件系统。
2. 输入新文件系统的详细信息。
3. IDs 从 VPC 提供子网。您可以 IDs 在 “环境管理” > “设置” > “网络” 选项卡中找到。
4. 选择提交。

Create new File System

Title

Enter a user friendly file system title

Eg. EFS 01

Name

Enter a file system name

File System name can only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

File System Provider

Select applicable file system type

EFS

Projects

Select applicable project

Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

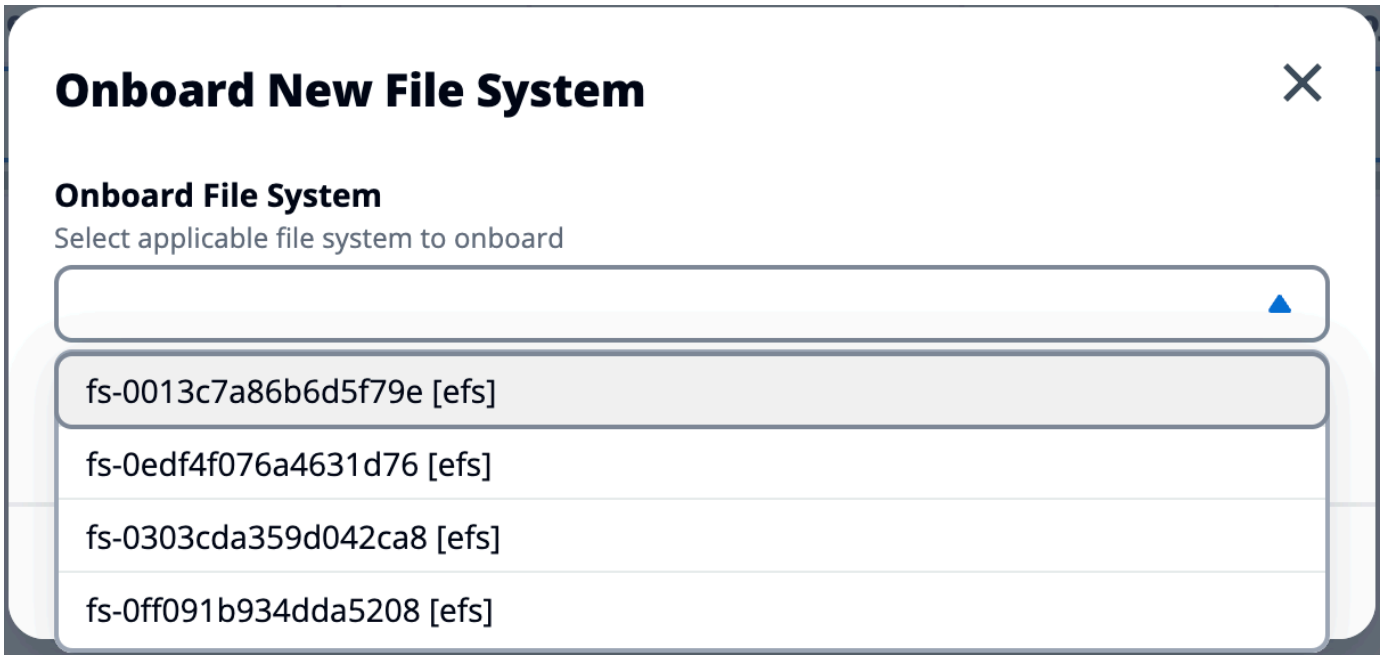
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

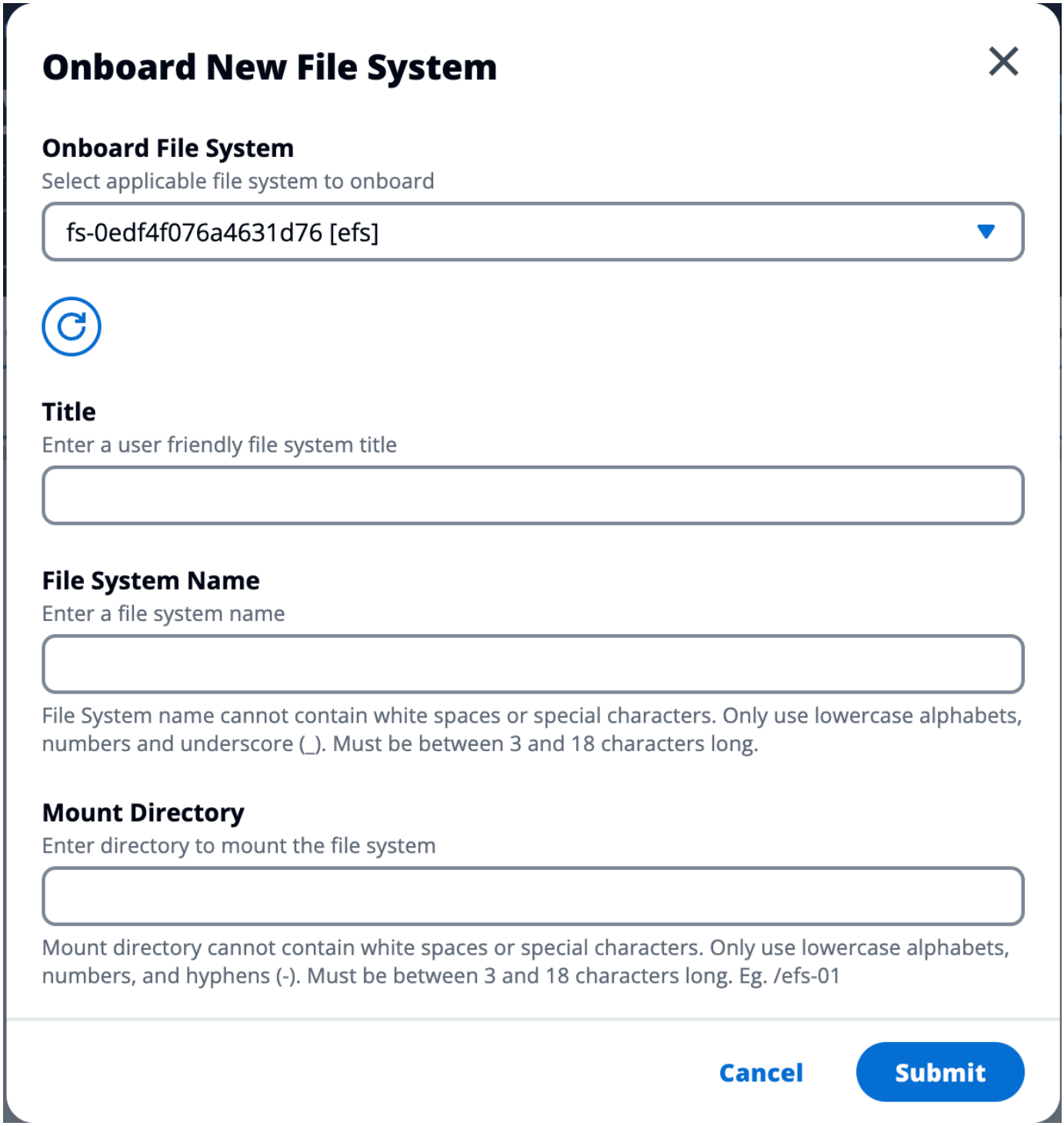
Enter directory to mount the file system

加载文件系统

1. 选择 “板载文件系统”。
2. 从下拉列表中选择一个文件系统。模态将扩展，并添加更多细节条目。

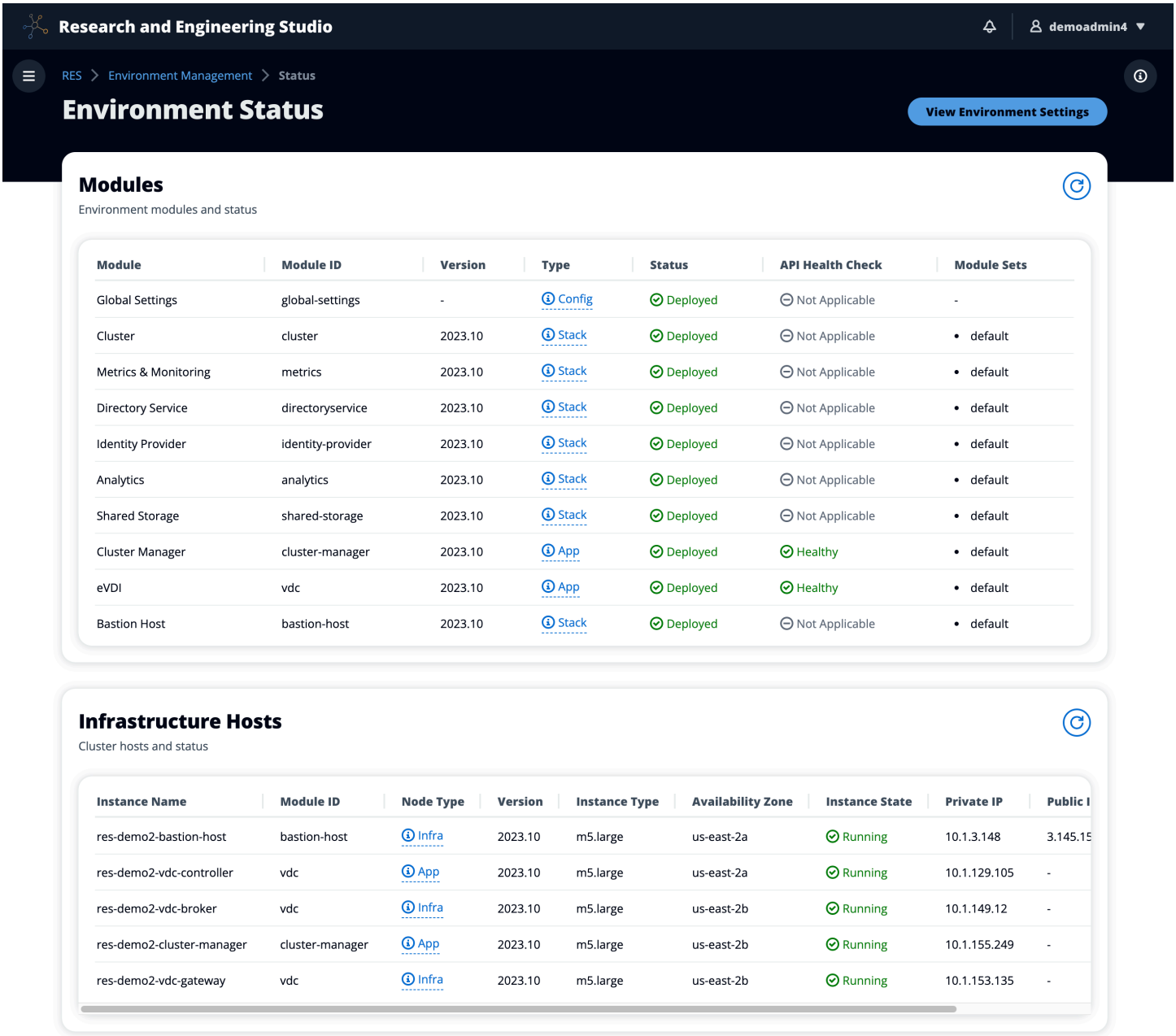


3. 输入文件系统详细信息。
4. 选择提交。



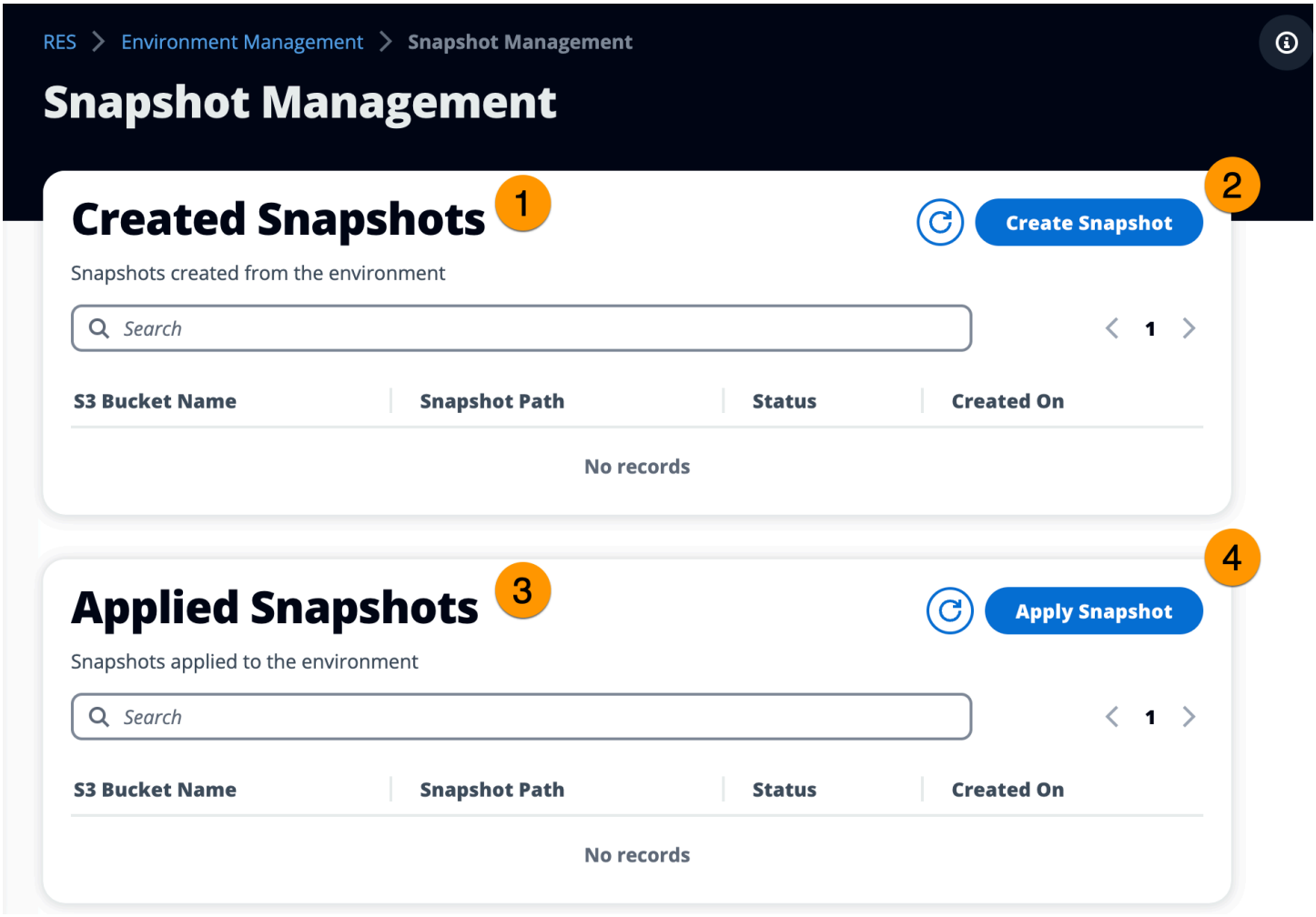
环境状态

“环境状态” 页面显示产品中已部署的软件和主机。它包括诸如软件版本、模块名称和其他系统信息之类的信息。



快照管理

快照管理简化了在环境之间保存和迁移数据的过程，从而确保了一致性和准确性。使用快照，您可以保存环境状态并将数据迁移到具有相同状态的新环境中。



在快照管理页面上，您可以：

1. 查看所有已创建的快照及其状态。
2. 创建快照。在创建快照之前，您需要创建一个具有相应权限的存储桶。
3. 查看所有已应用的快照及其状态。
4. 应用快照。

创建快照

在创建快照之前，您必须为 Amazon S3 存储桶提供必要的权限。有关创建存储桶的信息，请参阅创建存储桶。我们建议启用存储桶版本控制和服务器访问日志记录。配置后，可以在存储桶的“属性”选项卡中启用这些设置。

> **Note**
>
> 此 Amazon S3 存储桶的生命周期不会在产品内进行管理。您需要通过控制台管理存储桶的生命周期。

要向存储桶添加权限，请执行以下操作：

1. 从 Bucket s 列表中选择您创建的存储桶。
2. 选择 Permissions（权限）选项卡。
3. 在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。
4. 将以下语句添加到存储桶策略中。将这些值替换为您自己的值：

   - AWS_ACCOUNT_ID
   - RES_环境名称
   - AWS_REGION
   - S3_BUCKET_NAME

   > **Important**
   >
   > 支持有限的版本字符串 AWS。有关更多信息，请参阅 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html。

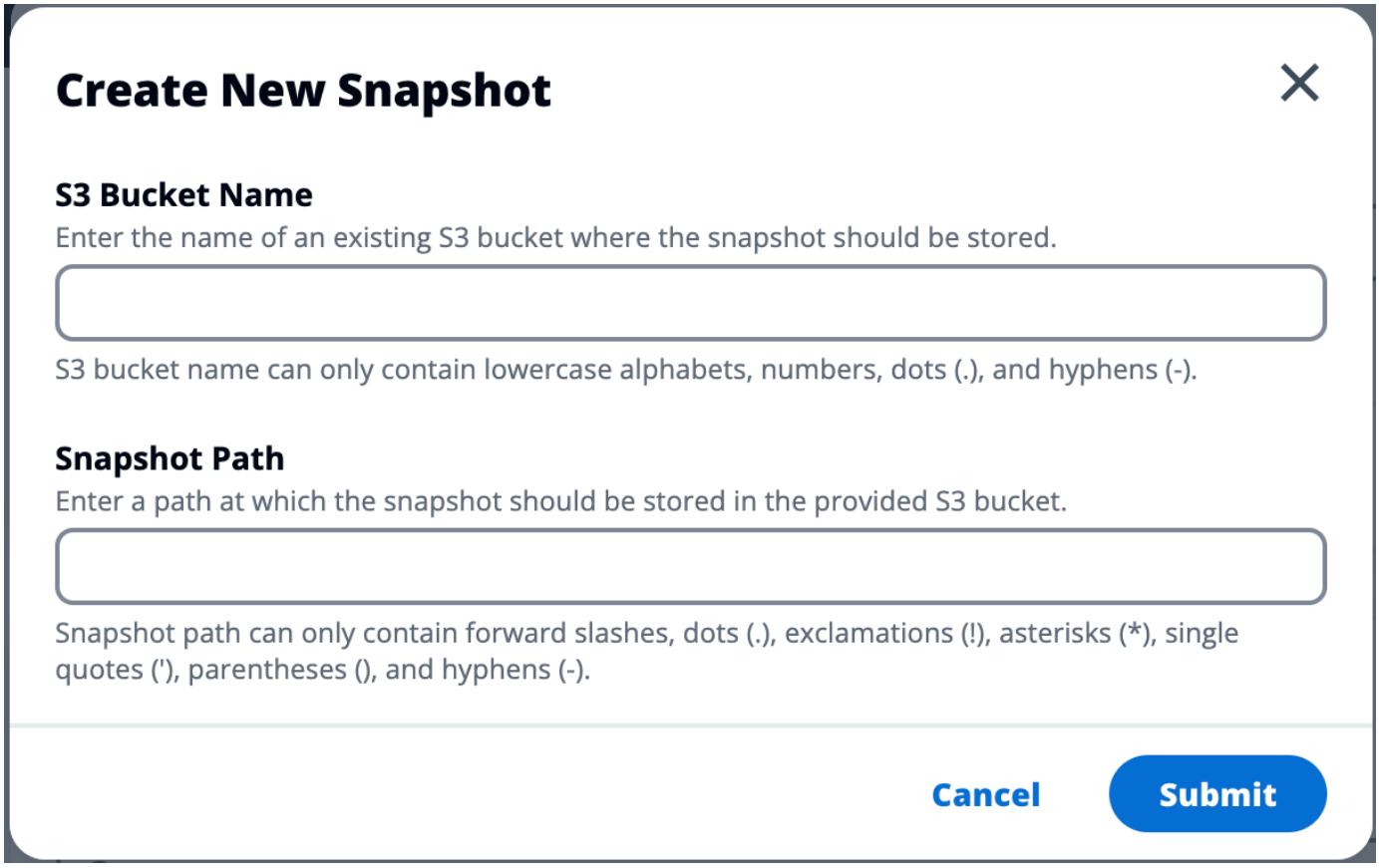
   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

要创建快照，请执行以下操作：

1. 选择创建快照。
2. 输入您创建的 Amazon S3 存储桶的名称。
3. 输入您希望将快照存储在存储桶中的路径。例如 **october2023/23**。
4. 选择提交。



5. 五到十分钟后，在“快照”页面上选择“刷新”以查看状态。在状态从“正在进行中”变为“已完成”之前，快照将无效。

应用快照

创建环境快照后，可以将该快照应用到新环境以迁移数据。您需要向存储桶添加新策略，允许环境读取快照。

应用快照会将用户权限、项目、软件堆栈、权限配置文件和文件系统等数据及其关联复制到新环境。不会复制用户会话。应用快照时，它会检查每条资源记录的基本信息，以确定其是否已经存在。对于重复的记录，快照会跳过在新环境中创建资源。对于相似的记录，例如共享名称或密钥，但其他基本资源信息各不相同，它将使用以下约定创建具有修改名称和密钥的新记录：`RecordName_SnapshotRESVersion_ApplySnapshotID`。`ApplySnapshotID`看起来像时间戳，用于标识应用快照的每次尝试。

在快照应用程序期间，快照会检查资源的可用性。不会创建新环境中不可用的资源。对于具有依赖资源的资源，快照会检查依赖资源的可用性。如果依赖资源不可用，它将创建没有依赖资源的主资源。

如果新环境未达到预期或出现故障，则可以查看 CloudWatch 日志组中的日志/res-<env-name>/cluster-manager以了解详细信息。每个日志都将有 [应用快照] 标签。应用快照后，您可以从the section called “快照管理”页面查看其状态。

要向存储桶添加权限，请执行以下操作：

1. 从 Bucket s 列表中选择您创建的存储桶。
2. 选择 Permissions（权限）选项卡。
3. 在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。
4. 将以下语句添加到存储桶策略中。将这些值替换为您自己的值：

   - AWS_ACCOUNT_ID
   - RES_环境名称
   - AWS_REGION
   - S3_BUCKET_NAME

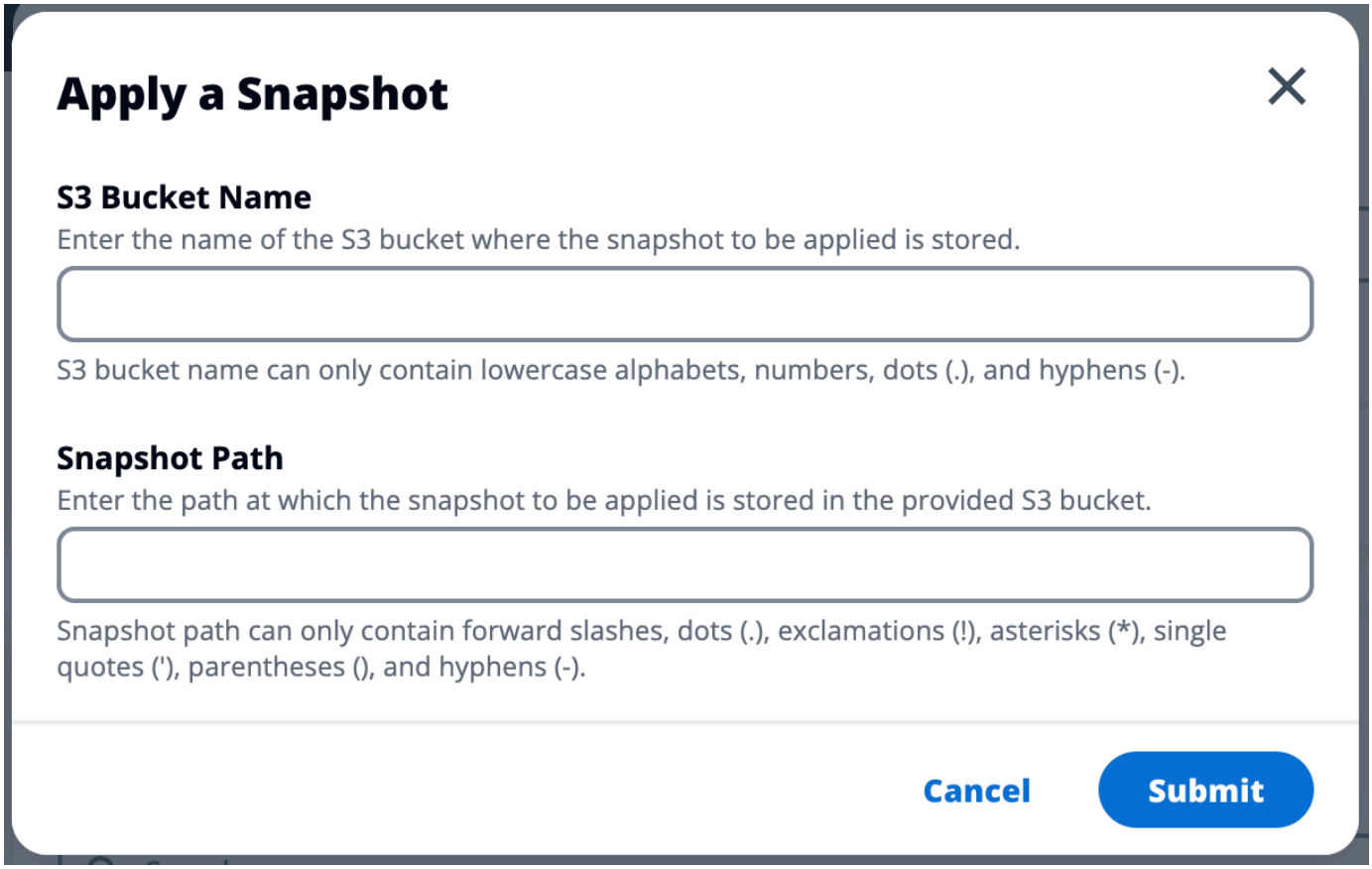
   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
```

```
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

要应用快照：

1. 选择 “应用快照”。
2. 输入包含快照的 Amazon S3 存储桶的名称。
3. 输入存储桶内快照的文件路径。
4. 选择提交。



5. 五到十分钟后，在 “快照管理” 页面上选择 “刷新” 以检查状态。

环境设置

环境设置显示产品配置的详细信息，例如：

- 常规

  显示配置产品的用户的管理员用户名和电子邮件等信息。您可以编辑门户网站标题和版权文本。

- 身份提供商

  显示诸如单点登录状态之类的信息。

- 网络

  显示 VPC ID、访问前缀列表 IDs 。

- 目录服务

  显示用户名和密码的活动目录设置和服务帐户密钥管理器 ARN。

Amazon S3 存储桶

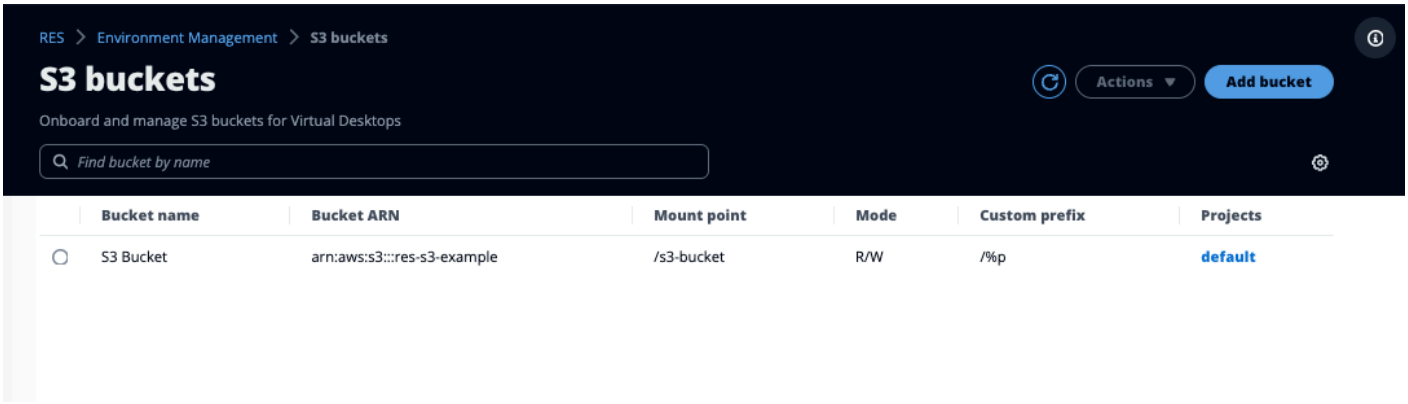
主题

挂载 Amazon S3 存储桶

研究与工程工作室 (RES) 支持将 Amazon S3 存储桶挂载到 Linux 虚拟桌面基础设施 (VDI) 实例。RES 管理员可以将 S3 存储桶载入 RES，将其附加到项目，编辑其配置，并在 “环境管理” 下的 “S3 存储桶” 选项卡中删除存储桶。

S3 存储桶控制面板提供了可供您使用的已载入 S3 存储桶的列表。在 S3 存储桶控制面板中，您可以：

1. 使用添加存储桶将 S3 存储桶加载到 RES。
2. 选择一个 S3 存储桶，然后使用操作菜单执行以下操作：
   - 编辑存储桶
   - 移除存储桶
3. 使用搜索字段按存储桶名称进行搜索并查找已加载的 S3 存储桶。



添加亚马逊 S3 存储桶

要将 S3 存储桶添加到您的 RES 环境，请执行以下操作：

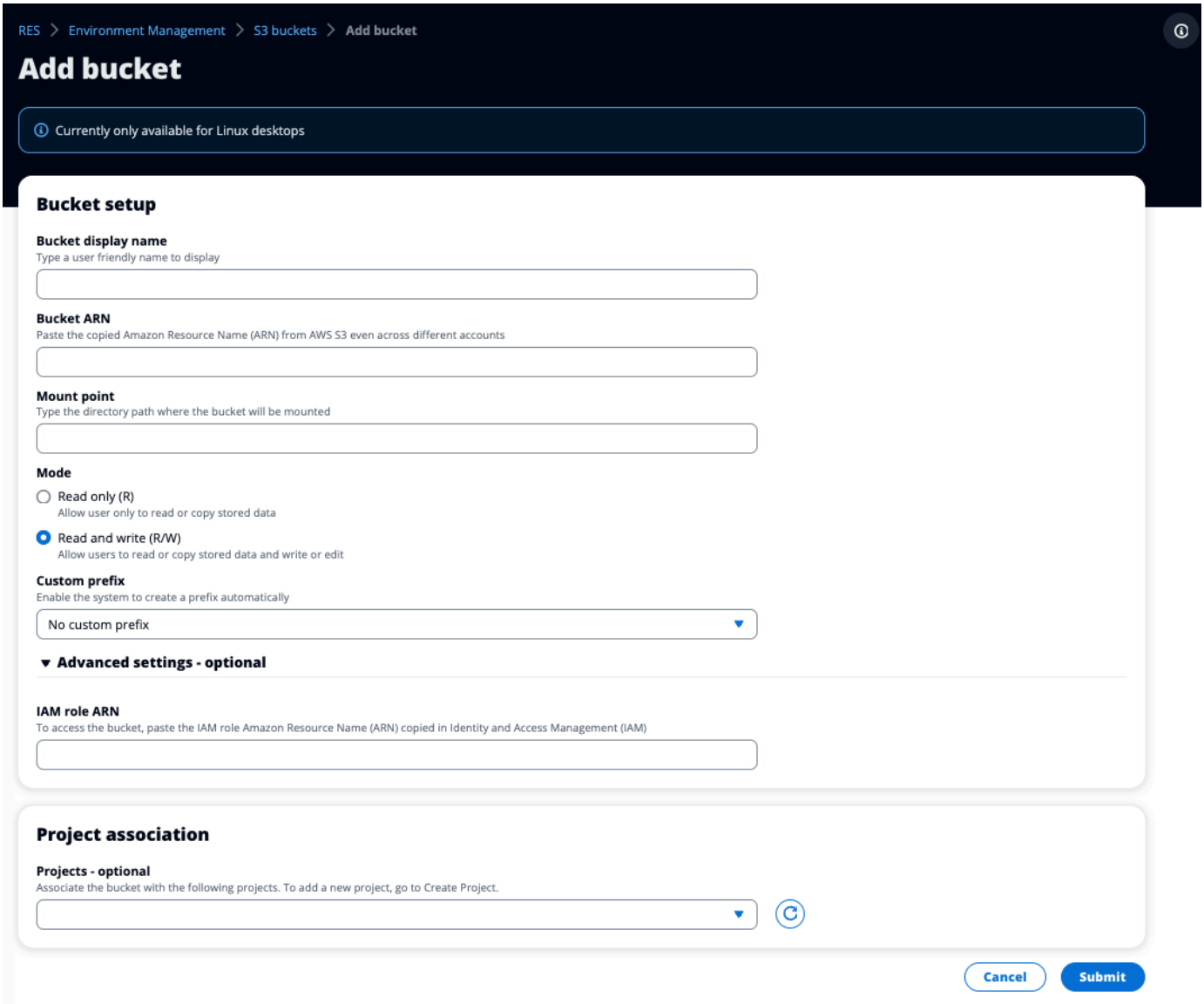
1. 选择 Add bucket (添加存储桶)。
2. 输入存储桶的详细信息，例如存储桶名称、ARN 和挂载点。

> **Important**
>
> - 创建后无法更改所提供的存储桶 ARN、挂载点和模式。
> - 存储桶 ARN 可以包含一个前缀，该前缀会将已加载的 S3 存储桶与该前缀隔离开来。

3. 选择一种加载存储桶的模式。

> **Important**
>
> - 有关数据隔离使用特定模式进行数据隔离的更多信息，请参阅。

4. 在“高级选项”下，您可以提供 IAM 角色 ARN 来挂载存储桶以进行跨账户访问。按照中的跨账户存储桶访问权限步骤创建跨账户访问所需的 IAM 角色。
5. （可选）将存储桶与项目关联，以后可以对其进行更改。但是，无法将 S3 存储桶装载到项目的现有 VDI 会话中。只有在项目与存储桶关联后启动的会话才会挂载存储桶。
6. 选择提交。

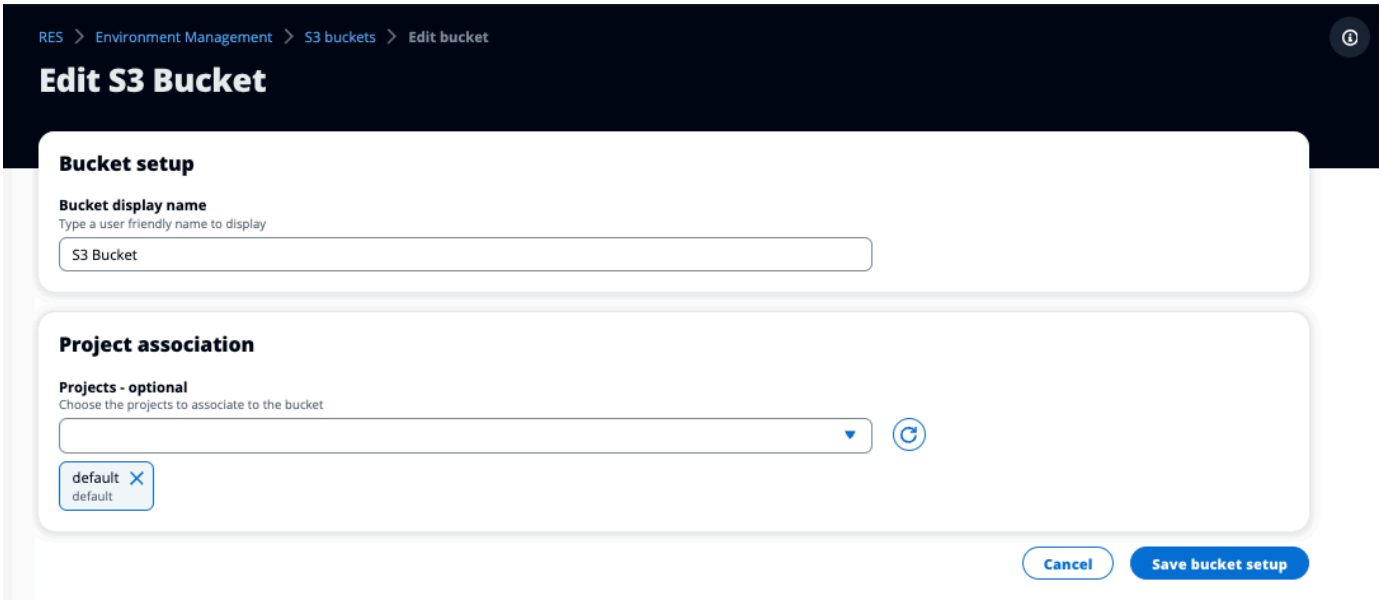


编辑 Amazon S3 存储桶

1. 在 S3 存储桶列表中选择一个 S3 存储桶。
2. 从 “操作” 菜单中选择 “编辑”。
3. 输入您的更新。

> **Important**
>
> - 将项目与 S3 存储桶关联不会将存储桶挂载到该项目的现有虚拟桌面基础架构 (VDI) 实例。只有在项目中启动的 VDI 会话与该存储桶关联后，该存储桶才会装载到该项目中启动的 VDI 会话。
> - 取消项目与 S3 存储桶的关联不会影响 S3 存储桶中的数据，但会导致桌面用户无法访问该数据。

4. 选择保存存储桶设置。



移除亚马逊 S3 存储桶

1. 在 S3 存储桶列表中选择一个 S3 存储桶。
2. 从 “操作” 菜单中选择 “删除”。

> **Important**
>
> - 您必须先从存储桶中移除所有项目关联。
> - 删除操作不会影响 S3 存储桶中的数据。它只会移除 S3 存储桶与 RES 的关联。
> - 移除存储桶将导致现有的 VDI 会话在该会话的凭证到期（大约 1 小时）时无法访问该存储桶中的内容。

数据隔离

将 S3 存储桶添加到 RES 时，您可以选择将存储桶内的数据隔离给特定的项目和用户。在添加存储桶页面上，您可以选择只读 (R) 或读写 (R/W) 模式。

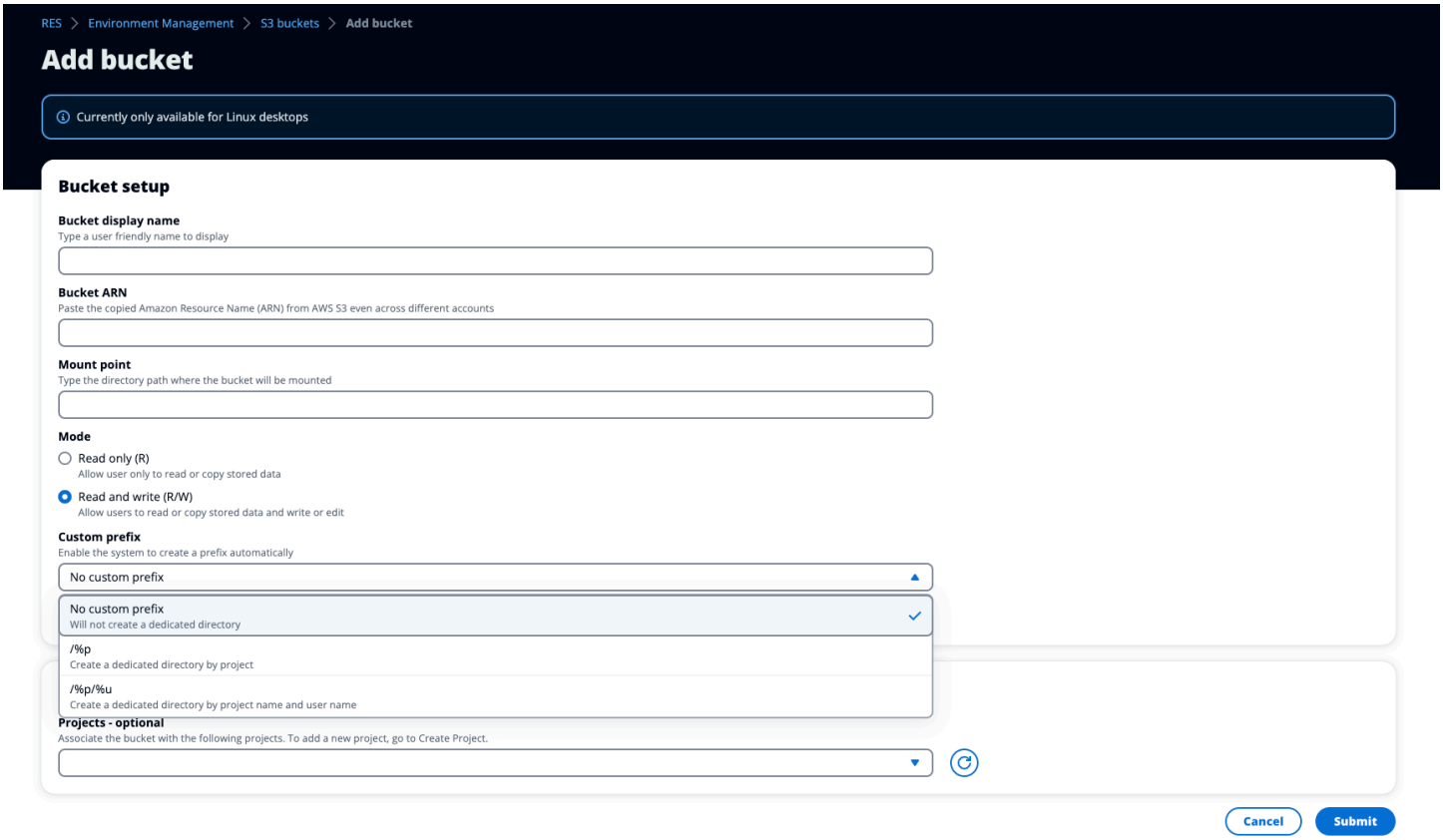
只读

如果选中，Read Only (R)则根据存储桶 ARN 的前缀（Amazon 资源名称）强制执行数据隔离。例如，如果管理员使用 ARN 向 RES 添加存储分区，arn:aws:s3:::*bucket-name/example-data*/并将此存储分区与项目 A 和项目 B 关联起来，则 VDIs 从项目 A 和项目 B 中启动的用户只能读取位于路径*bucket-name*下的数据。*/example-data*他们将无法访问该路径之外的数据。如果存储桶 ARN 中没有附加前缀，则整个存储桶将可供与其关联的任何项目使用。

读和写

如果Read and Write (R/W)选中，则仍会根据存储桶 ARN 的前缀强制执行数据隔离，如上所述。此模式还有其他选项，允许管理员为 S3 存储桶提供基于变量的前缀。选中后Read and Write (R/W)，“自定义前缀” 部分将变为可用，该部分提供包含以下选项的下拉菜单：

- 没有自定义前缀
- /%p
- /%p/%u



没有自定义数据隔离

如果No custom prefix选择“自定义前缀”，则在不进行任何自定义数据隔离的情况下添加存储桶。这允许与存储桶关联的任何项目具有读取和写入权限。例如，如果管理员使用No custom prefix选定的 ARN `arn:aws:s3:::bucket-name` 将存储分区添加到 RES，并将此存储分区与项目 A 和项目 B 相关联，则 VDIs 从项目 A 和项目 B 中启动的用户将拥有对该存储分区的无限制读写权限。

在每个项目层面进行数据隔离

如果/%p选择“自定义前缀”，则存储桶中的数据将与其关联的每个特定项目隔离。该%p变量表示项目代码。例如，如果管理员使用/%p选定的 ARN `arn:aws:s3:::bucket-name`、挂载点为的存储桶添加存储桶`/bucket`，并将该存储桶与项目 A 和项目 B 关联起来，则项目 A 中的用户 A 可以向写入文件。`/bucket`项目 A 中的用户 B 也可以看到用户 A 写入的文件`/bucket`。但是，如果用户 B 在项目 B 中启动 VDI 并进行查看`/bucket`，他们将看不到用户 A 写入的文件，因为数据是按项目隔离的。用户 A 写入的文件位于前缀下的 S3 存储桶中，/ProjectA而用户 B 只能在使用项目 B VDIs 中的文件/ProjectB时才能访问。

在每个项目、每个用户级别上进行数据隔离

如果/%p/%u选择“自定义前缀”，则存储桶中的数据将与该项目关联的每个特定项目和用户隔离。%p变量代表项目代码，%u代表用户名。例如，管理员使用 ARN `arn:aws:s3:::bucket-name` 将存储桶添加到 RES 中，/%p/%u选中且挂载点为。`/bucket`此存储桶与项目 A 和项目 B 相关联。项目 A 中的用户 A 可以向其写入文件`/bucket`。与之前只有%p隔离的场景不同，在这种情况下，用户 B 将看不到用户 A 在项目 A 中写入的文件`/bucket`，因为项目和用户都隔离了数据。用户 A 写入的文件位于前缀下的 S3 存储桶中，`/ProjectA/UserA`而用户 B 只能 VDIs 在项目 A 中使用他们的文件`/ProjectA/UserB`时才能访问。

跨账户存储桶访问权限

RES 可以从其他 AWS 账户挂载存储桶，前提是这些存储桶具有适当的权限。在以下场景中，账户 A 中的 RES 环境想要在账户 B 中挂载 S3 存储桶。

步骤 1：在部署 RES 的账户中创建 IAM 角色（这将称为账户 A）：

1. 登录需要访问 S3 存储桶的 RES 账户（账户 A）的 AWS 管理控制台。
2. 打开 IAM 控制台：
   a. 导航到 IAM 控制面板。
   b. 在导航窗格中，单选择 Policies。
3. 创建策略：
   a. 选择创建策略。
   b. 选择 JSON 选项卡。
   c. 粘贴以下 JSON 策略（`<BUCKET-NAME>`替换为账户 B 中的 S3 存储桶的名称）：

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
```

```
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

d. 选择下一步。

4. 查看并创建策略：

   a. 提供策略的名称（例如，AccessPolicy“S3”）。

   b. 添加可选描述以解释政策的用途。

   c. 查看策略并选择创建策略。

5. 打开 IAM 控制台：

   a. 导航到 IAM 控制面板。

   b. 在导航窗格中，选择角色。

6. 创建角色：

   a. 选择创建角色。

   b. 选择自定义信任策略作为可信实体的类型。

   c. 粘贴以下 JSON 策略（*<ACCOUNT_ID>*替换为账户 A 的实际账户 ID、*<ENVIRONMENT_NAME>* RES 部署的环境*<REGION>*名称以及 RES 部署到的 AWS 区域）：

      JSON

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

```
                "AWS":
 "arn:aws:iam::<ACCOUNT_ID>:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-<REGION>"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. 选择 “下一步”。

7. 附加权限策略：

   a. 搜索并选择您之前创建的策略。

   b. 选择 “下一步”。

8. 标记、查看和创建角色：

   a. 输入角色名称（例如，AccessRole“S3”）。

   b. 在 “步骤 3” 下，选择 “添加标签”，然后输入以下键和值：

      - 键：`res:Resource`
      - 值：`s3-bucket-iam-role`

   c. 查看角色并选择创建角色。

9. 在 RES 中使用 IAM 角色：

   a. 复制您创建的 IAM 角色 ARN。

   b. 登录 RES 控制台。

   c. 在左侧导航窗格中，选择 S3 存储桶。

   d. 选择添加存储桶，然后使用跨账户 S3 存储桶 ARN 填写表单。

   e. 选择 “高级设置-可选” 下拉列表。

   f. 在 IAM 角色 ARN 字段中输入角色 ARN。

   g. 选择 “添加存储桶”。

步骤 2：修改账户 B 中的存储桶策略

1. 登录账户 B 的 AWS 管理控制台

2. 打开 S3 控制台：

a. 导航到 S3 控制面板。

b. 选择您要授予访问权限的存储桶。

3. 编辑存储桶策略：

a. 选择 “权限” 选项卡，然后选择 “存储桶策略”。

b. 添加以下策略以授予账户 A 中的 IAM 角色访问存储桶的权限（*<AccountA_ID>*替换为账户 A 的实际账户 ID 和 *<BUCKET-NAME>* S3 存储桶的名称）：

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

c. 选择保存。

防止私有 VPC 中的数据泄露

为防止用户将数据从安全 S3 存储桶泄露到自己账户中的 S3 存储桶中，您可以附加 VPC 终端节点来保护您的私有 VPC。以下步骤说明如何为 S3 服务创建 VPC 终端节点，该终端节点支持访问您的账户中的 S3 存储桶以及任何其他拥有跨账户存储桶的账户。

1. 打开亚马逊 VPC 控制台：
   a. 登录到 AWS 管理控制台。
   b. 打开 Amazon VPC 控制台，网址为 https://console.aws.amazon.com/vpc/。
2. 为 S3 创建 VPC 终端节点：
   a. 在左侧导航窗格中，选择终端节点。
   b. 选择创建端点。
   c. 对于服务类别，请确保选中 AWS 服务。
   d. 在“服务名称”字段中，输入`com.amazonaws.`*`<region>`*`.s3`（*`<region>`*用您 AWS 所在的地区替换）或搜索“S3”。
   e. 从列表中选择 S3 服务。
3. 配置端点设置：
   a. 对于 VPC，请选择要在其中创建终端节点的 VPC。
   b. 对于子网，请选择部署期间用于 VDI 子网的两个私有子网。
   c. 对于启用 DNS 名称，请确保选中该选项。这允许将私有 DNS 主机名解析到端点网络接口。
4. 将策略配置为限制访问：
   a. 在“策略”下，选择“自定义”。
   b. 在策略编辑器中，输入限制访问您的账户或特定账户内资源的策略。以下是策略示例（*mybucket*替换为您的 S3 存储桶*444455556666*名称*111122223333*和您想要访问 IDs 的相应 AWS 账户）：

      JSON

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

```
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::mybucket",
                "arn:aws:s3:::mybucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",   // Your Account ID
                        "444455556666"    // Another Account ID
                    ]
                }
            }
        }
    ]
}
```

5. 创建端点：

   a. 检视您的设置。

   b. 选择创建终端节点。

6. 验证端点：

   a. 创建终端节点后，在 VPC 控制台中导航至 “终端节点” 部分。

   b. 选择新创建的端点。

   c. 验证 “状态” 是否为 “可用”。

按照这些步骤操作，您可以创建一个允许 S3 访问的 VPC 终端节点，但仅限于您的账户或指定账户 ID 中的资源。

故障排除

如何检查存储桶是否无法在 VDI 上挂载

如果存储桶无法在 VDI 上装载，则可以在几个位置检查是否存在错误。请按照以下步骤操作。

1. 查看 VDI 日志：

   a. 登录 AWS 管理控制台。

   b. 打开 EC2 控制台并导航到实例。

c. 选择您启动的 VDI 实例。

d. 通过会话管理器连接到 VDI。

e. 运行以下 命令：

```
sudo su
cd ~/bootstrap/logs
```

在这里，你可以找到引导日志。任何失败的详细信息都将在configure.log.{time}文件中找到。

此外，请查看/etc/message日志以获取更多详细信息。

2. 查看自定义凭证代理 CloudWatch Lambda 日志：

a. 登录 AWS 管理控制台。

b. 打开 CloudWatch 控制台并导航到日志组。

c. 搜索日志组/aws/lambda/*<stack-name>*-vdc-custom-credential-broker-lambda。

d. 检查第一个可用的日志组并在日志中找到所有错误。这些日志将包含有关为安装 S3 存储桶提供临时自定义凭证的潜在问题的详细信息。

3. 查看自定义凭证代理 API Gateway CloudWatch 日志：

a. 登录 AWS 管理控制台。

b. 打开 CloudWatch 控制台并导航到日志组。

c. 搜索日志组*<stack-name>*-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>。

d. 检查第一个可用的日志组并在日志中找到所有错误。这些日志将包含有关向 API Gateway 发出的挂载 S3 存储桶所需的自定义凭据的任何请求和响应的详细信息。

如何在入职后编辑存储桶的 IAM 角色配置

1. 登录 AWS DynamoDB 控制台。

2. 选择表格：

a. 在左侧导航窗格中，选择表。

b. 查找并选择*<stack-name>*.cluster-settings。

3. 扫描桌子：

   a. 选择 “浏览表格项目”。

   b. 确保已选择 “扫描”。

4. 添加过滤器：

   a. 选择 “筛选器” 以打开 “筛选器条目” 部分。

   b. 将过滤器设置为与您的密钥相匹配-

      - 属性：输入密钥。
      - 条件：选择 “开头为”。
      - 值：输入`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`*`<filesystem_id>`*替换为需要修改的文件系统的值。

5. 执行扫描：

   选择 “运行” 以使用筛选器运行扫描。

6. 检查值：

   如果该条目存在，请确保使用正确的 IAM 角色 ARN 正确设置该值。

   如果该条目不存在：

   a. 选择 “创建项目”。

   b. 输入商品详情：

      - 对于关键属性，请输入`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`。
      - 添加正确的 IAM 角色 ARN。

   c. 选择 “保存” 以添加该项目。

7. 重新启动 VDI 实例：

   重启实例， VDIs 确保再次挂载受错误 IAM 角色 ARN 影响的实例。

启用 CloudTrail

要使用 CloudTrail 控制台 CloudTrail 在您的账户中启用，请按照AWS CloudTrail 用户指南中使用 CloudTrail 控制台创建跟踪中提供的说明进行操作。 CloudTrail 将通过记录访问 S3 存储桶的 IAM 角色来记录对 S3 存储桶的访问权限。这可以链接回实例 ID，该实例ID链接到项目或用户。

密钥管理

研究与工程工作室使用以下秘密进行维护 AWS Secrets Manager。在创建环境期间，RES 会自动创建密钥。管理员在创建环境时输入的密钥作为参数输入。

密钥名称	描述	已生成的 RES	管理员已输入
<envname>-sso-client-secret	环境单点登录 OAuth2 客户机密钥	✓	
<envname>-vdc-client-secret	vdc ClientSecret	✓	
<envname>-vdc-client-id	vdc ClientId	✓	
<envname>-vdc-gateway-certificate-private-key	域的自签名证书私钥	✓	
<envname>-vdc-gateway-certificate-certificate	域的自签名证书	✓	
<envname>-cluster-manager-client-secret	集群管理器 ClientSecret	✓	
<envname>-cluster-manager-client-id	集群管理器 ClientId	✓	
<envname>-external-private-key	域的自签名证书私钥	✓	

密钥名称	描述	已生成的 RES	管理员已输入
<envname>-外部证书	域的自签名证书	✓	
<envname>-internal-private-key	域的自签名证书私钥	✓	
<envname>-内部证书	域的自签名证书	✓	
<envname>-目录服务-ServiceAccountUsername			✓
<envname>-目录服务-ServiceAccountPassword			✓

DynamoDB 的<envname>集群设置表中包含以下秘密 ARN 值：

键	来源
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_	堆栈
vdc.dcv_connection_gateway.certificate.private_key_secret_ar	堆栈
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	堆栈
diretoryservice.root_username_secret_arn	
vdc.client_secret	堆栈
cluster.load_balancers.external_alb.certificates.certicate_secret_arn	堆栈
cluster.load_balancers.internal_alb.certificates.certicate_secret_arn	堆栈

键	来源
目录服务.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certicates.private_key_secret_arn	堆栈
集群管理器.client_secret	

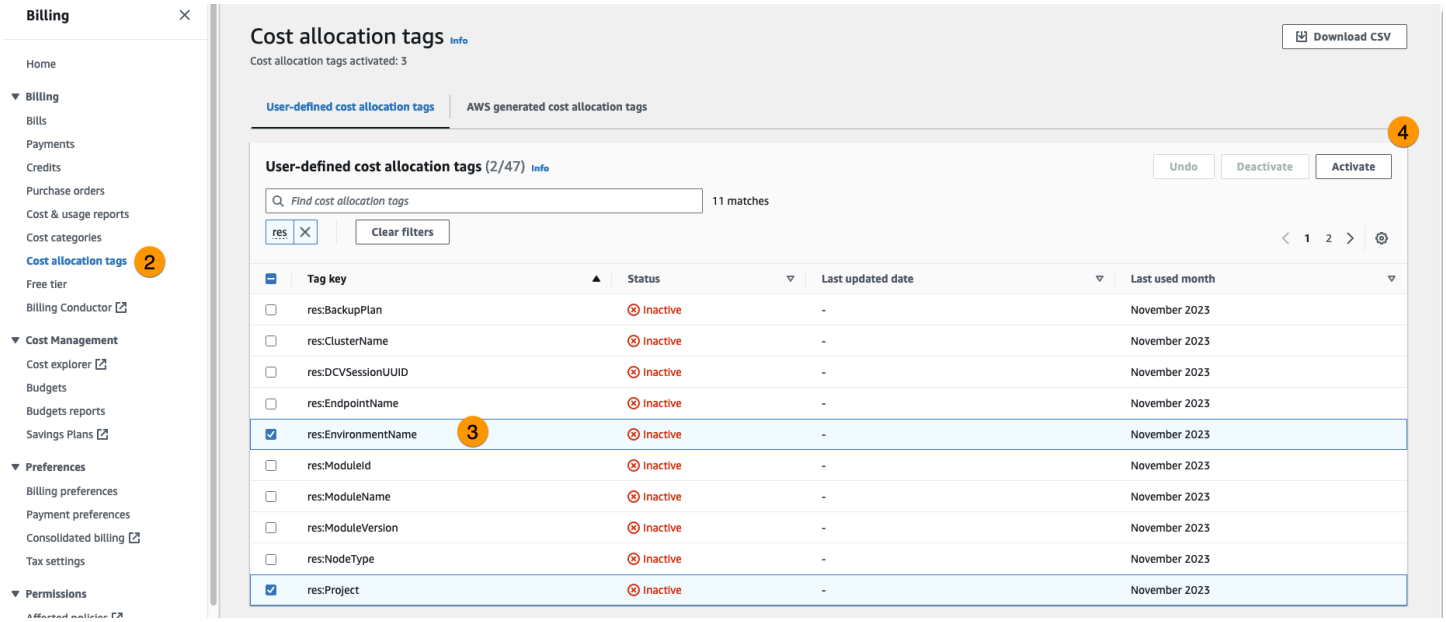
成本监测和控制

> **Note**
>
> 中不支持将研究和工程工作室项目关联到 AWS Budgets 。 AWS GovCloud (US)

我们建议通过AWS Cos t Explorer 创建预算，以帮助管理成本。价格可能会发生变化。如需了解全部详情，请参阅每项的定价网页the section called “AWS 本产品中的服务”。

为了帮助进行成本跟踪，您可以将 RES 项目与在其中创建的预算相关联 AWS Budgets。您首先需要激活账单成本分配标签内的环境标签。

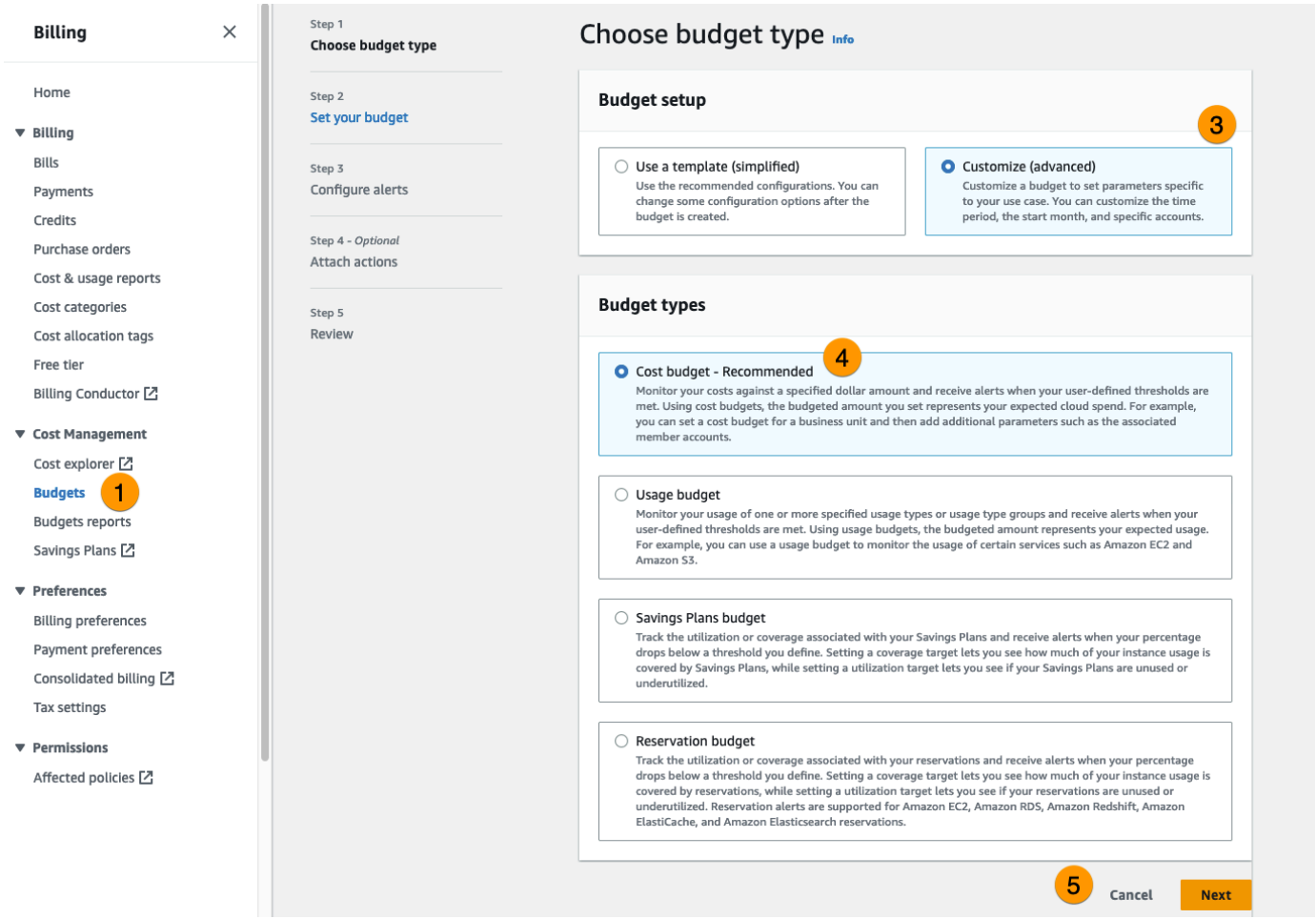
1. 登录 AWS Management Console 并打开 AWS 账单与成本管理 控制台，网址为https://console.aws.amazon.com/costmanagement/。
2. 选择成本分配标签。
3. 搜索并选择`res:Project`和`res:EnvironmentName`标签。
4. 选择激活。



> **Note**
>
> 部署后，RES 标签最多可能需要一天时间才会出现。

要为 RES 资源创建预算，请执行以下操作：

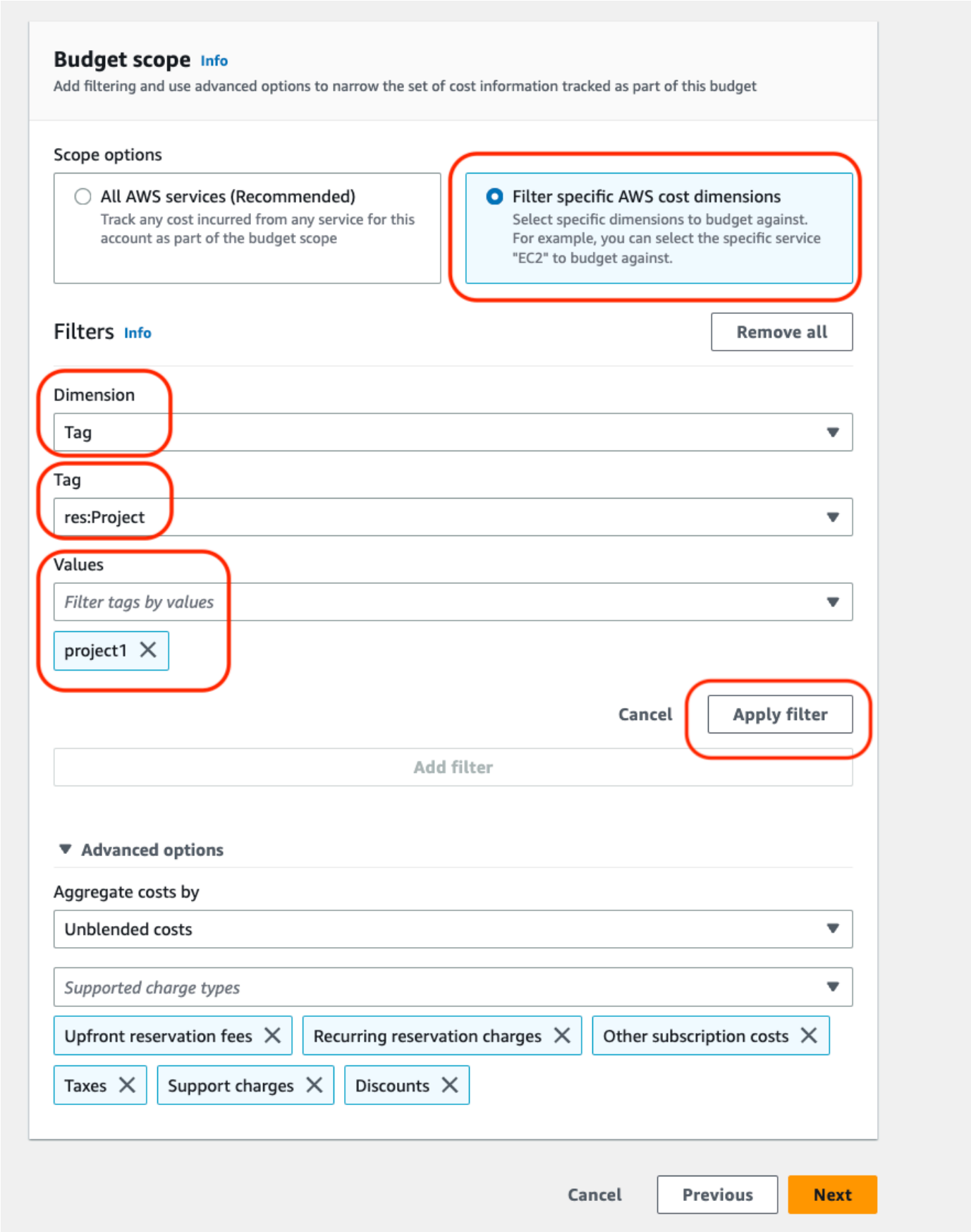
1. 在账单控制台中，选择预算。
2. 选择创建预算。
3. 在预算设置下，选择自定义（高级）。
4. 在预算类型下，选择成本预算-推荐。
5. 选择下一步。



6. 在详细信息下，为您的预算输入一个有意义的预算名称，以将其与账户中的其他预算区分开来。例如，[EnvironmentName]-[ProjectName]-[BudgetName]。
7. 在设置预算金额下，输入项目的预算金额。
8. 在预算范围下，选择筛选特定 AWS 成本维度。
9. 选择 添加筛选条件。
10. 在 “维度” 下，选择 “标签”。
11. 在 “标签” 下，选择 “RES: 项目”。

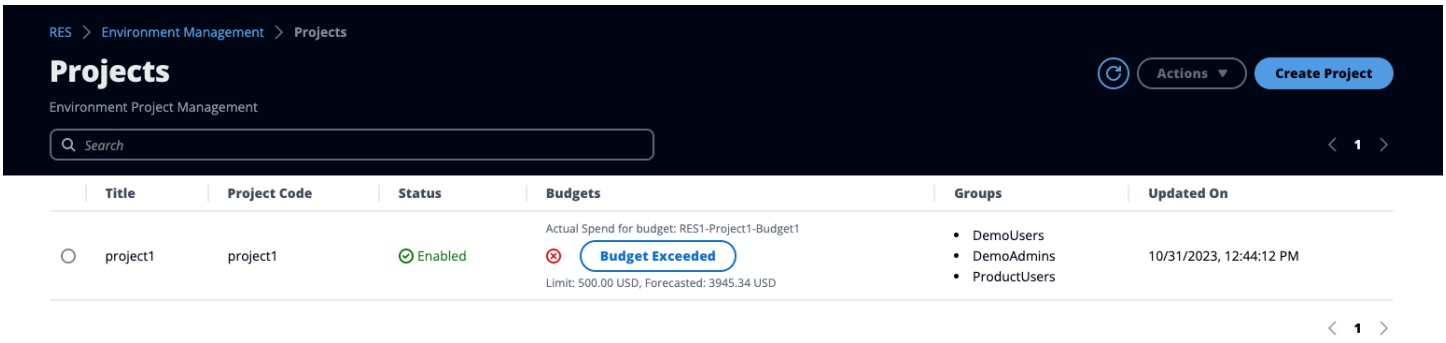
> **Note**
>
> 标签和值最多可能需要两天时间才能变为可用。项目名称可用后，您就可以创建预算。

12. 在 “值” 下，选择项目名称。
13. 选择 “应用筛选条件”，将项目筛选器附加到预算。
14. 选择下一步。


Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Filters Info
Remove all
Dimension
Tag
Tag
res:Project
Values
Filter tags by values
project1
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. （可选。）添加警报阈值。
16. 选择下一步。
17. （可选。）如果配置了警报，请使用附加操作为警报配置所需的操作。
18. 选择下一步。
19. 查看预算配置并确认在 “其他预算参数” 下设置了正确的标签。
20. 选择创建预算。

现在，预算已创建，您可以为项目启用预算。要为项目开启预算，请参阅the section called “编辑项目”。如果超出预算，虚拟桌面将被禁止启动。如果在启动台式机时超出预算，则该台式机将继续运行。



如果您需要更改预算，请返回控制台编辑预算金额。更改最多可能需要十五分钟才能在 RES 中生效。或者，您可以编辑项目以禁用预算。

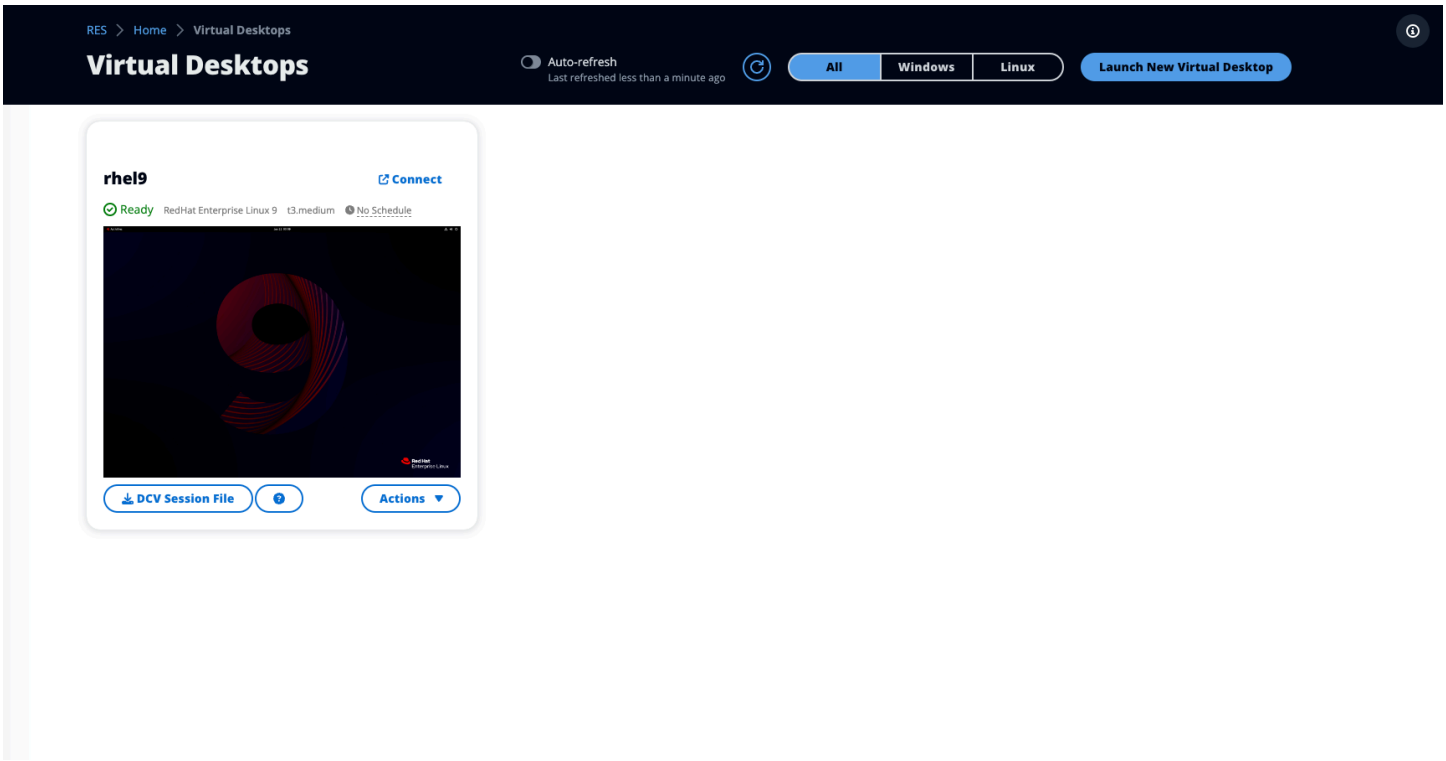
使用该产品

本节为用户提供有关使用虚拟桌面与其他用户协作的指导。

主题

虚拟桌面

虚拟桌面接口 (VDI) 模块允许用户在上 AWS创建和管理 Windows 或 Linux 虚拟桌面。用户可以在预先安装和配置自己喜欢的工具和应用程序的情况下启动 Amazon EC2 实例。



支持的操作系统

RES 目前支持使用以下操作系统启动虚拟桌面：

- 亚马逊 Linux 2 (x86 和 ARM64)

- Ubuntu 22.04.03 (x86)
- Windows 2019、2022 (x86)

启动新的桌面

1. 从菜单中选择 “我的虚拟桌面”。
2. 选择 “启动新虚拟桌面”。
3. 输入新桌面的详细信息。
4. 选择提交。

一张包含您的桌面信息的新卡片会立即出现，您的桌面将在 10-15 分钟内准备就绪。启动时间取决于所选映像。RES 会检测 GPU 实例并安装相关的驱动程序。

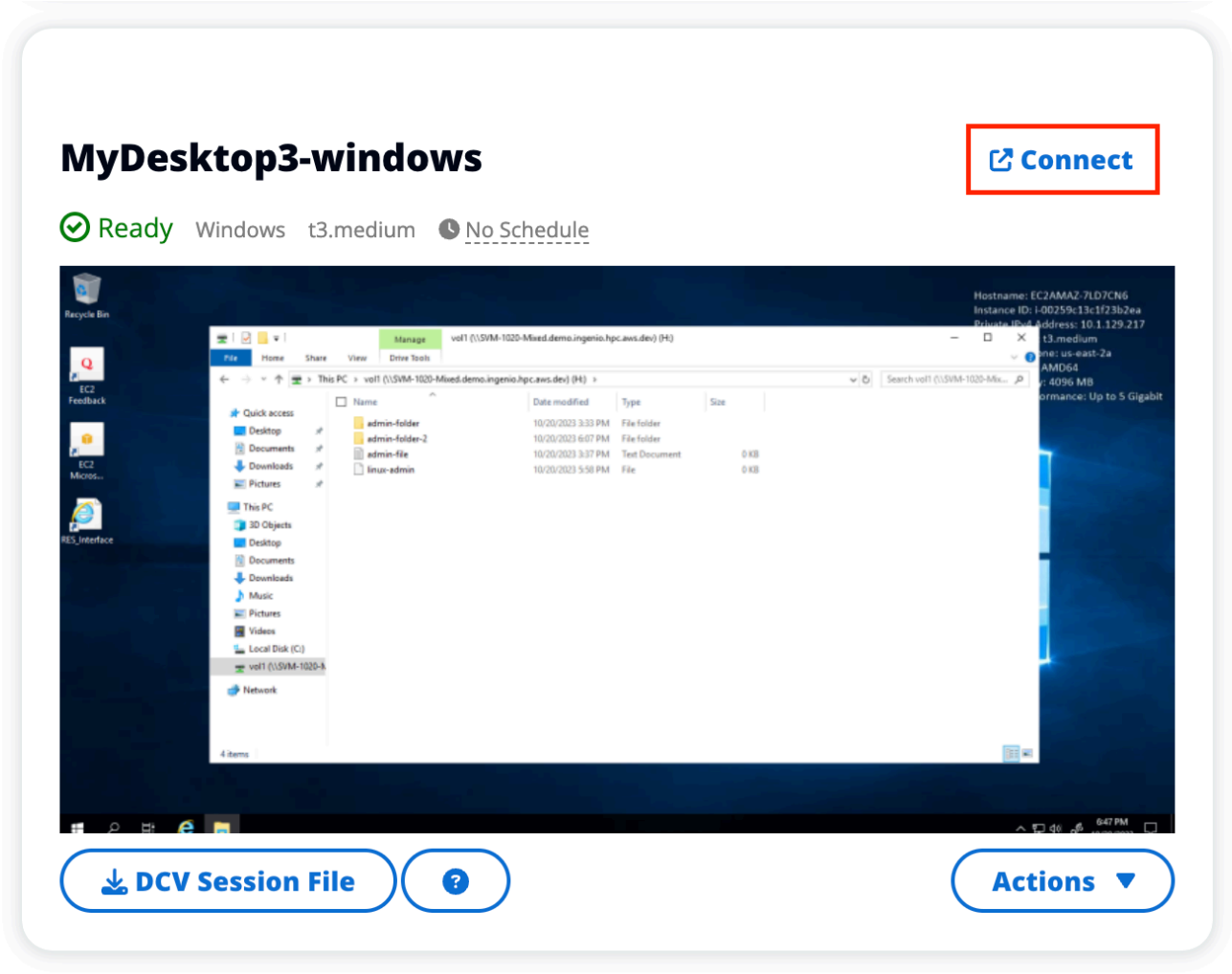
访问您的桌面

要访问虚拟桌面，请选择桌面卡，然后使用 Web 或 DCV 客户端进行连接。

Web connection

通过 Web 浏览器访问桌面是最简单的连接方法。

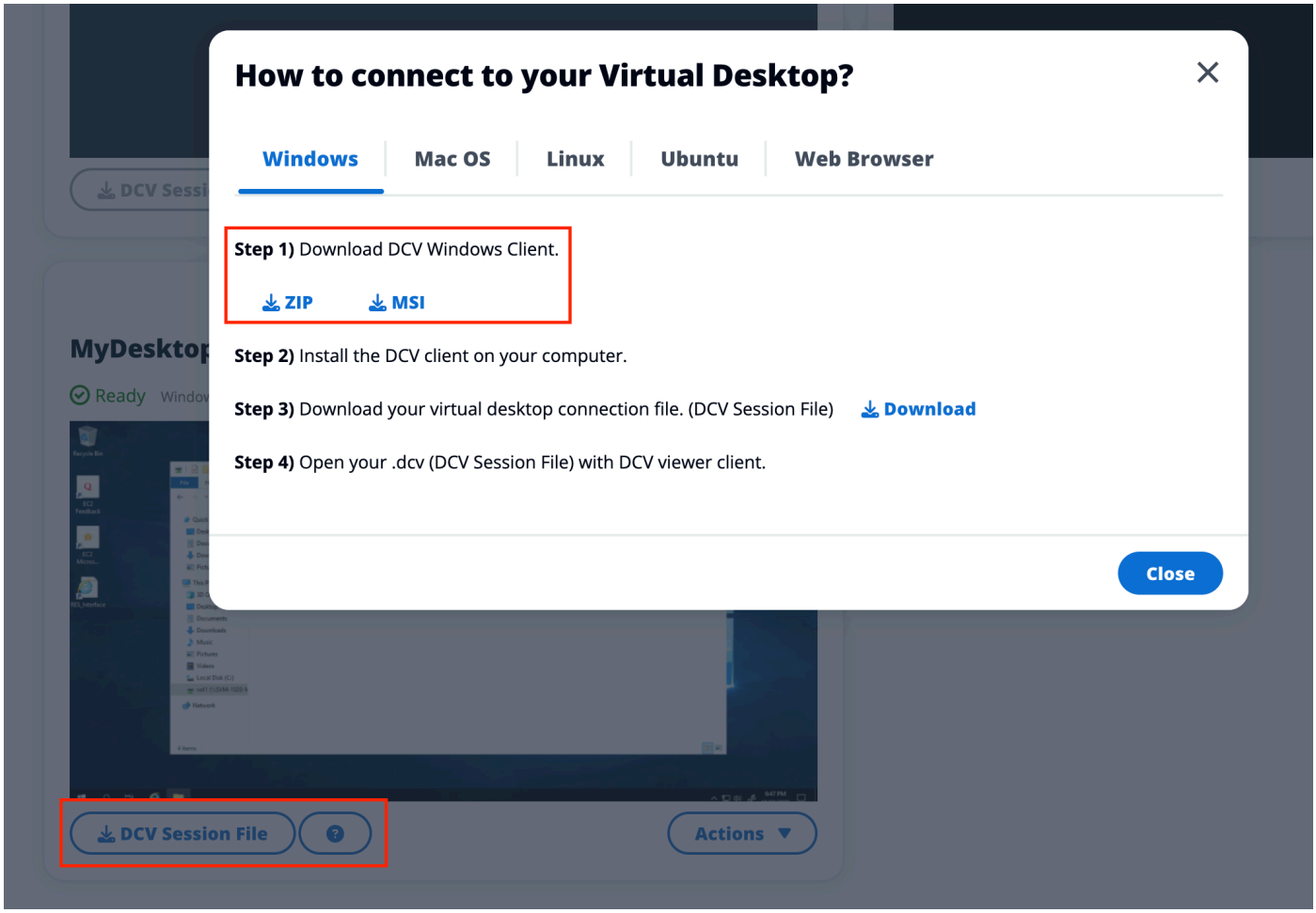
- 选择 Connect，或选择缩略图以直接通过浏览器访问您的桌面。



DCV connection

通过 DCV 客户端访问桌面可获得最佳性能。要通过 DCV 访问，请执行以下操作：

1. 选择 DCV 会话文件以下载。 dcv文件。您需要在系统上安装 DCV 客户端。
2. 有关安装说明，请选择？ 图标。



控制您的桌面状态

要控制桌面的状态，请执行以下操作：

1. 选择操作。
2. 选择虚拟桌面状态。您有四个州可供选择：

   - Stop (停止)

     已停止的会话不会丢失数据，您可以随时重新启动已停止的会话。

   - 重启

     重新启动当前会话。

   - 终止

永久结束会话。如果您使用的是临时存储，则终止会话可能会导致数据丢失。在终止之前，您应该将数据备份到 RES 文件系统。

- Hibernate

  您的桌面状态将保存在内存中。重新启动桌面后，您的应用程序将恢复，但所有远程连接都可能丢失。并非所有实例都支持休眠，且该选项只有在实例创建期间启用后才可用。要验证您的实例是否支持此状态，请参阅休眠先决条件。

修改虚拟桌面

您可以更新虚拟桌面的硬件或更改会话名称。

1. 在更改实例大小之前，必须停止会话：

   a. 选择操作。
   b. 选择虚拟桌面状态。
   c. 选择停止。

   > **Note**
   >
   > 您无法更新休眠会话的桌面大小。

2. 确认桌面已停止后，选择 “操作”，然后选择 “更新会话”。
3. 更改会话名称或选择所需的桌面大小。
4. 选择提交。
5. 实例更新后，重启桌面：

   a. 选择操作。
   b. 选择虚拟桌面状态。
   c. 选择启动。

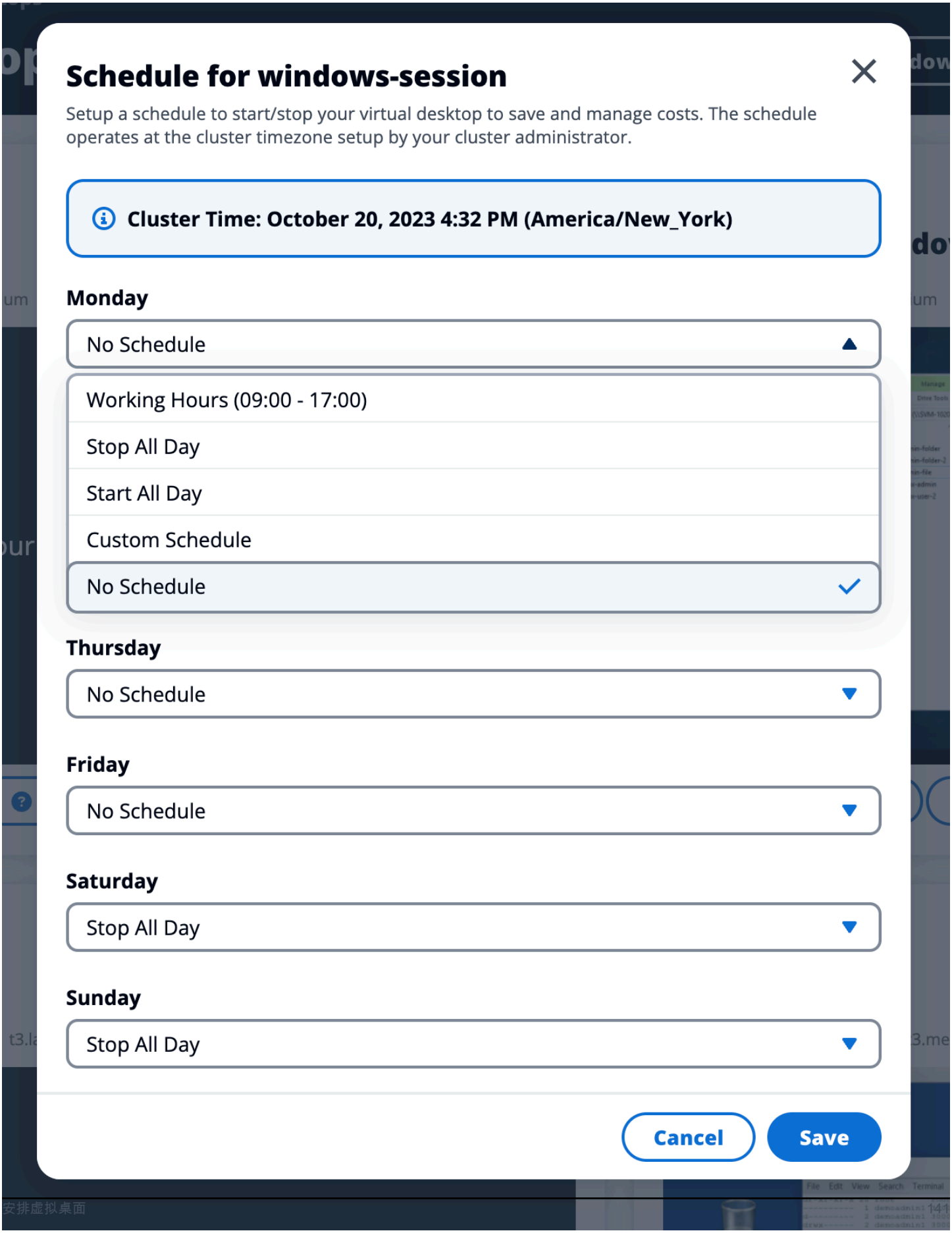
检索会话信息

1. 选择操作。
2. 选择 “显示信息”。

安排虚拟桌面

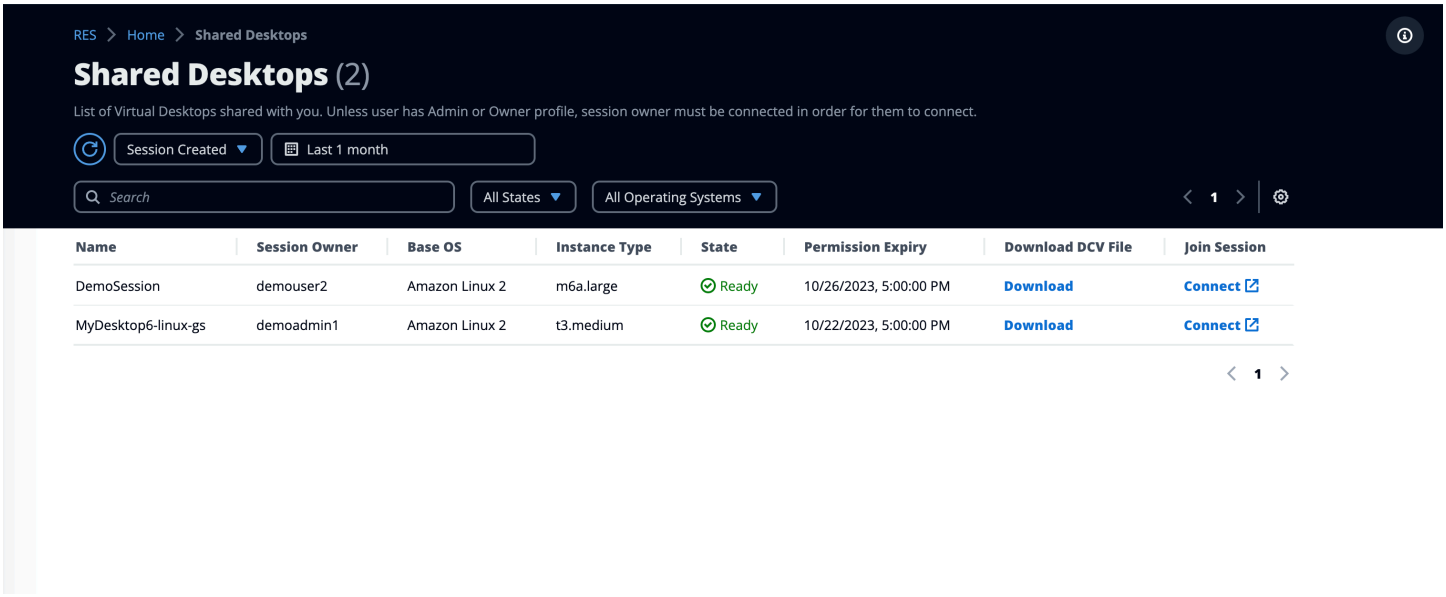
默认情况下，虚拟桌面没有时间表，在您停止或终止会话之前会一直处于活动状态。台式机在空闲时也会停止，以防止意外停止。空闲状态是由至少 15 分钟内没有活动连接和 CPU 使用率低于 15% 决定的。您可以将计划配置为自动启动和停止桌面。

1. 选择操作。
2. 选择 Schedule。
3. 设定每天的时间表。
4. 选择保存。


Schedule for windows-session
Setup a schedule to start/stop your virtual desktop to save and manage costs. The schedule operates at the cluster timezone setup by your cluster administrator.
Cluster Time: October 20, 2023 4:32 PM (America/New_York)
Monday
No Schedule
Working Hours (09:00 - 17:00)
Stop All Day
Start All Day
Custom Schedule
No Schedule
Thursday
No Schedule
Friday
No Schedule
Saturday
Stop All Day
Sunday
Stop All Day
Cancel
Save

共享桌面

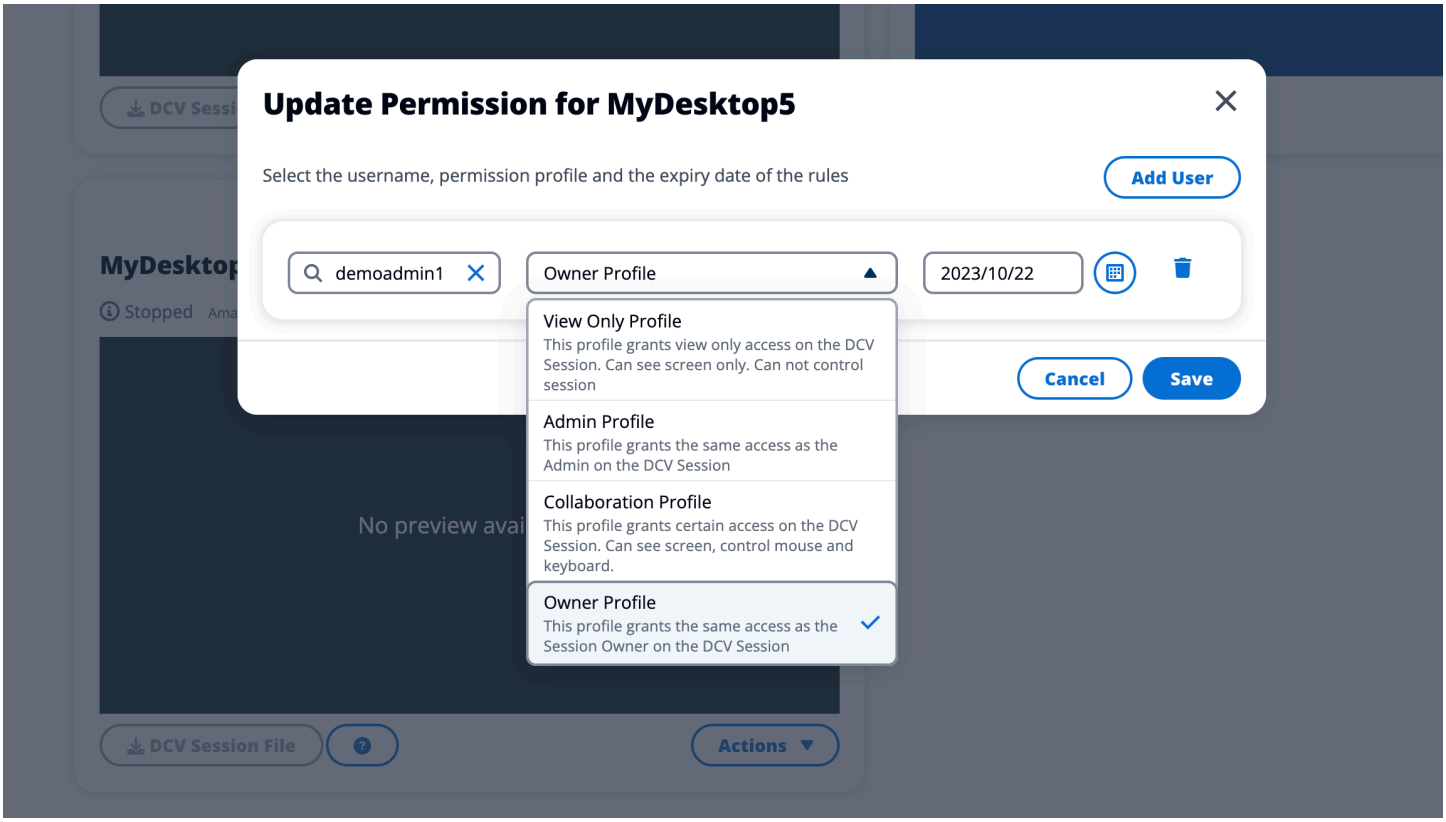
在共享桌面上，您可以看到已与您共享的桌面。要连接到桌面，除非您是管理员或所有者，否则还必须连接会话所有者。



共享会话时，您可以为合作者配置权限。例如，您可以向正在与之合作的队友授予只读访问权限。

共享桌面

1. 在桌面会话中，选择操作。
2. 选择会话权限。
3. 选择用户和权限级别。您也可以设置到期时间。
4. 选择保存。



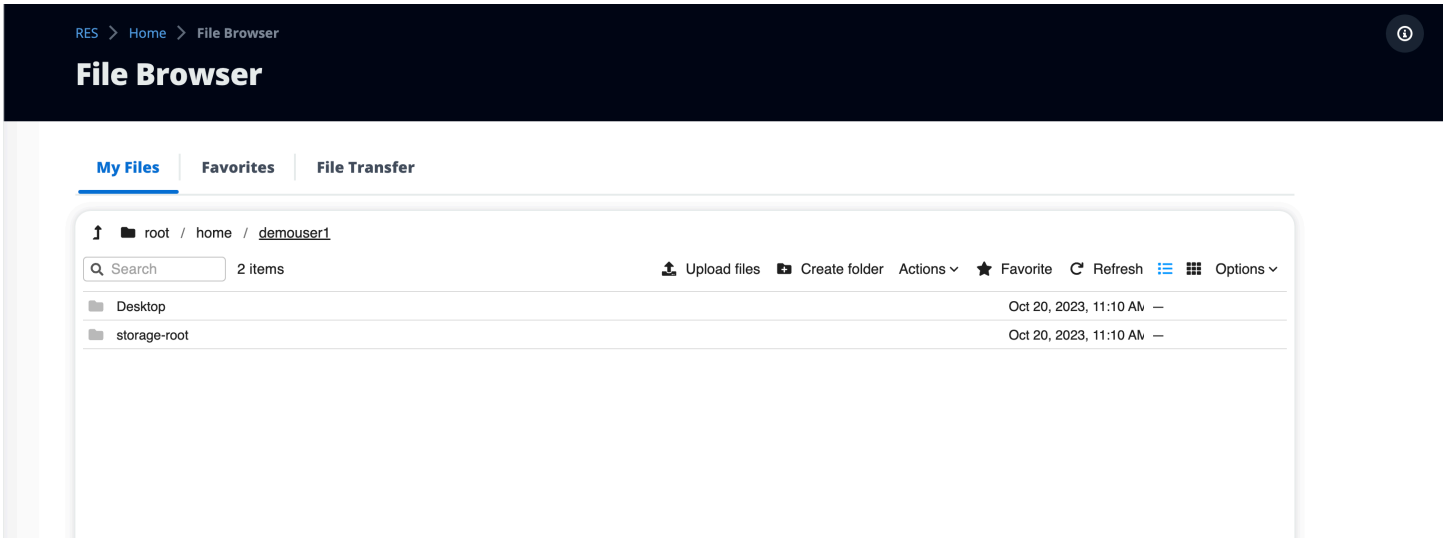
有关权限的更多信息，请参阅the section called “权限配置文件”。

访问共享桌面

在共享桌面中，您可以查看与您共享的桌面并连接到实例。您可以通过 Web 浏览器或 DCV 加入。要进行连接，请按照中的说明进行操作the section called “访问您的桌面”。

文件浏览器

文件浏览器允许您通过 Web 门户访问文件系统。您可以管理底层文件系统上您有权访问的所有可用文件。后端存储 (Amazon EFS) 适用于所有 Linux 节点。对于 Linux 和 Windows 节点，已 FSx 推出适用于 ONTAP 的版本。更新虚拟桌面上的文件与通过终端或基于 Web 的文件浏览器更新文件相同。



上传文件

1. 选择上传文件。
2. 要么删除文件，要么浏览要上传的文件。
3. 选择上传 (n) 个文件。

删除文件

1. 选择要删除的文件。
2. 选择操作。
3. 选择删除文件。

或者，也可以右键单击任何文件或文件夹，然后选择 “删除文件”。

管理收藏夹

要固定重要的文件和文件夹，可以将其添加到 “收藏夹”。

1. 选择文件或文件夹。
2. 选择 “收藏”。

或者，您可以右键单击任何文件或文件夹，然后选择 “收藏”。

> **Note**
>
> 收藏夹存储在本地浏览器中。如果您更换浏览器或清除缓存，则需要重新锁定收藏夹。

编辑文件

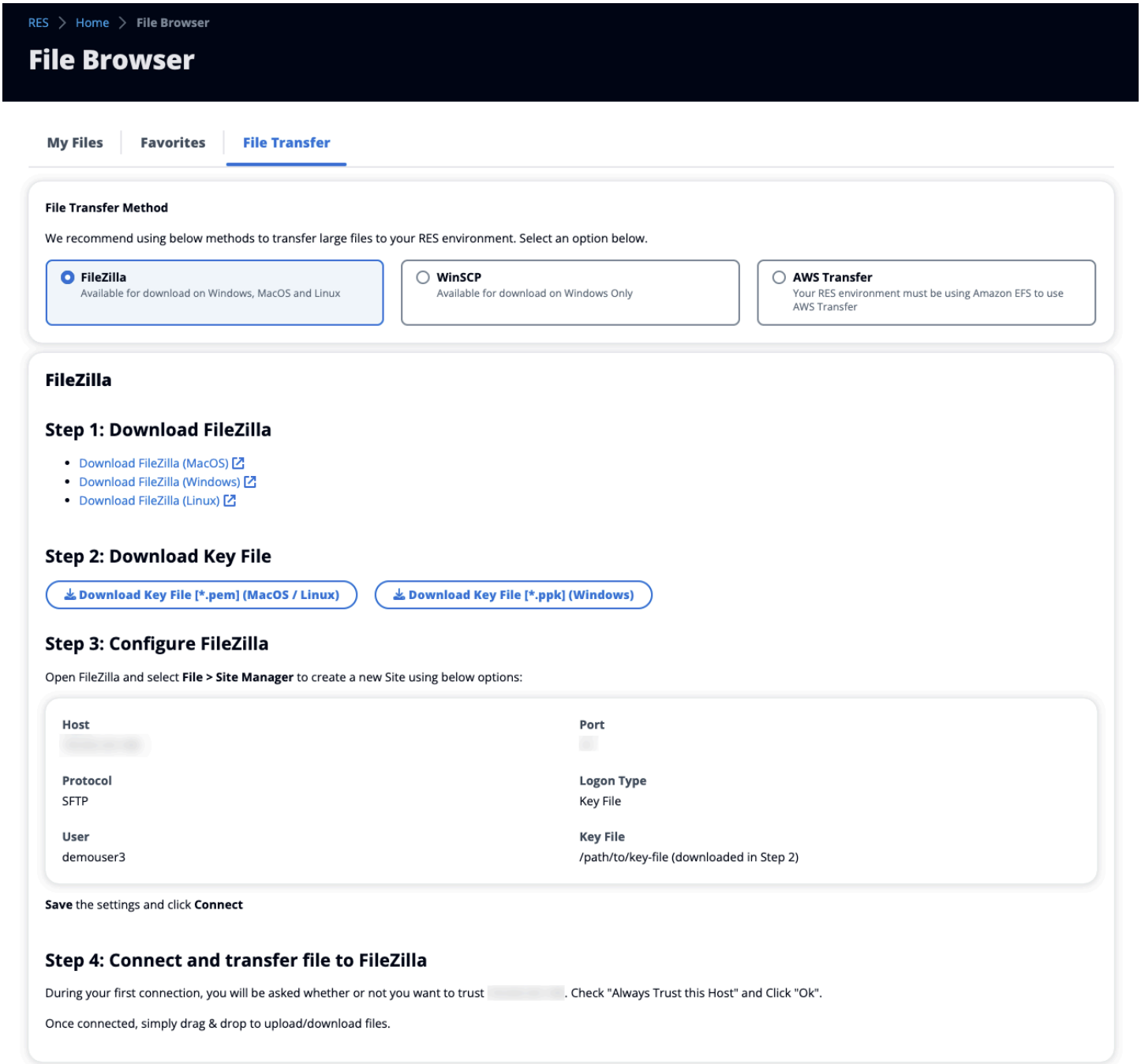
您可以在 Web 门户中编辑基于文本的文件的内容。

1. 选择要更新的文件。将打开一个包含文件内容的模态。
2. 进行更新并选择 “保存”。

传输文件

使用 “文件传输” 使用外部文件传输应用程序来传输文件。您可以从以下应用程序中进行选择，然后按照屏幕上的说明传输文件。

- FileZilla（Windows、macOS、Linux）
- WinSCP (Windows)
- AWS Transfer for FTP（亚马逊 EFS）



SSH 访问

要使用 SSH 访问堡垒主机，请执行以下操作：

1. 从 RES 菜单中选择 SSH 访问。
2. 按照屏幕上的说明使用 SSH 或 PuTTY 进行访问。

故障排除

本节包含有关如何监控系统以及如何对可能发生的特定问题进行故障排除的信息。

主题

详细内容：

常规调试和监控

本节包含有关在 RES 中何处可以找到信息的信息。

有用的日志和事件信息来源

保留的信息来源多种多样，可供故障排除和监控时参考。

环境 Amazon EC2 实例上的日志文件

日志文件存在于 RES 正在使用的 Amazon EC2 实例上。SSM 会话管理器可用于打开与实例的会话以检查这些文件。

在集群管理器和 vdc-controller 等基础设施实例上，可以在以下位置找到应用程序和其他日志。

- /opt/idea/app/logs/application.log
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log

- /var/log/cloud-init-output.log

在 Linux 虚拟桌面上，以下内容包含有用的日志文件

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages

在 Windows 虚拟桌面实例上，可以在以下网址找到日志

- PS C:\\ ProgramData n ice\ dcv\ log
- PS C:\\ n ice\ProgramData\ n ice\ DCVSessionManagerAgent\ log

在 Windows 上，可以在以下网址找到一些应用程序的日志记录：

- PS C:\Program Files\ NICE\ DCV\ Server\ bin

在 Windows 上，NICE DCV 证书文件可以在以下位置找到：

- C:\Windows\System32\config\systemprofile\AppData\ Local\ NICE\ dcv\

Amazon CloudWatch 日志组

Amazon EC2 和 AWS Lambda 计算资源将信息记录到亚马逊 CloudWatch 日志组。其中的日志条目可以在排查潜在问题时提供有用的信息，也可以提供一般信息。

这些群组的命名如下：

- `/aws/lambda/<envname>-/ - lambda related`
- */<envname>/*
  - `cluster-manager/ - main infrastructure host`
  - `vdc/ - virtual desktop related`
    - `dcv-broker/ - desktop related`
    - `dcv-connection-gateway/ - desktop related`
    - `controller/ - main desktop controller host`

- dcv-session/ - desktop session related

在检查日志组时，使用大写和小写字符串进行筛选可能会很有帮助，如下所示。这将仅输出那些包含注明字符串的消息。

```
?"ERROR" ?"error"
```

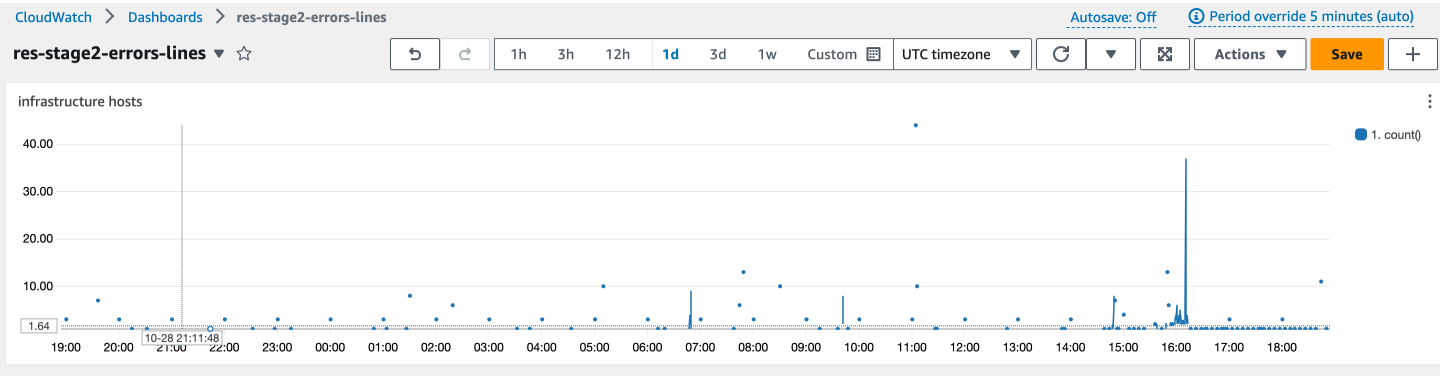
监控问题的另一种方法是创建包含显示感兴趣数据的微件的 Amazon CloudWatch 控制面板。

例如，创建一个小部件，用于计算字符串错误和错误的出现次数，并将它们绘制为线条。这种方法可以更轻松地检测潜在问题或表明模式已发生变化的趋势。

以下是基础架构主机的示例。要使用此功能，请连接查询行，并将<envname>和<region>属性替换为相应的值。

```
{
    "widgets": [
        {
            "type": "log",
            "x": 0,
            "y": 0,
            "width": 24,
            "height": 6,
            "properties": {
                "query": "SOURCE '/<envname>/vdc/controller' |
                    SOURCE '/<envname>/cluster-manager' |
                    SOURCE '/<envname>/vdc/dcv-broker' |
                   SOURCE '/<envname>/vdc/dcv-connection-gateway' |
                    fields @timestamp, @message, @logStream, @log\n|
                    filter @message like /(?i)(error|ERROR)/\n|
                    sort @timestamp desc|
                    stats count() by bin(30s)",
                "region": "<region>",
                "title": "infrastructure hosts",
                "view": "timeSeries",
                "stacked": false
            }
        }
    ]
}
```

控制板的示例可能如下所示：



CloudFormation 堆栈

在环境创建期间创建的 CloudFormation 堆栈包含与环境配置相关的资源、事件和输出信息。

对于每个堆栈，可以参阅 “事件”、“资源” 和 “输出” 选项卡，以获取有关堆栈的信息。

RES 堆栈：

- <envname>-bootstrap
- <envname>-集群
- <envname>-指标
- <envname>-目录服务
- <envname>-身份提供商
- <envname>-共享存储
- <envname>-集群管理器
- <envname>-vdc
- <envname>-堡垒主机

演示环境堆栈（如果您正在部署演示环境并且没有这些外部资源可用，则可以使用 AWS 高性能计算配方为演示环境生成资源。）

- <envname>
- <envname>-联网
- <envname>-DirectoryService
- <envname>-存储
- <envname>-WindowsManagementHost

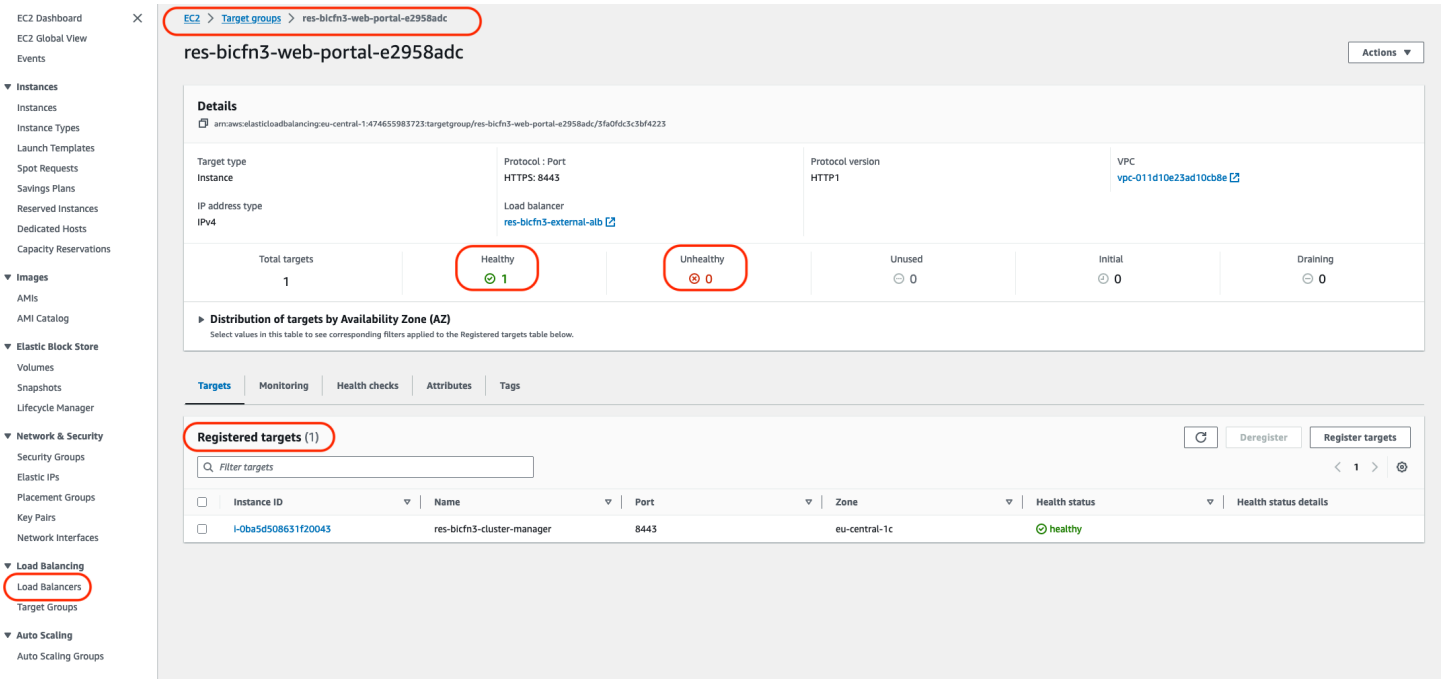
由于问题导致的系统故障，并反映在 Amazon A EC2 uto Scaling 群组活动中

如果 RES UIs 表示服务器错误，则原因可能是应用程序软件或其他问题。

每个基础设施 Amazon EC2 实例自动扩展组 (ASGs) 都包含一个 “活动” 选项卡，可用于检测实例的扩展活动。如果用户界面页面发现任何错误或无法访问，请检查亚马逊 EC2 控制台中是否有多个已终止的实例，并查看相关 ASG 的 Auto Scaling Group Activity 选项卡，以确定亚马逊 EC2 实例是否处于循环状态。

如果是，请使用实例的相关 Amazon CloudWatch 日志组来确定是否记录了可能表明问题原因的错误。在实例被标记为不健康并被 ASG 终止之前，也可以使用 SSM 会话控制台打开与该类型正在运行的实例的会话，并检查该实例上的日志文件以确定原因。

如果出现此问题，ASG 控制台可能会显示类似以下内容的活动。

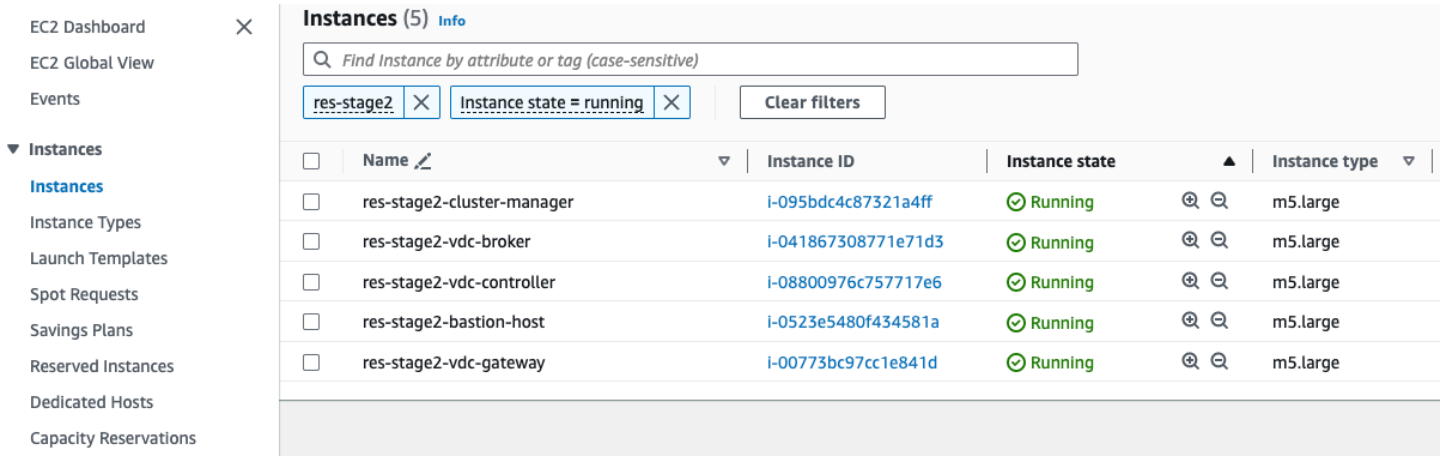


典型的亚马逊 EC2 控制台外观

本节包含系统在不同状态下运行的屏幕截图。

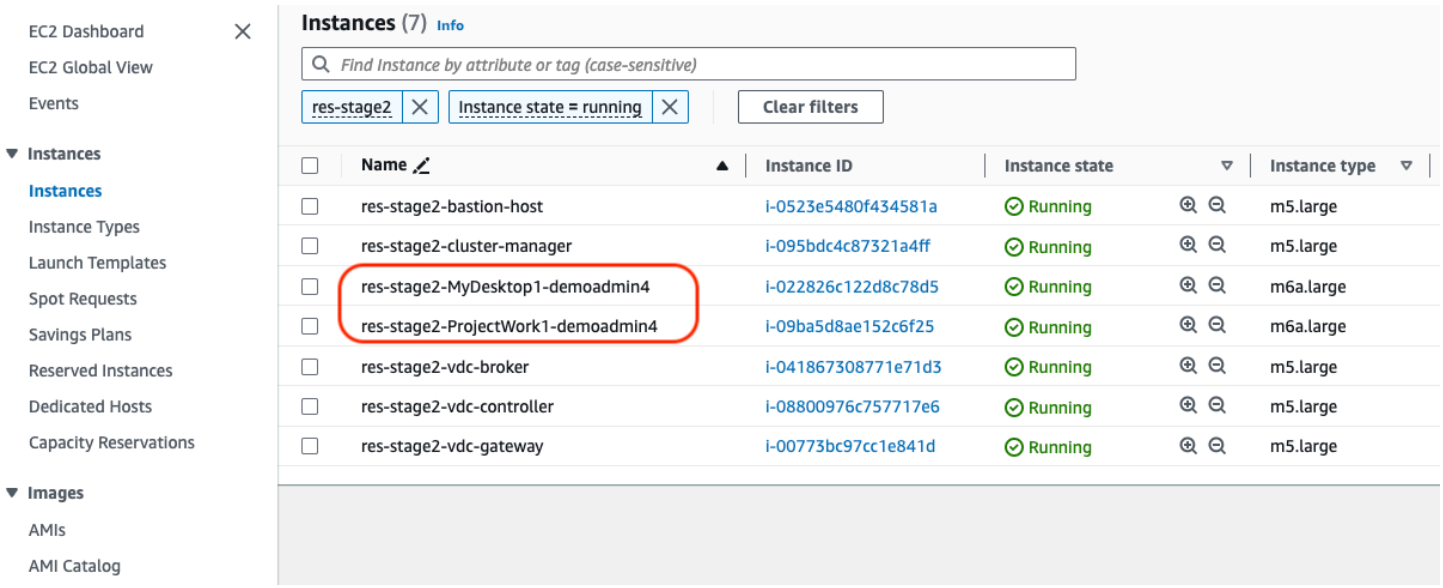
基础架构主机

当没有 EC2 台式机运行时，Amazon 控制台通常看起来与以下内容类似。显示的实例是 Amazon EC2 托管的 RES 基础设施。实例名称中的前缀是 RES 环境名称。



基础架构主机和虚拟桌面

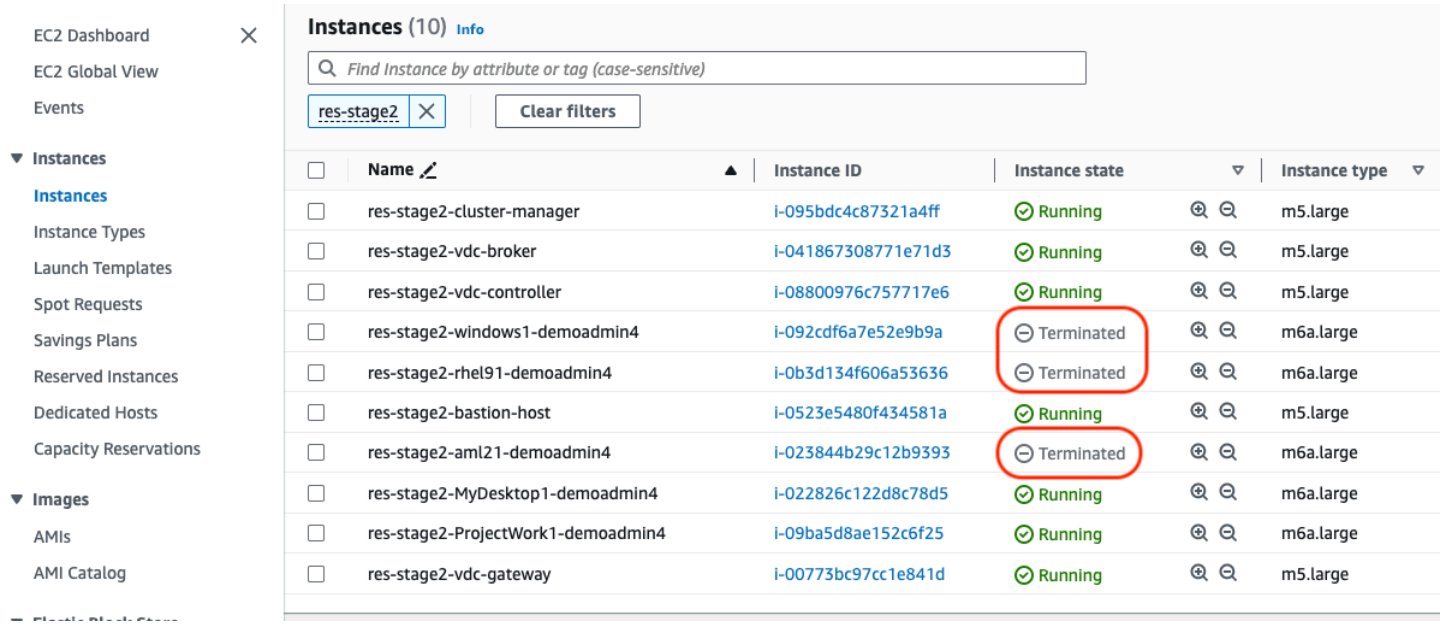
在 Amazon EC2 控制台中，当虚拟桌面运行时，它们看起来类似于以下内容。在这种情况下，虚拟桌面以红色标注。实例名称的后缀是创建桌面的用户。中间的名称是启动时设置的会话名称，可以是默认“MyDesktop”，也可以是用户设置的名称。



处于终止状态的主机

当 Amazon EC2 控制台显示已终止的实例时，它们通常是已终止的桌面主机。如果控制台包含处于终止状态的基础架构主机，特别是有多个相同类型的基础架构主机，则可能表示系统问题正在发生。

下图显示了已终止的桌面实例。



与活动目录 (AD) 相关的有用命令供参考

以下是 ldap 相关命令的示例，可以在基础架构主机上输入这些命令以查看 AD 配置相关信息。使用的域和其他参数应反映在创建环境时输入的参数。

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>
```

Windows DCV 调试

在 Windows 桌面上，您可以使用以下方式列出与其关联的会话：

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe'list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
 name:windows1)
```

查找 NICE DCV 版本信息

NICE DCV 用于虚拟桌面会话。AWS NICE DCV。以下示例说明如何确定所安装的 DCV 软件的版本。

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

NICE DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe' version

NICE DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

问题 RunBooks

下一节包含可能出现的问题、如何检测这些问题以及如何解决问题的建议。

- 安装问题
  - AWS CloudFormation 堆栈创建失败，并显示消息 “” WaitCondition 已收到失败消息。错误：状态。 TaskFailed”
  - 成功创建 AWS CloudFormation 堆栈后未收到电子邮件通知
  - 实例正在循环或 vdc 控制器处于故障状态
  - 由于依赖对象错误，无法删除环境 CloudFormation 堆栈
  - 创建环境时遇到 CIDR 块参数错误

- 编辑软件堆栈以添加项目时，项目不会出现在下拉列表中
- cluster-manager Amazon CloudWatch 日志显示 “< user-home-init > 账户还不可用。正在等待用户同步”（其中账户是用户名）
- 尝试登录时的 Windows 桌面显示 “您的帐户已被禁用。请咨询您的管理员”
- external/customer AD 配置的 DHCP 选项问题
- Firefox 错误 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

- 环境删除
  - res-xxx-cluster 堆栈处于 “DELETE_FAILED” 状态，由于 “角色无效或无法假设” 错误，无法手动删除
  - 收集日志
  - 正在下载 VDI 日志
  - 从 Linux EC2 实例下载日志
  - 从 Windows EC2 实例下载日志
  - 正在收集 WaitCondition 错误的 ECS 日志
- 演示环境
  - 处理对身份提供商的身份验证请求时出现演示环境登录错误

安装问题

主题

- AWS CloudFormation 堆栈创建失败，并显示消息 “” WaitCondition 已收到失败消息。错误：状态。TaskFailed”
- 成功创建 AWS CloudFormation 堆栈后未收到电子邮件通知
- 实例正在循环或 vdc 控制器处于故障状态
- 由于依赖对象错误，无法删除环境 CloudFormation 堆栈
- 创建环境时遇到 CIDR 块参数错误
- CloudFormation 创建环境期间堆栈创建失败
- 创建外部资源（演示）堆栈失败，并显示 AdDomainAdminNode CREATE_FAILED

.....

AWS CloudFormation 堆栈创建失败，并显示消息 “” WaitCondition 已收到失败消息。错误：状态。 TaskFailed”

要确定问题，请检查名为的 Amazon CloudWatch 日志组`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`。如果有多个同名的日志组，请检查第一个可用的日志组。日志中的错误消息将提供有关该问题的更多信息。

> **Note**
>
> 确认参数值中没有空格。

.....

成功创建 AWS CloudFormation 堆栈后未收到电子邮件通知

如果成功创建 AWS CloudFormation 堆栈后仍未收到电子邮件邀请，请验证以下内容：

1. 确认电子邮件地址参数输入正确。

   如果电子邮件地址不正确或无法访问，请删除并重新部署 Research and Engineering Studio 环境。
2. 请查看 Amazon EC2 控制台以获取循环实例的证据。

   如果有`<envname>`前缀显示为已终止的 Amazon EC2 实例，然后被新实例替换，则网络或 Active Directory 配置可能存在问题。
3. 如果您部署了 AWS 高性能计算配方来创建外部资源，请确认 VPC、私有子网和公有子网以及其他选定的参数是由堆栈创建的。

   如果任何参数不正确，则可能需要删除并重新部署 RES 环境。有关更多信息，请参阅 卸载产品。
4. 如果您使用自己的外部资源部署产品，请确认网络和 Active Directory 与预期配置相匹配。

   确认基础设施实例成功加入 Active Directory 至关重要。请尝试中的步骤the section called “实例正在循环或 vdc 控制器处于故障状态”来解决问题。

.....

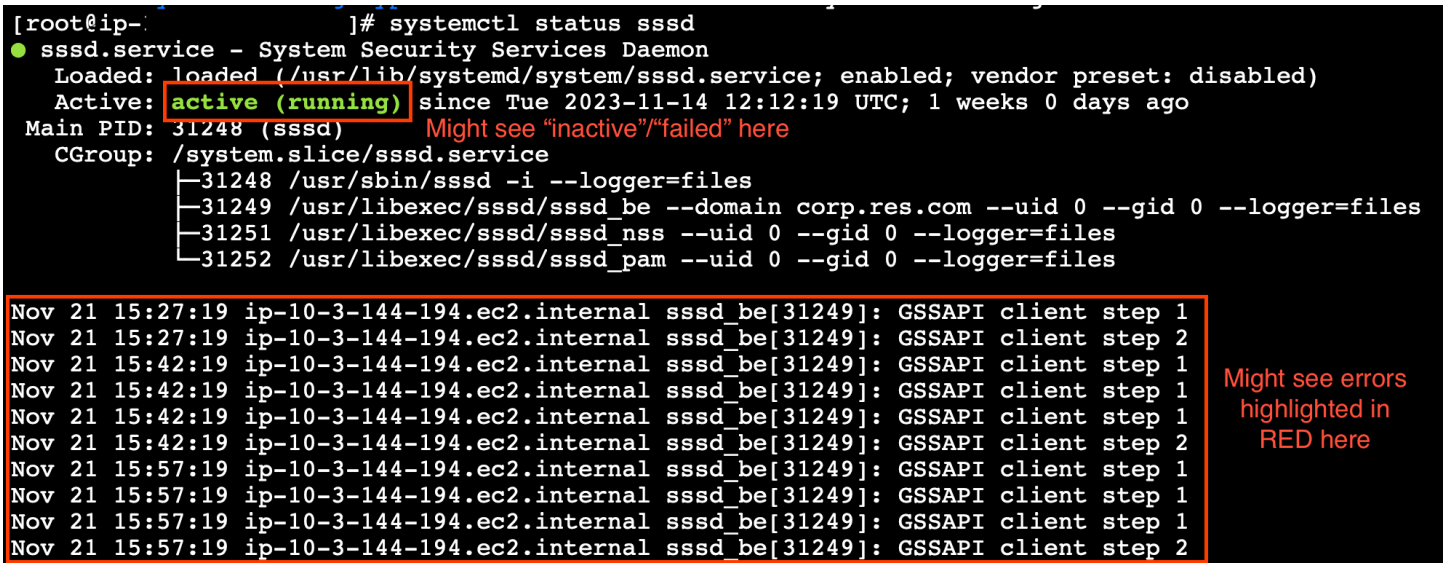
实例正在循环或 vdc 控制器处于故障状态

此问题最可能的原因是资源无法连接或加入 Active Directory。

要验证问题，请执行以下操作：

1. 在命令行中，在 vdc 控制器的运行实例上启动与 SSM 的会话。
2. 运行 `sudo su -`。
3. 运行 `systemctl status sssd`。

如果状态为非活动、失败或您在日志中看到错误，则说明该实例无法加入 Active Directory。



SSM 错误日志

要解决这个问题，请执行以下操作：

- 在同一个命令行实例中，运行`cat /root/bootstrap/logs/userdata.log`以调查日志。

该问题可能有三个可能的根本原因之一。

根本原因 1：输入的 ldap 连接详细信息不正确

查看日志。如果您多次看到以下内容重复，则说明该实例无法加入 Active Directory。

```
+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
```

```
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))
```

1. 验证在创建 RES 堆栈期间是否正确输入了以下各项的参数值。
   - directoryservice.ldap_connecti
   - 目录服务.ldap_base
   - 目录服务.users.ou
   - 目录 service.groups.ou
   - directoryservice.sudoers
   - directoryservice.com
   - 目录服务.name
2. 更新 DynamoDB 表中的所有错误值。该表位于 DynamoDB 控制台的 “表” 下方。表名应为**<stack name>**.cluster-settings。
3. 更新表后，删除当前运行环境实例的集群管理器和 vdc-Controller。自动扩展将使用 DynamoDB 表中的最新值启动新实例。

根本原因 2：输入的 ServiceAccount 用户名不正确

如果返回日志`Insufficient permissions to modify computer account`，则堆栈创建期间输入的 ServiceAccount 名称可能不正确。

1. 在 AWS 控制台中打开 Secrets Manager。
2. 搜索 directoryserviceServiceAccountUsername。秘诀应该是**<stack name>**-directoryservice-ServiceAccountUsername。
3. 打开密钥以查看详细信息页面。在 “机密值” 下，选择 “检索机密值”，然后选择 “纯文本”。
4. 如果该值已更新，请删除环境中当前正在运行的集群管理器和 vdc-controller 实例。自动缩放将使用 Secrets Manager 中的最新值启动新实例。

根本原因 3：输入的 ServiceAccount 密码不正确

如果显示日志`Invalid credentials`，则在创建堆栈时输入的 ServiceAccount 密码可能不正确。

1. 在 AWS 控制台中打开 Secrets Manager。
2. 搜索 `directoryserviceServiceAccountPassword`。秘诀应该是**`<stack name>`**`-directoryservice-ServiceAccountPassword`。
3. 打开密钥以查看详细信息页面。在 “机密值” 下，选择 “检索机密值”，然后选择 “纯文本”。
4. 如果您忘记了密码或者不确定输入的密码是否正确，则可以在 Active Directory 和 Secrets Manager 中重置密码。

   a. 要在中重置密码，请执行 AWS Managed Microsoft AD以下操作：

      i. 打开 AWS 控制台并转至 AWS Directory Service。

      ii. 选择您的 RES 目录的目录 ID，然后选择操作。

      iii. 选择重置用户密码。

      iv. 输入 ServiceAccount 用户名。

      v. 输入新密码，然后选择重置密码。

   b. 要在 Secrets Manager 中重置密码，请执行以下操作：

      i. 打开 AWS 控制台并前往 Secrets Manager。

      ii. 搜索 `directoryserviceServiceAccountPassword`。秘诀应该是**`<stack name>`**`-directoryservice-ServiceAccountPassword`。

      iii. 打开密钥以查看详细信息页面。在 “机密值” 下，选择 “检索密钥值”，然后选择 “纯文本”。

      iv. 选择编辑。

      v. 为 ServiceAccount 用户设置新密码，然后选择保存。

5. 如果您更新了该值，请删除环境中当前正在运行的集群管理器和 vdc-controller 实例。Auto Scaling 将使用最新值启动新实例。

.....

由于依赖对象错误，无法删除环境 CloudFormation 堆栈

如果由于依赖对象错误（例如）而导致**<env-name>**-vdc CloudFormation堆栈删除失败vdcdcvhostsecuritygroup，则可能是由于使用控制台在 RES 创建的子网或安全组中启动了 Amazon EC2 实例。 AWS

要解决此问题，请查找并终止所有以这种方式启动的 Amazon EC2 实例。然后，您可以继续删除环境。

.....

创建环境时遇到 CIDR 块参数错误

创建环境时，CIDR 块参数会出现错误，响应状态为 [FAILED]。

错误示例：

```
Failed to update cluster prefix list:
        An error occurred (InvalidParameterValue) when calling the
 ModifyManagedPrefixList operation:
        The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
 in the following form: 10.0.0.0/16.
```

为了解决这个问题，预期的格式是 x.x.0/24 或 x.x.0/32。

.....

CloudFormation 创建环境期间堆栈创建失败

创建环境涉及一系列资源创建操作。在某些区域，可能会出现容量问题，从而导致 CloudFormation 堆栈创建失败。

如果出现这种情况，请删除环境并重试创建。或者，您可以在其他区域重试创建。

.....

创建外部资源（演示）堆栈失败，并显示 AdDomainAdminNode CREATE_FAILED

如果演示环境堆栈创建失败并出现以下错误，则可能是由于 Amazon 在实例启动后的配置过程中意外进行了 EC2 修补。

```
AdDomainAdminNode CREATE_FAILED  Failed to receive 1 resource signal(s) within the
 specified duration
```

要确定失败原因，请执行以下操作：

1. 在 SSM 状态管理器中，检查是否已配置修补以及是否为所有实例配置了修补程序。
2. 在 SSM RunCommand/Automation 执行历史记录中，检查与补丁相关的 SSM 文档的执行是否与实例启动相吻合。
3. 在环境的 Amazon EC2 实例的日志文件中，查看本地实例日志以确定实例在配置期间是否重新启动。

如果问题是由修补引起的，请在启动后至少 15 分钟延迟 RES 实例的修补。

.....

身份管理问题

单点登录 (SSO) 和身份管理方面的大多数问题都是由于配置错误造成的。有关设置 SSO 配置的信息，请参阅：

- the section called “使用 IAM 身份中心设置 SSO”
- the section called “为单点登录 (SSO) 配置您的身份提供商”

要解决与身份管理相关的其他问题，请参阅以下疑难解答主题：

主题

- 我无权执行 iam：PassRole
- 我想允许 AWS 账户以外的人通过 AWS 资源访问我的研究与工程工作室
- 登录环境后，我会立即返回登录页面
- 尝试登录时出现 “未找到用户” 错误
- 已将用户添加到 Active Directory 中，但在
- 创建会话时用户不可用
- CloudWatch 集群管理器日志中出现超出大小限制错误

.....

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 RES。

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

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

在这种情况下，必须更新 Mary 的政策以允许她执行 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 AWS 账户以外的人通过 AWS 资源访问我的研究与工程工作室

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

要了解更多信息，请参阅以下内容：

- 要了解如何通过您拥有的 AWS 账户提供对资源的访问权限，请参阅 IAM 用户指南中的向您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何向第三方 AWS 账户提供对您的资源的访问权限，请参阅 IAM 用户指南中的向第三方 AWS 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 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）。
- 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 用户指南中的 IAM 角色与基于资源的策略有何不同。

.....

登录环境后，我会立即返回登录页面

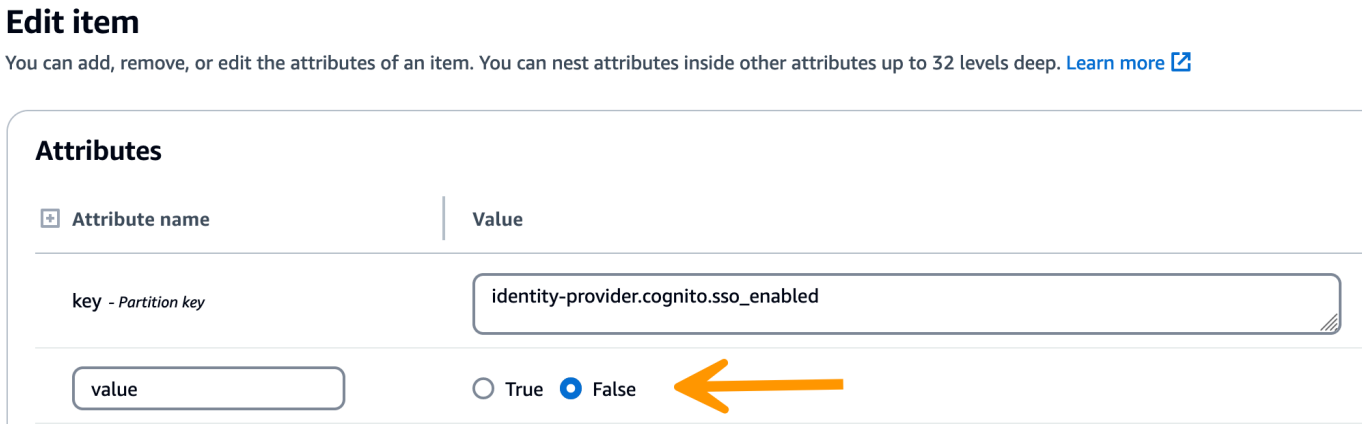
当您的 SSO 集成配置错误时，就会出现此问题。要确定问题所在，请检查控制器实例日志并查看配置设置中是否存在错误。

要查看日志，请执行以下操作：

1. 打开 CloudWatch 管理控制台。
2. 在日志组中，找到名为的组/*<environment-name>*/cluster-manager。
3. 打开日志组以搜索日志流中的任何错误。

要检查配置设置，请执行以下操作：

1. 打开 DynamoDB 控制台
2. 在表中，找到名为的表*<environment-name>*.cluster-settings。
3. 打开表格并选择 “浏览表格项目”。
4. 展开筛选器部分，然后输入以下变量：
   - 属性名称-关键
   - 状况-包含
   - 价值 — sso
5. 选择运行。
6. 在返回的字符串中，验证 SSO 配置值是否正确。如果它们不正确，请将 sso_enabled 密钥的值更改为 False。



7. 返回 RES 用户界面重新配置 SSO。

.....

尝试登录时出现 “未找到用户” 错误

如果用户在尝试登录 RES 界面时收到 “未找到用户” 错误，并且该用户出现在 Active Directory 中：

- 如果 RES 中没有该用户，而您最近已将该用户添加到 AD
  - 用户可能尚未同步到 RES。RES 每小时同步一次，因此您可能需要等待并检查用户是否已在下次同步后添加。要立即同步，请按照中的步骤操作已将用户添加到 Active Directory 中，但在。
- 如果用户出现在 RES 中：
  1. 确保属性映射配置正确。有关更多信息，请参阅 为单点登录 (SSO) 配置您的身份提供商。
  2. 确保 SAML 主题和 SAML 电子邮件都映射到用户的电子邮件地址。

.....

已将用户添加到 Active Directory 中，但在

如果您已将用户添加到 Active Directory，但在 RES 中却缺少该用户，则需要触发广告同步。AD 同步由 Lambda 函数每小时执行一次，该函数将 AD 条目导入 RES 环境。有时，在添加新用户或群组后，下一个同步过程会有延迟。您可以通过 Amazon 简单队列服务手动启动同步。

手动启动同步过程：

1. 打开 Amazon SQS 控制台。
2. 从 “队列” 中选择<environment-name>-cluster-manager-tasks.fifo。
3. 选择 “发送和接收消息”。
4. 在邮件正文中，输入：

   ```
   { "name": "adsync.sync-from-ad", "payload": {} }
   ```

5. 在消息组 ID 中，输入：**adsync.sync-from-ad**
6. 在消息重复数据删除 ID 中，输入一个随机的字母数字字符串。此条目必须不同于前五分钟内拨打的所有电话，否则该请求将被忽略。

.....

创建会话时用户不可用

如果您是管理员，正在创建会话，但在创建会话时发现 Active Directory 中的用户不可用，则该用户可能需要首次登录。只能为活跃用户创建会话。活跃用户必须至少登录环境一次。

CloudWatch 集群管理器日志中出现超出大小限制错误

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11,
 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

如果您在 CloudWatch 集群管理器日志中收到此错误，那么 ldap 搜索可能返回了太多的用户记录。要解决此问题，请提高您的 IDP 的 ldap 搜索结果限制。

存储

主题

我通过 RES 创建了文件系统，但它没有挂载到 VDI 主机上

文件系统必须处于 “可用” 状态，然后才能由 VDI 主机装载。按照以下步骤验证文件系统是否处于所需状态。

Amazon EFS

1. 前往 Amazon EFS 控制台。
2. 检查文件系统状态是否为 “可用”。
3. 如果文件系统状态为 “不可用”，请等待，然后再启动 VDI 主机。

1. 前往 Amazon FSx 控制台。
2. 检查状态是否为可用。
3. 如果 “状态” 为 “不可用”，请等待，然后再启动 VDI 主机。

.....

我通过 RES 加载了一个文件系统，但它没有安装到 VDI 主机上

RES 上载入的文件系统应配置所需的安全组规则，以允许 VDI 主机挂载文件系统。由于这些文件系统是在 RES 外部创建的，因此 RES 不管理相关的安全组规则。

与已载入文件系统关联的安全组应允许以下入站流量：

- 来自 linux VDC 主机的 NFS 流量（端口：2049）
- 来自 Windows VDC 主机的中小型企业流量（端口：445）

.....

我无法从 VDI 主机 read/write 上打开

ONTAP 支持卷的 UNIX、NTFS 和混合安全风格。安全风格决定了 ONTAP 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

例如，如果卷使用 UNIX 安全风格，则由于 ONTAP 的多协议性质，SMB 客户端仍然可以访问数据（前提是它们必须正确进行身份验证和授权）。但是，ONTAP 使用 UNIX 权限，只有 UNIX 客户端才能使用本机工具修改这些权限。

权限处理用例示例

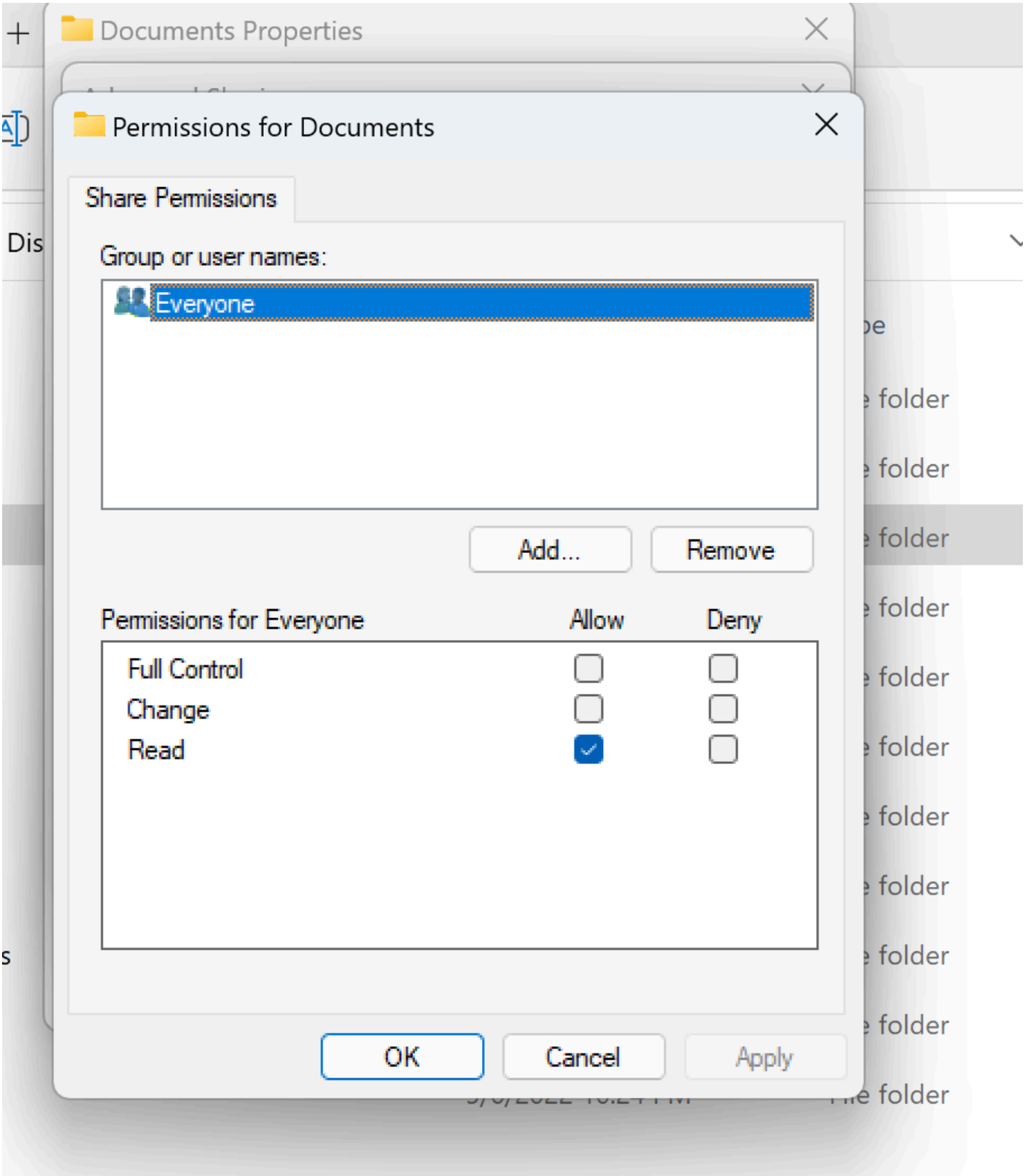
对 Linux 工作负载使用 UNIX 风格的

sudoer 可以为其他用户配置权限。例如，以下内容将授予所有成员对该/<project-name>目录的<group-ID>完全 read/write 权限：

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

在 Linux 和 Windows 工作负载中使用 NTFS 风格的音量

可以使用特定文件夹的共享属性来配置共享权限。例如，给定一个用户user_01和一个文件夹myfolder，你可以将Full ControlChange、或的权限设置Read为Allow或Deny：


Documents Properties
Permissions for Documents
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

如果 Linux 和 Windows 客户端都要使用该卷，我们需要在 SVM 上设置名称映射，将任何 Linux 用户名与相同用户名与域\ 用户名的 NetBIOS 域名格式相关联。这是在 Linux 和 Windows 用户之间进行转换所必需的。有关参考，请参阅使用 Amazon for NetApp ONTAP 启用多协议工作负载 FSx 。

.....

我从 RES 创建了 Amazon FSx for NetApp ONTAP 但它没有加入我的域名

当前，当您从 RES 控制台创建 Amazon FSx for NetApp ONTAP 时，文件系统已配置但不会加入域。要将创建的 ONTAP 文件系统 SVM 加入您的域，请参阅加入 SVMs Microsoft Active Directory 并按照亚马逊 FSx 控制台上的步骤进行操作。确保将所需权限委派给 AD 中的 Amazon FSx 服务账户。SVM 成功加入域后，转到 SVM 摘要 > 终端节点 > SMB DNS 名称，然后复制 DNS 名称，因为稍后将需要它。

加入域后，在集群设置 DynamoDB 表中编辑 SMB DNS 配置密钥：

1. 前往亚马逊 DynamoDB 控制台。
2. 选择 “表”，然后选择`<stack-name>-cluster-settings`。
3. 在 “浏览表格项目” 下，展开 “筛选器”，然后输入以下筛选器：
   - 属性名称-密钥
   - 条件-等于
   - 价值-`shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. 选择退回的商品，然后选择操作、编辑项目。
5. 使用您之前复制的 SMB DNS 名称更新该值。
6. 选择 “保存并关闭”。

此外，确保与文件系统关联的安全组按照 Amazon VPC 的文件系统访问控制中的建议允许流量。使用文件系统的新 VDI 主机现在可以挂载已加入的 SVM 和文件系统的域。

或者，您可以使用 RES Onboard File System 功能加载已加入域的现有文件系统——从 “环境管理” 中选择 “文件系统”、“板载文件系统”。

.....

快照

主题

- 快照的状态为 “失败”
- 快照应用失败，日志显示无法导入表。

.....

快照的状态为 “失败”

在 RES 快照页面上，如果快照的状态为 “失败”，则可以通过前往集群管理器的 Amazon CloudWatch 日志组中查看错误发生时间来确定原因。

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
  asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
  creating the snapshot: An error occurred (TableNotFoundException)
  when calling the UpdateContinuousBackups operation:
  Table not found: res-demo.accounts.sequence-config
```

.....

快照应用失败，日志显示无法导入表。

如果从先前环境中拍摄的快照无法应用于新环境，请查看集群管理器的 CloudWatch 日志以确定问题。如果问题提到无法导入所需的表，请验证快照是否处于有效状态。

1. 下载 metadata.json 文件并验证各个表的状态是否 ExportStatus 为 “已完成”。确保各个表都设置了`ExportManifest`字段。如果未找到上述字段集，则快照处于无效状态，无法与应用快照功能一起使用。
2. 启动快照创建后，请确保快照状态在 RES 中变为 “已完成”。快照创建过程最多需要 5 到 10 分钟。重新加载或重新访问 “快照管理” 页面，以确保成功创建快照。这将确保创建的快照处于有效状态。

.....

基础设施

主题

- 负载均衡器目标群组没有运行正常的实例

.....

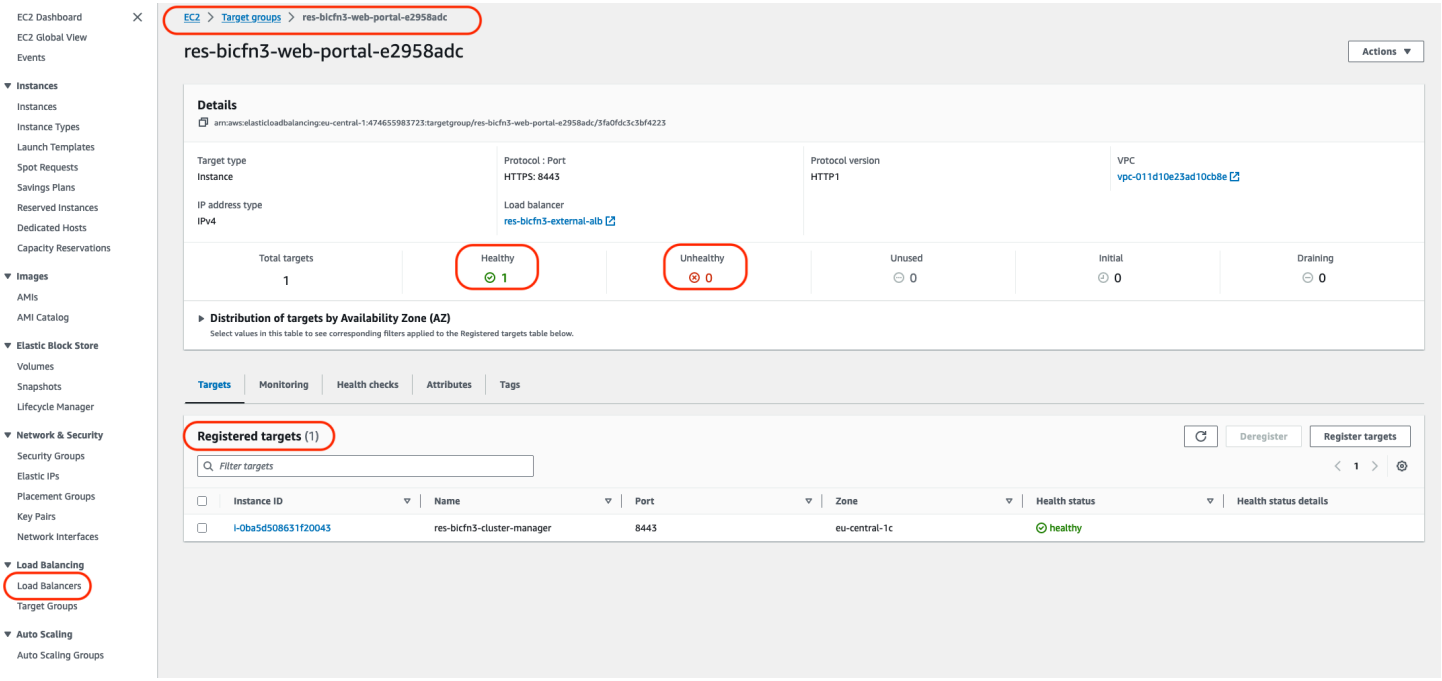
负载均衡器目标群组没有运行正常的实例

如果用户界面中出现服务器错误消息或桌面会话无法连接等问题，则可能表示基础设施 Amazon EC2 实例存在问题。

确定问题根源的方法是，首先检查亚马逊 EC2 控制台中是否存在任何似乎反复终止并被新 EC2 实例取代的亚马逊实例。如果是这样的话，查看 Amazon CloudWatch 日志可能会确定原因。

另一种方法是检查系统中的负载均衡器。如果在 Amazon EC2 控制台上找到的任何负载均衡器未显示任何已注册的运行正常的实例，则表明可能存在系统问题。

此处显示了正常外观的示例：



如果 “正常” 条目为 0，则表示没有 Amazon EC2 实例可用于处理请求。

如果 Unhealthy 条目不是 0，则表示 Amazon EC2 实例可能正在循环。这可能是由于安装的应用程序软件未通过运行状况检查所致。

如果 “正常” 和 “不健康” 条目均为 0，则表示可能存在网络配置错误。例如，公有子网和私有子网可能没有对应 AZs的子网。如果出现这种情况，则控制台上可能会有其他文本表明存在网络状态。

.....

启动虚拟桌面

主题

.....

以前运行的虚拟桌面无法再成功连接

如果桌面连接关闭或您无法再连接到该连接，则问题可能是由于底层 Amazon EC2 实例出现故障，或者 Amazon EC2 实例可能已在 RES 环境之外终止或停止。管理界面状态可能会继续显示就绪状态，但尝试连接失败。

应使用 Amazon EC2 控制台来确定实例是否已终止或停止。如果已停止，请尝试重新启动。如果状态终止，则必须创建另一个桌面。当新实例启动时，存储在用户主目录中的任何数据都应该仍然可用。

如果之前失败的实例仍显示在管理界面上，则可能需要使用管理界面将其终止。

.....

我只能启动 5 个虚拟桌面

用户可以启动的虚拟桌面数量的默认限制为 5。管理员可以使用管理界面进行更改，如下所示：

- 前往 “桌面设置”。
- 选择 “服务器” 选项卡。
- 在 DCV 会话面板中，单击右侧的编辑图标。
- 将 “每位用户允许的会话数” 中的值更改为所需的新值。
- 选择提交。
- 刷新页面以确认新设置已到位。

.....

桌面 Windows 连接尝试失败，并显示 “连接已关闭”。传输错误”

如果 Windows 桌面连接失败并显示界面错误 “连接已关闭。传输错误”，原因可能是由于在 Windows 实例上创建证书的 DCV 服务器软件存在问题。

Amazon CloudWatch 日志组<envname>/vdc/dcv-connection-gateway可能会使用类似以下内容的消息记录连接尝试错误：

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]

Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

如果发生这种情况，解决方案可能是使用 SSM 会话管理器打开与 Windows 实例的连接并删除以下 2 个与证书相关的文件：

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

应自动重新创建这些文件，后续的连接尝试可能会成功。

如果此方法解决了问题，并且新启动的 Windows 桌面产生相同的错误，请使用创建软件堆栈功能使用重新生成的证书文件创建固定实例的新 Windows 软件堆栈。这可能会生成可用于成功启动和连接的 Windows 软件堆栈。

.....

VDIs 停留在置备状态

如果桌面启动在管理界面中仍处于预配状态，则可能是由于多种原因造成的。

要确定原因，请检查桌面实例上的日志文件并查找可能导致问题的错误。本文档在标有 “有用的日志和事件信息源” 部分中包含相关信息的日志文件和 Amazon CloudWatch 日志组列表。

以下是此问题的潜在原因。

- 所使用的 AMI ID 已注册为软件堆栈，但 RES 不支持。

  由于 AMI 没有所需的预期配置或工具，引导程序配置脚本未能完成。实例（例如 Linux 实例）`/root/bootstrap/logs/`上的日志文件可能包含与此相关的有用信息。 AMIs 从 AWS Marketplace 中获取的 ID 可能不适用于 RES 桌面实例。它们需要测试以确认它们是否得到支持。

- 从自定义 AMI 启动 Windows 虚拟桌面实例时，不会执行用户数据脚本。

  默认情况下，用户数据脚本在 Amazon EC2 实例启动时运行一次。如果您从现有虚拟桌面实例创建 AMI，然后向 AMI 注册软件堆栈并尝试使用此软件堆栈启动另一个虚拟桌面，则用户数据脚本将无法在新虚拟桌面实例上运行。

  要修复此问题，请以管理员身份在用于创建 AMI 的原始虚拟桌面实例上打开 PowerShell 命令窗口，然后运行以下命令：

  ```
  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
  ```

  然后从该实例创建一个新的 AMI。您可以使用新的 AMI 注册软件堆栈，然后启动新的虚拟桌面。请注意，您也可以在仍处于配置状态的实例上运行相同的命令，然后重启该实例以修复虚拟桌面会话，但是从配置错误的 AMI 启动另一个虚拟桌面时，您将再次遇到相同的问题。

.....

VDIs 启动后进入错误状态

可能的问题 1：主文件系统为具有不同 POSIX 权限的用户提供了目录。

如果以下情况属实，这可能是你面临的问题：

1. 部署的 RES 版本为 2024.01 或更高版本。
2. 在部署 RES 堆栈期间，的属性设置`EnableLdapIDMapping`为`True`。

3. 在 RES 堆栈部署期间指定的主文件系统曾在 RES 2024.01 之前的版本中使用，或者在设置为的先前环境中使用。`EnableLdapIDMapping False`

解决步骤：删除文件系统中的用户目录。

1. SSM 到集群管理器主机。
2. `cd /home`.
3. `ls`-应列出目录名与用户名匹配的目录，例如`admin1`、`admin2`... 等。
4. 删除目录，`sudo rm -r 'dir_name'`。不要删除 ssm-user 和 ec2-user 目录。
5. 如果用户已经同步到新环境，请从用户的 DDB 表（clusteradmin 除外）中删除该用户的环境。
6. 启动 AD 同步-`sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` 在集群管理器 Amazon 中运行。 EC2
7. 从 RES 网页重启`Error`处于状态的 VDI 实例。验证 VDI 是否在大约 20 分钟后转换到`Ready`状态。

.....

虚拟桌面组件

主题

.....

Amazon EC2 实例在控制台中反复显示已终止

如果基础设施实例在 Amazon EC2 控制台中反复显示为已终止，则原因可能与其配置有关，并取决于基础设施实例的类型。以下是确定原因的方法。

如果 vdc-controller 实例在 Amazon EC2 控制台中显示重复的终止状态，则可能是由于密钥标签不正确所致。由 RES 维护的密钥具有标签，这些标签可用作附加到基础设施 Amazon EC2 实例的 IAM 访问控制策略的一部分。如果 vdc-controller 正在循环并且 CloudWatch 日志组中出现以下错误，则原因可能是未正确标记密钥。请注意，需要使用以下内容标记密钥：

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

此错误的 Amazon CloudWatch 日志消息将如下所示：

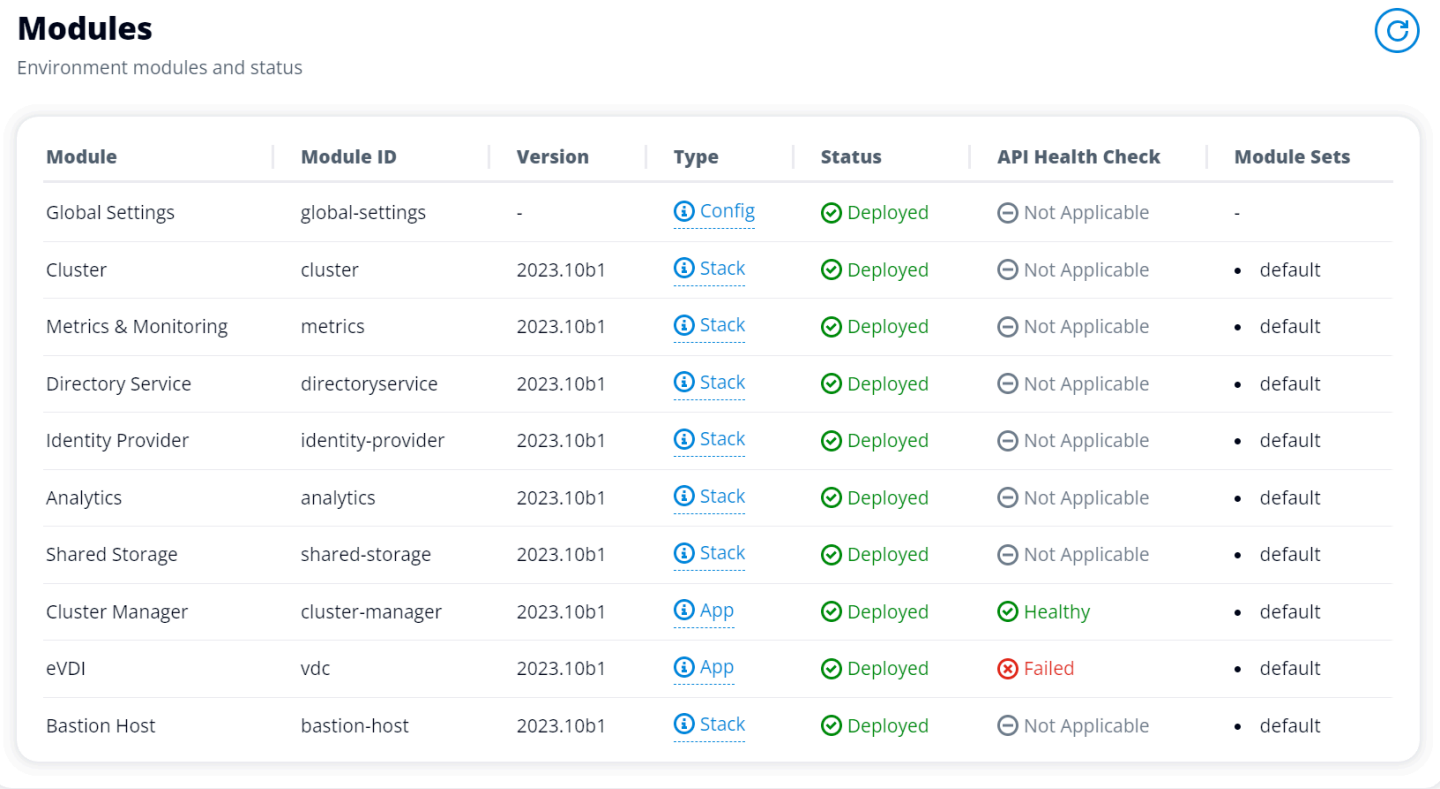
```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

检查 Amazon EC2 实例上的标签并确认它们与上面的列表相匹配。

.....

由于无法加入 AD/eVDi 模块显示 API Health Check 失败，vdc-controller 实例正在循环

如果 eVDi 模块的运行状况检查失败，它将在环境状态部分显示以下内容。



Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

在这种情况下，调试的一般路径是查看集群管理器CloudWatch日志。（查找名为的日志组`<env-name>/cluster-manager`。）

可能的问题：

- 如果日志包含文本`Insufficient permissions`，请确保创建 res 堆栈时给出的 ServiceAccount 用户名拼写正确。

  日志行示例：

  ```
  Insufficient permissions to modify computer account:
   CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
   000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - 您可以从 SecretsManager 控制台访问 RES 部署期间提供的 ServiceAccount 用户名。在 Secrets 管理器中找到相应的密钥，然后选择 “检索纯文本”。如果用户名不正确，请选择编辑以更新密码值。终止当前的集群管理器和 vdc-Controller 实例。新实例将处于稳定状态。

- 如果您正在使用由提供的外部资源堆栈创建的资源，则用户名必须ServiceAccount为 “”。如果在部署 RES 期间将该DisableADJoin参数设置为 False，请确保 ServiceAccount “” 用户有权在 AD 中创建计算机对象。

- 如果使用的用户名正确，但日志中包含文本Invalid credentials，则您输入的密码可能错误或已过期。

  日志行示例：

  ```
  {'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
   'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
   data 532, v4563'}
  ```

  - 通过在 Secr ets Manager 控制台中访问存储密码的密钥，您可以读取您在创建环境时输入的密码。选择密钥（例如<env_name>directoryserviceServiceAccountPassword），然后选择 “检索纯文本”。
  - 如果密钥中的密码不正确，请选择编辑以更新其在密钥中的值。终止当前的集群管理器和 vdc-Controller 实例。新实例将使用更新的密码并处于稳定状态。
  - 如果密码正确，则可能是连接的 Active Directory 中的密码已过期。你必须先在 Active Directory 中重置密码，然后更新密码。您可以通过 Directory Ser vice 控制台在 Active Direc tory 中重置用户的密码：
    1. 选择相应的目录 ID
    2. 选择 “操作”、“重置用户密码”，然后在表单中填写用户名（例如 ServiceAccount “”）和新密码。
    3. 如果新设置的密码与之前的密码不同，请更新相应的 Secret Manager 密钥中的密码（例如，<env_name>directoryserviceServiceAccountPassword.
    4. 终止当前的集群管理器和 vdc-Controller 实例。新实例将处于稳定状态。

编辑软件堆栈以添加项目时，项目不会出现在下拉列表中

此问题可能与以下与将用户帐户与 AD 同步相关的问题有关。如果出现此问题，请检查集群管理器 Amazon CloudWatch 日志组中是否存在错误 <user-home-init> account not available yet. waiting for user to be synced “”，以确定原因是相同还是相关。

---

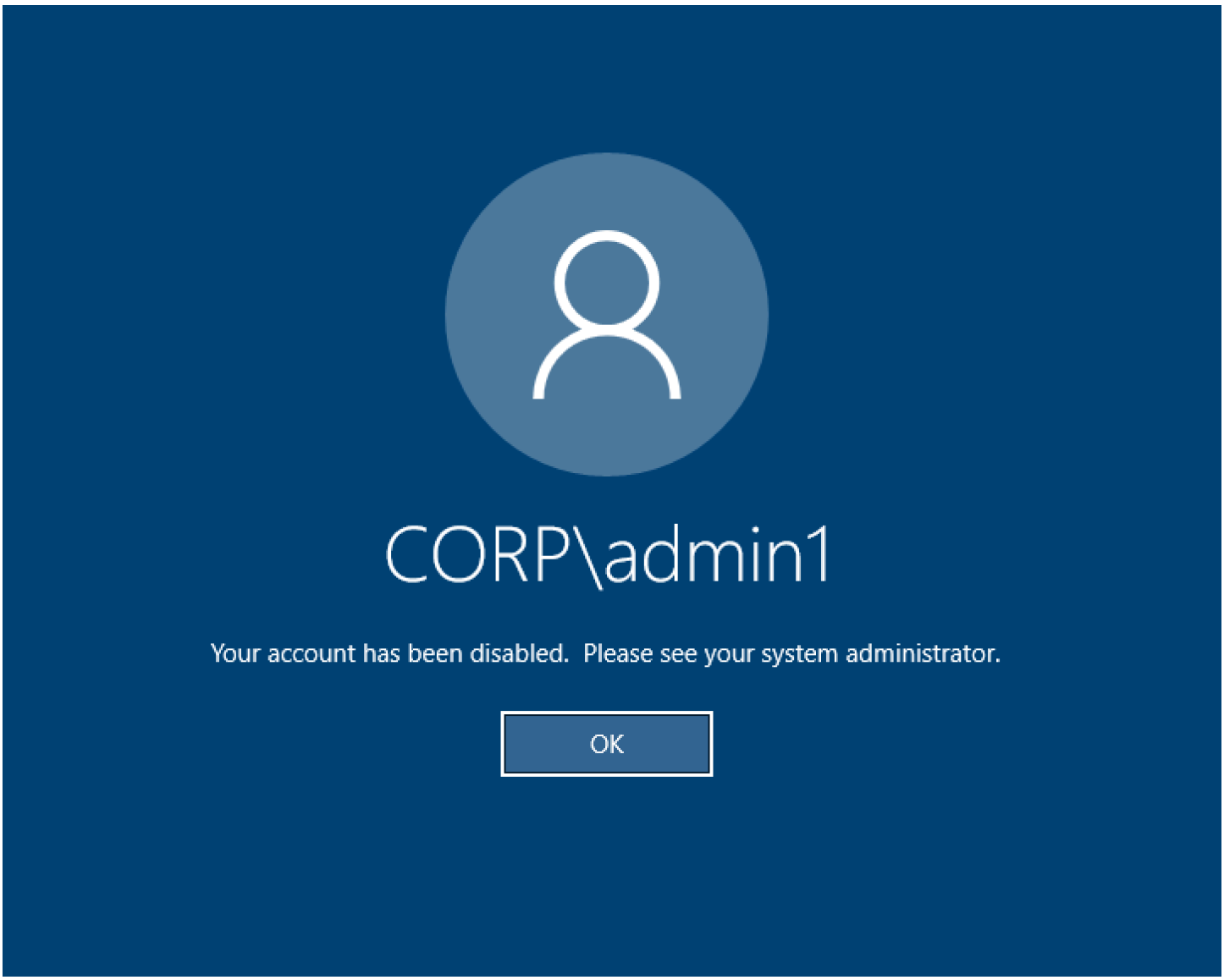
cluster-manager Amazon CloudWatch 日志显示 “< user-home-init > 账户还不可用。正在等待用户同步”（其中账户是用户名）

SQS 订阅者由于无法访问用户帐户而忙碌并陷入无限循环。在用户同步期间尝试为用户创建主文件系统时，会触发此代码。

它无法访问用户帐户的原因可能是没有为正在使用的 AD 正确配置 RES。例如，创建 BI/RES 环境时使用的`ServiceAccountUsername`参数值不正确，例如使用 “” 而不是 ServiceAccount “Admin”。

.....

尝试登录时的 Windows 桌面显示 “您的帐户已被禁用。请咨询您的管理员”



如果用户无法重新登录锁定屏幕，则可能表示该用户在通过 SSO 成功登录后，已在为 RES 配置的 AD 中被禁用。

如果在 AD 中禁用了用户帐户，SSO 登录应该会失败。

.....

external/customer AD 配置的 DHCP 选项问题

如果您在自己的 Active D "The connection has been closed. Transport error" irectory 中使用 RES 时遇到错误说明 Windows 虚拟桌面，请查看 dcv-connection-gateway Amazon CloudWatch 日志中是否有类似以下内容的内容：

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }

Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

如果您将 AD 域控制器用于自己的 VPC 的 DHCP 选项，则需要：

1. 将 AmazonProvided DNS 添加到两个域控制器 IPs。
2. 将域名设置为 ec2.internal。

此处显示了一个示例。如果没有此配置，Windows 桌面将显示传输错误，因为正在查 RES/DCV 找 ip-10-0-xx.ec2.internal 主机名。

.....

Firefox 错误 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

当你使用 Firefox 网络浏览器时，当你尝试连接到虚拟桌面时，你可能会遇到错误消息类型 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING。

原因是 RES Web 服务器设置为 TLS + Stapling On，但使用装订验证没有响应（参见 https://support.mozilla。 org/en-US/questions/1372483。

你可以按照以下地址的说明解决这个问题： https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing。

.....

环境删除

主题

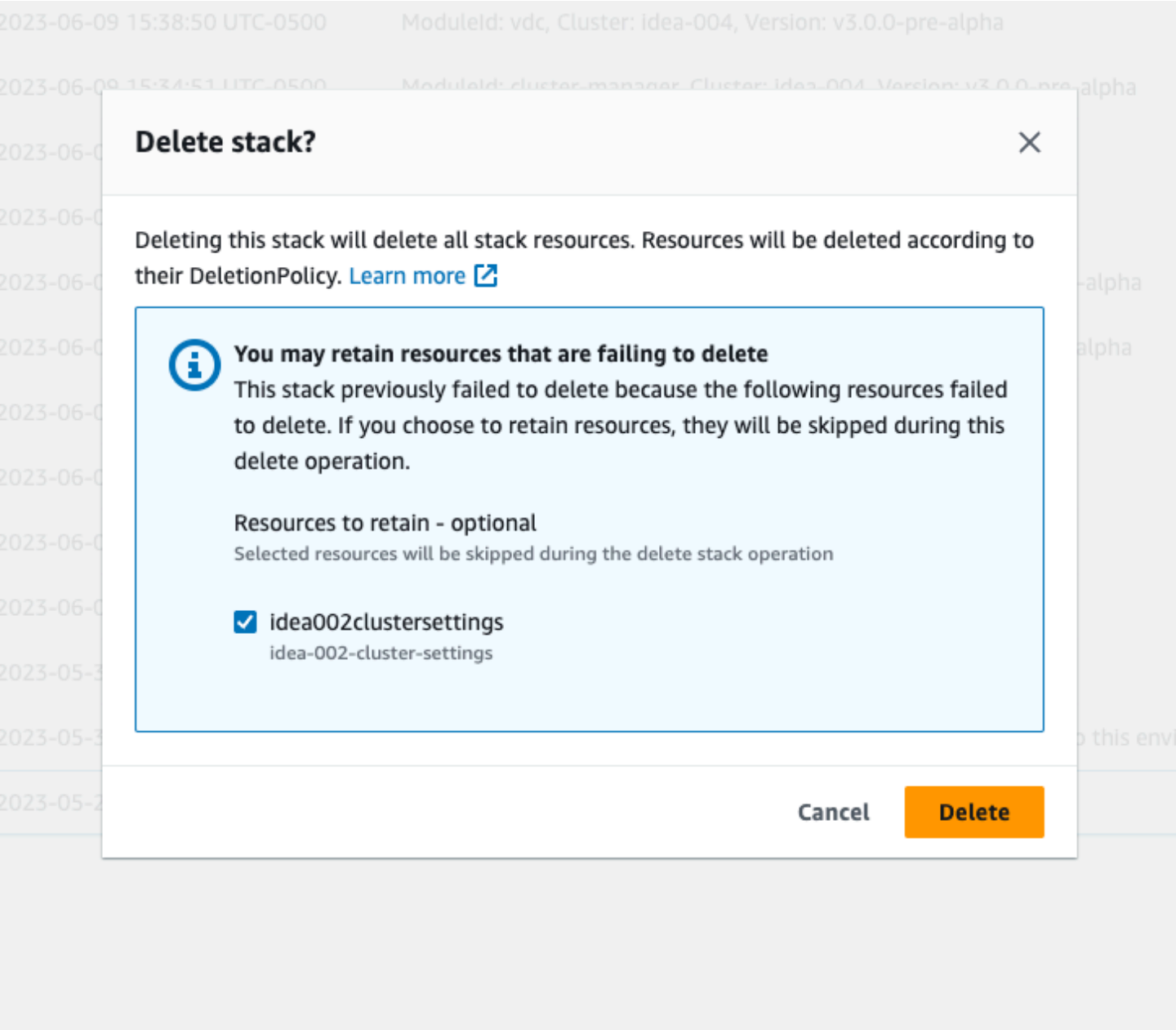
- res-xxx-cluster 堆栈处于 “DELETE_FAILED” 状态，由于 “角色无效或无法假设” 错误，无法手动删除
- 收集日志
- 正在下载 VDI 日志
- 从 Linux EC2 实例下载日志
- 从 Windows EC2 实例下载日志
- 正在收集 WaitCondition 错误的 ECS 日志

.....

res-xxx-cluster 堆栈处于 “DELETE_FAILED” 状态，由于 “角色无效或无法假设” 错误，无法手动删除

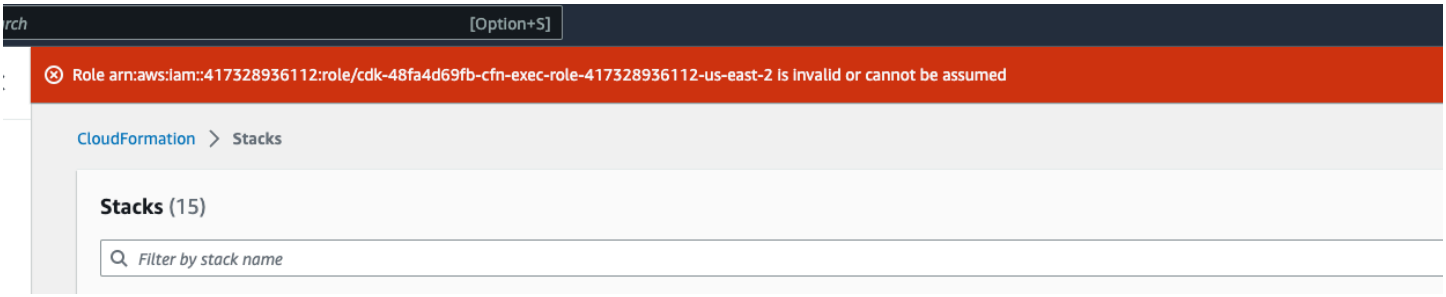
如果您注意到 “” res-xxx-cluster 堆栈处于 “DELETE_FAILED” 状态且无法手动删除，则可以执行以下步骤将其删除。

如果您看到堆栈处于 “DELETE_FAILED” 状态，请先尝试手动将其删除。它可能会弹出一个确认删除堆栈的对话框。选择删除。



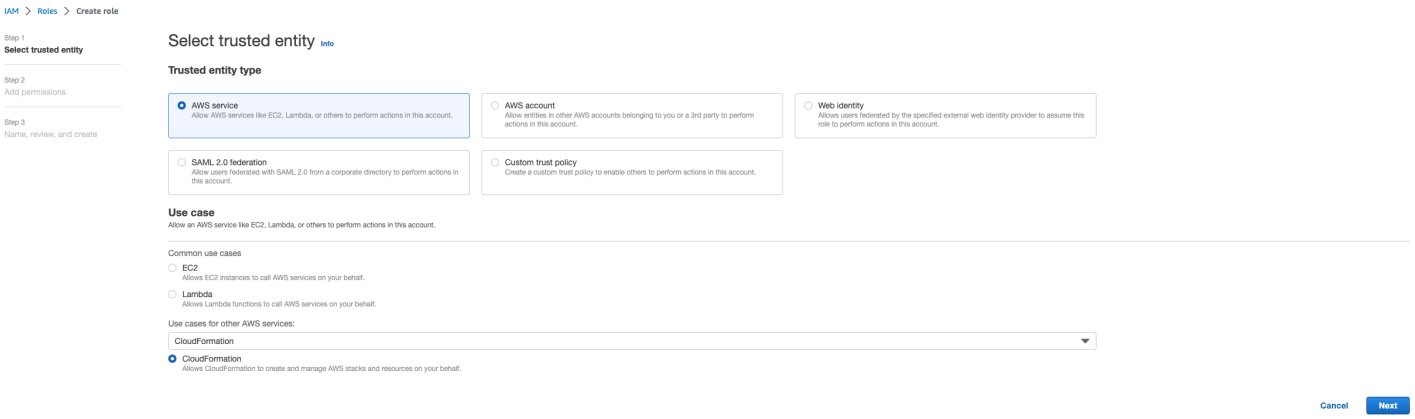
有时，即使您删除了所有必需的堆栈资源，您仍可能会看到选择要保留的资源的消息。在这种情况下，请选择所有资源作为“要保留的资源”，然后选择删除。

你可能会看到一个如下所示的错误 `Role: arn:aws:iam::... is Invalid or cannot be assumed`

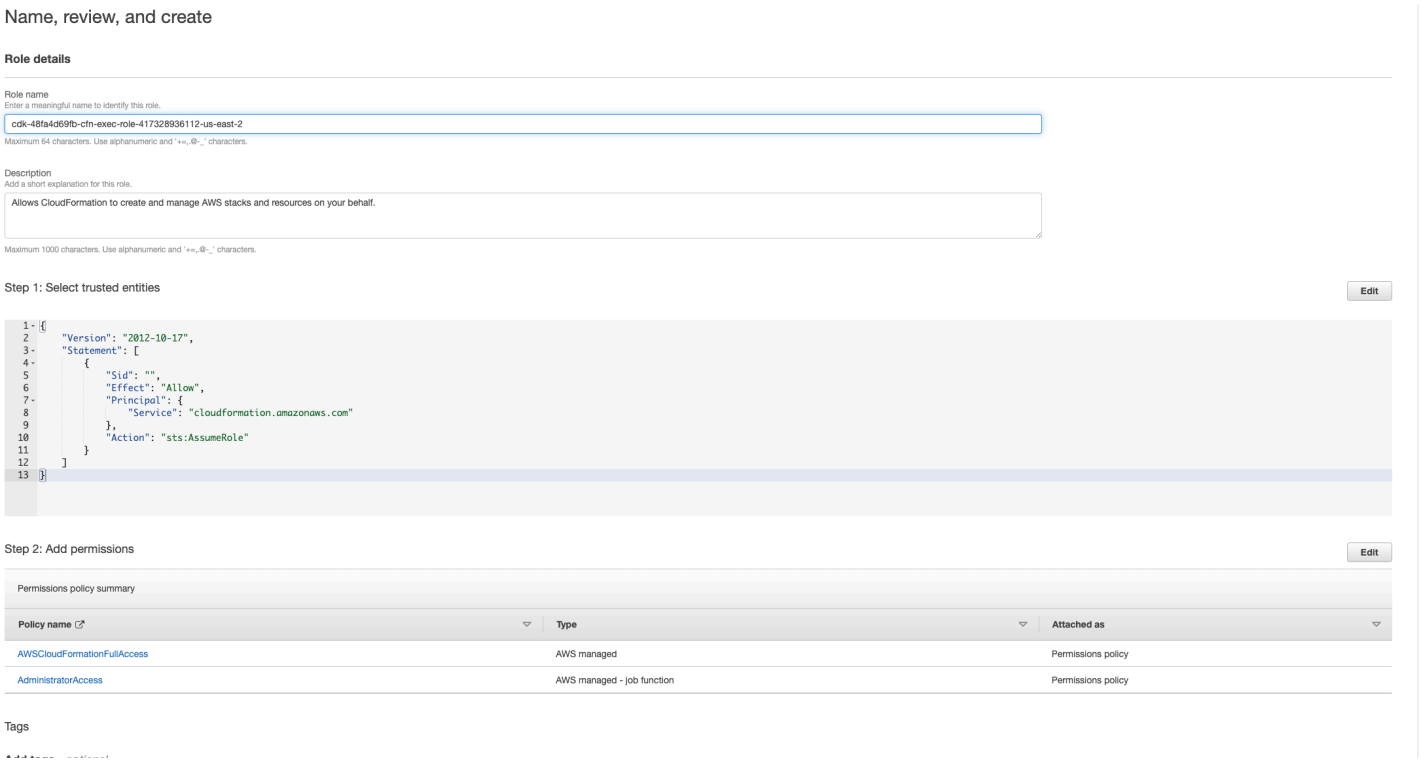


这意味着删除堆栈所需的角色在堆栈之前先被删除。要解决这个问题，请复制角色的名称。前往 IAM 控制台，使用此处所示的参数创建具有该名称的角色，这些参数是：

- 对于可信实体类型，请选择AWS 服务。
- 对于用例，请在 `Use cases for other AWS services` “选择” 下方`CloudFormation`。



选择下一步。确保为角色授予 “AWSCloudFormationFullAccess” 和 “AdministratorAccess” 权限。您的评论页面应如下所示：



然后返回 CloudFormation 控制台并删除堆栈。自创建角色以来，您现在应该可以将其删除。最后，前往 IAM 控制台并删除您创建的角色。

.....

收集日志

从 EC2 控制台登录 EC2 实例

- 按照以下说明登录您的 Linux EC2 实例。
- 按照以下说明登录到你的 Windows EC2 实例。然后打开 Windows PowerShell 以运行任何命令。

收集基础架构主机日志

1. Cluster-Manager：从以下位置获取集群管理器的日志，并将其附加到票证中。
   a. 日志组中的所有 CloudWatch 日志`<env-name>/cluster-manager`。
   b. `<env-name>-cluster-manager` EC2 实例上`/root/bootstrap/logs`目录下的所有日志。按照本节开头的 “从 EC2 控制台登录 EC2 实例” 中链接到的说明登录您的实例。
2. VDC-Controller：从以下位置获取 vdc-Controller 的日志，并将其附加到票证中。
   a. 日志组中的所有 CloudWatch 日志`<env-name>/vdc-controller`。

b. <env-name>-vdc-controller EC2 实例上/root/bootstrap/logs目录下的所有日志。按照本节开头的 “从 EC2 控制台登录 EC2 实例” 中链接到的说明登录您的实例。

轻松获取日志的方法之一是按照从 Linux EC2 实例下载日志本节中的说明进行操作。模块名称将是实例名称。

收集 VDI 日志

识别相应的 Amazon EC2 实例

如果用户启动了带有会话名称的 VDIVDI1，则 Amazon EC2 控制台上的相应实例名称将是。<env-name>-VDI1-<user name>

收集 Linux VDI 日志

按照本节开头 “从 EC2 控制台登录 EC2 实例” 中链接的说明，从 Amazon EC2 控制台登录相应的 Amazon EC2 实例。获取 VDI Amazon EC2 实例上/root/bootstrap/logs和/var/log/dcv/目录下的所有日志。

获取日志的方法之一是将它们上传到 s3，然后从那里下载。为此，您可以按照以下步骤从一个目录中获取所有日志，然后将其上传：

1. 按照以下步骤在/root/bootstrap/logs目录下复制 dcv 日志：

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. 现在，按照下一节中列出的步骤下载日志。正在下载 VDI 日志

收集 Windows VDI 日志

按照本节开头 “从 EC2 控制台登录 EC2 实例” 中链接的说明，从 Amazon EC2 控制台登录相应的 Amazon EC2 实例。获取 VDI EC2 实例上$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\目录下的所有日志。

获取日志的方法之一是将它们上传到 S3，然后从那里下载。为此，请按照下一节中列出的步骤进行操作-正在下载 VDI 日志。

.....

正在下载 VDI 日志

1. 更新 VDI EC2 实例 IAM 角色以允许 S3 访问。
2. 转到 EC2 控制台并选择您的 VDI 实例。
3. 选择它正在使用的 IAM 角色。
4. 在 “添加权限” 下拉菜单的 “权限策略” 部分，选择 “附加策略”，然后选择 AmazonS3 FullAccess 策略。
5. 选择添加权限以附加该策略。
6. 之后，根据您的 VDI 类型，按照下面列出的步骤下载日志。模块名称将是实例名称。
   a. 从 Linux EC2 实例下载日志适用于 Linux。
   b. 从 Windows EC2 实例下载日志适用于 Windows。
7. 最后，编辑角色以删除AmazonS3FullAccess策略。

> **Note**
>
> 所有角色都 VDIs 使用相同的 IAM 角色，即 <env-name>-vdc-host-role-<region>

.....

从 Linux EC2 实例下载日志

登录您要从中下载日志的 EC2 实例，然后运行以下命令将所有日志上传到 s3 存储桶：

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

之后，转到 S3 控制台，选择带有名称的存储桶，<environment_name>-cluster-<region>-<aws_account_number>然后下载之前上传的<module_name>_logs.tar.gz文件。

.....

从 Windows EC2 实例下载日志

登录您要从中下载日志的 EC2 实例，然后运行以下命令将所有日志上传到 S3 存储桶：

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

之后，转到 S3 控制台，选择带有名称的存储桶，<environment_name>-cluster-<region>-<aws_account_number>然后下载之前上传的<module_name>_logs.zip文件。

.....

正在收集 WaitCondition 错误的 ECS 日志

1. 转到已部署的堆栈并选择 “资源” 选项卡。
2. 展开部署 ResearchAndEngineeringStudio→ 安装程序 → 任务 CreateTaskDef→ CreateContainer→ LogGroup，然后选择要打开日志的 CloudWatch 日志组。
3. 从该日志组中获取最新的日志。

.....

演示环境

主题

- 处理对身份提供商的身份验证请求时出现演示环境登录错误

.....

处理对身份提供商的身份验证请求时出现演示环境登录错误

问题

如果您尝试登录并收到 “处理身份提供商的身份验证请求时出现意外错误”，则您的密码可能已过期。这可能是你尝试登录的用户的密码，也可以是你的 Active Directory Service 账户。

缓解方法

1. 在目录服务控制台中重置用户和服务帐户密码。
2. 更新 S ecrets Manager 中的服务帐户密码，使其与您在上面输入的新密码相匹配：
   - 对于 Keycloak 堆栈：PasswordSecret-... -RESExternal-... -DirectoryService-... 附带描述：微软 Active Directory 的密码
   - 对于 RES：res-ServiceAccountPassword-... 带描述：Active Directory Service 账户密码
3. 转到EC2 控制台并终止集群管理器实例。Auto Scaling 规则将自动触发新实例的部署。

.....

已知问题

- 2024.x 已知问题
  - (2024.06) 当 AD 组名称包含空格时，应用快照失败
  - (2024.04-2024.04.02) 提供的 IAM 权限边界未附加到 VDI 实例的角色
  - （2024.04.02 及更早版本）ap-southeast-2（悉尼）中的 Windows NVIDIA 实例无法启动
  - (2024.04 和 2024.04.01) RES 删除失败 GovCloud
  - (2024.04-2024.04.02) Linux 虚拟桌面在重启时可能处于 “恢复” 状态
  - (2024.04.02 及更早版本) 无法同步 “ SAMAccount姓名” 属性包含大写字母或特殊字符的 AD 用户
  - （2024.04.02 及更早版本）用于访问堡垒主机的私钥无效
  - （2024.06 及更早版本）在 AD 同步期间，群组成员未与 RES 同步
  - （2024.06 及更早版本）CVE-2024-6387、Regre SSHion、和 Ubuntu 中的安全漏洞 RHEL9 VDIs

2024.x 已知问题

.....

(2024.06) 当 AD 组名称包含空格时，应用快照失败

问题

如果 AD 组的名称中包含空格，则 RES 2024.06 将无法应用先前版本的快照。

在 AD 同步期间，集群管理器 CloudWatch 日志（在<environment-name>/cluster-manager日志组下）将包含以下错误：

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

该错误是由于 RES 仅接受符合以下要求的组名：

- 它只能包含小写和大写的 ASCII 字母、数字、破折号 (-)、句点 (.) 和下划线 (_)
- 不允许使用破折号 (-) 作为第一个字符
- 它不能含有空格。

受影响的版本

2024.06

缓解方法

1. 要下载补丁脚本和补丁文件（patch.py 和 g roupname_regex.patch），请运行以下命令，<output-directory>替换为要存放文件的目录和 RES 环境<environment-name>的名称：

   a. 该补丁仅适用于 RES 2024.06

   b. 补丁脚本需要 AWS CLI v2、Python 3.9.16 或更高版本以及 Boto3。

   c. 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有 S3 权限来写入 RES 创建的存储桶：

      ```
      OUTPUT_DIRECTORY=<output-directory>
      ```

```
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. 导航到下载补丁脚本和补丁文件的目录。运行以下补丁命令：

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. 要为您的环境重启集群管理器实例，请运行以下命令：您也可以从 Amazon EC2 管理控制台终止该实例。

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> 该补丁允许 AD 组名称包含小写和大写的 ASCII 字母、数字、短划线 (-)、句点 (.)、下划线 (_) 以及总长度介于 1 到 30 之间（含）的空格。

.....

(2024.04-2024.04.02) 提供的 IAM 权限边界未附加到 VDI 实例的角色

这个问题

虚拟桌面会话无法正确继承其项目的权限边界配置。这是因为在项目创建期间，Boundary 参数定义的权限 IAMPermission边界未正确分配给该项目。

受影响的版本

2024.04-2024.04.02

缓解方法

请按照以下步骤正确继承分配给项目的权限边界： VDIs

1. 要下载补丁脚本和补丁文件（patch.py 和 vdi_host_role_permission_boundary.patch），请运行以下命令，替换<output-directory>为要存放文件的本地目录：

   a. 该补丁仅适用于 RES 2024.04.02。如果您使用的是版本 2024.04 或 2024.04.01，则可以按照公共文档中列出的次要版本更新的步骤将您的环境更新到 2024.04.02。

   b. 补丁脚本需要 AWS CLI v2)、Python 3.9.16 或更高版本以及 Boto3。

   c. 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有 S3 权限来写入 RES 创建的存储桶。

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. 导航到下载补丁脚本和补丁文件的目录。运行以下补丁命令，<environment-name>替换为 RES 环境的名称：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. 通过运行此命令在您的环境中重启集群管理器实例，<environment-name>替换为 RES 环境的名称。您也可以通过 Amazon EC2 管理控制台终止实例。

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
```

```
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

（2024.04.02 及更早版本）ap-southeast-2（悉尼）中的 Windows NVIDIA 实例无法启动

这个问题

Amazon 机器映像 (AMIs) 用于在 RES 中启动具有特定配置的虚拟桌面 (VDIs)。每个 AMI 都有一个关联 ID，该ID因地区而异。在 RES 中配置的用于在 ap-southeast-2（悉尼）中启动 Windows Nvidia 实例的 AMI ID 目前不正确。

ap-south `ami-0e190f8939a996caf` east-2（悉尼）中错误地列出了此类实例配置的 AMI-ID。`ami-027cf6e71e2e442f4`应改用 AMI ID。

用户在尝试使用默认 `ami-0e190f8939a996caf` AMI 启动实例时会遇到以下错误。

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id '[ami-0e190f8939a996caf]' does not exist
```

重现该错误的步骤，包括示例配置文件：

- 在 ap-southeast-2 区域部署 RES。
- 使用 Windows-NVIDIA 默认软件堆栈 (AMI ID) 启动实例。`ami-0e190f8939a996caf`

受影响的版本

所有 RES 版本 2024.04.02 或更早版本都受到影响

缓解方法

以下缓解措施已在 RES 版本 2024.01.01 上进行了测试：

- 使用以下设置注册新的软件堆栈
  - AMI ID：`ami-027cf6e71e2e442f4`

- 操作系统：Windows
- GPU 制造商：英伟达
- 最小。存储空间大小 (GB)：30
- 最小。内存 (GB): 4

- 使用此软件堆栈启动 Windows-NVIDIA 实例

.....

(2024.04 和 2024.04.01) RES 删除失败 GovCloud

这个问题

在 RES 删除工作流程中，UnprotectCognitoUserPoolLambda 会停用稍后将被删除的 Cognito 用户池的删除保护。Lambda 执行由启动。InstallerStateMachine

由于商业版和 GovCloud 区域之间的默认 AWS CLI 版本存在差异，因此 Lambda 中的update_user_pool调用在区域中 GovCloud 将失败。

客户在尝试删除 GovCloud 区域中的 RES 时会遇到以下错误：

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

重现错误的步骤：

- 在某个 GovCloud 区域部署 RES
- 删除 RES 堆栈

受影响的版本

RES 版本 2024.04 和 2024.04.01

缓解方法

以下缓解措施已在 RES 版本 2024.04 上进行了测试：

- 打开 UnprotectCognitoUserPool Lambda
  - 命名惯例：*<env-name>*-InstallerTasksUnprotectCognitoUserPool-...
- 运行时设置-> 编辑-> 选择 “运行时” Python 3.11-> “保存”。
- 打开 CloudFormation。
- 删除 RES 堆栈-> 取消选中 “保留安装程序资源”-> “删除”。

.....

(2024.04-2024.04.02) Linux 虚拟桌面在重启时可能处于 “恢复” 状态

这个问题

在手动或计划停止后重新启动时，Linux 虚拟桌面可能会停留在 “正在恢复” 状态。

实例重启后，S AWS ystems Manager 不会运行任何远程命令来创建新的 DCV 会话，并且 vdc-controller CloudWatch 日志（在日志组下）中缺少以下日志消息：<environment-name>/vdc/controller CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

受影响的版本

2024.04-2024.04.02

缓解方法

要恢复停留在 “正在恢复” 状态的虚拟桌面，请执行以下操作：

1. 从 EC2 控制台通过 SSH 进入问题实例。
2. 在实例上运行以下命令：

   ```
   sudo su -
   /bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
   configure_post_reboot.sh
   sudo reboot
   ```

3. 等待实例重启。

要防止新的虚拟桌面遇到同样的问题，请执行以下操作：

1. 要下载补丁脚本和补丁文件（patch.py 和 vdi_stuck_in_resuming_status.patch），请运行以下命令，替换为要存放文件的目录：<output-directory>

> **Note**
>
> - 该补丁仅适用于 RES 2024.04.02。
> - 补丁脚本需要 AWS CLI v2、Python 3.9.16 或更高版本以及 Boto3。
> - 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有 S3 权限来写入 RES 创建的存储桶。

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. 导航到下载补丁脚本和补丁文件的目录。运行以下补丁命令，<environment-name>替换为 RES 环境的<aws-region>名称和部署 RES 的区域：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. 要重新启动您的环境的 VDC 控制器实例，请运行以下命令，<environment-name>替换为 RES 环境的名称：

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 及更早版本) 无法同步 “ SAMAccount姓名” 属性包含大写字母或特殊字符的 AD 用户

这个问题

SSO 设置至少两个小时（两个 AD 同步周期）后，RES 无法同步 AD 用户。集群管理器 CloudWatch 日志（在<environment-name>/cluster-manager日志组下）在 AD 同步期间包含以下错误：

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

该错误是由于 RES 仅接受符合以下要求的 SAMAccount 用户名：

- 它只能包含小写的 ASCII 字母、数字、句点 (.)、下划线 (_)。
- 不允许使用句点或下划线作为第一个或最后一个字符。
- 它不能包含两个连续的句点或下划线（例如..、__、._、_。 ）。

受影响的版本

2024.04.02 及更早版本

缓解方法

1. 要下载补丁脚本和补丁文件（patch.py 和 s amaccountname_regex.patch），请运行以下命令，<output-directory>替换为要存放文件的目录：

   > **Note**
   >
   > - 该补丁仅适用于 RES 2024.04.02。
   > - 补丁脚本需要 AWS CLI v2、Python 3.9.16 或更高版本以及 Boto3。
   > - 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有 S3 权限来写入 RES 创建的存储桶。

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
 ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. 导航到下载补丁脚本和补丁文件的目录。运行以下补丁命令，<environment-name>替换为 RES 环境的名称：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. 要重新启动环境的集群管理器实例，请运行以下命令，<environment-name>替换为 RES 环境的名称。您也可以通过 Amazon EC2 管理控制台终止实例。

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

（2024.04.02 及更早版本）用于访问堡垒主机的私钥无效

这个问题

当用户从 RES 门户网站下载私钥以访问堡垒主机时，密钥的格式不正确，多行被下载为一行，这使得密钥无效。当用户尝试使用下载的密钥访问堡垒主机时，他们将收到以下错误：

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
```

```
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)
```

受影响的版本

2024.04.02 及更早版本

缓解方法

我们建议使用 Chrome 下载密钥，因为此浏览器不受影响。

或者，可以通过在密钥文件后面创建一个新行，在前面-----END PRIVATE KEY-----创建一个新行-----BEGIN PRIVATE KEY-----，来重新格式化密钥文件。

.....

（2024.06 及更早版本）在 AD 同步期间，群组成员未与 RES 同步

错误描述

如果 groupOU 与 UserOU 不同，群组成员将无法正确同步到 RES。

尝试同步 AD 组中的用户时，RES 会创建 ldapsearch 过滤器。当前过滤器错误地使用了 userOu 参数而不是 groupOU 参数。结果是搜索未能返回任何用户。只有在 UsersOU 和 groupOU 不同的情况下才会出现这种行为。

受影响的版本

此问题影响所有 RES 版本 2024.06 或更早版本

缓解方法

请按照以下步骤解决问题：

1. 要下载 patch.py 脚本和 group_member_sync_bug_fix.patch 文件，请运行以下命令，<output-directory>替换为要下载文件的本地目录和要修补的 RES 版本：<res_version>

   > **Note**
   >
   > - 补丁脚本需要 AWS CLI v2、Python 3.9.16 或更高版本以及 Boto3。
   > - 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有 S3 权限来写入 RES 创建的存储桶。

- 该补丁仅支持 RES 版本 2024.04.02 和 2024.06。如果您使用的是 2024.04 或 2024.04.01，则在应用补丁之前，可以按照中列出的步骤将您的环境先更新次要版本更新到 2024.04.02。
  - RES 版本：RES 2024.04.02

    补丁下载链接：20 24.04.02_group_member_sync_bug_fix.patch
  - 资源版本：RES 2024.06

    补丁下载链接：202 4.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. 导航到下载补丁脚本和补丁文件的目录。运行以下补丁命令，<environment-name>替换为 RES 环境的名称：

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. 要重新启动环境的集群管理器实例，请运行以下命令：

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

（2024.06 及更早版本）CVE-2024-6387、Regre SSHion、和 Ubuntu 中的安全漏洞 RHEL9 VDIs

错误描述

已在 OpenSSH 服务器中识别出名为 regre SSHion 的 CVE-2024-6387。此漏洞使未经身份验证的远程攻击者能够在目标服务器上执行任意代码，从而给使用 OpenSSH 进行安全通信的系统带来严重风险。

对于 RES，标准配置是通过堡垒主机通过 SSH 进入虚拟桌面，堡垒主机不受此漏洞的影响。但是，我们提供的默认 AMI（亚马逊系统映像） RHEL9 和所有 RES 版本中的 Ubuntu2024 VDIs （虚拟桌面基础架构）使用的是容易受到安全威胁攻击的 OpenSSH 版本。

这意味着现有 RHEL9 和 Ubuntu2024 VDIs 可能被利用，但攻击者需要访问堡垒主机。

有关该问题的更多细节可以在这里找到。

受影响的版本

此问题影响所有 RES 版本 2024.06 或更早版本。

缓解方法

Ubuntu RHEL9 和Ubuntu都发布了修复安全漏洞的OpenSSH补丁。可以使用平台的相应软件包管理器进行提取。

如果您已有 Ubuntu RHEL9 或 Ubuntu VDIs，我们建议您按照以下现有补丁 VDIs说明进行操作。要修补未来 VDIs，我们建议按照 P AT CH FUTURE 的 VDIs说明进行操作。这些说明描述了如何运行脚本以将平台更新应用于您的 VDIs。

现有补丁 VDIs

1. 运行以下命令将修补所有现有的 Ubuntu 和： RHEL9 VDIs
    a. 补丁脚本需要 AWS CLI v2。
    b. 为部署 RES 的账户和区域配置 AWS CLI，并确保您拥有发送 S AWS ystems Manager 运行命令的 Systems Manager 权限。

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. 您可以在 “运行命令” 页面上验证脚本是否成功运行。单击 “命令历史记录” 选项卡，选择最新的命令 ID，然后确认所有实例 IDs 都有成功消息。

补丁未来 VDIs

1. 要下载补丁脚本和补丁文件（patch.py 和 update_openssh.patch），请运行以下命令，<output-directory>替换为要下载文件的目录和 RES 环境<environment-name>的名称：

> **Note**
>
> - 该补丁仅适用于 RES 2024.06。
> - 补丁脚本需要 AWS CLI v2)、Python 3.9.16 或更高版本以及 Boto3。
> - 为部署 RES 的账户和区域配置 AWS CLI 副本，并确保您拥有 S3 权限来写入 RES 创建的存储桶。

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. 运行以下补丁命令：

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. 使用以下命令重新启动您的环境的 VDC 控制器实例：

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

Important

只有 RES 版本 2024.06 及更高版本支持修补 fut VDIs ure。要 VDIs 在版本早于 2024.06 的 RES 环境中修补 future，请首先使用以下说明将 RES 环境升级到 2024.06。主要版本更新

.....

版权声明

每个 Amazon EC2 实例都附带两个用于管理目的的远程桌面服务（终端服务）许可证。此信息可帮助您为管理员配置这些许可证。您也可以使用 AWS Systems Manager Session Manager，它允许在没有 RDP 且不需要 RDP 许可的情况下远程访问到 Amazon EC2 实例。如果需要额外的远程桌面服务许可证，则 CALs 应从微软或微软许可证经销商处购买远程桌面用户。 CALs 具有有效软件保障的远程桌面用户可享受许可证移动性优势，可以将其带到 AWS 默认（共享）租户环境。有关携带不带软件保障或许可证移动性权益的许可证的信息，请参阅常见问题解答的此部分。

客户有责任对本文档中的信息进行单独评测。本文件：(a) 仅供参考，(b) 代表 AWS 当前的产品供应和做法，如有更改，恕不另行通知，以及 (c) 不产生其关联公司、供应商或许可方的任何承诺或保证。AWS AWS 产品或服务 “按原样” 提供，不附带任何形式的担保、陈述或条件，无论是明示还是暗示。AWS 对客户的责任和责任受 AWS 协议的控制，本文档不属于其客户之间的任何协议，也不会对其 AWS 进行修改。

Research and Engineering Studio AWS 是根据 Apache 软件基金会提供的 Apache 许可版本 2.0 的条款获得许可的。

修订

有关更多信息，请参阅存储库中的 changelog.md 文件。 GitHub

日期	更改

2024 年 8 月	• 发布版本 2024.08 —
	  • 增加了对将 Amazon S3 存储桶挂载到 Linux 虚拟桌面基础设施 (VDI) 实例的支持。请参阅Amazon S3 存储桶。
	  • 增加了对自定义项目权限的支持，这是一种允许自定义现有角色和添加自定义角色的增强权限模型。请参阅权限配置文件。
	• 用户指南：扩展了该故障排除部分。

2024 年 6 月	• 发布版本 2024.06 — Ubuntu 支持，项目所有者权限。 • 用户指南：已添加 创建演示环境
2024 年 4 月	发布版本 2024.04 — RES就绪模板 AMIs 和项目启动模板
2024 年 3 月	其他疑难解答主题、 CloudWatch 日志保留、卸载次要版本
2024 年 2 月	发布版本 2024.01.01 — 更新的部署模板
2024 年 1 月	发布版本 2024.01
2023 年 12 月	GovCloud 已添加路线和模板
2023 年 11 月	初始版本

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。