aws

Manual do usuário

Estúdio de Pesquisa e Engenharia

Estúdio de Pesquisa e Engenharia: Manual do usuário

Table of Contents

Visão geral

O Research and Engineering Studio (RES) é um produto de código aberto AWS compatível que permite que os administradores de TI forneçam um portal na web para cientistas e engenheiros executarem cargas de trabalho de computação técnica. AWS O RES fornece um painel único para que os usuários iniciem desktops virtuais seguros para realizar pesquisas científicas, design de produtos, simulações de engenharia ou cargas de trabalho de análise de dados. Os usuários podem se conectar ao portal RES usando suas credenciais corporativas existentes e trabalhar em projetos individuais ou colaborativos.

Os administradores podem criar espaços de colaboração virtual chamados projetos para que um conjunto específico de usuários acessem recursos compartilhados e colaborem. Os administradores podem criar suas próprias pilhas de software de aplicativos (AMIs) e permitir que usuários de RES iniciem desktops virtuais Windows ou Linux e permitam o acesso aos dados do projeto por meio de sistemas de arquivos compartilhados. Os administradores podem atribuir pilhas de software e sistemas de arquivos e restringir o acesso somente aos usuários do projeto. Os administradores podem usar a telemetria integrada para monitorar o uso do ambiente e solucionar problemas do usuário. Eles também podem definir orçamentos para projetos individuais para evitar o consumo excessivo de recursos. Como o produto é de código aberto, os clientes também podem personalizar a experiência do usuário do portal RES para atender às suas próprias necessidades.

O RES está disponível sem custo adicional e você paga somente pelos AWS recursos necessários para executar seus aplicativos.

Este guia fornece uma visão geral do Research and Engineering Studio on AWS, sua arquitetura e componentes de referência, considerações para planejar a implantação e etapas de configuração para implantar RES na nuvem da Amazon Web Services (AWS).

Recursos e benefícios

O Research and Engineering Studio on AWS fornece os seguintes recursos:

Interface de usuário baseada na Web

- O RES fornece um portal baseado na web que administradores, pesquisadores e engenheiros podem usar para acessar e gerenciar seus espaços de trabalho de pesquisa e engenharia. Cientistas e engenheiros não precisam ter experiência Conta da AWS em nuvem para usar RES.

Configuração baseada em projetos

Use projetos para definir permissões de acesso, alocar recursos e gerenciar orçamentos para um conjunto de tarefas ou atividades. Atribua pilhas de software específicas (sistemas operacionais e aplicativos aprovados) e recursos de armazenamento a um projeto para obter consistência e conformidade. Monitore e gerencie os gastos por projeto.

Ferramentas de colaboração

Cientistas e engenheiros podem convidar outros membros do projeto para colaborar com eles, definindo os níveis de permissões que eles querem que esses colegas tenham. Essas pessoas podem entrar no RES para se conectar a esses desktops.

Integração com a infraestrutura de gerenciamento de identidade existente

Integre-se à sua infraestrutura existente de gerenciamento de identidade e serviços de diretório para permitir a conexão ao portal RES com a identidade corporativa existente de um usuário e atribuir permissões a projetos usando associações existentes de usuários e grupos.

Armazenamento persistente e acesso a dados compartilhados

Para fornecer aos usuários acesso a dados compartilhados em sessões de desktop virtual, conecte-se aos seus sistemas de arquivos existentes ou crie novos sistemas de arquivos no RES. Os serviços de armazenamento compatíveis incluem o Amazon Elastic File System para desktops Linux e o Amazon FSx NetApp for ONTAP para desktops Windows e Linux.

Monitoramento e emissão de relatórios

Use o painel de análise para monitorar o uso de recursos para tipos de instância, pilhas de software e tipos de sistema operacional. O painel também fornece um detalhamento do uso de recursos por projetos para geração de relatórios.

Gerenciamento de orçamento e custos

Vincule AWS Budgets seus projetos de RES para monitorar os custos de cada projeto. Se você exceder seu orçamento, poderá limitar o lançamento de sessões de VDI.

Conceitos e definições

Esta seção descreve os principais conceitos e define a terminologia específica deste produto:

Navegador de arquivos

Um navegador de arquivos faz parte da interface de usuário do RES, na qual os usuários atualmente conectados podem visualizar seu sistema de arquivos.

Sistema de arquivos

O sistema de arquivos atua como um contêiner para os dados do projeto (geralmente chamado de conjuntos de dados). Ele fornece uma solução de armazenamento dentro dos limites de um projeto e melhora a colaboração e o controle de acesso aos dados.

Administrador global

Um delegado administrativo com acesso aos recursos de RES que são compartilhados em um ambiente de RES. O escopo e as permissões abrangem vários projetos. Eles podem criar ou modificar projetos e designar proprietários de projetos. Eles podem delegar ou atribuir permissões aos proprietários e membros do projeto. Às vezes, a mesma pessoa atua como administrador do RES, dependendo do tamanho da organização.

Projeto

Um projeto é uma partição lógica dentro do aplicativo que serve como um limite distinto para dados e recursos computacionais, garantindo a governança do fluxo de dados e impedindo o compartilhamento de dados e do host VDI entre projetos.

Permissões baseadas em projetos

As permissões baseadas em projetos descrevem uma partição lógica de dados e hosts VDI em um sistema em que vários projetos podem existir. O acesso de um usuário aos dados e aos hosts de VDI em um projeto é determinado por suas funções associadas. Um usuário deve ter acesso (ou associação ao projeto) atribuído a cada projeto ao qual ele precisa de acesso. Caso contrário, um usuário não conseguirá acessar os dados do projeto e os VDIs quando não tiver recebido a associação.

Membro do projeto

Um usuário final de recursos RES (VDI, armazenamento, etc.). O escopo e as permissões são restritos aos projetos aos quais estão atribuídos. Eles não podem delegar nem atribuir nenhuma permissão.

Proprietário de projeto

Um delegado administrativo com acesso e propriedade sobre um projeto específico. O escopo e as permissões são restritos ao (s) projeto (s) de sua propriedade. Eles podem atribuir permissões aos membros do projeto nos projetos que possuem.

Pilha de software

As pilhas de software são Amazon Machine Images (AMI) com metadados específicos de RES com base em qualquer sistema operacional que um usuário tenha selecionado para provisionar para seu host VDI.

Hospedeiros VDI

Os hosts de instância de desktop virtual (VDI) permitem que os membros do projeto acessem dados e ambientes computacionais específicos do projeto, garantindo espaços de trabalho seguros e isolados.

Para obter uma referência geral dos AWS termos, consulte o AWS glossário na Referência AWS geral.

Visão geral da arquitetura

Esta seção fornece um diagrama de arquitetura para os componentes implantados com este produto.

Diagrama de arquitetura

A implantação deste produto com os parâmetros padrão implanta os seguintes componentes em seu. Conta da AWS

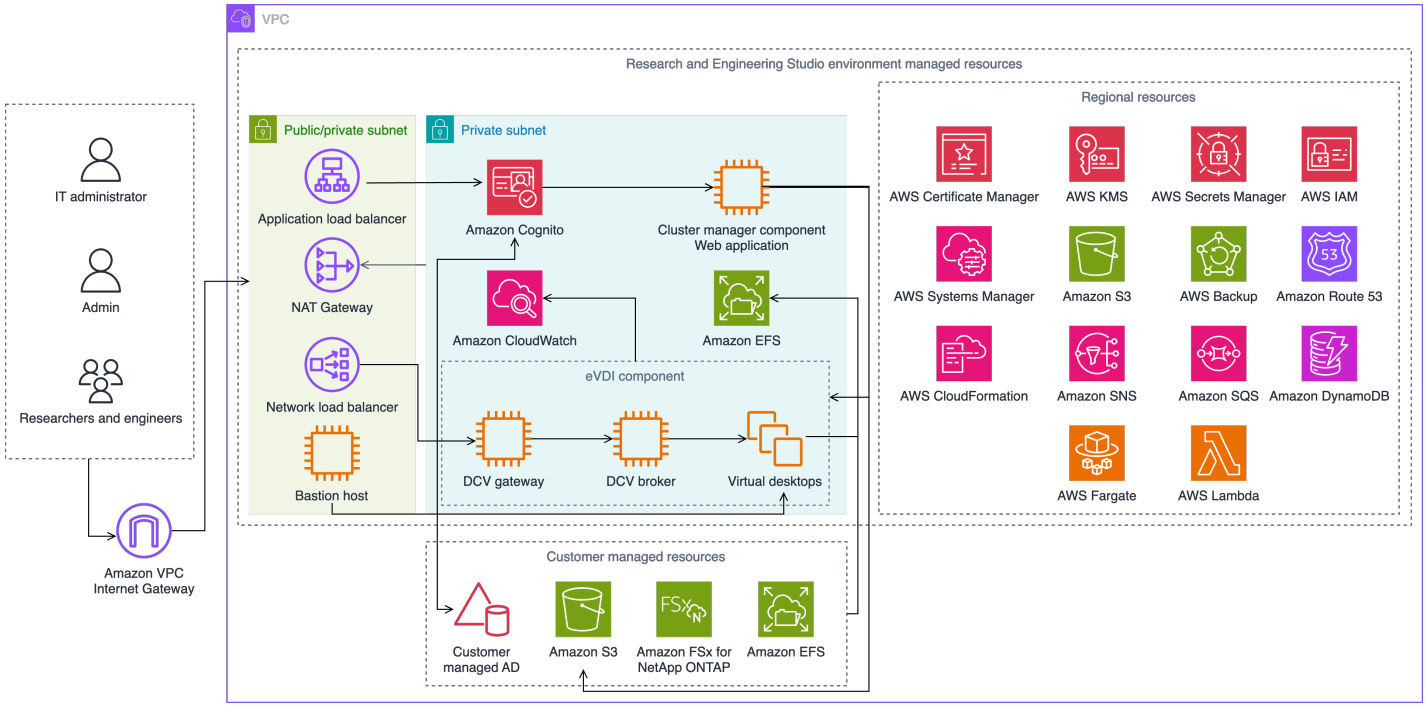


Figura 1: Estúdio de Pesquisa e Engenharia em AWS arquitetura

> **Note**
>
> AWS CloudFormationos recursos são criados a partir de AWS Cloud Development Kit (AWS CDK) construções.

O fluxo de processo de alto nível para os componentes do produto implantados com o AWS CloudFormation modelo é o seguinte:

1. O RES instala componentes para o portal da web, bem como:
   a. Componente de desktop virtual de engenharia (eVDI) para cargas de trabalho interativas

b. Componente de métricas

   A Amazon CloudWatch recebe métricas dos componentes do eVDI.

c. Componente Bastion Host

   Os administradores podem se conectar ao componente bastion host usando SSH para gerenciar a infraestrutura subjacente.

2. O RES instala componentes em sub-redes privadas por trás de um gateway NAT. Os administradores acessam as sub-redes privadas por meio do Application Load Balancer (ALB) ou do componente Bastion Host.
3. O Amazon DynamoDB armazena a configuração do ambiente.
4. AWS Certificate Manager(ACM) gera e armazena um certificado público para o Application Load Balancer (ALB).

   > **Note**
   >
   > Recomendamos usar AWS Certificate Manager para gerar um certificado confiável para seu domínio.

5. O Amazon Elastic File System (EFS) hospeda o sistema de `/home` arquivos padrão montado em todos os hosts de infraestrutura aplicáveis e sessões eVDI Linux.
6. O RES usa o Amazon Cognito para criar um usuário inicial de bootstrap chamado clusteradmin e envia credenciais temporárias para o endereço de e-mail fornecido durante a instalação. O clusteradmin deve alterar a senha com o primeiro login.
7. O Amazon Cognito se integra ao Active Directory e às identidades de usuário da sua organização para gerenciamento de permissões.
8. As zonas de segurança permitem que os administradores restrinjam o acesso a componentes específicos do produto com base nas permissões.

AWSserviços neste produto

Serviço da AWS	Descrição
Amazon Elastic Compute Cloud	Principal. Fornece os serviços de computaçã o subjacentes para criar desktops virtuais com

Serviço da AWS	Descrição
	o sistema operacional e a pilha de software escolhidos.
Elastic Load Balancing	Principal. Os hosts Bastion, cluster-manager e VDI são criados em grupos de Auto Scaling por trás do balanceador de carga. O ELB equilibra o tráfego do portal da web em todos os hosts RES.
Amazon Virtual Private Cloud	Principal. Todos os componentes principais do produto são criados em sua VPC.
Amazon Cognito	Principal. Gerencia as identidades e a autenticação dos usuários. Os usuários do Active Directory são mapeados para usuários e grupos do Amazon Cognito para autenticar os níveis de acesso.
Amazon Elastic File System	Principal. Fornece o sistema de `/home` arquivos para o navegador de arquivos e os hosts VDI, bem como sistemas de arquivos externos compartilhados.
Amazon DynamoDB	Principal. Armazena dados de configuração, como usuários, grupos, projetos, sistemas de arquivos e configurações de componentes.
AWS Systems Manager	Principal. Armazena documentos para executar comandos para gerenciamento de sessões de VDI.
AWS Lambda	Principal. Oferece suporte às funcionalidades do produto, como atualizar configurações na tabela do DynamoDB, iniciar fluxos de trabalho de sincronização do Active Directory e atualizar a lista de prefixos.

Serviço da AWS	Descrição
Amazon CloudWatch	Suporte. Fornece métricas e registros de atividades para todos os hosts do Amazon EC2 e funções do Lambda.
Amazon Simple Storage Service	Suporte. Armazena binários de aplicativos para inicialização e configuração do host.
AWS Key Management Service	Suporte. Usado para criptografia em repouso com filas do Amazon SQS, tabelas do DynamoDB e tópicos do Amazon SNS.
AWS Secrets Manager	Suporte. Armazena credenciais da conta de serviço no Active Directory e certificados autoassinados para VDIs.
AWS CloudFormation	Suporte. Fornece um mecanismo de implantaç ão para o produto.
AWS Identity and Access Management	Suporte. Restringe o nível de acesso dos hosts.
Amazon Route 53	Suporte. Cria uma zona hospedada privada para resolver o balanceador de carga interno e o nome de domínio do bastion host.
Amazon Simple Queue Service	Suporte. Cria filas de tarefas para suportar execuções assíncronas.
Amazon Simple Notification Service	Suporte. Suporta o modelo de assinante de publicação entre os componentes da VDI, como o controlador e os hosts.
AWS Fargate	Suporte. Instala, atualiza e exclui ambientes usando tarefas do Fargate.
Gateway de arquivos Amazon FSx	Opcional. Fornece sistema de arquivos compartilhado externo.

Serviço da AWS	Descrição
Amazon FSx para ONTAP NetApp	Opcional. Fornece sistema de arquivos compartilhado externo.
AWS Certificate Manager	Opcional. Gera um certificado confiável para seu domínio personalizado.
AWS Backup	Opcional. Oferece recursos de backup para hosts, sistemas de arquivos e DynamoDB do Amazon EC2.

Crie um ambiente de demonstração

Siga as etapas desta seção para experimentar o Research and Engineering Studio em AWS. Esta demonstração implanta um ambiente de não produção com um conjunto mínimo de parâmetros usando o modelo de pilha de ambiente de AWS demonstração do Research and Engineering Studio. Ele usa um servidor Keycloak para SSO.

Observe que depois de implantar a pilha, você deve seguir as etapas Etapas de pós-implantação abaixo para configurar os usuários no ambiente antes de fazer o login.

Crie uma pilha de demonstração com um clique

Essa AWS CloudFormation pilha cria todos os componentes exigidos pelo Research and Engineering Studio.

Tempo de implantação: ~90 minutos

Pré-requisitos

Tópicos

- Crie um Conta da AWS com um usuário administrativo
- Crie um par de chaves SSH do Amazon EC2
- Aumente as cotas de serviço

Crie um Conta da AWS com um usuário administrativo

Você deve ter um Conta da AWS com um usuário administrativo:

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática

recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Crie um par de chaves SSH do Amazon EC2

Se você não tiver o par de chaves SSH do Amazon EC2, precisará criar um. Para obter mais informações, consulte Criar um par de chaves usando o Amazon EC2 no Guia do usuário do Amazon EC2.

Aumente as cotas de serviço

Recomendamos aumentar as cotas de serviço para:

- Amazon VPC
  - Aumente a cota de endereços IP elásticos por gateway NAT de cinco para oito
  - Aumente os gateways NAT por zona de disponibilidade de cinco para dez
- Amazon EC2
  - Aumente os IPs elásticos do EC2-VPC de cinco para dez

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região . É possível solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas. Para ter mais informações, consulte the section called “Cotas para AWS serviços neste produto”.

Crie recursos e parâmetros de entrada

1. Faça login no AWS Management Console e abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Verifique se você está na sua conta de administrador.

2. Inicie o modelo no console.
3. Em Parâmetros, revise os parâmetros desse modelo de produto e modifique-os conforme necessário.

Parâmetro	Padrão	Descrição
EnvironmentName	*< res-demo >*	Um nome exclusivo dado ao seu ambiente RES começando com res- e não mais que 11 caracteres.
AdministratorEmail		O endereço de e-mail do usuário que está concluind o a configuração do produto. Além disso, esse usuário funciona como um usuário incomparável se houver uma falha na integração de login único do Active Directory.
KeyPair		O par de chaves usado para se conectar aos hosts da infraestrutura.
ID do cliente CIDR	<0.0.0.0/0>	Filtro de endereço IP que limita a conexão com o sistema. Você pode atualizar o ClientIpCidr após a implantação.
InboundPrefixList		(Opcional) Forneça uma lista gerenciada de prefixos para IPs com permissão para acessar diretamente a interface do usuário da web e o SSH no host bastion.

Etapas de pós-implantação

1. Redefinir senhas de usuário em `AWS Directory Service` — A pilha de demonstração cria quatro usuários com nomes de usuário que você pode usar:`admin1`, `user1admin2`, e. `user2`

   a. Acesse o console do Directory Service.

   b. Selecione o ID do diretório para seu ambiente. Você pode obter o ID do diretório na saída da `<StackName>*DirectoryService*` pilha.

   c. No menu suspenso Ação no canto superior direito, selecione Redefinir senha do usuário.

   d. Para todos os usuários que você deseja usar, coloque o nome de usuário e digite a senha que você deseja ter e selecione Redefinir senha.

2. Depois de redefinir as senhas de usuário, você precisará esperar que o Research and Engineering Studio sincronize os usuários no ambiente. O Research and Engineering Studio sincroniza os usuários a cada hora às xx.00. Você pode esperar que isso aconteça ou seguir as etapas listadas Usuário adicionado no Active Directory, mas ausente do RES para sincronizar os usuários imediatamente.

Sua implantação agora está pronta. Use o EnvironmentUrl que você recebeu em seu e-mail para acessar a interface do usuário, ou você também pode obter o mesmo URL da saída da pilha implantada. Agora você pode fazer login no ambiente do Research and Engineering Studio com o usuário e a senha para os quais você redefiniu a senha no Active Directory.

Planeje a implantação

Custo

O Research and Engineering Studio on AWS está disponível sem custo adicional, e você paga somente pelos AWS recursos necessários para executar seus aplicativos. Para ter mais informações, consulte AWSserviços neste produto.

> **Note**
>
> Você é responsável pelo custo dos AWS serviços usados durante a execução deste produto. Recomendamos criar um orçamento AWS Cost Explorerpara ajudar a gerenciar os custos. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada AWS serviço usado neste produto.

Segurança

Quando você cria sistemas na AWS infraestrutura, as responsabilidades de segurança são compartilhadas entre você AWS e. Esse modelo de responsabilidade compartilhada reduz sua carga operacional porque AWS opera, gerencia e controla os componentes, incluindo o sistema operacional do host, a camada de virtualização e a segurança física das instalações nas quais os serviços operam. Para obter mais informações sobre AWS segurança, visite Nuvem AWS Segurança.

Perfis do IAM

AWS Identity and Access Management As funções (IAM) permitem que os clientes atribuam políticas e permissões de acesso granulares a serviços e usuários no Nuvem AWS. Esse produto cria funções do IAM que concedem às AWS Lambda funções do produto e às instâncias do Amazon EC2 acesso para criar recursos regionais.

O RES oferece suporte a políticas baseadas em identidade no IAM. Quando implantado, o RES cria políticas para definir a permissão e o acesso do administrador. O administrador que implementa o produto cria e gerencia usuários finais e líderes de projeto dentro do Active Directory do cliente existente integrado ao RES. Para obter mais informações, consulte Criação de políticas do IAM no Guia do usuário do AWS Identity and Access Management.

O administrador da sua organização pode gerenciar o acesso do usuário com um diretório ativo. Quando os usuários finais acessam a interface de usuário do RES, o RES é autenticado com o Amazon Cognito.

Grupos de segurança

Os grupos de segurança criados neste produto foram projetados para controlar e isolar o tráfego de rede entre as funções Lambda, instâncias EC2, instâncias CSR de sistemas de arquivos e endpoints VPN remotos. Recomendamos que você revise os grupos de segurança e restrinja ainda mais o acesso conforme necessário após a implantação do produto.

Criptografia de dados

Por padrão, o Research and Engineering Studio on AWS (RES) criptografa os dados do cliente em repouso e em trânsito usando uma chave de propriedade da RES. Ao implantar o RES, você pode especificar um AWS KMS key. O RES usa suas credenciais para conceder acesso à chave. Se você fornecer dados próprios e gerenciados por um cliente AWS KMS key, os dados do cliente em repouso serão criptografados usando essa chave.

O RES criptografa os dados do cliente em trânsito usando SSL/TLS. Exigimos o TLS 1.2, mas recomendamos o TLS 1.3.

Suportado Regiões da AWS

Este produto usa serviços que atualmente não estão disponíveis em todos Regiões da AWS. Você deve lançar este produto em um Região da AWS local onde todos os serviços estejam disponíveis. Para obter a disponibilidade mais atual dos AWS serviços por região, consulte a Lista de Região da AWS todos os serviços.

O Research and Engineering Studio on AWS é suportado no seguinte Regiões da AWS:

Nome da região	
Leste dos EUA (Ohio)	Canadá (Central)
Leste dos EUA (Norte da Virgínia)	Europa (Frankfurt)
Oeste dos EUA (N. da Califórnia)	Europa (Irlanda)

Nome da região	
Oeste dos EUA (Oregon)	Europa (Londres)
Ásia-Pacífico (Mumbai)	Europa (Milão)
Ásia-Pacífico (Seul)	Europa (Paris)
Ásia-Pacífico (Singapura)	Israel (Tel Aviv)
Ásia-Pacífico (Sydney)	AWS GovCloud (Oeste dos EUA)
Ásia-Pacífico (Tóquio)	

Cotas

As cotas de serviço, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para sua Conta da AWS.

Cotas para AWS serviços neste produto

Verifique se você tem cota suficiente para cada um dos serviços implementados neste produto. Para obter mais informações, consulte as Service Quotas do AWS.

Para este produto, recomendamos aumentar as cotas para os seguintes serviços:

- Amazon Virtual Private Cloud
- Amazon EC2

Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

AWS CloudFormation cotas

Você Conta da AWS tem AWS CloudFormation cotas que você deve conhecer ao lançar a pilha neste produto. Ao entender essas cotas, você pode evitar erros de limitação que impediriam

a implantação bem-sucedida desse produto. Para obter mais informações, consulte AWS CloudFormation as cotas no Guia do AWS CloudFormation usuário.

Planejamento da resiliência

O produto implanta uma infraestrutura padrão com o número e o tamanho mínimos de instâncias do Amazon EC2 para operar o sistema. Para melhorar a resiliência em ambientes de produção em grande escala, recomendamos aumentar as configurações padrão de capacidade mínima dentro dos grupos de Auto Scaling (ASG) da infraestrutura. Aumentar o valor de uma instância para duas instâncias oferece o benefício de várias zonas de disponibilidade (AZ) e reduz o tempo de restauração da funcionalidade do sistema em caso de perda inesperada de dados.

As configurações do ASG podem ser personalizadas no console do Amazon EC2 em https://console.aws.amazon.com/ec2/. O produto cria quatro ASGs por padrão, com cada nome terminando com `-asg`. Você pode alterar os valores mínimos e desejados para um valor adequado ao seu ambiente de produção. Escolha o grupo que você deseja modificar e, em seguida, escolha Ações e Editar. Para obter mais informações sobre ASGs, consulte Dimensionar o tamanho do seu grupo de Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Implemente o produto

> **Note**
>
> Este produto usa AWS CloudFormation modelos e pilhas para automatizar sua implantação. Os CloudFormation modelos descrevem os AWS recursos incluídos neste produto e suas propriedades. A CloudFormation pilha provisiona os recursos descritos nos modelos.

Antes de lançar o produto, analise o custo, a arquitetura, a segurança da rede e outras considerações discutidas anteriormente neste guia.

Tópicos

Pré-requisitos

Tópicos

Crie um Conta da AWS com um usuário administrativo

Você deve ter um Conta da AWS com um usuário administrativo:

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Crie um par de chaves SSH do Amazon EC2

Se você não tiver o par de chaves SSH do Amazon EC2, precisará criar um. Para obter mais informações, consulte Criar um par de chaves usando o Amazon EC2 no Guia do usuário do Amazon EC2.

Aumente as cotas de serviço

Recomendamos aumentar as cotas de serviço para:

- Amazon VPC
  - Aumente a cota de endereços IP elásticos por gateway NAT de cinco para oito
  - Aumente os gateways NAT por zona de disponibilidade de cinco para dez
- Amazon EC2
  - Aumente os IPs elásticos do EC2-VPC de cinco para dez

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região . É possível solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas. Para ter mais informações, consulte the section called “Cotas para AWS serviços neste produto”.

Crie um domínio público (opcional)

Recomendamos usar um domínio personalizado para o produto para ter um URL fácil de usar. Você precisará registrar um domínio usando o Amazon Route 53 ou outro provedor e importar um

certificado para o domínio que está usando AWS Certificate Manager. Se você já tem um domínio público e um certificado, pode pular esta etapa.

1. Siga as instruções para registrar um domínio no Route53. Você deve receber um e-mail de confirmação.
2. Recupere a zona hospedada do seu domínio. Isso é criado automaticamente pelo Route53.
   a. Abra o console do Route53.
   b. Escolha Zonas hospedadas no painel de navegação à esquerda.
   c. Abra a zona hospedada criada para seu nome de domínio e copie o ID da zona hospedada.
3. Abra AWS Certificate Manager e siga estas etapas para solicitar um certificado de domínio. Verifique se você está na região em que planeja implantar a solução.
4. Escolha Listar certificados na navegação e encontre sua solicitação de certificado. A solicitação deve estar pendente.
5. Escolha sua ID do certificado para abrir a solicitação.
6. Na seção Domínios, escolha Criar registros no Route53. A solicitação levará aproximadamente dez minutos para ser processada.
7. Depois que o certificado for emitido, copie o ARN da seção Status do certificado.

Criar domínio (GovCloud somente)

Se você estiver implantando na região AWS GovCloud (Oeste dos EUA), precisará concluir essas etapas de pré-requisito.

1. Implante a AWS CloudFormation pilha de certificados na AWS conta de partição comercial em que o domínio público hospedado foi criado.
2. Nas CloudFormation saídas do certificado, localize e anote o `CertificateARN` e. `PrivateKeySecretARN`
3. Na conta da GovCloud partição, crie um segredo com o valor da `CertificateARN` saída. Observe o novo ARN secreto e adicione duas tags ao segredo para poder `vdc-gateway` acessar o valor do segredo:
   a. vermelho: ModuleName = virtual-desktop-controller
   b. res: EnvironmentName = [nome do ambiente] (Isso pode ser res-demo.)

4. Na conta da GovCloud partição, crie um segredo com o valor da `PrivateKeySecretArn` saída. Observe o novo ARN secreto e adicione duas tags ao segredo para poder `vdc-gateway` acessar o valor do segredo:

   a. vermelho: ModuleName = virtual-desktop-controller

   b. res: EnvironmentName = [nome do ambiente] (Isso pode ser res-demo.)

Forneça recursos externos

Quando você implanta o Research and Engineering Studio no AWS, você precisará de recursos externos usados pelo produto. O RES espera que esses recursos existam quando implantados.

- Rede (VPC, sub-redes públicas e privadas)

  É aqui que você executará as instâncias do EC2 usadas para hospedar o ambiente, o Active Directory (AD) e o armazenamento compartilhado.

- Armazenamento (Amazon EFS)

  Os volumes de armazenamento contêm arquivos e dados necessários para a infraestrutura de desktop virtual (VDI).

- Serviço de diretório (AWS Directory Service for Microsoft Active Directory)

  O serviço de diretório autentica os usuários nas páginas do ambiente.

- Um segredo que contém a senha da conta de serviço

  O Research and Engineering Studio acessa os segredos que você fornece, incluindo a senha da conta de serviço, usando AWS Secrets Manager.

> **Tip**
>
> Se você estiver implantando um ambiente de demonstração e não tiver esses recursos externos disponíveis, poderá usar receitas de computação de AWS alto desempenho para gerar os recursos externos. Consulte a seção a seguir,Crie recursos externos, para implantar recursos em sua conta.
> Para implantações de demonstração na região AWS GovCloud (Oeste dos EUA), você precisará concluir as etapas de pré-requisito em. Criar domínio (GovCloud somente)

Configure o LDAPS em seu ambiente (opcional)

Se você planeja usar a comunicação LDAPS em seu ambiente, você deve concluir estas etapas para criar e anexar certificados ao controlador de domínio AWS Managed Microsoft AD (AD) para fornecer comunicação entre AD e RES.

1. Siga as etapas fornecidas em Como habilitar o LDAPS do lado do servidor para seu. AWS Managed Microsoft AD Você pode pular essa etapa se já tiver habilitado o LDAPS.
2. Depois de confirmar que o LDAPS está configurado no AD, exporte o certificado do AD:
    a. Acesse seu servidor do Active Directory.
    b. Abra PowerShell como administrador.
    c. Execute `certmgr.msc` para abrir a lista de certificados.
    d. Abra a lista de certificados abrindo primeiro as Autoridades de Certificação Raiz Confiáveis e depois os Certificados.
    e. Selecione e segure (ou clique com o botão direito do mouse) o certificado com o mesmo nome do seu servidor AD e escolha Todas as tarefas e, em seguida, Exportar.
    f. Escolha X.509 codificado em Base-64 (.CER) e escolha Avançar.
    g. Selecione um diretório e escolha Avançar.
3. Crie um segredo em AWS Secrets Manager:

    Ao criar seu segredo no Secrets Manager, escolha Outro tipo de segredos em Tipo de segrdo e cole o certificado codificado PEM no campo Texto sem formatação.
4. Observe o ARN criado e insira-o como `DomainTLSCertificateSecretARN` parâmetro em. the section called “Etapa 1: lançar o produto”

Configurar uma VPC privada (opcional)

A implantação do Research and Engineering Studio em uma VPC isolada oferece segurança aprimorada para atender aos requisitos de conformidade e governança da sua organização. No entanto, a implantação padrão do RES depende do acesso à Internet para instalar dependências. Para instalar o RES em uma VPC privada, você precisará atender aos seguintes pré-requisitos:

Tópicos

- Prepare imagens de máquina da Amazon (AMIs)
- Configurar endpoints de VPC

- Conecte-se a serviços sem VPC endpoints
- Definir parâmetros de implantação de VPC privados

Prepare imagens de máquina da Amazon (AMIs)

1. Baixe dependências. Para implantar em uma VPC isolada, a infraestrutura RES exige a disponibilidade de dependências sem ter acesso público à Internet.
2. Crie uma função do IAM com acesso somente de leitura ao Amazon S3 e identidade confiável como Amazon EC2.

   a. Abra o console do IAM em https://console.aws.amazon.com/iam/.

   b. Em Funções, escolha Criar função.

   c. Na página Selecionar entidade confiável:

      - Em Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
      - Para Caso de uso em Serviço ou caso de uso, selecione EC2 e escolha Avançar.

   d. Em Adicionar permissões, selecione as seguintes políticas de permissão e escolha Avançar:

      - Amazon S3 ReadOnlyAccess
      - Amazon SSM ManagedInstanceCore
      - EC2 InstanceProfileForImageBuilder

   e. Adicione um nome e uma descrição da função e escolha Criar função.
3. Crie o componente EC2 image builder:

   a. Abra o console https://console.aws.amazon.com/imagebuilder do EC2 Image Builder em.

   b. Em Recursos salvos, escolha Componentes e escolha Criar componente.

   c. Na página Criar componente, insira os seguintes detalhes:

      - Em Tipo de componente, escolha Construir.
      - Para obter detalhes do componente, escolha:

Parâmetro	Entrada do usuário
Sistema operacional (SO) de imagem	Linux

Parâmetro	Entrada do usuário
Versões de sistema operacional compatíveis	Amazon Linux 2
Nome do componente	Escolha um nome como: *< research-and-engineering-studio - infrastructure>*
Versão do componente.	Recomendamos começar com 1.0.0.
Descrição	Entrada opcional do usuário.

d. Na página Criar componente, escolha Definir conteúdo do documento.

i. Antes de inserir o conteúdo do documento de definição, você precisará de um URI de arquivo para o arquivo tar.gz. Faça o upload do arquivo tar.gz fornecido pelo RES para um bucket do Amazon S3 e copie o URI do arquivo das propriedades do bucket.

ii. Insira o seguinte:

> **Note**
>
> `AddEnvironmentVariables`é opcional e você pode removê-lo se não precisar de variáveis de ambiente personalizadas em seus hosts de infraestrutura.
> Se você estiver `http_proxy` configurando variáveis de `https_proxy` ambiente, os `no_proxy` parâmetros são necessários para evitar que a instância use proxy para consultar localhost, metadados da instância, endereços IP e serviços compatíveis com endpoints de VPC.

```
#  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. Escolha Criar componente.

4. Crie uma receita de imagem do Image Builder.

   a. Na página Criar receita, insira o seguinte:

Seção	Parâmetro	Entrada do usuário
Detalhes da receita	Nome	Insira um nome apropriado, como res-recipe-linux-x 86.
	Version (Versão)	Insira uma versão, normalmente começando com 1.0.0.
	Descrição	Adicione uma descrição opcional.
Imagem base	Selecionar imagem	Selecione imagens gerenciadas.
	SO	Amazon Linux
	Origem da imagem	Início rápido (gerenciado pela Amazon)
	Nome da imagem	Amazon Linux 2 x86
	Opções de controle automático de versão	Use a versão mais recente do sistema operacional disponível.
Configuração da instância	–	Mantenha tudo nas configurações padrão e certifique-se de que Remover agente SSM após a execução do pipeline não esteja selecionado.
Diretório de trabalho	Caminho do diretório de trabalho	/root/bootstrap/re s_dependencies

Seção	Parâmetro	Entrada do usuário
Componentes	Componentes de construção	Pesquise e selecione o seguinte: • Gerenciado pela Amazon: -2-linux aws-cli-version • Gerenciado pela Amazon: amazon-cloudwatch-agent-linux • De sua propriedade: componente do Amazon EC2 criado anteriormente. Coloque seu Conta da AWS ID e atual Região da AWS nos campos.
	Componentes de teste	Pesquise e selecione: • Gerenciado pela Amazon: simple-boot-test-linux

b. Escolha Create recipe (Criar fórmula).

5. Crie a configuração da infraestrutura do Image Builder.

a. Em Recursos salvos, escolha Configurações de infraestrutura.

b. Escolha Criar configuração de infraestrutura.

c. Na página Criar configuração de infraestrutura, digite o seguinte:

Seção	Parâmetro	Entrada do usuário
Geral	Nome	Insira um nome apropriado, como res-infra-linux-x 86.

Seção	Parâmetro	Entrada do usuário
	Descrição	Adicione uma descrição opcional.
	Perfil do IAM	Selecione a função do IAM criada anteriormente.
AWS infraestrutura	Tipo de instância	Escolha t3.medium.

	VPC, sub-rede e grupos de segurança	Selecione uma opção que permita acesso à Internet e acesso ao bucket do Amazon S3. Se precisar criar um grupo de segurança, você pode criar um no console do Amazon EC2 com as seguintes entradas:
		• VPC: selecione a mesma VPC que está sendo usada para a configura ção da infraestrutura. Essa VPC deve ter acesso à Internet.
		• Regra de entrada:
		  • Tipo: SSH
		  • Source (Origem): personalizado
		  • Bloco CIDR: 0.0.0.0/0

d. Escolha Criar configuração de infraestrutura.

6. Crie um novo pipeline do EC2 Image Builder:

a. Acesse Image pipelines e escolha Create image pipeline.

b. Na página Especificar detalhes do pipeline, insira o seguinte e escolha Avançar:

- Nome do pipeline e descrição opcional
- Em Programação de criação, defina uma programação ou escolha Manual se quiser iniciar o processo de preparação da AMI manualmente.

c. Na página Escolher receita, escolha Usar receita existente e insira o nome da receita criada anteriormente. Escolha Próximo.

d. Na página Definir processo de imagem, selecione os fluxos de trabalho padrão e escolha Avançar.

e. Na página Definir configuração de infraestrutura, escolha Usar configuração de infraestrutura existente e insira o nome da configuração de infraestrutura criada anteriormente. Escolha Próximo.

f. Na página Definir configurações de distribuição, considere o seguinte para suas seleções:

- A imagem de saída deve residir na mesma região do ambiente RES implantado, para que o RES possa iniciar adequadamente instâncias hospedeiras de infraestrutura a partir dele. Usando padrões de serviço, a imagem de saída será criada na região em que o serviço EC2 Image Builder está sendo usado.
- Se quiser implantar RES em várias regiões, você pode escolher Criar novas configurações de distribuição e adicionar mais regiões lá.

g. Analise suas seleções e escolha Criar funil.

7. Execute o pipeline do EC2 Image Builder:

a. Em Pipelines de imagem, encontre e selecione o pipeline que você criou.

b. Escolha Ações e escolha Executar pipeline.

O pipeline pode levar aproximadamente 45 minutos a uma hora para criar uma imagem de AMI.

8. Anote o ID da AMI para a AMI gerada e use-o como entrada para o parâmetro da InfrastructureHost AMI emthe section called “Etapa 1: lançar o produto”.

Configurar endpoints de VPC

Para implantar RES e iniciar desktops virtuais, Serviços da AWS exija acesso à sua sub-rede privada. Você deve configurar VPC endpoints para fornecer o acesso necessário e precisará repetir essas etapas para cada endpoint.

1. Se os endpoints não tiverem sido configurados anteriormente, siga as instruções fornecidas em Access e AWS service (Serviço da AWS) usando uma interface VPC endpoint.
2. Selecione uma sub-rede privada em cada uma das duas zonas de disponibilidade.

AWS service (Serviço da AWS)	Nome do serviço
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*.cloudformation
Amazon CloudWatch	com.amazonaws.*region*.monitoring
CloudWatch Registros da Amazon	com.amazonaws.*region*.logs
Amazon DynamoDB	com.amazonaws. *region* .dynamodb (requer um endpoint de gateway)
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*.elasticfilesystem
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon EventBridge	com.amazonaws.*region*.events
Amazon FSx	com.amazonaws.*region*.fsx
AWS Key Management Service	com.amazonaws.*region*.kms
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
Amazon S3	com.amazonaws. *region* .s3 (requer um endpoint de gateway criado por padrão no RES.)
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager

AWS service (Serviço da AWS)	Nome do serviço
Amazon SES	com.amazonaws. *region* .email-smtp (não suportado nas seguintes zonas de disponibilidade: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 e 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

Conecte-se a serviços sem VPC endpoints

Para se integrar a serviços que não oferecem suporte a endpoints de VPC, você pode configurar um servidor proxy em uma sub-rede pública da sua VPC. Siga estas etapas para criar um servidor proxy com o acesso mínimo necessário para uma implantação do Research and Engineering Studio usando o AWS Identity Center como seu provedor de identidade.

1. Execute uma instância Linux na sub-rede pública da VPC que você usará para sua implantação de RES.
   - Família Linux — Amazon Linux 2 ou Amazon Linux 3
   - Arquitetura — x86
   - Tipo de instância — t2.micro ou superior
   - Grupo de segurança — TCP na porta 3128 de 0.0.0.0/0
2. Conecte-se à instância para configurar um servidor proxy.
   a. Abra a conexão http.
   b. Permita a conexão com os seguintes domínios de todas as sub-redes relevantes:

- .amazonaws.com (para serviços genéricos) AWS
- .amazoncognito.com (para o Amazon Cognito)
- .awsapps.com (para Identity Center)
- .signin.aws (para o Identity Center)
- . amazonaws-us-gov.com (para Gov Cloud)

c. Negue todas as outras conexões.

d. Ative e inicie o servidor proxy.

e. Observe a PORTA na qual o servidor proxy escuta.

3. Configure sua tabela de rotas para permitir o acesso ao servidor proxy.

   a. Acesse seu console VPC e identifique as tabelas de rotas das sub-redes que você usará para hosts de infraestrutura e hosts VDI.

   b. Edite a tabela de rotas para permitir que todas as conexões de entrada acessem a instância do servidor proxy criada nas etapas anteriores.

   c. Faça isso para tabelas de rotas para todas as sub-redes (sem acesso à Internet) que você usará para infraestrutura/VDIS.

4. Modifique o grupo de segurança da instância EC2 do servidor proxy e certifique-se de que ele permita conexões TCP de entrada na PORTA na qual o servidor proxy está escutando.

Definir parâmetros de implantação de VPC privados

Emthe section called “Etapa 1: lançar o produto”, espera-se que você insira determinados parâmetros no AWS CloudFormation modelo. Certifique-se de definir os parâmetros a seguir, conforme observado, para implantar com êxito na VPC privada que você acabou de configurar.

Parâmetro	Entrada
InfrastructureHostAMI	Use o ID da AMI de infraestrutura criado emthe section called “Prepare imagens de máquina da Amazon (AMIs)”.
IsLoadBalancerInternetFacing	Definido como falso.

Parâmetro	Entrada
LoadBalancerSubnets	Escolha sub-redes privadas sem acesso à Internet.
InfrastructureHostSubnets	Escolha sub-redes privadas sem acesso à Internet.
VdiSubnets	Escolha sub-redes privadas sem acesso à Internet.
ClientIP	Você pode escolher seu CIDR de VPC para permitir o acesso a todos os endereços IP da VPC.

Crie recursos externos

Essa CloudFormation pilha cria certificados de rede, armazenamento, diretório ativo e domínio (se um PortalDomainName for fornecido). Você deve ter esses recursos externos disponíveis para implantar o produto.

Você pode baixar o modelo de receitas antes da implantação.

Tempo de implantação: aproximadamente 40 a 90 minutos

1. Faça login no AWS Management Console e abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Verifique se você está na sua conta de administrador.

2. Inicie o modelo no console.

   Se você estiver implantando na região AWS GovCloud (Oeste dos EUA), inicie o modelo na conta de GovCloud partição.

3. Insira os parâmetros do modelo:

Parâmetro	Padrão	Descrição
DomainName	`corp.res.com`	Domínio usado para o diretório ativo. O valor padrão é fornecido no `LDIF` arquivo que configura os usuários do bootstrap. Se você quiser usar os usuários padrão, deixe o valor como padrão. Para alterar o valor, atualize e forneça um `LDIF` arquivo separado. Isso não precisa corresponder ao domínio usado para o Active Directory.
SubDomain (GovCloud somente)		Esse parâmetro é opcional para regiões comerciai s, mas obrigatório para GovCloud regiões. Se você fornecer um SubDomain, o parâmetro será prefixado ao DomainName fornecido . O nome de domínio do Active Directory fornecido se tornará um subdomínio.

Parâmetro	Padrão	Descrição
AdminPassword		A senha do administrador do Active Directory (nome de usuário`Admin`). Esse usuário é criado no Active Directory para a fase inicial de inicializ ação e não é usado depois. Observação: a senha desse usuário deve atender aos requisitos de complexidade da senha do Active Directory .
ServiceAccountPassword		Senha usada para criar uma conta de serviço (`ReadOnlyUser`). Essa conta é usada para sincroniz ação. Importante: a partir da versão 2024.06 do Research and Engineering Studio, você deve fornecer um ARN secreto que contenha a senha em texto simples para o. ServiceAccount Observação: a senha desse usuário deve atender aos requisitos de complexidade da senha do Active Directory .

Parâmetro	Padrão	Descrição
Par de chaves		Conecta as instâncias administrativas usando um cliente SSH. Observação: o Gerenciador de AWS Systems Manager sessões também pode ser usado para se conectar às instâncias.
Caminho LDIFS3	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	O caminho do Amazon S3 para um arquivo LDIF importado durante a fase de inicialização da configuração do Active Directory. Para obter mais informações, consulte LDIF Support. O parâmetro é pré-preenchido com um arquivo que cria vários usuários no diretório ativo. Para visualizar o arquivo, consulte o arquivo res.ldif disponível em. GitHub
ClientIpCidr		O endereço IP a partir do qual você acessará o site. Por exemplo, você pode selecionar seu endereço IP e usá-lo `[IPADDRESS]/32` para permitir apenas o acesso do seu host. Você pode atualizar essa pós-implantação.

Parâmetro	Padrão	Descrição
ClientPrefixList		Insira uma lista de prefixos para fornecer acesso aos nós de gerenciamento do Active Directory. Para obter informações sobre como criar uma lista de prefixos gerenciada, consulte Trabalhar com listas de prefixos gerenciadas pelo cliente.
EnvironmentName	`res-[environment name]`	Se `PortalDomainName` for fornecido, esse parâmetro será usado para adicionar tags aos segredos gerados para que possam ser usados no ambiente. Isso precisará corresponder ao `EnvironmentName` parâmetro usado ao criar a pilha RES. Se você estiver implantando vários ambientes em sua conta, isso precisará ser exclusivo.

Parâmetro	Padrão	Descrição
PortalDomainName		Para GovCloud implantaç ões, não insira esse parâmetro. Os certificados e segredos foram criados manualmente durante os pré-requisitos. O nome de domínio da conta no Amazon Route 53. Se isso for fornecido , um certificado público e um arquivo de chave serão gerados e enviados para AWS Secrets Manager. Se você tiver seu próprio domínio e certificados, esse parâmetro `Environme ntName` pode ser deixado em branco.

4. Marque todas as caixas de seleção em Capacidades e escolha Criar pilha.

Etapa 1: lançar o produto

Siga as step-by-step instruções nesta seção para configurar e implantar o produto em sua conta.

Tempo de implantação: Aproximadamente 60 minutos

Você pode baixar o CloudFormation modelo desse produto antes de implantá-lo.

Se você estiver implantando em AWS GovCloud (Oeste dos EUA), use esse modelo.

res-stack - Use esse modelo para iniciar o produto e todos os componentes associados. A configuração padrão implanta a pilha principal do RES e os recursos de autenticação, front-end e back-end.

> **Note**
>
> AWS CloudFormation os recursos são criados a partir de construções AWS Cloud Development Kit (AWS CDK) (AWS CDK).

O AWS CloudFormation modelo implanta o Research and Engineering Studio AWS no Nuvem AWS. Você deve atender aos pré-requisitos antes de lançar a pilha.

1. Faça login no AWS Management Console e abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
2. Inicie o modelo.

   Para implantar em AWS GovCloud (Oeste dos EUA), inicie este modelo.
3. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar a solução de outra forma Região da AWS, use o seletor de região na barra de navegação do console.

   > **Note**
   >
   > Este produto usa o serviço Amazon Cognito, que atualmente não está disponível para todos. Regiões da AWS Você deve lançar este produto em um Região da AWS local onde o Amazon Cognito esteja disponível. Para obter a disponibilidade mais atual por região, consulte a Lista de Região da AWS todos os serviços.
4. Em Parâmetros, revise os parâmetros desse modelo de produto e modifique-os conforme necessário. Se você implantou os recursos externos automatizados, poderá encontrar esses parâmetros na guia Saídas da pilha de recursos externos.

Parâmetro	Padrão	Descrição
EnvironmentName	`< res-demo >`	Um nome exclusivo dado ao seu ambiente RES começando com res- e não mais que 11 caracteres.
AdministratorEmail		O endereço de e-mail do usuário que está concluind

Parâmetro	Padrão	Descrição
		o a configuração do produto. Além disso, esse usuário funciona como um usuário inovador se houver uma falha na integração de login único do Active Directory.
InfrastructureHostAMI	ami- *[somente números ou letras]*	(Opcional) Você pode fornecer uma ID de AMI personalizada para usar em todos os hosts da infraestr utura. O sistema operacional básico atualmente suportado é o Amazon Linux 2. Para ter mais informações, consulte Configurar AMIs prontas para RES.
SSH KeyPair		O par de chaves usado para se conectar aos hosts da infraestrutura.
ClientIP	*x.x.x .0/24 ou x.x.x .0/32*	Filtro de endereço IP que limita a conexão com o sistema. Você pode atualizar o ClientIpCidr após a implantação.
ClientPrefixList		(Opcional) Forneça uma lista gerenciada de prefixos para IPs com permissão para acessar diretamente a interface do usuário da web e o SSH no host bastion.

Parâmetro	Padrão	Descrição
IAM PermissionBoundary		(Opcional) Você pode fornecer um ARN de política gerenciada que será anexado como limite de permissão a todas as funções criadas no RES. Para ter mais informações, consulte Definindo limites de permissão personalizados.
VpcId		IP da VPC em que as instâncias serão iniciadas.
IsLoadBalancerInternetFacing		Selecione true para implantar o balanceador de carga voltado para a Internet (requer sub-redes públicas para o balanceador de carga). Para implantações que precisam de acesso restrito à Internet, selecione false.

Parâmetro	Padrão	Descrição
LoadBalancerSubnets		Selecione pelo menos duas sub-redes em diferentes zonas de disponibilidade nas quais os balanceadores de carga serão iniciados . Para implantações que precisam de acesso restrito à Internet, escolha sub-redes privadas. Para implantações que precisam de acesso à Internet, escolha sub-redes públicas. Se mais de dois foram criados pela pilha de rede externa, selecione todos os que foram criados.
InfrastructureHostSubnets		Selecione pelo menos duas sub-redes privadas em diferentes zonas de disponibilidade nas quais os hosts de infraestrutura serão lançados. Se mais de dois foram criados pela pilha de rede externa, selecione todos os que foram criados.
VdiSubnets		Selecione pelo menos duas sub-redes privadas em diferentes zonas de disponibilidade nas quais as instâncias de VDI serão iniciadas . Se mais de dois foram criados pela pilha de rede externa, selecione todos os que foram criados.

Parâmetro	Padrão	Descrição
ActiveDirectoryName	`corp.res.com`	Domínio para o diretório ativo. Ele não precisa corresponder ao nome de domínio do portal.
ANÚNCIO ShortName	`corp`	O nome curto do diretório ativo. Isso também é chamado de nome NetBIOS.
Base LDAP	`DC=corp,DC=res,DC=com`	Um caminho LDAP para a base dentro da hierarquia LDAP.
URI de conexão LDAP		Um único caminho ldap:// que pode ser acessado pelo servidor host do Active Directory. Se você implantou os recursos externos automatizados com o domínio padrão do AD, poderá usar ldap: //corp.res.com.
ServiceAccountUserName	ServiceAccount	Nome de usuário de uma conta de serviço usada para se conectar ao AD. Essa conta deve ter acesso para criar computadores dentro do ComputerSOU.
ServiceAccountPasswordSecretArn		Forneça um ARN secreto que contenha a senha em texto simples para o. ServiceAccount

Parâmetro	Padrão	Descrição
Sou do usuário		Unidade organizacional dentro do AD para usuários que sincronizarão.
Grupo SOU		Unidade organizacional dentro do AD para grupos que serão sincronizados.
SudoerSou		Unidade organizacional dentro do AD para usuários globais.
SudoersGroupName	Administradores do RES	Nome do grupo que contém todos os usuários com acesso sudoer nas instância s na instalação e acesso de administrador no RES.
SOU de computador		Unidade organizacional dentro do AD à qual as instâncias se juntarão.
DomínioTLS ARN Certifica teSecret		(Opcional) Forneça um ARN secreto do certificado TLS de domínio para permitir a comunicação TLS com o AD.

Parâmetro	Padrão	Descrição
EnableLdapMapeamento de ID		Determina se os números UID e GID são gerados pelo SSSD ou se os números fornecidos pelo AD são usados. Defina como Verdadeiro para usar UID e GID gerados por SSSD ou Falso para usar UID e GID fornecidos pelo AD. Na maioria dos casos, esse parâmetro deve ser definido como True.
Desabilitar Adjoin	Falso	Para evitar que os hosts Linux se juntem ao domínio do diretório, altere para True. Caso contrário, deixe a configuração padrão de False.
ServiceAccountUserDN		Forneça o nome distinto (DN) do usuário da conta de serviço no Diretório.
SharedHomeFilesystemID		Um ID EFS a ser usado no sistema de arquivos doméstico compartilhado para hosts Linux VDI.
CustomDomainNamefo rWebApp		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a parte da web do sistema.

Parâmetro	Padrão	Descrição
CustomDomainNameforVDI		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a parte VDI do sistema.
Certificado ACM EAR NforWebApp		(Opcional) Ao usar a configuração padrão, o produto hospeda o aplicativo web sob o domínio amazonaws.com. Você pode hospedar os serviços do produto em seu domínio. Se você implantou os recursos externos automatizados, eles foram gerados para você e as informações podem ser encontradas nas saídas da pilha res-bi. Se você precisar gerar um certificado para seu aplicativo web, consulteGuia de configuração.
CertificateSecretARN para VDI		(Opcional) Esse segredo do ARN armazena o certificado público do certificado público do seu portal da web. Se você definir um nome de domínio do portal para seus recursos externos automatizados, poderá encontrar esse valor na guia Saídas da pilha res-bi.

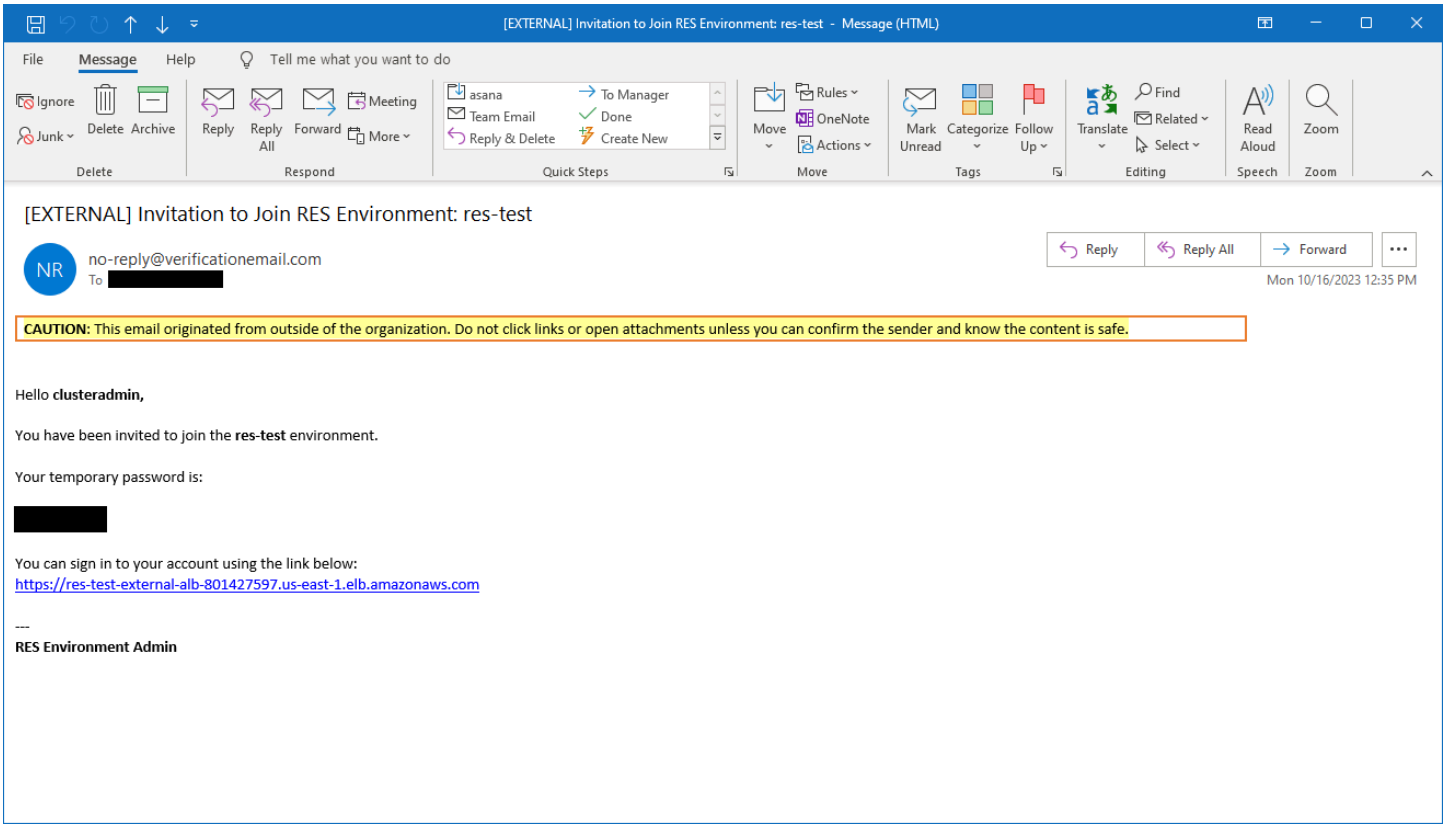
Parâmetro	Padrão	Descrição
PrivateKeySecretARN para VDI		(Opcional) Esse segredo do ARN armazena a chave privada do certificado do seu portal da web. Se você definir um nome de domínio do portal para seus recursos externos automatizados, poderá encontrar esse valor na guia Saídas da pilha res-bi.

5. Selecione Create stack (Criar pilha) para implantar a pilha.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve receber o status CREATE_COMPLETE em aproximadamente 60 minutos.

Etapa 2: faça login pela primeira vez

Depois que a pilha de produtos for implantada em sua conta, você receberá um e-mail com suas credenciais. Use o URL para entrar na sua conta e configurar o espaço de trabalho para outros usuários.



Depois de entrar pela primeira vez, você pode definir as configurações no portal da web para se conectar ao provedor de SSO. Para obter informações sobre a configuração pós-implantação, consulte o. Guia de configuração

Atualize o produto

O Research and Engineering Studio (RES) tem dois métodos de atualização do produto que dependem se a atualização da versão é maior ou menor.

O RES usa um esquema de controle de versão baseado em datas. Uma versão principal usa o ano e o mês, e uma versão secundária adiciona um número de sequência quando necessário. Por exemplo, a versão 2024.01 foi lançada em janeiro de 2024 como uma versão principal; a versão 2024.01.01 foi uma atualização de lançamento secundária dessa versão.

Tópicos

Principais atualizações da versão

O Research and Engineering Studio usa instantâneos para oferecer suporte à migração de um ambiente RES anterior para o mais recente sem perder as configurações do ambiente. Você também pode usar esse processo para testar e verificar as atualizações do seu ambiente antes de integrar os usuários.

Para atualizar seu ambiente com a versão mais recente do RES:

1. Crie um instantâneo do seu ambiente atual. Consulte the section called “Criar um snapshot”.
2. Reimplante o RES com a nova versão. Consulte the section called “Etapa 1: lançar o produto”.
3. Aplique o snapshot ao seu ambiente atualizado. Consulte the section called “Aplicar um instantâneo”.
4. Verifique se todos os dados foram migrados com sucesso para o novo ambiente.

Atualizações de versões menores

Para atualizações de versões menores do RES, não é necessária uma nova instalação. Você pode atualizar a pilha RES existente atualizando seu AWS CloudFormation modelo. Verifique a versão do seu ambiente RES atual AWS CloudFormation antes de implantar a atualização. Você pode encontrar o número da versão no início do modelo.

Por exemplo: `"Description": "RES_2024.1"`

Para fazer uma pequena atualização de versão:

1. Baixe o AWS CloudFormation modelo mais recente emthe section called “Etapa 1: lançar o produto”.
2. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
3. Em Pilhas, encontre e selecione a pilha principal. Deve aparecer como*<stack-name>*.
4. Selecione Atualizar.
5. Escolha Substituir modelo atual.
6. Para Template source (Origem do template), escolha Upload a template file (Fazer upload de um arquivo de template).
7. Escolha Escolher arquivo e faça o upload do modelo que você baixou.
8. Em Especificar detalhes da pilha, escolha Avançar. Você não precisa atualizar os parâmetros.
9. Em Configurar opções de pilha, escolha Avançar.
10. Em Revisão<stack-name>, escolha Enviar.

Desinstalar o produto

Você pode desinstalar o Research and Engineering Studio on AWS product do AWS Management Console ou usando AWS Command Line Interface o. Você deve excluir manualmente os buckets do Amazon Simple Storage Service (Amazon S3) criados por este produto. Este produto não exclui automaticamente < EnvironmentName >- shared-storage-security-group caso você tenha armazenado dados para reter.

Usando o AWS Management Console

1. Faça login no AWS CloudFormation console.
2. Na página Pilhas, selecione a pilha de instalação desse produto.
3. Escolha Delete.

Usando AWS Command Line Interface

Determine se o AWS Command Line Interface (AWS CLI) está disponível em seu ambiente. Para obter instruções de instalação, consulte O que é o AWS Command Line Interface no Guia AWS CLI do usuário. Depois de confirmar que o AWS CLI está disponível e configurado para a conta do administrador na região em que o produto foi implantado, execute o comando a seguir.

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

Excluindo o shared-storage-security-group

> **Warning**
>
> O produto mantém esse sistema de arquivos por padrão para proteger contra perda não intencional de dados. Se você optar por excluir o grupo de segurança e os sistemas de arquivos associados, todos os dados retidos nesses sistemas serão excluídos permanentemente. Recomendamos fazer backup dos dados ou reatribuí-los a um novo grupo de segurança.

1. Faça login AWS Management Console e abra o console do Amazon EFS em https://console.aws.amazon.com/efs/.
2. Exclua todos os sistemas de arquivos associados a <RES-stack-name>-shared-storage-security-group. Como alternativa, você pode reatribuir esses sistemas de arquivos a outro grupo de segurança para manter os dados.
3. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
4. Exclua o <RES-stack-name>-shared-storage-security-group.

Excluindo os buckets do Amazon S3

Este produto está configurado para reter o bucket Amazon S3 criado pelo produto (para implantação em uma região opcional) se você decidir excluir AWS CloudFormation a pilha para evitar perda acidental de dados. Depois de desinstalar o produto, você pode excluir manualmente esse bucket do S3 se não precisar reter os dados. Siga estas etapas para excluir o bucket do Amazon S3.

1. Faça login AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha Buckets no painel de navegação.
3. Localize os `stack-name` buckets do S3.
4. Selecione cada bucket do Amazon S3 e escolha Esvaziar. Você deve esvaziar cada balde.
5. Selecione o bucket do S3 e escolha Excluir.

Para excluir buckets do S3 usando AWS CLI, execute o seguinte comando:

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

> **Note**
>
> O `--force` comando esvazia o bucket de seu conteúdo.

Guia de configuração

Este guia de configuração fornece instruções pós-implantação para um público técnico sobre como personalizar e integrar ainda mais o AWS produto com o Research and Engineering Studio.

Tópicos

Gerenciando usuários e grupos

O Research and Engineering Studio pode usar qualquer provedor de identidade compatível com SAML 2.0. Se você implantou o RES usando os recursos externos ou planeja usar o IAM Identity Center, consultethe section called “Configurando o SSO com o IAM Identity Center”. Se você tiver seu próprio provedor de identidade compatível com SAML 2.0, consulte. the section called “Configurando seu provedor de identidade para login único (SSO)”

Tópicos

Configurando o SSO com o IAM Identity Center

Se você ainda não tiver uma central de identidade conectada ao Active Directory gerenciado, comece comthe section called “Configure uma central de identidade”. Se você já tem uma central de identidade conectada ao Active Directory gerenciado, comece comthe section called “Conecte-se a uma central de identidade”.

> **Note**
>
> Se você estiver implantando na região AWS GovCloud (Oeste dos EUA), configure o SSO na conta de AWS GovCloud (US) partição em que você implantou o Research and Engineering Studio.

Etapa 1: configurar uma central de identidade

Habilitando o centro de identidade

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. Abra o Identity Center.
3. Escolha Habilitar.
4. Escolha Ativar com AWS Organizations.
5. Escolha Continuar.

> **Note**
>
> Verifique se você está na mesma região em que tem seu Active Directory gerenciado.

Conectando o centro de identidade ao Active Directory gerenciado

Depois de ativar a central de identidade, conclua estas etapas de configuração recomendadas:

1. Na navegação, escolha Configurações.
2. Em Fonte de identidade, escolha Ações e escolha Alterar fonte de identidade.
3. Em Diretórios existentes, selecione seu diretório.
4. Selecione Next (Próximo).
5. Revise suas alterações e insira **`ACCEPT`** na caixa de confirmação.
6. Escolha Alterar origem de identidade.

Sincronização de usuários e grupos com o centro de identidade

Quando as alterações forem the section called “Conectando o centro de identidade ao Active Directory gerenciado” concluídas, um banner verde deverá aparecer.

1. No banner de confirmação, escolha Iniciar configuração guiada.
2. Em Configurar mapeamentos de atributos, escolha Avançar.
3. Na seção Usuário, insira os usuários que você deseja sincronizar.
4. Escolha Adicionar.
5. Selecione Next (Próximo).
6. Revise suas alterações e escolha Salvar configuração.
7. O processo de sincronização pode levar alguns minutos. Se você receber uma mensagem de aviso sobre usuários que não estão sincronizando, escolha Retomar sincronização.

Como habilitar usuários

1. No menu, escolha Usuários.
2. Escolha o (s) usuário (s) para o qual você deseja habilitar o acesso.
3. Escolha Habilitar acesso do usuário.

Etapa 2: conectar-se a uma central de identidade

Configurando o aplicativo no Identity Center

1. Faça login no AWS Management Console e abra o IAM Identity Center em https://console.aws.amazon.com/singlesignon/.
2. Selecione Aplicações.
3. Escolha Adicionar aplicação.
4. Em Preferências de configuração, escolha Eu tenho um aplicativo que eu quero configurar.
5. Em Tipo de aplicação, escolha SAML 2.0.
6. Selecione Next (Próximo).
7. Insira o nome de exibição e a descrição que você gostaria de usar.
8. Em Metadados do IAM Identity Center, copie o link para o arquivo de metadados SAML do IAM Identity Center. Você precisará disso ao configurar o SSO com o portal RES.

9. Em Propriedades do aplicativo, insira o URL inicial do aplicativo. Por exemplo, < your-portal-domain >/sso.
10. Em URL do ACS do aplicativo, insira o URL de redirecionamento do portal RES. Para encontrar isso:
    a. Em Gerenciamento do ambiente, escolha Configurações gerais.
    b. Selecione a guia Identity provider.
    c. Em Single Sign-On, você encontrará o URL de redirecionamento do SAML.
11. Em Público do Application SAML, insira o URN do Amazon Cognito. Para criar a urna:
    a. No portal RES, abra Configurações gerais.
    b. Na guia Provedor de identidade, localize o ID do grupo de usuários.
    c. Adicione o ID do grupo de usuários a essa string:

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

12. Selecione Enviar.

Configurando mapeamentos de atributos para o aplicativo

1. No Identity Center, abra os detalhes do aplicativo criado.
2. Escolha Ações e escolha Editar mapeamentos de atributos.
3. Em Assunto, insira $ {user:email}.
4. Em Formato, escolha Endereço de e-mail.
5. Escolha Adicionar novo mapeamento de atributo.
6. Em Atributo do usuário no aplicativo, insira e-mail.
7. Em Mapear para esse valor de string ou atributo de usuário no IAM Identity Center, insira $ {user:email}.
8. Em Formato, insira não especificado.
9. Escolha Salvar alterações.

Adicionar usuários ao aplicativo no Identity Center

1. No Identity Center, abra Usuários atribuídos para seu aplicativo criado e escolha Atribuir usuários.

2. Selecione os usuários aos quais você deseja atribuir acesso ao aplicativo.
3. Escolha Atribuir usuários.

Configurando o SSO no ambiente RES

1. No ambiente do Research and Engineering Studio, abra Configurações gerais em Gerenciamento de ambiente.
2. Abra a guia Provedor de identidade.
3. Em Login único, escolha o botão de edição ao lado de Status.
4. Preencha o formulário com as seguintes informações:
    a. Escolha SAML.
    b. Em Nome do provedor, insira um nome amigável.
    c. Selecione Inserir URL do endpoint do documento de metadados.
    d. Insira o URL que você copiou durante the section called “Configurando o aplicativo no Identity Center”
    e. Em Atributo de e-mail do provedor, insira e-mail.
    f. Selecione Enviar.
5. Atualize a página e verifique se o Status é exibido como ativado.

Configurando seu provedor de identidade para login único (SSO)

O Research and Engineering Studio se integra a qualquer provedor de identidade SAML 2.0 para autenticar o acesso do usuário ao portal RES. Essas etapas fornecem instruções para a integração com o provedor de identidade SAML 2.0 escolhido. Se você pretende usar o IAM Identity Center, consultethe section called “Configurando o SSO com o IAM Identity Center”.

> **Note**
>
> O e-mail do usuário deve corresponder à declaração SAML do IDP e ao Active Directory. Você precisará conectar seu provedor de identidade ao Active Directory e sincronizar os usuários periodicamente.

Tópicos

- Configure seu provedor de identidade
- Configure o RES para usar seu provedor de identidade
- Configurando seu provedor de identidade em um ambiente que não seja de produção
- Depurando problemas de IdP do SAML

Configure seu provedor de identidade

Esta seção fornece as etapas para configurar seu provedor de identidade com informações do grupo de usuários do RES Amazon Cognito.

1. O RES pressupõe que você tenha um AD (AD AWS gerenciado ou um AD autoprovisionado) com as identidades de usuário permitidas para acessar o portal e os projetos do RES. Conecte seu AD ao seu provedor de serviços de identidade e sincronize as identidades dos usuários. Consulte a documentação do seu provedor de identidade para saber como conectar seu AD e sincronizar identidades de usuário. Por exemplo, consulte Usando o Active Directory como fonte de identidade no Guia AWS IAM Identity Center do Usuário.
2. Configure um aplicativo SAML 2.0 para RES em seu provedor de identidade (IdP). Essa configuração requer os seguintes parâmetros:
   - URL de redirecionamento do SAML — O URL que seu IdP usa para enviar a resposta do SAML 2.0 ao provedor de serviços.

     > **Note**
     >
     > Dependendo do IdP, o URL de redirecionamento de SAML pode ter um nome diferente:
     >
     > - URL do aplicativo
     > - URL do Assertion Consumer Service (ACS)
     > - URL de vinculação do ACS POST

     Para obter o URL

     1. Faça login no RES como administrador ou administrador de cluster.
     2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.
     3. Escolha o URL de redirecionamento de SAML.

- URI do público do SAML — O ID exclusivo da entidade do público do SAML no lado do provedor de serviços.

  > **Note**
  >
  > Dependendo do IdP, o URI do público do SAML pode ter um nome diferente:
  >
  > - ClientID
  > - Público SAML do aplicativo
  > - ID da entidade SP

  Forneça a entrada no formato a seguir.

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

  Para encontrar seu URI de público do SAML

  1. Faça login no RES como administrador ou administrador de cluster.
  2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.
  3. Escolha ID do grupo de usuários.

3. A declaração SAML publicada no RES deve ter os seguintes campos/declarações definidos como o endereço de e-mail do usuário:
   - Assunto do SAML ou NameID
   - E-mail SAML
4. Seu IdP adiciona campos/declarações à declaração SAML, com base na configuração. O RES exige esses campos. A maioria dos provedores preenche automaticamente esses campos por padrão. Consulte as entradas e valores de campo a seguir se precisar configurá-los.

   - AudienceRestriction— Definido com`urn:amazon:cognito:sp:user-pool-id`. `user-pool-id`Substitua pelo ID do seu grupo de usuários do Amazon Cognito.

     ```
     <saml:AudienceRestriction>
     ```

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

- Resposta — `InResponseTo` Defina como`https://user-pool-domain/saml2/idpresponse`. *`user-pool-domain`*Substitua pelo nome de domínio do seu grupo de usuários do Amazon Cognito.

```
<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— `Recipient` Defina o `saml2/idpresponse` endpoint do grupo de usuários e `InResponseTo` o ID original da solicitação SAML.

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

- AuthnStatement— Configure da seguinte forma:

```
<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. Se seu aplicativo SAML tiver um campo de URL de logout, defina-o como:. <*`domain-url`*>`/saml2/logout`

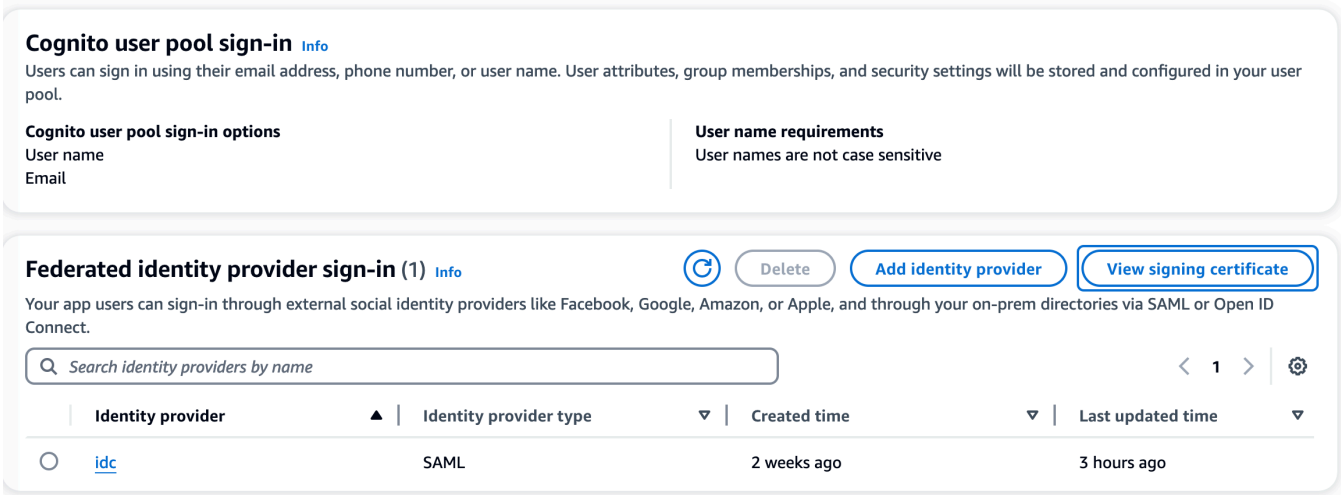
Para obter o URL do domínio

1. Faça login no RES como administrador ou administrador de cluster.
2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.
3. Escolha o URL do domínio.

6. Se o seu IdP aceitar um certificado de assinatura para estabelecer confiança com o Amazon Cognito, baixe o certificado de assinatura do Amazon Cognito e carregue-o no seu IdP.

Para obter o certificado de assinatura

1. Abra o console do Amazon Cognito em Getting Started with the AWS Management Console
2. Selecione seu grupo de usuários. Seu grupo de usuários deve ser `res-<environment name>-user-pool`.
3. Escolha a guia Experiência de login.
4. Na seção Login do provedor de identidade federado, escolha Exibir certificado de assinatura.



Você pode usar esse certificado para configurar o IDP do Active Directory, adicionar um `relying party trust` e habilitar o suporte ao SAML nessa parte confiável.

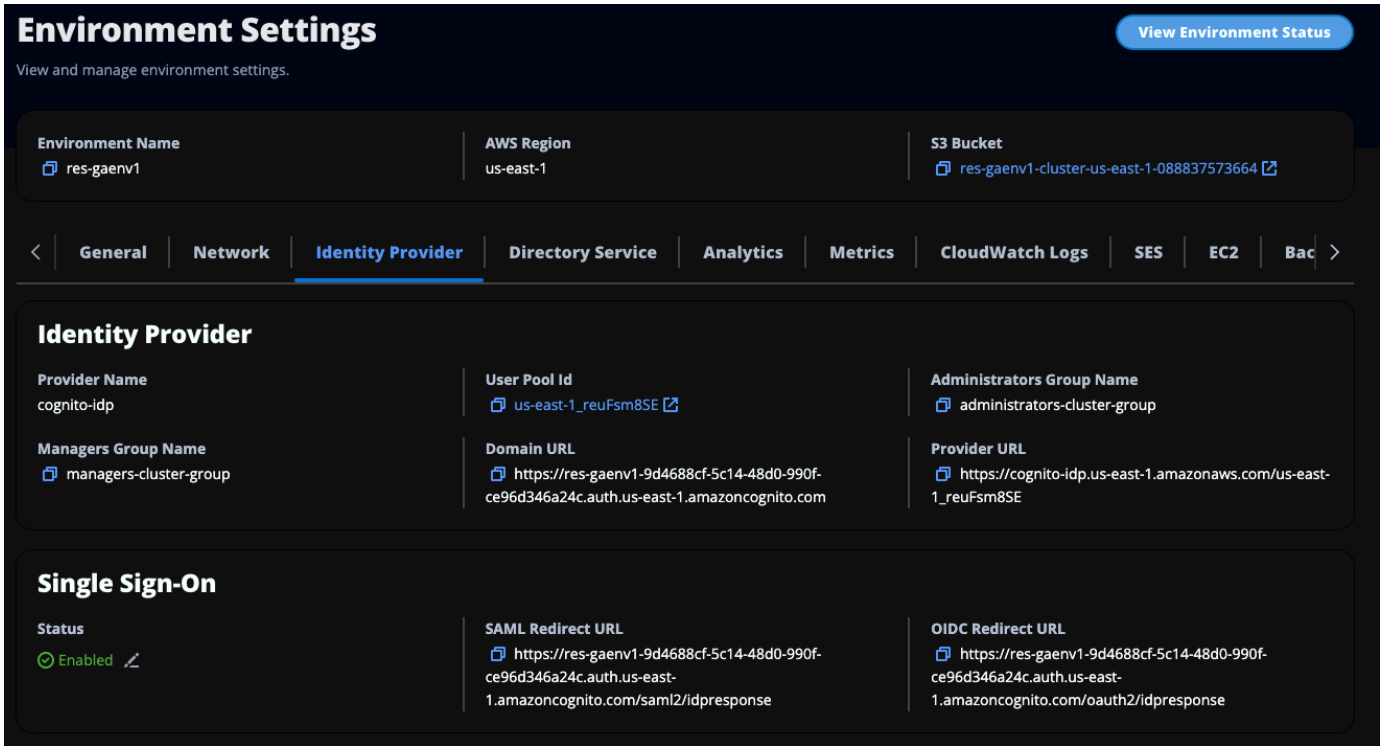
> **Note**
>
> Isso não se aplica ao Keycloak e ao IDC.

5. Depois que a configuração do aplicativo estiver concluída, baixe o XML ou URL dos metadados do aplicativo SAML 2.0. Você o usa na próxima seção.

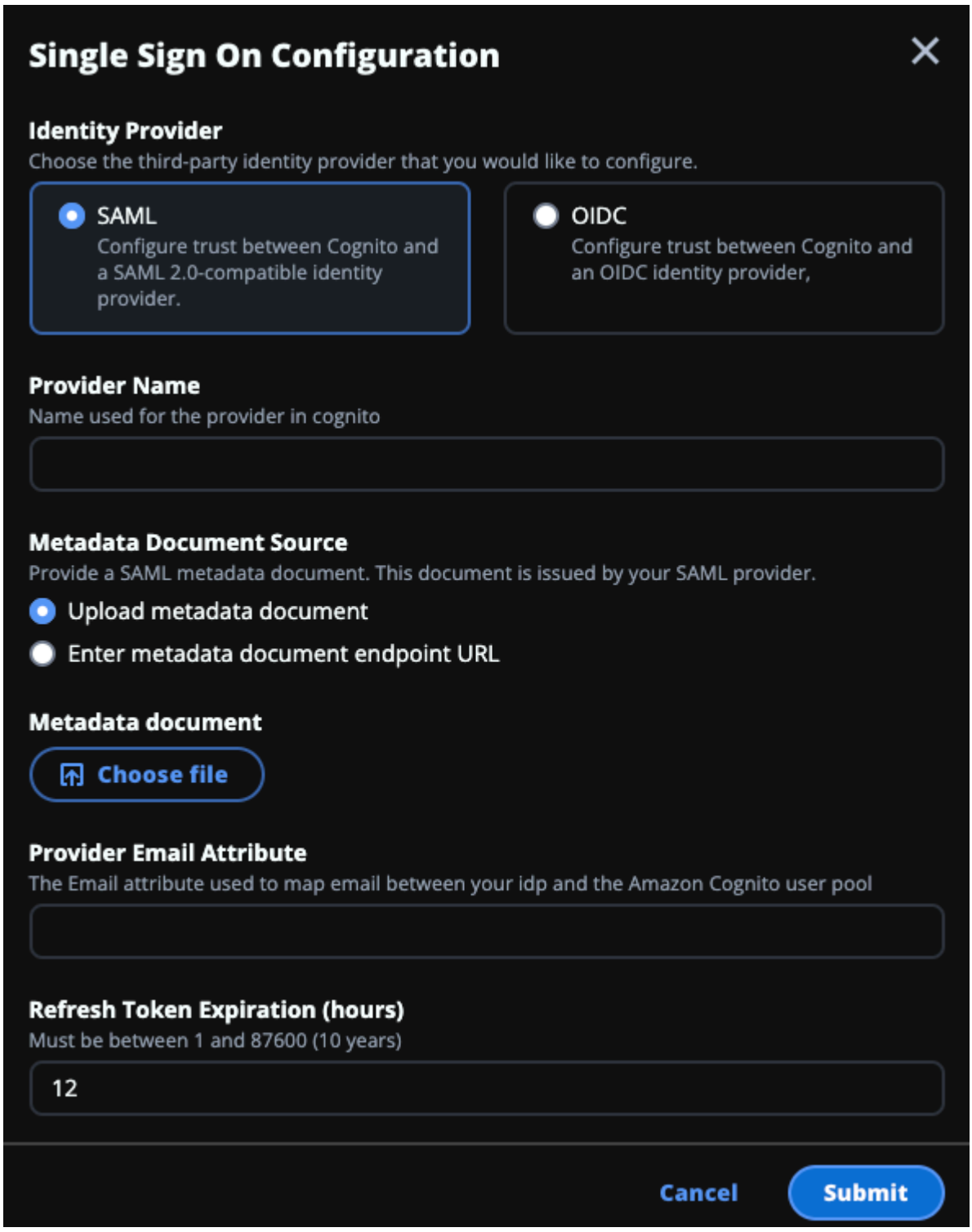
Configure o RES para usar seu provedor de identidade

Para concluir a configuração de login único para RES

1. Faça login no RES como administrador ou administrador de cluster.
2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.



3. Em Single Sign-On, escolha o ícone de edição ao lado do indicador de status para abrir a página de Configuração de Single Sign On.



a. Em Identity Provider, escolha SAML.

b. Em Nome do provedor, insira um nome exclusivo para seu provedor de identidade.

> **Note**
>
> Os seguintes nomes não são permitidos:
>
> - Cognito
> - IdentityCenter

c. Em Fonte do documento de metadados, escolha a opção apropriada e carregue o documento XML de metadados ou forneça a URL do provedor de identidade.

d. Em Atributo de e-mail do provedor, insira o valor do texto`email`.

e. Selecione Enviar.

4. Recarregue a página de configurações do ambiente. O login único é ativado se a configuração estiver correta.

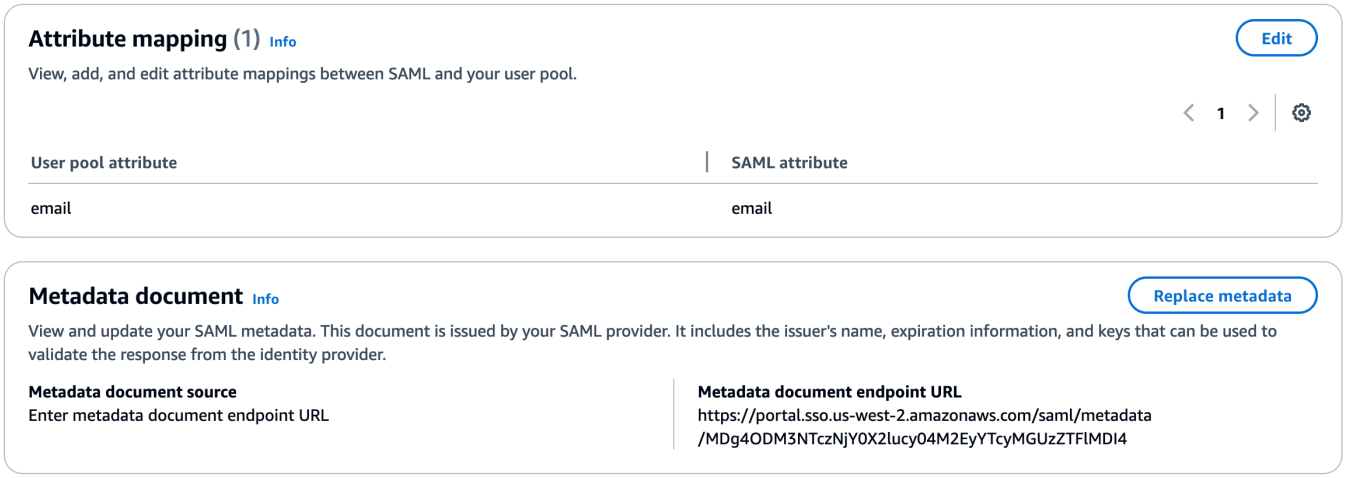
Configurando seu provedor de identidade em um ambiente que não seja de produção

Se você usou os recursos externos fornecidos para criar um ambiente RES de não produção e configurou o IAM Identity Center como seu provedor de identidade, talvez queira configurar um provedor de identidade diferente, como o Okta. O formulário de habilitação do RES SSO solicita três parâmetros de configuração:

1. Nome do provedor — Não pode ser modificado
2. Documento de metadados ou URL — Pode ser modificado
3. Atributo de e-mail do provedor — Pode ser modificado

Para modificar o documento de metadados e o atributo de e-mail do provedor, faça o seguinte:

1. Acesse o console do Amazon Cognito.
2. Na navegação, escolha Grupos de usuários.
3. Escolha seu grupo de usuários para ver a visão geral do grupo de usuários.
4. Na guia Experiência de login, acesse Login do provedor de identidade federado e abra seu provedor de identidade configurado.
5. Geralmente, você só precisará alterar os metadados e deixar o mapeamento de atributos inalterado. Para atualizar o mapeamento de atributos, escolha Editar. Para atualizar o documento de metadados, escolha Substituir metadados.



6. Se você editou o mapeamento de atributos, precisará atualizar a `<environment name>.cluster-settings` tabela no DynamoDB.

   a. Abra o console do DynamoDB e escolha Tabelas na navegação.

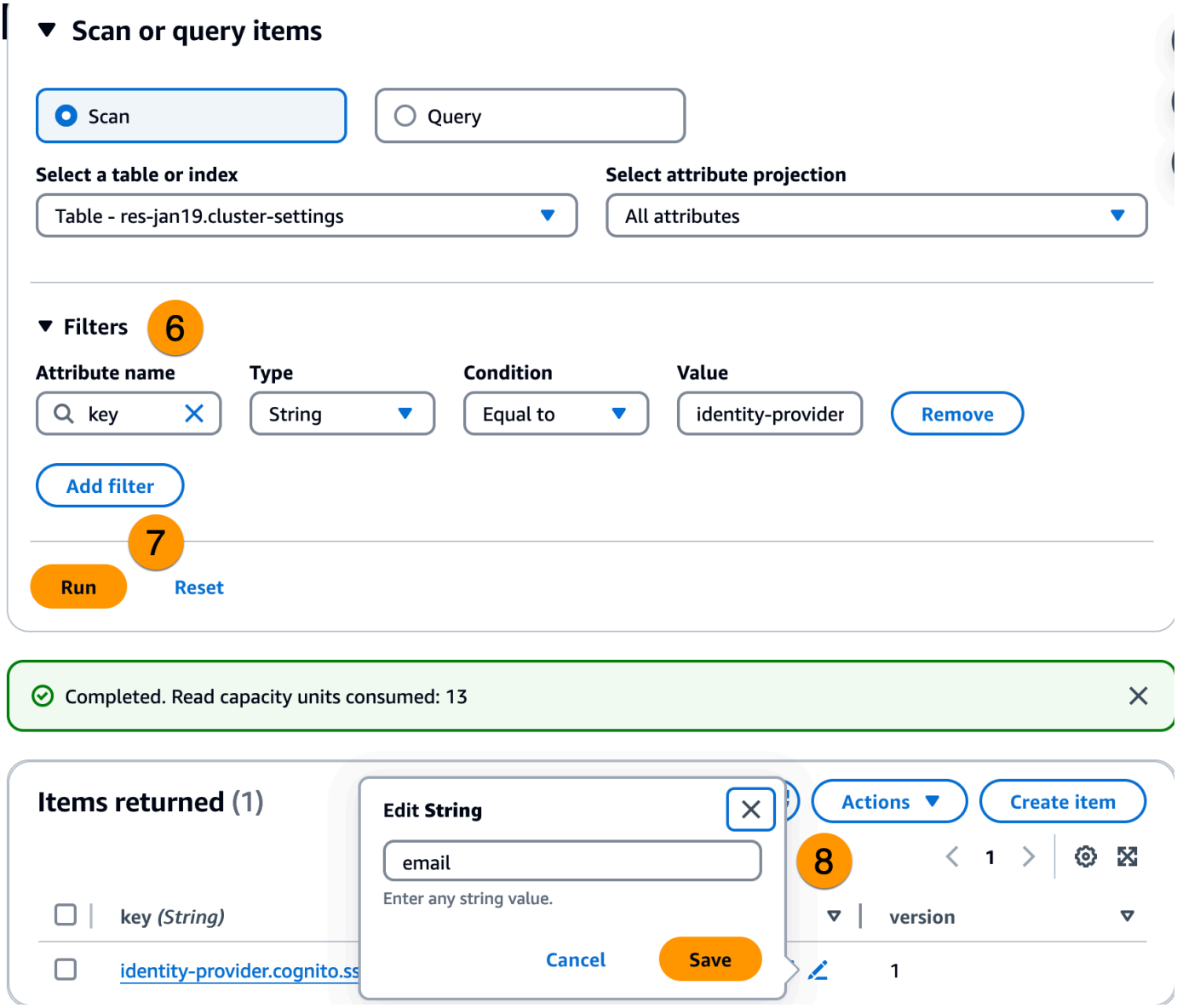
   b. Encontre e selecione a `<environment name>.cluster-settings` tabela e, no menu Ações, escolha Explorar itens.

   c. Em Digitalizar ou consultar itens, acesse Filtros e insira os seguintes parâmetros:

      - Nome do atributo — `key`
      - Valor — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Escolha Executar.

7. Em Itens retornados, encontre a `identity-provider.cognito.sso_idp_provider_email_attribute` string e escolha Editar para modificar a string de acordo com suas alterações no Amazon Cognito.



Depurando problemas de IdP do SAML

SAML-Tracer — Você pode usar essa extensão no navegador Chrome para rastrear solicitações SAML e verificar os valores de asserção SAML. Para obter mais informações, consulte SAML-tracer na loja virtual do Chrome.

Ferramentas de desenvolvedor do SAML — OneLogin fornece ferramentas que você pode usar para decodificar o valor codificado do SAML e verificar os campos obrigatórios na declaração do SAML. Para obter mais informações, consulte Base 64 Decode + Inflate no OneLogin site.

Amazon CloudWatch Logs — Você pode verificar seus registros de RES em CloudWatch Logs em busca de erros ou avisos. Seus registros estão em um grupo de registros com o formato do nome*res-environment-name*/cluster-manager.

Documentação do Amazon Cognito — Para obter mais informações sobre a integração do SAML com o Amazon Cognito, consulte Adicionar provedores de identidade do SAML a um grupo de usuários no Guia do desenvolvedor do Amazon Cognito.

Definindo senhas para usuários

1. No AWS Directory Service console, selecione o diretório para a pilha criada.
2. No menu Ações, escolha Redefinir senha do usuário.
3. Escolha o usuário e insira uma nova senha.
4. Escolha Redefinir senha.

Criação de subdomínios

Se você estiver utilizando um domínio personalizado, você precisará configurar subdomínios para suportar as partes web e VDI do seu portal.

> **Note**
>
> Se você estiver implantando na região AWS GovCloud (Oeste dos EUA), configure o aplicativo web e os subdomínios VDI na conta de partição comercial que hospeda a zona hospedada pública do domínio.

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Encontre o domínio que você criou e escolha Criar registro.
3. Insira web como o nome do registro.
4. Escolha CNAME como o tipo de registro.
5. Em Valor, insira o link que você recebeu no e-mail inicial.
6. Escolha Create records (Criar registros).
7. Para criar um registro para o VDC, recupere o endereço NLB.

a. Faça login no AWS Management Console e abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
b. Selecione `<environment-name>-vdc`.
c. Escolha Recursos e abra`<environmentname>-vdc-external-nlb`.
d. Copie o nome DNS do NLB.

8. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
9. Encontre seu domínio e escolha Criar registro.
10. Em Nome do registro, insira`vdc`.
11. Em Tipo de registro, selecione CNAME.
12. Para o NLB, insira o DNS.
13. Escolha Create record (Criar registro).

Criar um certificado ACM

Por padrão, o RES hospeda o portal da web em um balanceador de carga de aplicativos usando o domínio amazonaws.com. Para usar seu próprio domínio, você precisará configurar um certificado SSL/TLS público fornecido por você ou solicitado pelo AWS Certificate Manager (ACM). Se você usar o ACM, receberá um nome de AWS recurso que precisará fornecer como parâmetro para criptografar o canal SSL/TLS entre o cliente e o host de serviços web.

> **Tip**
>
> Se você estiver implantando o pacote de demonstração de recursos externos, precisará inserir o domínio escolhido `PortalDomainName` ao implantar a pilha de recursos externos. the section called “Crie recursos externos”

Para criar um certificado para domínios personalizados:

1. No console, abra AWS Certificate Managerpara solicitar um certificado público. Se você estiver implantando em AWS GovCloud (Oeste dos EUA), crie o certificado em sua conta de GovCloud partição.
2. Escolha Solicitar um certificado público e escolha Avançar.

3. Em Nomes de domínio, solicite um certificado para ambos `*.PortalDomainName` `PortalDomainName` e.
4. Em Método de validação, escolha Validação de DNS.
5. Escolha Solicitar.
6. Na lista de certificados, abra os certificados solicitados. Cada certificado terá a validação pendente como status.

> **Note**
>
> Se você não vê seus certificados, atualize a lista.

7. Execute um destes procedimentos:
   - Implantação comercial: nos detalhes do certificado para cada certificado solicitado, escolha Criar registros no Route 53. O status do certificado deve mudar para Emitido.
   - GovCloud implantação: se você estiver implantando em AWS GovCloud (Oeste dos EUA), copie a chave e o valor CNAME. Na conta de partição comercial, use os valores para criar um novo registro na zona hospedada pública. O status do certificado deve mudar para Emitido.
8. Copie o novo ARN do certificado a ser inserido como parâmetro para. `ACMCertificateARNforWebApp`

CloudWatch Registros da Amazon

O Research and Engineering Studio cria os seguintes grupos de registros CloudWatch durante a instalação. Consulte a tabela a seguir para ver as retenções padrão:

CloudWatch Grupos de registros	Retention
/aws/lambda/ < >-cluster-endpoints installation-stack-name	Nunca expire
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	Nunca expire
/aws/lambda/ < >-cluster-settings installation-stack-name	Nunca expire

CloudWatch Grupos de registros	Retention
/aws/lambda/ < >-oauth-credentials installation-stack-name	Nunca expire
/aws/lambda/ < >- installation-stack-name self-signed-certificate	Nunca expire
/aws/lambda/ < >- installation-stack-name update-cluster-prefix-list	Nunca expire
/aws/lambda/ < >- installation-stack-name vdc-scheduled-event-transformer	Nunca expire
/aws/lambda/ < >- -escopo do cliente installation-stack-name vdc-update-cluster-manager	Nunca expire
/< >/gerenciador installation-stack-name de cluster	3 meses
/< installation-stack-name >/vdc/controlador	3 meses
/< installation-stack-name >/vdc/dcv-broker	3 meses
/< >/vdc/ installation-stack-name dcv-connection-gateway	3 meses

Se quiser alterar a retenção padrão de um grupo de registros, acesse o CloudWatch console em https://console.aws.amazon.com/cloudwatch/ e siga as instruções para Alterar a retenção de dados de registro em CloudWatch Registros.

Definindo limites de permissão personalizados

A partir de 2024.04, você pode, opcionalmente, modificar as funções criadas pelo RES anexando limites de permissão personalizados. Um limite de permissão personalizado pode ser definido como parte da AWS CloudFormation instalação do RES fornecendo o ARN do limite de permissão como parte do parâmetro do IAM. PermissionBoundary Nenhum limite de permissão é definido em nenhuma função RES se esse parâmetro for deixado em branco. Abaixo está a lista de ações que

as funções de RES exigem para operar. Certifique-se de que qualquer limite de permissão que você planeja usar explicitamente permita as seguintes ações:

```
[
    {
        "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:*"
        ]
    }
]
```

Configurar AMIs prontas para RES

Com AMIs prontas para RES, você pode pré-instalar dependências RES para instâncias de desktop virtual (VDIs) em suas AMIs personalizadas. O uso de AMIs prontas para RES melhora os tempos de inicialização das instâncias de VDI usando imagens pré-preparadas. Usando o EC2 Image Builder, você pode criar e registrar suas AMIs como novas pilhas de software. Para obter mais informações sobre o Image Builder, consulte o Guia do usuário do Image Builder.

Antes de começar, você deve implantar a versão mais recente do RES.

Tópicos

Prepare a função do IAM para acessar o ambiente RES

Para acessar o serviço de ambiente RES a partir do EC2 Image Builder, você deve criar ou modificar uma função do IAM chamada InstanceProfileForImageBuilder RES-EC2. Para obter informações sobre como configurar uma função do IAM para uso no Image Builder, consulte AWS Identity and Access Management (IAM) no Guia do usuário do Image Builder.

Sua função exige:

- Os relacionamentos confiáveis incluem o serviço Amazon EC2
- Políticas do AmazonSSM ManagedInstanceCore e EC2 InstanceProfileForImageBuilder
- Política de RES personalizada com acesso limitado do DynamoDB e do Amazon S3 ao ambiente RES implantado

  (Essa política pode ser um documento de política gerenciado pelo cliente ou incorporado ao cliente.)

Entidade de relacionamento confiável:

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

Política de RES:

```
{
    "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/*"
        }
    ]
```

```
}
```

Crie o componente EC2 Image Builder

Siga as instruções para Criar um componente usando o console do Image Builder no Guia do usuário do Image Builder.

Insira os detalhes do seu componente:

1. Em Tipo, escolha Construir.
2. Para Sistema operacional (SO) de imagem, escolha Linux ou Windows.
3. Em Nome do componente, insira um nome significativo, como**`research-and-engineering-studio-vdi-<operating-system>`**.
4. Insira o número da versão do seu componente e, opcionalmente, adicione uma descrição.
5. Para o documento de definição, insira o arquivo de definição a seguir. Se você encontrar algum erro, o arquivo YAML é sensível ao espaço e é a causa mais provável.

   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. Crie qualquer tag opcional e escolha Criar componente.

Prepare sua receita do EC2 Image Builder

> **Note**
>
> Atualmente, o CentOS 7 está programado para chegar end-of-life em 30/06/2024. A versão 2024.06 do Research and Engineering Studio será a última versão a oferecer suporte ao CentOS 7.

Uma fórmula do EC2 Image Builder define a imagem base a ser usada como ponto de partida para criar uma nova imagem, junto com o conjunto de componentes que você adiciona para personalizar sua imagem e verificar se tudo funciona conforme o esperado. Você deve criar ou modificar uma receita para construir a AMI de destino com as dependências de software RES necessárias. Para obter mais informações sobre receitas, consulte Gerenciar receitas.

O RES suporta os seguintes sistemas operacionais de imagem:

- Amazon Linux 2 (x86 e ARM64)
- CentOS 7 (x86 e ARM64)
- RHEL 7 (x86), 8 (x86) e 9 (x86)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Abra o console https://console.aws.amazon.com/imagebuilder do EC2 Image Builder em.
2. Em Recursos salvos, escolha Receitas de imagens.
3. Escolha Create image recipe (Criar fórmula de imagem).
4. Insira um nome exclusivo e um número de versão.
5. Escolha uma imagem base compatível com RES.

6. Em Configuração da instância, instale um agente SSM se um não vier pré-instalado. Insira as informações em Dados do usuário e quaisquer outros dados necessários do usuário.

   > **Note**
   >
   > Para obter informações sobre como instalar um agente SSM, consulte:
   >
   > - Instalação manual do SSM Agent em instâncias do EC2 para Linux
   > - Instalando e desinstalando manualmente o SSM Agent em instâncias do EC2 para Windows Server

7. Para receitas baseadas em Linux, adicione o componente de `aws-cli-version-2-linux` compilação gerenciado pela Amazon à receita. Os scripts de instalação do RES usam o AWS CLI para fornecer acesso VDI aos valores de configuração das configurações de cluster do DynamoDB. O Windows não exige esse componente.
8. Adicione o componente EC2 Image Builder criado para seu ambiente Linux ou Windows e insira os valores de parâmetros necessários. Os seguintes parâmetros são entradas obrigatórias: RES AWSAccountID EnvNameEnvRegion, RES e RES. EnvReleaseVersion

   > **Important**
   >
   > Para ambientes Linux, você deve adicionar esses componentes em ordem, com o componente de `aws-cli-version-2-linux` compilação adicionado primeiro.

9. (Recomendado) Adicione o componente de `simple-boot-test-<linux-or-windows>` teste gerenciado pela Amazon para verificar se a AMI pode ser iniciada. Essa é uma recomendação mínima. Você pode selecionar outros componentes de teste que atendam às suas necessidades.
10. Complete todas as seções opcionais, se necessário, adicione outros componentes desejados e escolha Criar receita.

Modify a recipe

Se você tiver uma receita existente do EC2 Image Builder, poderá usá-la adicionando os seguintes componentes:

1. Para receitas baseadas em Linux, adicione o componente de `aws-cli-version-2-linux` compilação gerenciado pela Amazon à receita. Os scripts de instalação do RES usam o AWS

CLI para fornecer acesso VDI aos valores de configuração das configurações de cluster do DynamoDB. O Windows não exige esse componente.

2. Adicione o componente EC2 Image Builder criado para seu ambiente Linux ou Windows e insira os valores de parâmetros necessários. Os seguintes parâmetros são entradas obrigatórias: RES AWSAccountID EnvNameEnvRegion, RES e RES. EnvReleaseVersion

> **Important**
>
> Para ambientes Linux, você deve adicionar esses componentes em ordem, com o componente de `aws-cli-version-2-linux` compilação adicionado primeiro.

3. Complete todas as seções opcionais, se necessário, adicione outros componentes desejados e escolha Criar receita.

Configurar a infraestrutura do EC2 Image Builder

Você pode usar configurações de infraestrutura para especificar a infraestrutura do Amazon EC2 que o Image Builder usa para criar e testar sua imagem do Image Builder. Para uso com RES, você pode optar por criar uma nova configuração de infraestrutura ou usar uma existente.

- Para criar uma nova configuração de infraestrutura, consulte Criar uma configuração de infraestrutura.
- Para usar uma configuração de infraestrutura existente, atualize uma configuração de infraestrutura.

Para configurar sua infraestrutura do Image Builder:

1. Para a função do IAM, insira a função na qual você configurou anteriormentethe section called “Prepare a função do IAM para acessar o ambiente RES”.
2. Em Tipo de instância, escolha um tipo com pelo menos 4 GB de memória e compatível com a arquitetura básica de AMI escolhida. Veja os tipos de instância do Amazon EC2.
3. Para VPC, sub-rede e grupos de segurança, você deve permitir o acesso à Internet para baixar pacotes de software. O acesso também deve ser permitido à tabela do `cluster-settings` DynamoDB e ao bucket do cluster Amazon S3 do ambiente RES.

Configurar o pipeline de imagens do Image Builder

O pipeline de imagens do Image Builder reúne a imagem base, os componentes para construção e teste, a configuração da infraestrutura e as configurações de distribuição. Para configurar um pipeline de imagem para AMIs prontas para RES, você pode optar por criar um novo pipeline ou usar um existente. Para obter mais informações, consulte Criar e atualizar pipelines de imagem da AMI no Guia do usuário do Image Builder.

Create a new Image Builder pipeline

1. Abra o console do Image Builder emhttps://console.aws.amazon.com/imagebuilder.
2. Na navegação, escolha Pipelines de imagem.
3. Escolha Criar pipeline de imagens.
4. Especifique os detalhes do seu funil inserindo um nome exclusivo, uma descrição opcional, uma programação e uma frequência.
5. Em Escolher receita, escolha Usar receita existente e selecione a receita criada emthe section called “Prepare sua receita do EC2 Image Builder”. Verifique se os detalhes da receita estão corretos.
6. Em Definir processo de criação de imagem, escolha o fluxo de trabalho padrão ou personalizado, dependendo do caso de uso. Na maioria dos casos, os fluxos de trabalho padrão são suficientes. Para obter mais informações, consulte Configurar fluxos de trabalho de imagem para seu pipeline do EC2 Image Builder.
7. Em Definir configuração de infraestrutura, escolha Escolher configuração de infraestrutura existente e selecione a configuração de infraestrutura criada emthe section called “Configurar a infraestrutura do EC2 Image Builder”. Verifique se os detalhes da sua infraestrutura estão corretos.
8. Em Definir configurações de distribuição, escolha Criar configurações de distribuição usando padrões de serviço. A imagem de saída deve residir no Região da AWS mesmo ambiente do RES. Usando padrões de serviço, a imagem será criada na região em que o Image Builder é usado.
9. Analise os detalhes do funil e escolha Criar funil.

Modify an existing Image Builder pipeline

1. Para usar um pipeline existente, modifique os detalhes para usar a receita criada emthe section called “Prepare sua receita do EC2 Image Builder”.

2. Escolha Salvar alterações.

Execute o pipeline de imagens do Image Builder

Para produzir a imagem de saída configurada, você deve iniciar o pipeline de imagem. O processo de construção pode levar até uma hora, dependendo do número de componentes na receita da imagem.

Para executar o pipeline de imagens:

1. Em Pipelines de imagem, selecione o pipeline criado emthe section called “Configurar o pipeline de imagens do Image Builder”.
2. Em Ações, escolha Executar pipeline.

Registre uma nova pilha de software no RES

1. Siga as instruções the section called “Pilhas de software (AMIs)” para registrar uma pilha de software.
2. Em ID da AMI, insira a ID da AMI da imagem de saída incorporadathe section called “Execute o pipeline de imagens do Image Builder”.

Guia do administrador

Este guia do administrador fornece instruções adicionais para um público técnico sobre como personalizar e integrar ainda mais o Research and Engineering Studio on AWS product.

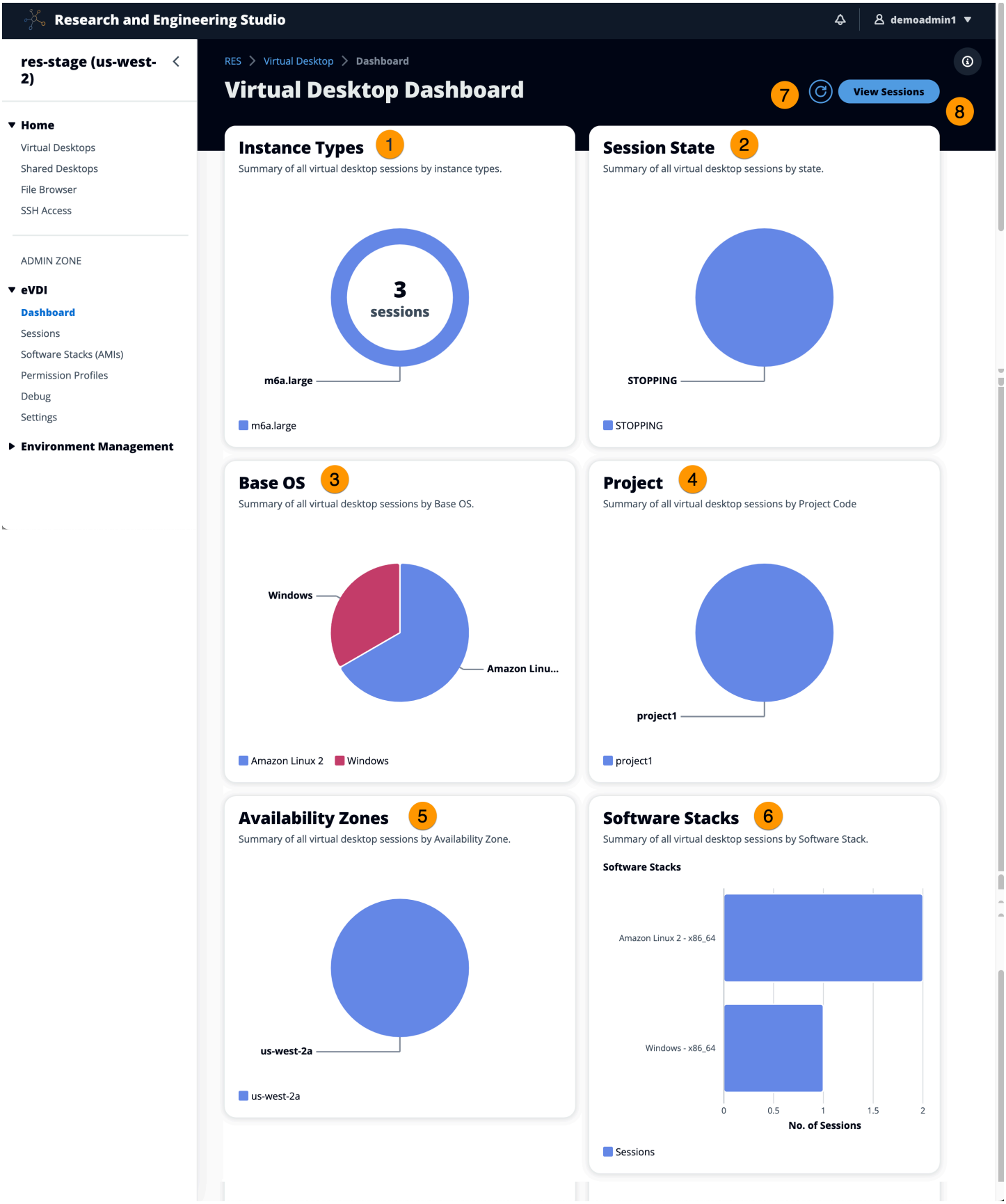
Tópicos

Gerenciamento de sessões

O gerenciamento de sessões fornece um ambiente flexível e interativo para desenvolver e testar sessões. Como usuário administrativo, você pode permitir que os usuários criem e gerenciem sessões interativas em seus ambientes de projeto.

Tópicos

Painel


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

O Painel de Gerenciamento de Sessões fornece aos administradores uma visão rápida de:

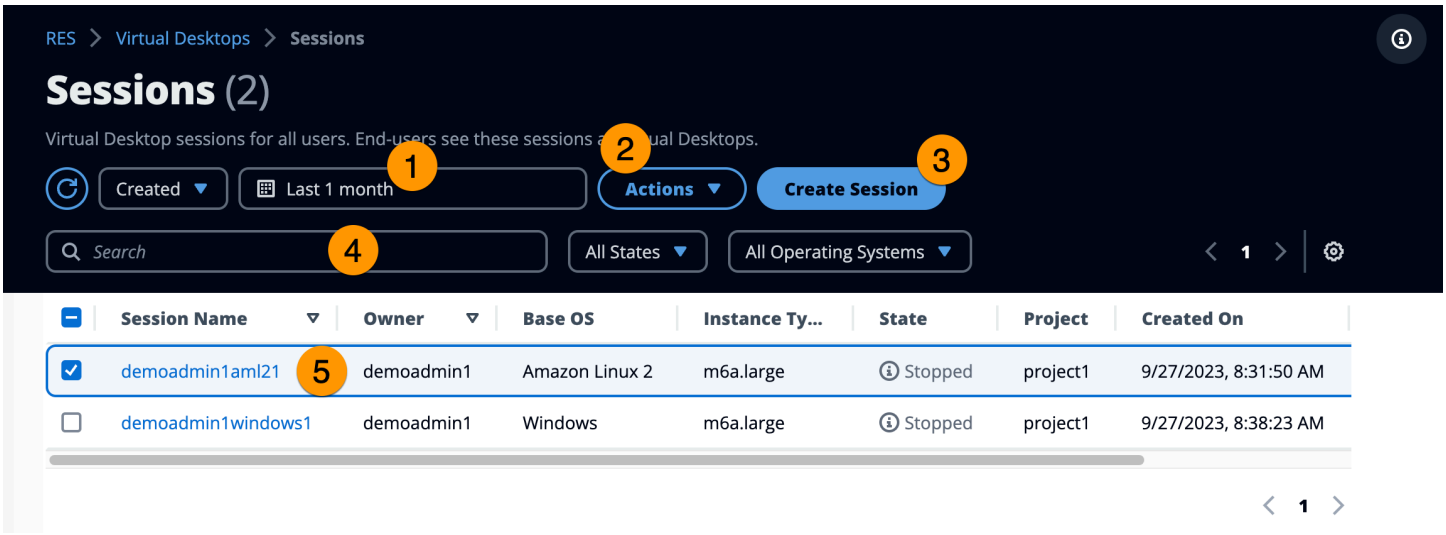
1. Tipos de instância
2. Estados da sessão
3. Sistema operacional básico
4. Projetos
5. Zonas de disponibilidade
6. Pilhas de software

Além disso, os administradores podem:

7. Atualize o painel para atualizar as informações.
8. Escolha Exibir sessões para navegar até Sessões.

Sessões

As sessões exibem todos os desktops virtuais criados no Research and Engineering Studio. Na página Sessões, você pode filtrar e visualizar as informações da sessão ou criar uma nova sessão.



1. Use o menu para filtrar os resultados por sessões criadas ou atualizadas dentro de um período de tempo especificado.
2. Selecione uma sessão e use o menu Ações para:
   a. Retomar sessão (s)
   b. Sessões de parar/hibernar

c. Sessão (ões) de parada forçada/hibernação

d. Encerrar sessão (s)

e. Forçar o encerramento da (s) sessão (s)

f. Sessão (s) Health

g. Crie uma pilha de software

3. Escolha Criar sessão para criar uma nova sessão.
4. Pesquise uma sessão por nome e filtre por estado e sistema operacional.
5. Escolha o nome da sessão para ver mais detalhes.

Crie uma sessão.

1. Escolha Criar sessão. O modal Launch New Virtual Desktop é aberto.
2. Insira os detalhes da nova sessão.
3. (Opcional.) Ative Mostrar opções avançadas para fornecer detalhes adicionais, como ID da sub-rede e tipo de sessão DCV.
4. Selecione Enviar.

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.

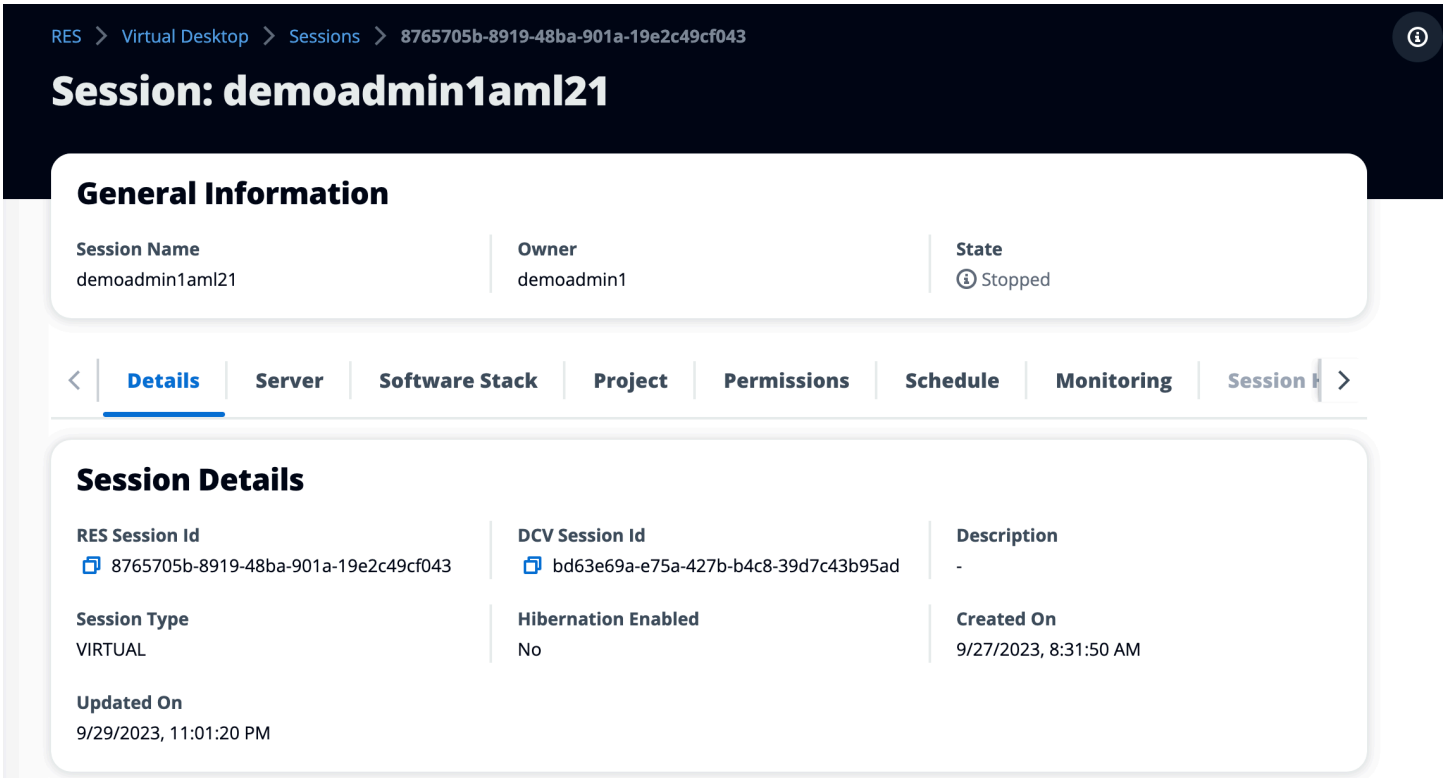
Virtual Desktop Size
Select a virtual desktop instance type

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

10

Detalhes da sessão

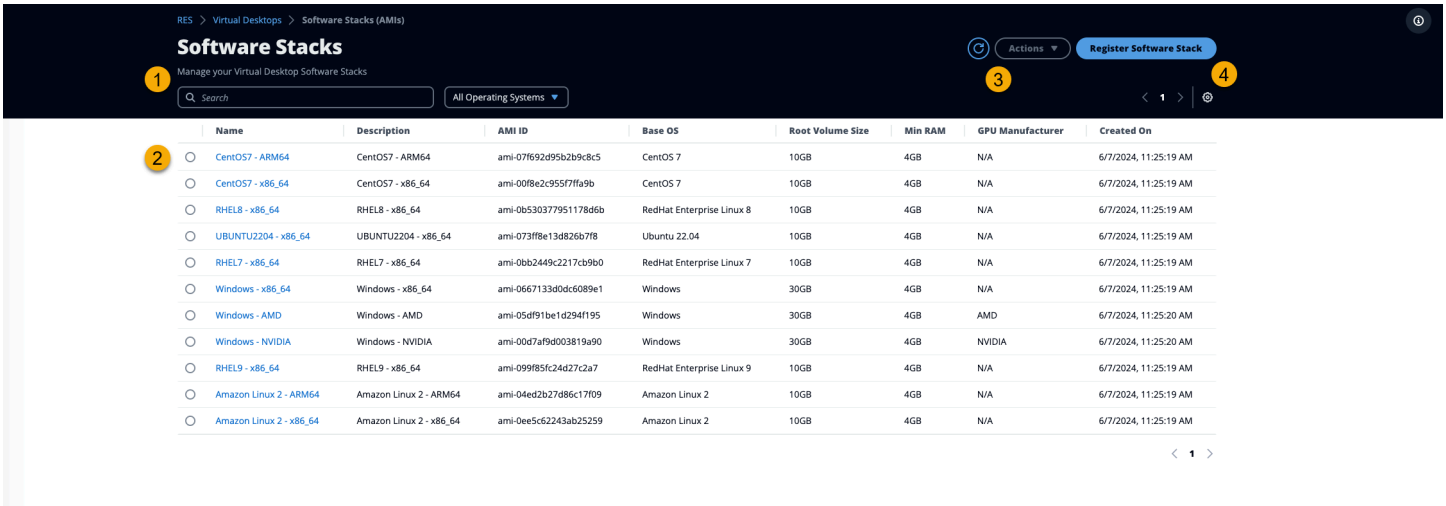
Na lista Sessões, escolha o Nome da sessão para ver os detalhes da sessão.



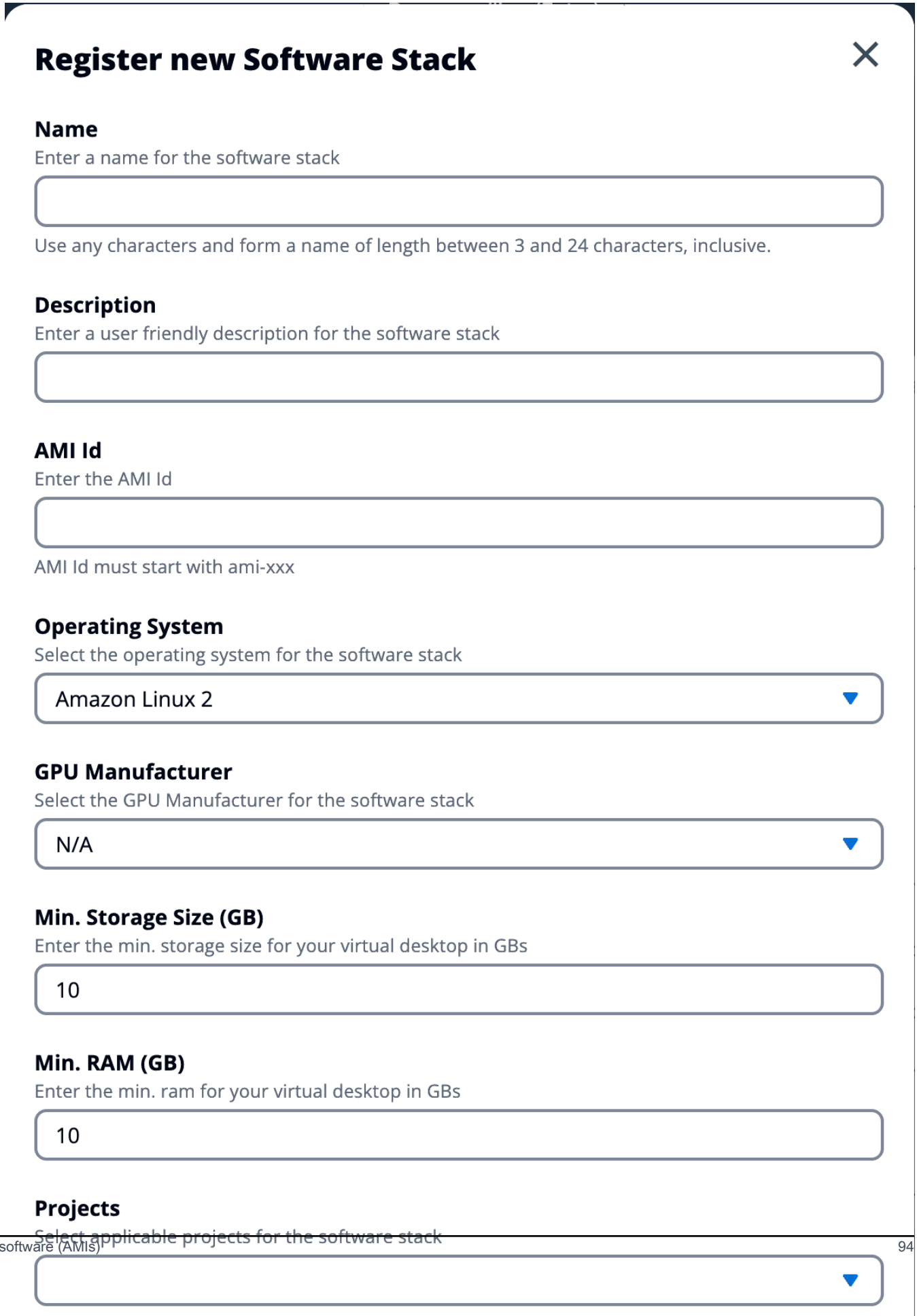
Pilhas de software (AMIs)

> **Note**
>
> Para executar a pilha de software CentSO7 fornecida AWS GovCloud (US), você precisará assinar a AMI AWS Marketplace usando sua conta padrão vinculada.

Na página Software Stacks, você pode configurar Amazon Machine Images (AMIs) e gerenciar as AMIs existentes.



1. Para pesquisar uma pilha de software existente, use o menu suspenso do sistema operacional para filtrar por sistema operacional.
2. Escolha o nome de uma pilha de software para ver detalhes sobre a pilha.
3. Depois de selecionar uma pilha de software, use o menu Ações para editar a pilha e atribuí-la a um projeto.
4. O botão Registrar pilha de software permite criar uma nova pilha:
    1. Escolha Registrar pilha de software.
    2. Insira os detalhes da nova pilha de software.
    3. Selecione Enviar.


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

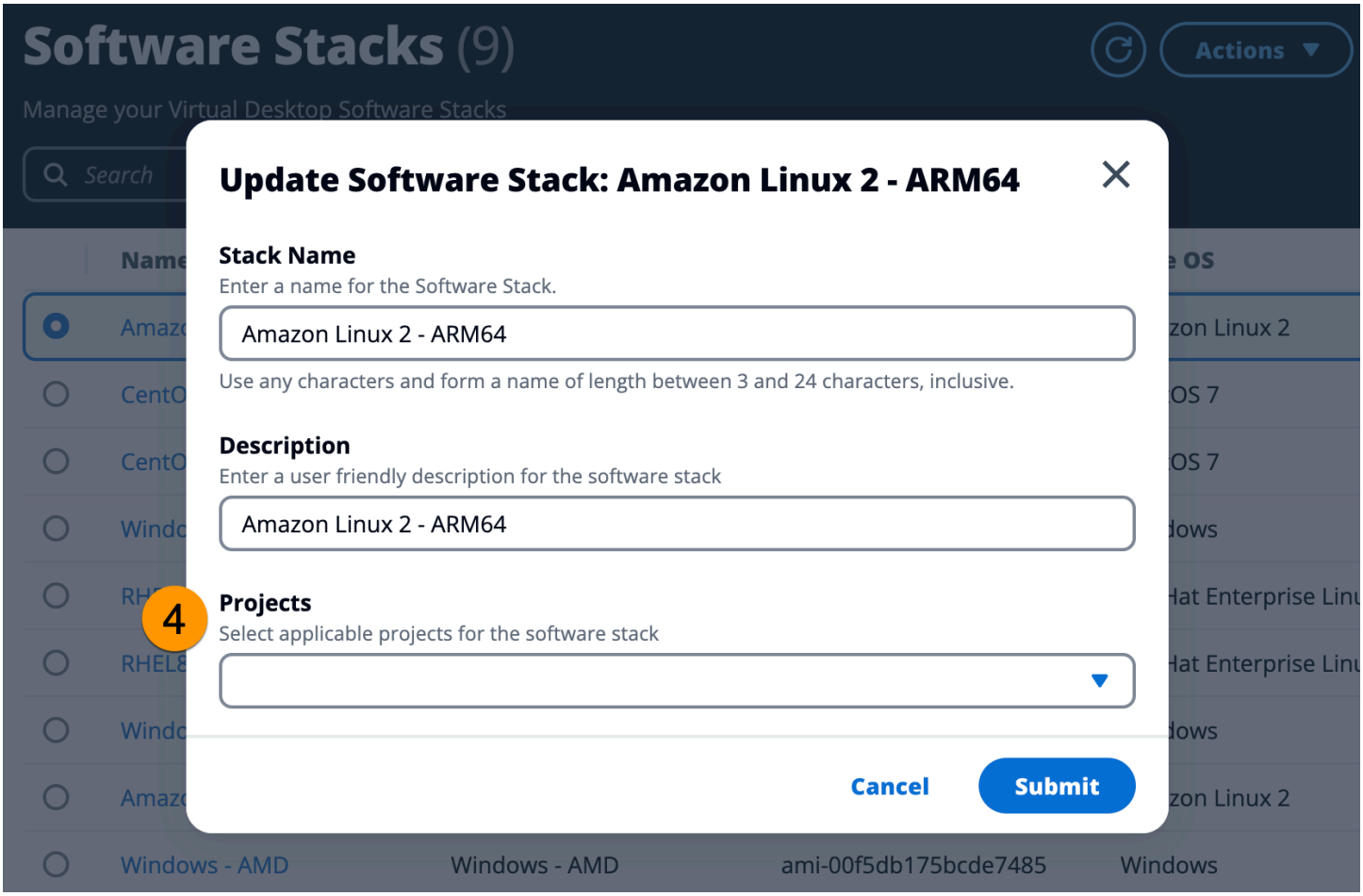
Atribuir pilha de software a um projeto

Ao criar uma nova pilha de software, você pode atribuir a pilha aos projetos. Se você precisar adicionar a pilha a um projeto após a criação inicial, faça o seguinte:

> **Note**
>
> Você só pode atribuir pilhas de software a projetos dos quais você é membro.

1. Selecione a pilha de software que você precisa adicionar a um projeto na página Pilhas de software.
2. Escolha Ações.
3. Selecione a opção Editar.
4. Use o menu suspenso Projetos para selecionar o projeto.
5. Selecione Enviar.

Você também pode editar a pilha de software na página de detalhes da pilha.

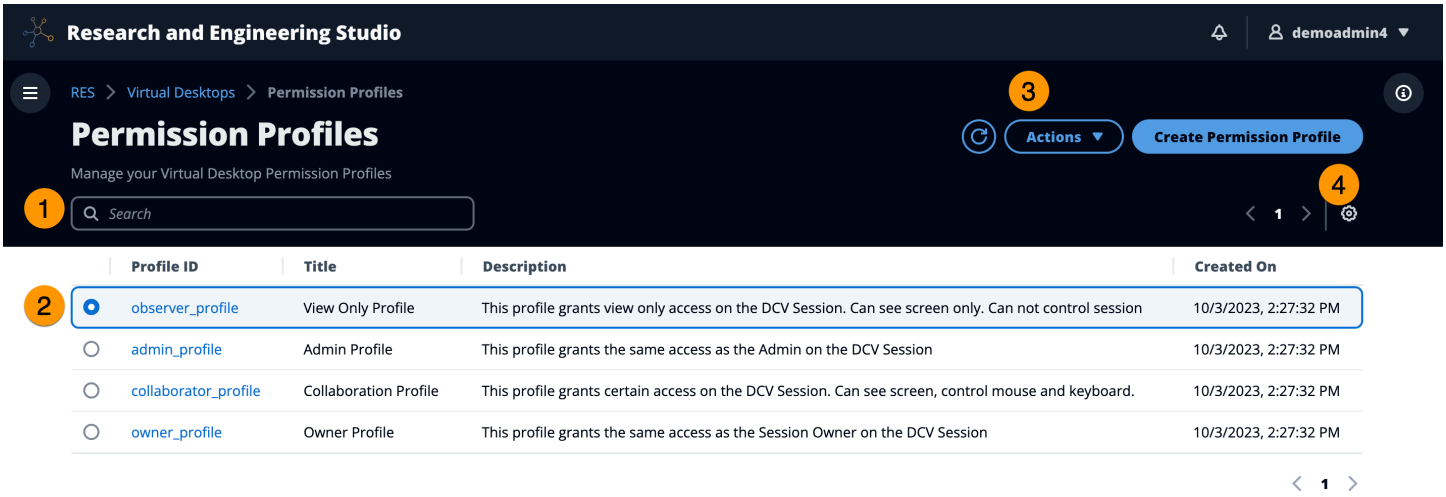


Veja os detalhes da pilha de software

Na lista de pilhas de software, escolha o nome da pilha de software para ver os detalhes. Na página de detalhes, você também pode escolher Editar para editar a pilha de software.

Perfis de permissão

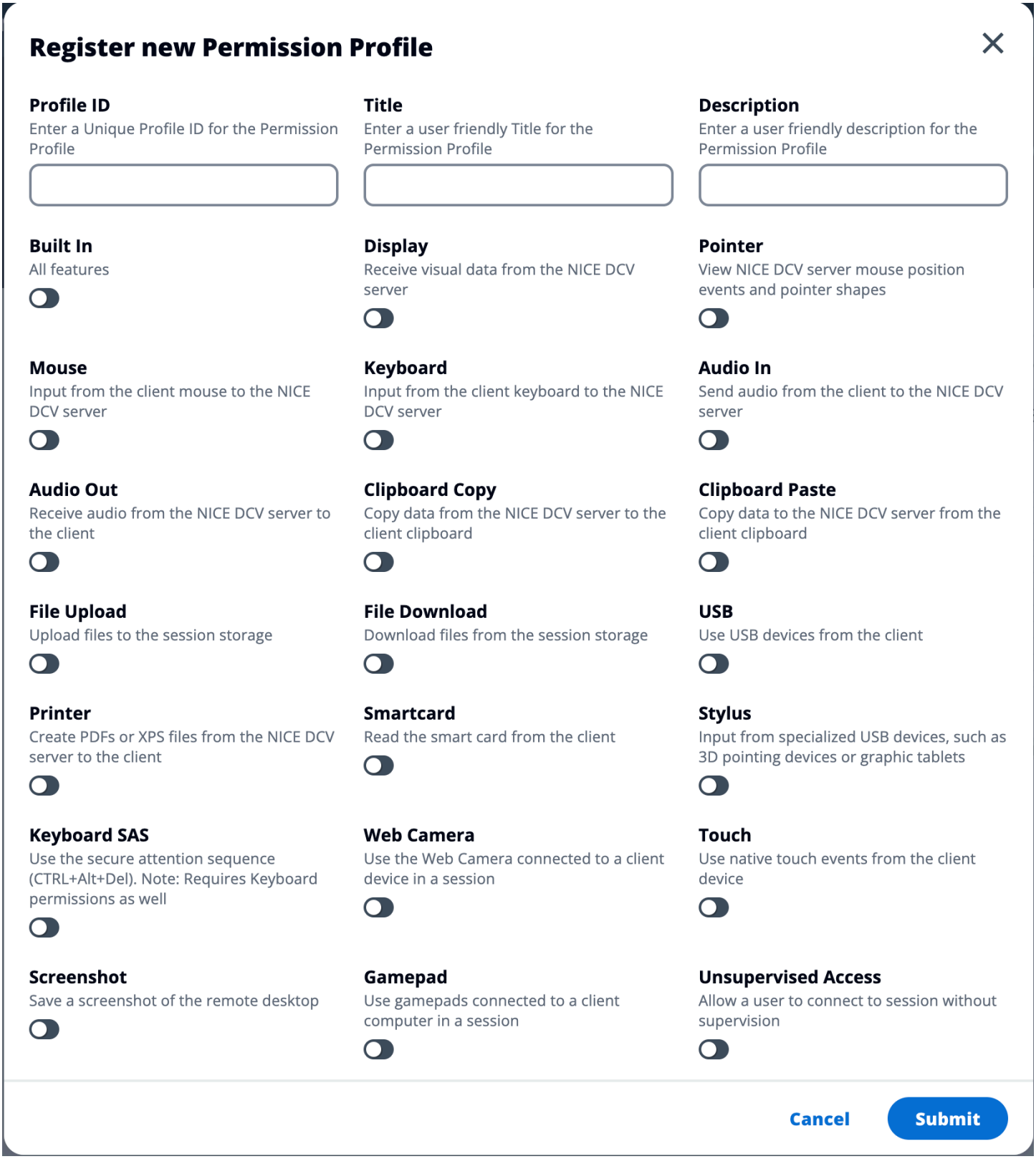
Use perfis de permissão para criar e gerenciar perfis reutilizáveis para obter permissões.



1. Pesquise um perfil de permissão.
2. Escolha a ID do perfil para ver os detalhes.
3. Quando um perfil é selecionado, use o menu Ações para editar o perfil.
4. Escolha Criar perfil de permissão para criar um novo perfil.

Crie um perfil de permissão

1. Escolha Criar perfil de permissão.
2. Insira os detalhes do novo perfil e use os botões de permissão para selecionar permissões para o perfil.
3. Selecione Enviar.


Register new Permission Profile
Profile ID
Enter a Unique Profile ID for the Permission Profile
Title
Enter a user friendly Title for the Permission Profile
Description
Enter a user friendly description for the Permission Profile
Built In
All features
Display
Receive visual data from the NICE DCV server
Pointer
View NICE DCV server mouse position events and pointer shapes
Mouse
Input from the client mouse to the NICE DCV server
Keyboard
Input from the client keyboard to the NICE DCV server
Audio In
Send audio from the client to the NICE DCV server
Audio Out
Receive audio from the NICE DCV server to the client
Clipboard Copy
Copy data from the NICE DCV server to the client clipboard
Clipboard Paste
Copy data to the NICE DCV server from the client clipboard
File Upload
Upload files to the session storage
File Download
Download files from the session storage
USB
Use USB devices from the client
Printer
Create PDFs or XPS files from the NICE DCV server to the client
Smartcard
Read the smart card from the client
Stylus
Input from specialized USB devices, such as 3D pointing devices or graphic tablets
Keyboard SAS
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
Web Camera
Use the Web Camera connected to a client device in a session
Touch
Use native touch events from the client device
Screenshot
Save a screenshot of the remote desktop
Gamepad
Use gamepads connected to a client computer in a session
Unsupervised Access
Allow a user to connect to session without supervision
Cancel
Submit

Editar um perfil de permissão

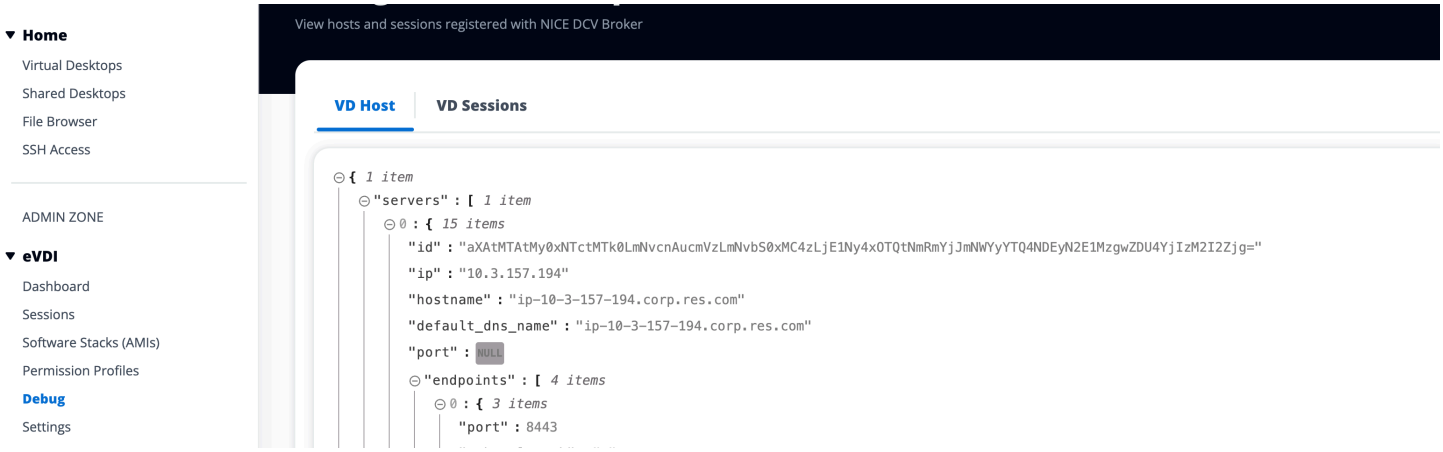
1. Selecione o perfil de permissão que você precisa editar na página Perfis de permissão.
2. Escolha Ações.
3. Escolha Editar perfil de permissão.
4. Edite o perfil.
5. Selecione Enviar.

Exibir detalhes do perfil de permissão

Na lista Perfis de permissão, escolha a ID do perfil para ver os detalhes. Na página de detalhes, você também pode escolher Editar para editar o perfil de permissão.

Depuração

O painel de depuração exibe o tráfego de mensagens associado aos desktops virtuais. Você pode usar esse painel para observar a atividade entre os anfitriões. A guia VD Host exibe a atividade específica da instância e a guia VD Sessions exibe a atividade da sessão em andamento.

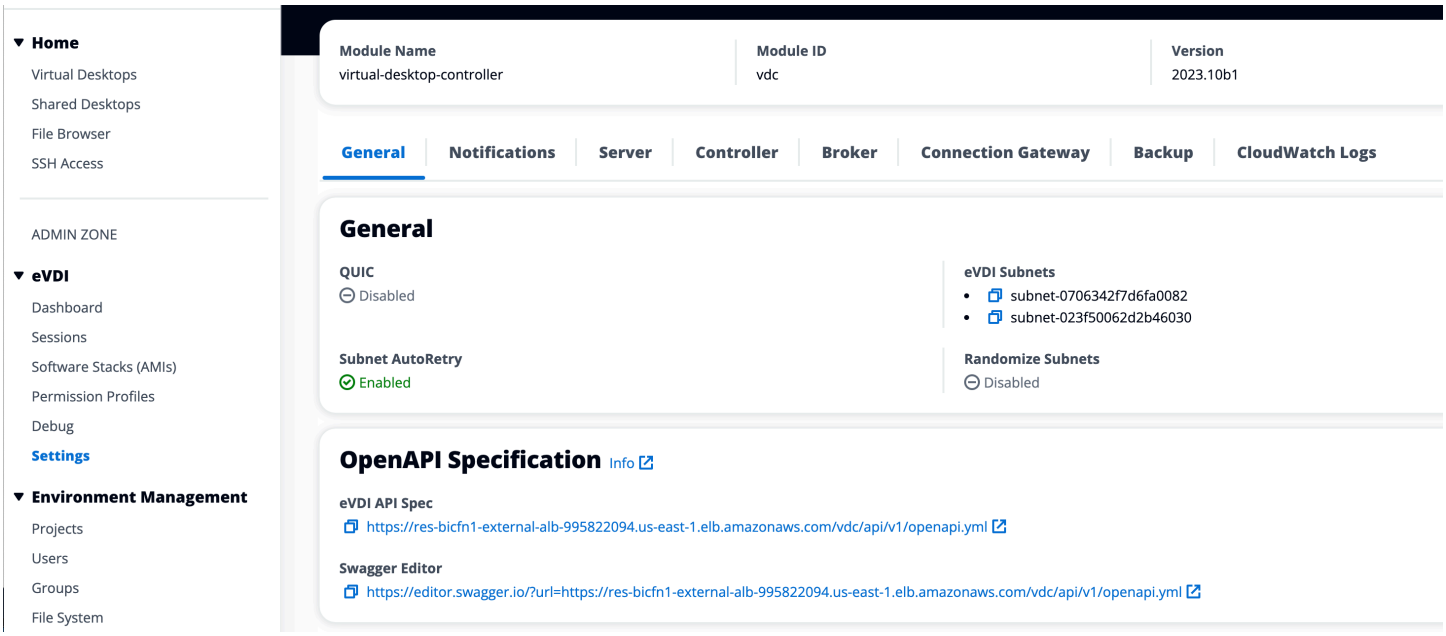


Configurações da área de trabalho

Você pode usar a página Configurações da área de trabalho para configurar os recursos associados às áreas de trabalho virtuais. A guia Servidor fornece acesso a configurações como:

- Tempo limite de inatividade da sessão DCV
- Aviso de tempo limite de inatividade

- Limite de utilização da CPU
- Sessões permitidas por usuário



Gestão do meio ambiente

Na seção de gerenciamento ambiental do RES, os usuários administrativos podem criar e gerenciar ambientes isolados para seus projetos de pesquisa e engenharia. Esses ambientes podem incluir recursos computacionais, armazenamento e outros componentes necessários, tudo dentro de um ambiente seguro. Os usuários podem configurar e personalizar esses ambientes para atender aos requisitos específicos de seus projetos, facilitando a experimentação, o teste e a iteração de suas soluções sem afetar outros projetos ou ambientes.

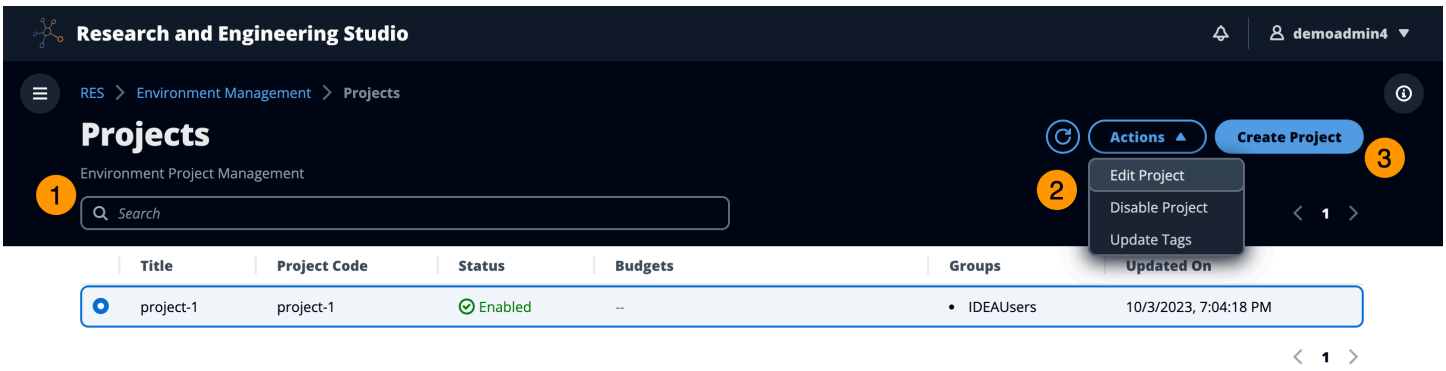
Tópicos

Projetos

Os projetos formam um limite para desktops, equipes e orçamentos virtuais. Ao criar um projeto, você define suas configurações, como nome, descrição e configuração do ambiente. Os projetos geralmente incluem um ou mais ambientes, que podem ser personalizados para atender aos requisitos específicos do seu projeto, como o tipo e o tamanho dos recursos computacionais, a pilha de software e a configuração de rede.

Tópicos

Exibir projetos



O painel Projetos fornece uma lista dos projetos disponíveis para você. No painel Projetos, você pode:

1. Você pode usar o campo de pesquisa para encontrar projetos.
2. Quando um projeto é selecionado, você pode usar o menu Ações para:
   a. Editar um projeto
   b. Desativar ou ativar um projeto
   c. Atualizar as tags do projeto

3. Você pode escolher Criar projeto para criar um novo projeto.

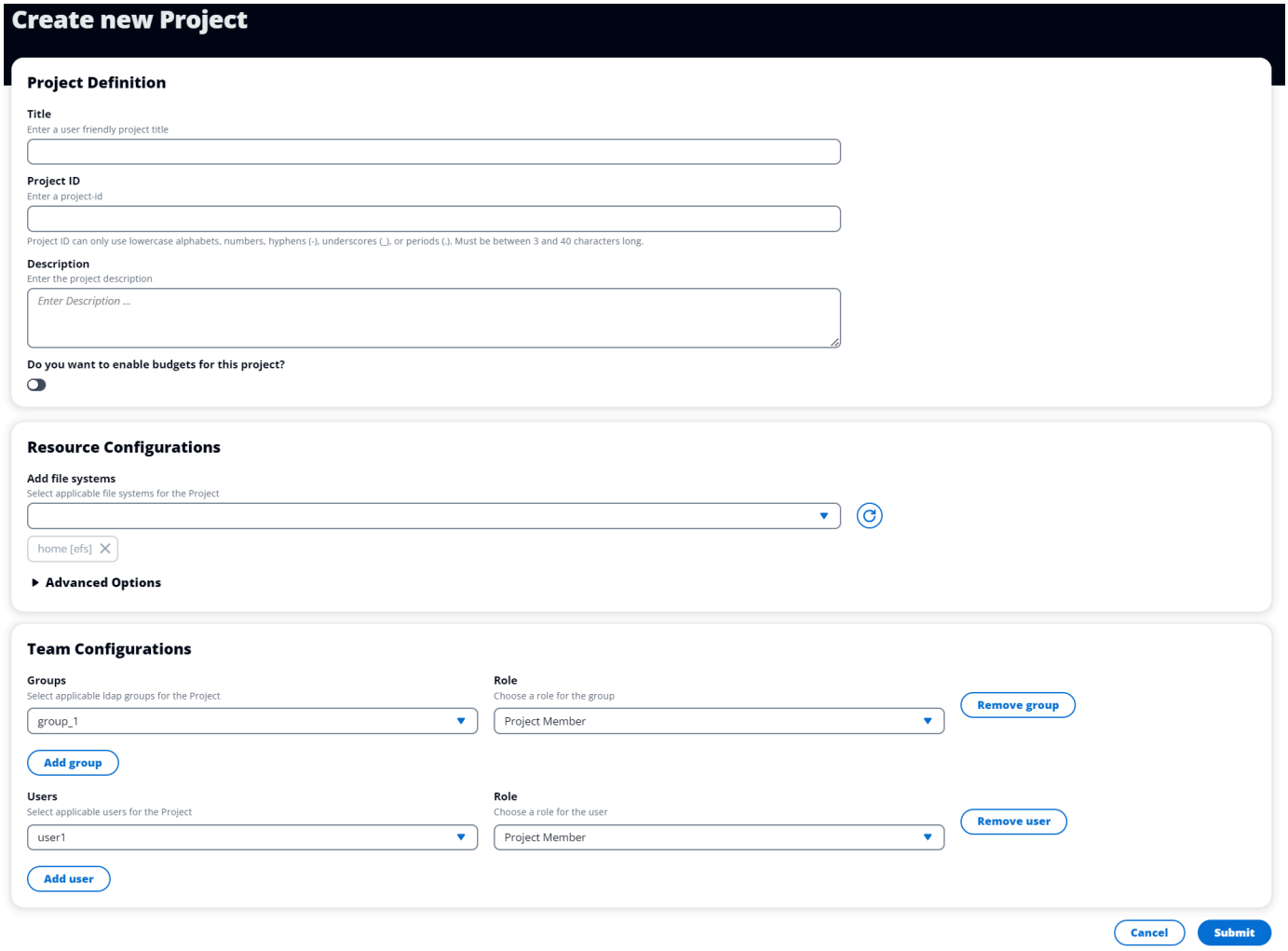
Criar um projeto

1. Escolha Criar projeto.
2. Insira os detalhes do projeto.

   O ID do projeto é uma tag de recurso que pode ser usada para rastrear a alocação de custos em AWS Cost Explorer Service. Para obter mais informações, consulte Ativação de tags de alocação de custos definidas pelo usuário.

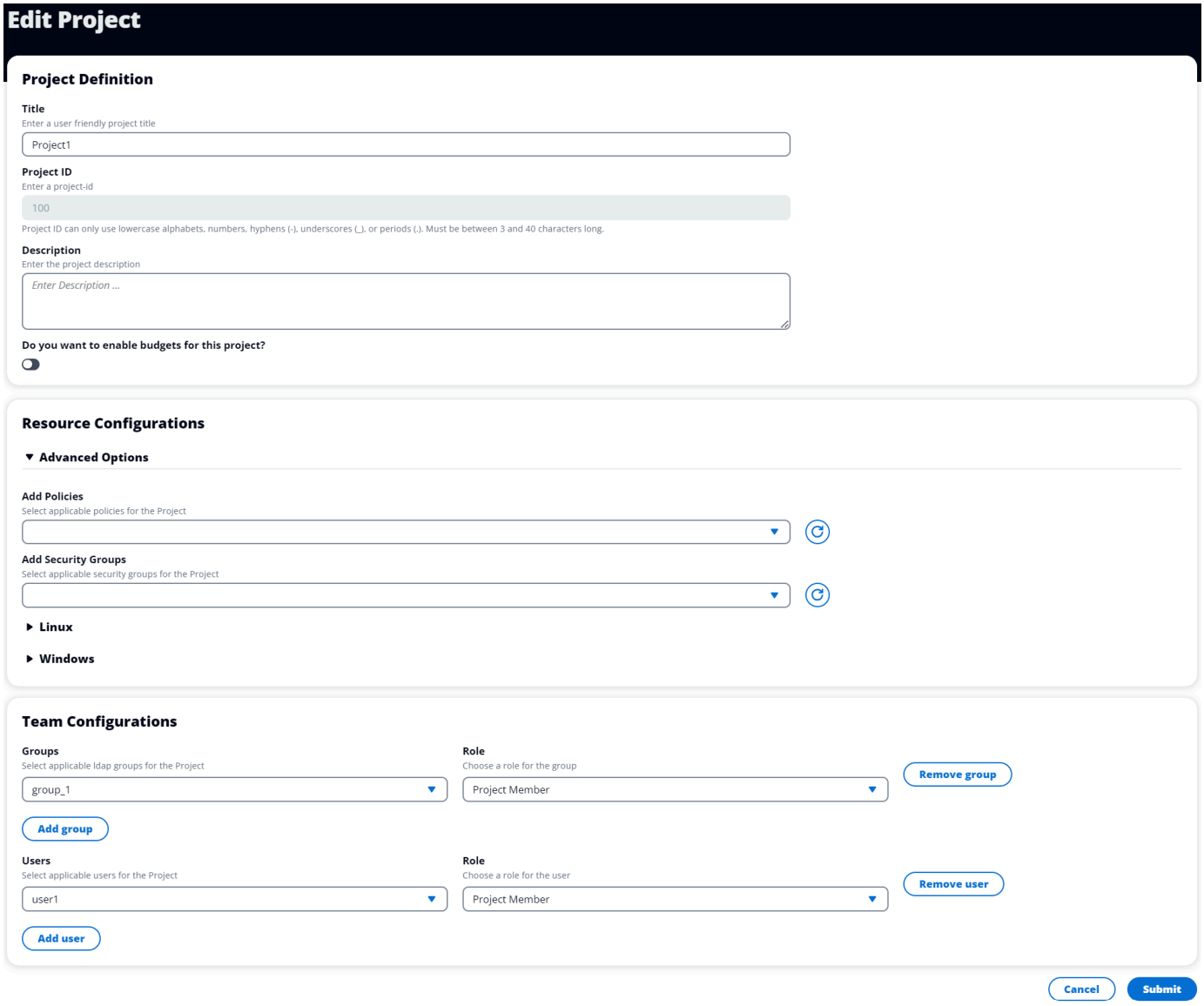
   > **Important**
   >
   > O ID do projeto não pode ser alterado após a criação.

   Para obter informações sobre opções avançadas, consulteAdicionar um modelo de lançamento.
3. (Opcional) Ative os orçamentos para o projeto. Para obter mais informações sobre orçamentos, consulte. Monitoramento e controle de custos
4. Atribua aos usuários e/ou grupos a função apropriada (“Membro do projeto” ou “Proprietário do projeto”). Veja Permissões as ações que cada função pode realizar.
5. Selecione Enviar.



Editar um projeto

1. Selecione um projeto na lista de projetos.
2. No menu Ações, escolha Editar projeto.
3. Insira suas atualizações. Se você pretende habilitar orçamentos, consulte Monitoramento e controle de custos para obter mais informações. Para obter informações sobre opções avançadas, consulteAdicionar um modelo de lançamento.
4. Selecione Enviar.



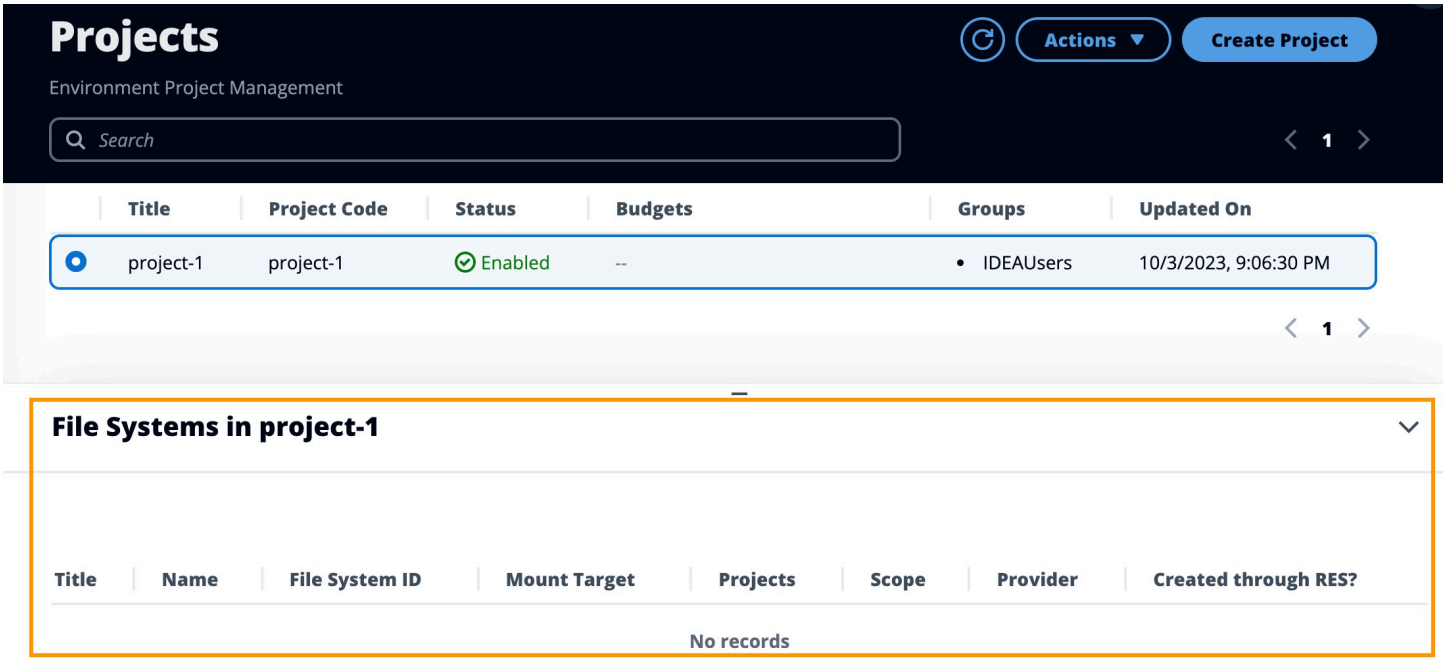
Adicionar ou remover tags de um projeto

As tags do projeto atribuirão tags a todas as instâncias criadas nesse projeto.

1. Selecione um projeto na lista de projetos.
2. No menu Ações, escolha Atualizar tags.
3. Escolha Adicionar tags e insira um valor para Chave.
4. Para remover tags, escolha Remover ao lado da tag que você deseja remover.

Exibir sistemas de arquivos associados a um projeto

Quando um projeto é selecionado, você pode expandir o painel Sistemas de arquivos na parte inferior da tela para visualizar os sistemas de arquivos associados ao projeto.



Adicionar um modelo de lançamento

Ao criar ou editar um projeto, você pode adicionar modelos de lançamento usando as Opções avançadas na configuração do projeto. Os modelos de lançamento fornecem configurações adicionais, como grupos de segurança, políticas do IAM e scripts de lançamento para todas as instâncias de VDI dentro do projeto.

Adicionar políticas

Você pode adicionar uma política do IAM para controlar o acesso à VDI para todas as instâncias implantadas em seu projeto. Para integrar uma política, marque a política com o seguinte par de valores-chave:

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

Para obter mais informações sobre as funções do IAM, consulte Políticas e permissões no IAM.

Adição de grupos de segurança

Você pode adicionar um grupo de segurança para controlar os dados de entrada e saída de todas as instâncias de VDI em seu projeto. Para integrar um grupo de segurança, marque o grupo de segurança com o seguinte par de valores-chave:

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

Para obter mais informações sobre grupos de segurança, consulte Controle o tráfego para seus AWS recursos usando grupos de segurança no Guia do usuário da Amazon VPC.

Adicionar scripts de lançamento

Você pode adicionar scripts de lançamento que serão iniciados em todas as sessões de VDI em seu projeto. O RES suporta a iniciação de scripts para Linux e Windows. Para iniciar o script, você pode escolher:

Executar script quando a VDI é iniciada

Essa opção inicia o script no início de uma instância de VDI antes que qualquer configuração ou instalação do RES seja executada.

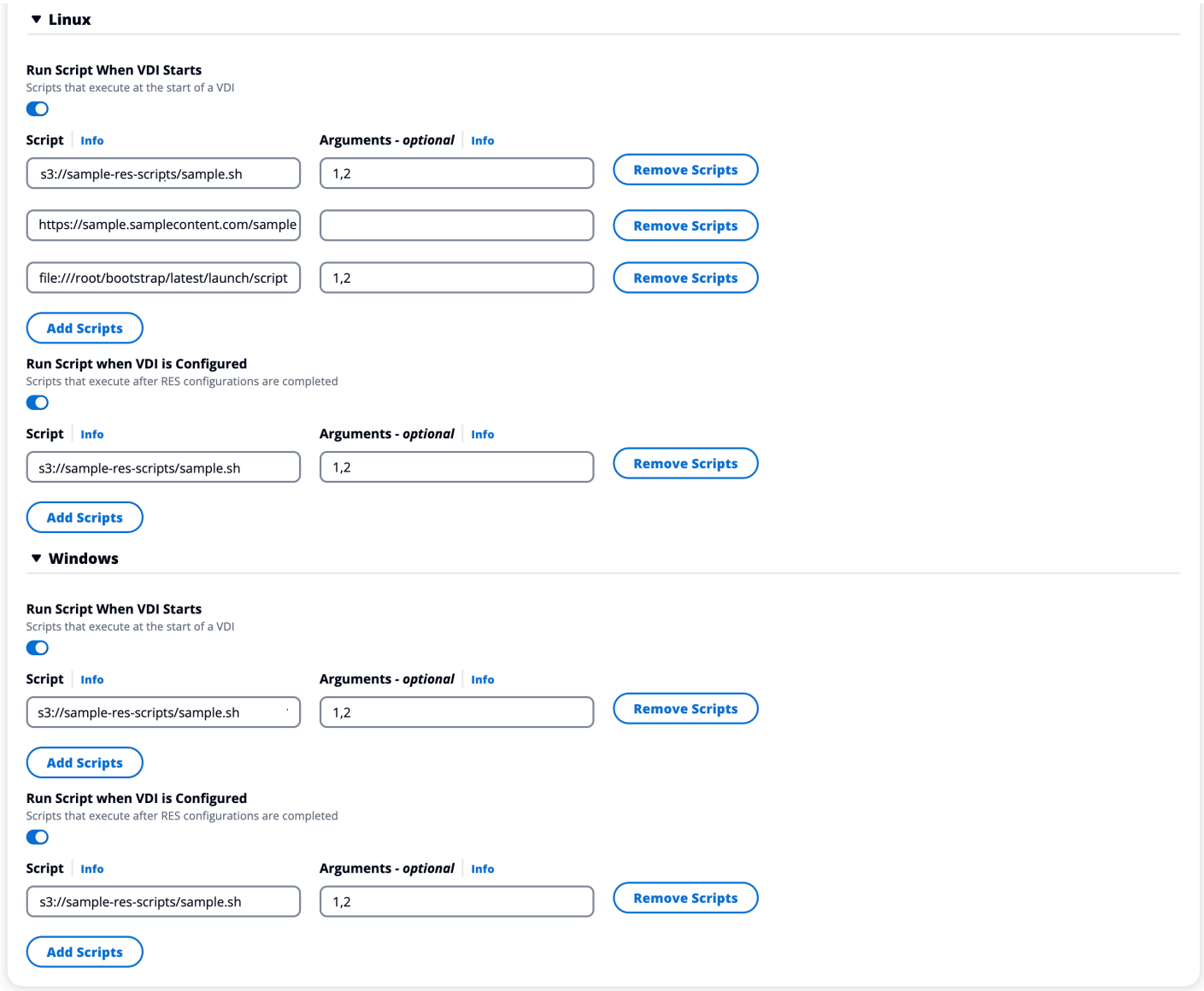
Executar script quando o VDI estiver configurado

Essa opção inicia o script após a conclusão das configurações do RES.

Os scripts oferecem suporte às seguintes opções:

Configuração do script	Exemplo
URI do S3	s3://bucketname/script.sh
URL de HTTPS	https://sample.samplecontent.com/sample
Arquivo local	arquivo: ///user/scripts/example.sh

Para Argumentos, forneça quaisquer argumentos separados por uma vírgula.

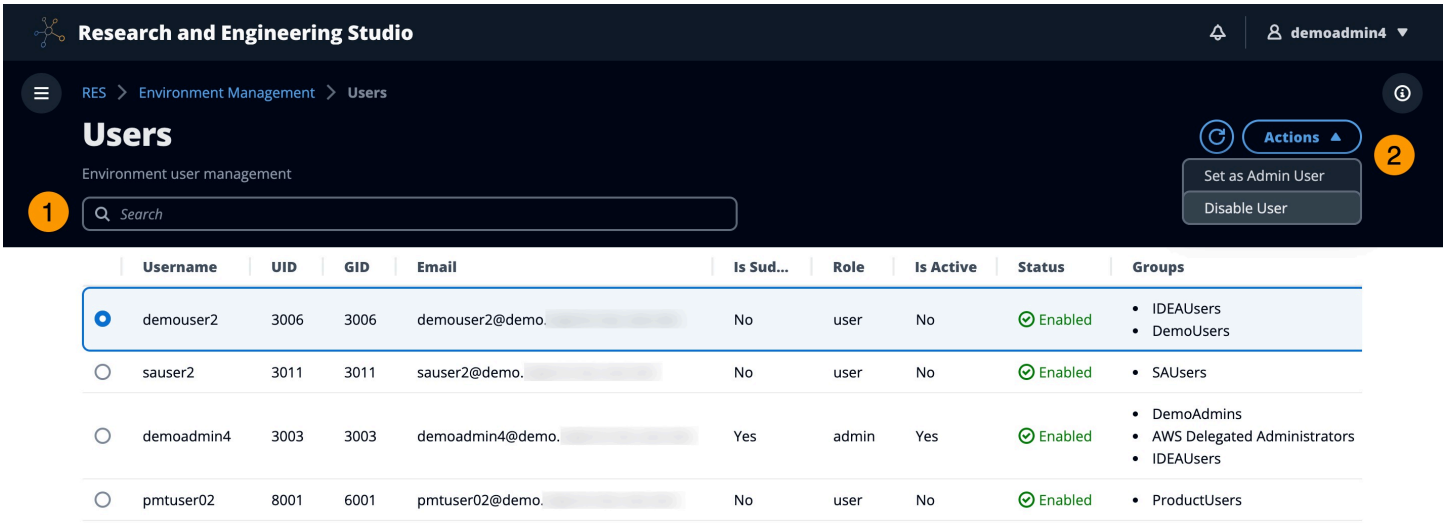


Exemplo de uma configuração de projeto

Usuários

Todos os usuários sincronizados do seu diretório ativo aparecerão na página Usuários. Os usuários são sincronizados pelo usuário cluster-admin durante a configuração do produto. Para obter mais informações sobre a configuração inicial do usuário, consulte Guia de configuração o.

> **Note**
>
> Os administradores só podem criar sessões para usuários ativos. Por padrão, todos os usuários ficarão inativos até entrarem no ambiente do produto. Se um usuário estiver inativo, peça que ele faça login antes de criar uma sessão para ele.

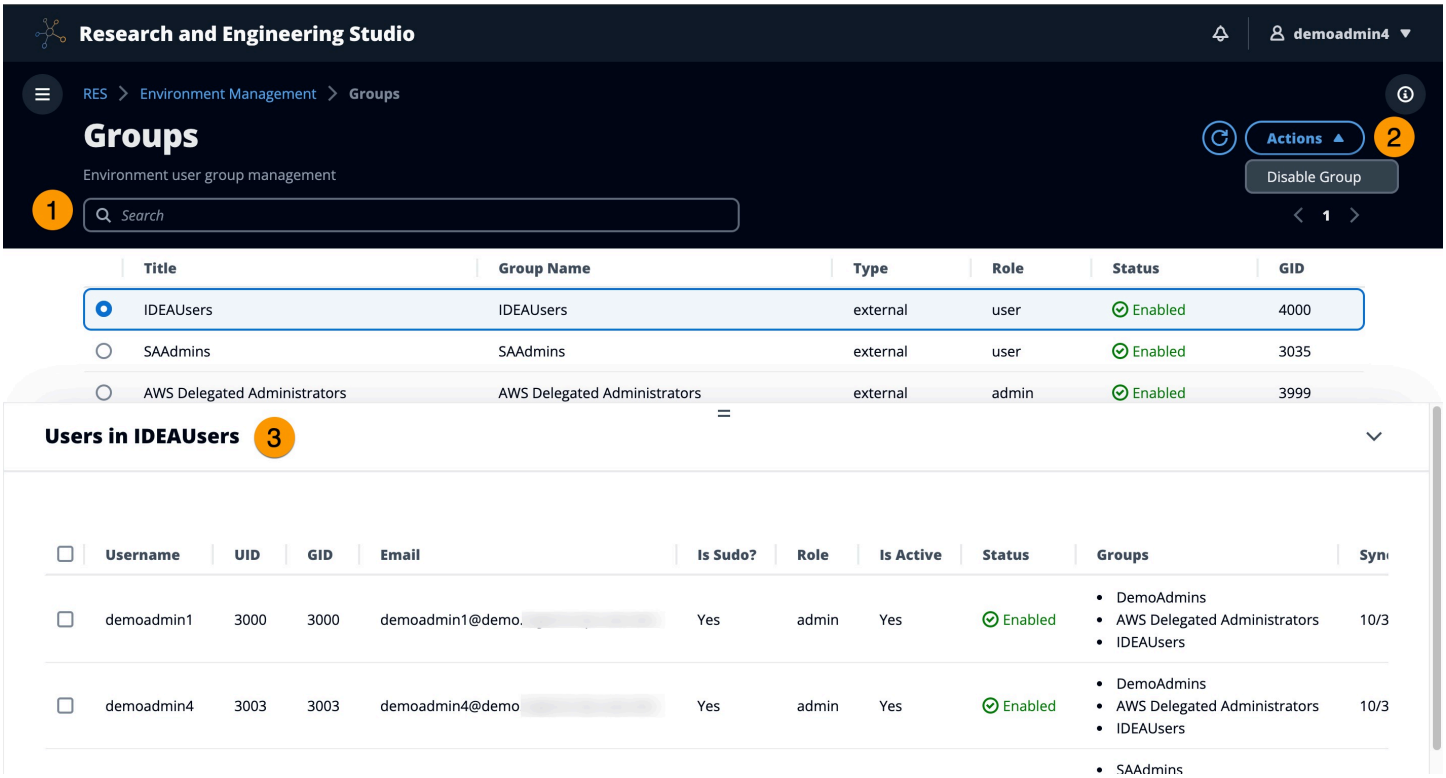


Na página Usuários, você pode:

1. Pesquisar usuários.
2. Quando um nome de usuário for selecionado, use o menu Ações para:
    a. Definir como usuário administrador
    b. Desativar usuário

Grupos

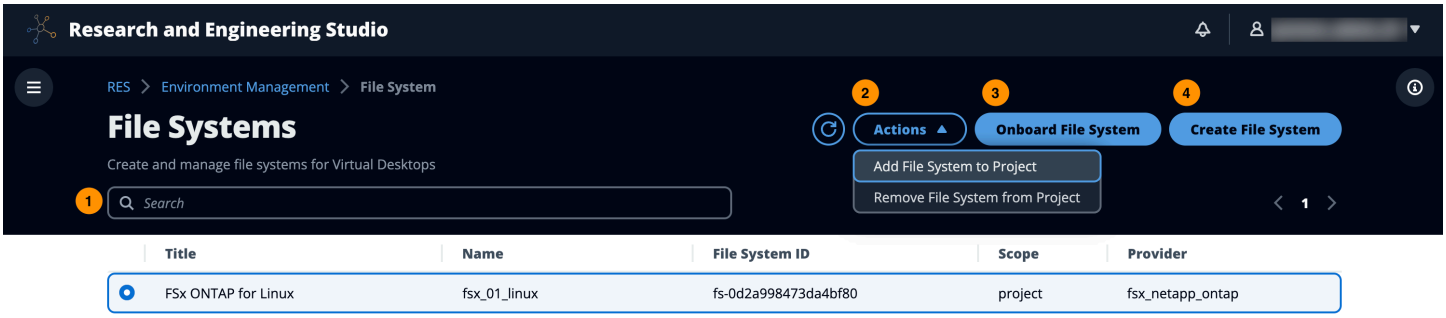
Todos os grupos sincronizados do Active Directory aparecem na página Grupos. Para obter mais informações sobre configuração e gerenciamento de grupos, consulte Guia de configuração o.



Na página Grupos, você pode:

1. Pesquise grupos de usuários.
2. Quando um grupo de usuários é selecionado, use o menu Ações para desativar ou ativar um grupo.
3. Quando um grupo de usuários é selecionado, você pode expandir o painel Usuários na parte inferior da tela para visualizar os usuários no grupo.

Sistemas de arquivos



Na página Sistemas de arquivos, você pode:

1. Pesquise sistemas de arquivos.
2. Quando um sistema de arquivos for selecionado, use o menu Ações para:
    a. Adicionar o sistema de arquivos a um projeto
    b. Remover o sistema de arquivos de um projeto
3. Integre um novo sistema de arquivos.
4. Crie um sistema de arquivos.
5. Quando um sistema de arquivos é selecionado, você pode expandir o painel na parte inferior da tela para visualizar os detalhes do sistema de arquivos.

Crie um sistema de arquivos

1. Escolha Criar sistema de arquivos.
2. Insira os detalhes do novo sistema de arquivos.
3. Forneça IDs de sub-rede da VPC. Você pode encontrar as IDs na guia Gerenciamento de ambiente > Configurações > Rede.
4. Selecione Enviar.

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

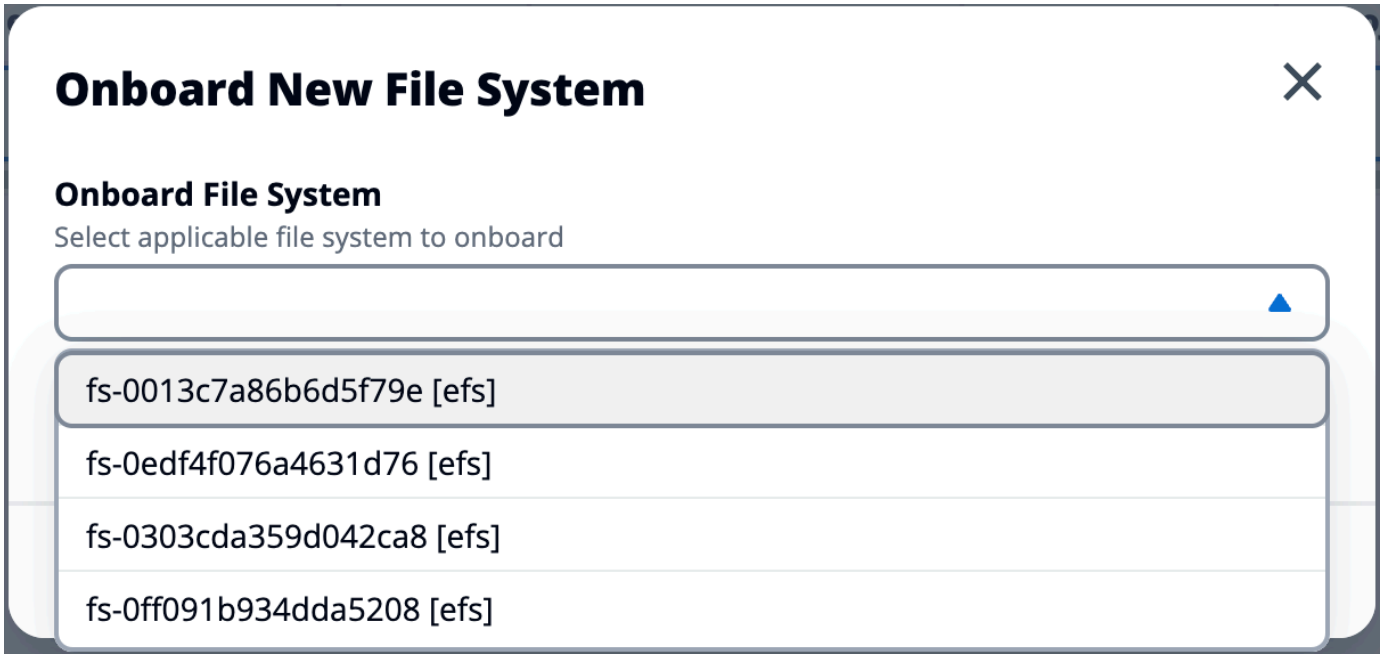
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

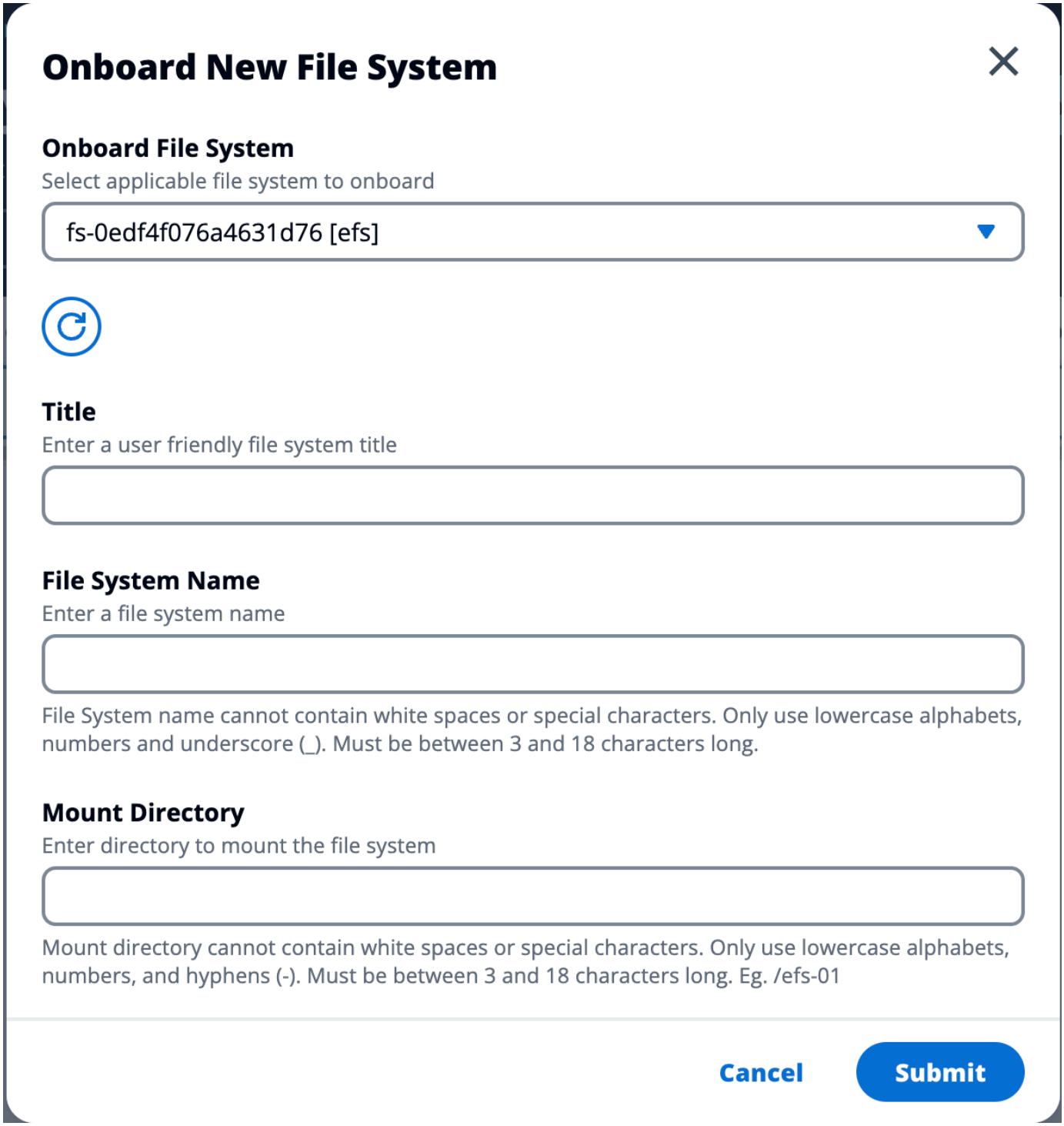
Enter directory to mount the file system

Integrar um sistema de arquivos

1. Escolha Sistema de arquivos integrado.
2. Selecione um sistema de arquivos no menu suspenso. O modal se expandirá com entradas adicionais de detalhes.

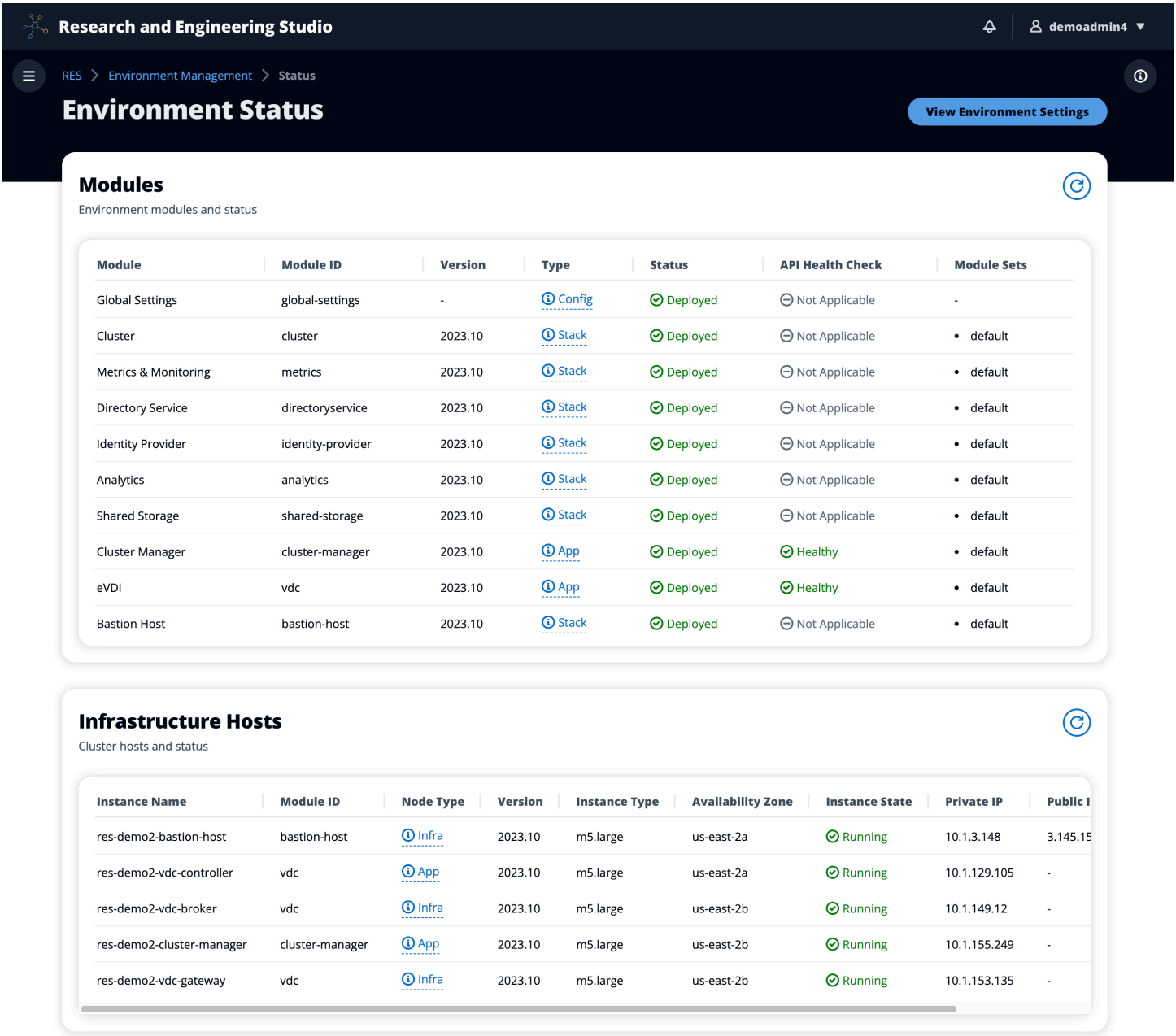


3. Insira os detalhes do sistema de arquivos.
4. Selecione Enviar.



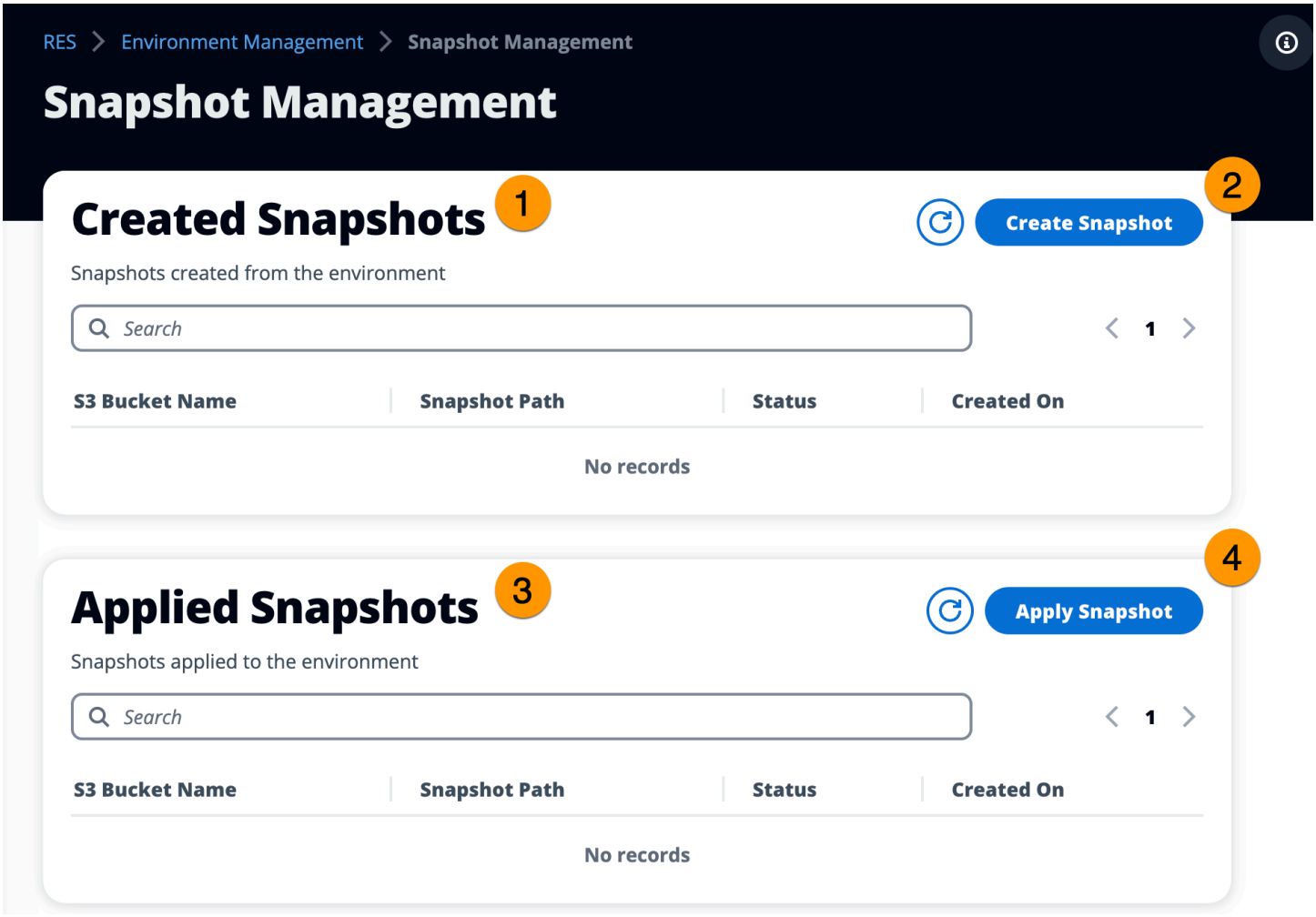
Status do ambiente

A página Status do ambiente exibe o software e os hosts implantados no produto. Ele inclui informações como versão do software, nomes de módulos e outras informações do sistema.



Gerenciamento de instantâneos

O gerenciamento de instantâneos simplifica o processo de salvar e migrar dados entre ambientes, garantindo consistência e precisão. Com os instantâneos, você pode salvar o estado do seu ambiente e migrar dados para um novo ambiente com o mesmo estado.



Na página de gerenciamento de snapshots, você pode:

1. Visualize todos os instantâneos criados e seus status.
2. Crie um instantâneo. Antes de criar um snapshot, você precisará criar um bucket com as permissões apropriadas.
3. Visualize todos os instantâneos aplicados e seus status.
4. Aplique um instantâneo.

Criar um snapshot

Antes de criar um snapshot, você deve fornecer um bucket do Amazon S3 com as permissões necessárias. Para obter informações sobre como criar um bucket, consulte Criar um bucket. Recomendamos ativar o controle de versão do bucket e o registro de acesso ao servidor. Essas configurações podem ser ativadas na guia Propriedades do bucket após o provisionamento.

> **Note**
>
> O ciclo de vida desse bucket Amazon S3 não será gerenciado dentro do produto. Você precisará gerenciar o ciclo de vida do bucket a partir do console.

Para adicionar permissões ao bucket:

1. Escolha o bucket que você criou na lista Buckets.
2. Escolha a aba Permissões.
3. Em Bucket policy (Política de bucket), escolha Edit (Editar).
4. Adicione a seguinte declaração à política do bucket. Substitua esses valores pelos seus próprios:
   - AWS_ACCOUNT_ID
   - RES_NOME_DO_AMBIENTE
   - AWS_REGION
   - S3_BUCKET_NAME

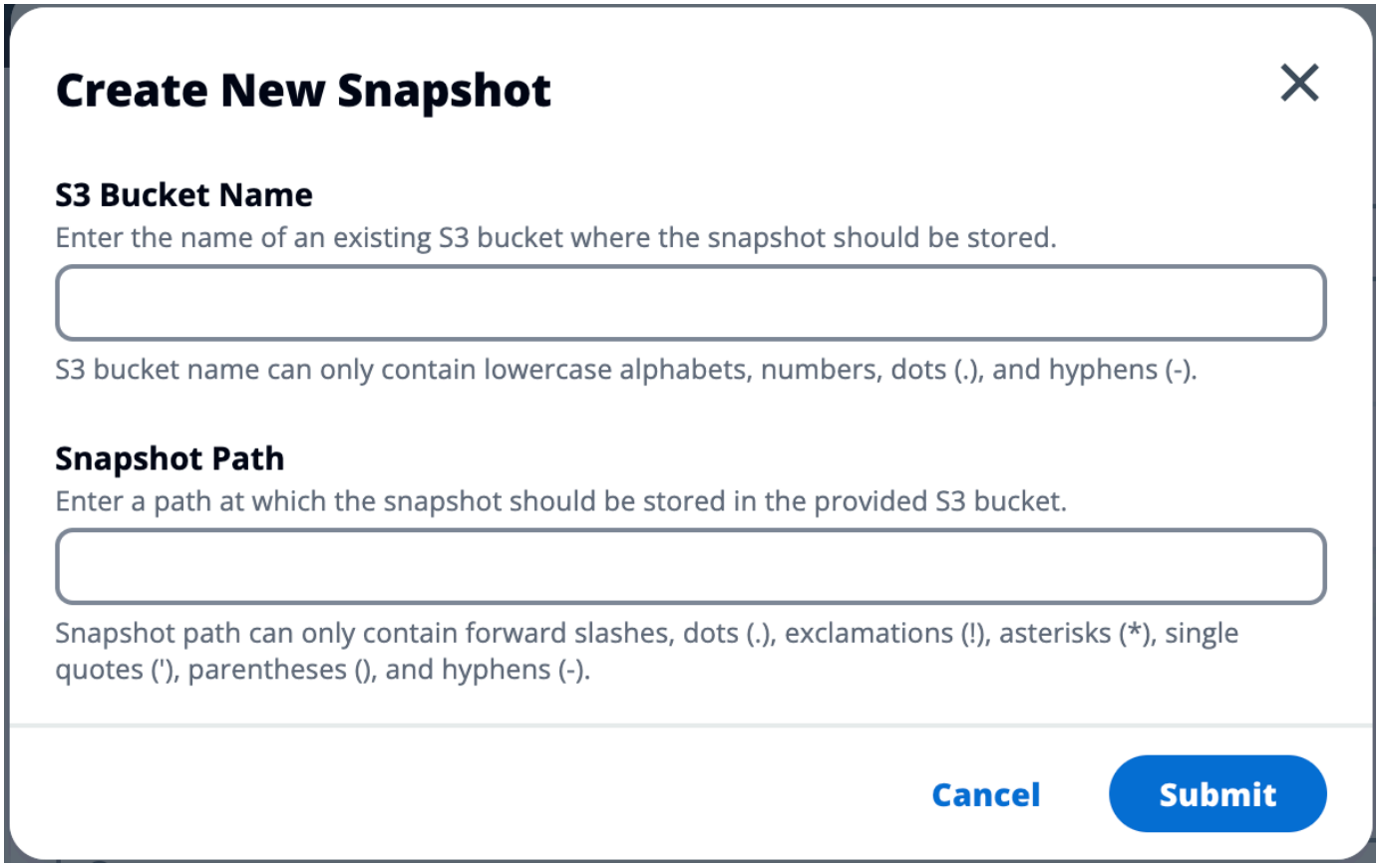
> **Important**
>
> Existem strings de versões limitadas suportadas pelo AWS. Para obter mais informações, consulte https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}: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": "*"
        }
    ]
}
```

Para criar o instantâneo:

1. Escolha Create Snapshot (Criar snapshot).
2. Insira o nome do bucket do Amazon S3 que você criou.
3. Insira o caminho em que você gostaria que o instantâneo fosse armazenado no bucket. Por exemplo, **`october2023/23`**.
4. Selecione Enviar.



5. Depois de cinco a dez minutos, escolha Atualizar na página Snapshots para verificar o status. Um snapshot não será válido até que o status mude de IN_PROGRESS para COMPLETED.

Aplicar um instantâneo

Depois de criar um instantâneo de um ambiente, você pode aplicar esse instantâneo a um novo ambiente para migrar dados. Você precisará adicionar uma nova política ao bucket, permitindo que o ambiente leia o snapshot.

A aplicação de um snapshot copia dados como permissões de usuário, projetos, pilhas de software, perfis de permissão e sistemas de arquivos com suas associações em um novo ambiente. As sessões do usuário não serão replicadas. Quando o instantâneo é aplicado, ele verifica as informações básicas de cada registro de recurso para determinar se ele já existe. Para registros duplicados, o instantâneo ignora a criação de recursos no novo ambiente. Para registros semelhantes, como compartilhar um nome ou chave, mas outras informações básicas de recursos variam, ele criará um novo registro com um nome e uma chave modificados usando a seguinte convenção:`RecordName_SnapshotRESVersion_ApplySnapshotID`. `ApplySnapshotID`Parece um carimbo de data/hora e identifica cada tentativa de aplicar um instantâneo.

Durante a aplicação do snapshot, o snapshot verifica a disponibilidade dos recursos. O recurso não disponível para o novo ambiente não será criado. Para recursos com um recurso dependente, o snapshot verifica a disponibilidade do recurso dependente. Se o recurso dependente não estiver disponível, ele criará o recurso principal sem o recurso dependente.

Se o novo ambiente não for o esperado ou falhar, você poderá verificar os CloudWatch registros encontrados no grupo de registros `/res-<env-name>/cluster-manager` para obter detalhes. Cada registro terá a tag [aplicar instantâneo]. Depois de aplicar um snapshot, você pode verificar seu status na the section called “Gerenciamento de instantâneos” página.

Para adicionar permissões ao bucket:

1. Escolha o bucket que você criou na lista Buckets.
2. Escolha a aba Permissões.
3. Em Bucket policy (Política de bucket), escolha Edit (Editar).
4. Adicione a seguinte declaração à política do bucket. Substitua esses valores pelos seus próprios:

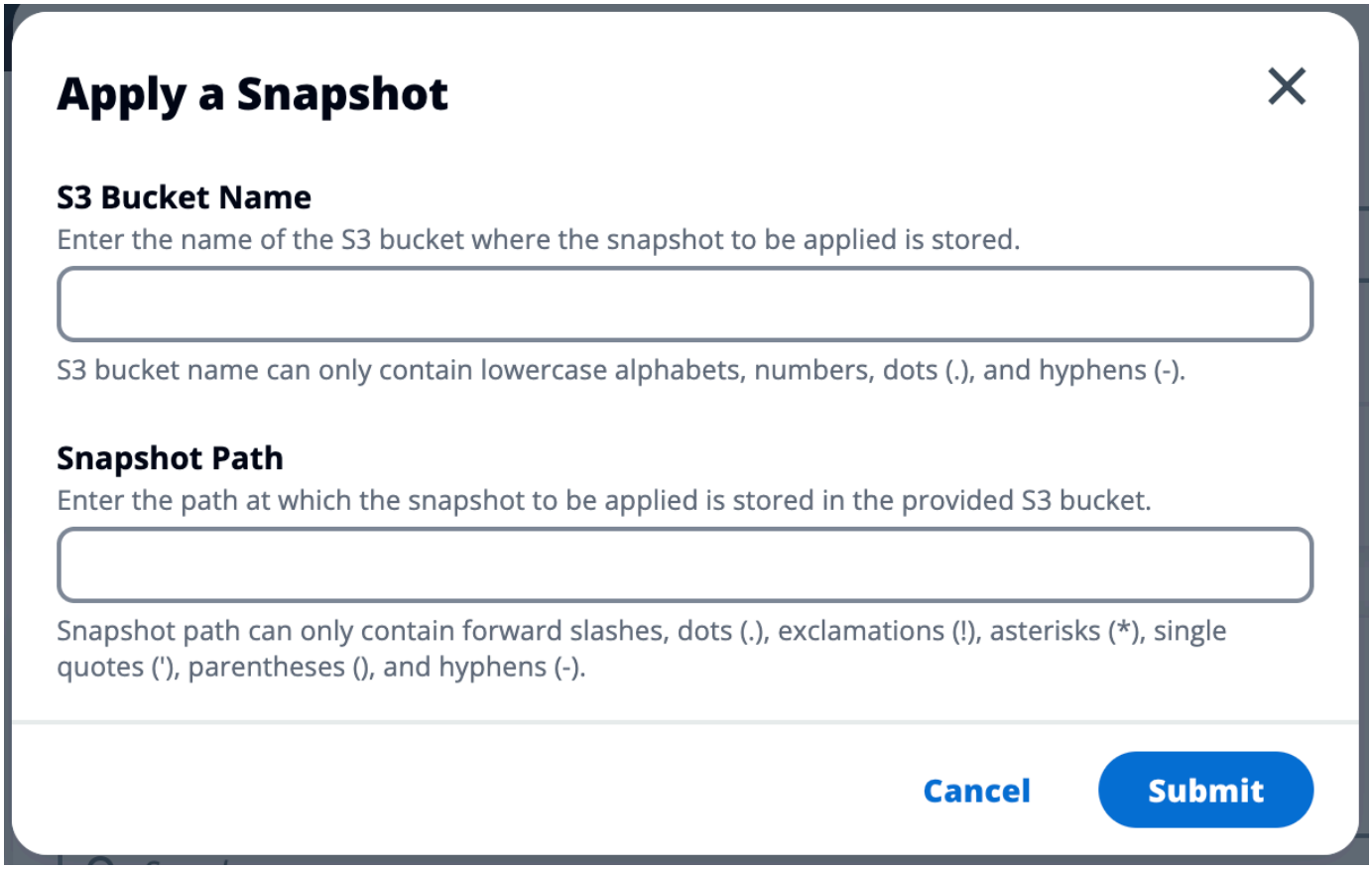
   - AWS_ACCOUNT_ID
   - RES_NOME_DO_AMBIENTE
   - AWS_REGION
   - S3_BUCKET_NAME

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}: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": "*"
        }
    ]
}
```

Para aplicar um instantâneo:

1. Escolha Aplicar instantâneo.
2. Insira o nome do bucket do Amazon S3 que contém o snapshot.
3. Insira o caminho do arquivo para o snapshot dentro do bucket.
4. Selecione Enviar.



5. Depois de cinco a dez minutos, escolha Atualizar na página de gerenciamento do Snapshot para verificar o status.

Configurações de ambiente

As configurações do ambiente exibem detalhes da configuração do produto, como:

- Geral

  Exibe informações como nome de usuário do administrador e e-mail do usuário que provisionou o produto. Você pode editar o título do portal da web e o texto de direitos autorais.

- Provedor de identidades

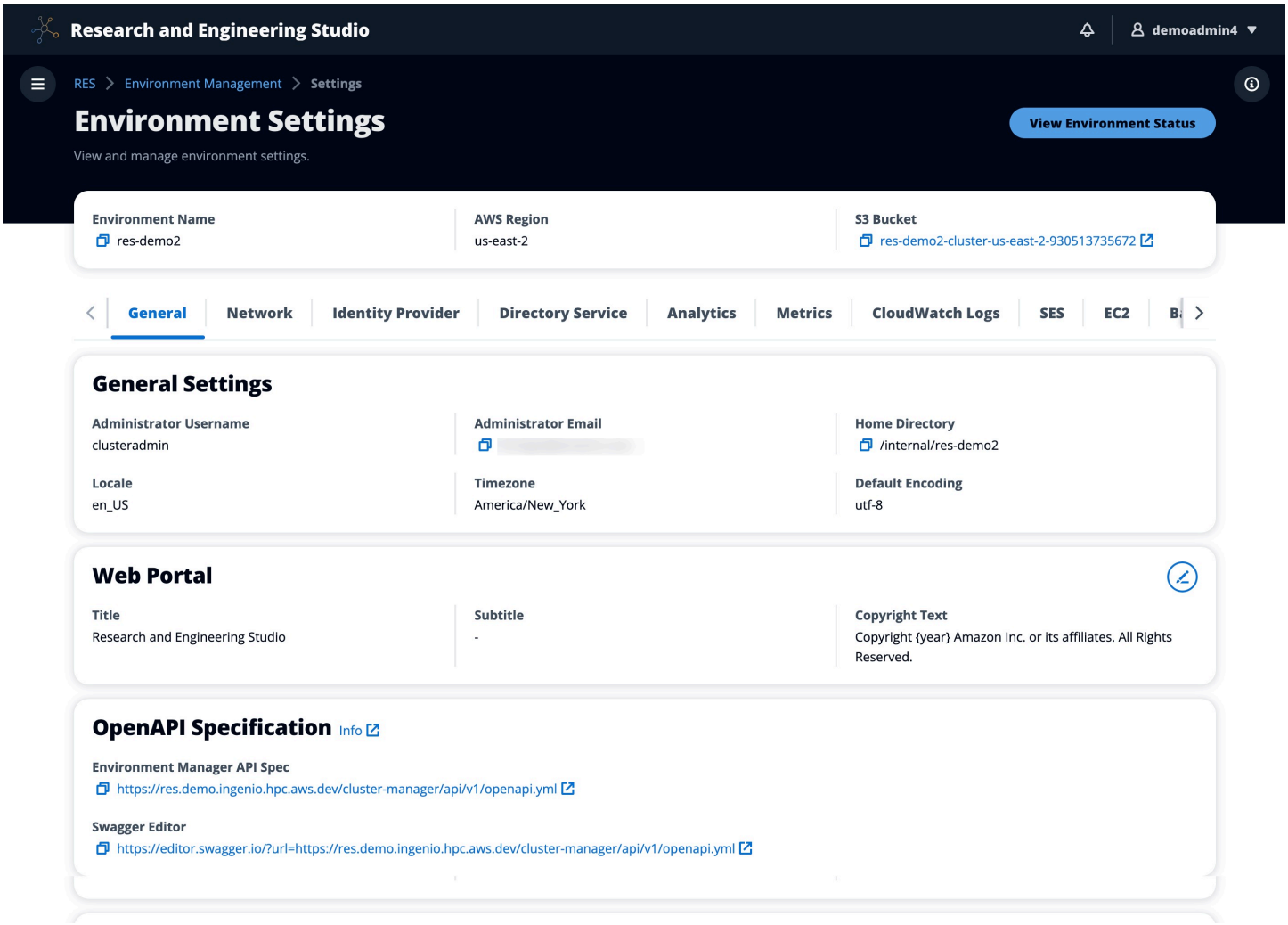
  Exibe informações como o status do Single Sign-On.

- Rede

  Exibe ID da VPC e IDs da lista de prefixos para acesso.

- Directory Service

Exibe as configurações do Active Directory e o ARN do gerenciador de segredos da conta de serviço para nome de usuário e senha.



Gerenciamento de segredos

O Research and Engineering Studio mantém os seguintes segredos usando AWS Secrets Manager. O RES cria segredos automaticamente durante a criação do ambiente. Os segredos inseridos pelo administrador durante a criação do ambiente são inseridos como parâmetros.

Nome de segredo	Descrição	RES gerado	Administrador inserido
<envname>- sso-client-secret	Segredo do cliente OAuth2 de login único para o ambiente	✓	
<envname>- vdc-client-secret	vdc ClientSecret	✓	
<envname>- vdc-client-id	vdc ClientId	✓	
<envname>- vdc-gateway-certificate-private tecla	Chave privada de certificado autoassinada para domínio	✓	
<envname>- vdc-gateway-certificate-certificate	Certificado autoassinado para domínio	✓	
<envname>- cluster-manager-client-secret	gerenciador de clusters ClientSecret	✓	
<envname>- cluster-manager-client-id	gerenciador de clusters ClientId	✓	
<envname>- external-private-key	Chave privada de certificado autoassinada para domínio	✓	
<envname>-certificado externo	Certificado autoassinado para domínio	✓	
<envname>- internal-private-key	Chave privada de certificado autoassinada para domínio	✓	
<envname>-certificado interno	Certificado autoassinado para domínio	✓	

Nome de segredo	Descrição	RES gerado	Administrador inserido
<envname>-serviço de diretório - ServiceAccountUsername			✓
<envname>-serviço de diretório - ServiceAccountPassword			✓

Os seguintes valores secretos de ARN estão contidos na tabela <envname>-cluster-settings no DynamoDB:

Chave	Origem
provedor de identidade.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	stack (pilha)
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	stack (pilha)
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	stack (pilha)
directoryservice.root_username_secret_arn	
vdc.client_secret	stack (pilha)
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	stack (pilha)
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	stack (pilha)
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	

Chave	Origem
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	stack (pilha)
cluster-manager.client_secret	

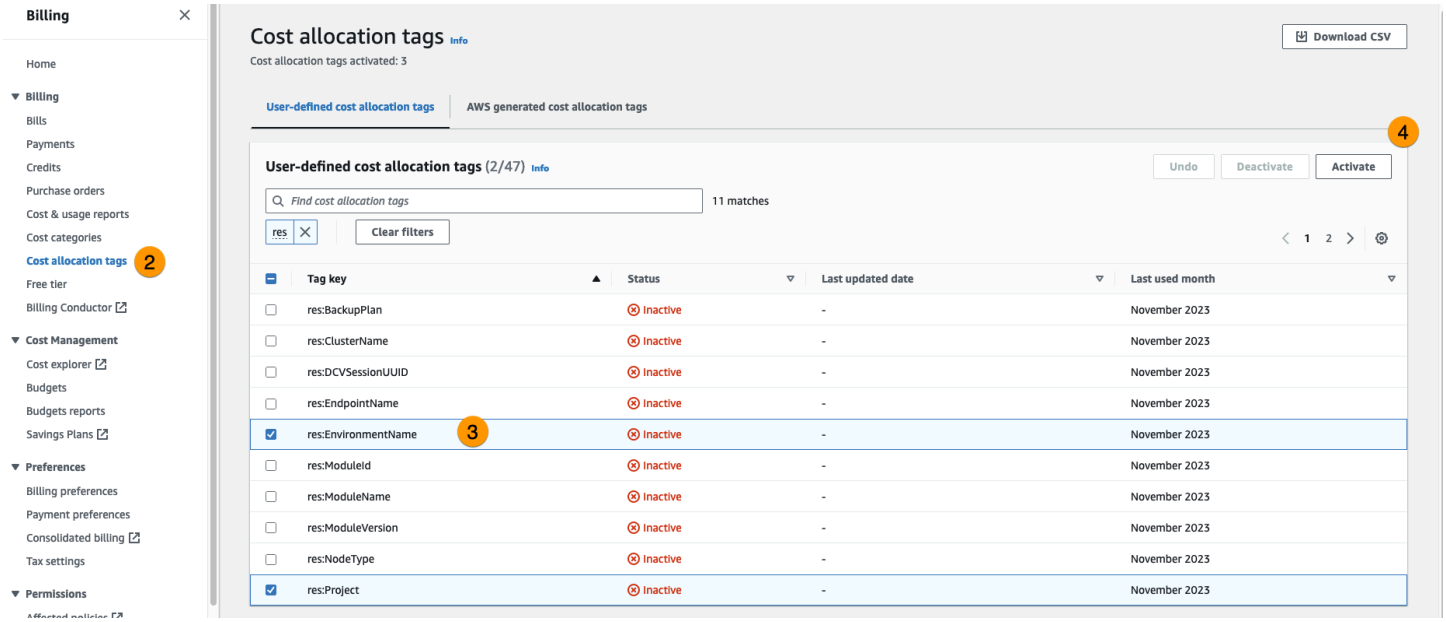
Monitoramento e controle de custos

> **Note**
>
> A associação de projetos do Research and Engineering Studio a não AWS Budgets é suportada no AWS GovCloud (US).

Recomendamos criar um orçamento por meio do AWS Cost Explorer para ajudar a gerenciar os custos. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada um dosthe section called “AWSserviços neste produto”.

Para ajudar no controle de custos, você pode associar projetos de RES aos orçamentos criados em. AWS Budgets Primeiro, você precisará ativar as tags de ambiente dentro das tags de alocação de custos de faturamento.

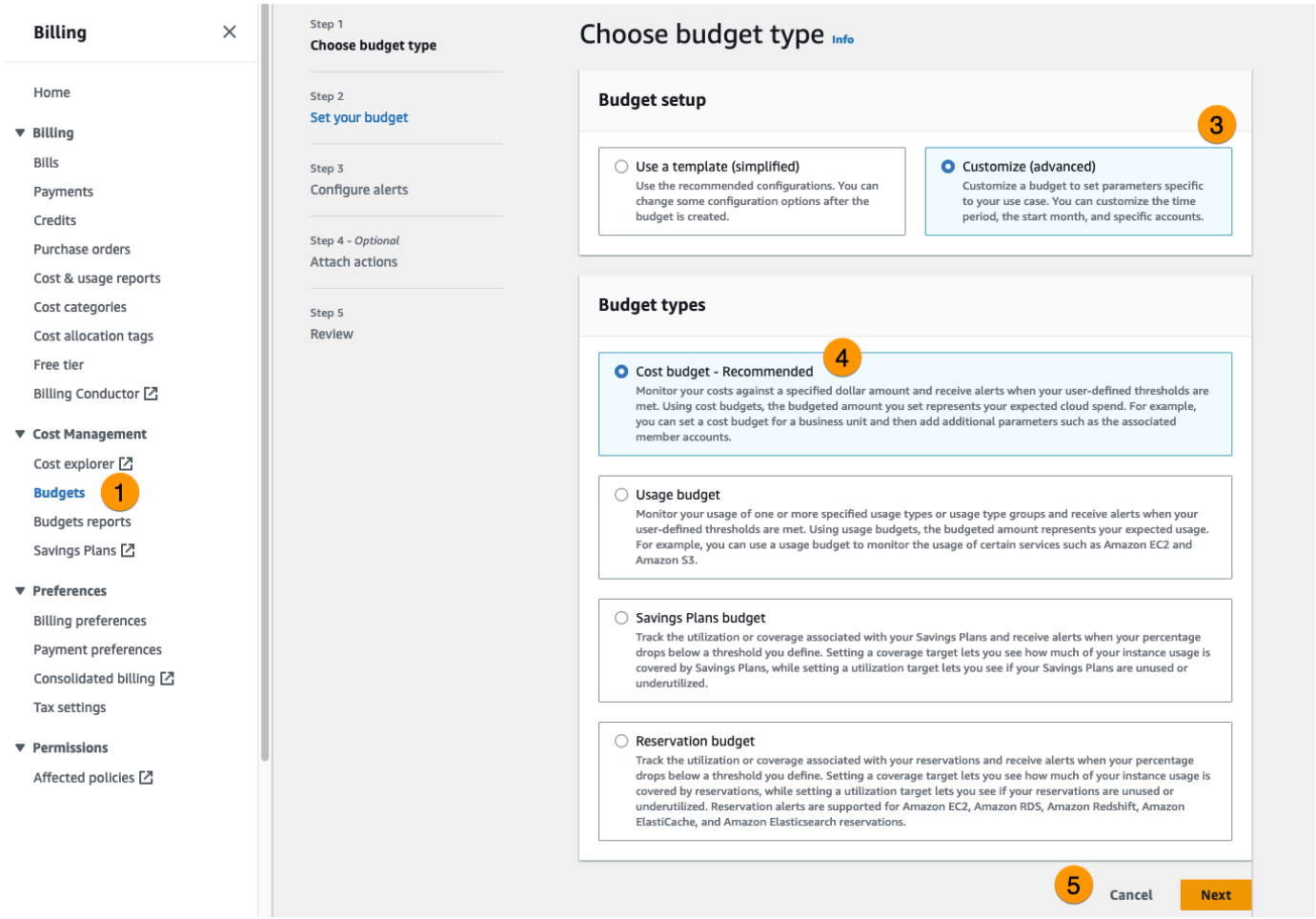
1. Faça login no AWS Management Console e abra o AWS Billing console em https://console.aws.amazon.com/billing/.
2. Escolha Tags de alocação de custos.
3. Pesquise e selecione as `res:Project` `res:EnvironmentName` tags e.
4. Selecione Ativar.



> **Note**
>
> Pode levar até um dia para que as tags RES apareçam após a implantação.

Para criar um orçamento para recursos de RES:

1. No console de faturamento, escolha Orçamentos.
2. Escolha Criar um orçamento.
3. Em Configurar orçamento, escolha Personalizar (avançado).
4. Em Tipos de orçamento, escolha Orçamento de custo - Recomendado.
5. Escolha Próximo.

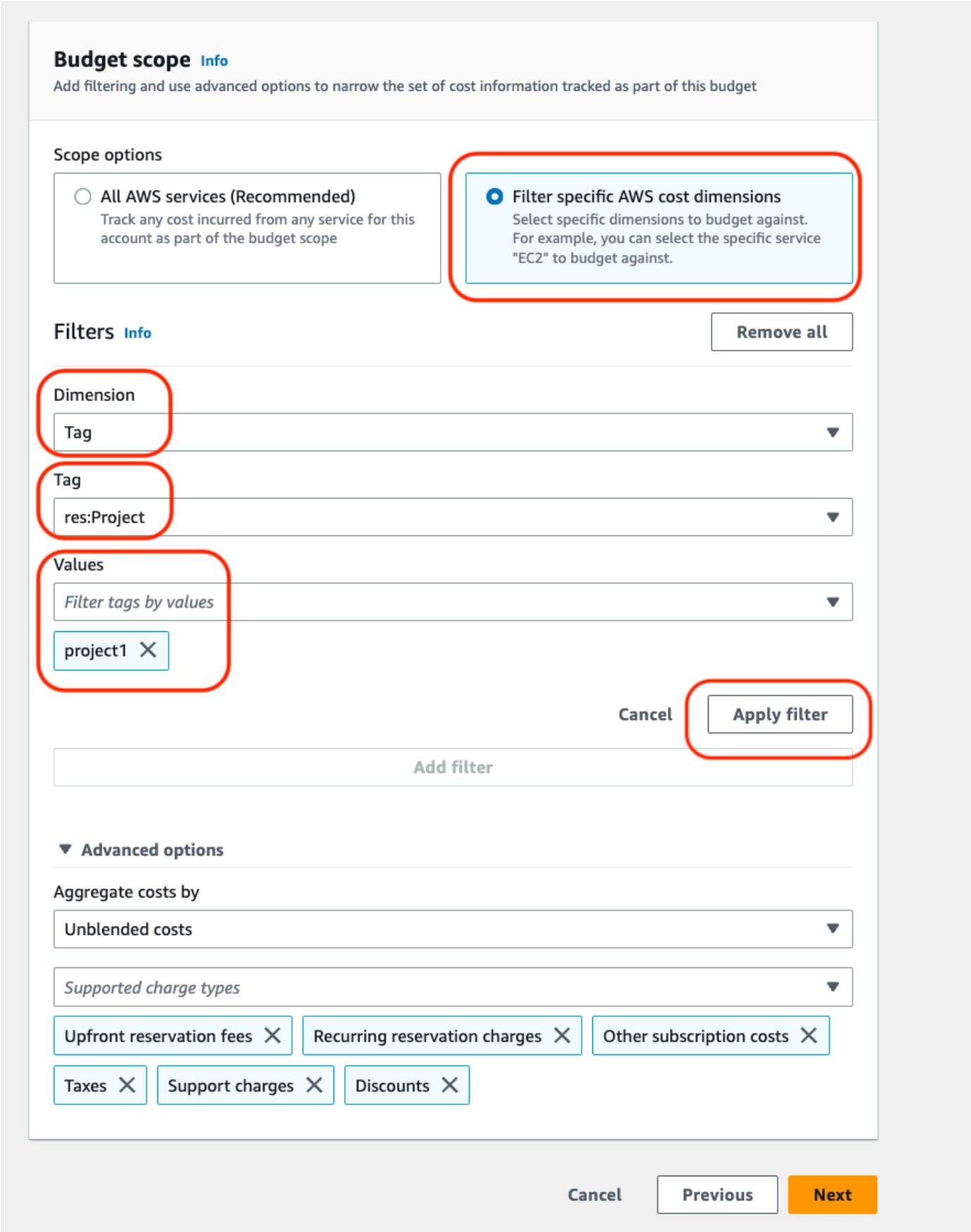


6. Em Detalhes, insira um nome de orçamento significativo para seu orçamento para diferenciá-lo de outros orçamentos em sua conta. Por exemplo, [EnvironmentName] - [ProjectName] - [BudgetName].
7. Em Definir valor do orçamento, insira o valor orçado para seu projeto.
8. Em Escopo do orçamento, escolha Filtrar dimensões AWS de custo específicas.
9. Escolha Adicionar filtro.
10. Em Dimensão, escolha Tag.
11. Em Tag, selecione RES:Project.

> **Note**
>
> Pode levar até dois dias para que as tags e os valores fiquem disponíveis. Você pode criar um orçamento quando o nome do projeto estiver disponível.

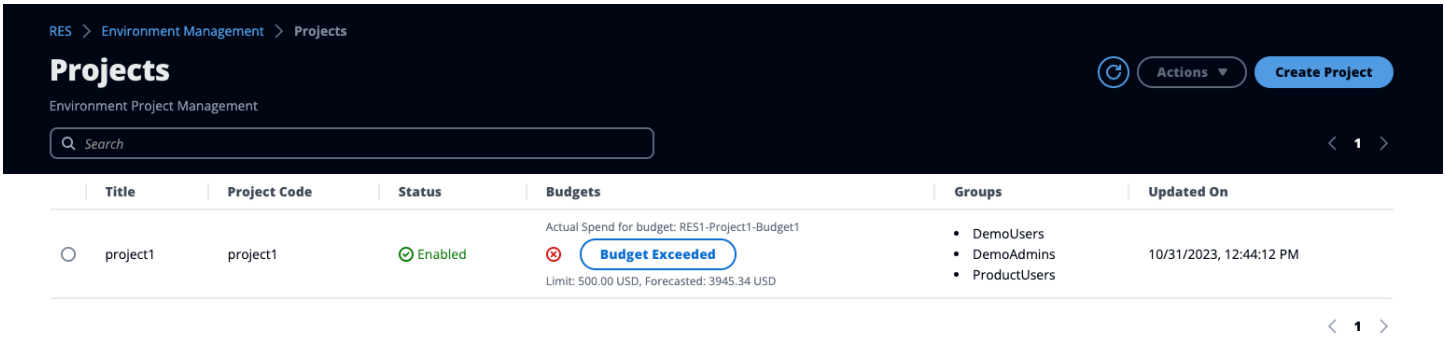
12. Em Valores, selecione o nome do projeto.

13. Escolha Aplicar filtro para anexar o filtro do projeto ao orçamento.
14. Escolha Próximo.


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. (Opcional.) Adicione um limite de alerta.
16. Escolha Próximo.
17. (Opcional.) Se um alerta foi configurado, use Anexar ações para configurar as ações desejadas com o alerta.
18. Escolha Próximo.
19. Revise a configuração do orçamento e confirme se a tag correta foi definida em Parâmetros adicionais de orçamento.
20. Escolha Criar orçamento.

Agora que o orçamento foi criado, você pode habilitar o orçamento para projetos. Para ativar os orçamentos de um projeto, consulte. the section called “Editar um projeto” Os desktops virtuais serão impedidos de serem lançados se o orçamento for excedido. Se o orçamento for excedido durante o lançamento de um desktop, o desktop continuará funcionando.



Se você precisar alterar seu orçamento, retorne ao console para editar o valor do orçamento. Pode levar até quinze minutos para que a alteração entre em vigor no RES. Como alternativa, você pode editar um projeto para desativar um orçamento.

Permissões

	Membro do projeto	Proprietário do projeto	Administrador global	Escopo
Adicionar usuários como membro do		X	X	Proprietário do projeto: projetos que eles possuem

	Membro do projeto	Proprietário do projeto	Administrador global	Escopo
projeto/proprietário do projeto				Administrador global: qualquer projeto
Adicionar grupos como membro do projeto/proprietário do projeto		X	X	Proprietário do projeto: projetos que eles possuem Administrador global: qualquer projeto
Remoção de usuários		X	X	Proprietário do projeto: projetos que eles possuem Administrador global: qualquer projeto
Remover grupos		X	X	Proprietário do projeto: projetos que eles possuem Administrador global: qualquer projeto

	Membro do projeto	Proprietário do projeto	Administrador global	Escopo
Iniciar/interromper instâncias de VDI	X	X	X	Membro do projeto/proprietário do projeto: instâncias de VDI que eles possuem quando fazem parte de um projeto. Administrador global: qualquer instância de VDI.

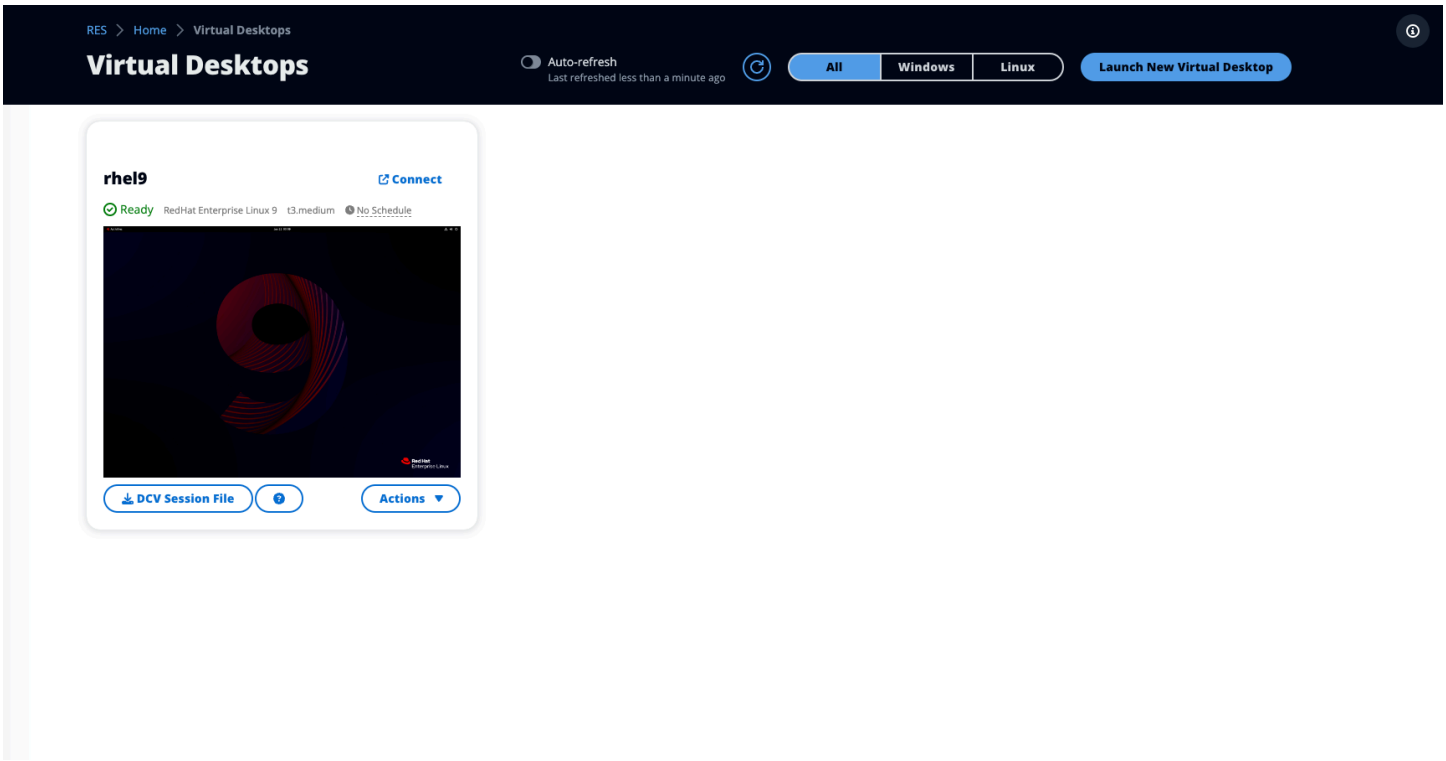
Use o produto

Esta seção oferece orientação aos usuários sobre o uso de desktops virtuais para colaborar com outros usuários.

Tópicos

Áreas de trabalho virtuais

O módulo de interface de desktop virtual (VDI) permite que os usuários criem e gerenciem desktops virtuais Windows ou Linux em. AWS Os usuários podem iniciar instâncias do Amazon EC2 com suas ferramentas e aplicativos favoritos pré-instalados e configurados.



Sistemas operacionais compatíveis

> **Note**
>
> Atualmente, o CentOS 7 está programado para chegar end-of-life em 30/06/2024. A versão 2024.06 do Research and Engineering Studio será a última versão a oferecer suporte ao CentOS 7.

Atualmente, o RES suporta o lançamento de desktops virtuais usando os seguintes sistemas operacionais:

- Amazon Linux 2 (x86 e ARM64)
- CentOS 7 (x86 e ARM64)
- RHEL 7 (x86), 8 (x86) e 9 (x86)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Inicie um novo desktop

1. No menu, escolha Meus desktops virtuais.
2. Escolha Iniciar nova área de trabalho virtual.
3. Insira os detalhes do seu novo desktop.
4. Selecione Enviar.

Um novo cartão com as informações da área de trabalho aparece instantaneamente e sua área de trabalho estará pronta para uso em 10 a 15 minutos. O tempo de inicialização depende da imagem selecionada. O RES detecta instâncias de GPU e instala os drivers relevantes.

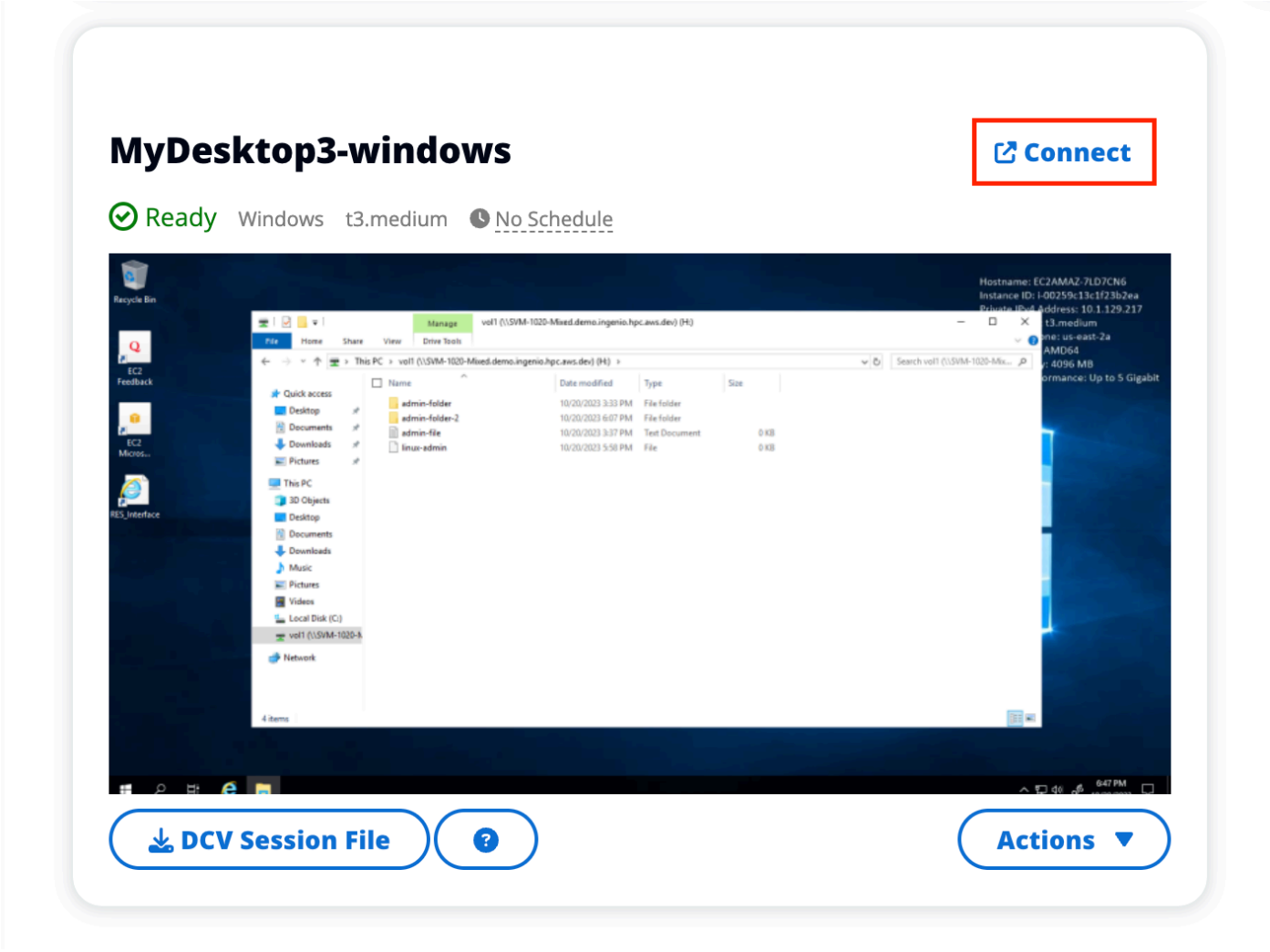
Acesse sua área de trabalho

Para acessar uma área de trabalho virtual, escolha a placa para a área de trabalho e conecte-se usando o cliente web ou DCV.

Web connection

Acessar sua área de trabalho por meio do navegador da web é o método mais fácil de conexão.

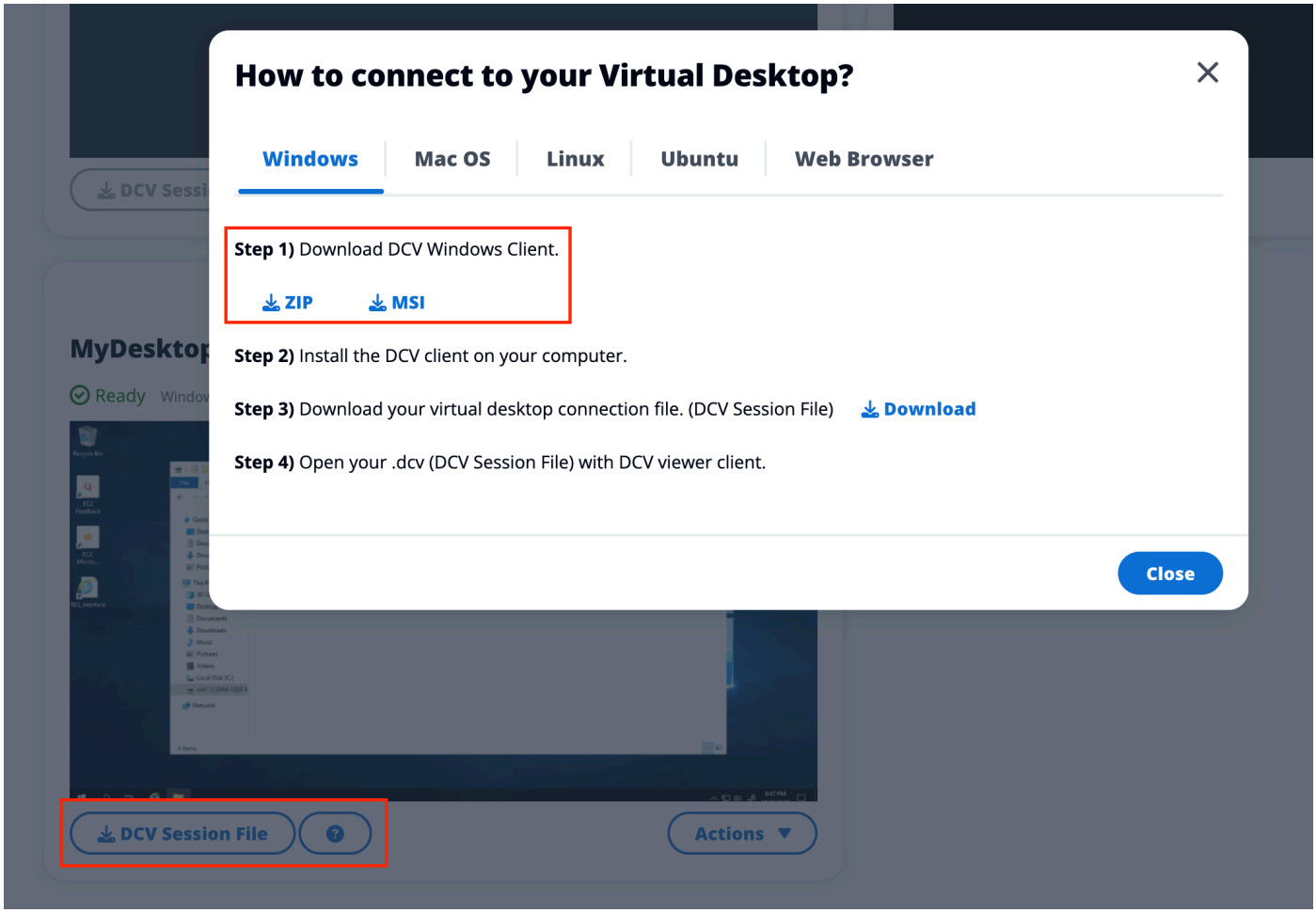
- Escolha Connect ou escolha a miniatura para acessar sua área de trabalho diretamente pelo navegador.



DCV connection

Acessar seu desktop por meio de um cliente DCV oferece o melhor desempenho. Para acessar via DCV:

1. Escolha Arquivo de sessão DCV para baixar o. `dcv`arquivo. Você precisará de um cliente DCV instalado em seu sistema.
2. Para obter instruções de instalação, escolha a opção? ícone.



Controle o estado do seu desktop

Para controlar o estado da sua área de trabalho:

1. Escolha Ações.
2. Escolha o estado da área de trabalho virtual. Você tem quatro estados para escolher:

   - Interromper

     Uma sessão interrompida não sofrerá perda de dados e você poderá reiniciá-la a qualquer momento.

   - Reinicializar

     Reinicializa a sessão atual.

   - Encerrar

Encerra permanentemente uma sessão. O encerramento de uma sessão pode causar perda de dados se você estiver usando armazenamento temporário. Você deve fazer backup de seus dados no sistema de arquivos RES antes de finalizar.

- Hibernar

  O estado da sua área de trabalho será salvo na memória. Quando você reinicia a área de trabalho, seus aplicativos são retomados, mas todas as conexões remotas podem ser perdidas. Nem todas as instâncias oferecem suporte à hibernação, e a opção só está disponível se tiver sido ativada durante a criação da instância. Para verificar se sua instância é compatível com esse estado, consulte Pré-requisitos de hibernação.

Modificar uma área de trabalho virtual

Você pode atualizar o hardware da sua área de trabalho virtual ou alterar o nome da sessão.

1. Antes de fazer alterações no tamanho da instância, você deve interromper a sessão:

   a. Escolha Ações.

   b. Escolha o estado da área de trabalho virtual.

   c. Escolha Parar.

   > **Note**
   >
   > Você não pode atualizar o tamanho da área de trabalho para sessões em hibernação.

2. Depois de confirmar que a área de trabalho foi interrompida, escolha Ações e, em seguida, selecione Atualizar sessão.
3. Altere o nome da sessão ou escolha o tamanho da área de trabalho que você gostaria.
4. Selecione Enviar.
5. Depois que suas instâncias forem atualizadas, reinicie seu desktop:

   a. Escolha Ações.

   b. Escolha o estado da área de trabalho virtual.

   c. Escolha Iniciar.

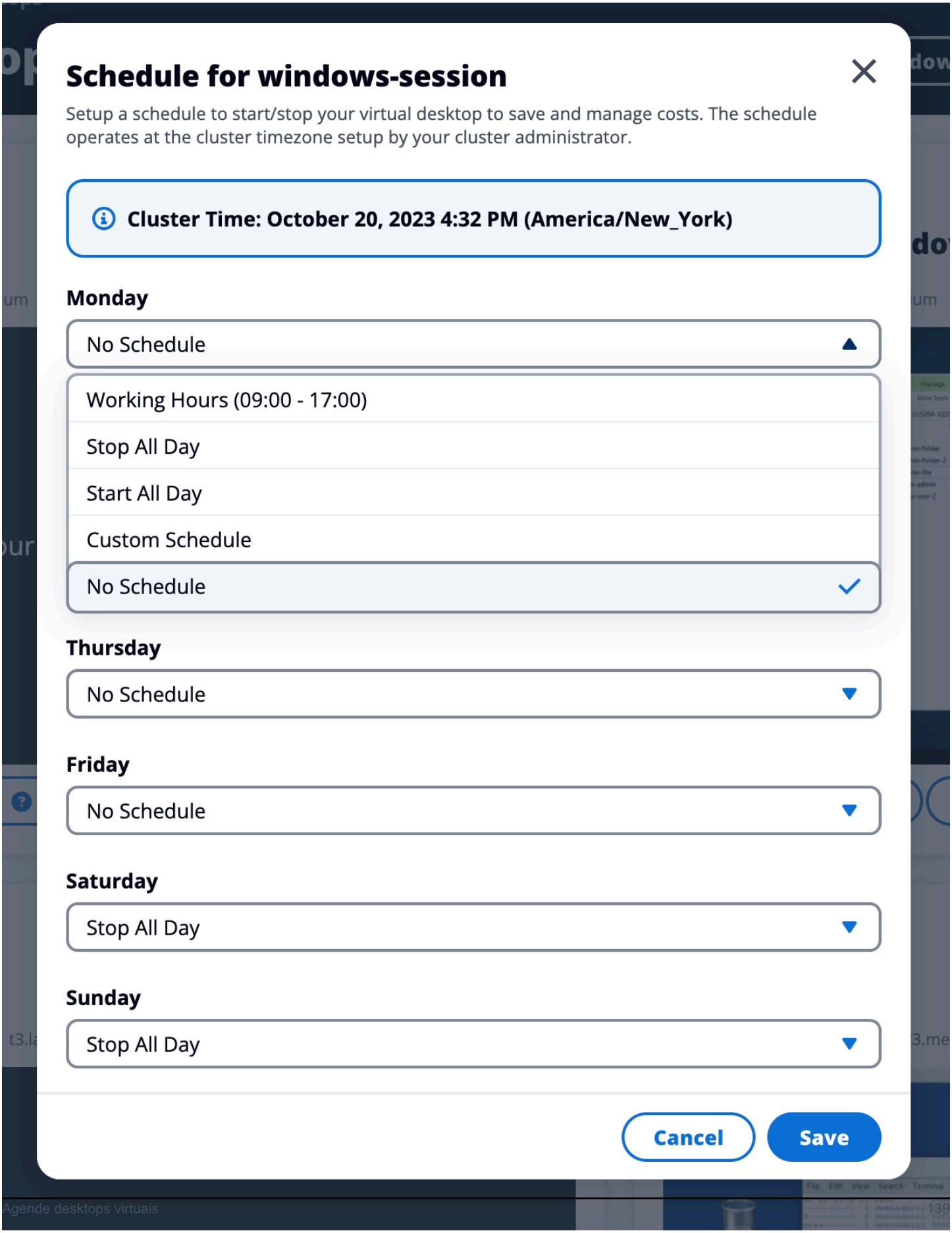
Recuperar informações da sessão

1. Escolha Ações.
2. Escolha Mostrar informações.

Agende desktops virtuais

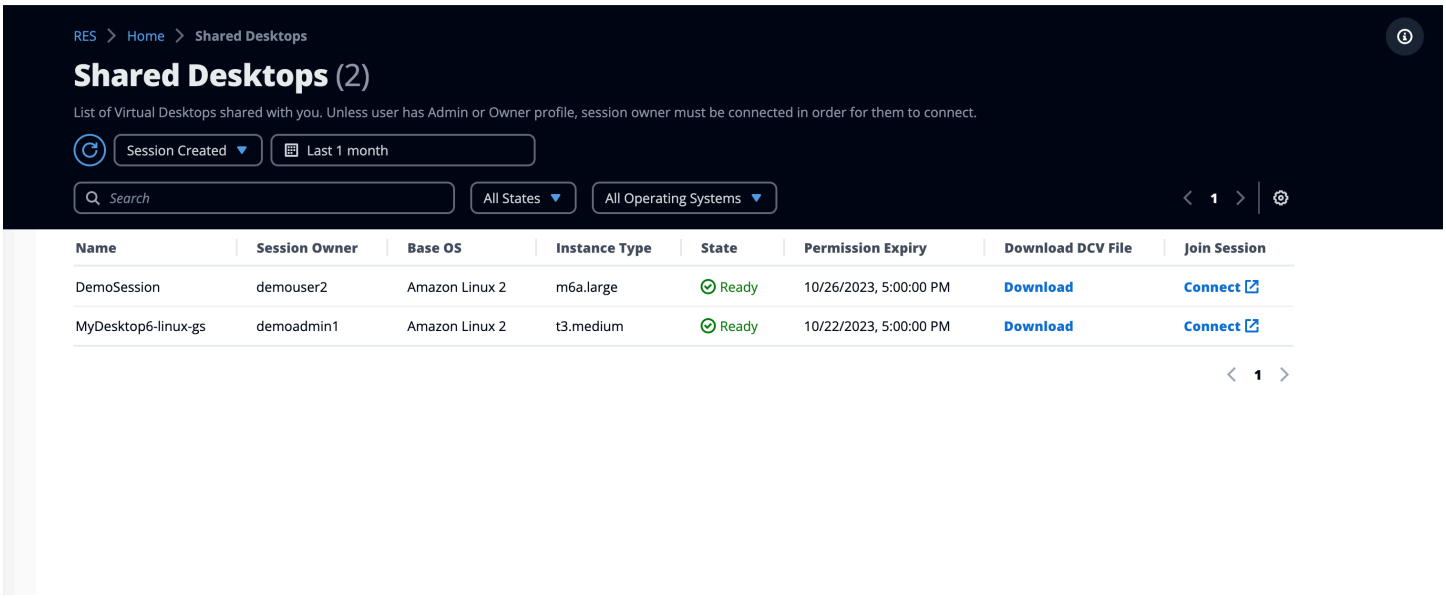
Por padrão, os desktops virtuais não têm uma agenda e permanecerão ativos até que você interrompa ou encerre a sessão. Os desktops também param se estiverem ociosos para evitar paradas acidentais. Um estado ocioso é determinado pela ausência de conexão ativa e pelo uso da CPU abaixo de 15% por pelo menos 15 minutos. Você pode configurar um agendamento para iniciar e parar automaticamente sua área de trabalho.

1. Escolha Ações.
2. Escolha Schedule (Programação)
3. Defina sua programação para cada dia.
4. Escolha Salvar.


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

Desktops compartilhados

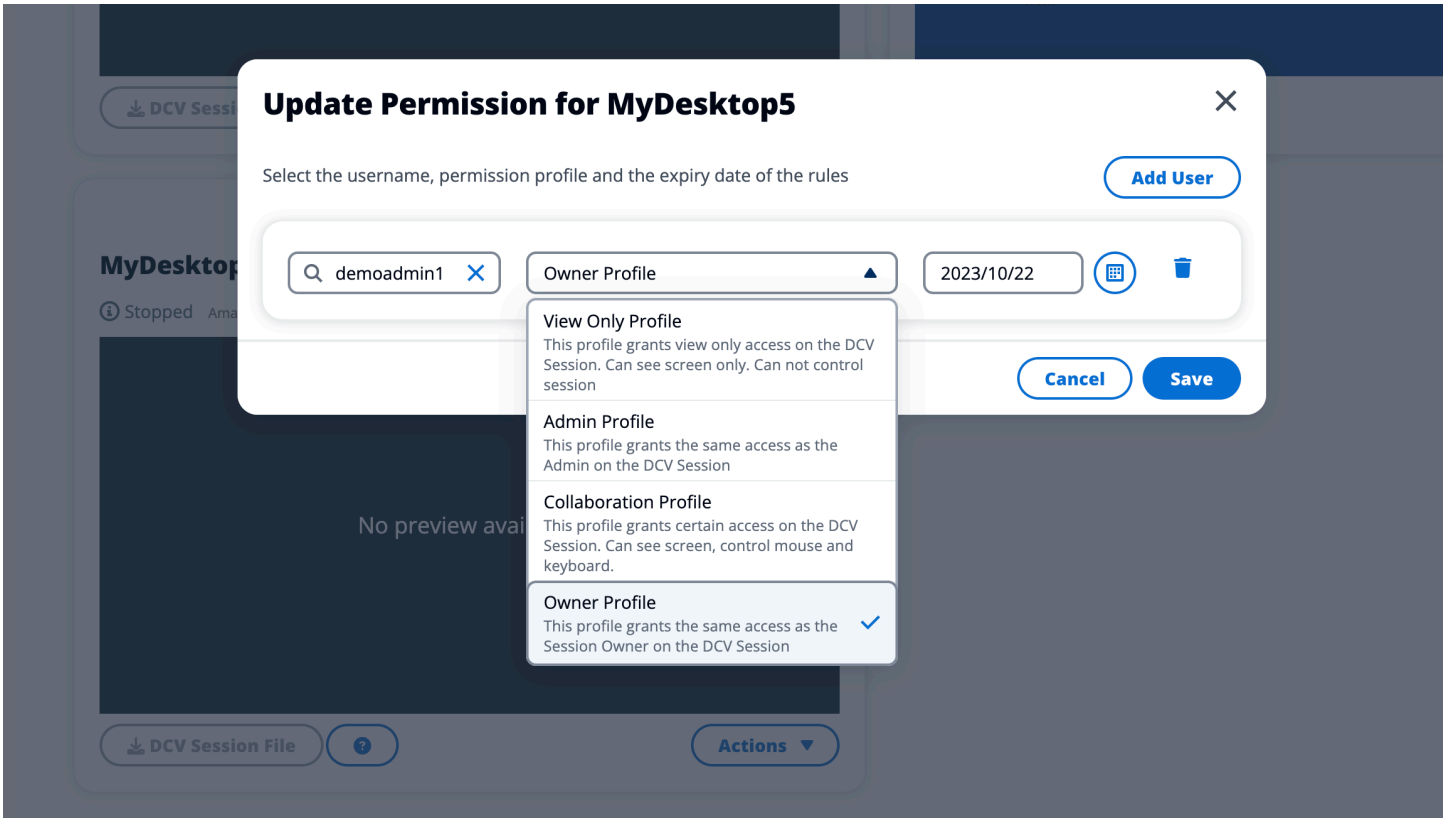
Em áreas de trabalho compartilhadas, você pode ver as áreas de trabalho que foram compartilhadas com você. Para se conectar a um desktop, o proprietário da sessão também deve estar conectado, a menos que você seja administrador ou proprietário.



Ao compartilhar uma sessão, você pode configurar permissões para seus colaboradores. Por exemplo, você pode dar acesso somente de leitura a um colega de equipe com quem você está colaborando.

Compartilhar uma área de trabalho

1. Na sua sessão de desktop, escolha Ações.
2. Escolha Permissões da sessão.
3. Escolha o usuário e o nível de permissão. Você também pode definir um prazo de expiração.
4. Escolha Salvar.



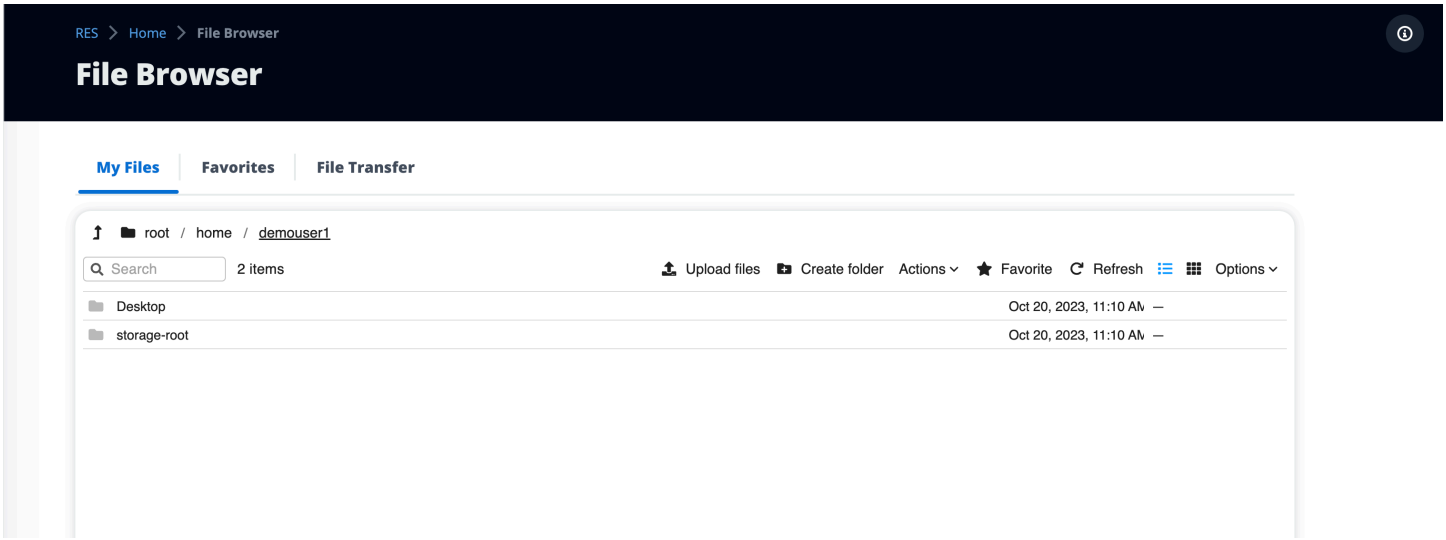
Para obter mais informações sobre permissões, consultethe section called “Perfis de permissão”.

Acesse uma área de trabalho compartilhada

Em Desktops compartilhados, você pode visualizar os desktops compartilhados com você e se conectar a uma instância. Você pode entrar por meio de um navegador da web ou DCV. Para se conectar, siga as instruções emthe section called “Acesse sua área de trabalho”.

Navegador de arquivos

O navegador de arquivos permite que você acesse sistemas de arquivos por meio do portal da web. Você pode gerenciar todos os arquivos disponíveis que você tem permissão para acessar no sistema de arquivos subjacente. O armazenamento de back-end (Amazon EFS) está disponível para todos os nós Linux. Para nós Linux e Windows, o FSx for ONTAP está disponível. Atualizar arquivos em sua área de trabalho virtual é o mesmo que atualizar um arquivo por meio do terminal ou do navegador de arquivos baseado na web.



Carregar arquivo (s)

1. Escolha Carregar um arquivo.
2. Solte os arquivos ou procure os arquivos a serem carregados.
3. Escolha Carregar (n) arquivos.

Excluir arquivo (s)

1. Selecione o (s) arquivo (s) que você deseja excluir.
2. Escolha Ações.
3. Escolha Excluir arquivos.

Como alternativa, você também pode clicar com o botão direito do mouse em qualquer arquivo ou pasta e escolher Excluir arquivos.

Gerenciar favoritos

Para fixar arquivos e pastas importantes, você pode adicioná-los aos Favoritos.

1. Selecione um arquivo ou pasta.
2. Escolha Favorito.

Como alternativa, você pode clicar com o botão direito do mouse em qualquer arquivo ou pasta e escolher Favorito.

> **Note**
>
> Os favoritos são armazenados no navegador local. Se você alterar o navegador ou limpar o cache, precisará fixar novamente seus favoritos.

Editar arquivos

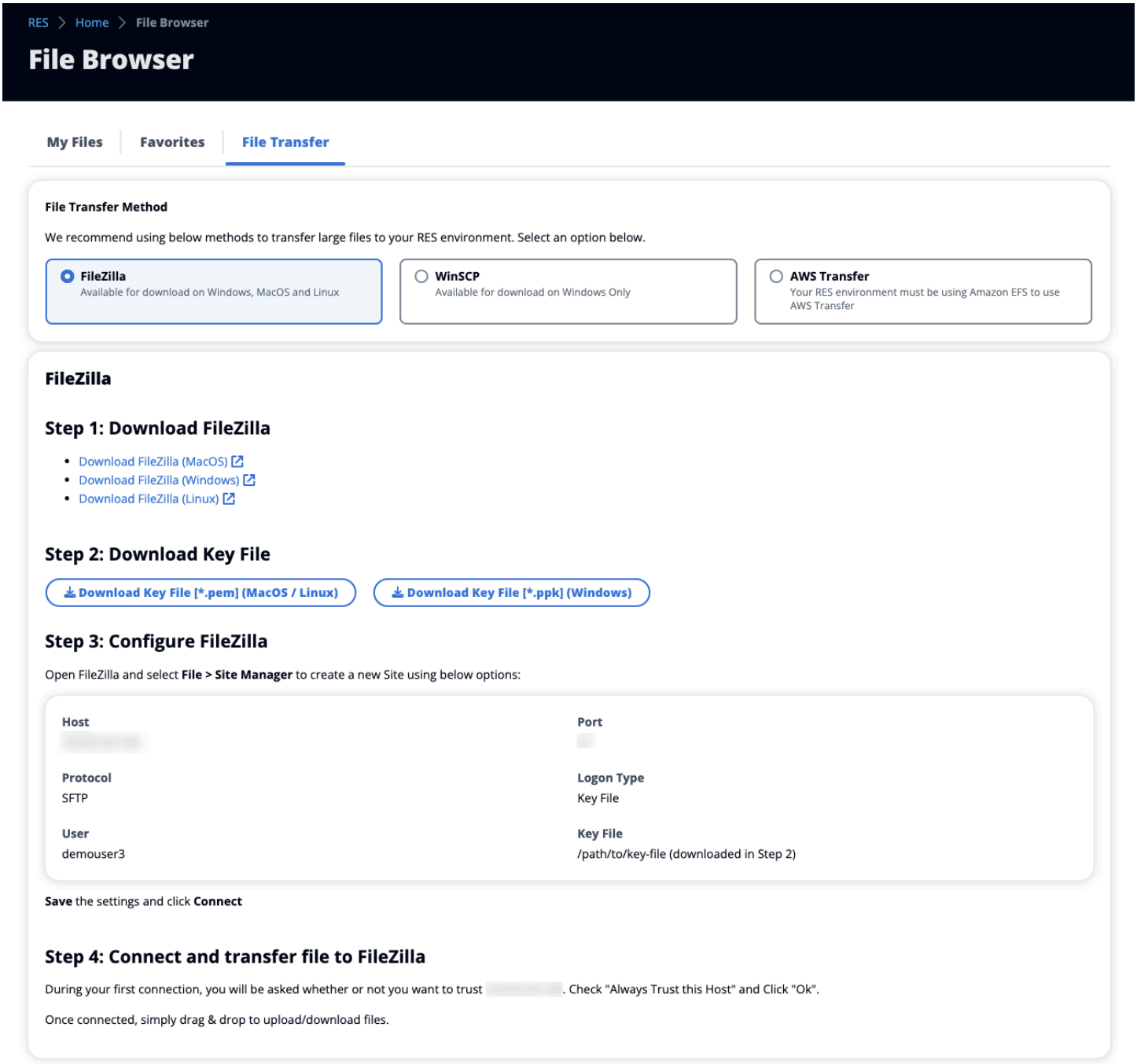
Você pode editar o conteúdo de arquivos baseados em texto no portal da web.

1. Escolha o arquivo que você deseja atualizar. Um modal será aberto com o conteúdo do arquivo.
2. Faça suas atualizações e escolha Salvar.

Transferir arquivos

Use a Transferência de arquivos para usar aplicativos externos de transferência de arquivos para transferir arquivos. Você pode selecionar um dos seguintes aplicativos e seguir as instruções na tela para transferir arquivos.

- FileZilla (Windows, macOS, Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)



Acesso a SSH

Para usar o SSH para acessar o bastion host:

1. No menu RES, escolha Acesso SSH.
2. Siga as instruções na tela para usar SSH ou PuTTY para acesso.

Solução de problemas

Este documento contém informações sobre como monitorar o sistema e como solucionar problemas específicos que possam ocorrer. Se você não conseguir encontrar a solução para um problema, talvez encontre tópicos adicionais de solução de problemas em GitHub.

Tópicos

Problemas de instalação

Tópicos

AWS CloudFormation falha ao criar a pilha com a mensagem “mensagem de falha WaitCondition recebida”. Erro: Estados. TaskFailed”

Para identificar o problema, examine o grupo de CloudWatch registros da Amazon chamado`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. Se houver vários grupos de registros com o mesmo nome, examine o primeiro disponível. Uma mensagem de erro nos registros fornecerá mais informações sobre o problema.

> **Note**
>
> Confirme se os valores dos parâmetros não têm espaços.

Notificação por e-mail não recebida após a criação bem-sucedida das AWS CloudFormation pilhas

Se um convite por e-mail não foi recebido após a AWS CloudFormation criação bem-sucedida, verifique o seguinte:

1. Confirme se o parâmetro do endereço de e-mail foi inserido corretamente.

   Se o endereço de e-mail estiver incorreto ou não puder ser acessado, exclua e reimplante o ambiente do Research and Engineering Studio.
2. Verifique o console do Amazon EC2 para obter evidências de instâncias cíclicas.

   Se houver instâncias do Amazon EC2 com o `<envname>` prefixo aparecendo como encerrado e depois forem substituídas por uma nova instância, pode haver um problema com a configuração da rede ou do Active Directory.
3. Se você implantou as receitas de computação de AWS alto desempenho para criar seus recursos externos, confirme se a VPC, as sub-redes públicas e privadas e outros parâmetros selecionados foram criados pela pilha.

   Se algum dos parâmetros estiver incorreto, talvez seja necessário excluir e reimplantar o ambiente RES. Para ter mais informações, consulte Desinstalar o produto.
4. Se você implantou o produto com seus próprios recursos externos, confirme se a rede e o Active Directory correspondem à configuração esperada.

   Confirmar que as instâncias de infraestrutura ingressaram com sucesso no Active Directory é fundamental. Experimente as etapas the section called “Ciclismo de instâncias ou controlador vdc em estado de falha” para resolver o problema.

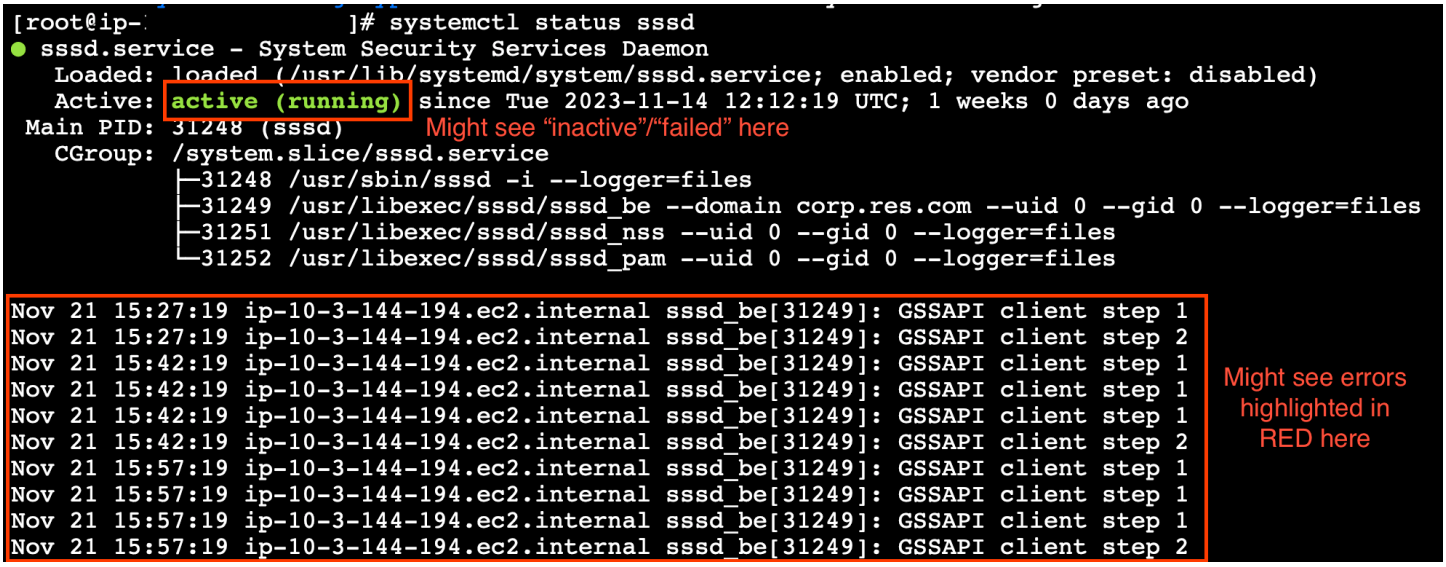
Ciclismo de instâncias ou controlador vdc em estado de falha

A causa mais provável desse problema é a incapacidade de os recursos se conectarem ou ingressarem no Active Directory.

Para verificar o problema:

1. Na linha de comando, inicie uma sessão com SSM na instância em execução do controlador vdc.
2. Executar `sudo su -`.
3. Executar `systemctl status sssd`.

Se o status for inativo, falhar ou você ver erros nos registros, a instância não conseguiu ingressar no Active Directory.



Registro de erros do SSM

Para resolver o problema:

- Na mesma instância da linha de comando, execute `cat /root/bootstrap/logs/userdata.log` para investigar os registros.

O problema pode ser uma das três possíveis causas principais.

Causa raiz 1: detalhes incorretos da conexão ldap inseridos

Revise os registros. Se você ver o seguinte repetido várias vezes, a instância não conseguiu ingressar no 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. Verifique se os valores dos parâmetros a seguir foram inseridos corretamente durante a criação da pilha RES.
   - directoryservice.ldap_connection_uri
   - serviço de diretório.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - nome do serviço de diretório.name
2. Atualize todos os valores incorretos na tabela do DynamoDB. A tabela é encontrada no console do DynamoDB em Tabelas. O nome da tabela deve ser**`[stack name]`**`.cluster-settings`.
3. Depois de atualizar a tabela, exclua o cluster-manager e o vdc-controller que estão executando as instâncias do ambiente no momento. O Auto Scaling iniciará novas instâncias usando os valores mais recentes da tabela do DynamoDB.

Causa raiz 2: nome de ServiceAccount usuário incorreto inserido

Se os registros retornarem`Insufficient permissions to modify computer account`, o ServiceAccount nome inserido durante a criação da pilha pode estar incorreto.

1. No AWS console, abra o Secrets Manager.
2. Pesquise por `directoryserviceServiceAccountUsername`. O segredo deveria ser**`[stack name]`**`-directoryservice-ServiceAccountUsername`.
3. Abra o segredo para ver a página de detalhes. Em Valor secreto, escolha Recuperar valor secreto e escolha Texto sem formatação.

4. Se o valor tiver sido atualizado, exclua as instâncias cluster-manager e vdc-controller do ambiente atualmente em execução. O escalonamento automático iniciará novas instâncias usando o valor mais recente do Secrets Manager.

Causa raiz 3: ServiceAccount senha incorreta inserida

Se os registros forem exibidos`Invalid credentials`, a ServiceAccount senha inserida durante a criação da pilha pode estar incorreta.

1. No AWS console, abra o Secrets Manager.
2. Pesquise por `directoryserviceServiceAccountPassword`. O segredo deveria ser**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
3. Abra o segredo para ver a página de detalhes. Em Valor secreto, escolha Recuperar valor secreto e escolha Texto sem formatação.
4. Se você esqueceu a senha ou não tem certeza se a senha digitada está correta, você pode redefinir a senha no Active Directory e no Secrets Manager.
    a. Para redefinir a senha em AWS Managed Microsoft AD:
        i. Abra o AWS console e vá para AWS Directory Service.
        ii. Selecione o ID do diretório para seu diretório RES e escolha Ações.
        iii. Escolha Redefinir senha de usuário.
        iv. Insira o ServiceAccount nome de usuário.
        v. Insira uma nova senha e escolha Redefinir senha.
    b. Para redefinir a senha no Secrets Manager:
        i. Abra o AWS console e vá para o Secrets Manager.
        ii. Pesquise por `directoryserviceServiceAccountPassword`. O segredo deveria ser**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
        iii. Abra o segredo para ver a página de detalhes. Em Valor secreto, escolha Recuperar valor secreto e escolha Texto sem formatação.
        iv. Selecione a opção Editar.
        v. Defina uma nova senha para o ServiceAccount usuário e escolha Salvar.

5. Se o valor tiver sido atualizado, exclua as instâncias cluster-manager e vdc-controller do ambiente atualmente em execução. O Auto Scaling iniciará novas instâncias usando o valor mais recente.

Falha ao excluir a CloudFormation pilha de ambiente devido a um erro no objeto dependente

Se a exclusão da **`[env-name]`**`-vdc` CloudFormation pilha falhar devido a um erro de objeto dependente, como o`vdcdcvhostsecuritygroup`, isso pode ser devido a uma instância do Amazon EC2 que foi executada em uma sub-rede ou grupo de segurança criado pelo RES usando o console. AWS

Para resolver o problema, localize e encerre todas as instâncias do Amazon EC2 iniciadas dessa maneira. Em seguida, você pode retomar a exclusão do ambiente.

Erro encontrado no parâmetro de bloco CIDR durante a criação do ambiente

Ao criar um ambiente, aparece um erro para o parâmetro do bloco CIDR com um status de resposta de [FALHOU].

Exemplo de erro:

```
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.
```

Para resolver o problema, o formato esperado é x.x.x.0/24 ou x.x.x.0/32.

CloudFormation falha na criação da pilha durante a criação do ambiente

A criação de um ambiente envolve uma série de operações de criação de recursos. Em algumas regiões, pode ocorrer um problema de capacidade que faz com que a criação da CloudFormation pilha falhe.

Se isso ocorrer, exclua o ambiente e repita a criação. Como alternativa, você pode tentar novamente a criação em uma região diferente.

A criação da pilha de recursos externos (demo) falha com AdDomainAdminNode CREATE_FAILED

Se a criação da pilha do ambiente de demonstração falhar com o seguinte erro, pode ser devido à ocorrência inesperada de patches do Amazon EC2 durante o provisionamento após o lançamento da instância.

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

Para determinar a causa da falha:

1. No SSM State Manager, verifique se o patch está configurado e se está configurado para todas as instâncias.
2. No histórico de execução do RunCommand SSM/Automation, verifique se a execução de um documento SSM relacionado à correção coincide com o lançamento de uma instância.
3. Nos arquivos de log das instâncias do Amazon EC2 do ambiente, revise o registro da instância local para determinar se a instância foi reinicializada durante o provisionamento.

Se o problema foi causado por uma correção, adie a correção das instâncias RES pelo menos 15 minutos após o lançamento.

Problemas de gerenciamento de identidade

A maioria dos problemas com o login único (SSO) e o gerenciamento de identidade ocorre devido à configuração incorreta. Para obter informações sobre como definir sua configuração de SSO, consulte:

- the section called “Configurando o SSO com o IAM Identity Center”
- the section called “Configurando seu provedor de identidade para login único (SSO)”

Para solucionar outros problemas relacionados ao gerenciamento de identidades, consulte os seguintes tópicos de solução de problemas:

Tópicos

- Ao fazer login no ambiente, eu volto imediatamente para a página de login

Ao fazer login no ambiente, eu volto imediatamente para a página de login

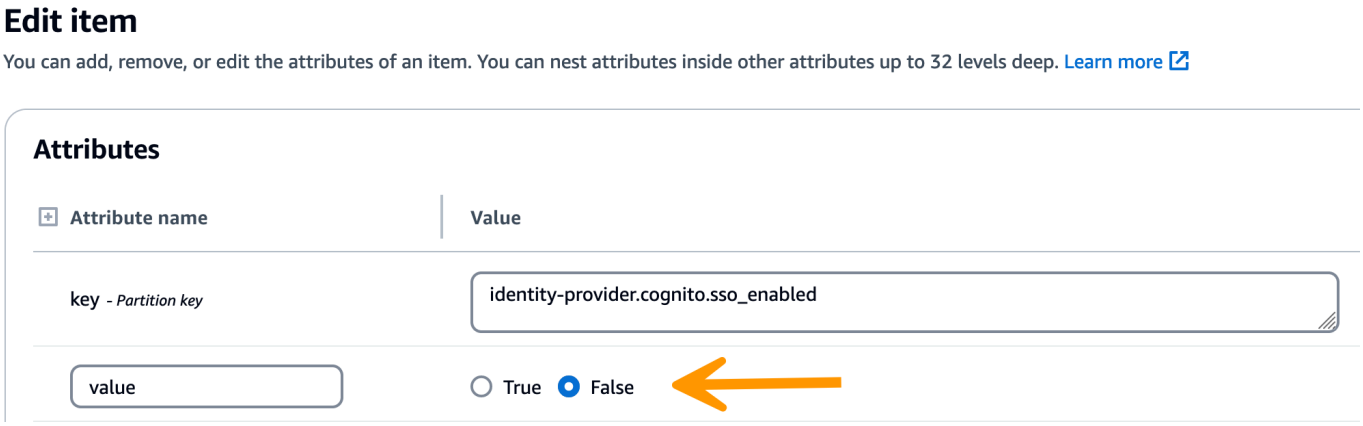
Esse problema ocorre quando sua integração de SSO está configurada incorretamente. Para determinar o problema, verifique os registros da instância do controlador e verifique se há erros nas configurações.

Para verificar os registros:

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Em Grupos de registros, encontre o grupo chamado`/<environment-name>/cluster-manager`.
3. Abra o grupo de registros para pesquisar erros nos fluxos de registros.

Para verificar as configurações:

1. Abra o console do DynamoDB em https://console.aws.amazon.com/dynamodb/.
2. Em Tabelas, encontre a tabela chamada`<environment-name>.cluster-settings`.
3. Abra a tabela e escolha Explorar itens da tabela.
4. Expanda a seção de filtros e insira as seguintes variáveis:
   - Nome do atributo — chave
   - Condição — contém
   - Valor — sso
5. Escolha Executar.
6. Na string retornada, verifique se os valores de configuração do SSO estão corretos. Se estiverem incorretos, altere o valor da chave sso_enabled para False.



7. Retorne à interface de usuário do RES para reconfigurar o SSO.

Erro “Usuário não encontrado” ao tentar fazer login

Se você receber o erro “Usuário não encontrado” ao fazer login na interface RES, o usuário estará presente no Active Directory, mas não no RES. Se você adicionou recentemente o usuário ao AD, ele possivelmente não está sincronizado com o RES. O RES sincroniza de hora em hora, então talvez seja necessário esperar e verificar se o usuário foi adicionado após a próxima sincronização. Para sincronizar imediatamente, siga as etapas emthe section called “Usuário adicionado no Active Directory, mas ausente do RES”.

Se o usuário estiver presente no RES:

1. Certifique-se de que o mapeamento de atributos esteja configurado corretamente. Para ter mais informações, consulte the section called “Configurando seu provedor de identidade para login único (SSO)”.
2. Certifique-se de que o assunto do SAML e o e-mail do SAML sejam mapeados para o endereço de e-mail do usuário.

Usuário adicionado no Active Directory, mas ausente do RES

Se você adicionou um usuário ao Active Directory, mas ele está ausente no RES, a sincronização do AD precisa ser acionada. A sincronização do AD é realizada de hora em hora por uma função Lambda para importar entradas do AD para o ambiente RES. Ocasionalmente, há um atraso até que o próximo processo de sincronização seja executado após a adição de novos usuários ou grupos. Você pode iniciar a sincronização manualmente a partir do Amazon Simple Queue Service.

Inicie o processo de sincronização manualmente:

1. Abra o console do Amazon SQS em https://console.aws.amazon.com/sqs/.
2. Em Filas, selecione`<environment-name>-cluster-manager-tasks.fifo`.
3. Escolha Send and receive messages (Enviar e receber mensagens).
4. Em Corpo da mensagem, digite:

   `{ "name": "adsync.sync-from-ad", "payload": {} }`
5. Em ID do grupo de mensagens, digite: **`adsync.sync-from-ad`**
6. Em ID de desduplicação de mensagens, insira uma sequência de caracteres alfanumérica aleatória. Essa entrada deve ser diferente de todas as chamadas em cinco minutos ou a solicitação será ignorada.

Usuário indisponível ao criar uma sessão

Se você for um administrador criando uma sessão, mas descobrir que um usuário que está no Active Directory não está disponível ao criar uma sessão, talvez o usuário precise fazer login pela primeira vez. As sessões só podem ser criadas para usuários ativos. Os usuários ativos devem fazer login no ambiente pelo menos uma vez.

Erro de limite de tamanho excedido no log do gerenciador de CloudWatch clusters

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

Se você receber esse erro no log do CloudWatch gerenciador de cluster, a pesquisa ldap pode ter retornado muitos registros de usuário. Para corrigir esse problema, aumente o limite de resultados de pesquisa ldap do seu IDP.

Avisos

Cada instância do Amazon EC2 vem com duas licenças de Serviços de Desktop Remoto (Serviços de Terminal) para fins administrativos. Essas informações estão disponíveis para ajudá-lo a provisionar essas licenças para seus administradores. Você também pode usar AWS Systems Manager Session Manager, o que permite a comunicação remota para instâncias do Amazon EC2 sem RDP e sem a necessidade de licenças RDP. Se forem necessárias licenças adicionais dos Serviços de Área de Trabalho Remota, as CALs de usuário da Área de Trabalho Remota devem ser adquiridas da Microsoft ou de um revendedor de licenças da Microsoft. As CALs de usuários de desktop remoto com o Software Assurance ativo têm benefícios da Mobilidade de Licenças e podem ser levadas para ambientes de locatários AWS padrão (compartilhados). Para obter informações sobre como obter licenças sem os benefícios do Software Assurance ou da Mobilidade de Licenças, consulte esta seção das perguntas frequentes.

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas AWS atuais de produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. AWS as responsabilidades e obrigações para com seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum acordo entre AWS e seus clientes.

O Research and Engineering Studio on AWS é licenciado sob os termos da Licença Apache Versão 2.0, disponível na The Apache Software Foundation.

Revisões

Para obter mais informações, consulte o arquivo CHANGELOG.md no repositório. GitHub

Data	Alteração
Novembro de 2023	Lançamento inicial
Dezembro de 2023	GovCloud direções e modelos adicionados
Janeiro de 2024	Versão de lançamento 2024.01
Fevereiro de 2024	Versão de lançamento 2024.01.01 — modelo de implantação atualizado
Março de 2024	Tópicos adicionais de solução de problemas , retenção de CloudWatch registros, desinstal ação de versões secundárias
Abril de 2024	Versão de lançamento 2024.04 — AMIs prontas para RES e modelos de lançamento de projetos
Junho de 2024	• Versão de lançamento 2024.06 — Suporte ao Ubuntu, permissões do proprietário do projeto. • Guia do usuário: adicionado Crie um ambiente de demonstração

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.