



Manual do usuário

Estúdio de Pesquisa e Engenharia



Estúdio de Pesquisa e Engenharia: Manual do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Visão geral	1
Atributos e benefícios	1
Conceitos e definições	2
Visão geral da arquitetura	5
Diagrama de arquitetura	5
AWS serviços neste produto	6
Ambiente de demonstração	10
Crie uma pilha de demonstração com um clique	10
Pré-requisitos	10
Crie recursos e parâmetros de entrada	11
Etapas de pós-implantação	12
Planeje a implantação	14
Custo	14
Segurança	14
IAMfunções	15
Grupos de segurança	15
Criptografia de dados	15
Considerações sobre a segurança do produto	16
Cotas	19
Cotas para AWS serviços neste produto	19
AWS CloudFormation cotas	20
Planejamento da resiliência	20
Suportado Regiões da AWS	20
Implemente o produto	23
Pré-requisitos	23
Crie um Conta da AWS com um usuário administrativo	23
Crie um par de EC2 SSH chaves da Amazon	24
Aumente as cotas de serviço	24
Crie um domínio público (opcional)	24
Criar domínio (GovCloud somente)	25
Forneça recursos externos	26
Configure LDAPS em seu ambiente (opcional)	27
Configurar um privado VPC (opcional)	27
Crie recursos externos	39

Etapa 1: lançar o produto	45
Etapa 2: faça login pela primeira vez	54
Atualize o produto	56
Principais atualizações da versão	56
Atualizações de versões menores	56
Desinstalar o produto	58
Usando o AWS Management Console	58
Usando AWS Command Line Interface	58
Excluindo o shared-storage-security-group	58
Excluindo os buckets do Amazon S3	59
Guia de configuração	60
Gerenciando usuários e grupos	60
Configuração SSO com o IAM Identity Center	60
Configurando seu provedor de identidade para SSO	64
Definindo senhas para usuários	74
Criação de subdomínios	74
Crie um ACM certificado	75
CloudWatch Registros da Amazon	76
Definindo limites de permissão personalizados	77
Pronto para configuração RES AMIs	82
Prepare a IAM função para acessar o RES ambiente	82
Criar componente EC2 Image Builder	84
Prepare sua receita do EC2 Image Builder	88
Configurar a infraestrutura do EC2 Image Builder	90
Configurar o pipeline de imagens do Image Builder	91
Execute o pipeline de imagens do Image Builder	92
Registre uma nova pilha de software no RES	92
Guia do administrador	93
Gerenciamento de segredos	93
Monitoramento e controle de custos	96
Gerenciamento de sessões	100
Painel	102
Sessões	103
Pilhas de software () AMIs	106
Depuração	110
Configurações da área de trabalho	111

Gestão do meio ambiente	112
Status do ambiente	113
Configurações de ambiente	113
Usuários	114
Grupos	115
Projetos	116
Política de permissão	123
Sistemas de arquivos	138
Gerenciamento de instantâneos	143
Buckets do Amazon S3	149
Use o produto	166
SSHacesso	166
Áreas de trabalho virtuais	166
Inicie um novo desktop	167
Acesse seu desktop	168
Controle o estado do seu desktop	170
Modificar uma área de trabalho virtual	172
Recuperar informações da sessão	173
Agende desktops virtuais	173
VDIparada automática	176
Desktops compartilhados	178
Compartilhar uma área de trabalho	178
Acesse uma área de trabalho compartilhada	180
Navegador de arquivos	180
Carregar arquivo (s)	181
Excluir arquivo (s)	181
Gerenciar favoritos	182
Editar arquivos	182
Transferir arquivos	183
Solução de problemas	185
Depuração e monitoramento gerais	188
Fontes úteis de informações sobre registros e eventos	189
Aparência típica EC2 do console Amazon	193
DCVDepuração do Windows	195
Encontre informações sobre a DCV versão da Amazon	196
Problema RunBooks	196

Problemas de instalação	198
Problemas de gerenciamento de identidade	208
Armazenamento	212
Snapshots	217
Infraestrutura	218
Lançamento de desktops virtuais	219
Componente de desktop virtual	224
Exclusão do ambiente	230
Ambiente de demonstração	237
Problemas conhecidos	238
Problemas conhecidos 2024.x	238
Avisos	256
Revisões	257
.....	cclix

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 RES fornece um painel único para que os usuários iniciem desktops virtuais seguros para realizar pesquisas científicas, projetos de produtos, simulações de engenharia ou cargas de trabalho de análise de dados. Os usuários podem se conectar ao RES portal 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 (usando [Amazon Machine Images](#) ou AMIs) e permitir que RES os usuários 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 RES portal para atender às suas próprias necessidades.

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 RES para implantação 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

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 fazer login para se RES 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 RES portal com a identidade corporativa existente de um usuário e atribuir permissões a projetos usando associações de usuários e grupos existentes.

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 nelesRES. Os serviços de armazenamento compatíveis incluem o Amazon Elastic File System para desktops Linux e o Amazon FSx NetApp 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 RES projetos para monitorar os custos de cada projeto. Se você exceder seu orçamento, poderá limitar o lançamento das VDI sessões.

Conceitos e definições

Esta seção descreve os principais conceitos e define a terminologia específica do Research and Engineering Studio sobre AWS:

Navegador de arquivos

Um navegador de arquivos faz parte da interface do RES usuário em que os usuários que estão 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 RES recursos que são compartilhados em um RES ambiente. 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 RES administrador, 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; isso garante a governança do fluxo de dados e evita o compartilhamento de dados e VDI hosts entre projetos.

Permissões baseadas em projetos

As permissões baseadas em projetos descrevem uma partição lógica de dados e VDI hosts em um sistema em que vários projetos podem existir. O acesso de um usuário aos dados e aos VDI hosts 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, o usuário não conseguirá acessar os dados do projeto e VDIs quando não tiver recebido a associação.

Membro do projeto

Um usuário final de RES recursos (armazenamento VDI, 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 RES metadados específicos com base em qualquer sistema operacional que um usuário tenha selecionado para provisionar para seu host. VDI

VDI hospeda

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 sua Conta da AWS

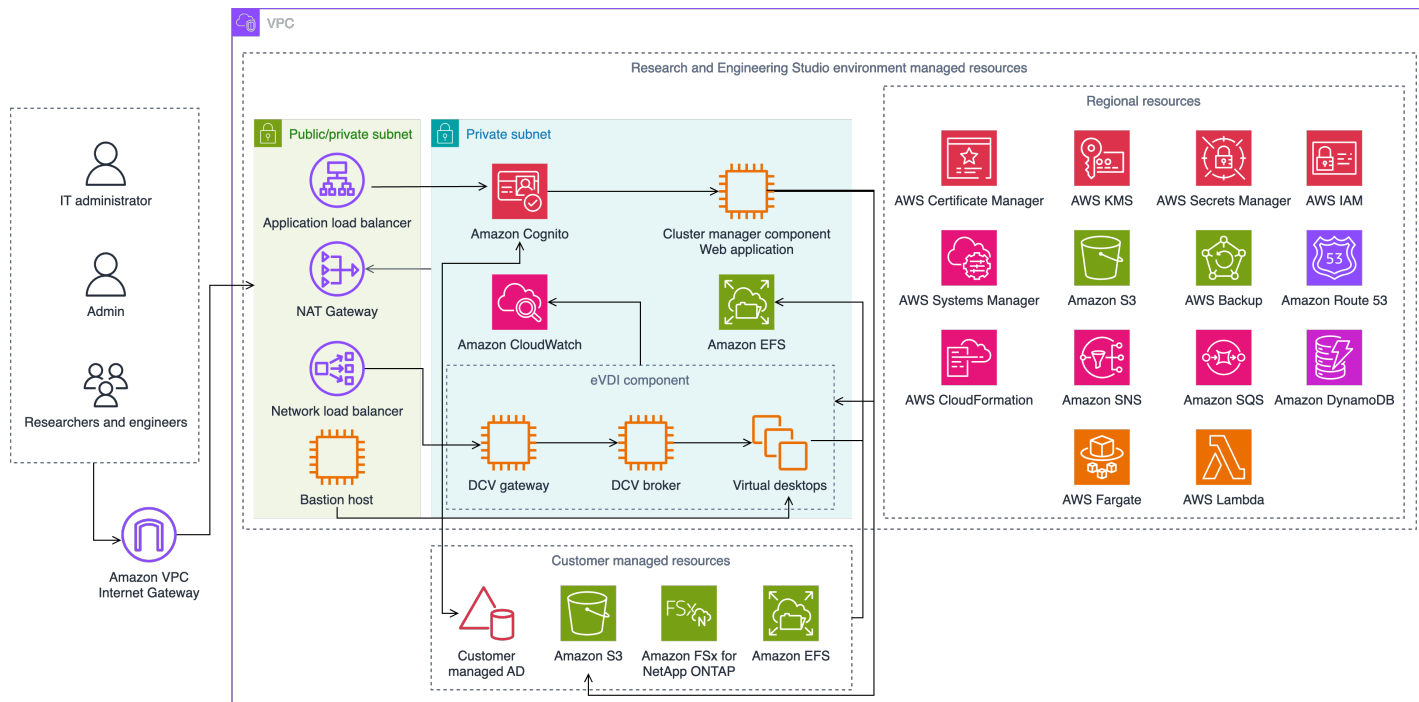


Figura 1: Estúdio de Pesquisa e Engenharia em AWS arquitetura

Note

AWS CloudFormation os 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. RESinstala componentes para o portal da web, bem como:
 - a. Componente de desktop virtual (eVDI) de engenharia para cargas de trabalho interativas

b. Componente de métricas

A Amazon CloudWatch recebe métricas dos VDI componentes eletrônicos.

c. Componente Bastion Host

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

2. REinstala componentes em sub-redes privadas atrás 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 VDI Linux.
6. RESusa 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 na primeira vez que fizer 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.

AWS serviços neste produto

AWS serviço	Tipo	Descrição
Amazon Elastic Compute Cloud	Serviços	Fornecer os serviços de computação subjacentes para

AWS serviço	Tipo	Descrição
		criar desktops virtuais com o sistema operacional e a pilha de software escolhidos.
Elastic Load Balancing	Serviços	O Bastion, o gerenciador de clusters e os VDI hosts são criados em grupos de Auto Scaling por trás do balanceador de carga. ELB equilibra o tráfego do portal da web entre RES os hosts.
Amazon Virtual Private Cloud	Serviços	Todos os componentes principais do produto são criados dentro do seu VPC.
Amazon Cognito	Serviços	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	Serviços	Fornecer o sistema de /home arquivos para o navegador de arquivos e VDI os hosts, bem como sistemas de arquivos externos compartilhados.
Amazon DynamoDB	Serviços	Armazena dados de configuração, como usuários, grupos, projetos, sistemas de arquivos e configurações de componentes.

AWS serviço	Tipo	Descrição
AWS Systems Manager (Gerenciador de sistemas)	Serviços	Armazena documentos para executar comandos para gerenciamento de VDI sessões.
AWS Lambda	Serviços	Oferece suporte às funcionalidades do produto, como atualizar as configurações na tabela do DynamoDB, iniciar fluxos de trabalho de sincronização do Active Directory e atualizar a lista de prefixos.
Amazon CloudWatch	Apoiando	Fornecer métricas e registros de atividades para todos os EC2 hosts da Amazon e funções do Lambda.
Amazon Simple Storage Service	Apoiando	Armazena binários de aplicativos para inicialização e configuração do host.
AWS Key Management Service	Apoiando	Usado para criptografia em repouso com SQS filas da Amazon, tabelas do DynamoDB e tópicos da Amazon. SNS
AWS Secrets Manager	Apoiando	Armazena credenciais da conta de serviço no Active Directory e certificados autoassinados para VDIs
AWS CloudFormation	Apoiando	Fornecer um mecanismo de implantação para o produto.

AWS serviço	Tipo	Descrição
AWS Identity and Access Management	Apoiando	Restringe o nível de acesso dos hosts.
Amazon Route 53	Apoiando	Cria uma zona hospedada privada para resolver o balanceador de carga interno e o nome de domínio do bastion host.
Amazon Simple Queue Service	Apoiando	Cria filas de tarefas para suportar execuções assíncronas.
Amazon Simple Notification Service	Apoiando	Suporta o modelo de assinante de publicação entre VDI componentes como o controlador e os hosts.
AWS Fargate	Apoiando	Instala, atualiza e exclui ambientes usando tarefas do Fargate.
Amazon FSx File Gateway	Opcional	Fornecer sistema de arquivos compartilhado externo.
Amazon FSx para NetApp ONTAP	Opcional	Fornecer 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 EC2 hosts, sistemas de arquivos e DynamoDB da Amazon.

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 instruções [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 EC2 SSH chaves da Amazon](#)
- [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 a <https://portal.aws.amazon.com/billing/inscrição>.
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 AWS é 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 EC2 SSH chaves da Amazon

Se você não tiver o Amazon EC2 SSH key pair, precisará criar um. Para obter mais informações, consulte [Criar um par de chaves usando a Amazon EC2](#) no Guia EC2 do usuário da Amazon.

Aumente as cotas de serviço

Recomendamos [aumentar as cotas de serviço](#) para:

- [Amazon VPC](#)
 - Aumente a cota de endereços IP elásticos por NAT gateway de cinco para oito
 - Aumente os NAT gateways por zona de disponibilidade de cinco para dez
- [Amazon EC2](#)
 - Aumente o EC2 - VPC Elástico IPs 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 obter 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	<i><res-demo></i>	Um nome exclusivo dado ao seu RES ambiente

Parâmetro	Padrão	Descrição
		começando com res-, não mais que 11 caracteres e sem letras maiúsculas.
AdministratorEmail		O endereço de e-mail do usuário que está concluindo 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.
ClientIPcidr	<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 permitir o acesso direto à interface do usuário da Web e SSH ao Bastion Host.

4. Selecione Criar pilha.

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 escolha 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

Esta seção contém informações sobre custo, segurança, regiões suportadas e cotas que podem ajudá-lo a planejar sua implantação do Research and Engineering Studio em AWS.

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 obter mais informações, consulte [AWS serviços neste produto](#).

Note

Você é responsável pelo custo dos AWS serviços usados durante a execução deste produto. Recomendamos criar um [orçamento 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 AWS serviço usado neste produto.

Segurança

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) de descreve isso como segurança na nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Research and Engineering Studio on AWS, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Para entender como aplicar o modelo de responsabilidade compartilhada com os AWS serviços usados pelo Research and Engineering Studio, consulte [Considerações de segurança para os serviços deste produto](#). Para obter mais informações sobre AWS segurança, acesse [Nuvem AWS Segurança](#).

IAMfunções

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

RESoferece suporte a políticas baseadas em identidade em. IAM Quando implantado, 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 cliente existente com RES o Active Directory integrado. Para obter mais informações, consulte [Criação de IAM políticas](#) 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 do RES usuário, RES efetua a autenticação 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 funçõesEC2, instâncias, instâncias de CSR sistemas de arquivos e VPN endpoints remotos do Lambda. 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 RES própria. Ao implantarRES, você pode especificar um AWS KMS key. RESusa suas credenciais para conceder acesso à chave. Se você fornecer um cliente de propriedade e gerenciamento AWS KMS key, os dados do cliente em repouso serão criptografados usando essa chave.

REScriptografa os dados do cliente em trânsito usandoSSL/TLS. Exigimos TLS 1,2, mas recomendamos TLS 1,3.

Considerações de segurança para os serviços deste produto

Para obter informações mais detalhadas sobre as considerações de segurança dos serviços usados pelo Research and Engineering Studio, siga os links nesta tabela:

AWS informações de segurança do serviço	Tipo de serviço	Como o serviço é usado em RES
Amazon Elastic Compute Cloud	Serviços	Fornecer os serviços de computação subjacentes para criar desktops virtuais com o sistema operacional e a pilha de software escolhidos.
Elastic Load Balancing	Serviços	O Bastion, o gerenciador de clusters e os VDI hosts são criados em grupos de Auto Scaling por trás do balanceador de carga. ELB equilibra o tráfego do portal da web entre RES os hosts.
Amazon Virtual Private Cloud	Serviços	Todos os componentes principais do produto são criados dentro do seu VPC.
Amazon Cognito	Serviços	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	Serviços	Fornecer o sistema de /home arquivos para o navegador de arquivos e VDI os hosts, bem

AWS informações de segurança do serviço	Tipo de serviço	Como o serviço é usado em RES
		como sistemas de arquivos externos compartilhados.
Amazon DynamoDB	Serviços	Armazena dados de configuração, como usuários, grupos, projetos, sistemas de arquivos e configurações de componentes.
AWS Systems Manager (Gerenciador de sistemas)	Serviços	Armazena documentos para executar comandos para gerenciamento de VDI sessões.
AWS Lambda	Serviços	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.
Amazon CloudWatch	Apoiando	Fornecer métricas e registros de atividades para todos os EC2 hosts da Amazon e funções do Lambda.
Amazon Simple Storage Service	Apoiando	Armazena binários de aplicativos para inicialização e configuração do host.

AWS informações de segurança do serviço	Tipo de serviço	Como o serviço é usado em RES
AWS Key Management Service	Apoiando	Usado para criptografia em repouso com SQS filas da Amazon, tabelas do DynamoDB e tópicos da Amazon. SNS
AWS Secrets Manager	Apoiando	Armazena credenciais da conta de serviço no Active Directory e certificados autoassinados para. VDIs
AWS CloudFormation	Apoiando	Fornecer um mecanismo de implantação para o produto.
AWS Identity and Access Management	Apoiando	Restringe o nível de acesso dos hosts.
Amazon Route 53	Apoiando	Cria uma zona hospedada privada para resolver o balanceador de carga interno e o nome de domínio do bastion host.
Amazon Simple Queue Service	Apoiando	Cria filas de tarefas para suportar execuções assíncronas.
Amazon Simple Notification Service	Apoiando	Suporta o modelo de assinante de publicação entre VDI componentes como o controlador e os hosts.
AWS Fargate	Apoiando	Instala, atualiza e exclui ambientes usando tarefas do Fargate.

AWS informações de segurança do serviço	Tipo de serviço	Como o serviço é usado em RES
Amazon FSx File Gateway	Opcional	Fornecer sistema de arquivos compartilhado externo.
Amazon FSx para NetApp ONTAP	Opcional	Fornecer 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 EC2 hosts, sistemas de arquivos e DynamoDB da Amazon.

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 EC2 instâncias da Amazon para operar o sistema. Para melhorar a resiliência em ambientes de produção em grande escala, recomendamos aumentar as configurações de capacidade mínima padrão nos grupos de Auto Scaling da infraestrutura (). ASG 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.

ASGs configurações podem ser personalizadas no EC2 console da Amazon 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. Selecione o grupo que você deseja modificar e, em seguida, escolha Ações e selecione Editar. Para obter mais informações sobre ASGs, consulte [Dimensionar o tamanho do seu grupo de Auto Scaling](#) no Guia do usuário do Amazon Auto EC2 Scaling.

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	Região	Versões anteriores	Versão mais recente (2024.10)
Leste dos EUA (Norte da Virgínia)	us-east-1	sim	sim

Nome da região	Região	Versões anteriores	Versão mais recente (2024.10)
Leste dos EUA (Ohio)	us-east-2	sim	sim
Oeste dos EUA (N. da Califórnia)	us-west-1	sim	sim
Oeste dos EUA (Oregon)	us-west-2	sim	sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	sim	sim
Ásia-Pacífico (Seul)	ap-northeast-2	sim	sim
Ásia-Pacífico (Mumbai)	ap-south-1	sim	sim
Ásia-Pacífico (Singapura)	ap-southeast-1	sim	sim
Ásia-Pacífico (Sydney)	ap-southeast-2	sim	sim
Canadá (Central)	ca-central-1	sim	sim
Europa (Frankfurt)	eu-central-1	sim	sim
Europa (Milão)	eu-south-1	sim	sim
Europa (Irlanda)	eu-west-1	sim	sim
Europa (Londres)	eu-west-2	sim	sim
Europa (Paris)	eu-west-3	sim	sim
Europa (Estocolmo)	eu-north-1	não	sim
Israel (Tel Aviv)	il-central-1	sim	sim

Nome da região	Região	Versões anteriores	Versão mais recente (2024.10)
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	sim	sim

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](#)
- [Crie recursos externos](#)
- [Etapa 1: lançar o produto](#)
- [Etapa 2: faça login pela primeira vez](#)

Pré-requisitos

Tópicos

- [Crie um Conta da AWS com um usuário administrativo](#)
- [Crie um par de EC2 SSH chaves da Amazon](#)
- [Aumente as cotas de serviço](#)
- [Crie um domínio público \(opcional\)](#)
- [Criar domínio \(GovCloud somente\)](#)
- [Forneça recursos externos](#)
- [Configure LDAPS em seu ambiente \(opcional\)](#)
- [Configurar um privado VPC \(opcional\)](#)

Crie um Conta da AWS com um usuário administrativo

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

1. Abra a <https://portal.aws.amazon.com/billing/inscrição>.
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 AWS é 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 EC2 SSH chaves da Amazon

Se você não tiver o Amazon EC2 SSH key pair, precisará criar um. Para obter mais informações, consulte [Criar um par de chaves usando a Amazon EC2](#) no Guia EC2 do usuário da Amazon.

Aumente as cotas de serviço

Recomendamos [aumentar as cotas de serviço](#) para:

- [Amazon VPC](#)
 - Aumente a cota de endereços IP elásticos por NAT gateway de cinco para oito.
 - Aumente os NAT gateways por zona de disponibilidade de cinco para dez.
- [Amazon EC2](#)
 - Aumente o EC2 - VPC Elástico IPs 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 obter mais informações, consulte [Cotas para AWS serviços neste produto](#).

Crie um domínio público (opcional)

Recomendamos usar um domínio personalizado para o produto para que ele seja fácil de usar URL. 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) e estiver usando um domínio personalizado para o Research and Engineering Studio, 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 segredo ARN 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 segredo ARN 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

O Research and Engineering Studio on AWS espera que os seguintes recursos externos existam quando for implantado.

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

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

- Armazenamento (AmazonEFS)

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 no RES 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 LDAPS em seu ambiente (opcional)

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

1. Siga as etapas fornecidas em [Como habilitar o lado do servidor LDAPS](#) para seu. AWS Managed Microsoft AD Você pode pular essa etapa se já tiver ativado LDAPS.
2. Depois de confirmar que LDAPS está configurado no AD, exporte o certificado 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. Selecione 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 secreto e cole seu certificado PEM codificado no campo Texto simples.
4. Observe o ARN criado e insira-o como `DomainTLSCertificateSecretARN` parâmetro em [Etapa 1: lançar o produto](#).

Configurar um privado VPC (opcional)

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

Tópicos

- [Prepare imagens de máquinas da Amazon \(AMIs\)](#)
- [Configurar VPC endpoints](#)

- [Conecte-se a serviços sem VPC endpoints](#)
- [Definir parâmetros VPC de implantação privada](#)

Prepare imagens de máquinas da Amazon (AMIs)

1. Baixe [dependências](#). Para ser implantada de forma isolada VPC, a RES infraestrutura exige a disponibilidade de dependências sem ter acesso público à Internet.
2. Crie uma IAM função com acesso somente de leitura e identidade confiável do Amazon S3 como Amazon. EC2
 - a. Abra o IAM console 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, escolha EC2 Avançar.
 - d. Em Adicionar permissões, selecione as seguintes políticas de permissão e escolha Avançar:
 - Amazon S3 ReadOnlyAccess
 - AmazonSSMManaged InstanceCore
 - EC2InstanceProfileForImageBuilder
 - e. Adicione um nome e uma descrição da função e escolha Criar função.
3. Crie o componente construtor de EC2 imagens:
 - a. Abra o console do EC2 Image Builder em <https://console.aws.amazon.com/imagebuilder>.
 - 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	Insira um nome como: <i><research-and-engineering-studio-infrastructure></i>
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 arquivo URI para o arquivo tar.gz. Faça o upload do arquivo tar.gz fornecido por RES para um bucket do Amazon S3 e copie o arquivo URI 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 que oferecem suporte a endpoints. 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.

Seção	Parâmetro	Entrada do usuário
	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 Remove SSM agente após a execução do pipeline não esteja selecionado.
Diretório de trabalho	Caminho do diretório de trabalho	/root/bootstrap/re s_dependências

Seção	Parâmetro	Entrada do usuário
Componentes	Componentes de construção	<p>Pesquise e selecione o seguinte:</p> <ul style="list-style-type: none"> • Gerenciado pela Amazon: <code>-2-linux aws-cli-version</code> • Gerenciado pela Amazon: <code>amazon-cloudwatch-agent-linux</code> • De sua propriedade: EC2 componente da Amazon criado anteriormente. Coloque seu Conta da AWS ID e atual Região da AWS nos campos.
	Componentes de teste	<p>Pesquise e selecione:</p> <ul style="list-style-type: none"> • Gerenciado pela Amazon: <code>simple-boot-test-linux</code>

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, insira o seguinte:

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

Seção	Parâmetro	Entrada do usuário
	Descrição	Adicione uma descrição opcional.
	IAMPapel	Selecione a IAM função criada anteriormente.
AWS infraestrutura	Tipo de instância	Escolha t3.medium.
	VPC, sub-rede e grupos de segurança	<p>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 EC2 console da Amazon com as seguintes entradas:</p> <ul style="list-style-type: none"> • VPC: selecione o mesmo que VPC está sendo usado para a configuração da infraestrutura. Isso VPC deve ter acesso à Internet. • Regra de entrada: <ul style="list-style-type: none"> • Tipo: SSH • Source (Origem): personalizado • CIDRbloco: 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 Criar cronograma, defina um cronograma ou escolha Manual se quiser iniciar o processo de AMI cozimento 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 RES ambiente implantado, para que RES possa iniciar adequadamente as instâncias hospedeiras da infraestrutura a partir dela. 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 a elas.
 - g. Revise 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 selecione Executar pipeline.

O pipeline pode levar aproximadamente de 45 minutos a uma hora para criar uma AMI imagem.
 8. Anote o AMI ID do gerado AMI e use-o como entrada para o InfrastructureHost AMI parâmetro em [the section called “Etapa 1: lançar o produto”](#).

Configurar VPC endpoints

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 no [Access e AWS service \(Serviço da AWS\) usando um VPC endpoint de interface](#).
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. <i>region</i> .escalonamento automático de aplicativos
AWS CloudFormation	com.amazonaws. <i>region</i> cloudformation.
Amazon CloudWatch	com.amazonaws. <i>region</i> .monitoramento
CloudWatch Registros da Amazon	com.amazonaws. <i>region</i> .registros
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb (requer um endpoint de gateway)
Amazon EC2	com.amazonaws. <i>region</i> ec2.
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
Amazon Elastic File System	com.amazonaws. <i>region</i> elasticfilesystem.
Elastic Load Balancing	com.amazonaws. <i>region</i> . balanceamento de carga elástico
Amazon EventBridge	com.amazonaws. <i>region</i> .events
Amazon FSx	com.amazonaws. <i>region</i> .fsx
AWS Key Management Service	com.amazonaws. <i>region</i> kms.
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-streams
AWS Lambda	com.amazonaws. <i>region</i> lambda.

AWS service (Serviço da AWS)	Nome do serviço
Amazon S3	com.amazonaws. <i>region</i> .s3 (Requer um endpoint de gateway criado por padrão em.) RES Endpoints adicionais da interface Amazon S3 são necessários para a montagem cruzada de buckets em um ambiente isolado. Consulte Acesso aos endpoints da interface do Amazon Simple Storage Service .
AWS Secrets Manager	com.amazonaws. <i>region</i> secretsmanager.
Amazon SES	com.amazonaws. <i>region</i> .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. <i>region</i> .sts
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> sqs.
AWS Systems Manager	com.amazonaws. <i>region</i> .ec2 mensagens.
	com.amazonaws. <i>region</i> ssm.
	com.amazonaws. <i>region</i> .mensagens.ssm

Conecte-se a serviços sem VPC endpoints

Para se integrar a serviços que não oferecem suporte a VPC endpoints, você pode configurar um servidor proxy em uma sub-rede pública do seu 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 RES implantação.

- 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 o PORT que o servidor proxy escuta.
 3. Configure sua tabela de rotas para permitir o acesso ao servidor proxy.
 - a. Acesse seu VPC console e identifique as tabelas de rotas das sub-redes que você usará para hosts e VDI hosts de infraestrutura.
 - 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 Infrastructure/. VDIs
 4. Modifique o grupo de segurança da EC2 instância do servidor proxy e certifique-se de que ele permita TCP conexões de entrada PORT na qual o servidor proxy está escutando.

Definir parâmetros VPC de implantação privada

Em [the section called “Etapa 1: lançar o produto”](#), espera-se que você insira determinados parâmetros no AWS CloudFormation modelo. Certifique-se de definir os seguintes parâmetros, conforme observado, para implantar com sucesso na área privada VPC que você acabou de configurar.

Parâmetro	Entrada
InfrastructureHostAMI	Use o AMI ID de infraestrutura criado em the section called “Prepare imagens de máquinas da Amazon (AMIs)” .
IsLoadBalancerInternetFacing	Definido como falso.
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 VPC CIDR para permitir o acesso a todos os endereços VPC IP.

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 comerciais, 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.
AdminPassword		A senha do administrador do Active Directory (nome de usuárioAdmin). Esse usuário

Parâmetro	Padrão	Descrição
		<p>é criado no Active Directory para a fase inicial de inicialização e não é usado depois.</p> <p>Importante: o formato desse campo pode ser (1) uma senha de texto simples ou (2) o formato ARN de um AWS segredo formatado como um par chave/valor. <code>{"password": "somepassword"}</code></p> <p>Observação: a senha desse usuário deve atender aos requisitos de complexidade da senha do Active Directory.</p>

Parâmetro	Padrão	Descrição
ServiceAccountPassword		<p>Senha usada para criar uma conta de serviço (ReadOnlyUser). Essa conta é usada para sincronização.</p> <p>Importante: o formato desse campo pode ser (1) uma senha de texto simples ou (2) o formato ARN de um AWS segredo formatado como um par chave/valor. <code>{"password": "somepassword"}</code></p> <p>Observação: a senha desse usuário deve atender aos requisitos de complexidade da senha do Active Directory.</p>
Par de chaves		<p>Conecta as instâncias administrativas usando um SSH cliente.</p> <p>Observação: o Gerenciador de AWS Systems Manager sessões também pode ser usado para se conectar às instâncias.</p>

Parâmetro	Padrão	Descrição
LDIFS3Path	<code>aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif</code>	<p>O caminho do Amazon S3 para um LDIF arquivo importado durante a fase de inicialização da configuração do Active Directory. Para obter mais informações, consulte LDIFSupport. O parâmetro é pré-preenchido com um arquivo que cria vários usuários no Active Directory.</p> <p>Para visualizar o arquivo, consulte o arquivo res.ldif disponível em. GitHub</p>
ClientIpCidr		<p>O endereço IP a partir do qual você acessará o site. Por exemplo, você pode selecionar seu endereço IP e usá-lo <code>[IPADDRESS]/32</code> para permitir apenas o acesso do seu host. Você pode atualizar essa pós-implantação.</p>

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- <i>[environment name]</i>	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 RES pilha. Se você estiver implantando vários ambientes em sua conta, isso precisará ser exclusivo.

Parâmetro	Padrão	Descrição
PortalDomainName		Para GovCloud implantações, 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 EnvironmentName 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 RES principal 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 esse 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	<i><res-demo></i>	Um nome exclusivo dado ao seu RES ambiente começando com res-, não mais que 11 caracteres e sem letras maiúsculas.

Parâmetro	Padrão	Descrição
AdministratorEmail		O endereço de e-mail do usuário que está concluindo 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	eu sou- <i>[numbers or letters only]</i>	(Opcional) Você pode fornecer um AMI ID personalizado para usar em todos os hosts da infraestrutura. O sistema operacional básico atualmente suportado é o Amazon Linux 2. Para obter mais informações, consulte Pronto para configuração RES AMIs .
SSHKeyPair		O par de chaves usado para se conectar aos hosts da infraestrutura.
ClientIP	<i>x.x.x.0/24</i> ou <i>x.x.x.0/32</i>	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 permitir o acesso direto à interface do usuário da Web e SSH ao Bastion Host.

Parâmetro	Padrão	Descrição
IAMPermissionBoundary		(Opcional) Você pode fornecer uma política gerenciada ARN que será anexada como limite de permissão a todas as funções criadas em RES. Para obter mais informações, consulte Definindo limites de permissão personalizados .
VpcId		ID do VPC local 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, selecione sub-redes privadas. Para implantações que precisam de acesso à Internet, selecione 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 VDI instâncias serão iniciadas . Se mais de dois foram criados pela pilha de rede externa, selecione todos os que foram criados.

Parâmetro	Padrão	Descrição
ActiveDirectoryName	<i>corp.res.com</i>	Domínio para o diretório ativo. Ele não precisa corresponder ao nome de domínio do portal.
ADShortName	<i>corp</i>	O nome curto do diretório ativo. Isso também é chamado de BIOS nome da rede.
LDAPBase	<i>DC=corp,DC=res,DC=com</i>	Um LDAP caminho para a base dentro da LDAP hierarquia.
LDAPConnectionURI		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.
ServiceAccountCredentialsSecretArn		Forneça um segredo ARN que contenha o nome de usuário e a senha do ServiceAccount usuário do Active Directory, formatados como um par de chave/valor nome de usuário: senha.
Sou do usuário		Unidade organizacional dentro do AD para usuários que sincronizarão.

Parâmetro	Padrão	Descrição
Grupo SOU		Unidade organizacional dentro do AD para grupos que serão sincronizados.
SudoersGroupName	RESAdministrators	Nome do grupo que contém todos os usuários com acesso sudoer nas instâncias na instalação e acesso de administrador ativado RES.
SOU de computador		Unidade organizacional dentro do AD à qual as instâncias se juntarão.
omainTLSCertificateSegredo D ARN		(Opcional) Forneça um segredo de TLS certificado de domínio ARN para permitir a TLS comunicação com o AD.
EnableLdapIDMapping		Determina se UID e GID números são gerados por SSSD ou se os números fornecidos pelo AD são usados. Defina como Verdadeiro para usar SSSD gerado UID e GID Falso para usar UID e GID fornecido pelo AD. Na maioria dos casos, esse parâmetro deve ser definido como True.

Parâmetro	Padrão	Descrição
DisableADJoin	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 EFS ID a ser usado para o sistema de arquivos doméstico compartilhado para hosts Linux. VDI
CustomDomainNameforWebApp		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a parte web do sistema.
CustomDomainNameforVDI		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a VDI parte do sistema.

Parâmetro	Padrão	Descrição
ACMCertificateARNforWebApp		(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, consulte Guia de configuração .
CertificateSecretARNforVDI		(Opcional) Esse ARN secreto 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.

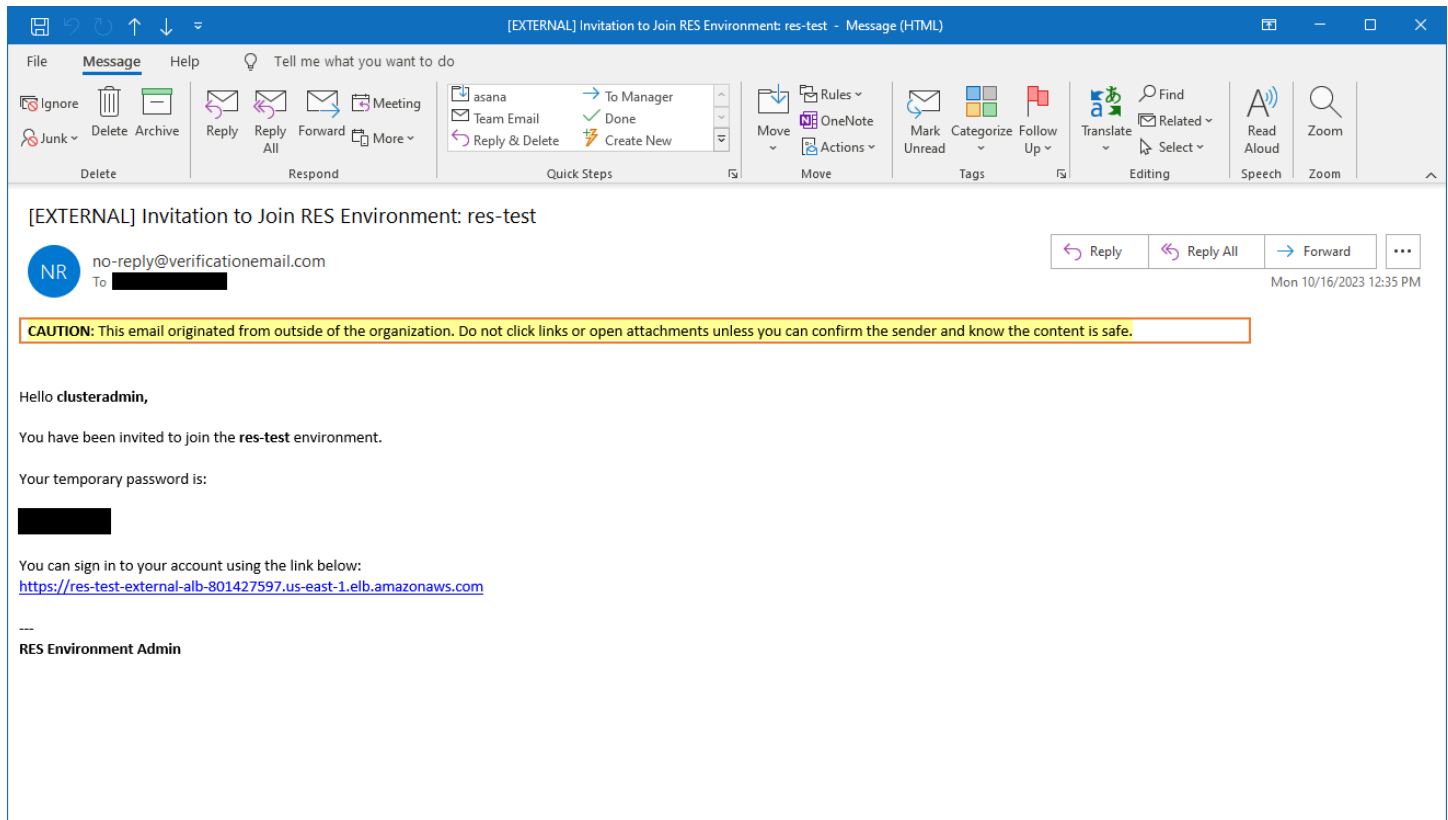
Parâmetro	Padrão	Descrição
PrivateKeySecretARNforVDI		(Opcional) Esse ARN segredo armazena a chave privada do certificado do seu portal da web. Se você definir um nome de domínio do portal para seus recursos externos automatizados, poderá encontrar esse valor na guia Saídas da pilha res-bi.

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 COMPLETE status CREATE _ 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 SSO provedor. Para obter informações sobre a configuração pós-implantação, consulte o [Guia de configuração](#). Observe que `clusteradmin` é uma conta inovadora. Você pode usá-la para criar projetos e atribuir membros de usuários ou grupos a esses projetos; ela não pode atribuir pilhas de software nem implantar um desktop sozinha.

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.

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](#)
- [Atualizações de versões menores](#)

Principais atualizações da versão

O Research and Engineering Studio usa instantâneos para oferecer suporte à migração de um RES ambiente 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 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 RES, não é necessária uma nova instalação. Você pode atualizar a RES pilha existente atualizando seu AWS CloudFormation modelo. Verifique a versão do seu RES ambiente 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 em [the 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 [console do AWS CloudFormation](#).
2. Na página Pilhas, selecione a pilha de instalação desse produto.
3. Escolha Excluir.

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 no AWS Management Console e abra o EFS console da Amazon em <https://console.aws.amazon.com/efs/>.
2. Exclua todos os sistemas de arquivos associados `<RES-stack-name>-shared-storage-security-group` a. 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 EC2 console da Amazon 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 no 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](#)
- [Criação de subdomínios](#)
- [Crie um ACM certificado](#)
- [CloudWatch Registros da Amazon](#)
- [Definindo limites de permissão personalizados](#)
- [Pronto para configuração RES AMIs](#)

Gerenciando usuários e grupos

O Research and Engineering Studio pode usar qualquer provedor de identidade compatível com SAML 2.0. Se você implantou RES usando recursos externos ou planeja usar o IAM Identity Center, consulte [Configurando o login único \(SSO\) com IAM o Identity Center](#). Se você tiver seu próprio provedor de identidade compatível com SAML 2.0, consulte [Configurando seu provedor de identidade para login único \(\) SSO](#).

Tópicos

- [Configurando o login único \(SSO\) com IAM o Identity Center](#)
- [Configurando seu provedor de identidade para login único \(\) SSO](#)
- [Definindo senhas para usuários](#)

Configurando o login único (SSO) com IAM o Identity Center

Se você ainda não tiver uma central de identidade conectada ao Active Directory gerenciado, comece com [Etapa 1: configurar uma central de identidade](#). Se você já tem uma central de identidade conectada ao Active Directory gerenciado, comece com [Etapa 2: conectar-se a uma central de identidade](#).


 Note

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

Etapa 1: configurar uma central de identidade

Habilitando o IAM Identity Center

1. Faça login no [console do AWS Identity and Access Management](#).
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 gerenciou o Active Directory.

Conectando o IAM Identity Center a um Active Directory gerenciado

Depois de habilitar o IAM Identity Center, conclua estas etapas de configuração recomendadas:

1. No painel de navegação, selecione Configurações.
2. Em Fonte de identidade, escolha Ações e escolha Alterar fonte de identidade.
3. Em Diretórios existentes, selecione seu diretório.
4. Escolha 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

Depois que as alterações feitas [Conectando o IAM Identity Center a um Active Directory gerenciado](#) forem concluídas, um banner verde de confirmação será exibido.

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. Escolha 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. Selecione o (s) usuário (s) para quem você deseja habilitar o acesso.
3. Escolha Habilitar acesso do usuário.

Etapa 2: conectar-se a uma central de identidade

Configurando o aplicativo no IAM Identity Center

1. Abra o [console do IAM Identity Center](#).
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 aplicativo, escolha SAML2.0.
6. Escolha 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 SAMLmetadados do IAM Identity Center. Você precisará disso ao configurar o IAM Identity Center com o RES portal.

9. Em Propriedades do aplicativo, insira o início do aplicativo URL. Por exemplo, <your-portal-domain>/sso.
10. Em Aplicativo ACS URL, insira o redirecionamento URL do RES portal. Para encontrar isso:
 - a. Em Gerenciamento do ambiente, escolha Configurações gerais.
 - b. Selecione a guia Provedor de identidade.
 - c. Em Single Sign-On, você encontrará o SAML Redirecionamento. URL
11. Em SAML Público do aplicativo, insira o Amazon CognitoURN.

Para criar a urna:

- a. No RES portal, 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. Depois de entrar no Amazon CognitoURN, escolha Enviar.

Configurando mapeamentos de atributos para o aplicativo

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

Adicionar usuários ao aplicativo no IAM 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 IAM Identity Center dentro do RES ambiente

1. No ambiente do Research and Engineering Studio, em Gerenciamento do ambiente, abra Configurações gerais.
2. Abra a guia Provedor de identidade.
3. Em Logon único, escolha Editar (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. Escolha Inserir ponto final URL do documento de metadados.
 - d. Insira o URL que você copiou durante [Configurando o aplicativo no IAM 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 RES portal. Essas etapas fornecem instruções para a integração com o provedor de identidade SAML 2.0 escolhido. Se você pretende usar o IAM Identity Center, consulte [Configurando o login único \(SSO\) com IAM o Identity Center](#).

Note

O e-mail do usuário deve corresponder à IDP SAML declaração 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 RES para usar seu provedor de identidade](#)
- [Configurando seu provedor de identidade em um ambiente que não seja de produção](#)
- [Depurando problemas de SAML IdP](#)

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. RES presume 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. 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 seu provedor de identidade (IdP). Essa configuração requer os seguintes parâmetros:
 - SAMLRedirecionamento URL — O URL que seu IdP usa para enviar a resposta 2.0 SAML ao provedor de serviços.

Note

Dependendo do IdP, o SAML redirecionamento URL pode ter um nome diferente:

- Aplicação URL
- Assertion Consumer Service () ACS URL
- ACSPOSTVinculação URL

Para obter o URL

1. Faça login RES como administrador ou administrador de cluster.
2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.

3. Escolha SAMLRedirecionar URL.

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

Note

Dependendo do IdP, o SAML público URI pode ter um nome diferente:

- ClientID
- SAML Público do aplicativo
- ID da entidade SP

Forneça a entrada no formato a seguir.

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

Para encontrar seu SAML público URI

1. Faça login 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 SAML declaração postada RES deve ter os seguintes campos/declarações definidos como o endereço de e-mail do usuário:
- SAML Assunto ou NameID
 - SAML e-mail
4. Seu IdP adiciona campos/declarações à SAML declaração, com base na configuração. RES requer 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 como `urn:amazon:cognito:sp:user-pool-id`. Substituir *user-pool-id* com o 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`. Substituir *user-pool-domain* com o 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 SAML solicitação.

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

Para obter o domínio URL

1. Faça login RES como administrador ou administrador de cluster.
 2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.
 3. Escolha o domínio URL.
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 `es-environment name-user-pool`.
3. Selecione a guia Experiência de login.
4. Na seção Login do provedor de identidade federado, escolha Exibir certificado de assinatura.

The screenshot displays the AWS Cognito console interface. The top section is titled "Cognito user pool sign-in" and includes a description: "Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool." Below this, there are two columns: "Cognito user pool sign-in options" with "User name" and "Email" listed, and "User name requirements" with the note "User names are not case sensitive".

The bottom section is titled "Federated identity provider sign-in (1)" and includes a "View signing certificate" button. Below the title is a search bar labeled "Search identity providers by name" and a table of providers. The table has columns for "Identity provider", "Identity provider type", "Created time", and "Last updated time". One provider is listed: "idc" with type "SAML", created "2 weeks ago", and last updated "3 hours ago".

Identity provider	Identity provider type	Created time	Last updated time
idc	SAML	2 weeks ago	3 hours ago

Você pode usar esse certificado para configurar o Active DirectoryIDP, adicionar um relying party trust e habilitar o SAML suporte a essa parte confiável.

Note

Isso não se aplica ao Keycloak e. IDC

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

Configure RES para usar seu provedor de identidade

Para concluir a configuração de login único para RES

1. Faça login RES como administrador ou administrador de cluster.
2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.

The screenshot shows the 'Environment Settings' page for an environment named 'res-gaenv1'. The 'Identity Provider' tab is selected, showing configuration for a Cognito Identity Provider. The 'Single Sign-On' section is also visible, showing that SSO is enabled.

Environment Settings		
Environment Name	AWS Region	S3 Bucket
res-gaenv1	us-east-1	res-gaenv1-cluster-us-east-1-088837573664
Identity Provider		
Provider Name	User Pool Id	Administrators Group Name
cognito-idp	us-east-1_reuFsm8SE	administrators-cluster-group
Managers Group Name	Domain URL	Provider URL
managers-cluster-group	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_reuFsm8SE
Single Sign-On		
Status	SAML Redirect URL	OIDC Redirect URL
Enabled	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com/saml2/idpresponse	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com/oauth2/idpresponse

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.

Single Sign On Configuration ✕

Identity Provider

Choose the third-party identity provider that you would like to configure.

SAML
Configure trust between Cognito and a SAML 2.0-compatible identity provider.

OIDC
Configure trust between Cognito and an OIDC identity provider,

Provider Name

Name used for the provider in cognito

Metadata Document Source

Provide a SAML metadata document. This document is issued by your SAML provider.

Upload metadata document

Enter metadata document endpoint URL

Metadata document

Provider Email Attribute

The Email attribute used to map email between your idp and the Amazon Cognito user pool

Refresh Token Expiration (hours)

Must be between 1 and 87600 (10 years)

- Em Identity Provider, escolha SAML.
- 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 XML documento de metadados ou forneça-o URL do provedor de identidade.
 - d. Em Atributo de e-mail do provedor, insira o valor do textoemail.
 - 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 RES ambiente 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 RES SSO habilitação 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. Selecione 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.

Attribute mapping (1) [Info](#) Edit

View, add, and edit attribute mappings between SAML and your user pool. < 1 > ⚙

User pool attribute	SAML attribute
email	email

Metadata document [Info](#) Replace metadata

View and update your SAML metadata. This document is issued by your SAML provider. It includes the issuer's name, expiration information, and keys that can be used to validate the response from the identity provider.

<p>Metadata document source Enter metadata document endpoint URL</p>	<p>Metadata document endpoint URL https://portal.sso.us-west-2.amazonaws.com/saml/metadata/MDg4ODM3NTczNjY0X2lucy04M2EyYUcyMGUzZTFIMDI4</p>
---	--

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, selecione 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.

▼ **Scan or query items**

Scan
 Query

Select a table or index: Table - res-jan19.cluster-settings
 Select attribute projection: All attributes

▼ **Filters** 6

Attribute name	Type	Condition	Value	
key	String	Equal to	identity-provider	Remove

Add filter

Run Reset 7

✔ Completed. Read capacity units consumed: 13
✕

Items returned (1)

- key (String)
- [identity-provider.cognito.ss](#)

Edit String ✕

email

Enter any string value.

Cancel
Save

Actions Create item

8 < 1 > ⚙ ✕

▼ | version ▼

1

Depurando problemas de SAML IdP

SAML-tracer — Você pode usar essa extensão no navegador Chrome para rastrear SAML solicitações e verificar os valores das SAML afirmações. Para obter mais informações, consulte [SAML-tracer](#) na loja virtual do Chrome.

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

Amazon CloudWatch Logs — Você pode verificar seus RES registros 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 SAML integração com o Amazon Cognito, [consulte SAML Adicionar provedores de identidade 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, selecione Redefinir senha do usuário.
3. Selecione o usuário e digite uma nova senha.
4. Escolha Redefinir senha.

Criação de subdomínios

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

Note

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

1. Abra o [console do Route 53](#).
2. Encontre o domínio que você criou e escolha Criar registro.
3. Insira 'web' como o nome do registro.
4. Selecione 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 oVDC, recupere o NLB endereço.
 - a. Abra o [console de AWS CloudFormation](#).

- b. Selecione `<environment-name>-vdc`.
 - c. Escolha Recursos e abra `<environmentname>-vdc-external-nlb`.
 - d. Copie o DNS nome doNLB.
8. Abra o [console do Route 53](#).
 9. Encontre seu domínio e escolha Criar registro.
 10. Em Nome do registro, insira `vdc`.
 11. Em Tipo de registro, selecione CNAME.
 12. Para oNLB, insira DNS o.
 13. Escolha Create record (Criar registro).

Crie um ACM certificado

Por padrão, 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 TLS certificado públicoSSL/fornecido por você ou solicitado de AWS Certificate Manager (ACM). Se você usarACM, receberá um nome de AWS recurso que precisará fornecer como parâmetro para criptografar o TLS canalSSL/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.

[Crie recursos externos](#)

Para criar um certificado para domínios personalizados:

1. No console, abra [AWS Certificate Manager](#) para 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` e `PortalDomainName`.
4. Em Método de validação, escolha DNSvalidação.

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 CNAME chave e o valor. 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 certificado ARN 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/ <i><installation-stack-name></i> -cluster-endpoints	Nunca expire
/aws/lambda/ <i><installation-stack-name></i> -cluster-manager-scheduled-ad-sync	Nunca expire
/aws/lambda/ <i><installation-stack-name></i> -cluster-settings	Nunca expire

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

Se você quiser alterar a retenção padrão de um grupo de registros, acesse o [CloudWatch console](#) 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 RES anexando limites de permissão personalizados. Um limite de permissão personalizado pode ser definido como parte

da RES AWS CloudFormation instalação fornecendo o limite de permissão ARN como parte do parâmetro. IAMPermissionBoundary Nenhum limite de permissão será definido em nenhuma RES função se esse parâmetro for deixado em branco. Abaixo está a lista de ações que as RES funções 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:*"
  ]
}
]
```

Pronto para configuração RES AMIs

Com o Amazon Machine Images (AMIs) RES pronto para uso, você pode pré-instalar RES dependências para instâncias de desktop virtual (VDIs) em suas instâncias personalizadas. AMIs O uso RES de -ready AMIs melhora os tempos de inicialização de VDI instâncias usando imagens pré-criadas. Usando o EC2 Image Builder, você pode criar e registrar suas pilhas de software AMIs como novas. 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 IAM função para acessar o RES ambiente](#)
- [Criar componente EC2 Image Builder](#)
- [Prepare sua receita do EC2 Image Builder](#)
- [Configurar a infraestrutura do EC2 Image Builder](#)
- [Configurar o pipeline de imagens do Image Builder](#)
- [Execute o pipeline de imagens do Image Builder](#)
- [Registre uma nova pilha de software no RES](#)

Prepare a IAM função para acessar o RES ambiente

Para acessar o serviço de RES ambiente a partir do EC2 Image Builder, você deve criar ou modificar uma IAM função chamada RES -EC2InstanceProfileForImageBuilder. Para obter informações sobre como configurar uma IAM função 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 EC2 serviço Amazon.
- A mazonSSMManaged InstanceCore e EC2InstanceProfileForImageBuilder políticas.
- RESPolítica personalizada com acesso limitado do DynamoDB e do Amazon S3 ao ambiente implantado. RES

(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"
    }
  ]
}
```

RESpolítica:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RES DynamoDB Access",
      "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.*",
            "vdc.host_modules.*"
          ]
        }
      }
    },
    {
      "Sid": "RES S3 Access",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": [
        "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-Account-ID}/idea/vdc/res-ready-install-script-packages/*",

```

```

        "arn:aws:s3:::research-engineering-studio-{AWS-Region}/host_modules/*"
    ]
}
]
}

```

Criar 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 YAML arquivo 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_{{ RESEnvReleaseVersion }}.tar.gz'
          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


Uma receita 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 o destino AMI com as dependências de RES software necessárias. Para obter mais informações sobre receitas, consulte [Gerenciar receitas](#).

RESsuporta os seguintes sistemas operacionais de imagem:

- Amazon Linux 2 (x86 eARM64)
- Ubuntu 22.04.3 (x86)
- RHEL8 (x86) e 9 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe


1. Abra o console do EC2 Image Builder em <https://console.aws.amazon.com/imagebuilder>.
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. Selecione uma imagem base suportada porRES.
6. Em Configuração da instância, instale um SSM agente 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 SSM agente, consulte:

- [Instalação manual do SSM Agente em EC2 instâncias para Linux.](#)
- [Instalação e desinstalação manual do SSM Agente em EC2 instâncias do Windows Server.](#)

7. Para receitas baseadas em Linux, adicione o componente de `aws-cli-version-2-linux` compilação gerenciado pela Amazon à receita. RESos scripts de instalação usam o AWS CLI para fornecer VDI acesso 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: `AWSAccountIDRESEnvName`, `RESEnvRegion`, e `RESEnvReleaseVersion`

 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 ele AMI pode ser lançado. 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. RESos scripts de instalação usam o AWS CLI para fornecer VDI acesso 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: `AWSAccountIDRESEnvName`, `RESEnvRegion`, e `RESEnvReleaseVersion`

 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 EC2 infraestrutura da Amazon que o Image Builder usa para criar e testar sua imagem do Image Builder. Para usar 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. Em IAM função, insira a função na qual você configurou anteriormente [Prepare a IAM função para acessar o RES ambiente](#).
2. Em Tipo de instância, escolha um tipo com pelo menos 4 GB de memória e compatível com a AMI arquitetura base escolhida. Veja os [tipos de EC2 instância da Amazon](#).
3. Para VPC grupos de sub-rede e 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 RES -readyAMIs, você pode optar por criar um novo pipeline ou usar um existente. Para obter mais informações, consulte [Criar e atualizar pipelines de AMI imagem](#) no Guia do usuário do Image Builder.

Create a new Image Builder pipeline

1. Abra o console do Image Builder em <https://console.aws.amazon.com/imagebuilder>.
2. No painel de 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 em [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 em [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 RES ambiente. 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 em [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 em [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 AMIID, insira o AMI ID da imagem de saída incorporada [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 segredos](#)
- [Monitoramento e controle de custos](#)
- [Gerenciamento de sessões](#)
- [Gestão do meio ambiente](#)

Gerenciamento de segredos

O Research and Engineering Studio mantém os seguintes segredos usando AWS Secrets Manager. REScria 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	RESgerado	Administrador inserido
<code><envname> -sso-client-secret</code>	Segredo do OAuth2 cliente de login único para o ambiente	✓	
<code><envname> -vdc-client-secret</code>	vdc ClientSecret	✓	
<code><envname> -vdc-client-id</code>	vdc ClientId	✓	
<code><envname> -vdc-gateway-certificate-private-key</code>	Chave privada de certificado autoassinada para domínio	✓	
<code><envname> -vdc-gateway-</code>	Certificado autoassinado para domínio	✓	

Nome de segredo	Descrição	RESgerado	Administrador inserido
certificate-certificate			
<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> -external-certificate	Certificado autoassinado para domínio	✓	
<envname> -internal-private-key	Chave privada de certificado autoassinada para domínio	✓	
<envname> -internal-certificate	Certificado autoassinado para domínio	✓	
<envname> -director-service-ServiceAccountUserDN	O atributo Nome Distinto (DN) do ServiceAccount usuário.	✓	

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

Chave	Origem
<code>identity-provider.cognito.sso_client_secret</code>	
<code>vdc.dcv_connection_gateway.certificates.certificate_secret_arn</code>	stack (pilha)
<code>vdc.dcv_connection_gateway.certificates.private_key_secret_arn</code>	stack (pilha)
<code>cluster.load_balancers.internal_alb.certificates.private_key_secret_arn</code>	stack (pilha)
<code>directoryservice.root_username_secret_arn</code>	
<code>vdc.client_secret</code>	stack (pilha)
<code>cluster.load_balancers.external_alb.certificates.certificate_secret_arn</code>	stack (pilha)
<code>cluster.load_balancers.internal_alb.certificates.certificate_secret_arn</code>	stack (pilha)
<code>directoryservice.root_password_secret_arn</code>	
<code>cluster.secretsmanager.kms_key_id</code>	
<code>cluster.load_balancers.external_alb.certificates.private_key_secret_arn</code>	stack (pilha)
<code>cluster-manager.client_secret</code>	

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 dos [the section called “AWS serviços neste produto”](#).

Para ajudar no controle de custos, você pode associar RES projetos 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` e `res:EnvironmentName` tags e.
4. Selecione Ativar.

The screenshot shows the AWS Billing console interface for 'Cost allocation tags'. The left sidebar contains navigation options like 'Billing', 'Cost Management', and 'Preferences'. The main content area is titled 'Cost allocation tags' and shows 'Cost allocation tags activated: 3'. There are two tabs: 'User-defined cost allocation tags' (selected) and 'AWS generated cost allocation tags'. A search bar contains 'res' and shows '11 matches'. A table lists various tags with columns for 'Tag key', 'Status', 'Last updated date', and 'Last used month'. The 'res:EnvironmentName' and 'res:Project' tags are checked in the 'Tag key' column. The 'Activate' button is highlighted in the top right corner of the table area.

Tag key	Status	Last updated date	Last used month
<input type="checkbox"/> res:BackupPlan	Inactive	-	November 2023
<input type="checkbox"/> res:ClusterName	Inactive	-	November 2023
<input type="checkbox"/> res:DCVSessionUUID	Inactive	-	November 2023
<input type="checkbox"/> res:EndpointName	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:EnvironmentName	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleId	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleName	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleVersion	Inactive	-	November 2023
<input type="checkbox"/> res:NodeType	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:Project	Inactive	-	November 2023

Note

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


Para criar um orçamento para RES recursos:

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.

The screenshot shows the AWS Billing console interface for creating a budget. On the left is a navigation sidebar with categories like Billing, Cost Management, Preferences, and Permissions. The 'Budgets' link is highlighted with a red circle '1'. The main content area is titled 'Choose budget type' and includes a progress bar with five steps: 'Choose budget type', 'Set your budget', 'Configure alerts', 'Attach actions', and 'Review'. The 'Budget setup' section offers two options: 'Use a template (simplified)' and 'Customize (advanced)', with the latter selected and marked with a red circle '3'. The 'Budget types' section offers four options: 'Cost budget - Recommended', 'Usage budget', 'Savings Plans budget', and 'Reservation budget', with the first one selected and marked with a red circle '4'. At the bottom right, there are 'Cancel' and 'Next' buttons, with 'Next' highlighted and marked with a red circle '5'.

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 X

Cancel

Apply filter

Add filter

Advanced options

Aggregate costs by

Unblended costs

Supported charge types

Upfront reservation fees X

Recurring reservation charges X

Other subscription costs X

Taxes X

Support charges X

Discounts X

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.

The screenshot shows the 'Projects' page in the deRES interface. The breadcrumb is 'RES > Environment Management > Projects'. The page title is 'Projects' and the subtitle is 'Environment Project Management'. There is a search bar and a 'Create Project' button. Below is a table with the following data:

Title	Project Code	Status	Budgets	Groups	Updated On
project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 Budget Exceeded Limit: 500.00 USD, Forecasted: 3945.34 USD	<ul style="list-style-type: none"> • DemoUsers • DemoAdmins • ProductUsers 	10/31/2023, 12:44:12 PM

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 dentro de RES. Como alternativa, você pode editar um projeto para desativar um orçamento.

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](#)
- [Sessões](#)

- [Pilhas de software \(\) AMIs](#)
- [Depuração](#)
- [Configurações da área de trabalho](#)

Painel

Research and Engineering Studio demoadmin1

res-stage (us-west-2) RES > Virtual Desktop > Dashboard

Virtual Desktop Dashboard

1 Instance Types Summary of all virtual desktop sessions by instance types.

Instance Type	Count
m6a.large	3

2 Session State Summary of all virtual desktop sessions by state.

Session State	Count
STOPPING	3

3 Base OS Summary of all virtual desktop sessions by Base OS.

Base OS	Count
Amazon Linux 2	2
Windows	1

4 Project Summary of all virtual desktop sessions by Project Code.

Project Code	Count
project1	3

5 Availability Zones Summary of all virtual desktop sessions by Availability Zone.

Availability Zone	Count
us-west-2a	3

6 Software Stacks Summary of all virtual desktop sessions by Software Stack.

Software Stack	No. of Sessions
Amazon Linux 2 - x86_64	2
Windows - x86_64	1

7 **8** [View 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.

RES > Virtual Desktops > Sessions

Sessions (2)

Virtual Desktop sessions for all users. End-users see these sessions as Virtual Desktops.

Created ▾ Last 1 month 1 Actions ▾ Create Session 3

Search 4 All States ▾ All Operating Systems ▾ < 1 > ⚙

<input type="checkbox"/>	Session Name ▾	Owner ▾	Base OS	Instance Ty...	State	Project	Created On
<input checked="" type="checkbox"/>	demoadmin1aml21 5	demoadmin1	Amazon Linux 2	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:31:50 AM
<input type="checkbox"/>	demoadmin1windows1	demoadmin1	Windows	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:38:23 AM

< 1 >

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. Selecione 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 DCV sessão.
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

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

Detalhes da sessão

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

RES > Virtual Desktop > Sessions > 8765705b-8919-48ba-901a-19e2c49cf043

Session: demoadmin1aml21

General Information

Session Name	Owner	State
demoadmin1aml21	demoadmin1	Stopped

< **Details** | Server | Software Stack | Project | Permissions | Schedule | Monitoring | Session | >

Session Details

RES Session Id	DCV Session Id	Description
8765705b-8919-48ba-901a-19e2c49cf043	bd63e69a-e75a-427b-b4c8-39d7c43b95ad	-
Session Type	Hibernation Enabled	Created On
VIRTUAL	No	9/27/2023, 8:31:50 AM
Updated On		
9/29/2023, 11:01:20 PM		

Pilhas de software () AMIs

Note

Para executar a pilha de SO7 software Cent fornecida AWS GovCloud (US), você precisará se inscrever AWS Marketplace usando AMI sua [conta padrão vinculada](#).

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

RES > Virtual Desktops > Software Stacks (AMIs)

Software Stacks

Manage your Virtual Desktop Software Stacks

Search All Operating Systems ▼

Actions ▼ Register Software Stack

Name	Description	AMI ID	Base OS	Root Volume Size	Min RAM	GPU Manufacturer	Created On
<input type="radio"/> CentOS7 - ARM64	CentOS7 - ARM64	ami-07f692d95b2b9c8c5	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> CentOS7 - x86_64	CentOS7 - x86_64	ami-00f8e2c955f7ffa9b	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> RHEL8 - x86_64	RHEL8 - x86_64	ami-0b530377951178d6b	RedHat Enterprise Linux 8	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> UBUNTU2204 - x86_64	UBUNTU2204 - x86_64	ami-073ffe13d826b7f8	Ubuntu 22.04	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> RHEL7 - x86_64	RHEL7 - x86_64	ami-0bb2449c2217cb9b0	RedHat Enterprise Linux 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Windows - x86_64	Windows - x86_64	ami-0667133d0dc6089e1	Windows	30GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Windows - AMD	Windows - AMD	ami-05df91be1d294f195	Windows	30GB	4GB	AMD	6/7/2024, 11:25:20 AM
<input type="radio"/> Windows - NVIDIA	Windows - NVIDIA	ami-00d7af9d003819a90	Windows	30GB	4GB	NVIDIA	6/7/2024, 11:25:20 AM
<input type="radio"/> RHEL9 - x86_64	RHEL9 - x86_64	ami-099f85fc24d27c2a7	RedHat Enterprise Linux 9	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Amazon Linux 2 - ARM64	Amazon Linux 2 - ARM64	ami-04ed2b27d86c17f09	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Amazon Linux 2 - x86_64	Amazon Linux 2 - x86_64	ami-0ee5c62243ab25259	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM

1. Para pesquisar uma pilha de software existente, use o menu suspenso do sistema operacional para filtrar por sistema operacional.
2. Selecione 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

GPU Manufacturer

Select the GPU Manufacturer for the software stack

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

Projects

Select applicable projects for the software stack

Atribuir pilha de software a um projeto

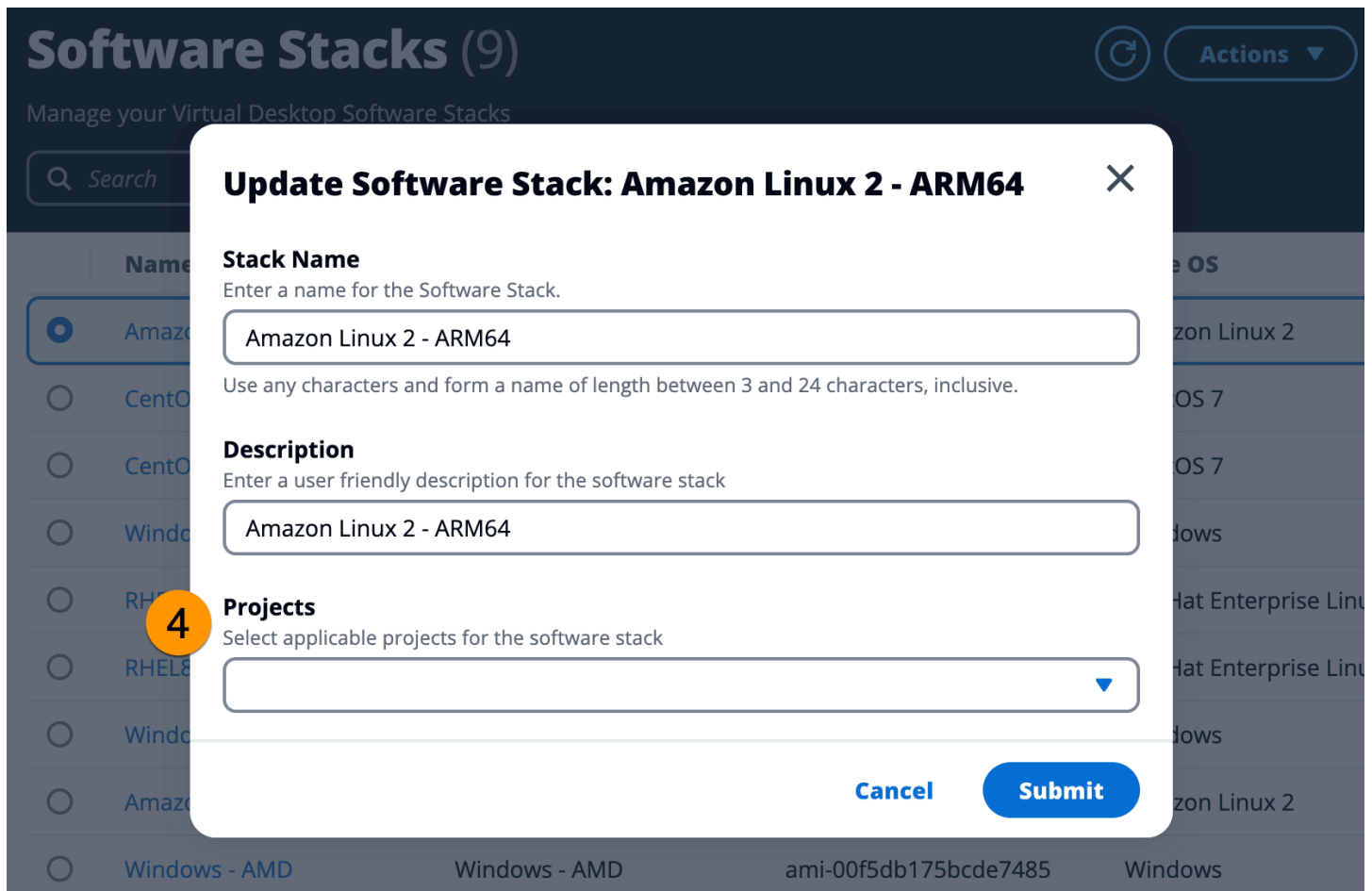
Ao criar uma nova pilha de software, você pode atribuir a pilha aos projetos. Se você precisar adicionar a pilha a um projeto após a criação inicial, faça o seguinte:

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.

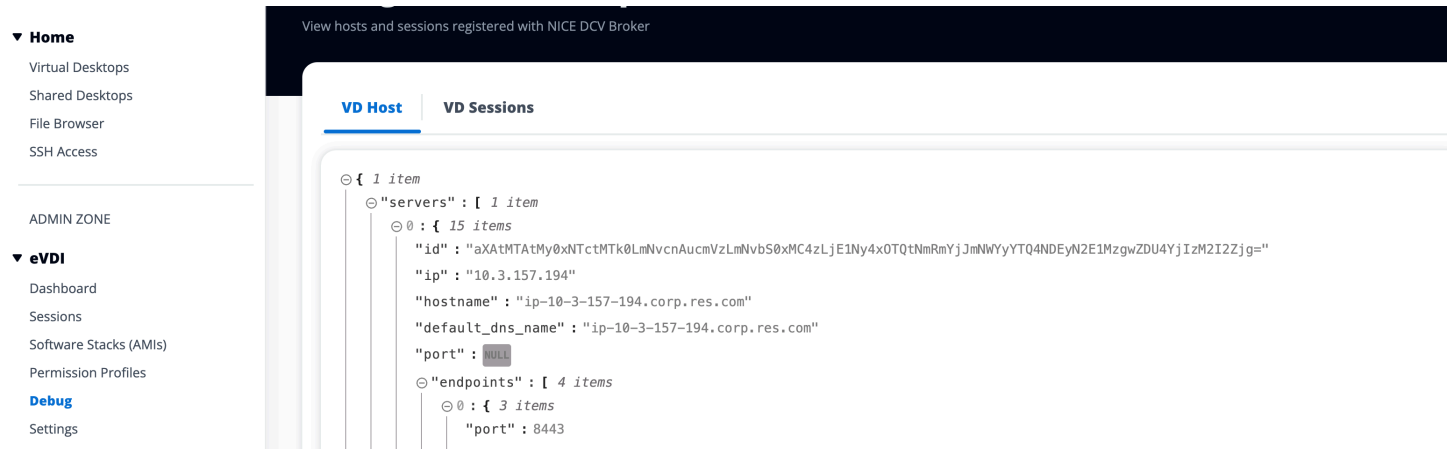


Veja os detalhes da pilha de software

Na lista Pilhas de software, selecione 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.

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:

DCVtempo limite de inatividade da sessão

O tempo após o qual a DCV sessão será automaticamente desconectada. Isso não altera o estado da sessão do desktop, apenas fecha a sessão do DCV cliente ou do navegador da web.

Aviso de tempo limite de inatividade

O tempo após o qual um aviso de inatividade será fornecido ao cliente.

CPUlimite de utilização

A CPU utilização deve ser considerada ociosa.

Sessões permitidas por usuário

O número de VDI sessões que um usuário individual pode ter em um determinado momento. Se um usuário atingir ou exceder esse valor, isso impedirá que ele inicie novas sessões na página Meus desktops virtuais. A capacidade de iniciar sessões por meio da página Sessões não é afetada por esse valor.

Tamanho máximo do volume da raiz

O tamanho padrão do volume raiz em sessões de desktop virtual.

Tipos de instância permitidos

A lista de famílias e tamanhos de instâncias que podem ser lançados para esse RES ambiente. As combinações de família e tamanho de instâncias são aceitas. Por exemplo, se você

especificar 'm7a', todos os tamanhos da família m7a estarão disponíveis para lançamento como sessões. VDI Se você especificar 'm7a.24xlarge', somente m7a.24xlarge estará disponível para lançamento como uma sessão. VDI Essa lista afeta todos os projetos no ambiente.

The screenshot displays the 'Virtual Desktop Settings' page for the 'res-beta08 (us-east-2)' environment. The page is divided into several sections: 'DCV Session' and 'DCV Host'. The 'DCV Session' section includes 'Idle Timeout' (1440 minutes), 'Idle Timeout Warning' (300 seconds), and 'CPU Utilization Threshold' (30%). The 'DCV Host' section includes 'Allowed Security Groups' (empty), 'Allowed Instance Types' (a1.metal, c4.xlarge, g4ad, m6a, m6g, t3, g6-12xlarge), 'Max Root Volume Size' (100 GB), and 'Denied Instance Types' (empty). The page also shows a navigation menu on the left with categories like 'Desktops', 'Session Management', and 'Environment Management'.

Gestão do meio ambiente

Na seção Gerenciamento ambiental doRES, 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

- [Status do ambiente](#)
- [Configurações de ambiente](#)
- [Usuários](#)
- [Grupos](#)
- [Projetos](#)
- [Política de permissão](#)
- [Sistemas de arquivos](#)
- [Gerenciamento de instantâneos](#)
- [Buckets do Amazon S3](#)

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.

Research and Engineering Studio demoadmin4

RES > Environment Management > Status

Environment Status

[View Environment Settings](#)

Modules

Environment modules and status

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

Infrastructure Hosts

Cluster hosts and status

Instance Name	Module ID	Node Type	Version	Instance Type	Availability Zone	Instance State	Private IP	Public IP
res-demo2-bastion-host	bastion-host	Infra	2023.10	m5.large	us-east-2a	Running	10.1.3.148	3.145.15
res-demo2-vdc-controller	vdc	App	2023.10	m5.large	us-east-2a	Running	10.1.129.105	-
res-demo2-vdc-broker	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.149.12	-
res-demo2-cluster-manager	cluster-manager	App	2023.10	m5.large	us-east-2b	Running	10.1.155.249	-
res-demo2-vdc-gateway	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.153.135	-

Configurações de ambiente

A página de configurações do ambiente exibe 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 VPC ID, lista de IDs prefixos para acesso.

- Directory Service

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

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.

Research and Engineering Studio

RES > Environment Management > Users

Users

Environment user management

1 Search

2 Actions

- Set as Admin User
- Disable User

	Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
<input checked="" type="radio"/>	demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> IDEAUsers DemoUsers
<input type="radio"/>	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> SAUsers
<input type="radio"/>	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers
<input type="radio"/>	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> ProductUsers

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.

Research and Engineering Studio

RES > Environment Management > Groups

Groups

Environment user group management

Search

Title	Group Name	Type	Role	Status	GID
IDEAUsers	IDEAUsers	external	user	Enabled	4000
SAdmins	SAdmins	external	user	Enabled	3035
AWS Delegated Administrators	AWS Delegated Administrators	external	admin	Enabled	3999

Users in IDEAUsers

Username	UID	GID	Email	Is Sudo?	Role	Is Active	Status	Groups	Syn
demoadmin1	3000	3000	demoadmin1@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers 	10/3
demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers SAdmins 	10/3

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.

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](#)
- [Criar um projeto](#)

- [Editar um projeto](#)
- [Adicionar ou remover tags de um projeto](#)
- [Exibir sistemas de arquivos associados a um projeto](#)
- [Adicionar um modelo de lançamento](#)

Exibir projetos

The screenshot shows the 'Projects' panel in the Research and Engineering Studio. The panel has a dark theme and includes a search bar (1), a table of projects, and an actions menu (2) with a 'Create Project' button (3).

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUUsers	10/3/2023, 7:04:18 PM

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, consulte [Adicionar 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. O sistema de arquivos do diretório inicial pode usar o Sistema de Arquivos Pessoal Compartilhado (padrão)EFS, FSx para Lustre ou armazenamento em volume. FSx NetApp ONTAP EBS

É importante observar que o sistema de arquivos doméstico compartilhado,, EFS FSx para Lustre, FSx NetApp ONTAP pode ser compartilhado em vários projetos e. VDIs No entanto, a opção de armazenamento VDI em EBS volume exigirá que cada membro desse projeto tenha seu próprio diretório inicial que não seja compartilhado entre outros VDIs projetos.

Create new Project

Project Definition

Title

Enter a user friendly project title

Project ID

Enter a project-id

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (_), or periods (.). Must be between 3 and 40 characters long.

Description

Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

Storage resources

Add file systems and/or S3 buckets to the project.

**Home directory filesystem**

Select the filesystem that will be used to create the user home directories on Linux desktops.

**► Advanced Options**

- Atribua aos usuários e/ou grupos a função apropriada (“Membro do projeto” ou “Proprietário do projeto”). Veja [Perfis de permissões padrão](#) as ações que cada função pode realizar.
- Selecione Enviar.

Create new Project

Project Definition

Title
Enter a user friendly project title

Project ID
Enter a project-id

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (_), or periods (.). Must be between 3 and 40 characters long.

Description
Enter the project description

Enter Description ...

Do you want to enable budgets for this project?

Resource Configurations

Add file systems
Select applicable file systems for the Project

home [efs] X

▶ **Advanced Options**

Team Configurations

Groups Select applicable ldap groups for the Project	Role Choose a role for the group	Remove group
group_1	Project Member	
Add group		
Users Select applicable users for the Project	Role Choose a role for the user	Remove user
user1	Project Member	
Add user		

Cancel **Submit**

Editar um projeto

- Selecione um projeto na lista de projetos.
- No menu Ações, escolha Editar projeto.
- Insira suas atualizações. Se você pretende habilitar orçamentos, consulte [Monitoramento e controle de custos](#) para obter mais informações. Para obter informações sobre opções avançadas, consulte [Adicionar um modelo de lançamento](#).
- Selecione Enviar.

Edit Project

Project Definition

Title
Enter a user friendly project title

Project ID
Enter a project-id

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (_), or periods (.). Must be between 3 and 40 characters long.

Description
Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

▼ **Advanced Options**

Add Policies
Select applicable policies for the Project

Add Security Groups
Select applicable security groups for the Project

► **Linux**

► **Windows**

Team Configurations

Groups Select applicable ldap groups for the Project	Role Choose a role for the group	<input type="button" value="Remove group"/>
<input type="text" value="group_1"/> <input type="button" value="Add group"/>	<input type="text" value="Project Member"/> <input type="button" value="Remove group"/>	
Users Select applicable users for the Project	Role Choose a role for the user	<input type="button" value="Remove user"/>
<input type="text" value="user1"/> <input type="button" value="Add user"/>	<input type="text" value="Project Member"/> <input type="button" value="Remove user"/>	

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.

The screenshot shows the 'Projects' management interface. At the top, there's a header with 'Projects' and 'Environment Project Management'. A search bar is present. Below the header is a table of projects. One project, 'project-1', is selected. Below the table, a panel titled 'File Systems in project-1' is expanded, showing a table with columns: Title, Name, File System ID, Mount Target, Projects, Scope, Provider, and Created through RES?. The table currently shows 'No records'.

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUsers	10/3/2023, 9:06:30 PM

Title	Name	File System ID	Mount Target	Projects	Scope	Provider	Created through RES?
No records							

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, IAM políticas e scripts de lançamento para todas as VDI instâncias do projeto.

Adicionar políticas

Você pode adicionar uma IAM política para controlar o VDI acesso de 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 IAM funções, consulte [Políticas e permissões em IAM](#).

Adição de grupos de segurança

Você pode adicionar um grupo de segurança para controlar os dados de saída e entrada de todas as VDI instâncias do 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 VPC do usuário da Amazon.

Adicionar scripts de lançamento

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

Execute o script ao VDI iniciar

Essa opção inicia o script no início de uma VDI instância antes da execução de qualquer RES configuração ou instalação.

Executar script quando VDI estiver configurado

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

Os scripts oferecem suporte às seguintes opções:

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

Para Argumentos, forneça quaisquer argumentos separados por uma vírgula.

▼ Linux

Run Script When VDI Starts
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="https://sample.samplecontent.com/sample"/>	<input type="text"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="file:///root/bootstrap/latest/launch/script"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Run Script when VDI is Configured
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

▼ Windows

Run Script When VDI Starts
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Run Script when VDI is Configured
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Exemplo de uma configuração de projeto

Política de permissão

O Research and Engineering Studio (RES) permite que um usuário administrativo crie perfis de permissão personalizados que concedem aos usuários selecionados permissões adicionais para gerenciar o projeto do qual fazem parte. Cada projeto vem com dois [perfis de permissão padrão](#): “Membro do projeto” e “Proprietário do projeto”, que podem ser personalizados após a implantação.

Atualmente, os administradores podem conceder duas coleções de permissões usando um perfil de permissão:

1. Permissões de gerenciamento de projetos que consistem em “Atualizar a associação do projeto”, que permite que um usuário designado adicione outros usuários e grupos ou os remova de um projeto, e “Atualizar o status do projeto”, que permite que um usuário designado ative ou desative um projeto.
2. VDIpermissões de gerenciamento de sessão que consistem em “Criar sessão”, que permite que um usuário designado crie uma VDI sessão em seu projeto, e “Criar/encerrar a sessão de outro usuário”, que permite que um usuário designado crie ou encerre as sessões de outros usuários em um projeto.

Dessa forma, os administradores podem delegar permissões baseadas em projetos a não administradores em seu ambiente.

Tópicos

- [Permissões de gerenciamento de projetos](#)
- [VDIpermissões de gerenciamento de sessão](#)
- [Gerenciando perfis de permissão](#)
- [Perfis de permissões padrão](#)
- [Limites do ambiente](#)
- [Perfis de compartilhamento de desktop](#)

Permissões de gerenciamento de projetos

Atualizar a associação ao projeto

Essa permissão permite que usuários não administradores que a receberam adicionem e removam usuários ou grupos de um projeto. Também permite que eles definam o perfil de permissão e decidam o nível de acesso para todos os outros usuários e grupos desse projeto.

Team Configurations

Groups Info

group_1 ▼

group_2 ▼

[Add group](#)

No users attached. Click 'Add user' below to get started.

[Add user](#)

Permission profile Info

Project Owner ▼

Project Member ▼

⚠ Users/groups assigned to this permission profile can grant themselves or others higher privileges for this project by re-assigning personnel to a different permission profile

[Remove](#)

[Remove](#)

[Cancel](#) [Submit](#)

Atualizar o status do projeto

Essa permissão permite que usuários não administradores que a receberam habilitem ou desabilitem um projeto usando o botão Ações na página Projetos.

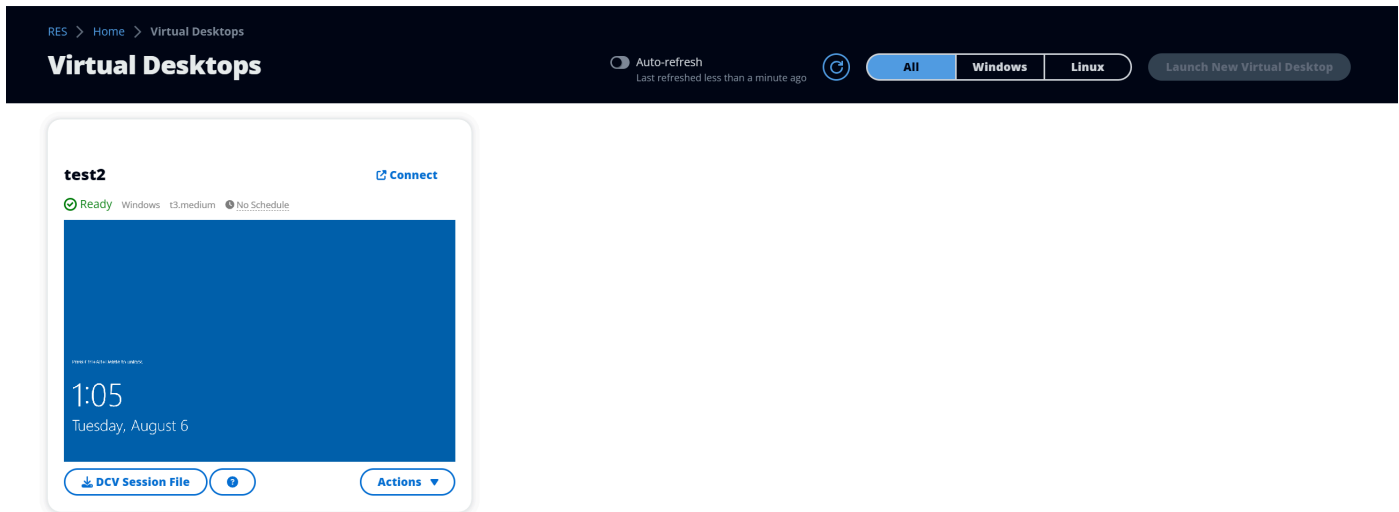
Title	Project Code	Status	Budgets	Groups	Users	Updated On
project2	Project2	Enabled	--	• group_2	• user1	7/15/2024, 11:45:22 AM
project3	Project3	Enabled	--	• group_1 • group_2	-	7/15/2024, 8:05:20 AM

VDIpermissões de gerenciamento de sessão

Crie uma sessão.

Controla se um usuário tem permissão ou não para iniciar sua própria VDI sessão na página Meus desktops virtuais. Desative essa opção para impedir que usuários não administradores iniciem suas próprias VDI sessões. Os usuários sempre podem parar e encerrar suas próprias VDI sessões.

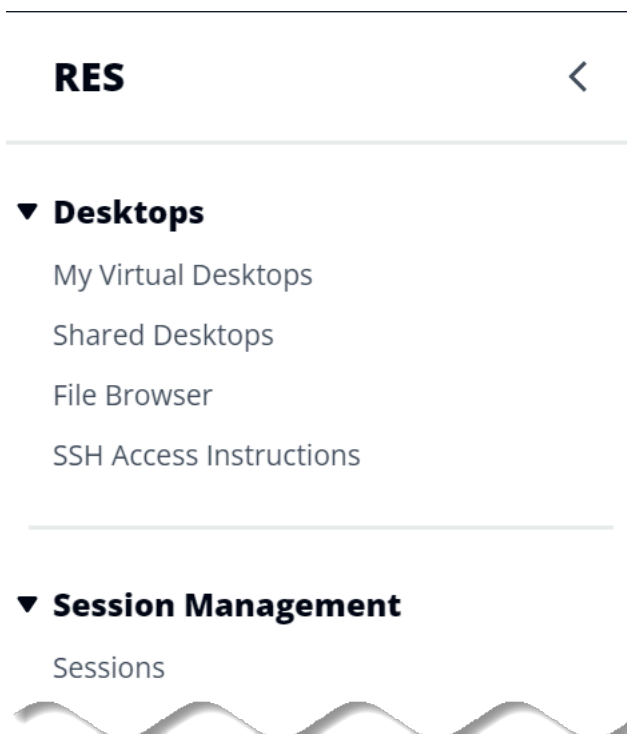
Se um usuário não administrador não tiver permissões para criar uma sessão, o botão Iniciar nova área de trabalho virtual será desativado para ele, conforme mostrado aqui:



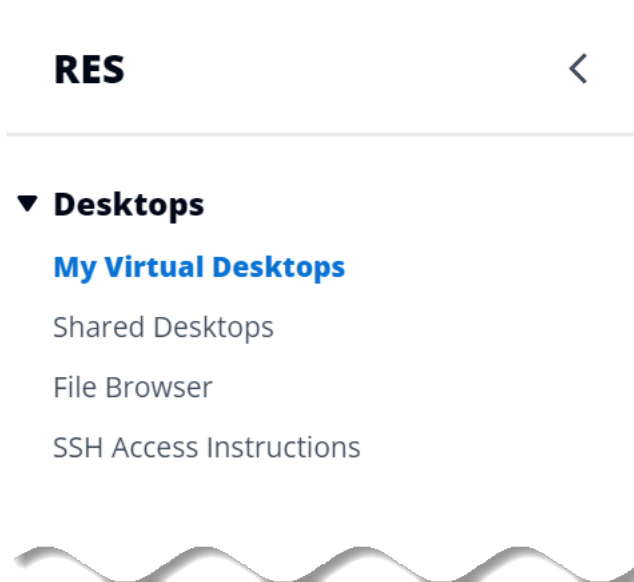
Crie ou encerre as sessões de outras pessoas

Permite que usuários não administradores acessem a página Sessões a partir do painel de navegação esquerdo. Esses usuários poderão iniciar VDI sessões para outros usuários nos projetos em que receberam essa permissão.

Se um usuário não administrador tiver permissão para iniciar sessões para outros usuários, o painel de navegação esquerdo exibirá o link Sessões em Gerenciamento de sessões, conforme mostrado aqui:



Se um usuário não administrador não tiver permissão para criar sessões para outras pessoas, seu painel de navegação esquerdo não exibirá o Gerenciamento de Sessões, conforme mostrado aqui:

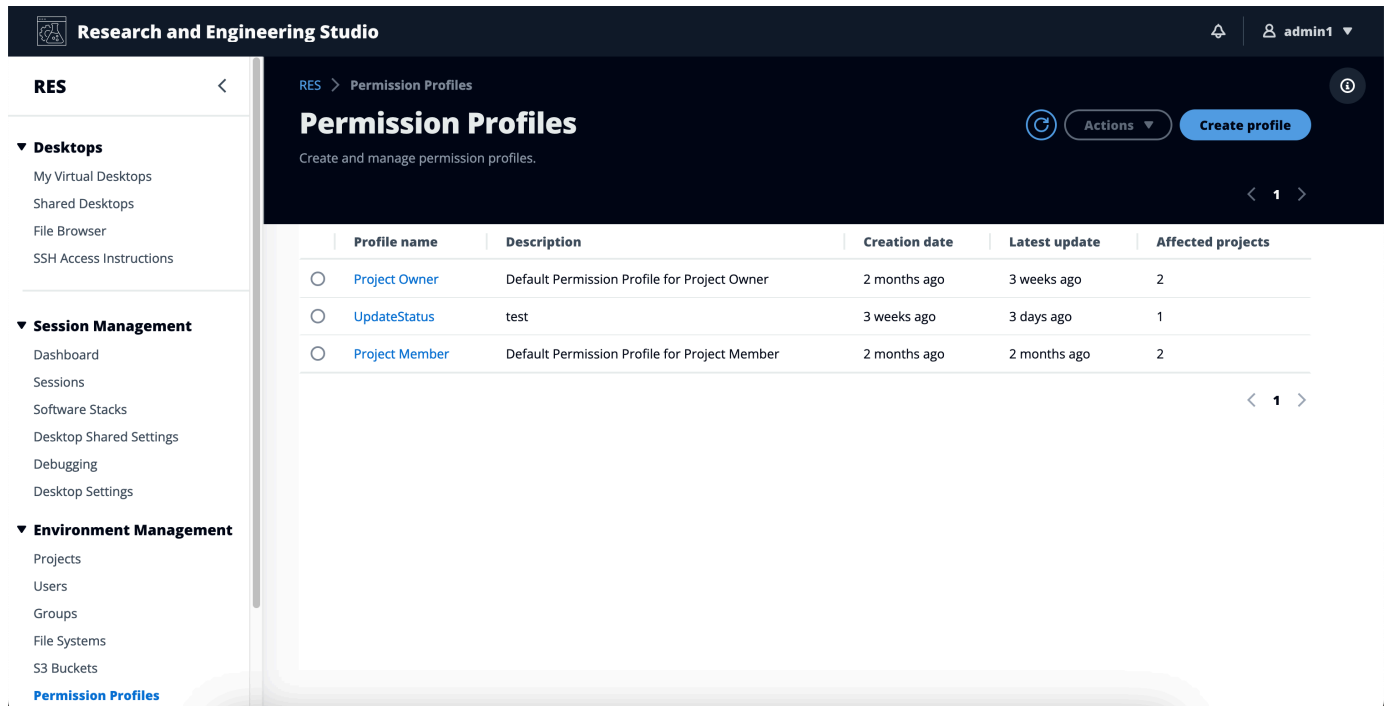


Gerenciando perfis de permissão

Como RES administrador, você pode realizar as seguintes ações para gerenciar perfis de permissão.

Listar perfis de permissão

- Na página do console do Research and Engineering Studio, escolha Perfis de permissão no painel de navegação esquerdo. Nessa página, você pode criar, atualizar, listar, visualizar e excluir perfis de permissão.



The screenshot shows the 'Permission Profiles' page in the Research and Engineering Studio. The page has a dark header with the studio name and a user profile 'admin1'. A left sidebar contains navigation options under 'RES', including Desktops, Session Management, and Environment Management. The main content area features a title 'Permission Profiles' and a subtitle 'Create and manage permission profiles.' Below this is a table with the following data:

	Profile name	Description	Creation date	Latest update	Affected projects
<input type="radio"/>	Project Owner	Default Permission Profile for Project Owner	2 months ago	3 weeks ago	2
<input type="radio"/>	UpdateStatus	test	3 weeks ago	3 days ago	1
<input type="radio"/>	Project Member	Default Permission Profile for Project Member	2 months ago	2 months ago	2

Exibir perfis de permissão

1. Na página principal de Perfis de permissão, selecione o nome do perfil de permissão que você deseja visualizar. Nessa página, você pode editar ou excluir o perfil de permissão selecionado.

RES > Permission Profiles > Project Owner

Project Owner

Edit Delete

General Settings

Profile ID project_owner	Description Default Permission Profile for Project Owner	Creation date 3 weeks ago
		Latest update 3 weeks ago

Permissions Affected projects

Permissions (4)

Permissions granted to this permission profile.

Project management permissions (selected 2/2)

Update project membership Update users and groups associated with a project. Enabled	Update project status Enable or disable a project. Enabled
---	---

VDI session management permissions (selected 2/2)

Create session Create your own session. Users can always terminate their own sessions with or without this permission. Enabled	Create/Terminate other's session Create/Terminate another user's session within a project. Enabled
---	---

- Selecione a guia Projetos afetados para ver os projetos que atualmente usam o perfil de permissão.

RES > Permission Profiles > Project Owner

Project Owner

Edit Delete

General Settings

Profile ID project_owner	Description Default Permission Profile for Project Owner	Creation date 2 months ago
		Latest update 4 hours ago

Permissions Affected projects

Affected projects (2)

List of projects using this permission profile.

Project name	Groups	Users
Project1	1	2
Project3	2	0

Crie perfis de permissão

1. Na página principal de Perfis de permissão, escolha Criar perfil para criar um perfil de permissão.
2. Insira um nome e uma descrição do perfil de permissão e selecione as permissões a serem concedidas aos usuários ou grupos que você atribui a esse perfil.

RES > Permission Profiles > Create Profile

Create permission profile

Permission profile definition

Profile name
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

Profile description
Optionally add more details to describe the specific profile

Enter Profile description ...

Permissions
Permissions granted to this permission profile.

Project management permissions

Update project membership Update users and groups associated with a project. <input type="checkbox"/>	Update project status Enable or disable a project. <input type="checkbox"/>
--	--

VDI session management permissions

Create session Create a session within a project. <input type="checkbox"/>	Create/Terminate other's session Create/Terminate another user's session within a project. <input type="checkbox"/>
---	--

Cancel Create profile

Editar perfis de permissão

- Na página principal de Perfis de permissão, selecione um perfil clicando no círculo ao lado dele, escolha Ações e escolha Editar perfil para atualizar esse perfil de permissão.

RES > Permission Profiles > Project Member > Edit

Edit Project Member

Permission profile definition

Profile name
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

Profile description
Optionally add more details to describe the specific profile

Permissions

Permissions granted to this permission profile.

Project management permissions

Update project membership Update users and groups associated with a project. <input type="checkbox"/>	Update project status Enable or disable a project. <input type="checkbox"/>
--	--

VDI session management permissions

Create session Create your own session. Users can always terminate their own sessions with or without this permission. <input checked="" type="checkbox"/>	Create/Terminate other's session Create/Terminate another user's session within a project. <input type="checkbox"/>
---	--

[Cancel](#) [Save changes](#)

Excluir perfis de permissão

- Na página principal de Perfis de Permissão, selecione um perfil clicando no círculo ao lado dele, escolha Ações e escolha Excluir perfil. Você não pode excluir um perfil de permissão usado por nenhum projeto existente.

The screenshot shows the 'Permission Profiles' page in the RES interface. A green notification bar at the top states: '1 permission profile deleted successfully. This deletion did not impact any ongoing projects.' The page title is 'Permission Profiles' with a subtitle 'Create and manage permission profiles.' Below the title is a table with the following data:

Profile name	Description	Creation date	Latest update	Affected projects
Project Owner	Default Permission Profile for Project Owner	2 months ago	3 minutes ago	2
Project Member	Default Permission Profile for Project Member	2 months ago	2 months ago	2

Perfis de permissões padrão

Cada RES projeto vem com dois perfis de permissão padrão que os administradores globais podem configurar. (Além disso, os administradores globais podem criar e modificar novos perfis de permissão para um projeto.) A tabela a seguir mostra as permissões permitidas para os perfis de permissão padrão: “Membro do projeto” e “Proprietário do projeto”. Os perfis de permissão e as permissões que eles concedem a usuários selecionados de um projeto só se aplicam ao projeto ao qual pertencem; os administradores globais são superusuários que têm todas as permissões abaixo em todos os projetos.

Permissões	Descrição	Membro do projeto	Proprietário do projeto	
Criar sessão	Crie sua própria sessão. Os usuários sempre podem interromper e encerrar suas próprias sessões com	X	X	

Permissões	Descrição	Membro do projeto	Proprietário do projeto
	ou sem essa permissão.		
Criar/encerrar sessões de outras pessoas	Crie ou encerre a sessão de outro usuário em um projeto.		X
Atualizar associação ao projeto	Atualize usuários e grupos associados a um projeto.		X
Atualizar status do projeto	Ative ou desative um projeto.		X

Limites do ambiente

Os limites do ambiente permitem que os administradores configurem permissões que entrarão em vigor globalmente para todos os usuários. Isso inclui permissões como acesso ao Navegador de Arquivos e Permissões de Desktop.

Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled permissions in the environment boundaries can be modified in roles and profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

▼ File browser permissions (enabled 1/1)

- Access data**
Display File browser in the navigation menu and access data via web portal.

▼ Desktop permissions (enabled 12/12)

- | | | |
|---|---|---|
| <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Display
Receive visual data from the NICE DCV server <input checked="" type="checkbox"/> Pointer
View NICE DCV server mouse position events and pointer shapes <input checked="" type="checkbox"/> Mouse
Input from the client mouse to the NICE DCV server <input checked="" type="checkbox"/> Audio Out
Receive audio from the NICE DCV server to the client | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Keyboard
Input from the client keyboard to the NICE DCV server <input checked="" type="checkbox"/> Keyboard SAS
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well <input checked="" type="checkbox"/> Screenshot
Save a screenshot of the remote desktop | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Clipboard Copy
Copy data from the NICE DCV server to the client clipboard <input checked="" type="checkbox"/> Clipboard Paste
Copy data to the NICE DCV server from the client clipboard <input checked="" type="checkbox"/> File Upload
Upload files to the session storage <input checked="" type="checkbox"/> File Download
Download files from the session storage |
|---|---|---|

▼ Desktop advanced settings (enabled 8/8)

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Audio In
Send audio from the client to the NICE DCV server <input checked="" type="checkbox"/> Printer
Create PDFs or XPS files from the NICE DCV server to the client | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> USB
Use USB devices from the client <input checked="" type="checkbox"/> Smartcard
Read the smart card from the client <input checked="" type="checkbox"/> Stylus
Input from specialized USB devices, such as 3D pointing devices or graphic tablets | <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Web Camera
Use the Web Camera connected to a client device in a session <input checked="" type="checkbox"/> Touch
Use native touch events from the client device <input checked="" type="checkbox"/> Gamepad
Use gamepads connected to a client computer in a session |
|---|--|--|

Configurando o acesso ao navegador de arquivos

Os administradores podem ativar ou desativar os dados de acesso em Permissões do navegador de arquivos. Se os dados do Access estiverem desativados, os usuários não verão a navegação do Navegador de Arquivos em seu portal da web e não poderão carregar ou baixar dados anexados ao sistema de arquivos global. Quando os dados do Access estão habilitados, os usuários têm acesso à navegação do Navegador de Arquivos em seu portal da web, o que lhes permite carregar ou baixar dados anexados ao sistema de arquivos global.

Quando o recurso de dados do Access é ativado e depois desativado, os usuários que já estão conectados ao portal da web não conseguirão carregar ou baixar arquivos, mesmo que estejam na página correspondente. Além disso, o menu de navegação desaparecerá quando eles atualizarem a página.

Configurando as permissões da área de trabalho

Os administradores podem ativar ou desativar as permissões de desktop para gerenciar globalmente a VDI funcionalidade de todos os proprietários. Todas essas permissões, ou um subconjunto, podem

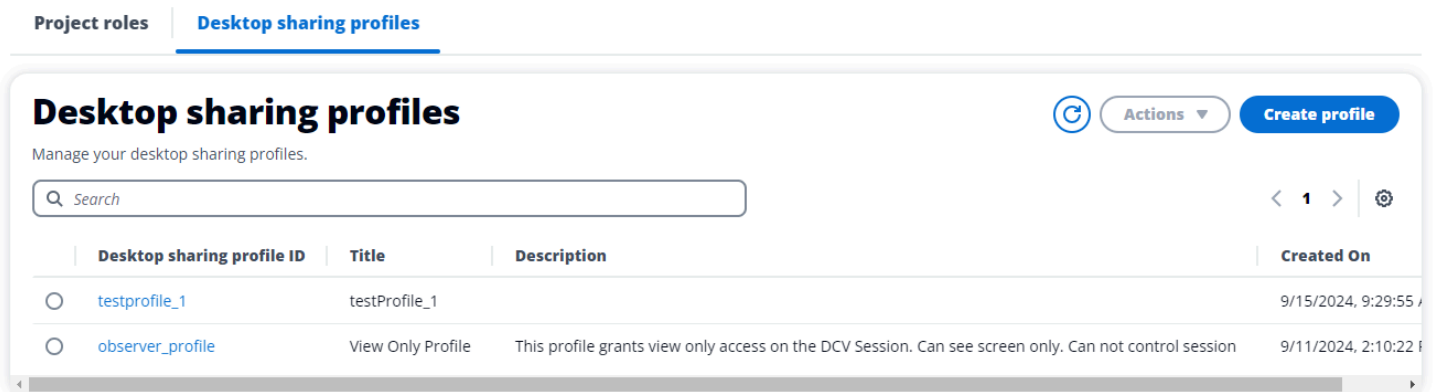
ser usadas para criar perfis de compartilhamento de área de trabalho que determinam quais ações podem ser executadas pelos usuários com quem a área de trabalho é compartilhada. Se alguma permissão da área de trabalho estiver desativada, isso desativará automaticamente as permissões correspondentes nos perfis de compartilhamento da área de trabalho. Essas permissões serão rotuladas como “Desativadas globalmente”. Mesmo que o administrador habilite essa permissão de desktop novamente, a permissão no perfil de compartilhamento de desktop permanecerá desativada até que o administrador a ative manualmente.

Perfis de compartilhamento de desktop

Os administradores podem criar novos perfis e personalizá-los. Esses perfis podem ser acessados por todos os usuários e são usados ao compartilhar uma sessão com outras pessoas. As permissões máximas concedidas nesses perfis não podem exceder as permissões de desktop permitidas globalmente.

Criar perfil

Os administradores podem escolher Criar perfil para criar um novo perfil. Em seguida, eles podem inserir um nome de perfil, uma descrição de perfil, definir as permissões desejadas e salvar suas alterações.



The screenshot displays the 'Desktop sharing profiles' management page. At the top, there are two tabs: 'Project roles' and 'Desktop sharing profiles', with the latter being active. The main heading is 'Desktop sharing profiles' with a refresh icon and an 'Actions' dropdown menu. A 'Create profile' button is visible in the top right. Below the heading is a search bar with the placeholder text 'Search'. A table lists the existing profiles:

	Desktop sharing profile ID	Title	Description	Created On
<input type="radio"/>	testprofile_1	testProfile_1		9/15/2024, 9:29:55
<input type="radio"/>	observer_profile	View Only Profile	This profile grants view only access on the DCV Session. Can see screen only. Can not control session	9/11/2024, 2:10:22

Profile definition

Profile name

Assign a name to the profile.

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

Profile description - optional

Optionally add more details to describe the specific profile.

Permissions

Permissions granted to this sharing profile. To enable the permissions that are 'Disabled globally', go back to the Environment boundaries and enable them there.

▼ Desktop permissions (enabled 12/12)

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

Audio Out

Receive audio from the NICE DCV server to the client

Unsupervised Access

Allow a user to connect to session without supervision

Keyboard

Input from the client keyboard to the NICE DCV server

Keyboard SAS

Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well

Screenshot

Save a screenshot of the remote desktop

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

► Desktop advanced settings (enabled 8/8)

Cancel

Save changes

Editar perfil

Para editar um perfil:

1. Selecione o perfil desejado.
2. Escolha Ações e, em seguida, selecione Editar para modificar o perfil.
3. Ajuste as permissões conforme necessário.
4. Escolha Salvar alterações.

Quaisquer alterações feitas no perfil serão aplicadas imediatamente às sessões abertas atuais.

Desktop sharing profiles

Manage your desktop sharing profiles.

Desktop sharing profile ID	Title	Description	Created On
<input checked="" type="radio"/> testprofile_1	testProfile_1		9/15/2024, 9:29:55
<input type="radio"/> observer_profile	View Only Profile	This profile grants view only access on the DCV Session. Can see screen only. Can not control session	9/11/2024, 2:10:22

Profile definition

Profile name

Assign a name to the profile.

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

Profile description - optional

Optionally add more details to describe the specific profile.

Permissions

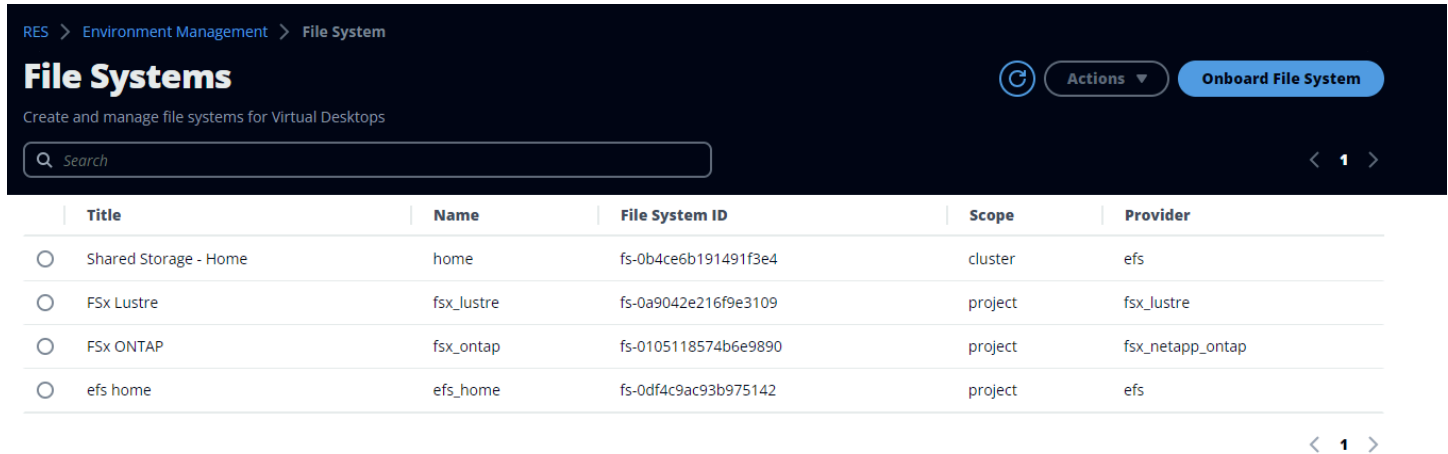
Permissions granted to this sharing profile. To enable the permissions that are 'Disabled globally', go back to the Environment boundaries and enable them there.

▼ Desktop permissions (enabled 12/12)

- 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
- Audio Out**
Receive audio from the NICE DCV server to the client
- Unsupervised Access**
Allow a user to connect to session without supervision
- Keyboard**
Input from the client keyboard to the NICE DCV server
- Keyboard SAS**
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
- Screenshot**
Save a screenshot of the remote desktop
- 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

► Desktop advanced settings (enabled 8/8)

Sistemas de arquivos



The screenshot shows the AWS File Systems console. At the top, there is a breadcrumb trail: RES > Environment Management > File System. The main heading is "File Systems" with a sub-heading "Create and manage file systems for Virtual Desktops". There are buttons for "Actions" and "Onboard File System". A search bar is present with the text "Search". Below the search bar is a table with the following columns: Title, Name, File System ID, Scope, and Provider. The table contains four rows of data.

	Title	Name	File System ID	Scope	Provider
<input type="radio"/>	Shared Storage - Home	home	fs-0b4ce6b191491f3e4	cluster	efs
<input type="radio"/>	FSx Lustre	fsx_lustre	fs-0a9042e216f9e3109	project	fsx_lustre
<input type="radio"/>	FSx ONTAP	fsx_ontap	fs-0105118574b6e9890	project	fsx_netapp_ontap
<input type="radio"/>	efs home	efs_home	fs-0df4c9ac93b975142	project	efs

Na página Sistemas de arquivos, você pode:

1. Pesquise sistemas de arquivos.
2. Quando um sistema de arquivos é selecionado, use o menu Ações para:
 - a. Adicione 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.

Tópicos

- [Crie um sistema de arquivos](#)
- [Integrar um 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 a sub-rede IDs doVPC. Você pode encontrar o IDs na guia Gerenciamento do 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

Projects

Select applicable project



Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

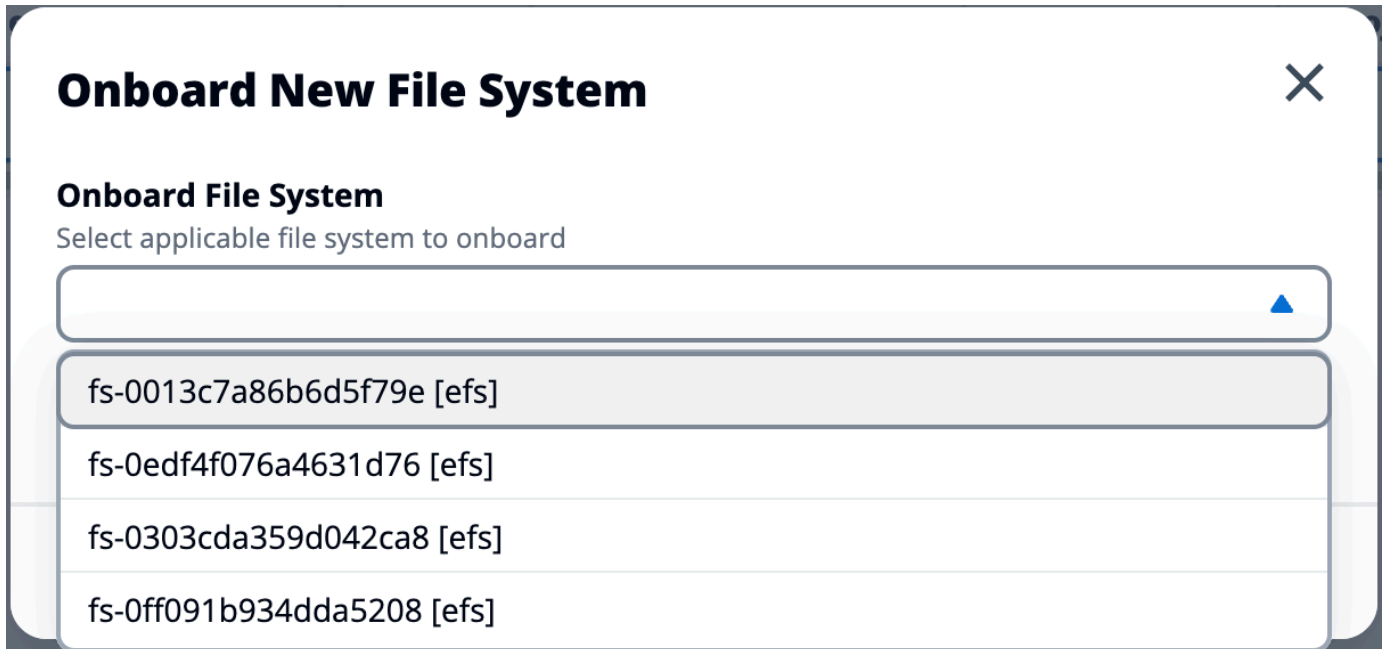
Subnet ID 1 and Subnet ID 2 should be in two different AZs

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.

Note

Por padrão, administradores e proprietários de projetos podem escolher um sistema de arquivos doméstico ao criar um novo projeto, que não pode ser editado posteriormente. Os sistemas de arquivos destinados a serem usados como diretórios base em projetos devem ser integrados definindo o caminho do Mount Directory como `/home`. Isso preencherá o sistema de arquivos integrado nas opções suspensas do sistema de arquivos do diretório inicial. Esse recurso ajuda a manter os dados isolados entre os projetos, pois somente os usuários associados ao projeto terão acesso ao sistema de arquivos por meio de seus VDI. VDIsmontará o sistema de arquivos no ponto de montagem selecionado durante a integração de um sistema de arquivos.

4. Selecione Enviar.

Onboard New File System



Onboard File System

Select applicable file system to onboard

fs-0edf4f076a4631d76 [efs]



Title

Enter a user friendly file system title

File System Name

Enter a file system name

File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

Mount Directory

Enter directory to mount the file system

Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01

Cancel

Submit

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.

The screenshot displays the 'Snapshot Management' interface. At the top, there is a breadcrumb trail: 'RES > Environment Management > Snapshot Management'. The main title is 'Snapshot Management'. Below this, there are two main sections: 'Created Snapshots' and 'Applied Snapshots'. Each section has a search bar, a table with columns 'S3 Bucket Name', 'Snapshot Path', 'Status', and 'Created On', and a 'No records' message. The 'Created Snapshots' section has a 'Create Snapshot' button, and the 'Applied Snapshots' section has an 'Apply Snapshot' button. Numbered callouts (1, 2, 3, 4) highlight the search bar, the 'Create Snapshot' button, the 'Created Snapshots' title, and the 'Apply Snapshot' button respectively.

RES > Environment Management > Snapshot Management

Created Snapshots

Snapshots created from the environment

Search

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

Create Snapshot

Applied Snapshots

Snapshots applied to the environment

Search

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

Apply Snapshot

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 seu status.
4. Aplique um instantâneo.

Tópicos

- [Criar um snapshot](#)
- [Aplicar 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 do 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. Selecione o bucket que você criou na lista Buckets.
2. Selecione a guia 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_ENVIRONMENT_NAME
 - 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.

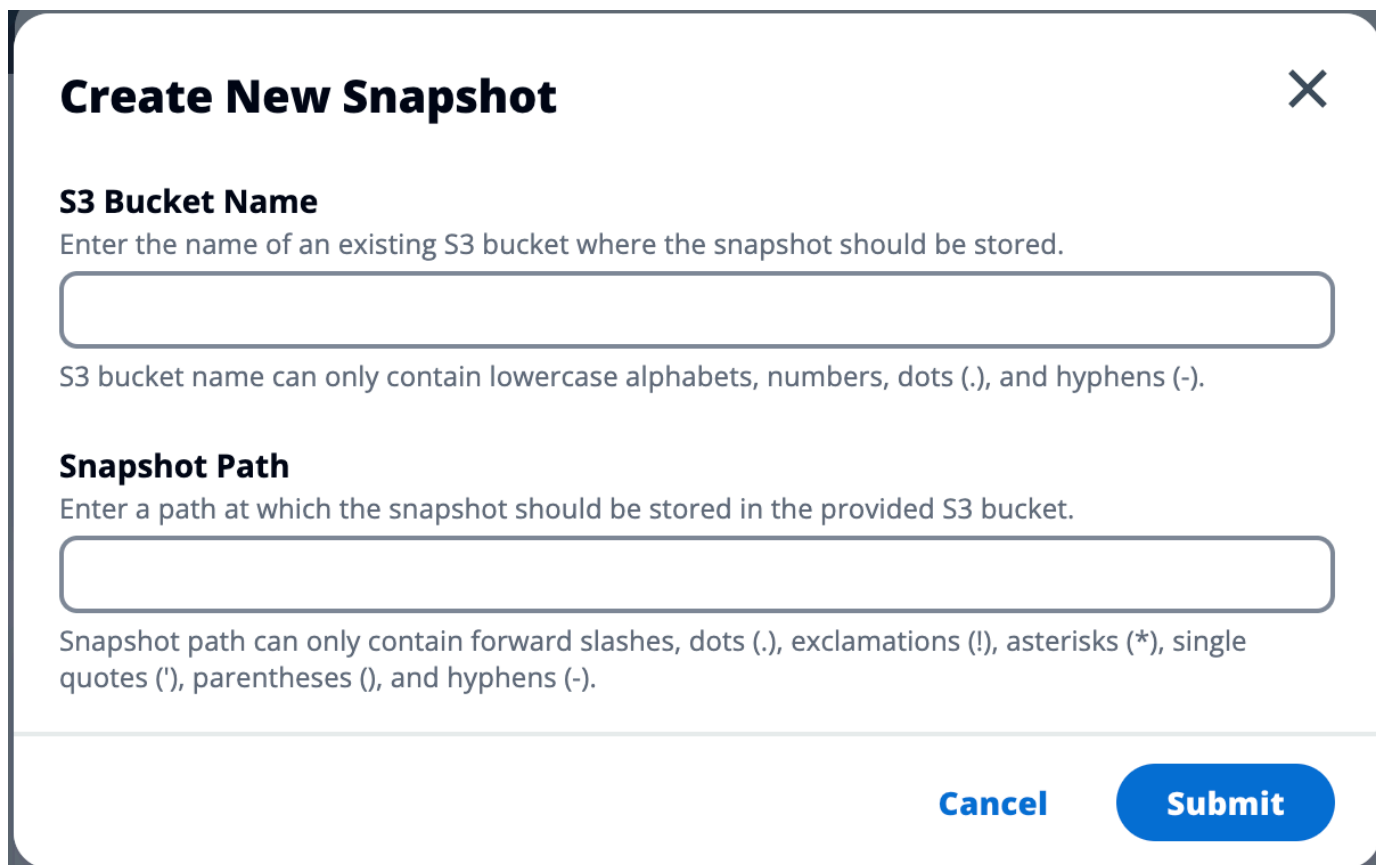
```

{
  "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.



Create New Snapshot ✕

S3 Bucket Name
Enter the name of an existing S3 bucket where the snapshot should be stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

Snapshot Path
Enter a path at which the snapshot should be stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamations (!), asterisks (*), single quotes ('), parentheses (), and hyphens (-).

Cancel **Submit**

5. Depois de cinco a dez minutos, escolha Atualizar na página Snapshots para verificar o status. Um instantâneo 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. Selecione o bucket que você criou na lista Buckets.
2. Selecione a guia 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_ENVIRONMENT_NAME`
- `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.

Apply a Snapshot ✕

S3 Bucket Name
Enter the name of the S3 bucket where the snapshot to be applied is stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

Snapshot Path
Enter the path at which the snapshot to be applied is stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamations (!), asterisks (*), single quotes ('), parentheses (), and hyphens (-).

Cancel **Submit**

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

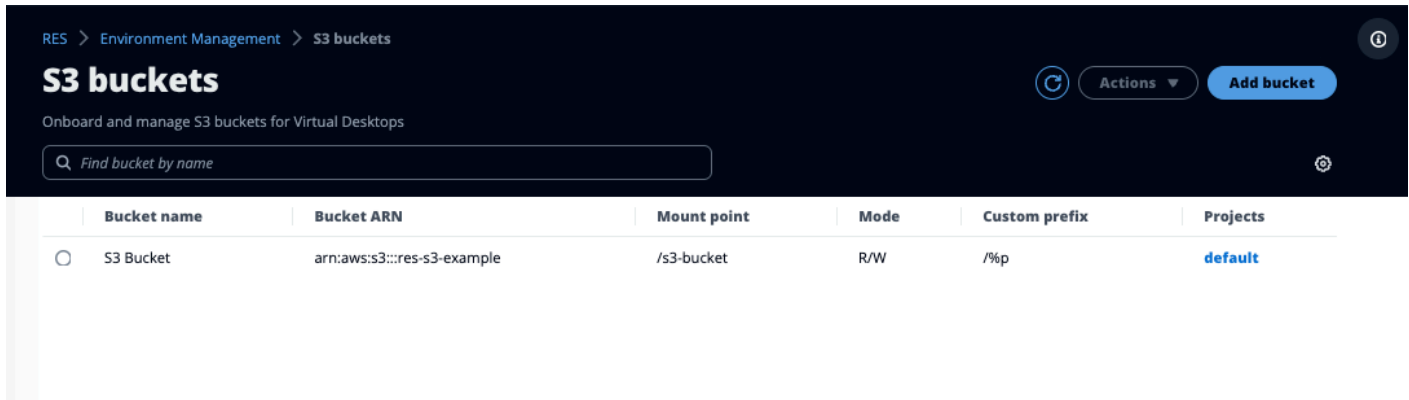
Buckets do Amazon S3

O Research and Engineering Studio (RES) suporta a montagem de [buckets do Amazon S3](#) em instâncias da infraestrutura de desktop virtual Linux (VDI). RESOs administradores podem integrar buckets do S3RES, anexá-los aos projetos, editar suas configurações e remover buckets na guia buckets do S3 em Gerenciamento do ambiente.

O painel de buckets do S3 fornece uma lista dos buckets do S3 integrados disponíveis para você. No painel de buckets do S3, você pode:

1. Use Adicionar bucket para integrar um bucket do S3. RES
2. Selecione um bucket do S3 e use o menu Ações para:
 - Editar um bucket
 - Remova um balde

3. Use o campo de pesquisa para pesquisar pelo nome do bucket e encontrar buckets S3 integrados.



As seções a seguir descrevem como gerenciar buckets do Amazon S3 em seus projetos. RES

Tópicos

- [Pré-requisitos do bucket Amazon S3 para implantações isoladas VPC](#)
- [Adicionar um bucket do Amazon S3](#)
- [Editar um bucket do Amazon S3](#)
- [Remover um bucket do Amazon S3](#)
- [Isolamento de dados](#)
- [Acesso ao bucket entre contas](#)
- [Prevenindo a exfiltração de dados em um ambiente privado VPC](#)
- [Solução de problemas](#)
- [Habilitando CloudTrail](#)

Pré-requisitos do bucket Amazon S3 para implantações isoladas VPC

Se você estiver implantando o Research and Engineering Studio de forma isolada VPC, siga estas etapas para atualizar os parâmetros de configuração lambda após a implantação RES em sua AWS conta.

1. Faça login no console Lambda da AWS conta em que o Research and Engineering Studio está implantado.
2. Encontre e navegue até a função Lambda chamada. *<RES-EnvironmentName>-vdc-custom-credential-broker-lambda*
3. Selecione a guia Configuração da função.

The screenshot shows the AWS Lambda console interface. At the top, there's a notification bar and a 'Function overview' section with tabs for 'Diagram' and 'Template'. Below that, there's a 'Configuration' tab with a sub-tab for 'Environment variables (16)'. The 'Environment variables' table is visible, with the following data:

Key	Value
AWS_STS_REGIONAL_ENDPOINTS	regional
CLUSTER_NAME	
CLUSTER_SETTINGS_TABLE_NAME	
DCV_HOST_DB_HASH_KEY	instance_id
DCV_HOST_DB_IDEA_SESSION_ID_KEY	idea_session_id
DCV_HOST_DB_IDEA_SESSION_OWNER_KEY	idea_session_owner
MODULE_ID	vdc
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_AND_USERNAME_PREFIX	PROJECT_NAME_AND_USERNAME_PREFIX
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_PREFIX	PROJECT_NAME_PREFIX
OBJECT_STORAGE_NO_CUSTOM_PREFIX	NO_CUSTOM_PREFIX

- No lado esquerdo, escolha Variáveis de ambiente para visualizar essa seção.
- Escolha Editar e adicione a seguinte nova variável de ambiente à função:
 - Chave: `AWS_STS_REGIONAL_ENDPOINTS`
 - Valor: `regional`
- Escolha Salvar.

Adicionar um bucket do Amazon S3

Para adicionar um bucket S3 ao seu RES ambiente:

- Escolha Add bucket (Adicionar bucket).
- Insira os detalhes do bucketARN, como nome do bucket e ponto de montagem.

Important

- O bucketARN, o ponto de montagem e o modo fornecidos não podem ser alterados após a criação.

- O bucket ARN pode conter um prefixo que isolará o bucket S3 integrado desse prefixo.

3. Selecione um modo para integrar seu bucket.

 Important

- Consulte [Isolamento de dados](#) para obter mais informações relacionadas ao isolamento de dados com modos específicos.

4. Em Opções avançadas, você pode fornecer uma IAM função ARN para montar os buckets para acesso entre contas. Siga as etapas [Acesso ao bucket entre contas](#) para criar a IAM função necessária para acesso entre contas.
5. (Opcional) Associe o bucket aos projetos, que podem ser alterados posteriormente. No entanto, um bucket do S3 não pode ser montado nas VDI sessões existentes de um projeto. Somente as sessões iniciadas após o projeto ter sido associado ao bucket montarão o bucket.
6. Selecione Enviar.

RES > Environment Management > S3 buckets > Add bucket

Add bucket

Currently only available for Linux desktops

Bucket setup

Bucket display name
Type a user friendly name to display

Bucket ARN
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

Mount point
Type the directory path where the bucket will be mounted

Mode

Read only (R)
Allow user only to read or copy stored data

Read and write (R/W)
Allow users to read or copy stored data and write or edit

Custom prefix
Enable the system to create a prefix automatically


No custom prefix

▼ **Advanced settings - optional**

IAM role ARN
To access the bucket, paste the IAM role Amazon Resource Name (ARN) copied in Identity and Access Management (IAM)

Project association

Projects - optional
Associate the bucket with the following projects. To add a new project, go to Create Project.

Editar um bucket do Amazon S3

1. Selecione um bucket do S3 na lista de buckets do S3.
2. No menu Ações, selecione Editar.
3. Insira suas atualizações.

⚠ Important

- Associar um projeto a um bucket S3 não montará o bucket nas instâncias existentes da infraestrutura de desktop virtual (VDI) desse projeto. O bucket só será montado em VDI sessões iniciadas em um projeto após o bucket ter sido associado a esse projeto.
- Desassociar um projeto de um bucket do S3 não afetará os dados no bucket do S3, mas fará com que os usuários de desktop percam o acesso a esses dados.

4. Escolha Salvar configuração do bucket.

The screenshot shows the 'Edit S3 Bucket' configuration page. At the top, there is a breadcrumb trail: 'RES > Environment Management > S3 buckets > Edit bucket'. The page title is 'Edit S3 Bucket'. Below the title, there are two main sections: 'Bucket setup' and 'Project association'. In the 'Bucket setup' section, there is a 'Bucket display name' field with the text 'S3 Bucket' and a subtext 'Type a user friendly name to display'. In the 'Project association' section, there is a 'Projects - optional' dropdown menu with the text 'Choose the projects to associate to the bucket'. The dropdown menu is currently empty, but there is a 'default' tag with an 'x' icon and the text 'default' below it. At the bottom right of the form, there are two buttons: 'Cancel' and 'Save bucket setup'.

Remover um bucket do Amazon S3

1. Selecione um bucket do S3 na lista de buckets do S3.
2. No menu Ações, selecione Remover.

⚠ Important

- Primeiro, você deve remover todas as associações de projetos do bucket.
- A operação de remoção não afeta os dados no bucket do S3. Ele remove apenas a associação do bucket do S3 com RES.

- A remoção de um bucket fará com que VDI as sessões existentes percam o acesso ao conteúdo desse bucket quando as credenciais da sessão expirarem (aproximadamente 1 hora).

Isolamento de dados

Ao adicionar um bucket do S3RES, você tem opções para isolar os dados dentro do bucket para projetos e usuários específicos. Na página Adicionar bucket, você pode selecionar um modo de Somente leitura (R) ou Leitura e gravação (R/W).

Somente leitura

Se `Read Only (R)` selecionado, o isolamento de dados é imposto com base no prefixo do bucket (ARN Amazon Resource Name). Por exemplo, se um administrador adicionar um intervalo ao RES uso do ARN `arn:aws:s3:::bucket-name/example-data/` e associar esse intervalo ao Projeto A e ao Projeto B, os usuários que iniciam a VDIs partir do Projeto A e do Projeto B só poderão ler os dados localizados `bucket-name` abaixo do caminho `/example-data`. Eles não terão acesso aos dados fora desse caminho. Se não houver prefixo anexado ao bucketARN, o bucket inteiro será disponibilizado para qualquer projeto associado a ele.

Ler e escrever

Se `Read and Write (R/W)` for selecionado, o isolamento de dados ainda será aplicado com base no prefixo do bucketARN, conforme descrito acima. Esse modo tem opções adicionais para permitir que os administradores forneçam prefixos baseados em variáveis para o bucket do S3. Quando `Read and Write (R/W)` selecionada, fica disponível uma seção de prefixo personalizado que oferece um menu suspenso com as seguintes opções:

- Sem prefixo personalizado
- `/%p`
- `/%p/%u`

RES > Environment Management > S3 buckets > Add bucket

Add bucket

Currently only available for Linux desktops

Bucket setup

Bucket display name
Type a user friendly name to display

Bucket ARN
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

Mount point
Type the directory path where the bucket will be mounted

Mode

Read only (R)
Allow user only to read or copy stored data

Read and write (R/W)
Allow users to read or copy stored data and write or edit

Custom prefix
Enable the system to create a prefix automatically

No custom prefix

No custom prefix
Will not create a dedicated directory

/%p
Create a dedicated directory by project

/%p/%u
Create a dedicated directory by project name and user name

Projects - optional
Associate the bucket with the following projects. To add a new project, go to Create Project.

Cancel Submit

Sem isolamento de dados personalizado

Quando `No custom prefix` selecionado para Prefixo personalizado, o bucket é adicionado sem nenhum isolamento de dados personalizado. Isso permite que qualquer projeto associado ao bucket tenha acesso de leitura e gravação. Por exemplo, se um administrador adicionar um intervalo ao RES uso do ARN `arn:aws:s3:::bucket-name` com `No custom prefix` selecionado e associar esse intervalo ao Projeto A e ao Projeto B, os usuários que iniciam a VDIs partir do Projeto A e do Projeto B terão acesso irrestrito de leitura e gravação ao intervalo.

Isolamento de dados em um nível por projeto

Quando `/%p` selecionado para Prefixo personalizado, os dados no bucket são isolados para cada projeto específico associado a ele. A `%p` variável representa o código do projeto. Por exemplo, se um administrador adicionar um bucket ao RES usar o ARN `arn:aws:s3:::bucket-name` com `/%p` selecionado e um ponto de montagem de `/buckete` associa esse bucket ao Projeto A e ao Projeto B, então o Usuário A no Projeto A pode gravar um arquivo no `/bucket`. O usuário B no Projeto A também pode ver o arquivo em que o usuário A escreveu. `/bucket`. No entanto, se o Usuário B iniciar a VDI no Projeto B e examinar `/bucket`, eles não verão o arquivo que o

usuário A escreveu, pois os dados são isolados pelo projeto. O arquivo que o usuário A escreveu é encontrado no bucket do S3 sob o prefixo, /ProjectA enquanto o usuário B só pode acessar usando /ProjectB o arquivo VDIs do Projeto B.

Isolamento de dados em nível por projeto e por usuário

Quando /%p/%u selecionado para Prefixo personalizado, os dados no bucket são isolados para cada projeto específico e usuário associado a esse projeto. A %p variável representa o código do projeto e %u representa o nome de usuário. Por exemplo, um administrador adiciona um bucket ao RES usar o ARN `arn:aws:s3:::bucket-name` com /%p/%u selecionado e um ponto de montagem do `/bucket`. Esse bucket está associado ao Projeto A e ao Projeto B. O usuário A no Projeto A pode gravar um arquivo no `/bucket`. Ao contrário do cenário anterior, com apenas %p isolamento, o usuário B, nesse caso, não verá o arquivo que o usuário A escreveu no Projeto A em `/bucket`, pois os dados são isolados pelo projeto e pelo usuário. O arquivo que o usuário A escreveu é encontrado no bucket do S3 sob o prefixo, /ProjectA/UserA enquanto o usuário B só pode acessá-lo /ProjectA/UserB ao usá-lo VDIs no Projeto A.

Acesso ao bucket entre contas

REStem a capacidade de montar buckets de outras AWS contas, desde que esses buckets tenham as permissões corretas. No cenário a seguir, um RES ambiente na Conta A deseja montar um bucket do S3 na Conta B.

Etapa 1: Crie uma IAM função na conta que RES está implantada (ela será chamada de Conta A):

1. Faça login no console AWS de gerenciamento da RES conta que precisa acessar o bucket do S3 (Conta A).
2. Abra o IAM console:
 - a. Navegue até o IAM painel.
 - b. No painel de navegação, escolha Políticas.
3. Crie uma política:
 - a. Escolha Criar política.
 - b. Selecione a guia JSON.
 - c. Cole a seguinte JSON política (<BUCKET-NAME> substitua pelo nome do bucket do S3 localizado na Conta B):

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

- d. Escolha Próximo.
4. Revise e crie a política:
 - a. Forneça um nome para a política (por exemplo, "S3 AccessPolicy").
 - b. Adicione uma descrição opcional para explicar a finalidade da política.
 - c. Revise a política e escolha Criar política.
 5. Abra o IAM console:
 - a. Navegue até o IAM painel.
 - b. No painel de navegação, escolha Perfis.
 6. Crie uma função:
 - a. Selecione Criar função.
 - b. Escolha Política de confiança personalizada como o tipo de entidade confiável.
 - c. Cole a JSON política a seguir (<ACCOUNT_ID> substitua pela ID da conta real da Conta A, <ENVIRONMENT_NAME> pelo nome do ambiente da RES implantação e <REGION> pela AWS região na qual ela RES será implantada):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNT_ID>:role/<ENVIRONMENT_NAME>-
custom-credential-broker-lambda-role-<REGION>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- d. Escolha Próximo.
7. Anexe políticas de permissões:
 - a. Pesquise e selecione a política que você criou anteriormente.
 - b. Escolha Próximo.
 8. Marque, revise e crie a função:
 - a. Insira um nome de função (por exemplo, "S3 AccessRole").
 - b. Na Etapa 3, escolha Adicionar tag e, em seguida, insira a chave e o valor a seguir:
 - Chave: res:Resource
 - Valor: s3-bucket-iam-role
 - c. Revise a função e escolha Criar função.
 9. Use a IAM função em RES:
 - a. Copie a IAM função ARN que você criou.
 - b. Faça login no RES console.
 - c. No painel de navegação esquerdo, escolha S3 Bucket.
 - d. Escolha Adicionar bucket e preencha o formulário com o bucket S3 de várias contas. ARN
 - e. Escolha o menu suspenso Configurações avançadas - opcional.
 - f. Insira a função ARN no ARN campo da IAM função.
 - g. Escolha Adicionar bucket.

Etapa 2: modificar a política de bucket na Conta B

1. Faça login no console AWS de gerenciamento da conta B.
2. Abra o console S3:
 - a. Navegue até o painel do S3.
 - b. Selecione o bucket ao qual você deseja conceder acesso.
3. Edite a política do bucket:
 - a. Selecione a guia Permissões e escolha Política de bucket.
 - b. Adicione a política a seguir para conceder ao IAM papel da Conta A acesso ao bucket (substituir `<AccountA_ID>` com o ID real da conta A e `<BUCKET-NAME>` com o nome do bucket S3):

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

- c. Escolha Salvar.

Prevenindo a exfiltração de dados em um ambiente privado VPC

Para evitar que os usuários extraiam dados de buckets S3 seguros para seus próprios buckets S3 em suas contas, você pode anexar um VPC endpoint para proteger sua privacidade. VPC As etapas a seguir mostram como criar um VPC endpoint para o serviço S3 que ofereça suporte ao acesso aos buckets do S3 em sua conta, bem como a quaisquer contas adicionais que tenham buckets entre contas.

1. Abra o VPC console da Amazon:
 - a. Faça login no AWS Management Console.
 - b. Abra o VPC console da Amazon em <https://console.aws.amazon.com/vpc/>.
2. Crie um VPC endpoint para o S3:
 - a. No painel de navegação à esquerda, escolha Endpoints.
 - b. Escolha Criar Endpoint.
 - c. Em Service category (Categoria de serviços), certifique-se de que a opção serviços AWS esteja selecionada.
 - d. No campo Nome do serviço, digite com .amazonaws.<region>.s3 (<region> substitua pela sua AWS região) ou pesquise por "S3".
 - e. Selecione o serviço S3 na lista.
3. Defina as configurações do endpoint:
 - a. Para VPC, selecione o VPC local em que você deseja criar o endpoint.
 - b. Para Sub-redes, selecione as duas sub-redes privadas usadas para as sub-redes durante a VDI implantação.
 - c. Em Habilitar DNS nome, verifique se a opção está marcada. Isso permite que o DNS nome do host privado seja resolvido nas interfaces de rede do endpoint.
4. Configure a política para restringir o acesso:
 - a. Em Política, escolha Personalizado.
 - b. No editor de políticas, insira uma política que restrinja o acesso aos recursos da sua conta ou de uma conta específica. Aqui está um exemplo de política (substituir *mybucket* com o nome do seu bucket S3 e *111122223333* e *444455556666* com a AWS conta apropriada IDs que você deseja acessar):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [
            "111122223333", // Your Account ID
            "444455556666" // Another Account ID
          ]
        }
      }
    }
  ]
}
```

5. Crie o endpoint:
 - a. Examine suas configurações.
 - b. Escolha Criar endpoint.
6. Verifique o endpoint:
 - a. Depois que o endpoint for criado, navegue até a seção Endpoints no VPC console.
 - b. Selecione o endpoint recém-criado.
 - c. Verifique se o estado está disponível.

Seguindo essas etapas, você cria um VPC endpoint que permite acesso ao S3 restrito aos recursos da sua conta ou a um ID de conta especificado.

Solução de problemas

Como verificar se um balde não consegue ser montado em um VDI

Se um bucket não for montado em um VDI, há alguns locais onde você pode verificar se há erros. Siga as etapas abaixo.

1. Verifique os VDI registros:
 - a. Faça login no console AWS de gerenciamento.
 - b. Abra o EC2 console e navegue até Instâncias.
 - c. Selecione a VDI instância que você executou.
 - d. Conecte-se ao VDI por meio do Gerenciador de Sessões.
 - e. Execute os seguintes comandos:

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

Aqui, você encontrará os registros do bootstrap. Os detalhes de qualquer falha estarão localizados no `configure.log.{time}` arquivo.

Além disso, verifique o `/etc/message` registro para obter mais detalhes.

2. Verifique os registros personalizados do CloudWatch Lambda do Credential Broker:
 - a. Faça login no console AWS de gerenciamento.
 - b. Abra o CloudWatch console e navegue até Grupos de registros.
 - c. Pesquise o grupo de registros `/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.
 - d. Examine o primeiro grupo de registros disponível e localize quaisquer erros nos registros. Esses registros conterão detalhes sobre possíveis problemas, fornecendo credenciais personalizadas temporárias para montagem de buckets do S3.
3. Verifique os CloudWatch registros personalizados do Credential Broker API Gateway:
 - a. Faça login no console AWS de gerenciamento.
 - b. Abra o CloudWatch console e navegue até Grupos de registros.
 - c. Pesquise o grupo de registros `<stack-name>-vdc-custom-credential-broker-lambda-vdc-custom-credential-broker-api-gateway-access-logs<nonce>`.
 - d. Examine o primeiro grupo de registros disponível e localize quaisquer erros nos registros. Esses registros conterão detalhes sobre todas as solicitações e respostas ao API Gateway para obter as credenciais personalizadas necessárias para montar os buckets do S3.

Como editar a configuração da IAM função de um bucket após a integração

1. Faça login no [AWS DynamoDB Console](#).
2. Selecione a tabela:
 - a. No painel de navegação à esquerda, selecione Tables (Tabelas).
 - b. Encontre e selecione `<stack-name>.cluster-settings`.
3. Digitalize a tabela:
 - a. Escolha Explore table items (Explorar itens da tabela).
 - b. Verifique se a opção Escanear está selecionada.
4. Adicionar um filtro:
 - a. Escolha Filtros para abrir a seção de entrada do filtro.
 - b. Defina o filtro para corresponder à sua chave-
 - Atributo: insira a chave.
 - Condição: Selecione Começa com.
 - Valor: insira `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` substituindo `<filesystem_id>` com o valor do sistema de arquivos que precisa ser modificado.

5. Execute o escaneamento:

Escolha Executar para executar o escaneamento com o filtro.

6. Confira o valor:

Se a entrada existir, verifique se o valor está definido corretamente com a IAM função corretaARN.

Se a entrada não existir:

- a. Selecione Create Item (Criar item).
- b. Insira os detalhes do item:
 - Para o atributo-chave, insira `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
 - Adicione a IAM função corretaARN.

- c. Escolha Salvar para adicionar o item.
7. Reinicie as VDI instâncias:

Reinicialize a instância para garantir VDIs que as afetadas pela IAM função incorreta ARN sejam montadas novamente.

Habilitando CloudTrail

Para ativar CloudTrail sua conta usando o CloudTrail console, siga as instruções fornecidas em [Criação de uma trilha com o CloudTrail console](#) no Guia do AWS CloudTrail usuário. CloudTrail registrará o acesso aos buckets do S3 registrando a IAM função que os acessou. Isso pode ser vinculado a um ID de instância, que está vinculado a um projeto ou usuário.

Use o produto

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

Tópicos

- [SSHacesso](#)
- [Áreas de trabalho virtuais](#)
- [Desktops compartilhados](#)
- [Navegador de arquivos](#)

SSHacesso

Para usar SSH para acessar o bastion host:

1. No RES menu, escolha SSHacessar.
2. Siga as instruções na tela para usar um SSH ou o Pu TTY para acessar.

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 EC2 instâncias da Amazon com suas ferramentas e aplicativos favoritos pré-instalados e configurados.

Sistemas operacionais compatíveis

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

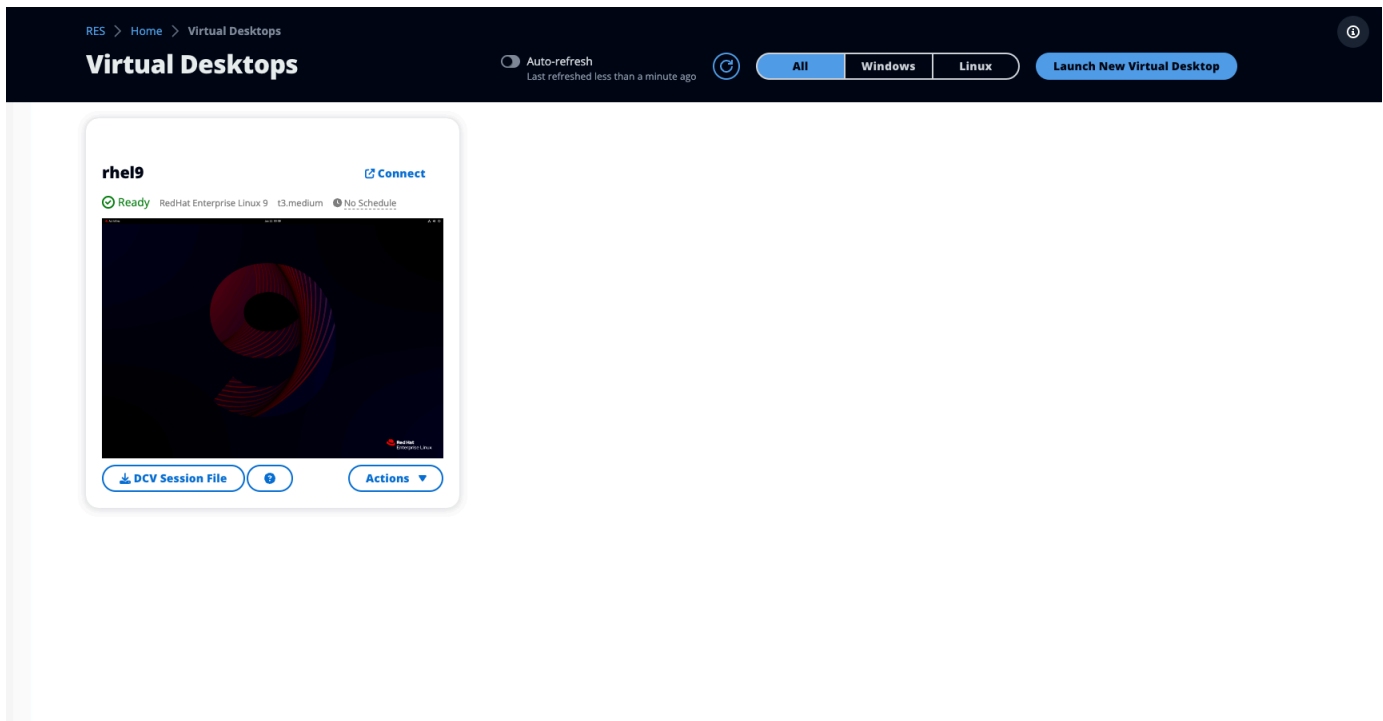
- Amazon Linux 2 (x86 e ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL8 (x86) e 9 (x86)
- Windows 2019, 2022 (x86)

Tópicos

- [Inicie um novo desktop](#)
- [Acesse seu desktop](#)
- [Controle o estado do seu desktop](#)
- [Modificar uma área de trabalho virtual](#)
- [Recuperar informações da sessão](#)
- [Agende desktops virtuais](#)
- [Parada automática da interface de desktop virtual](#)

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. RESdetecta GPU instâncias e instala os drivers relevantes.

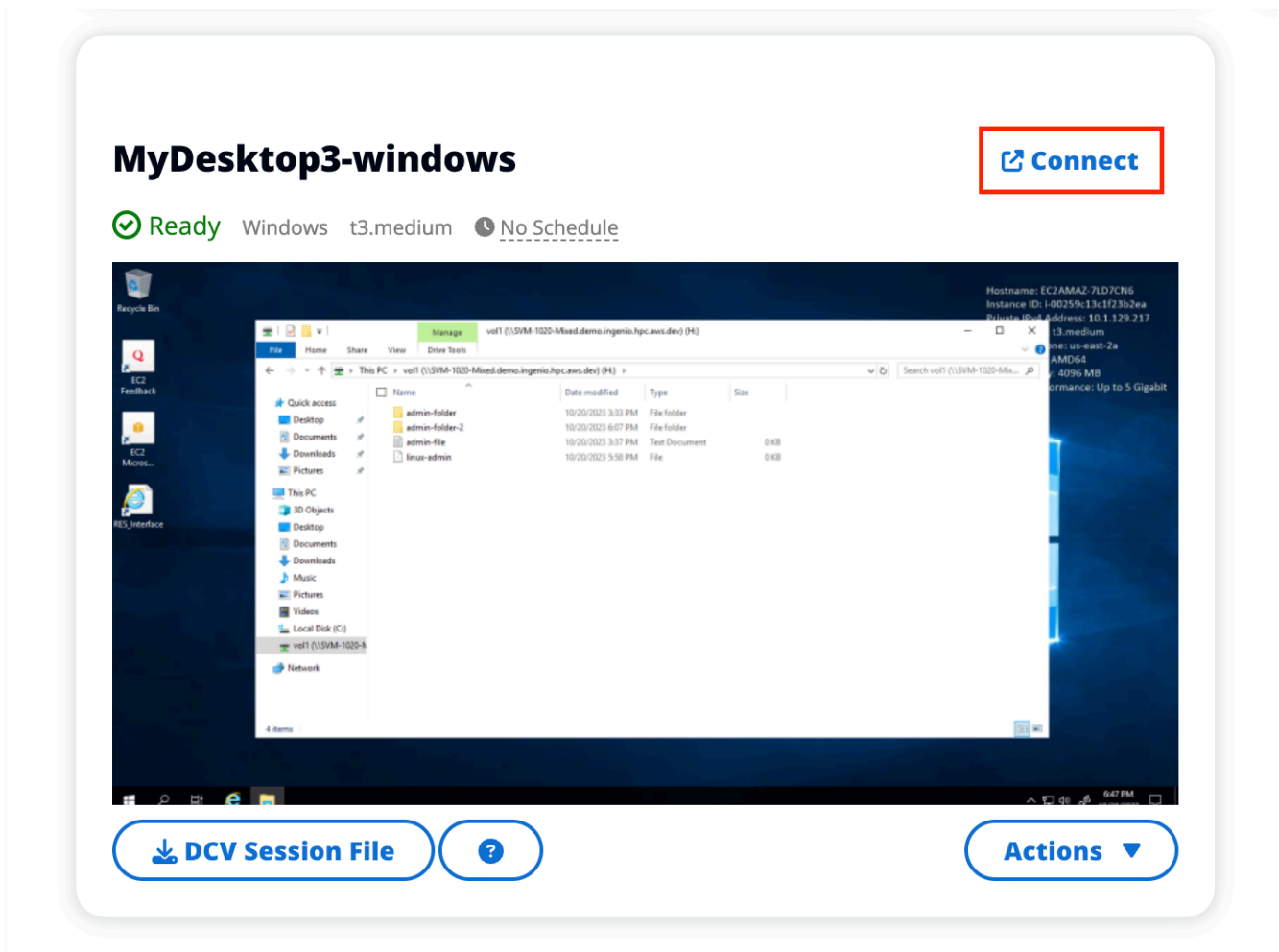
Acesse seu desktop

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

Web connection

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

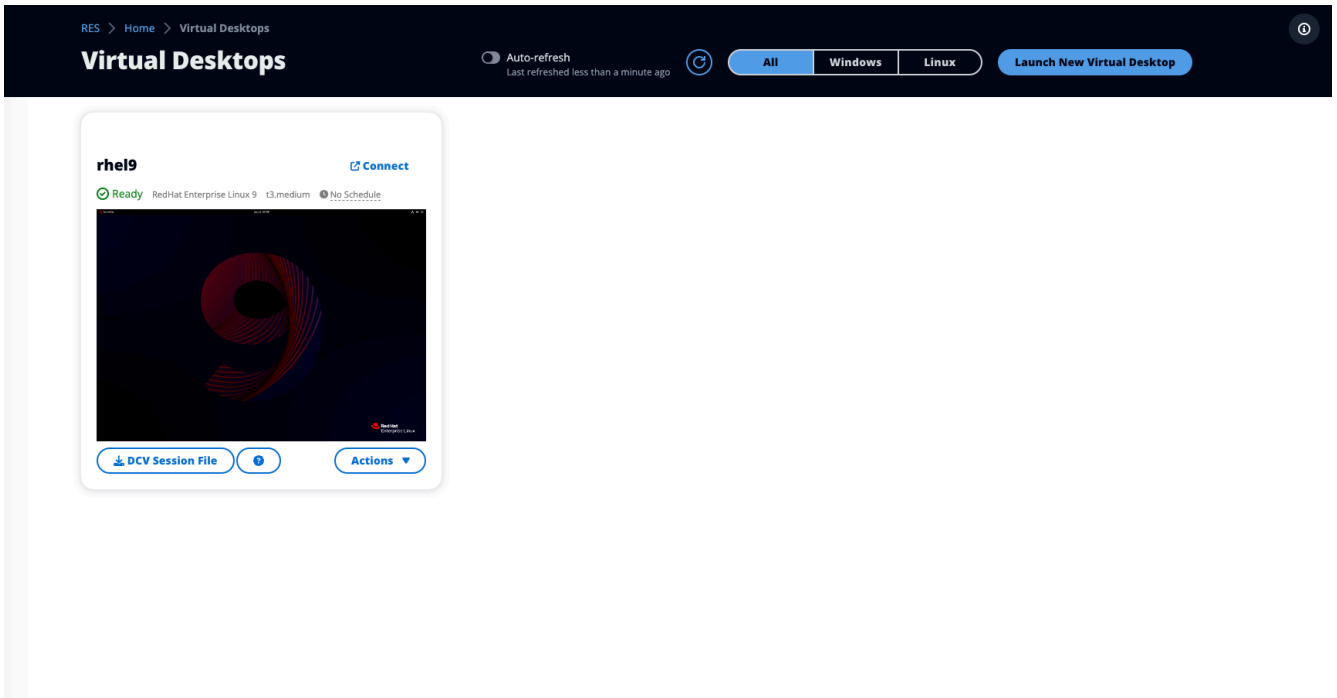
- Escolha Connect ou escolha a miniatura para acessar sua área de trabalho diretamente pelo navegador.



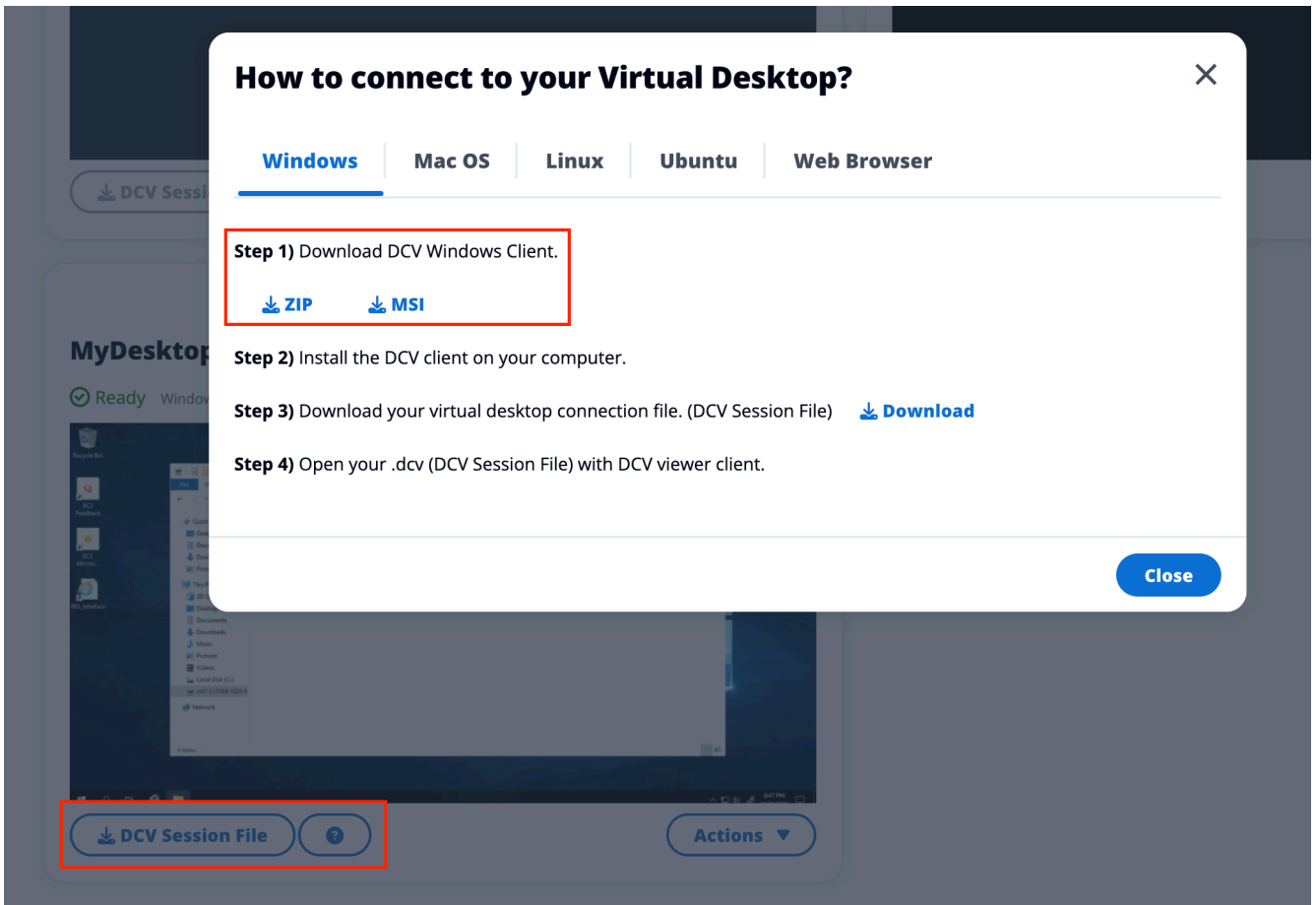
DCV connection

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

1. Escolha Arquivo de DCV sessão para baixar o .dcv arquivo. Você precisará de um DCV cliente instalado em seu sistema.



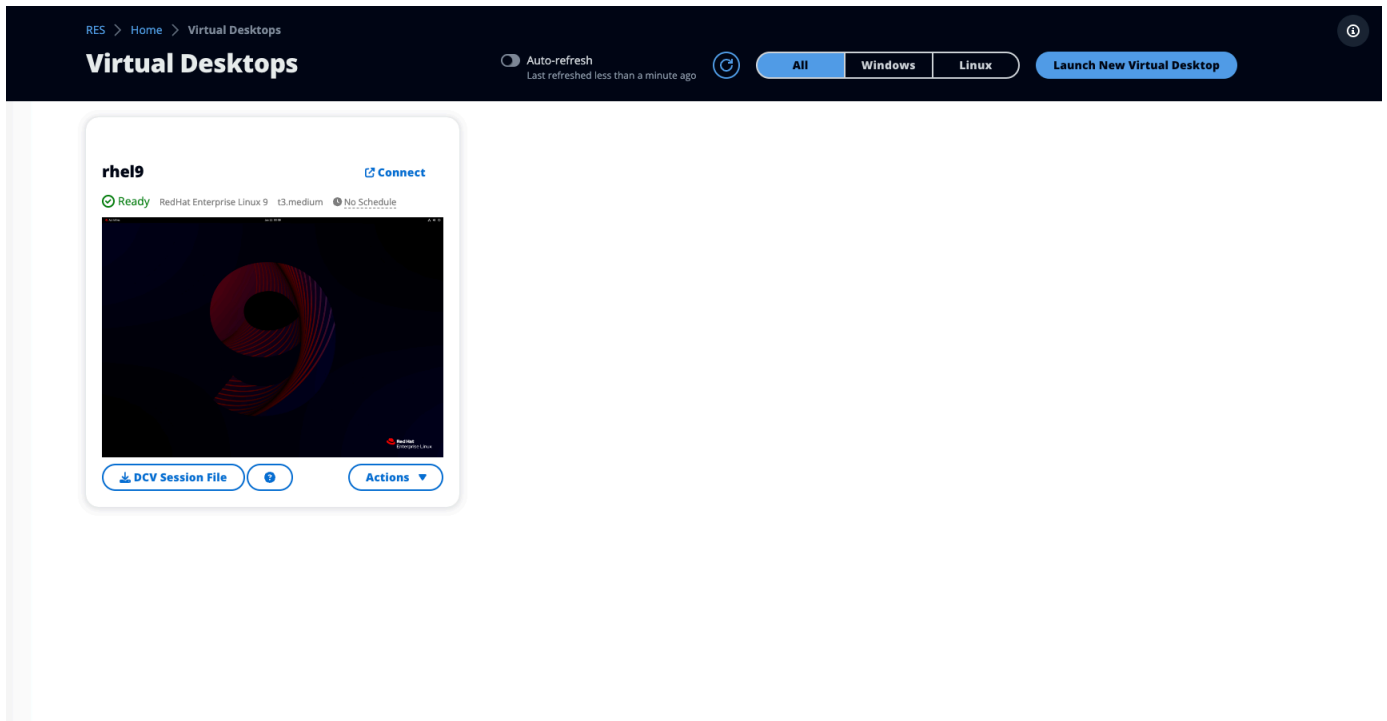
2. Para obter instruções de instalação, escolha a opção? ícone.



Controle o estado do seu desktop

Para controlar o estado do seu desktop:

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 RES sistema de arquivos antes de finalizar.

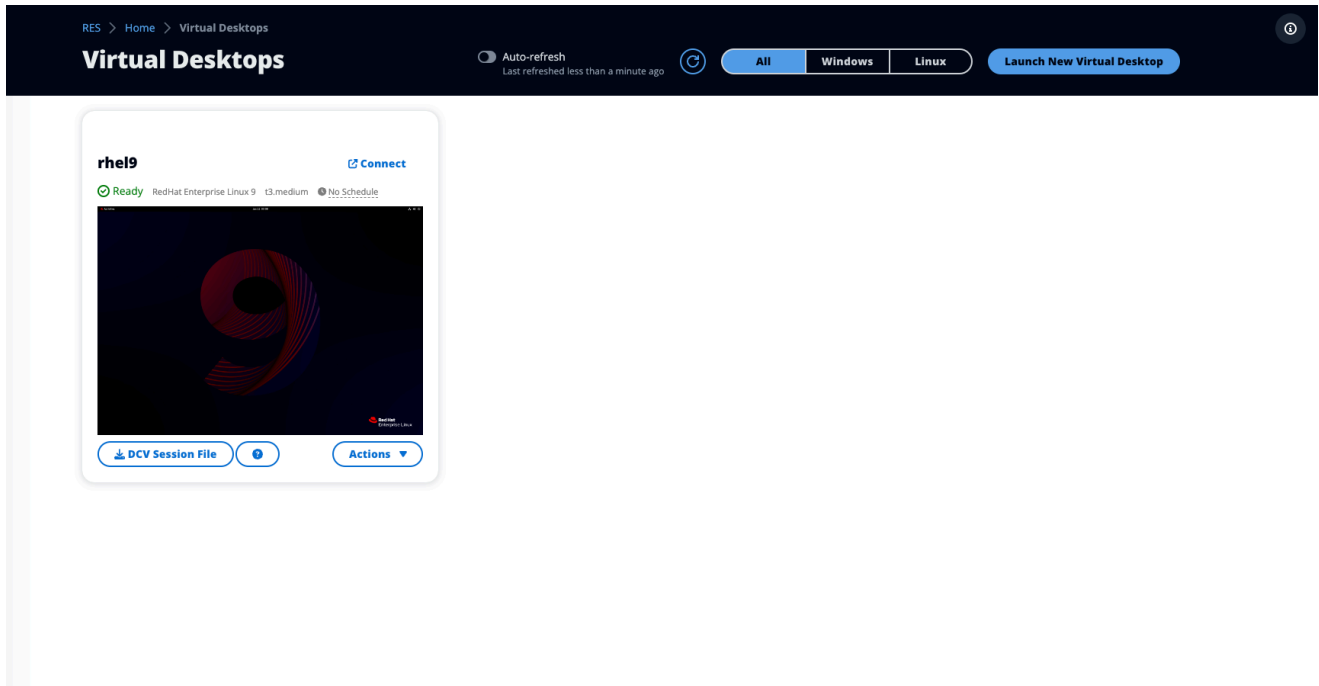
- Hibernar

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

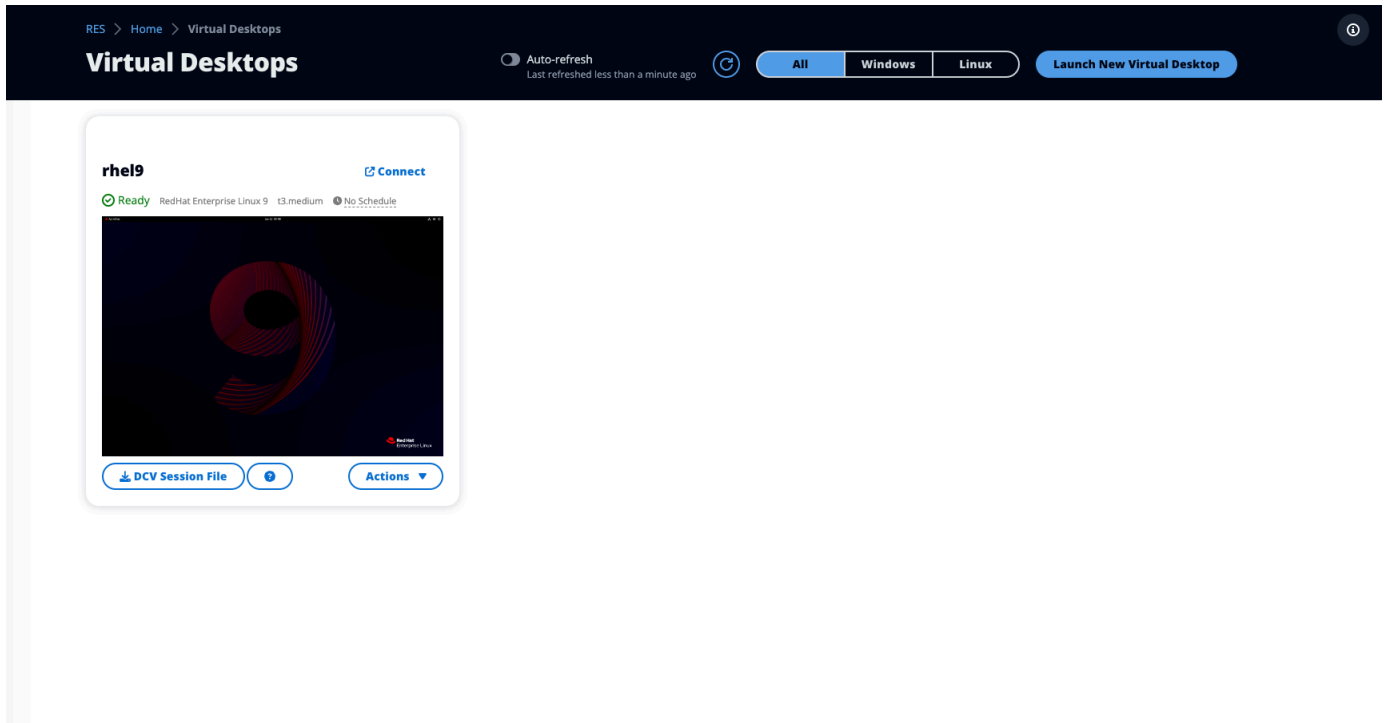
Você não pode atualizar o tamanho da área de trabalho para sessões em hibernação.

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.

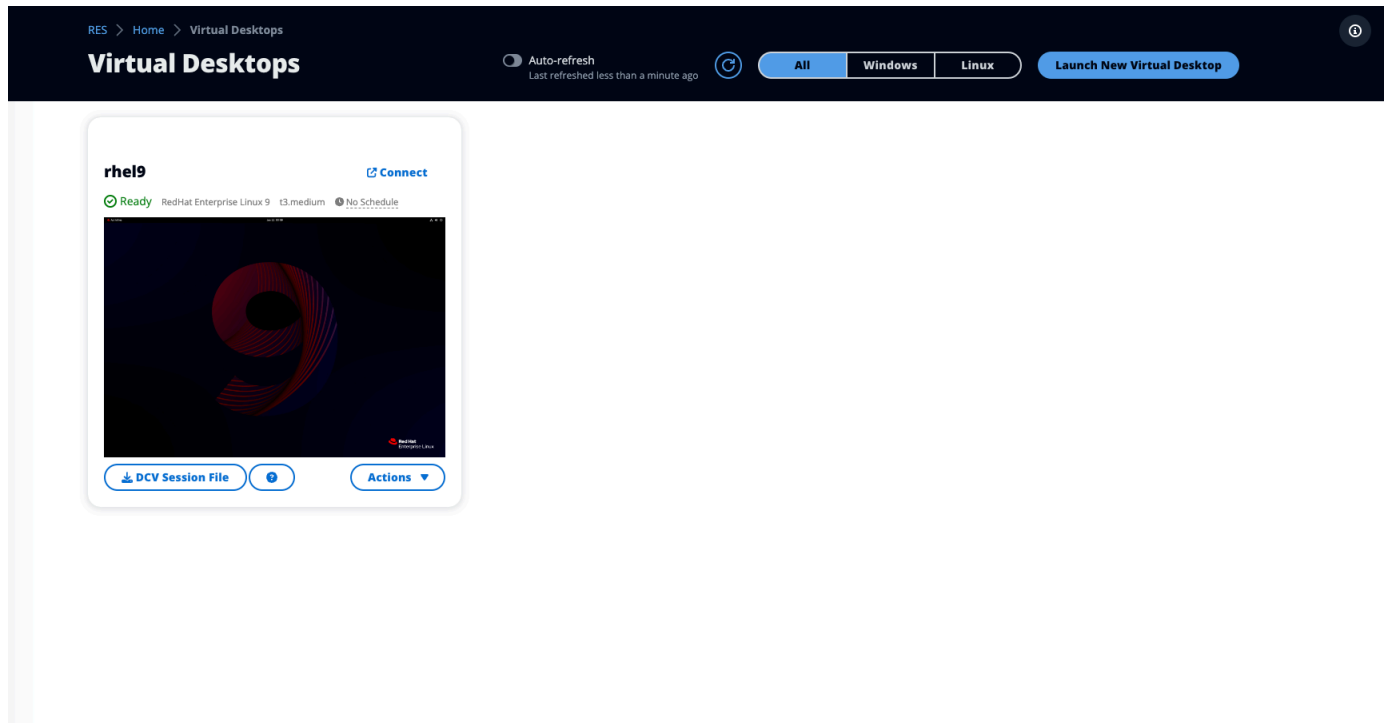


2. Escolha Mostrar informações.

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 CPU uso 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

Parada automática da interface de desktop virtual

Os administradores podem definir configurações para permitir que a inatividade VDIs seja interrompida ou encerrada. Há 4 configurações configuráveis:

1. Tempo limite de inatividade: as sessões inativas por esse tempo com CPU utilização abaixo do limite expirarão.
2. CPU limite de utilização: sessões sem interação e abaixo desse limite são consideradas inativas. Se for definido como 0, as sessões nunca serão consideradas inativas.
3. Estado de transição: após o tempo limite de inatividade, as sessões passarão para esse estado (interrompidas ou encerradas).
4. Aplicar agendamento: se selecionado, uma sessão que foi interrompida por estar ociosa pode ser retomada por sua programação diária.

Update Session Settings ✕

Idle Timeout (minutes)

Sessions idle for this time with CPU utilization below the threshold will time out

CPU Utilization Threshold (%)

Sessions under this threshold are considered idle

Transition State

Sessions will transition to this state after idle timeout

Enforce Schedule

Enable to allow schedule to resume a session that has been stopped for being idle

Allowed Sessions Per User

Maximum sessions allowed per user

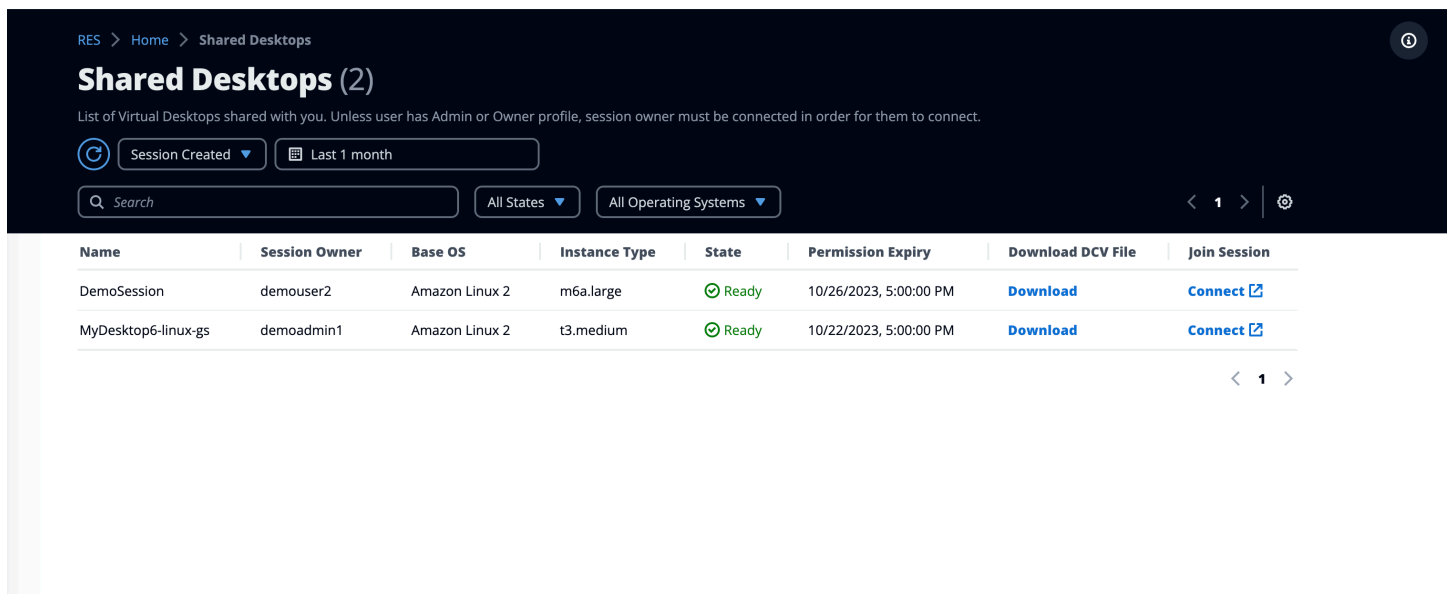
Cancel **Submit**

Essas configurações estão presentes na página Configurações da área de trabalho, na guia Servidor. Depois de atualizar as configurações de acordo com seus requisitos, clique em Enviar para salvar as configurações. As novas sessões usarão as configurações atualizadas, mas observe que as sessões existentes ainda usarão as configurações que tinham quando foram iniciadas.

Após o tempo limite, as sessões serão encerradas ou passarão para o STOPPED_IDLE estado com base em sua configuração. Os usuários poderão iniciar STOPPED_IDLE sessões a partir da interface do usuário.

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.



The screenshot shows the 'Shared Desktops' interface. At the top, there is a breadcrumb 'RES > Home > Shared Desktops' and a title 'Shared Desktops (2)'. Below the title, a subtitle reads: 'List of Virtual Desktops shared with you. Unless user has Admin or Owner profile, session owner must be connected in order for them to connect.' There are filters for 'Session Created' (Last 1 month) and 'All States' (All Operating Systems). A search bar is also present. The main content is a table with the following data:

Name	Session Owner	Base OS	Instance Type	State	Permission Expiry	Download DCV File	Join Session
DemoSession	demouser2	Amazon Linux 2	m6a.large	Ready	10/26/2023, 5:00:00 PM	Download	Connect
MyDesktop6-linux-gs	demoadmin1	Amazon Linux 2	t3.medium	Ready	10/22/2023, 5:00:00 PM	Download	Connect

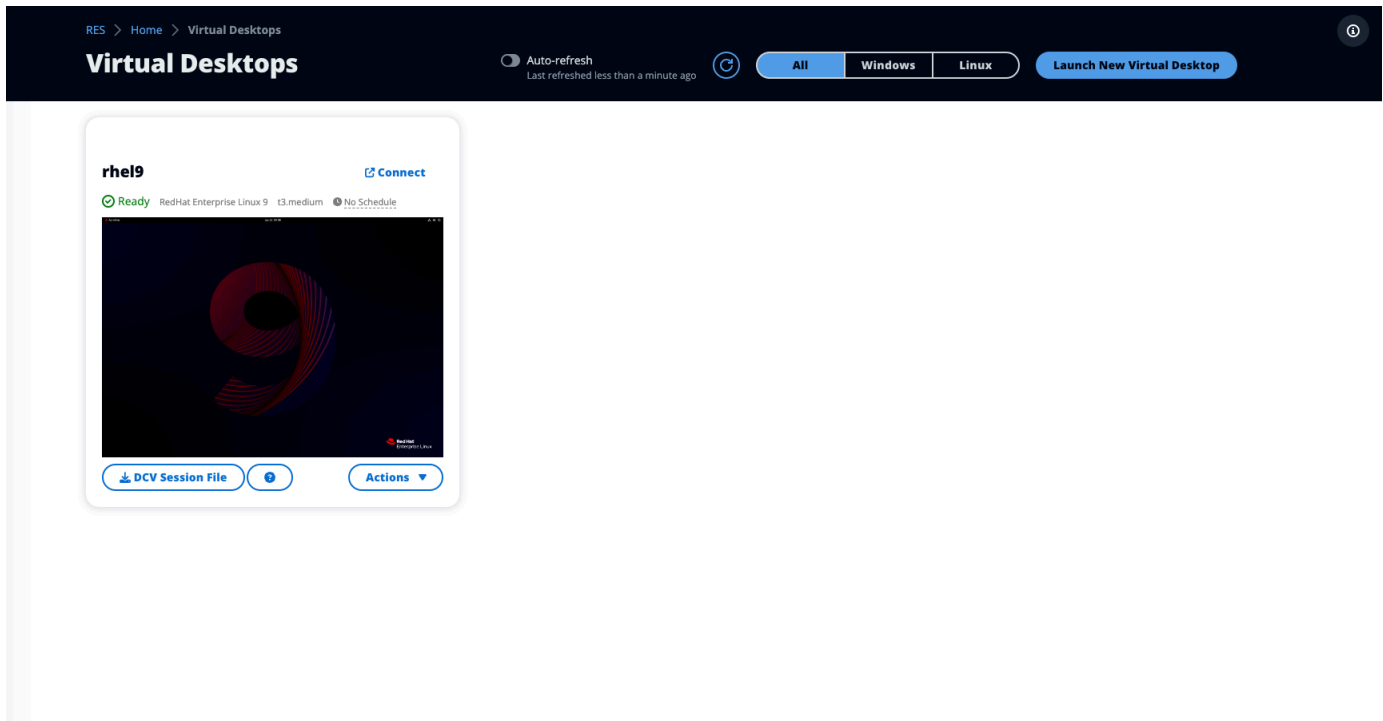
Ao compartilhar uma sessão, você pode configurar permissões para seus colaboradores. Por exemplo, você pode dar acesso somente de leitura a um colega de equipe com quem você está colaborando.

Tópicos

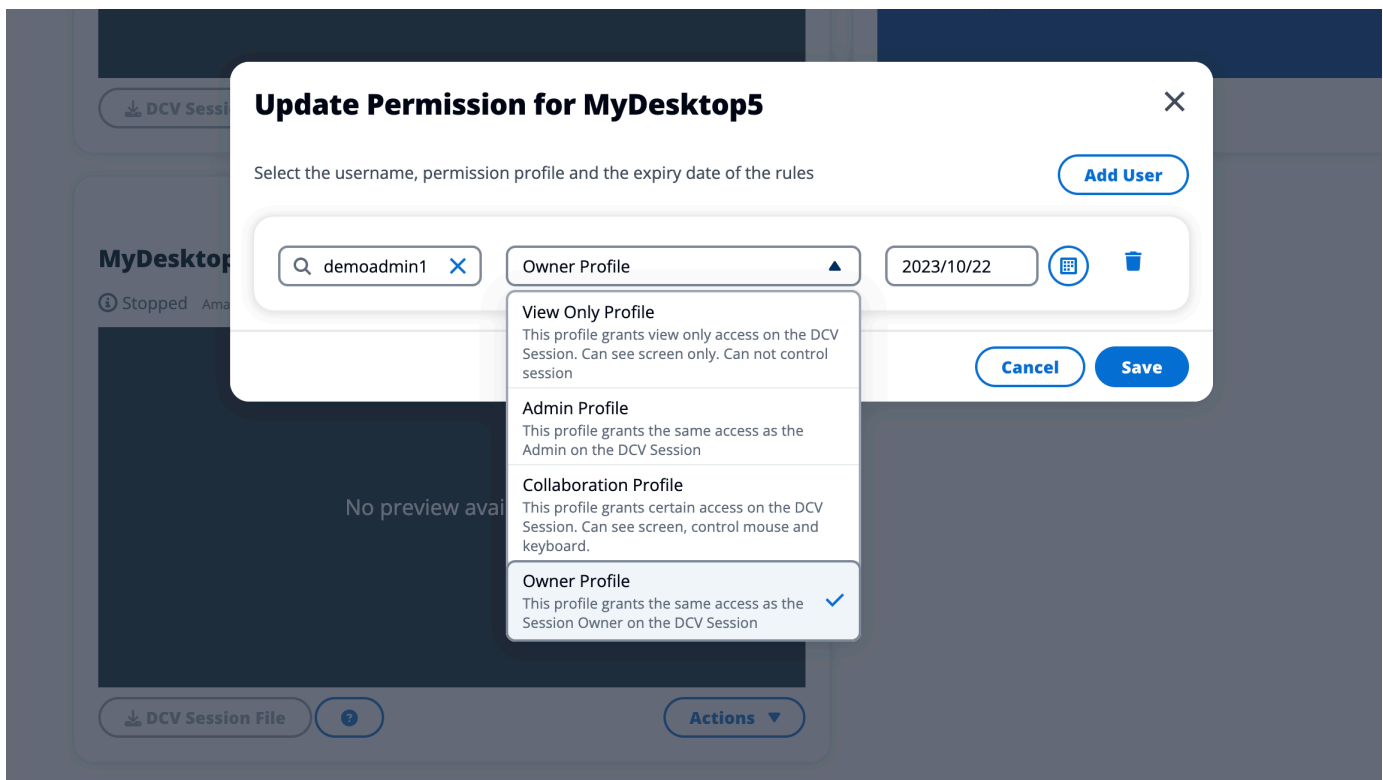
- [Compartilhar uma área de trabalho](#)
- [Acesse uma área de trabalho compartilhada](#)

Compartilhar uma área de trabalho

1. Em sua sessão de desktop, escolha Ações.



2. Selecione Permissões da sessão.
3. Selecione o usuário e o nível de permissão. Você também pode definir um prazo de expiração.
4. Escolha Salvar.



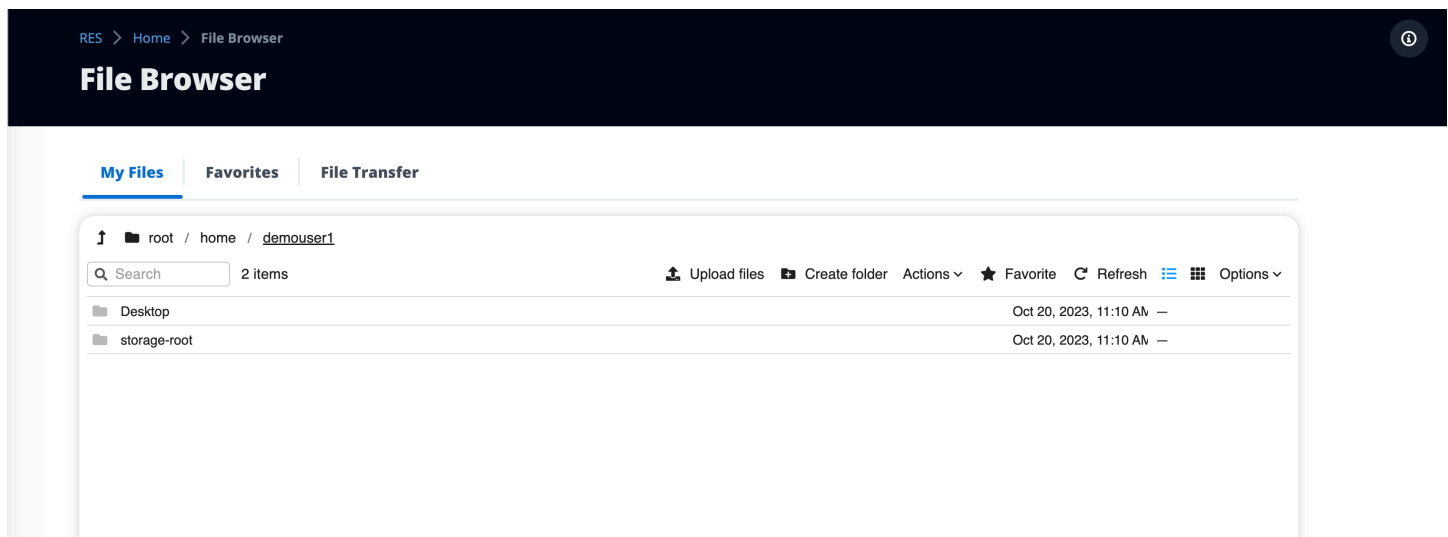
Para obter mais informações sobre permissões, consulte [the section called “Política de permissão”](#).

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 ingressar por meio de um navegador da web ou DCV. Para se conectar, siga as instruções em [Acesse seu desktop](#).

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 (AmazonEFS) está disponível para todos os nós Linux. Para nós Linux e Windows, 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.

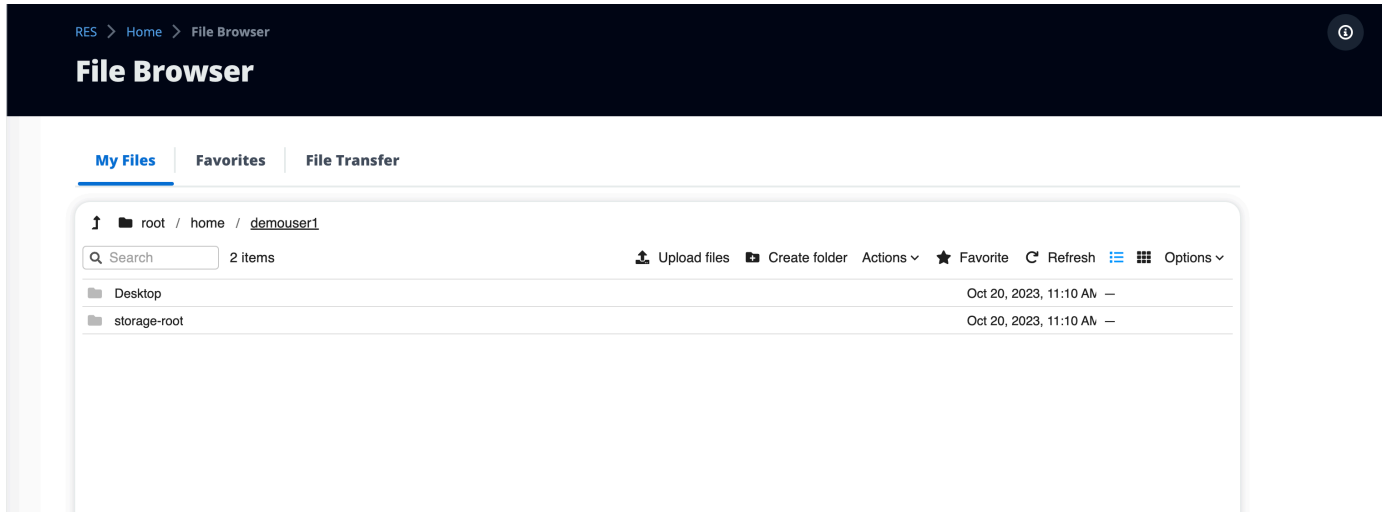


Tópicos

- [Carregar arquivo \(s\)](#)
- [Excluir arquivo \(s\)](#)
- [Gerenciar favoritos](#)
- [Editar arquivos](#)
- [Transferir arquivos](#)

Carregar arquivo (s)

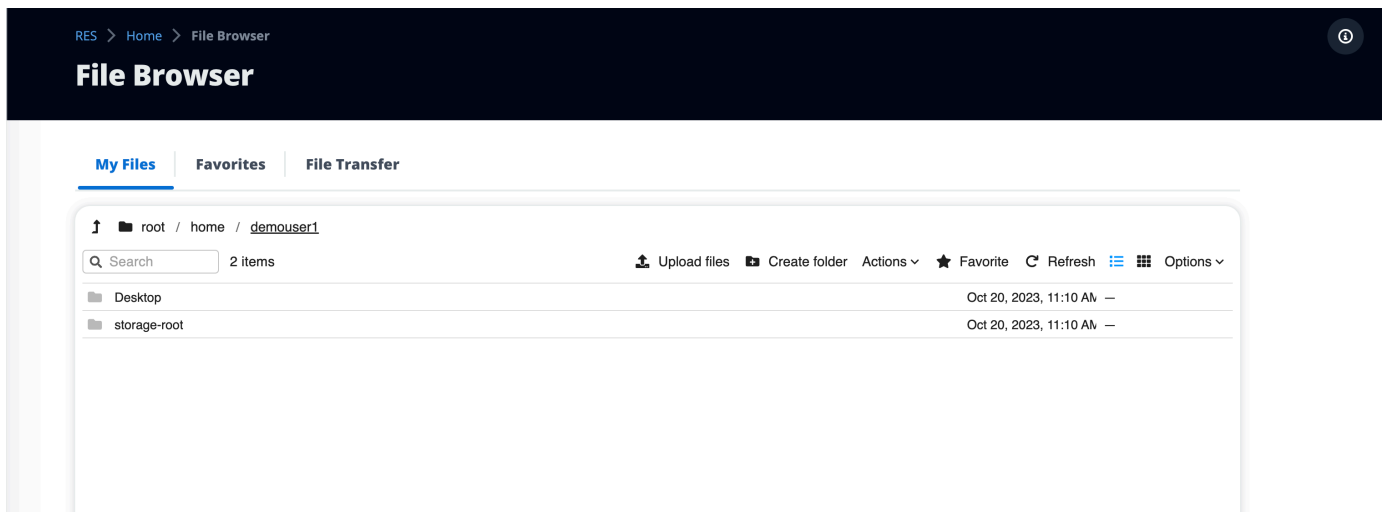
1. Escolha Carregar arquivos.



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.



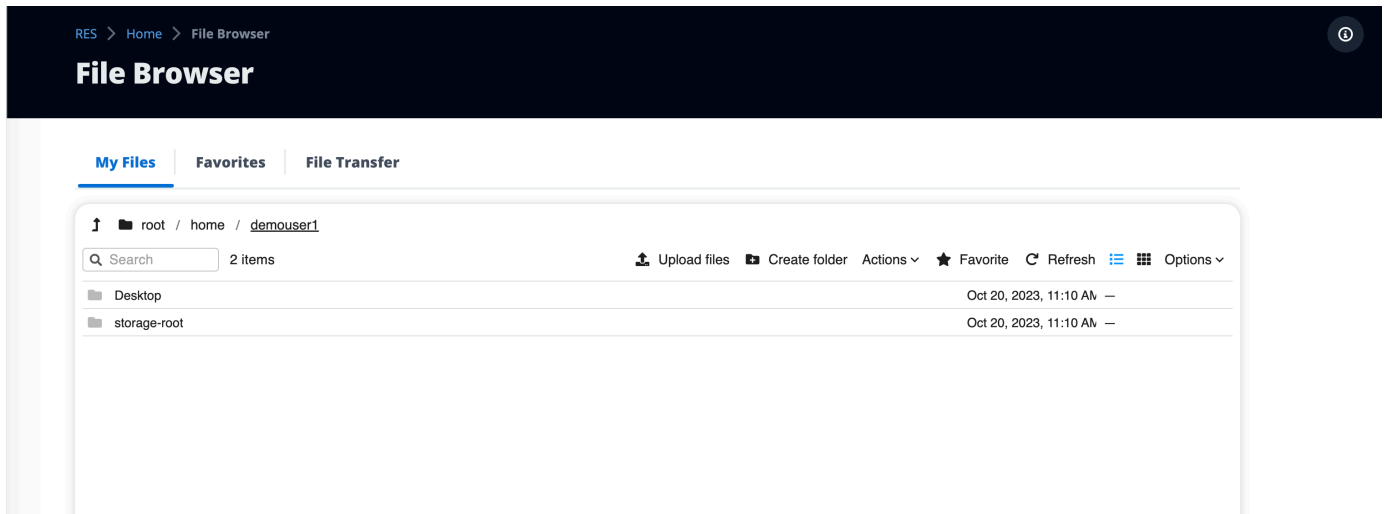
2. Escolha Ações.
3. Selecione Excluir arquivos.

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

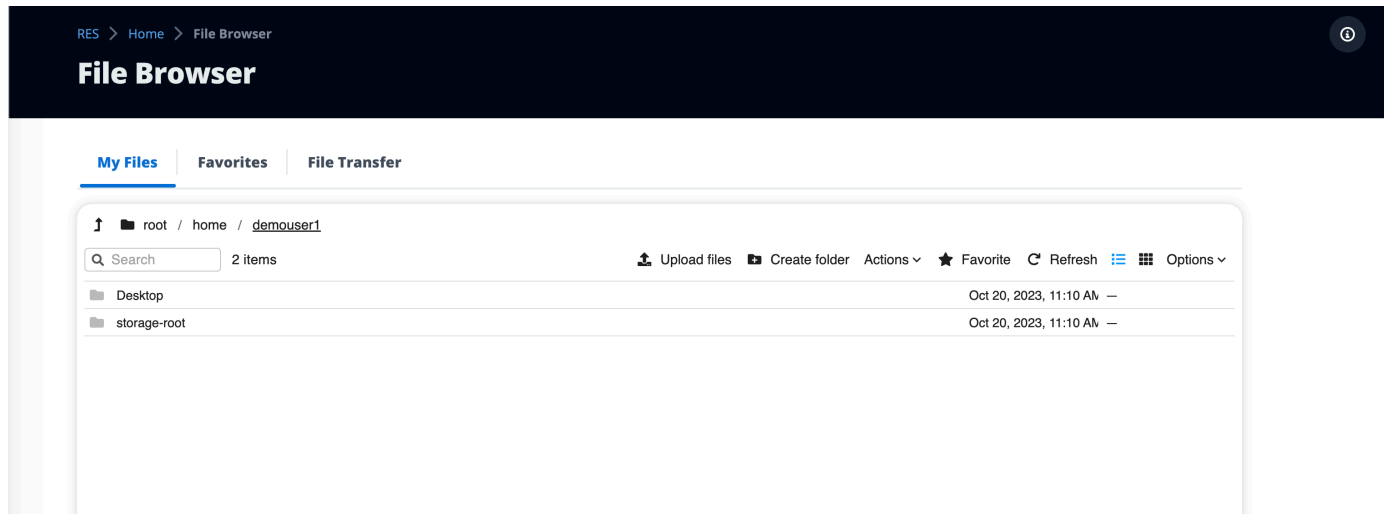
Note

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. Selecione 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)
- Win SCP (Windows)
- AWS Transfer for FTP (AmazonEFS)

RES > Home > File Browser

File Browser

My Files | **Favorites** | **File Transfer**

File Transfer Method

We recommend using below methods to transfer large files to your RES environment. Select an option below.

 FileZilla

Available for download on Windows, MacOS and Linux

 WinSCP

Available for download on Windows Only

 AWS Transfer

Your RES environment must be using Amazon EFS to use AWS Transfer

FileZilla

Step 1: Download FileZilla

- [Download FileZilla \(MacOS\)](#)
- [Download FileZilla \(Windows\)](#)
- [Download FileZilla \(Linux\)](#)

Step 2: Download Key File

[Download Key File \[*.pem\] \(MacOS / Linux\)](#)[Download Key File \[*.ppk\] \(Windows\)](#)

Step 3: Configure FileZilla

Open FileZilla and select **File > Site Manager** to create a new Site using below options:

Host [Redacted]	Port [Redacted]
Protocol SFTP	Logon Type Key File
User demouser3	Key File /path/to/key-file (downloaded in Step 2)

Save the settings and click **Connect**

Step 4: Connect and transfer file to FileZilla

During your first connection, you will be asked whether or not you want to trust [Redacted]. Check "Always Trust this Host" and Click "Ok".

Once connected, simply drag & drop to upload/download files.

Solução de problemas

Esta seção contém informações sobre como monitorar o sistema e como solucionar problemas específicos que possam ocorrer.

Tópicos

- [Depuração e monitoramento gerais](#)
- [Problema RunBooks](#)
- [Problemas conhecidos](#)

Conteúdo detalhado:

- [Depuração e monitoramento gerais](#)
 - [Fontes úteis de informações sobre registros e eventos](#)
 - [Arquivos de log no ambiente \(EC2instâncias da Amazon\)](#)
 - [CloudFormation Pilhas](#)
 - [Falhas do sistema devido a um problema e refletidas pela atividade de grupo do Amazon EC2 Auto Scaling](#)
 - [Aparência típica EC2 do console Amazon](#)
 - [Anfitriões de infraestrutura](#)
 - [Hosts de infraestrutura e desktops virtuais](#)
 - [Hosts em um estado encerrado](#)
 - [Comandos úteis relacionados ao Active Directory \(AD\) para referência](#)
 - [DCVDepuração do Windows](#)
 - [Encontre informações sobre a DCV versão da Amazon](#)
- [Problema RunBooks](#)
 - [Problemas de instalação](#)
 - [Quero configurar domínios personalizados após a instalação RES](#)
 - [AWS CloudFormation falha ao criar a pilha com a mensagem “mensagem de falha WaitCondition recebida”. Erro: Estados. TaskFailed”](#)
 - [Notificação por e-mail não recebida após a criação bem-sucedida das AWS CloudFormation pilhas](#)

- [Ciclismo de instâncias ou controlador vdc em estado de falha](#)
- [Falha ao excluir a CloudFormation pilha de ambiente devido a um erro no objeto dependente](#)
- [Erro encontrado para o parâmetro de CIDR bloco durante a criação do ambiente](#)
- [CloudFormation falha na criação da pilha durante a criação do ambiente](#)
- [A criação da pilha de recursos externos \(demonstração\) falha com `_AdDomainAdminNode CREATE FAILED`](#)
- [Problemas de gerenciamento de identidade](#)
 - [Não estou autorizado a realizar iam: PassRole](#)
 - [Quero permitir que pessoas fora da minha AWS conta acessem meu estúdio de pesquisa e engenharia sobre AWS recursos](#)
 - [Ao fazer login no ambiente, eu volto imediatamente para a página de login](#)
 - [Erro “Usuário não encontrado” ao tentar fazer login](#)
 - [Usuário adicionado no Active Directory, mas ausente do RES](#)
 - [Usuário indisponível ao criar uma sessão](#)
 - [Erro de limite de tamanho excedido no log do gerenciador de CloudWatch clusters](#)
- [Armazenamento](#)
 - [Eu criei o sistema de arquivos por meio dele, RES mas ele não é montado nos VDI hosts](#)
 - [Eu integrei um sistema de arquivos RES, mas ele não é montado nos hosts VDI](#)
 - [Não consigo ler/escrever nos hosts VDI](#)
 - [Exemplos de casos de uso de tratamento de permissões](#)
 - [Eu criei a Amazon FSx para NetApp ONTAP RES, mas ela não se juntou ao meu domínio](#)
- [Snapshots](#)
 - [Um Snapshot tem um status de Falha](#)
 - [Falha na aplicação de um Snapshot com registros indicando que as tabelas não puderam ser importadas.](#)
- [Infraestrutura](#)
 - [Grupos-alvo do balanceador de carga sem instâncias íntegras](#)
- [Lançamento de desktops virtuais](#)
 - [Um desktop virtual que estava funcionando anteriormente não consegue mais se conectar com êxito](#)
- [Só consigo iniciar 5 desktops virtuais](#)

- [As tentativas de conexão do Windows para desktop falham com “A conexão foi fechada”. Erro de transporte”](#)
- [VDI preso no estado de provisionamento](#)
- [VDI entrar em estado de erro após o lançamento](#)
- [Componente de desktop virtual](#)
 - [A EC2 instância da Amazon está sendo exibida repetidamente encerrada no console](#)
 - [A instância vdc-controller está circulando devido à falha ao ingressar no módulo AD/e VDI mostra Failed Health Check API](#)
 - [O projeto não aparece no menu suspenso ao editar a pilha de software para adicioná-lo](#)
 - [cluster-manager O registro CloudWatch da Amazon mostra “user-home-init< > conta ainda não disponível. Aguardando a sincronização do usuário” \(onde a conta é um nome de usuário\)](#)
 - [A área de trabalho do Windows na tentativa de login diz “Sua conta foi desativada. Consulte seu administrador”](#)
 - [DHCP Problemas de opções com a configuração do AD externa/do cliente](#)
 - [Erro do Firefox MOZILLA _ PKIX _ ERROR _ REQUIRED _ _ TLS _ FEATURE _ MISSING](#)
- [Exclusão do ambiente](#)
 - [res-xxx-cluster pilha no estado "DELETE_FAILED" e não pode ser excluída manualmente devido ao erro “A função é inválida ou não pode ser assumida”](#)
 - [Coletando registros](#)
 - [Baixando VDI registros](#)
 - [Baixando registros de EC2 instâncias Linux](#)
 - [Baixando registros de EC2 instâncias do Windows](#)
 - [Coletando ECS registros do WaitCondition erro](#)
- [Ambiente de demonstração](#)
 - [Erro de login no ambiente de demonstração ao lidar com a solicitação de autenticação ao provedor de identidade](#)
- [Problemas conhecidos 2024.x](#)
 - [Problemas conhecidos 2024.x](#)
 - [\(2024.08\) Os desktops virtuais falham ao montar o bucket de leitura/gravação do Amazon S3 com o bucket raiz e prefixo personalizado ARN](#)
 - [\(2024.06\) A aplicação do instantâneo falha quando o nome do grupo AD contém espaços](#)

- [\(2024.04-2024.04.02\) Limite de permissão fornecido IAM não anexado à função das instâncias VDI](#)
- [\(2024.04.02 e anteriores\) As instâncias do Windows NVIDIA em ap-southeast-2 \(Sydney\) falham ao iniciar](#)
- [\(2024.04 e 2024.04.01\) falha de exclusão em RES GovCloud](#)
- [\(2024.04 - 2024.04.02\) O desktop virtual Linux pode ficar preso no status "" na reinicialização RESUMING](#)
- [\(2024.04.02 e anteriores\) Falha ao sincronizar usuários do AD cujo SAMAccountName atributo inclui letras maiúsculas ou caracteres especiais](#)
- [\(2024.04.02 e anteriores\) A chave privada para acessar o bastion host é inválida](#)
- [\(2024.06 e anteriores\) Membros do grupo não sincronizados durante a RES sincronização do AD](#)
- [\(2024.06 e anteriores\) CVE -2024-6387, RegreSSHion, Vulnerabilidade de segurança no Ubuntu RHEL9 VDIs](#)

Depuração e monitoramento gerais

Esta seção contém informações sobre onde as informações podem ser encontradas RES.

- [Fontes úteis de informações sobre registros e eventos](#)
 - [Arquivos de log no ambiente \(EC2 instâncias da Amazon\)](#)
 - [CloudFormation Pilhas](#)
 - [Falhas do sistema devido a um problema e refletidas pela atividade de grupo do Amazon EC2 Auto Scaling](#)
- [Aparência típica EC2 do console Amazon](#)
 - [Anfitriões de infraestrutura](#)
 - [Hosts de infraestrutura e desktops virtuais](#)
 - [Hosts em um estado encerrado](#)
 - [Comandos úteis relacionados ao Active Directory \(AD\) para referência](#)
- [DCV Depuração do Windows](#)
- [Encontre informações sobre a DCV versão da Amazon](#)

Fontes úteis de informações sobre registros e eventos

Há várias fontes de informações retidas que podem ser referenciadas para fins de solução de problemas e monitoramento.

Arquivos de log no ambiente (EC2instâncias da Amazon)

Existem arquivos de log nas EC2 instâncias da Amazon em uso pelo RES. O Gerenciador de SSM Sessões pode ser usado para abrir uma sessão na instância para examinar esses arquivos.

Em instâncias de infraestrutura, como o gerenciador de cluster e o controlador vdc, os registros de aplicativos e outros podem ser encontrados nos seguintes locais.

- /opt/idea/app/logs/application.log
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssdl/
- /var/log/mensagens
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/.log cloud-init-output

Em um desktop virtual Linux, o seguinte contém arquivos de log úteis

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

No Windows, os registros de instâncias de desktop virtual podem ser encontrados em

- PS C:\ProgramData\nice\ dcv\ log
- PS C:\ProgramData\nice\DCVSessionManagerAgent\ log

No Windows, o registro de alguns aplicativos pode ser encontrado em:

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

No Windows, os arquivos de NICE DCV certificado podem ser encontrados em:

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

Grupos de CloudWatch log da Amazon

A Amazon EC2 e os recursos AWS Lambda computacionais registram informações nos Amazon CloudWatch Log Groups. As entradas de registro dentro delas podem fornecer informações úteis para solucionar possíveis problemas ou para obter informações gerais.

Esses grupos são nomeados da seguinte forma:

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

Ao examinar grupos de registros, pode ser útil filtrar usando cadeias de caracteres maiúsculas e minúsculas, como as seguintes. Isso produzirá somente as mensagens que contêm as sequências de caracteres anotadas.

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

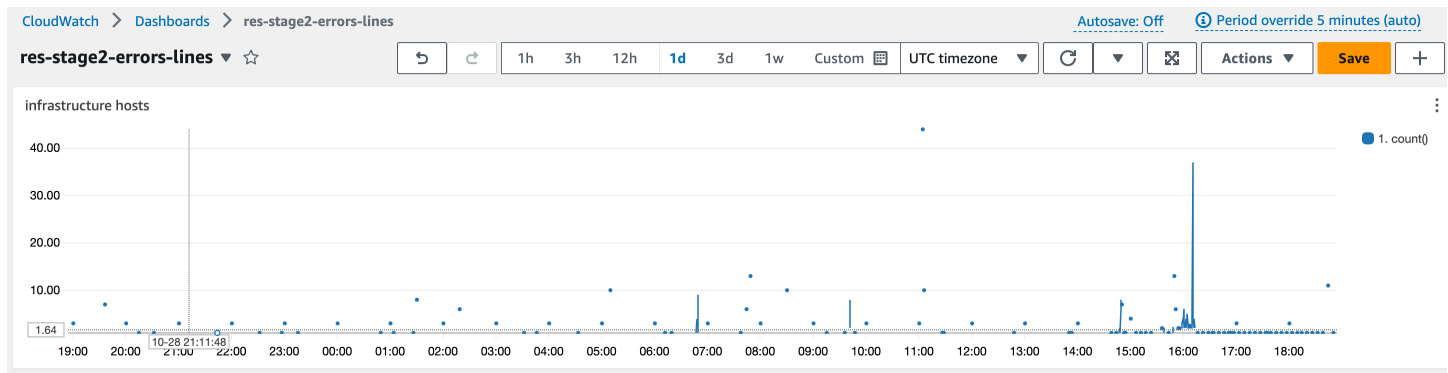
Outro método de monitoramento de problemas é criar CloudWatch painéis da Amazon que contêm widgets que exibem os dados de interesse.

Um exemplo é criar um widget que conte a ocorrência do erro das strings ERROR e represente-as graficamente como linhas. Esse método facilita a detecção da ocorrência de possíveis problemas ou tendências que indicam que ocorreu uma mudança no padrão.

Veja a seguir um exemplo disso para os hosts de infraestrutura. Para usar isso, concatene as linhas de consulta e substitua os <region> atributos <envname> e pelos valores apropriados.

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

Um exemplo do Painel pode aparecer da seguinte forma:



CloudFormation Pilhas

As CloudFormation pilhas criadas durante a criação do ambiente contêm recursos, eventos e informações de saída associadas à configuração do ambiente.

Para cada uma das pilhas, a guia Eventos, Recursos e Saídas pode ser consultada para obter informações sobre as pilhas.

RESpilhas:

- <envname>-bootstrap
- <envname>-cluster
- <envname>-métricas
- <envname>- serviço de diretório
- <envname>-provedor de identidade
- <envname>-armazenamento compartilhado
- <envname>-gerenciador de clusters
- <envname>-vdc
- <envname>-anfitrião-bastião

Demo Environment Stack (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 recursos para um ambiente de demonstração.)

- <envname>
- <envname>-Trabalho em rede
- <envname>- DirectoryService
- <envname>-Armazenamento
- <envname>- WindowsManagementHost

Falhas do sistema devido a um problema e refletidas pela atividade de grupo do Amazon EC2 Auto Scaling

Se RES UIs indicarem erros no servidor, a causa pode ser um software aplicativo ou outro problema.

Cada um dos grupos de escalonamento automático de EC2 instâncias da Amazon (ASGs) de infraestrutura contém uma guia Atividade que pode ser útil para detectar a atividade de escalabilidade das instâncias. Se as páginas da interface do usuário apresentarem algum erro ou não estiverem acessíveis, verifique se há várias instâncias encerradas no EC2 console da Amazon

e verifique a guia Auto Scaling Group Activity para ver as ASG relacionadas para determinar se as instâncias da EC2 Amazon estão em ciclo.

Nesse caso, use o grupo de CloudWatch log relacionado da Amazon para a instância para determinar se erros estão sendo registrados que possam indicar a causa do problema. Também pode ser possível usar o console de SSM sessão para abrir uma sessão em uma instância em execução desse tipo e examinar os arquivos de log na instância para determinar a causa antes que a instância seja marcada como não íntegra e encerrada pelo. ASG

O ASG console pode mostrar uma atividade semelhante à seguinte se esse problema estiver ocorrendo.

The screenshot shows the Amazon EC2 console interface for a Target Group named 'res-bicfn3-web-portal-e2958adc'. The breadcrumb navigation is 'EC2 > Target groups > res-bicfn3-web-portal-e2958adc'. The 'Load Balancers' menu item in the left sidebar is circled in red. The 'Details' section shows the following information:

- Target type: Instance
- Protocol: Port: HTTPS: 8443
- Protocol version: HTTP1
- VPC: vpc-011d10e23ad10cb8e
- IP address type: IPv4
- Load balancer: res-bicfn3-external-alb

The 'Distribution of targets by Availability Zone (AZ)' section shows:

Total targets	1	Healthy	1	Unhealthy	0	Unused	0	Initial	0	Draining	0
---------------	---	---------	---	-----------	---	--------	---	---------	---	----------	---

The 'Registered targets (1)' table is shown below:

Instance ID	Name	Port	Zone	Health status	Health status details
i-0ba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1-c	healthy	

Aparência típica EC2 do console Amazon

Esta seção contém capturas de tela do sistema operando em vários estados.

Anfitriões de infraestrutura

O EC2 console da Amazon, quando nenhum desktop está em execução, geralmente é semelhante ao seguinte. As instâncias mostradas são a RES infraestrutura que a Amazon EC2 hospeda. O prefixo no nome de uma instância é o nome do RES ambiente.

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Instances (5) Info

Find Instance by attribute or tag (case-sensitive)

res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

Hosts de infraestrutura e desktops virtuais

No EC2 console da Amazon, quando os desktops virtuais estão em execução, eles parecem semelhantes aos seguintes. Nesse caso, os desktops virtuais são anotados em vermelho. O sufixo do nome da instância é o usuário que criou a área de trabalho. O nome no centro é o Nome da sessão definido no momento da inicialização e pode ser o padrão MyDesktop "" ou o nome definido pelo usuário.

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

Instances (7) Info

Find Instance by attribute or tag (case-sensitive)

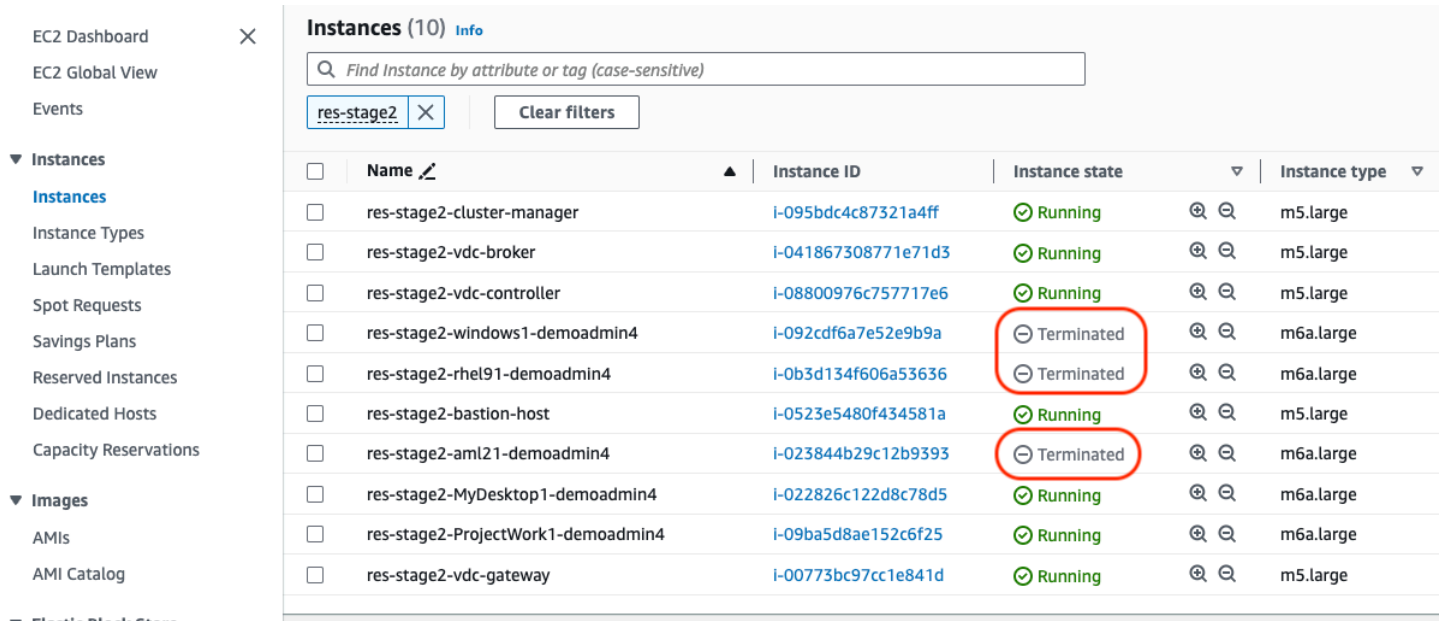
res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
<input type="checkbox"/>	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

Hosts em um estado encerrado

Quando o EC2 console da Amazon mostra instâncias encerradas, elas geralmente são hosts de desktop que foram encerradas. Se o console incluir hosts de infraestrutura em estado encerrado, especialmente se houver vários do mesmo tipo, isso pode indicar um problema no sistema em andamento.

A imagem a seguir mostra instâncias de desktop que foram encerradas.



<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-windows1-demoadmin4	i-092cdf6a7e52e9b9a	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-rhel91-demoadmin4	i-0b3d134f606a53636	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-aml21-demoadmin4	i-023844b29c12b9393	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
<input type="checkbox"/>	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

Comandos úteis relacionados ao Active Directory (AD) para referência

Veja a seguir exemplos de comandos relacionados ao Ldap que podem ser inseridos em hosts de infraestrutura para visualizar informações relacionadas à configuração do AD. O domínio e outros parâmetros usados devem refletir aqueles inseridos no momento da criação do ambiente.

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

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

DCVDepuração do Windows

Em uma área de trabalho do Windows, você pode listar a sessão associada a ela usando o seguinte:

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

Encontre informações sobre a DCV versão da Amazon

A Amazon DCV é utilizada para sessões de desktop virtual. [AWS Amazon DCV](#). Os exemplos a seguir mostram como determinar a versão do DCV software instalado.

Linux

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

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

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

Windows

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

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

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

Problema RunBooks

A seção a seguir contém problemas que podem ocorrer, como detectá-los e sugestões sobre como resolvê-los.

- [Problemas de instalação](#)
 - [Quero configurar domínios personalizados após a instalação RES](#)
 - [AWS CloudFormation falha ao criar a pilha com a mensagem “mensagem de falha WaitCondition recebida”. Erro: Estados. TaskFailed”](#)
 - [Notificação por e-mail não recebida após a criação bem-sucedida das AWS CloudFormation pilhas](#)

- [Ciclismo de instâncias ou controlador vdc em estado de falha](#)
- [Falha ao excluir a CloudFormation pilha de ambiente devido a um erro no objeto dependente](#)
- [Erro encontrado para o parâmetro de CIDR bloco durante a criação do ambiente](#)
- [CloudFormation falha na criação da pilha durante a criação do ambiente](#)
- [A criação da pilha de recursos externos \(demonstração\) falha com `_ AdDomainAdminNode CREATE FAILED`](#)
- [Problemas de gerenciamento de identidade](#)
 - [Não estou autorizado a realizar iam: PassRole](#)
 - [Quero permitir que pessoas fora da minha AWS conta acessem meu estúdio de pesquisa e engenharia sobre AWS recursos](#)
 - [Ao fazer login no ambiente, eu volto imediatamente para a página de login](#)
 - [Erro “Usuário não encontrado” ao tentar fazer login](#)
 - [Usuário adicionado no Active Directory, mas ausente do RES](#)
 - [Usuário indisponível ao criar uma sessão](#)
 - [Erro de limite de tamanho excedido no log do gerenciador de CloudWatch clusters](#)
- [Armazenamento](#)
 - [Eu criei o sistema de arquivos por meio dele, RES mas ele não é montado nos VDI hosts](#)
 - [Eu integrei um sistema de arquivos RES, mas ele não é montado nos hosts VDI](#)
 - [Não consigo ler/escrever nos hosts VDI](#)
 - [Exemplos de casos de uso de tratamento de permissões](#)
 - [Eu criei a Amazon FSx para NetApp ONTAP RES, mas ela não se juntou ao meu domínio](#)
- [Snapshots](#)
 - [Um Snapshot tem um status de Falha](#)
 - [Falha na aplicação de um Snapshot com registros indicando que as tabelas não puderam ser importadas.](#)
- [Infraestrutura](#)
 - [Grupos-alvo do balanceador de carga sem instâncias íntegras](#)
- [Lançamento de desktops virtuais](#)
 - [Um desktop virtual que estava funcionando anteriormente não consegue mais se conectar com êxito](#)
- [So consigo iniciar 5 desktops virtuais](#)

- [As tentativas de conexão do Windows para desktop falham com “A conexão foi fechada”. Erro de transporte”](#)
- [VDI preso no estado de provisionamento](#)
- [VDI entrar em estado de erro após o lançamento](#)
- [Componente de desktop virtual](#)
 - [A EC2 instância da Amazon está sendo exibida repetidamente encerrada no console](#)
 - [A instância vdc-controller está circulando devido à falha ao ingressar no módulo AD/e VDI mostra Failed Health Check API](#)
 - [O projeto não aparece no menu suspenso ao editar a pilha de software para adicioná-lo](#)
 - [cluster-manager O registro CloudWatch da Amazon mostra “user-home-init< > conta ainda não disponível. Aguardando a sincronização do usuário” \(onde a conta é um nome de usuário\)](#)
 - [A área de trabalho do Windows na tentativa de login diz “Sua conta foi desativada. Consulte seu administrador”](#)
 - [DHCP Problemas de opções com a configuração do AD externa/do cliente](#)
 - [Erro do Firefox MOZILLA _ PKIX _ ERROR _ REQUIRED _ _ TLS _ FEATURE _ MISSING](#)
- [Exclusão do ambiente](#)
 - [res-xxx-cluster pilha no estado "DELETE_FAILED" e não pode ser excluída manualmente devido ao erro “A função é inválida ou não pode ser assumida”](#)
 - [Coletando registros](#)
 - [Baixando VDI registros](#)
 - [Baixando registros de EC2 instâncias Linux](#)
 - [Baixando registros de EC2 instâncias do Windows](#)
 - [Coletando ECS registros do WaitCondition erro](#)
- [Ambiente de demonstração](#)
 - [Erro de login no ambiente de demonstração ao lidar com a solicitação de autenticação ao provedor de identidade](#)

Problemas de instalação


Tópicos

- [Quero configurar domínios personalizados após a instalação RES](#)

- [AWS CloudFormation falha ao criar a pilha com a mensagem “mensagem de falha WaitCondition recebida”. Erro: Estados. TaskFailed”](#)
- [Notificação por e-mail não recebida após a criação bem-sucedida das AWS CloudFormation pilhas](#)
- [Ciclismo de instâncias ou controlador vdc em estado de falha](#)
- [Falha ao excluir a CloudFormation pilha de ambiente devido a um erro no objeto dependente](#)
- [Erro encontrado para o parâmetro de CIDR bloco durante a criação do ambiente](#)
- [CloudFormation falha na criação da pilha durante a criação do ambiente](#)
- [A criação da pilha de recursos externos \(demonstração\) falha com _ AdDomainAdminNode CREATE FAILED](#)

.....

Quero configurar domínios personalizados após a instalação RES

 Note

Pré-requisitos: Você deve armazenar o certificado e o PrivateKey conteúdo em um segredo do Secrets Manager antes de executar essas etapas.

Adicionar certificados ao cliente web

1. Atualize o certificado anexado ao ouvinte do balanceador de carga external-alb:
 - a. Navegue até o balanceador de carga RES externo no AWS console em EC2> Balanceamento de carga > Balanceadores de carga.
 - b. Procure o balanceador de carga que segue a convenção de nomenclatura. *<env-name>-external-alb*
 - c. Verifique os ouvintes conectados ao balanceador de carga.
 - d. Atualize o ouvinte que tem um TLS certificado DefaultSSL/anexado com os detalhes do novo certificado.
 - e. Salve as alterações.
2. Na tabela de configurações do cluster:
 - a. Encontre a tabela de configurações de cluster em DynamoDB -> Tabelas ->. *<env-name>.cluster-settings*

- b. Acesse Explorar itens e filtrar por atributo — nome “chave”, tipo “string”, condição “contém” e valor “external_alb”.
 - c. `cluster.load_balancers.external_alb.certificates.provided` Defina como Verdadeiro.
 - d. Atualize o valor `decluster.load_balancers.external_alb.certificates.custom_dns_name`. Esse é o nome de domínio personalizado para a interface de usuário da web.
 - e. Atualize o valor `decluster.load_balancers.external_alb.certificates.acm_certificate_arn`. Esse é o Amazon Resource Name (ARN) para o certificado correspondente armazenado no Amazon Certificate Manager (ACM).
3. Atualize o registro correspondente do subdomínio Route53 que você criou para seu cliente web para apontar para o DNS nome do balanceador de carga externo do laboratório. `<env-name>-external-alb`
 4. Se já SSO estiver configurado no ambiente, reconfigure SSO com as mesmas entradas que você usou inicialmente no botão Configurações gerais > Provedor de identidade > Login único > Status > Editar no portal da RES web.

Adicione certificados ao VDI

1. Conceda permissão ao RES aplicativo para realizar uma GetSecret operação no segredo adicionando as seguintes tags aos segredos:
 - `res:EnvironmentName : <env-name>`
 - `res:ModuleName : virtual-desktop-controller`
2. Na tabela de configurações do cluster:
 - a. Encontre a tabela de configurações de cluster em DynamoDB -> Tabelas ->. `<env-name>.cluster-settings`
 - b. Acesse Explorar itens e filtrar por atributo — nome “chave”, tipo “string”, condição “contém” e valor “dvc_connection_gateway”.
 - c. `vdc.dvc_connection_gateway.certificate.provided` Defina como Verdadeiro.
 - d. Atualize o valor `devdc.dvc_connection_gateway.certificate.custom_dns_name`. Esse é o nome de domínio personalizado para VDI acesso.

- e. Atualize o valor `devdc.dcv_connection_gateway.certificate.certificate_secret_arn`. Esse é ARN o segredo que contém o conteúdo do certificado.
 - f. Atualize o valor `devdc.dcv_connection_gateway.certificate.private_key_secret_arn`. Esse é ARN o segredo que contém o conteúdo da chave privada.
3. Atualize o modelo de execução usado para a instância do gateway:
- a. Abra o grupo Auto Scaling no AWS console em EC2> Auto Scaling > Auto Scaling Groups.
 - b. Selecione o grupo de escalonamento automático do gateway que corresponde ao RES ambiente. O nome segue a convenção `<env-name>-vdc-gateway-asg` de nomenclatura.
 - c. Encontre e abra o modelo de lançamento na seção de detalhes.
 - d. Em Detalhes > Ações > escolha Modificar modelo (Criar nova versão).
 - e. Role para baixo até Detalhes avançados.
 - f. Role até a parte inferior, até Dados do usuário.
 - g. Procure as palavras `CERTIFICATE_SECRET_ARN` `PRIVATE_KEY_SECRET_ARN` e. Atualize esses valores com o ARNs conteúdo fornecido aos segredos que contém o certificado (consulte a etapa 2.c) e a chave privada (consulte a etapa 2.d).
 - h. Certifique-se de que o grupo Auto Scaling esteja configurado para usar a versão recém-criada do modelo de lançamento (na página do grupo Auto Scaling).
4. Atualize o registro correspondente do subdomínio Route53 que você criou para seus desktops virtuais para apontar para o DNS nome do balanceador de carga nlb externo: `<env-name>-external-nlb`
5. Encerre a instância existente do `dcv-gateway: <env-name>-vdc-gateway` e espere que uma nova seja ativada.

.....

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 criação bem-sucedida das AWS CloudFormation pilhas, 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 EC2 console da Amazon para obter evidências de casos de ciclismo.

Se houver EC2 instâncias da Amazon com o <envname> prefixo que aparecem como encerradas e depois são 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 as VPC sub-redes públicas e privadas e outros parâmetros selecionados foram criados pela pilha.

Se algum dos parâmetros estiver incorreto, talvez seja necessário excluir e replantar o RES ambiente. Para obter 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 do (s) recurso (s) de se conectar ou ingressar no Active Directory.

Para verificar o problema:

1. Na linha de comando, inicie uma sessão 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.

```
[root@ip-... ]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
 Main PID: 31248 (sss)           Might see "inactive"/"failed" here
   CGroup: /system.slice/sss.service
           └─31248 /usr/sbin/sss -i --logger=files
             └─31249 /usr/libexec/sss/sss_be --domain corp.res.com --uid 0 --gid 0 --logger=files
               └─31251 /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger=files
                 └─31252 /usr/libexec/sss/sss_pam --uid 0 --gid 0 --logger=files

Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
```

Might see errors highlighted in RED here

SSMregistro de erros

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 ter 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 RES pilha.
 - `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 redefini-la 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 RES diretório e escolha Ações.
 - iii. Selecione Redefinir senha do 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 você atualizou o valor, 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 `ovdcvhostsecuritygroup`, isso pode ser devido a uma EC2 instância da Amazon que foi executada em uma RES sub-rede ou grupo de segurança criado usando o console. AWS

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

.....

Erro encontrado para o parâmetro de CIDR bloco durante a criação do ambiente

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

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 (demonstração) 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 EC2 patches da Amazon 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 de SSM RunCommand /Automation, verifique se a execução de um SSM documento relacionado a patches coincide com o lançamento de uma instância.
3. Nos arquivos de log das EC2 instâncias Amazon 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 RES instâncias 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 a uma configuração incorreta. Para obter informações sobre como definir sua SSO configuração, consulte:

- [the section called “Configuração SSO com o IAM Identity Center”](#)
- [the section called “Configurando seu provedor de identidade para SSO”](#)

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

Tópicos

- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meu estúdio de pesquisa e engenharia sobre AWS recursos](#)
- [Ao fazer login no ambiente, eu volto imediatamente para a página de login](#)
- [Erro “Usuário não encontrado” ao tentar fazer login](#)
- [Usuário adicionado no Active Directory, mas ausente do RES](#)
- [Usuário indisponível ao criar uma sessão](#)
- [Erro de limite de tamanho excedido no log do gerenciador de CloudWatch clusters](#)

.....

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a PassRole ação iam:, suas políticas devem ser atualizadas para permitir que você transfira uma função para RES o.

Alguns AWS serviços permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado marymajor tenta usar o console para realizar uma ação no. RES No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela execute a PassRole ação iam:. Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

.....

Quero permitir que pessoas fora da minha AWS conta acessem meu estúdio de pesquisa e engenharia sobre AWS recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber como fornecer acesso aos seus recursos em todas AWS as contas que você possui, consulte [Fornecer acesso a um IAM usuário em outra AWS conta que você possui](#) no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos para AWS contas de terceiros, consulte [Como fornecer acesso a AWS contas pertencentes a terceiros](#) no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte [Fornecendo acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte [Como as IAM funções diferem das políticas baseadas em recursos](#) no Guia do usuário. IAM

.....

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

Esse problema ocorre quando sua SSO integração 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](#).
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](#)
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 SSO de configuração estão corretos. Se estiverem incorretos, altere o valor da chave `sso_enabled` para `False`.

Edit item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#) 

Attributes

Attribute name	Value
key - Partition key	identity-provider.cognito.sso_enabled
value	<input type="radio"/> True <input checked="" type="radio"/> False 

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

.....

Erro “Usuário não encontrado” ao tentar fazer login

Se um usuário receber o erro “Usuário não encontrado” ao tentar fazer login na RES interface e estiver presente no Active Directory:

- Se o usuário não estiver presente RES e você o tiver adicionado recentemente ao AD
 - É possível que o usuário ainda não esteja sincronizado com. RES RESsincroniza 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 em [Usuário adicionado no Active Directory, mas ausente do RES](#).
- Se o usuário estiver presente em RES:
 1. Certifique-se de que o mapeamento de atributos esteja configurado corretamente. Para obter mais informações, consulte [Configurando seu provedor de identidade para login único \(\) SSO](#).
 2. Certifique-se de que o SAML assunto e o SAML e-mail 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 RES, a sincronização do AD precisa ser acionada. A sincronização do AD é realizada de hora em hora por uma função Lambda que importa entradas do AD para o RES ambiente. 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 [SQSconsole da Amazon](#).
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 deduplicação de mensagens, insira uma sequência de caracteres alfanumérica aleatória. Essa entrada deve ser diferente de todas as chamadas feitas nos últimos 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 seu limite IDP de resultados de pesquisa ldap.

.....

Armazenamento

Tópicos

- [Eu criei o sistema de arquivos por meio dele, RES mas ele não é montado nos VDI hosts](#)
- [Eu integrei um sistema de arquivos RES, mas ele não é montado nos hosts VDI](#)
- [Não consigo ler/escrever nos hosts VDI](#)
- [Eu criei a Amazon FSx para NetApp ONTAPRES, mas ela não se juntou ao meu domínio](#)

.....

Eu criei o sistema de arquivos por meio dele, RES mas ele não é montado nos VDI hosts

Os sistemas de arquivos precisam estar no estado “Disponível” antes de poderem ser montados pelos VDI hosts. Siga as etapas abaixo para validar se o sistema de arquivos está no estado necessário.

Amazon EFS

1. Acesse o [EFSSconsole da Amazon](#).
2. Verifique se o estado do sistema de arquivos está Disponível.
3. Se o estado do sistema de arquivos não estiver Disponível, aguarde antes de iniciar VDI os hosts.

Amazon FSx ONTAP

1. Acesse o [FSxconsole da Amazon](#).
2. Verifique se o status está disponível.
3. Se o status não estiver disponível, aguarde antes de iniciar VDI os hosts.

.....

Eu integrei um sistema de arquivos RES, mas ele não é montado nos hosts VDI

Os sistemas de arquivos integrados RES devem ter as regras de grupo de segurança necessárias configuradas para permitir que VDI os hosts montem os sistemas de arquivos. Como esses sistemas de arquivos são criados externamente RES, RES não gerencia as regras de grupo de segurança associadas.

O grupo de segurança associado aos sistemas de arquivos integrados deve permitir o seguinte tráfego de entrada:

- NFS tráfego (porta: 2049) dos hosts Linux VDC
- SMB tráfego (porta: 445) dos hosts do Windows VDC

.....

Não consigo ler/escrever nos hosts VDI

ONTAP suporta NTFS e estilo MIXED de segurança para os volumes. Os estilos de segurança determinam o tipo de permissão ONTAP usada para controlar o acesso aos dados e qual tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa o estilo de UNIX segurança, SMB os clientes ainda podem acessar os dados (desde que sejam autenticados e autorizados adequadamente) devido à natureza multiprotocolo do. No entanto, ONTAP usa UNIX permissões que somente UNIX clientes podem modificar usando ferramentas nativas.

Exemplos de casos de uso de tratamento de permissões

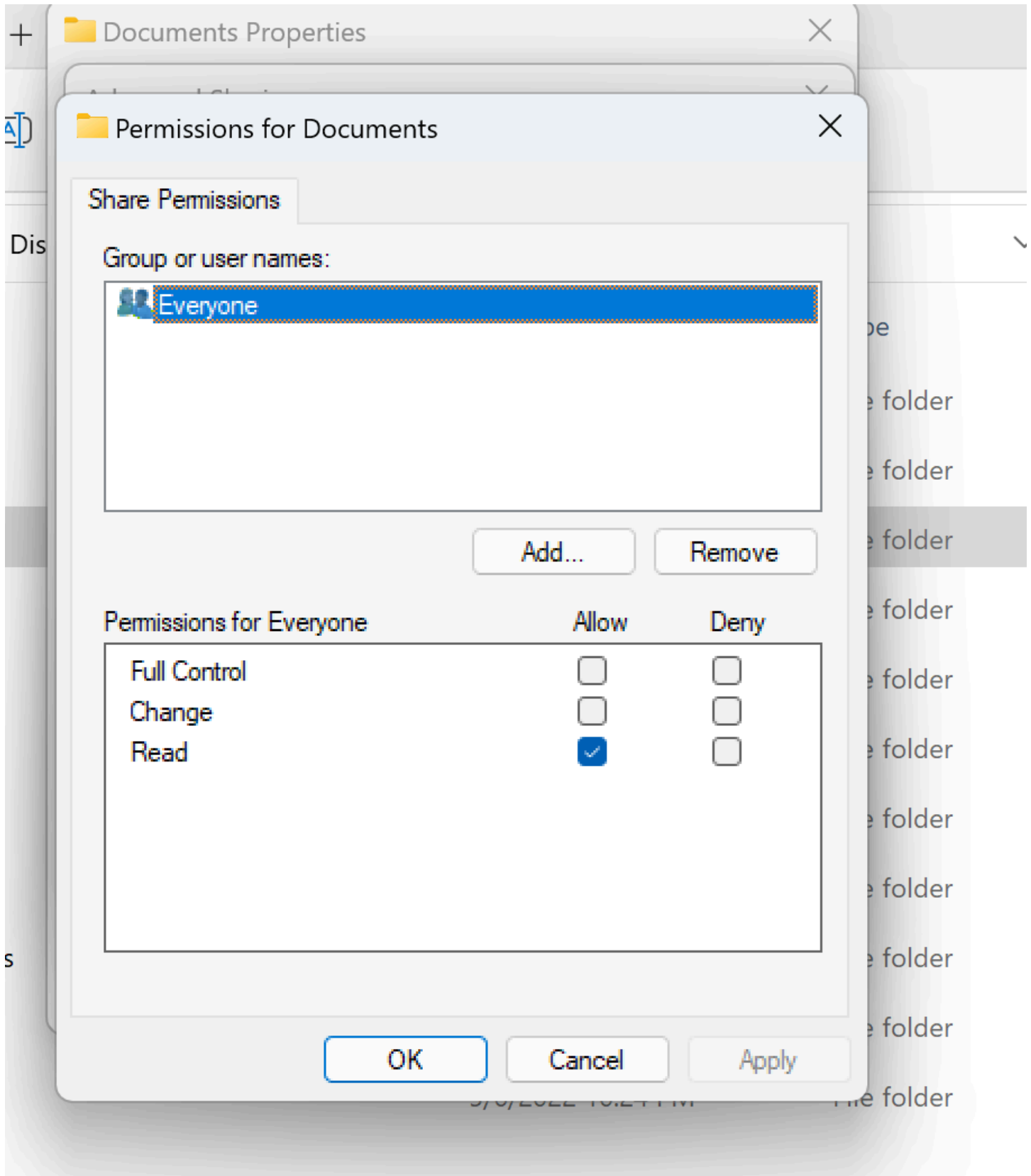
Usando o volume UNIX de estilo com cargas de trabalho do Linux

As permissões podem ser configuradas pelo sudoer para outros usuários. Por exemplo, o seguinte daria a todos os membros permissões <group-ID> completas de leitura/gravação no /<project-name> diretório:

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

Usando o volume de NTFS estilo com cargas de trabalho do Linux e do Windows

As permissões de compartilhamento podem ser configuradas usando as propriedades de compartilhamento de uma pasta específica. Por exemplo, considerando um usuário `user_01` e uma pasta `myfolder`, você pode definir permissões de `Full Control`, ou `Read` para `Allow` ou `Deny`:



Se o volume for usado por clientes Linux e Windows, precisamos configurar um mapeamento de nomes SVM que associe qualquer nome de usuário Linux ao mesmo nome de usuário com o formato de nome de BIOS domínio Net de domínio\ nome de usuário. Isso é necessário para traduzir entre usuários do Linux e do Windows. Para referência, consulte [Habilitando cargas de trabalho multiprotocolo com a Amazon FSx](#) para. NetApp ONTAP

.....

Eu criei a Amazon FSx para NetApp ONTAPRES, mas ela não se juntou ao meu domínio

Atualmente, quando você cria o Amazon FSx for a NetApp ONTAP partir do RES console, o sistema de arquivos é provisionado, mas não se junta ao domínio. Para unir o sistema de ONTAP arquivos criado SVM ao seu domínio, consulte [SVMsIngressar em um Microsoft Active Directory](#) e siga as etapas no [FSxconsole da Amazon](#). Certifique-se de que [as permissões necessárias sejam delegadas à conta de FSx serviços da Amazon](#) no AD. Depois de SVM ingressar no domínio com sucesso, vá para SVM Summary > Endpoints > SMB DNS name e copie o DNS nome, pois você precisará dele posteriormente.

Depois de ingressar no domínio, edite a chave de SMB DNS configuração na tabela do DynamoDB de configurações do cluster:

1. Acesse o console do [Amazon DynamoDB](#).
2. Escolha Tabelas e, em seguida, escolha <stack-name>-cluster-settings.
3. Em Explorar itens da tabela, expanda Filtros e insira o seguinte filtro:
 - Nome do atributo - chave
 - Condição - Igual a
 - Valor - shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns
4. Selecione o item devolvido, depois Ações, Editar item.
5. Atualize o valor com o SMB DNS nome que você copiou anteriormente.
6. Escolha Save and close.

Além disso, garanta que o grupo de segurança associado ao sistema de arquivos permita o tráfego conforme recomendado no [Controle de acesso ao sistema de arquivos com a Amazon VPC](#). VDIOs novos hosts que usam o sistema de arquivos agora poderão montar o sistema associado ao domínio SVM e o sistema de arquivos.

Como alternativa, você pode integrar um sistema de arquivos existente que já esteja associado ao seu domínio usando o recurso Sistema de arquivos RES integrado. Em Gerenciamento de ambiente, escolha Sistemas de arquivos, Sistema de arquivos integrado.

.....

Snapshots

Tópicos

- [Um Snapshot tem um status de Falha](#)
 - [Falha na aplicação de um Snapshot com registros indicando que as tabelas não puderam ser importadas.](#)
-

Um Snapshot tem um status de Falha

Na página RES Snapshots, se um snapshot tiver o status Falha, a causa pode ser determinada acessando o grupo de CloudWatch log da Amazon para o gerenciador de cluster no momento em que o erro ocorreu.

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

.....

Falha na aplicação de um Snapshot com registros indicando que as tabelas não puderam ser importadas.

Se um instantâneo tirado de um ambiente anterior não for aplicado em um novo ambiente, consulte os CloudWatch registros do cluster-manager para identificar o problema. Se o problema mencionar que a nuvem de tabelas necessária não pode ser importada, verifique se o instantâneo está em um estado válido.

1. Faça o download do arquivo metadata.json e verifique se o status das várias ExportStatus tabelas está. COMPLETED Certifique-se de que as várias tabelas tenham o ExportManifest campo definido. Se você não encontrar o conjunto de campos acima, o instantâneo está em um estado inválido e não pode ser usado com a funcionalidade de aplicar instantâneo.
2. Depois de iniciar a criação de um instantâneo, certifique-se de que o status do instantâneo seja ativado. COMPLETED RES O processo de criação do Snapshot leva de 5 a 10 minutos. Recarregue ou visite novamente a página de gerenciamento de instantâneos para garantir que o instantâneo tenha sido criado com sucesso. Isso garantirá que o instantâneo criado esteja em um estado válido.

Infraestrutura

Tópicos

- [Grupos-alvo do balanceador de carga sem instâncias íntegras](#)

Grupos-alvo do balanceador de carga sem instâncias íntegras

Se problemas como mensagens de erro do servidor aparecerem na interface do usuário ou se as sessões de desktop não conseguirem se conectar, isso pode indicar um problema nas EC2 instâncias de infraestrutura da Amazon.

Os métodos para determinar a origem do problema são primeiro verificar se há EC2 instâncias da Amazon no EC2 console da Amazon que pareçam estar sendo encerradas repetidamente e substituídas por novas instâncias. Se for esse o caso, verificar os CloudWatch registros da Amazon pode determinar a causa.

Outro método é verificar os balanceadores de carga no sistema. Uma indicação de que pode haver problemas no sistema é se algum balanceador de carga encontrado no EC2 console da Amazon não mostrar nenhuma instância íntegra registrada.

Um exemplo de aparência normal é mostrado aqui:

EC2 Dashboard × [EC2](#) > [Target groups](#) > [res-bicfn3-web-portal-e2958adc](#)

res-bicfn3-web-portal-e2958adc

Actions ▾

Details

aws:elasticloadbalancing:eu-central-1:474655983723:targetgroup/res-bicfn3-web-portal-e2958adc/3fa0f6c3c3bf4223

Target type Instance	Protocol : Port HTTPS: 8443	Protocol version HTTP1	VPC vpc-011d10e23ad10cb8e
IP address type IPv4	Load balancer res-bicfn3-external-alb		

Total targets	Healthy 1	Unhealthy 0	Unused 0	Initial 0	Draining 0
---------------	--------------	----------------	-------------	--------------	---------------

► **Distribution of targets by Availability Zone (AZ)**
Select values in this table to see corresponding filters applied to the Registered targets table below.

Registered targets (1)

Instance ID	Name	Port	Zone	Health status	Health status details
i-Oba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1c	healthy	

Se a entrada Healthy for 0, isso indica que nenhuma EC2 instância da Amazon está disponível para processar solicitações.

Se a entrada Não íntegra for diferente de 0, isso indica que uma EC2 instância da Amazon pode estar circulando. Isso pode ser devido ao fato de o software do aplicativo instalado não passar pelas verificações de saúde.

Se as entradas íntegras e não íntegras forem 0, isso indica uma possível configuração incorreta da rede. Por exemplo, as sub-redes pública e privada podem não ter correspondências. AZs Se essa condição ocorrer, pode haver texto adicional no console indicando que o estado da rede existe.

Lançamento de desktops virtuais

Tópicos

- [Um desktop virtual que estava funcionando anteriormente não consegue mais se conectar com êxito](#)
- [Só consigo iniciar 5 desktops virtuais](#)
- [As tentativas de conexão do Windows para desktop falham com “A conexão foi fechada”. Erro de transporte”](#)
- [VDI preso no estado de provisionamento](#)

- [VDI entrar em estado de erro após o lançamento](#)

.....

Um desktop virtual que estava funcionando anteriormente não consegue mais se conectar com êxito

Se uma conexão de desktop for fechada ou você não puder mais se conectar a ela, o problema pode ser devido à falha da instância subjacente da Amazon ou a EC2 instância da Amazon EC2 pode ter sido encerrada ou interrompida fora do ambiente. RES O status da interface do usuário do administrador pode continuar mostrando um estado pronto, mas as tentativas de se conectar a ele falham.

O Amazon EC2 Console deve ser usado para determinar se a instância foi encerrada ou interrompida. Se parar, tente iniciá-lo novamente. Se o estado for encerrado, outra área de trabalho precisará ser criada. Todos os dados armazenados no diretório inicial do usuário ainda devem estar disponíveis quando a nova instância for iniciada.

Se a instância que falhou anteriormente ainda aparecer na interface de usuário do administrador, talvez ela precise ser encerrada usando a interface do administrador.

.....

Só consigo iniciar 5 desktops virtuais

O limite padrão para o número de desktops virtuais que um usuário pode iniciar é 5. Isso pode ser alterado por um administrador usando a interface de usuário do administrador da seguinte forma:

- Vá para Configurações da área de trabalho.
- Selecione a guia Servidor.
- No painel DCVSessão, clique no ícone de edição à direita.
- Altere o valor em Sessões permitidas por usuário para o novo valor desejado.
- Selecione Enviar.
- Atualize a página para confirmar se a nova configuração está em vigor.

As tentativas de conexão do Windows para desktop falham com “A conexão foi fechada”. Erro de transporte”

Se uma conexão de desktop do Windows falhar com o erro de interface do usuário “A conexão foi fechada. Erro de transporte”, a causa pode ser devido a um problema no software do DCV servidor relacionado à criação do certificado na instância do Windows.

O grupo de CloudWatch registros da Amazon <envname>/vdc/dcv-connection-gateway pode registrar o erro de tentativa de conexão com mensagens semelhantes às seguintes:

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

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

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

Se isso ocorrer, uma solução pode ser usar o Gerenciador de SSM Sessões para abrir uma conexão com a instância do Windows e remover os dois arquivos relacionados ao certificado a seguir:

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

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

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

Os arquivos devem ser recriados automaticamente e uma tentativa de conexão subsequente pode ser bem-sucedida.

Se esse método resolver o problema e se novas inicializações de desktops Windows produzirem o mesmo erro, use a função Criar pilha de software para criar uma nova pilha de software Windows da instância fixa com os arquivos de certificado regenerados. Isso pode produzir uma pilha de software do Windows que pode ser usada para lançamentos e conexões bem-sucedidos.

.....

VDI preso no estado de provisionamento

Se a inicialização de um desktop permanecer no estado de provisionamento na interface do usuário do administrador, isso pode ser devido a vários motivos.

Para determinar a causa, examine os arquivos de log na instância de desktop e procure erros que possam estar causando o problema. Este documento contém uma lista de arquivos de log e grupos de CloudWatch log da Amazon que contêm informações relevantes na seção Fontes úteis de informações de registros e eventos.

A seguir estão as possíveis causas desse problema.

- O AMI id usado foi registrado como uma pilha de software, mas não é suportado pelo. RES
O script de provisionamento de bootstrap não foi concluído porque a Amazon Machine Image (AMI) não tem a configuração esperada ou as ferramentas necessárias. Os arquivos de log na instância, como `/root/bootstrap/logs/` em uma instância Linux, podem conter informações úteis sobre isso. AMIs retirados do AWS Marketplace podem não funcionar para instâncias de RES desktop. Eles precisam de testes para confirmar se são compatíveis.
- Os scripts de dados do usuário não são executados quando a instância da área de trabalho virtual do Windows é iniciada a partir de uma instância personalizada AMI.

Por padrão, os scripts de dados do usuário são executados uma vez quando uma EC2 instância da Amazon é iniciada. Se você criar um a AMI partir de uma instância de desktop virtual existente, depois registrar uma pilha de software com o AMI e tentar iniciar outro desktop virtual com essa pilha de software, os scripts de dados do usuário não serão executados na nova instância de desktop virtual.

Para corrigir o problema, abra uma janela de PowerShell comando como administrador na instância de desktop virtual original que você usou para criar o AMI e execute o seguinte comando:

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

Em seguida, crie um novo AMI a partir da instância. Você pode usar o novo AMI para registrar pilhas de software e depois iniciar novos desktops virtuais. Observe que você também pode executar o mesmo comando na instância que permanece no estado de provisionamento e reinicializar a instância para corrigir a sessão da área de trabalho virtual, mas você terá o mesmo problema novamente ao iniciar outra área de trabalho virtual a partir da configuração incorreta. AMI

.....

VDIs entrar em estado de erro após o lançamento

Possível problema 1: O sistema de arquivos inicial tem um diretório para o usuário com permissões diferentes. POSIX

Esse pode ser o problema que você enfrentará se os seguintes cenários forem verdadeiros:

1. A RES versão implantada é 2024.01 ou superior.
2. Durante a implantação da RES pilha, o atributo for EnableLdapIDMapping foi definido como True
3. O sistema de arquivos inicial especificado durante a implantação da RES pilha foi usado na versão anterior à RES 2024.01 ou foi usado em um ambiente anterior com definido como EnableLdapIDMapping False

Etapas de resolução: exclua os diretórios do usuário no sistema de arquivos.

1. SSM para o host do gerenciador de clusters.
2. `cd /home`.
3. `ls`- deve listar diretórios com nomes de diretórios que correspondam aos nomes de usuário, como `admin1`, `admin2`.. e assim por diante.
4. Exclua os diretórios, `sudo rm -r 'dir_name'`. Não exclua os diretórios `ssm-user` e `ec2-user`.
5. Se os usuários já estiverem sincronizados com o novo ambiente, exclua o usuário da DDB tabela do usuário (exceto `clusteradmin`).
6. Inicie a sincronização do AD - execute `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` no gerenciador de clusters Amazon. EC2

7. Reinicie a VDI instância no `ERROR` estado a partir da RES página da web. Valide a VDI transição para o Ready estado em cerca de 20 minutos.

Componente de desktop virtual

Tópicos

- [A EC2 instância da Amazon está sendo exibida repetidamente encerrada no console](#)
- [A instância vdc-controller está circulando devido à falha ao ingressar no módulo AD/e VDI mostra Failed Health Check API](#)
- [O projeto não aparece no menu suspenso ao editar a pilha de software para adicioná-lo](#)
- [cluster-manager O registro CloudWatch da Amazon mostra “user-home-init< > conta ainda não disponível. Aguardando a sincronização do usuário” \(onde a conta é um nome de usuário\)](#)
- [A área de trabalho do Windows na tentativa de login diz “Sua conta foi desativada. Consulte seu administrador”](#)
- [DHCPProblemas de opções com a configuração do AD externa/do cliente](#)
- [Erro do Firefox MOZILLA _ PKIX _ ERROR _ REQUIRED _ _ TLS _ FEATURE _ MISSING](#)

A EC2 instância da Amazon está sendo exibida repetidamente encerrada no console

Se uma instância de infraestrutura for exibida repetidamente como encerrada no EC2 console da Amazon, a causa pode estar relacionada à sua configuração e depender do tipo de instância de infraestrutura. A seguir estão os métodos para determinar a causa.

Se a instância vdc-controller mostrar estados encerrados repetidos no EC2 console da Amazon, isso pode ser devido a uma tag secreta incorreta. Os segredos mantidos por RES têm tags que são usadas como parte das políticas de controle de IAM acesso anexadas às EC2 instâncias de infraestrutura da Amazon. Se o controlador vdc estiver circulando e o erro a seguir aparecer no grupo de CloudWatch registros, a causa pode ser que um segredo não tenha sido marcado corretamente. Observe que o segredo precisa ser marcado com o seguinte:

```
{
  "res:EnvironmentName": "<envname>" # e.g. "res-demo"
```

```
"res:ModuleName": "virtual-desktop-controller"
}
```

A mensagem de CloudWatch registro da Amazon para esse erro será semelhante à seguinte:

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

Verifique as tags na EC2 instância da Amazon e confirme se elas correspondem à lista acima.

A instância vdc-controller está circulando devido à falha ao ingressar no módulo AD/e VDI mostra Failed Health Check API

Se o VDI módulo e estiver falhando na verificação de integridade, ele mostrará o seguinte na seção Status do ambiente.

Modules

Environment modules and status



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

Nesse caso, o caminho geral para a depuração é examinar os registros do gerenciador de clusters. [CloudWatch](#) (Procure o grupo de registros chamado <env-name>/cluster-manager.)

Possíveis problemas:

- Se os registros contiverem o texto `Insufficient permissions`, verifique se o `ServiceAccount` nome de usuário fornecido quando a pilha de resolução foi criada está escrito corretamente.

Exemplo de linha de registro:

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

- Você pode acessar o `ServiceAccount` nome de usuário fornecido durante a RES implantação a partir do [SecretsManager console](#). Encontre o segredo correspondente no gerenciador de segredos e escolha Recuperar texto sem formatação. Se o nome de usuário estiver incorreto, escolha Editar para atualizar o valor secreto. Encerre as instâncias atuais do gerenciador de cluster e do controlador vdc. As novas instâncias surgirão em um estado estável.
- O nome de usuário deve ser `ServiceAccount ""` se você estiver utilizando os recursos criados pela [pilha de recursos externos](#) fornecida. Se o `DisableADJoin` parâmetro foi definido como `False` durante a implantação do RES, verifique se o usuário `ServiceAccount ""` tem permissões para criar objetos de computador no AD.
- Se o nome de usuário usado estiver correto, mas os registros contiverem o texto `Invalid credentials`, a senha digitada pode estar errada ou ter expirado.

Exemplo de linha de registro:

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

- Você pode ler a senha digitada durante a criação do ambiente acessando o segredo que armazena a senha no [console do Secrets Manager](#). Selecione o segredo (por exemplo, <env_name>directoryserviceServiceAccountPassword) e escolha Recuperar texto sem formatação.

- Se a senha no segredo estiver incorreta, escolha Editar para atualizar seu valor no segredo. Encerre as instâncias atuais do gerenciador de cluster e do controlador vdc. As novas instâncias usarão a senha atualizada e aparecerão em um estado estável.
- Se a senha estiver correta, pode ser que a senha tenha expirado no Active Directory conectado. Você precisará primeiro redefinir a senha no Active Directory e depois atualizar o segredo. Você pode redefinir a senha do usuário no Active Directory a partir do [console do Directory Service](#):
 1. Escolha a ID de diretório apropriada
 2. Escolha Ações, Redefinir senha do usuário e preencha o formulário com o nome de usuário (por exemplo, "ServiceAccount") e a nova senha.
 3. Se a senha recém-definida for diferente da senha anterior, atualize a senha no segredo correspondente do Secret Manager (por exemplo, `<env_name>directoryserviceServiceAccountPassword`).
 4. Encerre as instâncias atuais do gerenciador de cluster e do controlador vdc. As novas instâncias surgirão em um estado estável.

.....

O projeto não aparece no menu suspenso ao editar a pilha de software para adicioná-lo

Esse problema pode estar relacionado ao seguinte problema associado à sincronização da conta do usuário com o AD. Se esse problema aparecer, verifique o erro `<user-home-init> account not available yet. waiting for user to be synced ""` no grupo de logs do gerenciador de clusters da CloudWatch Amazon para determinar se a causa é a mesma ou está relacionada.

.....

cluster-manager O registro CloudWatch da Amazon mostra “user-home-init< > conta ainda não disponível. Aguardando a sincronização do usuário” (onde a conta é um nome de usuário)

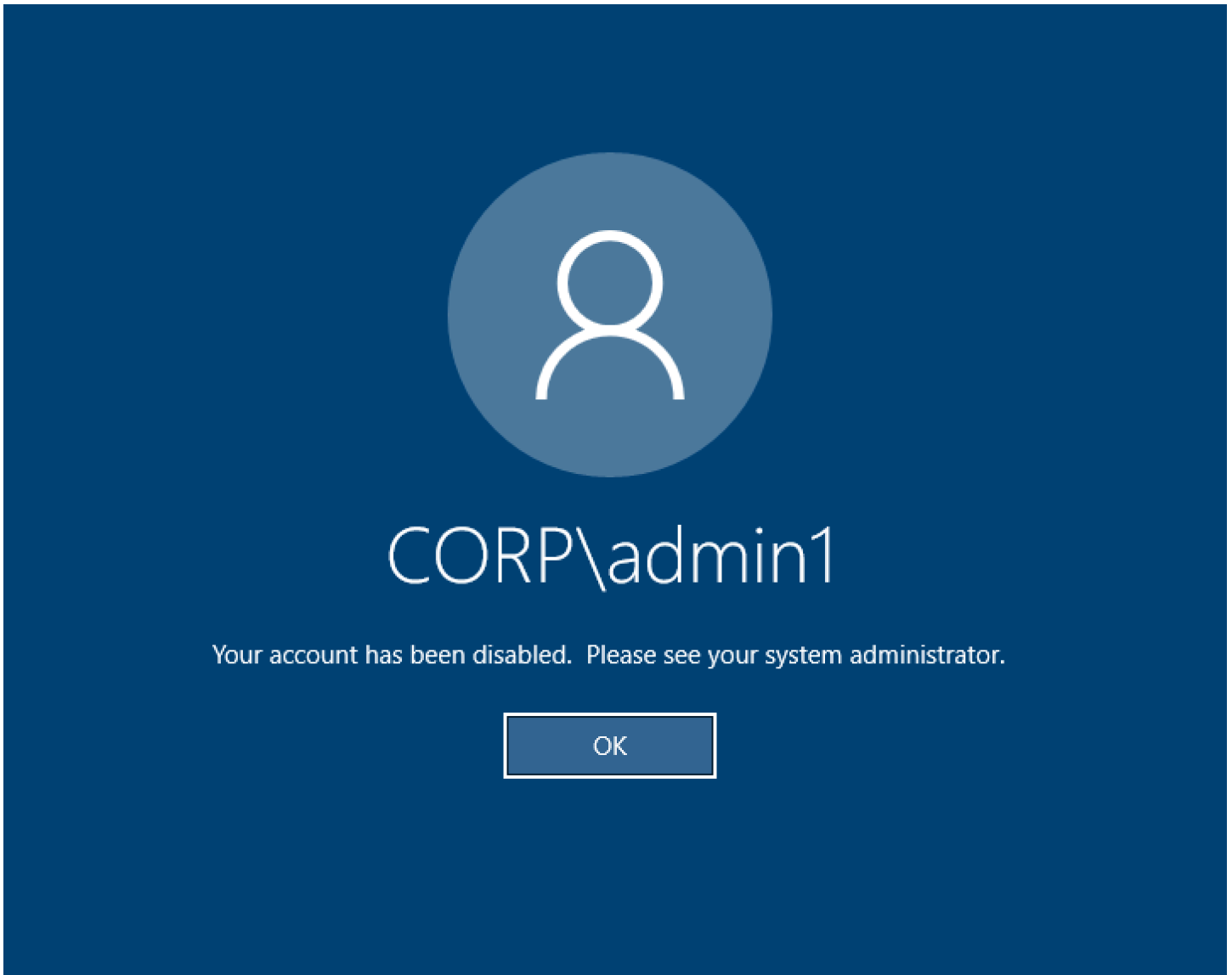
O SQS assinante está ocupado e preso em um loop infinito porque não consegue acessar a conta do usuário. Esse código é acionado ao tentar criar um sistema de arquivos doméstico para um usuário durante a sincronização do usuário.

O motivo pelo qual ele não consegue acessar a conta do usuário pode ser que não RES tenha sido configurado corretamente para o AD em uso. Um exemplo pode ser que o

ServiceAccountCredentialsSecretArn parâmetro usado na criação do RES BI/ambiente não era o valor correto.

.....

A área de trabalho do Windows na tentativa de login diz “Sua conta foi desativada. Consulte seu administrador”



Se o usuário não conseguir fazer login novamente em uma tela bloqueada, isso pode indicar que o usuário foi desativado no AD configurado para RES depois de ter feito login com sucesso viaSSO.

O SSO login deverá falhar se a conta do usuário tiver sido desativada no AD.

.....

DHCPProblemas de opções com a configuração do AD externa/do cliente

Se você encontrar um erro informando "The connection has been closed. Transport error" sobre desktops virtuais do Windows ao usar RES com seu próprio Active Directory, verifique se há algo semelhante ao seguinte no CloudWatch log da dcv-connection-gateway Amazon:

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

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

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

Se você estiver usando um controlador de domínio do AD para suas próprias DHCP opçõesVPC, você precisará:


1. Adicione AmazonProvided DNS aos dois controladores de domínioIPs.
2. Defina o nome do domínio como ec2.internal.

Um exemplo é mostrado aqui. Sem essa configuração, a área de trabalho do Windows exibirá um erro de transporte, porqueRES/DCVprocura o nome do host ip-10-0-x-xx.ec2.internal.

Domain name

 ec2.internal

Domain name servers

 10.0.2.168, 10.0.3.228,
AmazonProvidedDNS

.....

Erro do Firefox MOZILLA _ PKIX _ ERROR _ REQUIRED _ _ TLS _ FEATURE _
MISSING

Ao usar o navegador Firefox, você pode encontrar o tipo de mensagem de erro MOZILLA _ _ PKIX _
ERROR _ REQUIRED _ TLS _ FEATURE _ MISSING ao tentar se conectar a uma área de trabalho
virtual.

[A causa é que o servidor RES web está configurado com TLS + Stapling On, mas não está respondendo com Stapling Validation \(consulte https://support.mozilla.org/en-US/questions/1372483\).](https://support.mozilla.org/en-US/questions/1372483)

Você pode corrigir isso seguindo as instruções em: https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing.

.....

Exclusão do ambiente

Tópicos

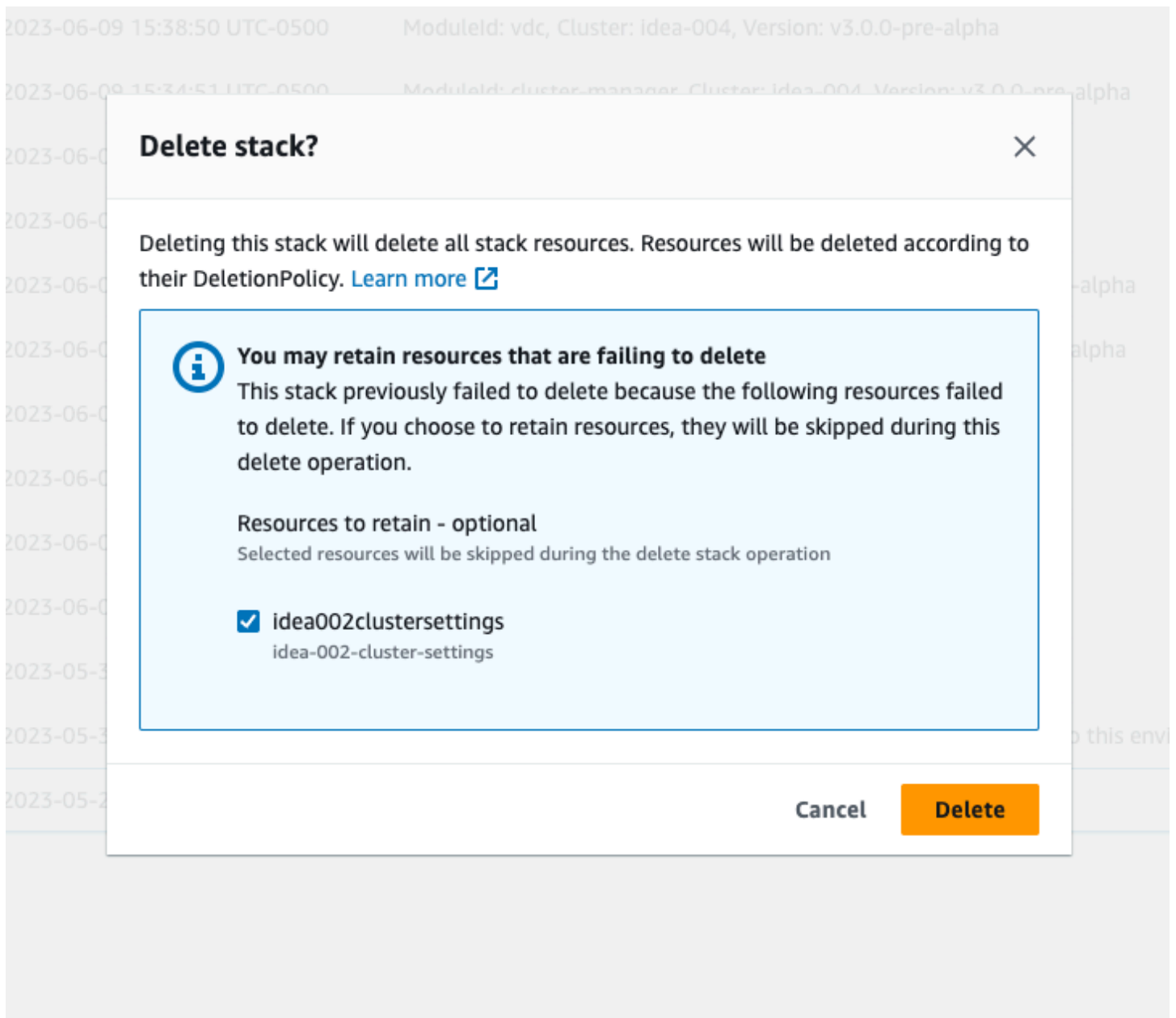
- [res-xxx-cluster pilha no estado "DELETE_FAILED" e não pode ser excluída manualmente devido ao erro "A função é inválida ou não pode ser assumida"](#)
- [Coletando registros](#)
- [Baixando VDI registros](#)
- [Baixando registros de EC2 instâncias Linux](#)
- [Baixando registros de EC2 instâncias do Windows](#)
- [Coletando ECS registros do WaitCondition erro](#)

.....

res-xxx-cluster pilha no estado "DELETE_FAILED" e não pode ser excluída manualmente devido ao erro "A função é inválida ou não pode ser assumida"

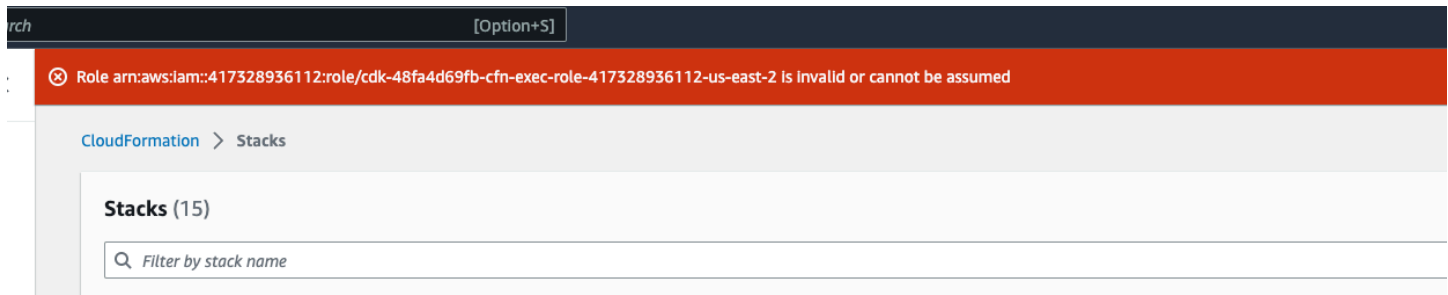
Se você perceber que a pilha res-xxx-cluster "" está no estado "DELETE_FAILED" e não pode ser excluída manualmente, execute as etapas a seguir para excluí-la.

Se você ver a pilha em um estado "DELETE_FAILED", primeiro tente excluí-la manualmente. Pode aparecer uma caixa de diálogo confirmando Excluir pilha. Escolha Excluir.



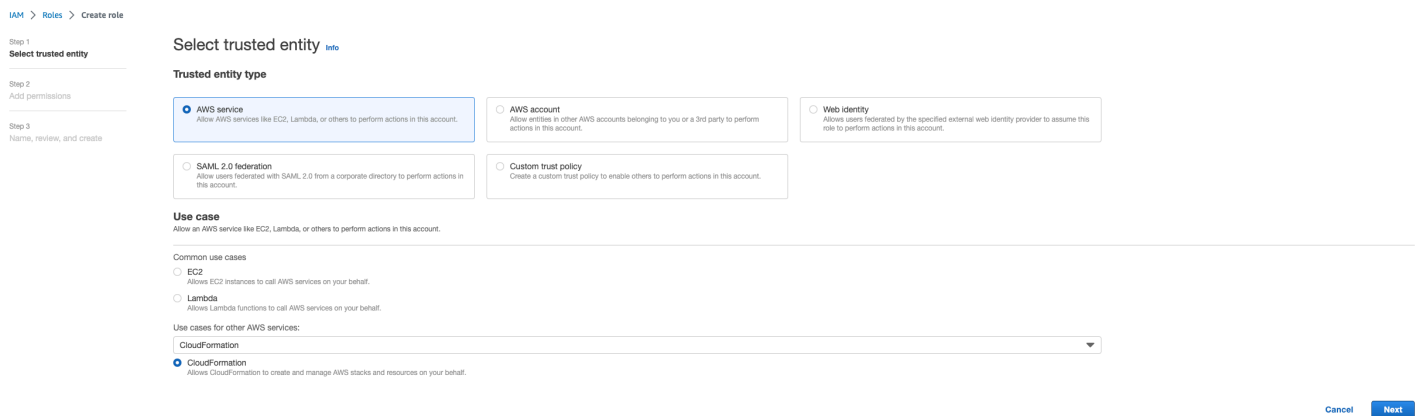
Às vezes, mesmo se você excluir todos os recursos necessários da pilha, ainda poderá ver a mensagem para selecionar os recursos a serem retidos. Nesse caso, selecione todos os recursos como “recursos a serem retidos” e escolha Excluir.

Você pode ver um erro que parece `Role: arn:aws:iam::... is Invalid or cannot be assumed`



Isso significa que a função necessária para excluir a pilha foi excluída primeiro, antes da pilha. Para contornar isso, copie o nome da função. Vá para o IAM console e crie uma função com esse nome usando os parâmetros mostrados aqui, que são:

- Para o tipo de entidade confiável, escolha AWS serviço.
- Para Caso de uso, em Use cases for other AWS services EscolherCloudFormation.



Escolha Próximo. Certifique-se de conceder as permissões `"` e `AWSCloudFormationFullAccess` 'AdministratorAccess' à função. Sua página de avaliação deve ter a seguinte aparência:

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

cdk-48fa4d69b-cfn-exec-role-417328936112-us-east-2

Maximum 64 characters. Use alphanumeric and '+,=,@,_' characters.

Description

Add a short explanation for this role.

Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,=,@,_' characters.

Step 1: Select trusted entities

Edit

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "",
6-       "Effect": "Allow",
7-       "Principal": {
8-         "Service": "cloudformation.amazonaws.com"
9-       },
10-      "Action": "sts:AssumeRole"
11-     }
12-   ]
13- ]

```

Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AWSCloudFormationFullAccess	AWS managed	Permissions policy
AdministratorAccess	AWS managed - job function	Permissions policy

Tags

Em seguida, volte para o CloudFormation console e exclua a pilha. Agora você deve conseguir excluí-la desde que criou a função. Por fim, acesse o IAM console e exclua a função que você criou.

Coletando registros

Fazer login em uma EC2 instância a partir do EC2 console

- Siga [estas instruções](#) para fazer login na sua EC2 instância Linux.
- Siga [estas instruções](#) para fazer login na sua EC2 instância do Windows. Em seguida, abra PowerShell o Windows para executar qualquer comando.

Coletando registros do host da infraestrutura

1. Gerenciador de cluster: obtenha registros do gerenciador de cluster nos seguintes locais e anexe-os ao ticket.
 - a. Todos os registros do grupo de CloudWatch registros<env-name>/cluster-manager.
 - b. Todos os registros no /root/bootstrap/logs diretório na <env-name>-cluster-manager EC2 instância. Siga as instruções vinculadas a “Fazer login em uma EC2 instância a partir do EC2 console” no início desta seção para fazer login na sua instância.

2. Controlador VDC: obtenha os registros do controlador vdc nos seguintes locais e anexe-os ao ticket.
 - a. Todos os registros do grupo de CloudWatch registros<env-name>/vdc-controller.
 - b. Todos os registros no /root/bootstrap/logs diretório na <env-name>-vdc-controller EC2 instância. Siga as instruções vinculadas a “Fazer login em uma EC2 instância a partir do EC2 console” no início desta seção para fazer login na sua instância.

Uma das maneiras de obter os registros com facilidade é seguir as instruções na [Baixando registros de EC2 instâncias Linux](#) seção. O nome do módulo seria o nome da instância.

Coletando VDI registros

Identifique a EC2 instância Amazon correspondente

Se um usuário iniciasse um VDI com nome de sessãoVDI1, o nome correspondente da instância no EC2 console da Amazon seria<env-name>-VDI1-<user name>.

Colete VDI registros do Linux

Faça login na EC2 instância correspondente da Amazon a partir do EC2 console da Amazon seguindo as instruções vinculadas em “Fazer login em uma EC2 instância a partir do EC2 console” no início desta seção. Obtenha todos os registros nos /var/log/dcv/ diretórios /root/bootstrap/logs e na EC2 instância da VDI Amazon.

Uma das maneiras de obter os registros seria enviá-los para o s3 e baixá-los de lá. Para isso, você pode seguir estas etapas para obter todos os registros de um diretório e depois carregá-los:

1. Siga estas etapas para copiar os registros dcv no /root/bootstrap/logs diretório:

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

2. Agora, siga as etapas listadas na próxima seção [Baixando VDI registros](#) para baixar os registros.

Colete VDI registros do Windows

Faça login na EC2 instância correspondente da Amazon a partir do EC2 console da Amazon seguindo as instruções vinculadas em “Fazer login em uma EC2 instância a partir do EC2

console” no início desta seção. Obtenha todos os registros no `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log` diretório da VDI EC2 instância.

Uma das maneiras de obter os registros seria enviá-los para o S3 e baixá-los de lá. Para fazer isso, siga as etapas listadas na próxima seção-[Baixando VDI registros](#).

Baixando VDI registros

1. Atualize a IAM função da VDI EC2 instância para permitir o acesso ao S3.
2. Acesse o EC2 console e selecione sua VDI instância.
3. Selecione a IAM função que está usando.
4. Na seção Políticas de permissão do menu suspenso Adicionar permissões, escolha Anexar políticas e selecione a política do FullAccessAmazonS3.
5. Escolha Adicionar permissões para anexar essa política.
6. Depois disso, siga as etapas listadas abaixo com base no seu VDI tipo para baixar os registros. O nome do módulo seria o nome da instância.
 - a. [Baixando registros de EC2 instâncias Linux](#) para Linux.
 - b. [Baixando registros de EC2 instâncias do Windows](#) para Windows.
7. Por fim, edite a função para remover a AmazonS3FullAccess política.

Note

Todos VDIs usam a mesma IAM função, que é `<env-name>-vdc-host-role-<region>`

Baixando registros de EC2 instâncias Linux

Faça login na EC2 instância da qual você deseja baixar os registros e execute os seguintes comandos para carregar todos os registros em um bucket s3:

```
sudo su -
```

```

ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

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

```

Depois disso, acesse o console do S3, selecione o bucket com o nome <environment_name>-cluster-<region>-<aws_account_number> e faça o download do <module_name>_logs.tar.gz arquivo carregado anteriormente.

.....

Baixando registros de EC2 instâncias do Windows

Faça login na EC2 instância da qual você deseja baixar os registros e execute os seguintes comandos para carregar todos os registros em um bucket do S3:

```

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

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

```

Depois disso, acesse o console do S3, selecione o bucket com o nome <environment_name>-cluster-<region>-<aws_account_number> e faça o download do <module_name>_logs.zip arquivo carregado anteriormente.

.....

Coletando ECS registros do WaitCondition erro

1. Vá até a pilha implantada e selecione a guia Recursos.
2. Expanda Implantar ResearchAndEngineeringStudio → Instalador CreateTaskDef → Tarefas CreateContainer → LogGroupe selecione o grupo de registros para abrir CloudWatch os registros.
3. Obtenha o registro mais recente desse grupo de registros.

.....

Ambiente de demonstração

Tópicos

- [Erro de login no ambiente de demonstração ao lidar com a solicitação de autenticação ao provedor de identidade](#)

.....

Erro de login no ambiente de demonstração ao lidar com a solicitação de autenticação ao provedor de identidade

Problema

Se você tentar fazer login e receber um “Erro inesperado ao processar a solicitação de autenticação ao provedor de identidade”, suas senhas podem ter expirado. Essa pode ser a senha do usuário com o qual você está tentando fazer login ou da sua Conta do Active Directory Service.

Mitigação

1. Redefina as senhas do usuário e da conta de serviço no [console do serviço de diretório](#).
2. Atualize as senhas da Conta de Serviço no [Secrets Manager](#) para que correspondam à nova senha inserida acima:
 - para a pilha Keycloak: -... PasswordSecret - RESExternal-... - DirectoryService-... com descrição: Senha para o Microsoft Active Directory
 - para RES: res- ServiceAccountPassword -... com Descrição: Senha da conta de serviço do Active Directory

3. Acesse o [EC2console](#) e encerre a instância do gerenciador de cluster. As regras do Auto Scaling acionarão automaticamente a implantação de uma nova instância.

Problemas conhecidos

- [Problemas conhecidos 2024.x](#)

- [\(2024.08\) Os desktops virtuais falham ao montar o bucket de leitura/gravação do Amazon S3 com o bucket raiz e prefixo personalizado ARN](#)
- [\(2024.06\) A aplicação do instantâneo falha quando o nome do grupo AD contém espaços](#)
- [\(2024.04-2024.04.02\) Limite de permissão fornecido IAM não anexado à função das instâncias VDI](#)
- [\(2024.04.02 e anteriores\) As instâncias do Windows NVIDIA em ap-southeast-2 \(Sydney\) falham ao iniciar](#)
- [\(2024.04 e 2024.04.01\) falha de exclusão em RES GovCloud](#)
- [\(2024.04 - 2024.04.02\) O desktop virtual Linux pode ficar preso no status "" na reinicialização RESUMING](#)
- [\(2024.04.02 e anteriores\) Falha ao sincronizar usuários do AD cujo SAMAccountName atributo inclui letras maiúsculas ou caracteres especiais](#)
- [\(2024.04.02 e anteriores\) A chave privada para acessar o bastion host é inválida](#)
- [\(2024.06 e anteriores\) Membros do grupo não sincronizados durante a RES sincronização do AD](#)
- [\(2024.06 e anteriores\) CVE -2024-6387, RegreSSHion, Vulnerabilidade de segurança no Ubuntu RHEL9 VDIs](#)

Problemas conhecidos 2024.x

(2024.08) Os desktops virtuais falham ao montar o bucket de leitura/gravação do Amazon S3 com o bucket raiz e prefixo personalizado ARN

Descrição do bug

O Research and Engineering Studio 2024.08 falha ao montar buckets S3 de leitura/gravação em uma instância de infraestrutura de desktop virtual (VDI) ao usar um bucket raiz (ou seja, `arn:aws:s3:::example-bucket`) e um prefixo personalizado ARN (nome do projeto ou nome do projeto e nome do usuário).

As configurações de bucket que não são afetadas por esse problema incluem:

- buckets somente para leitura
- compartimentos de leitura/gravação com um prefixo como parte do intervalo ARN (ou seja, `arn:aws:s3:::example-bucket/example-folder-prefix`) e prefixo personalizado (nome do projeto ou nome do projeto e nome do usuário)
- compartimentos de leitura/gravação com um repositório raiz ARN, mas sem prefixo personalizado

Depois de provisionar uma VDI instância, o diretório de montagem especificado para esse bucket do S3 não terá o bucket montado. Embora o diretório de montagem no VDI esteja presente, o diretório estará vazio e não conterá o conteúdo atual do bucket. Quando você grava um arquivo no diretório usando o terminal, o erro `Permission denied, unable to write a file` é gerado e o conteúdo do arquivo não é carregado no bucket S3 correspondente.

Versões afetadas

2024.08

Mitigação

1. Para baixar o script de patch e o arquivo de patch (`patch.pyes3_mount_custom_prefix_fix.patch`), execute o comando a seguir, `<output-directory>` substituindo-o pelo diretório em que você deseja baixar o script e o arquivo de patch e `<environment-name>` pelo nome do seu RES ambiente:
 - a. O patch só se aplica a RES 2024.08.
 - b. [O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.](#)
 - c. Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do Amazon S3 para gravar no bucket criado por RES

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

```
mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. Para encerrar a instância do Virtual Desktop Controller (vdc-controller) do seu ambiente, execute os comandos a seguir. (Você já definiu a ENVIRONMENT_NAME variável com o nome do seu RES ambiente na primeira etapa.)

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

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

Note

Para VPC configurações privadas, se você ainda não tiver feito isso, para a <RES-EnvironmentName>-vdc-custom-credential-broker-lambda função, certifique-se de adicionar o Environment variable nome AWS_STS_REGIONAL_ENDPOINTS e o valor deregional. Consulte [Pré-requisitos do bucket Amazon S3 para implantações isoladas VPC](#) Para mais informações.

4. Depois que o grupo-alvo que começa com o nome <RES-EnvironmentName>-vdc-ext ficar íntegro, VDIs será necessário lançar um novo que terá os buckets S3 de leitura/gravação com o bucket raiz ARN e o prefixo personalizado montados corretamente.

.....

(2024.06) A aplicação do instantâneo falha quando o nome do grupo AD contém espaços

Problema

RES2024.06 não aplica instantâneos de versões anteriores se os grupos do AD contiverem espaços em seus nomes.

Os registros do gerenciador de clusters (no grupo de CloudWatch registros) incluirão o `<environment-name>/cluster-manager` seguinte erro durante a sincronização do AD:

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

O erro resulta da aceitação RES somente de nomes de grupos que atendam aos seguintes requisitos:

- Ele só pode conter ASCII letras maiúsculas e minúsculas, dígitos, traço (-), ponto (.) e sublinhado (_)
- Não é permitido um traço (-) como primeiro caractere
- Ele nome não pode conter espaços.

Versões afetadas

2024.06

Mitigação

1. Para baixar o script e o arquivo de patch ([patch.py](#) e [groupname_regex.patch](#)), execute o comando a seguir, `<output-directory>` substituindo-o pelo diretório em que você deseja colocar os arquivos e pelo nome do seu ambiente: `<environment-name> RES`
 - a. O patch só se aplica a RES 2024.06
 - b. [O script de patch requer AWS CLIv2, Python 3.9.16 ou superior e Boto3.](#)
 - c. Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado por: RES

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

```
ENVIRONMENT_NAME=<environment-name>
```

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

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch:

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

3. Para reiniciar a instância do Cluster Manager para seu ambiente, execute os seguintes comandos: Você também pode encerrar a instância no Amazon EC2 Management Console.

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

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

Note

O patch permite que os nomes dos grupos do AD contenham ASCII letras maiúsculas e minúsculas, dígitos, traço (-), ponto (.), sublinhado (_) e espaços com um comprimento total entre 1 e 30, inclusive.

.....
(2024.04-2024.04.02) Limite de permissão fornecido IAM não anexado à função das instâncias VDI

O problema

As sessões de desktop virtual não estão herdando adequadamente a configuração do limite de permissão do projeto. Isso é resultado do limite de permissões definido pelo IAMPermissionBoundary parâmetro não ter sido atribuído adequadamente a um projeto durante a criação desse projeto.

Versões afetadas

2024.04 - 2024.04.02

Mitigação

Siga estas etapas para permitir VDIs herdar adequadamente o limite de permissões atribuído a um projeto:

1. Para baixar o script e o arquivo de patch ([patch.py](#) e [vdi_host_role_permission_boundary.patch](#)), execute o comando a seguir, substituindo-o pelo diretório local em que você gostaria de colocar os arquivos: `<output-directory>`
 - a. O patch só se aplica a RES 2024.04.02. Se você estiver na versão 2024.04 ou 2024.04.01, siga as [etapas listadas no documento público para pequenas atualizações de versão para atualizar seu ambiente para 2024.04.02](#).
 - b. [O script de patch requer AWS CLIv2\), Python 3.9.16 ou superior e Boto3](#).
 - c. Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado por. RES

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

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

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

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch, `<environment-name>` substituindo-o pelo nome do seu RES ambiente:

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

3. Reinicie a instância do cluster-manager em seu ambiente executando esse comando, <environment-name> substituindo-o pelo nome do seu ambiente. RES Você também pode encerrar a instância no Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

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

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

.....

(2024.04.02 e anteriores) As instâncias do Windows NVIDIA em ap-southeast-2 (Sydney) falham ao iniciar

O problema

As Amazon Machine Images (AMIs) são usadas para ativar desktops virtuais (VDIs) RES com configurações específicas. Cada um AMI tem uma ID associada que difere por região. O AMI ID configurado RES para iniciar instâncias Nvidia do Windows em ap-southeast-2 (Sydney) está incorreto no momento.

AMIO -ID ami-0e190f8939a996caf desse tipo de configuração de instância está listado incorretamente em ap-southeast-2 (Sydney). AMIO ID ami-027cf6e71e2e442f4 deve ser usado em vez disso.

Os usuários receberão o seguinte erro ao tentarem iniciar uma instância com o padrão ami-0e190f8939a996cafAMI.

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

Etapas para reproduzir o bug, incluindo um exemplo de arquivo de configuração:

- Implante RES na região ap-southeast-2.

- Execute uma instância usando a pilha de software (AMIIDami-0e190f8939a996caf) NVIDIA padrão do Windows.

Versões afetadas

Todas as RES versões 2024.04.02 ou anteriores são afetadas

Mitigação

A seguinte mitigação foi testada na RES versão 2024.01.01:

- Registre uma nova pilha de software com as seguintes configurações
 - AMIID: ami-027cf6e71e2e442f4
 - Sistema operacional: Windows
 - GPUFabricante: NVIDIA
 - Min. Tamanho de armazenamento (GB): 30
 - Min. RAM(GB): 4
- Use essa pilha de software para iniciar instâncias do Windows NVIDIA

.....

(2024.04 e 2024.04.01) falha de exclusão em RES GovCloud

O problema

Durante o fluxo de trabalho de RES exclusão, o UnprotectCognitoUserPool Lambda inativa a Proteção de Exclusão para grupos de usuários do Cognito, que serão excluídos posteriormente. A execução do Lambda é iniciada pelo. InstallerStateMachine

Devido às diferenças de AWS CLI versão padrão entre Commercial e GovCloud regiões, a update_user_pool chamada no Lambda falhará nas GovCloud regiões.

Os clientes receberão o seguinte erro ao tentarem excluir RES em GovCloud regiões:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection\n\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,\nSmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,\nVerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
```

DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags, AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting

Etapas para reproduzir o bug:

- Implemente RES em uma GovCloud região
- Exclua a RES pilha

Versões afetadas

RESversões 2024.04 e 2024.04.01

Mitigação

A seguinte mitigação foi testada na RES versão 2024.04:

- Abra o UnprotectCognitoUserPool Lambda
 - Convenção de nomenclatura: `<env-name>-InstallerTasksUnprotectCognitoUserPool-...`
- Configurações de tempo de execução -> Editar -> Selecione Tempo de execução Python 3.11 -> Salvar.
- Aberto CloudFormation.
- Exclua a RES pilha -> saia do recurso Retain Installer UNCHECKED -> Excluir.

.....

(2024.04 - 2024.04.02) O desktop virtual Linux pode ficar preso no status "" na reinicialização RESUMING

O problema

Os desktops virtuais Linux podem ficar presos no status "RESUMING" ao serem reiniciados após uma parada manual ou programada.

Depois que a instância é reiniciada, o AWS Systems Manager não executa nenhum comando remoto para criar uma nova DCV sessão e a seguinte mensagem de registro está ausente nos registros do vdc-controller (no grupo de CloudWatch registros): `<environment-name>/vdc/controller CloudWatch`

Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT

Versões afetadas

2024.04 - 2024.04.02

Mitigação

Para recuperar os desktops virtuais que estão presos no estado "RESUMING":


1. SSHna instância do problema a partir do EC2 console.
2. Execute os seguintes comandos na instância:

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

3. Aguarde a reinicialização da instância.

Para evitar que novos desktops virtuais tenham o mesmo problema:

1. Para baixar o script e o arquivo de patch ([patch.py](#) e [vdi_stuck_in_resuming_status.patch](#)), execute o comando a seguir, substituindo-o pelo diretório em que você deseja colocar os arquivos: `<output-directory>`

 Note

- O patch só se aplica a RES 2024.04.02.
- [O script de patch requer AWS CLIv2, Python 3.9.16 ou superior e Boto3.](#)
- Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado por. RES

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

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

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

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch, <environment-name> substituindo-o pelo nome do seu RES ambiente e <aws-region> pela região em que RES está implantado:

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

3. Para reiniciar a instância do VDC Controller para seu ambiente, execute os comandos a seguir, <environment-name> substituindo-a pelo nome do seu RES ambiente:

```
ENVIRONMENT_NAME=<environment-name>

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

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

.....

(2024.04.02 e anteriores) Falha ao sincronizar usuários do AD cujo SAMAccountName atributo inclui letras maiúsculas ou caracteres especiais

O problema

RES falha ao sincronizar usuários do AD depois de SSO configurado por pelo menos duas horas (dois ciclos de sincronização do AD). Os registros do gerenciador de cluster (no grupo de CloudWatch registros) incluem o <environment-name>/cluster-manager seguinte erro durante a sincronização do AD:

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

O erro resulta da aceitação RES apenas de um SAMAccount nome de usuário que atenda aos seguintes requisitos:

- Ele só pode conter ASCII letras minúsculas, dígitos, ponto (.), sublinhado (_).
- Não é permitido um ponto ou sublinhado como primeiro ou último caractere.
- Ele não pode conter dois pontos contínuos ou sublinhados (por exemplo, ..., __, ._, _.).

Versões afetadas

2024.04.02 e anteriores

Mitigação

1. Para baixar o script e o arquivo de patch ([patch.py](#) e [samaccountname_regex.patch](#)), execute o comando a seguir, substituindo-o pelo diretório em que você deseja <output-directory> colocar os arquivos:

Note

- O patch só se aplica a RES 2024.04.02.
- [O script de patch requer AWS CLiv2, Python 3.9.16 ou superior e Boto3.](#)
- Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado por RES

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

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

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

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch, <environment-name> substituindo-o pelo nome do seu RES ambiente:

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

3. Para reiniciar a instância do Cluster Manager para seu ambiente, execute os comandos a seguir, <environment-name> substituindo-a pelo nome do seu RES ambiente. Você também pode encerrar a instância no Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

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

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

.....

(2024.04.02 e anteriores) A chave privada para acessar o bastion host é inválida

O problema

Quando um usuário baixa a chave privada para acessar o bastion host a partir do portal da RES web, a chave não está bem formatada — várias linhas são baixadas como uma única linha, o que torna a chave inválida. O usuário receberá o seguinte erro ao tentar acessar o bastion host com a chave baixada:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

Versões afetadas

2024.04.02 e anteriores

Mitigação

Recomendamos usar o Chrome para baixar as chaves, pois esse navegador não é afetado.

Como alternativa, o arquivo de chave pode ser reformatado criando uma nova linha depois -----
BEGIN PRIVATE KEY----- e outra nova linha logo antes. -----END PRIVATE KEY-----
.....

(2024.06 e anteriores) Membros do grupo não sincronizados durante a RES sincronização do AD

Descrição do bug

Os membros do grupo não sincronizarão adequadamente RES se o GroupOU for diferente do UserOU.

REScria um filtro ldapsearch ao tentar sincronizar usuários de um grupo do AD. O filtro atual utiliza incorretamente o parâmetro userOU em vez do parâmetro groupOU. O resultado é que a pesquisa não retorna nenhum usuário. Esse comportamento ocorre somente nos casos em que os usuáriosSou e groupOU são diferentes.

Versões afetadas

Esse problema afeta todas as RES versões 2024.06 ou anteriores

Mitigação

Siga estas etapas para resolver o problema:

1. Para baixar o script patch.py e o arquivo group_member_sync_bug_fix.patch, execute os comandos a seguir, <output-directory> substituindo-os pelo diretório local em que você gostaria de baixar os arquivos e pela versão da qual deseja aplicar o patch: <res_version>
RES

Note

- [O script de patch requer AWS CLIv2, Python 3.9.16 ou superior e Boto3.](#)
- Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado por RES
- O patch suporta apenas RES as versões 2024.04.02 e 2024.06. Se você estiver usando 2024.04 ou 2024.04.01, siga as etapas listadas [Atualizações de versões menores](#) para primeiro atualizar seu ambiente para 2024.04.02 antes de aplicar o patch.

- RESVersão: RES 2024.04.02

Link para download do patch: [2024.04.02_group_member_sync_bug_fix.patch](#)

- RESVersão: RES 2024.06

Link para download do patch: [2024.06_group_member_sync_bug_fix.patch](#)

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

```
RES_VERSION=<res_version>
```

```
mkdir -p ${OUTPUT_DIRECTORY}
```

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

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

2. Navegue até o diretório em que o script e o arquivo de patch são baixados. Execute o seguinte comando de patch, <environment-name> substituindo-o pelo nome do seu RES ambiente:

```
cd ${OUTPUT_DIRECTORY}
```

```
ENVIRONMENT_NAME=<environment-name>
```

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

3. Para reiniciar a instância do cluster-manager do seu ambiente, execute os seguintes comandos:

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

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

.....

(2024.06 e anteriores) CVE -2024-6387, RegreSSHion, Vulnerabilidade de segurança no Ubuntu RHEL9 VDIs

Descrição do bug

[CVE-2024-6387](#), apelidado regreSSHion, foi identificado no servidor Open. SSH Essa vulnerabilidade permite que atacantes remotos e não autenticados executem códigos arbitrários no servidor de destino, representando um risco grave para os sistemas que utilizam o Open para comunicações seguras. SSH

PoisRES, a configuração padrão é passar do bastion host para SSH os desktops virtuais, e o bastion host não é afetado por essa vulnerabilidade. No entanto, o padrão AMI (Amazon Machine Image) que fornecemos RHEL9 e o Ubuntu2024 VDIs (Virtual Desktop Infrastructure) nas ALLRESversões utilizam uma SSH versão aberta que é vulnerável à ameaça à segurança.

Isso significa que o Ubuntu2024 existente RHEL9 e o Ubuntu2024 VDIs podem ser explorados, mas o atacante precisaria acessar o host bastion.

Mais detalhes sobre o problema podem ser encontrados [aqui](#).

Versões afetadas

Esse problema afeta todas as RES versões 2024.06 ou anteriores.

Mitigação

Tanto o Ubuntu RHEL9 quanto o Ubuntu lançaram patches para o OpenSSH, que corrigem a vulnerabilidade de segurança. Eles podem ser obtidos usando o respectivo gerenciador de pacotes da plataforma.

Se você já RHEL9 tem um UbuntuVDIs, recomendamos seguir as PATCHEXISTINGVDIsinstruções abaixo. Para corrigir o futureVDIs, recomendamos seguir as PATCHFUTUREVDIsinstruções. Essas instruções descrevem como executar um script para aplicar a atualização da plataforma em seuVDIs.

PATCH EXISTING VDIs

1. Execute o seguinte comando que corrigirá todo o Ubuntu existente e RHEL9VDIs:
 - a. O script de patch requer [AWS CLIv2](#).

- b. Configure o AWS CLI para a conta e a região em que RES está implantado e certifique-se de ter permissões do AWS Systems Manager para enviar um comando de execução do Systems Manager.

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

2. Você pode verificar se o script foi executado com êxito na [página Executar comando](#). Clique na guia Histórico de comandos, selecione o ID de comando mais recente e verifique se todas as instâncias IDs têm uma SUCCESS mensagem.

PATCH FUTURE VDIs

1. Para baixar o script e o arquivo de patch ([patch.py](#) e [update_openssh.patch](#)), execute os seguintes comandos, <output-directory> substituindo-os pelo diretório em que você deseja baixar os arquivos e <environment-name> pelo nome do seu ambiente: RES

Note

- O patch só se aplica a RES 2024.06.
- [O script de patch requer AWS CLIv2\), Python 3.9.16 ou superior e Boto3.](#)
- Configure sua cópia do AWS CLI para a conta e a região em que RES está implantada e certifique-se de ter permissões do S3 para gravar no bucket criado por. RES

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

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

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

2. Execute o seguinte comando de patch:

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

3. Reinicie a instância do VDC Controller para seu ambiente com os seguintes comandos:

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

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

⚠ Important

O patching future só VDIs é compatível com RES as versões 2024.06 e posteriores. Para corrigir o future VDIs em RES ambientes com versões anteriores a 2024.06, primeiro atualize o RES ambiente para 2024.06 usando as instruções em: [Principais atualizações da versão](#)

Avisos

Cada EC2 instância da Amazon 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 EC2 instâncias da Amazon sem RDP e sem a necessidade de RDP licenças. Se forem necessárias licenças adicionais dos Serviços de Área de Trabalho Remota, o usuário da Área de Trabalho Remota CALs deverá ser comprado da Microsoft ou de um revendedor de licenças da Microsoft. Usuários de desktop remoto CALs com o Software Assurance ativo têm benefícios da Mobilidade de Licenças e podem ser levados 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](#) doFAQ.

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 [CHANGELOGarquivo.md](#) no GitHub repositório.

Data	Alteração
Outubro de 2024	<ul style="list-style-type: none">• Versão de lançamento 2024.10: suporte adicionado para —<ul style="list-style-type: none">• Limites do ambiente.• Perfis de compartilhamento de desktop.• Parada automática da interface de desktop virtual.
Agosto de 2024	<ul style="list-style-type: none">• Versão de lançamento 2024.08: suporte adicionado para —<ul style="list-style-type: none">• montagem de buckets do Amazon S3 em instâncias da infraestrutura de desktop virtual Linux ()VDI. Consulte Buckets do Amazon S3.• permissões de projeto personalizadas, um modelo de permissão aprimorado que permite a personalização de funções existentes e a adição de funções personalizadas. Consulte Política de permissão.• Guia do usuário: expandiu a Solução de problemas seção.
Junho de 2024	<ul style="list-style-type: none">• Versão de lançamento 2024.06 — Suporte ao Ubuntu, permissões do proprietário do projeto.• Guia do usuário: adicionado Crie um ambiente de demonstração
Abril de 2024	Versão de lançamento 2024.04 — modelos RES prontos AMIs e de lançamento do projeto

Data	Alteração
Março de 2024	Tópicos adicionais de solução de problemas , retenção de CloudWatch registros, desinstalação de versões secundárias
Fevereiro de 2024	Versão de lançamento 2024.01.01 — modelo de implantação atualizado
Janeiro de 2024	Versão de lançamento 2024.01
Dezembro de 2023	GovCloud direções e modelos adicionados
Novembro de 2023	Lançamento inicial

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.