aws

Guia do usuário

Estúdio de Pesquisa e Engenharia

Estúdio de Pesquisa e Engenharia: Guia do usuário

Table of Contents

Visão geral

> **Important**
>
> Esta versão do Guia do Usuário abrange a versão 2024.12 do Research and Engineering Studio on. AWS Para a versão atual, consulte o Guia do AWS Usuário do Research and Engineering Studio.

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

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

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

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

Recursos e benefícios

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

Interface de usuário baseada na Web

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

Configuração baseada em projetos

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

Ferramentas de colaboração

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

Integração com a infraestrutura de gerenciamento de identidade existente

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

Armazenamento persistente e acesso a dados compartilhados

Para fornecer aos usuários acesso a dados compartilhados em sessões de desktop virtual, conecte-se aos seus sistemas de arquivos existentes no RES. Os serviços de armazenamento compatíveis incluem o Amazon Elastic File System para desktops Linux e o Amazon FSx for 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 projetos de RES para monitorar os custos de cada projeto. Se você exceder seu orçamento, poderá limitar o lançamento de sessões de VDI.

Conceitos e definições

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

Navegador de arquivos

Um navegador de arquivos faz parte da interface de usuário do RES, na qual 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 recursos de RES que são compartilhados em um ambiente de RES. O escopo e as permissões abrangem vários projetos. Eles podem criar ou modificar projetos e designar proprietários de projetos. Eles podem delegar ou atribuir permissões aos proprietários e membros do projeto. Às vezes, a mesma pessoa atua como administrador do RES, dependendo do tamanho da organização.

Projeto

Um projeto é uma partição lógica dentro do aplicativo que serve como um limite distinto para dados e recursos computacionais; isso garante a governança do fluxo de dados e evita o compartilhamento de dados e hosts de VDI entre projetos.

Permissões baseadas em projetos

As permissões baseadas em projetos descrevem uma partição lógica de dados e hosts VDI em um sistema em que vários projetos podem existir. O acesso de um usuário aos dados e aos hosts de VDI em um projeto é determinado por suas funções associadas. Um usuário deve ter acesso (ou associação ao projeto) atribuído a cada projeto ao qual ele precisa de acesso.

Caso contrário, o usuário não conseguirá acessar os dados do projeto e VDIs quando não tiver recebido a associação.

Membro do projeto

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

Proprietário de projeto

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

Pilha de software

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

Hospedeiros VDI

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

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

Visão geral da arquitetura

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

Diagrama de arquitetura

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

Figura 1: Estúdio de Pesquisa e Engenharia em AWS arquitetura

> **Note**
>
> AWS 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. O RES instala componentes para o portal da web, bem como:
   a. Componente de desktop virtual de engenharia (eVDI) para cargas de trabalho interativas
   b. Componente de métricas

      A Amazon CloudWatch recebe métricas dos componentes do eVDI.
   c. Componente Bastion Host

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

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

5. O Amazon Elastic File System (EFS) hospeda o sistema de `/home` arquivos padrão montado em todos os hosts de infraestrutura aplicáveis e sessões eVDI Linux.
6. O RES usa o Amazon Cognito para criar um usuário inicial de bootstrap chamado 'clusteradmin' e envia credenciais temporárias para o endereço de e-mail fornecido durante a instalação. O 'clusteradmin' deve alterar a senha 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	Fornece os serviços de computação subjacentes para criar desktops virtuais com o sistema operacional e a pilha de software escolhidos.
Elastic Load Balancing	Serviços	Os hosts Bastion, cluster-manager e VDI são criados em grupos de Auto Scaling por trás do balanceador de carga. O ELB equilibra o tráfego do portal da web em todos os hosts RES.

AWS serviço	Tipo	Descrição
Amazon Virtual Private Cloud	Serviços	Todos os componentes principais do produto são criados em sua 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	Fornece o sistema de `/home` arquivos para o navegador de arquivos e os hosts VDI, 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 Systems Manager (Gerenciador de sistemas)	Serviços	Armazena documentos para executar comandos para gerenciamento de sessões de VDI.
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.

AWS serviço	Tipo	Descrição
Amazon CloudWatch	Apoiando	Fornece 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 filas do Amazon SQS, tabelas do DynamoDB e tópicos do Amazon SNS.
AWS Secrets Manager	Apoiando	Armazena credenciais da conta de serviço no Active Directory e certificados autoassinados para. VDIs
AWS CloudFormation	Apoiando	Fornece 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.

AWS serviço	Tipo	Descrição
Amazon Simple Notification Service	Apoiando	Suporta o modelo de assinante de publicação entre os componentes da VDI, como o controlador e os hosts.
AWS Fargate	Apoiando	Instala, atualiza e exclui ambientes usando tarefas do Fargate.
Amazon FSx File Gateway	Opcional	Fornece sistema de arquivos compartilhado externo.
Amazon FSx para NetApp ONTAP	Opcional	Fornece sistema de arquivos compartilhado externo.
AWS Certificate Manager	Opcional	Gera um certificado confiável para seu domínio personali zado.
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 chaves Amazon EC2 SSH
- 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 ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

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

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

Crie um par de chaves Amazon EC2 SSH

Se você não tiver um par de chaves Amazon EC2 SSH, 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 gateway NAT de cinco para oito
  - Aumente os gateways NAT por zona de disponibilidade de cinco para dez
- Amazon EC2
  - Aumente o EC2 -VPC Elastic 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 . Você pode solicitar o aumento de algumas cotas, porém, algumas delas 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.

Parameter	Padrão	Descrição
EnvironmentName	*<res-demo>*	Um nome exclusivo dado ao seu ambiente RES começando com res-, não mais que 11 caracteres e sem letras maiúsculas.
AdministratorEmail		O endereço de e-mail do usuário que está concluind o a configuração do produto. Além disso, esse usuário funciona como um usuário incomparável se houver uma falha na integração de login único do Active Directory.
KeyPair		O par de chaves usado para se conectar aos hosts da infraestrutura.
Cliente IPCidr	<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 ao SSH no host bastion.

4. Selecione Criar pilha.

Etapas de pós-implantação

1. Agora você pode fazer login no ambiente de demonstração usando o usuário clusteradmin e a senha temporária enviada ao e-mail do administrador que você inseriu durante a configuração. Você será solicitado a criar uma nova senha em seu primeiro login.
2. Se você quiser usar o recurso “Entrar com o SSO da organização”, primeiro redefina as senhas de cada usuário com o qual gostaria de fazer login. Você pode redefinir as senhas dos usuários no AWS Directory Service. A pilha de demonstração cria quatro usuários com nomes de usuário que você pode usar: admin1, user1, admin2 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, digite o nome de usuário, digite a nova senha desejada e escolha Redefinir senha.
3. Depois de redefinir as senhas do usuário, vá para a página de login único para acessar o ambiente.

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 Explorerpara ajudar a gerenciar os custos. Os preços estão sujeitos a alterações. Para obter detalhes completos, consulte a página de preços de cada AWS serviço usado neste produto.

Segurança

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 responsabilidade compartilhada 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, consulteConsiderações de segurança para serviços deste produto. Para obter mais informações sobre AWS segurança, visite Nuvem AWS Segurança.

Perfis do IAM

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

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

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

Grupos de segurança

Os grupos de segurança criados neste produto foram projetados para controlar e isolar o tráfego de rede entre as funções EC2 , instâncias, sistemas de arquivos, instâncias CSR e endpoints remotos de VPN 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 de propriedade da RES. Ao implantar o RES, você pode especificar um AWS KMS key. O RES usa suas credenciais para conceder acesso à chave. Se você fornecer um cliente de propriedade e gerenciamento AWS KMS key, os dados do cliente em repouso serão criptografados usando essa chave.

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

Considerações de segurança para 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 no RES
Amazon Elastic Compute Cloud	Serviços	Fornece os serviços de computação subjacentes para criar desktops virtuais com o sistema operacional e a pilha de software escolhidos.
Elastic Load Balancing	Serviços	Os hosts Bastion, cluster-manager e VDI são criados em grupos de Auto Scaling por trás do balanceador de carga. O ELB equilibra o tráfego do portal da web em todos os hosts RES.
Amazon Virtual Private Cloud	Serviços	Todos os componentes principais do produto são criados em sua 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.

AWS informações de segurança do serviço	Tipo de serviço	Como o serviço é usado no RES
Amazon Elastic File System	Serviços	Fornece o sistema de `/home` arquivos para o navegador de arquivos e os hosts VDI, 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 Systems Manager (Gerenciador de sistemas)	Serviços	Armazena documentos para executar comandos para gerenciamento de sessões de VDI.
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	Fornece 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 no RES
AWS Key Management Service	Apoiando	Usado para criptografia em repouso com filas do Amazon SQS, tabelas do DynamoDB e tópicos do Amazon SNS.
AWS Secrets Manager	Apoiando	Armazena credenciais da conta de serviço no Active Directory e certificados autoassinados para. VDIs
AWS CloudFormation	Apoiando	Fornece 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 assíncron as.
Amazon Simple Notification Service	Apoiando	Suporta o modelo de assinante de publicação entre os componentes da VDI, 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 no RES
Amazon FSx File Gateway	Opcional	Fornece sistema de arquivos compartilhado externo.
Amazon FSx para NetApp ONTAP	Opcional	Fornece sistema de arquivos compartilhado externo.
AWS Certificate Manager	Opcional	Gera um certificado confiável para seu domínio personali zado.
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 padrão de capacidade mínima dentro dos grupos de Auto Scaling (ASG) da infraestrutura. Aumentar o valor de uma instância para duas instâncias oferece o benefício de várias zonas de disponibilidade (AZ) e reduz o tempo de restauração da funcionalidade do sistema em caso de perda inesperada de dados.

As configurações do ASG podem ser personalizadas no 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

Tópicos

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 ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

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

Crie um par de chaves Amazon EC2 SSH

Se você não tiver um par de chaves Amazon EC2 SSH, 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 gateway NAT de cinco para oito.
  - Aumente os gateways NAT por zona de disponibilidade de cinco para dez.
- Amazon EC2
  - Aumente o EC2 -VPC Elastic 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 . Você pode solicitar o aumento de algumas cotas, porém, algumas delas 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 ter um URL fácil de usar. Você precisará registrar um domínio usando o Amazon Route 53 ou outro provedor e importar um

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

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

Criar domínio (GovCloud somente)

Se você estiver implantando na região AWS GovCloud (Oeste dos EUA) 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 ARN secreto e adicione duas tags ao segredo para poder `vdc-gateway` acessar o valor do segredo:
   a. vermelho: ModuleName = virtual-desktop-controller
   b. res: EnvironmentName = [nome do ambiente] (Isso pode ser res-demo.)

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

   a. vermelho: ModuleName = virtual-desktop-controller

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

Forneça recursos externos

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 ambiente RES, o Active Directory (AD) e o armazenamento compartilhado.

- Armazenamento (Amazon EFS)

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

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

  O serviço de diretório autentica os usuários no ambiente RES.

- Um segredo que contém o nome de usuário e a senha da conta de serviço do Active Directory formatados como um par de valores-chave (nome de usuário, senha)

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

> **Tip**
>
> Se você estiver implantando um ambiente de demonstração e não tiver esses recursos externos disponíveis, poderá usar receitas de computação de AWS alto desempenho para gerar os recursos externos. Consulte a seção a seguir,Crie recursos externos, para implantar recursos em sua conta.

Para implantações de demonstração na região AWS GovCloud (Oeste dos EUA), você precisará concluir as etapas de pré-requisito em. Criar domínio (GovCloud somente)

Configure o LDAPS em seu ambiente (opcional)

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

1. Siga as etapas fornecidas em Como habilitar o LDAPS do lado do servidor para seu. AWS Managed Microsoft AD Você pode pular essa etapa se já tiver habilitado o LDAPS.
2. Depois de confirmar que o LDAPS está configurado no AD, exporte o certificado do AD:
    a. Acesse seu servidor do Active Directory.
    b. Abra PowerShell como administrador.
    c. Execute `certmgr.msc` para abrir a lista de certificados.
    d. Abra a lista de certificados abrindo primeiro as Autoridades de Certificação Raiz Confiáveis e depois os Certificados.
    e. Selecione e segure (ou clique com o botão direito do mouse) o certificado com o mesmo nome do seu servidor AD e escolha Todas as tarefas e, em seguida, Exportar.
    f. 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 de segrdo e cole o certificado codificado PEM no campo Texto sem formatação.
4. Observe o ARN criado e insira-o como `DomainTLSCertificateSecretARN` parâmetro em. Etapa 1: lançar o produto

Configurar uma VPC privada (opcional)

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

Tópicos

Prepare imagens de máquinas da Amazon (AMIs)

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

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

    b. Em Funções, escolha Criar função.

    c. Na página Selecionar entidade confiável:

    - Em Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
    - Para Caso de uso em Serviço ou caso de uso, escolha EC2Avançar.

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

    - Amazon S3 ReadOnlyAccess
    - Amazon SSMManaged InstanceCore
    - EC2InstanceProfileForImageBuilder

    e. Adicione um nome e uma descrição da função e, em seguida, escolha Criar função.
3. Crie o componente construtor de EC2 imagens:

    a. Abra o console do EC2 Image Builder emhttps://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:

Parameter	Entrada do usuário
Sistema operacional (SO) de imagem	Linux
Versões de sistema operacional compatíveis	Amazon Linux 2, RHEL8, ou RHEL9
Nome do componente	Insira um nome como: *<research-and-engineering-studio-infrastructure>*
Versão do componente.	Recomendamos começar com 1.0.0.
Descrição	Entrada opcional do usuário.

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

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

ii. Insira o seguinte:

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

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

```
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

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

```
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - |
                   echo -e "
                   http_proxy=http://<ip>:<port>
                   https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com,ecs.
{{ AWSRegion }}.amazonaws.com,.execute-api.{{ 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	Parameter	Entrada do usuário
Detalhes da receita	Nome	Insira um nome apropriado, como res-recipe-linux-x 86.
	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 ou Red Hat Enterprise Linux (RHEL)
	Origem da imagem	Início rápido (gerenciado pela Amazon)
	Nome da imagem	Amazon Linux 2 x86, Red Hat Enterprise Linux 8 x86 ou Red Hat Enterprise Linux 9 x86
	Opções de controle automático de versão	Use a versão mais recente do sistema operacional disponível.
Configuração da instância	–	Mantenha tudo nas configurações padrão e certifique-se de que Remover agente SSM após a execução do pipeline não esteja selecionado.

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

b. Escolha Create recipe (Criar fórmula).

5. Crie a configuração da infraestrutura do Image Builder.

a. Em Recursos salvos, escolha Configurações de infraestrutura.

b. Escolha Criar configuração de infraestrutura.

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

Seção	Parameter	Entrada do usuário
Geral	Nome	Insira um nome apropriado, como res-infra-linux-x 86.
	Descrição	Adicione uma descrição opcional.
	Perfil do IAM	Selecione a função do IAM criada anteriormente.
AWS infraestrutura	Tipo de instância	Escolha t3.medium.

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

   d. Escolha Criar configuração de infraestrutura.

6. Crie um novo pipeline do EC2 Image Builder:

a. Acesse Image pipelines e escolha Create image pipeline.

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

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

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

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

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

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

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

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 imagem de AMI.

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

Configurar endpoints de VPC

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

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

AWS service (Serviço da AWS)	Nome do serviço
Application Auto Scaling	com.amazonaws. *region*.escalonamento automático de aplicativos
AWS CloudFormation	com.amazonaws. *region*.formação em nuvem
Amazon CloudWatch	com.amazonaws. *region*.monitoramento
CloudWatch Registros da Amazon	com.amazonaws. *region*.registros
Amazon DynamoDB	com.amazonaws. *region*.dynamodb (requer um endpoint de gateway)
Amazon EC2	com.amazonaws. *region*.ec2
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon Elastic File System	com.amazonaws. *region*.sistema de arquivos elástico
Elastic Load Balancing	com.amazonaws. *region*. balanceamento de carga elástico
Amazon EventBridge	com.amazonaws. *region*.eventos
Amazon FSx	com.amazonaws. *region*.fsx

AWS service (Serviço da AWS)	Nome do serviço
AWS Key Management Service	com.amazonaws. *region*.kms
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
AWS Lambda	com.amazonaws. *region*.lambda
Amazon S3	com.amazonaws. *region*.s3 (Requer um endpoint de gateway criado por padrão no 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. *region*.gerente de segredos
Amazon Elastic Container Service	com.amazonaws. *region*.ecs
Amazon SES	com.amazonaws. *region*.email-smtp (Não suportado nas seguintes zonas de disponibilidade: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 e cac1-az4.)
AWS Security Token Service	com.amazonaws. *region*.sts
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
AWS Systems Manager	com.amazonaws. *region*.ec2 mensagens.
	com.amazonaws. *region*.sms
	com.amazonaws. *region*.mensagens.ssm

Conecte-se a serviços sem VPC endpoints

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

1. Execute uma instância Linux na sub-rede pública da VPC que você usará para sua implantação de RES.
   - Família Linux — Amazon Linux 2 ou Amazon Linux 3
   - Arquitetura — x86
   - Tipo de instância — t2.micro ou superior
   - Grupo de segurança — TCP na porta 3128 de 0.0.0.0/0
2. Conecte-se à instância para configurar um servidor proxy.
   a. Abra a conexão http.
   b. Permita a conexão com os seguintes domínios de todas as sub-redes relevantes:
      - .amazonaws.com (para serviços genéricos) AWS
      - .amazoncognito.com (para o Amazon Cognito)
      - .awsapps.com (para Identity Center)
      - .signin.aws (para o Identity Center)
      - . amazonaws-us-gov.com (para Gov Cloud)
   c. Negue todas as outras conexões.
   d. Ative e inicie o servidor proxy.
   e. Observe a PORTA na qual o servidor proxy escuta.
3. Configure sua tabela de rotas para permitir o acesso ao servidor proxy.
   a. Acesse seu console VPC e identifique as tabelas de rotas das sub-redes que você usará para hosts de infraestrutura e hosts VDI.
   b. Edite a tabela de rotas para permitir que todas as conexões de entrada acessem a instância do servidor proxy criada nas etapas anteriores.
   c. Faça isso para tabelas de rotas para todas as sub-redes (sem acesso à Internet) que você usará para Infrastructure/. VDIs

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

Definir parâmetros de implantação de VPC privados

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

Parameter	Entrada
InfrastructureHostAMI	Use o ID da AMI de infraestrutura criado emthe 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 CIDR de VPC para permitir o acesso a todos os endereços IP da VPC.
HttpProxy	Exemplo: `http://10.1.2.3:123`
HttpsProxy	Exemplo: `http://10.1.2.3:123`
NoProxy	Exemplo: `127.0.0.1,169.254.169.254,169.254.170.2,localhost,us-east-1.res,us-east-1.vpce.amazonaws.com,us-east-1.elb.amazonaws.com,s3.us-east-1.amazonaws.`

Parameter	Entrada
	`com,s3.dualstack.us-east-1.amazonaws.com,ec2.us-east-1.amazonaws.com,ec2.us-east-1.api.aws,ec2messages.us-east-1.amazonaws.com,ssm.us-east-1.amazonaws.com,ssmmessages.us-east-1.amazonaws.com,kms.us-east-1.amazonaws.com,secretsmanager.us-east-1.amazonaws.com,sqs.us-east-1.amazonaws.com,elasticloadbalancing.us-east-1.amazonaws.com,sns.us-east-1.amazonaws.com,logs.us-east-1.amazonaws.com,logs.us-east-1.api.aws,elasticfilesystem.us-east-1.amazonaws.com,fsx.us-east-1.amazonaws.com,dynamodb.us-east-1.amazonaws.com,api.ecr.us-east-1.amazonaws.com,.dkr.ecr.us-east-1.amazonaws.com,kinesis.us-east-1.amazonaws.com,.data-kinesis.us-east-1.amazonaws.com,.control-kinesis.us-east-1.amazonaws.com,events.us-east-1.amazonaws.com,cloudformation.us-east-1.amazonaws.com,sts.us-east-1.amazonaws.com,application-autoscaling.us-east-1.amazonaws.com,monitoring.us-east-1.amazonaws.com,ecs.us-east-1.amazonaws.com,.execute-api.us-east-1.amazonaws.com`

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:

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

Parameter	Padrão	Descrição
		Active Directory fornecido se tornará um subdomínio.
AdminPassword		A senha do administrador do Active Directory (nome de usuário`Admin`). Esse usuário é criado no Active Directory para a fase inicial de inicializ ação e não é usado depois. Importante: o formato desse campo pode ser (1) uma senha de texto simples ou (2) o ARN de um AWS segredo formatado como um par. key/value `{"passwor d":"somepassword"}` Observação: a senha desse usuário deve atender aos requisitos de complexidade da senha do Active Directory .

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

Parameter	Padrão	Descrição
LDIFS3Caminho	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	O caminho do Amazon S3 para um arquivo LDIF importado durante a fase de inicialização da configuração do Active Directory. Para obter mais informações, consulte LDIF Support. O parâmetro é pré-preenchido com um arquivo que cria vários usuários no Active Directory. Para visualizar o arquivo, consulte o arquivo res.ldif disponível em. GitHub
ClientIpCidr		O endereço IP a partir do qual você acessará o site. Por exemplo, você pode selecionar seu endereço IP e usá-lo `[IPADDRESS]/32` para permitir apenas o acesso do seu host. Você pode atualizar essa pós-implantação.

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

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

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

Etapa 1: lançar o produto

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

Tempo de implantação: aproximadamente 60 minutos

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

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

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

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

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

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

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

   > **Note**
   >
   > Este produto usa o serviço Amazon Cognito, que atualmente não está disponível para todos. Regiões da AWS Você deve lançar 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.

Parameter	Padrão	Descrição
EnvironmentName	`<res-demo>`	Um nome exclusivo dado ao seu ambiente RES começando com res-, não mais que 11 caracteres e sem letras maiúsculas.

Parameter	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- *[numbers or letters only]*	(Opcional) Você pode fornecer uma ID de AMI personalizada para usar em todos os hosts da infraestrutura. Os atualmente suportados OSes são Amazon Linux 2, RHEL8, ou RHEL9. Para obter mais informações, consulte Prepare imagens de máquinas da Amazon (AMIs).
SSHKeyPar		O par de chaves usado para se conectar aos hosts da infraestrutura.
ClientIP	*x.x.x*.0/24 ou .0/32 *x.x.x*	Filtro de endereço IP que limita a conexão com o sistema. Você pode atualizar o ClientIpCidr após a implantação.

Parameter	Padrão	Descrição
ClientPrefixList		(Opcional) Forneça uma lista gerenciada de prefixos para IPs permitir o acesso direto à interface do usuário da web e ao SSH no host bastion.
IAMPermissionLimite		(Opcional) Você pode fornecer um ARN de política gerenciada que será anexado como limite de permissão a todas as funções criadas no RES. Para obter mais informaçõ es, consulte Definindo limites de permissão personali zados.
VpcId		ID da VPC em que as instâncias serão iniciadas.
IsLoadBalancerInternetFacin g		Selecione true para implantar o balanceador de carga voltado para a Internet (requer sub-redes públicas para o balancead or de carga). Para implantaç ões que precisam de acesso restrito à Internet, selecione false.

Parameter	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 implantaç ões 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 disponibi lidade 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 disponibi lidade nas quais as instância s de VDI serão iniciadas . Se mais de dois foram criados pela pilha de rede externa, selecione todos os que foram criados.

Parameter	Padrão	Descrição
ActiveDirectoryName	`corp.res.com`	Domínio para o diretório ativo. Ele não precisa corresponder ao nome de domínio do portal.
ADShortNome	`corp`	O nome curto do diretório ativo. Isso também é chamado de nome NetBIOS.
Base LDAP	`DC=corp,DC=res,DC=com`	Um caminho LDAP para a base dentro da hierarquia LDAP.
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 ARN secreto que contenha o nome de usuário e a senha do usuário do Active Directory, formatado como um par nome de ServiceAccount usuário: senha. key/value
Sou do usuário		Unidade organizacional dentro do AD para usuários que sincronizarão.

Parameter	Padrão	Descrição
Grupo OU		Unidade organizacional dentro do AD para grupos que serão sincronizados.
SudoersGroupName	RESAdministrators	Nome do grupo que contém todos os usuários com acesso sudoer nas instância s na instalação e acesso de administrador no RES.
SOU de computador		Unidade organizacional dentro do AD à qual as instâncias se juntarão.
TLSCertificateSecretarN de domínio		(Opcional) Forneça um ARN secreto do certificado TLS de domínio para permitir a comunicação TLS com o AD.
EnableLdapIDMapping		Determina se os números UID e GID são gerados pelo SSSD ou se os números fornecidos pelo AD são usados. Defina como Verdadeiro para usar UID e GID gerados por SSSD ou Falso para usar UID e GID fornecidos pelo AD. Na maioria dos casos, esse parâmetro deve ser definido como True.

Parameter	Padrão	Descrição
Desativar ADJoin	Falso	Para evitar que os hosts Linux ingressem no domínio do diretório, altere para True. Caso contrário, deixe a configuração padrão de False.
ServiceAccountUserDN		Forneça o nome distinto (DN) do usuário da conta de serviço no Diretório.
SharedHomeFilesystemID		Um ID EFS a ser usado no sistema de arquivos doméstico compartilhado para hosts Linux VDI.
CustomDomainNamefo rWebApp		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a parte da web do sistema.
CustomDomainNameforVDI		(Opcional) Subdomínio usado pelo portal da web para fornecer links para a parte VDI do sistema.

Parameter	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, consulteGuia de configuração.
CertificateSecretARNforVDI		(Opcional) Esse segredo do ARN armazena o certificado público do certificado público do seu portal da web. Se você definir um nome de domínio do portal para seus recursos externos automatizados, poderá encontrar esse valor na guia Saídas da pilha res-bi.

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

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

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

Etapa 2: faça login pela primeira vez

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

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

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

Tópicos

Principais atualizações da versão

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

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

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

Atualizações de versões menores

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

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

Para fazer uma pequena atualização de versão:

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

Desinstalar o produto

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

Usando o AWS Management Console

1. Faça login no 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 console do Amazon EFS 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

Gerenciamento de identidades

O Research and Engineering Studio pode usar qualquer provedor de identidade compatível com SAML 2.0. Para usar o Amazon Cognito como um diretório de usuário nativo que permite que os usuários façam login no portal da Web e no Linux com base nas identidades de usuário do VDIs Cognito, consulte. Configurando usuários do Amazon Cognito Se você implantou o RES usando os recursos externos ou planeja usar o IAM Identity Center, consulteConfigurando o login único (SSO) com o IAM 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 usuários do Amazon Cognito

O Research and Engineering Studio (RES) permite que você configure o Amazon Cognito como um diretório de usuários nativo. Isso permite que os usuários façam login no portal da web e no

Linux com identidades de usuário do Amazon VDIs Cognito. Os administradores podem importar vários usuários para o grupo de usuários usando um arquivo csv do AWS console. Para obter mais detalhes sobre a importação em massa de usuários, consulte Importação de usuários para grupos de usuários a partir de um arquivo CSV no Guia do Desenvolvedor do Amazon Cognito. O RES suporta o uso de um diretório de usuário nativo baseado no Amazon Cognito e SSO juntos.

Configuração administrativa

Como administrador do RES, para configurar o ambiente do RES para usar o Amazon Cognito como um diretório de usuários, ative o botão Usar o Amazon Cognito como diretório de usuários na página de gerenciamento de identidades, que pode ser acessada na página Gerenciamento do ambiente. Para permitir que os usuários se registrem automaticamente, ative o botão de autorregistro do usuário na mesma página.

Fluxo de up/sign login do usuário

Se o autorregistro do usuário estiver ativado, você poderá fornecer aos usuários o URL do seu aplicativo web. Lá, os usuários encontrarão uma opção que diz Ainda não é usuário? Inscreva-se aqui.

Fluxo de inscrição

Usuários que escolhem Ainda não é usuário? Ao se inscrever aqui, será solicitado que você insira seu e-mail e senha para criar uma conta.

Como parte do fluxo de inscrição, os usuários deverão inserir o código de verificação recebido no e-mail para concluir o processo de inscrição.

Se a autoinscrição estiver desativada, os usuários não verão o link de inscrição. Os administradores devem configurar os usuários no Amazon Cognito fora do RES. (Consulte Criação de contas de usuário como administrador no Guia do Desenvolvedor do Amazon Cognito.)

Opções da página de login

Se o SSO e o Amazon Cognito estiverem habilitados, uma opção para entrar com o SSO da organização será exibida. Quando os usuários clicarem nessa opção, eles serão redirecionados para a página de login do SSO. Por padrão, os usuários se autenticarão com o Amazon Cognito se ele estiver ativado.

Restrições

- Seu nome do Grupo Amazon Cognito pode ter no máximo seis letras; somente letras minúsculas são aceitas.
- A inscrição no Amazon Cognito não permitirá dois endereços de e-mail com o mesmo nome de usuário, mas com um endereço de domínio diferente.
- Se o Active Directory e o Amazon Cognito estiverem habilitados e o sistema detectar um nome de usuário duplicado, somente os usuários do Active Directory poderão se autenticar. Os administradores devem tomar medidas para não configurar nomes de usuário duplicados entre o Amazon Cognito e seu Active Directory.
- Os usuários do Cognito não poderão iniciar com base no Windows, VDIs pois o RES não oferece suporte à autenticação baseada no Amazon Cognito para instâncias do Windows.

Sincronização

O RES sincroniza seu banco de dados com informações de usuários e grupos do Amazon Cognito a cada hora. Todos os usuários que pertencerem ao grupo “administradores” receberão o privilégio sudo em seus. VDIs

Você também pode iniciar a sincronização manualmente a partir do console Lambda.

Inicie o processo de sincronização manualmente:

1. Abra o console do lambda.
2. Pesquise o Cognito sync Lambda. Este Lambda segue esta convenção de nomenclatura:. *{RES_ENVIRONMENT_NAME}*`_cognito-sync-lambda`
3. Selecione Testar.
4. Na seção Evento de teste, escolha o botão Testar no canto superior direito. O formato do corpo do evento não importa.

Considerações de segurança para o Cognito

Antes da versão 2024.12, o registro de atividades do usuário, que faz parte do recurso do plano Amazon Cognito Plus, era ativado por padrão. Removemos isso de nossa implantação básica para economizar custos para clientes que desejam experimentar o RES. Você pode reativar esse recurso conforme necessário para se alinhar às configurações de segurança na nuvem da sua organização.

Sincronização do Active Directory

Configuração de tempo de execução

Todos os parâmetros CFN relacionados ao Active Directory (AD) são opcionais durante a instalação.

Após a instalação inicial, os administradores podem visualizar ou editar a configuração do AD no portal web RES, na página de gerenciamento de identidade:

Os administradores podem filtrar os usuários ou grupos a serem sincronizados por meio das novas opções Filtro de Usuários e Filtro de Grupos. Os filtros devem seguir a sintaxe do filtro LDAP. Um exemplo de filtro é:

```
(sAMAccountname=<user>)
```

Para qualquer ARN secreto fornecido em tempo de execução (por exemplo, `ServiceAccountCredentialsSecretArn` ou`DomainTLSCertificateSecretArn`), certifique-se de adicionar as seguintes tags ao segredo para RES para obter permissões para ler o valor secreto:

- chave: `res:EnvironmentName`, valor: *`<your RES environment name>`*
- chave: `res:ModuleName`, valor: `directoryservice`

Todas as atualizações de configuração do AD no portal da web serão coletadas automaticamente durante a próxima sincronização agendada do AD (de hora em hora). Talvez os usuários precisem reconfigurar o SSO depois de alterar a configuração do AD (por exemplo, se mudarem para um AD diferente).

Como executar manualmente a sincronização (versão 2024.12 e posterior)

O processo de sincronização do Active Directory foi movido do host de infraestrutura do Cluster Manager para uma tarefa única do Amazon Elastic Container Service (ECS) nos bastidores. O processo está programado para ser executado a cada hora e você pode encontrar uma tarefa do ECS em execução no console do Amazon ECS sob o *<res-environment-name>*`-ad-sync-cluster` cluster enquanto ela está em andamento.

Para iniciá-lo manualmente:

1. Navegue até o console do Lambda e pesquise o lambda chamado. *<res-environment>*`-scheduled-ad-sync`
2. Abra a função Lambda e vá para Teste
3. No Evento JSON, digite o seguinte:

```
{
    "detail-type": "Scheduled Event"
}
```

4. Escolha Testar.
5. Observe os registros da tarefa do AD Sync em execução em CloudWatch→ Grupos de registros →*<environment-name>*`/ad-sync`. Você verá os registros de cada uma das tarefas do ECS em execução. Selecione o mais recente para ver os registros.

> **Note**
>
> - Se você alterar os parâmetros do AD ou adicionar filtros do AD, o RES adicionará os novos usuários com os parâmetros recém-especificados e removerá os usuários que foram sincronizados anteriormente e não estão mais incluídos no espaço de pesquisa do LDAP.
> - O RES não pode remover um user/group que esteja ativamente atribuído a um projeto. Você deve remover usuários dos projetos para que o RES os remova do ambiente.

Configuração de SSO

Depois que a configuração do AD for fornecida, os usuários devem configurar o Single Sign-On (SSO) para poderem fazer login no portal web do RES como um usuário do AD. A configuração

do SSO foi movida da página Configurações gerais para a nova página de gerenciamento de identidade. Para obter mais informações sobre como configurar o SSO, consulteGerenciamento de identidades.

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

Se você ainda não tiver uma central de identidade conectada ao Active Directory gerenciado, comece comEtapa 1: configurar uma central de identidade. Se você já tem uma central de identidade conectada ao Active Directory gerenciado, comece comEtapa 2: conectar-se a uma central de identidade.

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

Etapa 1: configurar uma central de identidade

Habilitar 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 aplicação, escolha SAML 2.0.
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 metadados SAML do IAM Identity Center. Você precisará disso ao configurar o IAM Identity Center com o portal RES.
9. Em Propriedades do aplicativo, insira o URL inicial do aplicativo. Por exemplo, .`<your-portal-domain>/sso`
10. Em URL do ACS do aplicativo, insira o URL de redirecionamento do portal RES. Para encontrar isso:
    a. Em Gerenciamento do ambiente, escolha Configurações gerais.
    b. Selecione a guia Provedor de identidade.
    c. Em Single Sign-On, você encontrará o URL de redirecionamento do SAML.
11. Em Público do Application SAML, insira o URN do Amazon Cognito.

    Para criar a urna:

    a. No portal RES, abra Configurações gerais.
    b. Na guia Provedor de identidade, localize o ID do grupo de usuários.
    c. Adicione o ID do grupo de usuários a essa string:

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

12. Depois de inserir o URN do Amazon Cognito, 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 Formato, escolha Endereço de e-mail.
5. Escolha Adicionar novo mapeamento de atributo.

6. Em Atributo do usuário no aplicativo, insira “e-mail”.
7. Em Mapear para esse valor de string ou atributo de usuário no IAM Identity Center, insira**`${user:email}`**.
8. Em Formato, insira 'não especificado'.
9. Escolha Salvar alterações.

Adicionar usuários ao aplicativo no 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 ambiente RES

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 URL do endpoint do documento de metadados.
    d. Insira o URL que você copiou duranteConfigurando 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 portal RES. Essas etapas fornecem instruções para a integração

com o provedor de identidade SAML 2.0 escolhido. Se você pretende usar o IAM Identity Center, consulteConfigurando o login único (SSO) com o IAM Identity Center.

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

Tópicos

Configure seu provedor de identidade

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

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

     > **Note**
     >
     > Dependendo do IdP, o URL de redirecionamento de SAML pode ter um nome diferente:
     >
     > - URL da aplicação

- URL do Assertion Consumer Service (ACS)
- URL de vinculação do ACS POST

Para obter o URL

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

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

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

Forneça a entrada no formato a seguir.

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

Para encontrar seu URI de público do SAML

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

3. A declaração SAML publicada no RES deve ter o seguinte fields/claims definido como o endereço de e-mail do usuário:

- Assunto do SAML ou NameID
- E-mail SAML

4. Seu IdP é adicionado fields/claims à declaração do SAML, com base na configuração. O RES exige esses campos. A maioria dos provedores preenche automaticamente esses campos por padrão. Consulte as entradas e valores de campo a seguir se precisar configurá-los.

   - AudienceRestriction: defina como `urn:amazon:cognito:sp:`*`user-pool-id`*. *`user-pool-id`*Substitua pelo ID do seu grupo de usuários do Amazon Cognito.

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

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

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

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

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

   - AuthnStatement— Configure da seguinte forma:

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

```
    <saml2:AuthnContext>

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

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

   Para obter o URL do domínio

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

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

   Para obter o certificado de assinatura

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

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

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

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

Configure o RES para usar seu provedor de identidade

Para concluir a configuração de login único para RES

1. Faça login no RES como administrador ou administrador de cluster.
2. Navegue até Gerenciamento de ambiente ⇒ Configurações gerais ⇒ Provedor de identidade.
3. Em Single Sign-On, escolha o ícone de edição ao lado do indicador de status para abrir a página de Configuração de Single Sign On.

    a. Em Identity Provider, escolha SAML.

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

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

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

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

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

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

Se você usou os recursos externos fornecidos para criar um ambiente RES sem produção e configurou o IAM Identity Center como seu provedor de identidade, talvez queira configurar um

provedor de identidade diferente, como o Okta. O formulário de habilitação do RES SSO solicita três parâmetros de configuração:

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

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

1. Acesse o console do Amazon Cognito.
2. Na navegação, escolha Grupos de usuários.
3. 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.

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.

Depurando problemas de IdP do SAML

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

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

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

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

Definindo senhas para usuários

1. No AWS Directory Service console, selecione o diretório para a pilha criada.
2. No menu Ações, 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 as partes web e VDI do seu portal.

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

1. 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 Criar registros.
7. Para criar um registro para o VDC, recupere o endereço NLB.
    a. Abra o console de AWS CloudFormation.
    b. Selecione `<environment-name>-vdc`.
    c. Escolha Recursos e abra`<environmentname>-vdc-external-nlb`.
    d. Copie o nome DNS do NLB.
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 o NLB, insira o DNS.
13. Escolha Create record (Criar registro).

Criar um certificado ACM

Por padrão, o RES hospeda o portal da web em um balanceador de carga de aplicativos usando o domínio amazonaws.com. Para usar seu próprio domínio, você precisará configurar um SSL/TLS certificado público fornecido por você ou solicitado pelo AWS Certificate Manager (ACM). Se você usar o ACM, receberá um nome de AWS recurso que precisará fornecer como parâmetro para criptografar o SSL/TLS canal 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 Managerpara solicitar um certificado público. Se você estiver implantando em AWS GovCloud (Oeste dos EUA), crie o certificado em sua conta de GovCloud partição.
2. Escolha Solicitar um certificado público e escolha Avançar.
3. Em Nomes de domínio, solicite um certificado para ambos `*.PortalDomainName` `PortalDomainName` e.
4. Em Método de validação, escolha Validação de DNS.
5. Escolha Solicitar.
6. Na lista de certificados, abra os certificados solicitados. Cada certificado terá a validação pendente como status.

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

7. Execute um destes procedimentos:
   - Implantação comercial:

     Nos detalhes do certificado para cada certificado solicitado, escolha Criar registros no Route 53. O status do certificado deve mudar para Emitido.
   - GovCloud implantação:

     Se você estiver implantando em AWS GovCloud (Oeste dos EUA), copie a chave e o valor CNAME. Na conta de partição comercial, use os valores para criar um novo registro na zona hospedada pública. O status do certificado deve mudar para Emitido.
8. Copie o novo ARN do certificado a ser inserido como parâmetro para. `ACMCertificateARNforWebApp`

CloudWatch Registros da Amazon

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

CloudWatch Grupos de registros	Retenção
/aws/lambda/ *<installation-stack-name>*-cluster-endpoints	Nunca expire
/aws/lambda/ *<installation-stack-name>*-cluster-manager-scheduled-ad-sync	Nunca expire
/aws/lambda/ *<installation-stack-name>*-cluster-settings	Nunca expire
/aws/lambda/ *<installation-stack-name>*-oauth-credentials	Nunca expire
/aws/lambda/ *<installation-stack-name>*-self-signed-certificate	Nunca expire
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	Nunca expire
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	Nunca expire
/aws/lambda/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope	Nunca expire
/*<installation-stack-name>* /cluster-manager	3 meses
/*<installation-stack-name>* /vdc/controller	3 meses
/*<installation-stack-name>* /vdc/dcv-broker	3 meses

CloudWatch Grupos de registros	Retenção
/*<installation-stack-name>* /vdc/dcv-connection-gateway	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 pelo RES anexando limites de permissão personalizados. Um limite de permissão personalizado pode ser definido como parte da AWS CloudFormation instalação do RES fornecendo o ARN do limite de permissão como parte do parâmetro Boundary. IAMPermission Nenhum limite de permissão é definido em nenhuma função RES se esse parâmetro for deixado em branco. Abaixo está a lista de ações que as funções de RES exigem para operar. Certifique-se de que qualquer limite de permissão que você planeja usar explicitamente permita as seguintes ações:

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

```
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
```

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

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

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

Configurar pronto para RES AMIs

Com o Amazon Machine Images (AMIs) pronto para RES-ready, você pode pré-instalar dependências RES para instâncias de desktop virtual (VDIs) em suas instâncias personalizadas. AMIs O uso do Res-Ready AMIs melhora os tempos de inicialização das instâncias de VDI usando as 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 função do IAM para acessar o ambiente RES
- 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 função do IAM para acessar o ambiente RES

Para acessar o serviço de ambiente RES a partir do EC2 Image Builder, você deve criar ou modificar uma função do IAM chamada RES- EC2InstanceProfileForImageBuilder. Para obter informações sobre como configurar uma função do IAM para uso no Image Builder, consulte AWS Identity and Access Management (IAM) no Guia do usuário do Image Builder.

Sua função exige:

- Relacionamentos confiáveis incluem o EC2 serviço Amazon.
- Amazon SSMManaged InstanceCore e EC2 InstanceProfileForImageBuilder políticas.
- Política de RES personalizada com acesso limitado do DynamoDB e do Amazon S3 ao ambiente RES implantado.

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

Entidade de relacionamento confiável:

JSON

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

Política de RES:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:us-east-1:111122223333:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*",
                        "cluster-manager.host_modules.*",
                        "identity-provider.cognito.enable_native_user_login"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::{RES-EnvironmentName}-cluster-us-
east-1-111122223333/idea/vdc/res-ready-install-script-packages/*",
                "arn:aws:s3:::research-engineering-studio-us-east-1/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 arquivo YAML é sensível ao espaço e é a causa mais provável.

   Linux

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

```
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
```

```
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

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

```
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
 res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
       - name: Reboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

6. Crie qualquer tag opcional e escolha Criar componente.

Prepare sua receita do EC2 Image Builder

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 a AMI de destino com as dependências de software RES necessárias. Para obter mais informações sobre receitas, consulte Gerenciar receitas.

O RES suporta os seguintes sistemas operacionais de imagem:

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

Create a new recipe

1. Abra o console do EC2 Image Builder emhttps://console.aws.amazon.com/imagebuilder.
2. Em Recursos salvos, escolha Receitas de imagens.
3. Escolha Criar fórmula de imagem.
4. Insira um nome exclusivo e um número de versão.
5. Selecione uma imagem base compatível com RES.
6. Em Configuração da instância, instale um agente SSM se um não vier pré-instalado. Insira as informações em Dados do usuário e quaisquer outros dados necessários do usuário.

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

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

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

8. Adicione o componente EC2 Image Builder criado para seu ambiente Linux ou Windows e insira os valores de parâmetros necessários. Os seguintes parâmetros são entradas obrigatórias: AWSAccount ID, RESEnv nome, RESEnv região e. RESEnv ReleaseVersion

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

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

Modify a recipe

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

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

   > **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 uso com RES, você pode optar por criar uma nova configuração de infraestrutura ou usar uma existente.

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

Para configurar sua infraestrutura do Image Builder:

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

Configurar o pipeline de imagens do Image Builder

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

Create a new Image Builder pipeline

1. Abra o console do Image Builder emhttps://console.aws.amazon.com/imagebuilder.
2. 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 emPrepare 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 emConfigurar a infraestrutura do EC2 Image Builder. Verifique se os detalhes da sua infraestrutura estão corretos.
8. Em Definir configurações de distribuição, escolha Criar configurações de distribuição usando padrões de serviço. A imagem de saída deve residir no Região da AWS mesmo ambiente do RES. Usando padrões de serviço, a imagem será criada na região em que o Image Builder é usado.
9. Analise os detalhes do funil e escolha Criar funil.

Modify an existing Image Builder pipeline

1. Para usar um pipeline existente, modifique os detalhes para usar a receita criada emPrepare 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 emConfigurar o pipeline de imagens do Image Builder.
2. Em Ações, escolha Executar pipeline.

Registre uma nova pilha de software no RES

1. Siga as instruções the section called “Pilhas de software () AMIs” para registrar uma pilha de software.
2. Em ID da AMI, insira a ID da AMI da imagem de saída incorporadaExecute 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

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

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

Nome de segredo	Descrição	RES gerado	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> -directoryservice-ServiceAccountUserDN`	O atributo Nome Distinto (DN) do ServiceAccount usuário.	✓	

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

Chave	Origem
`identity-provider.cognito.sso_client_secret`	
`vdc.dcv_connection_gateway.certificate.certificate_secret_arn`	pilha
`vdc.dcv_connection_gateway.certificate.private_key_secret_arn`	pilha
`cluster.load_balancers.internal_alb.certificates.private_key_secret_arn`	pilha
`directoryservice.root_username_secret_arn`	
`vdc.client_secret`	pilha
`cluster.load_balancers.external_alb.certificates.certificate_secret_arn`	pilha
`cluster.load_balancers.internal_alb.certificates.certificate_secret_arn`	pilha
`directoryservice.root_password_secret_arn`	
`cluster.secretsmanager.kms_key_id`	
`cluster.load_balancers.external_alb.certificates.private_key_secret_arn`	pilha
`cluster-manager.client_secret`	

Monitoramento e controle de custos

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

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

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

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

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

Para criar um orçamento para recursos de RES:

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

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

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

12. Em Valores, selecione o nome do projeto.
13. Escolha Aplicar filtro para anexar o filtro do projeto ao orçamento.
14. Escolha Próximo.
15. (Opcional.) Adicione um limite de alerta.
16. Escolha Próximo.
17. (Opcional.) Se um alerta foi configurado, use Anexar ações para configurar as ações desejadas com o alerta.
18. Escolha Próximo.
19. Revise a configuração do orçamento e confirme se a tag correta foi definida em Parâmetros adicionais de orçamento.
20. Escolha Criar orçamento.

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

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

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

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

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

Além disso, os administradores podem:

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

Sessões

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

1. Use o menu para filtrar os resultados por sessões criadas ou atualizadas dentro de um período de tempo especificado.
2. Selecione uma sessão e use o menu Ações para:
   a. Retomar sessão (s)
   b. Stop/Hibernate Sessão (s)
   c. Stop/Hibernate Sessão (ões) de força
   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 sessão DCV.
4. Selecione Enviar.

Detalhes da sessão

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

Pilhas de software () AMIs

> **Note**
>
> Para executar a pilha SO7 de software Cent fornecida AWS GovCloud (US), você precisará assinar a AMI AWS Marketplace usando sua conta padrão vinculada.

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

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.

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. Escolha 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:

Tempo limite de inatividade da sessão DCV

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

Aviso de tempo limite de inatividade

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

Limite de utilização de CPU

: A utilização da CPU deve ser considerada ociosa.

Sessões permitidas por usuário

: O número de sessões de VDI 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 ambiente RES. 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 serem iniciados como sessões de VDI. Se você especificar 'm7a.24xlarge', somente m7a.24xlarge estará disponível para ser iniciado como uma sessão de VDI. Essa lista afeta todos os projetos no ambiente.

Gestão ambiental

Na seção Gerenciamento de ambiente do Research and Engineering Studio, 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

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.

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 o ID da VPC e a lista IDs de prefixos para acesso.
- Directory Service

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

Usuários

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

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

Na página Usuários, você pode:

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

Grupos

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

Na página Grupos, você pode:

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

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

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

Criar um projeto

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

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

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

   Para obter informações sobre opções avançadas, consulteAdicionar um modelo de lançamento.
3. (Opcional) Ative os orçamentos para o projeto. Para obter mais informações sobre orçamentos, consulte. Monitoramento e controle de custos
4. O sistema de arquivos do diretório inicial pode usar o Sistema de Arquivos Pessoal Compartilhado (padrão), o EFS, FSx para armazenamento em volume Lustre, FSx NetApp ONTAP ou EBS.

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

5. Atribua aos and/or grupos de usuários a função apropriada (“Membro do projeto” ou “Proprietário do projeto”). Veja Perfis de permissões padrão as ações que cada função pode realizar.
6. Selecione Enviar.

Editar um projeto

1. Selecione um projeto na lista de projetos.
2. No menu Ações, escolha Editar projeto.
3. Insira suas atualizações.

   Se você pretende habilitar orçamentos, consulte Monitoramento e controle de custos para obter mais informações. Ao escolher um orçamento para o projeto, pode haver alguns segundos de atraso para que as opções suspensas de orçamento sejam carregadas. Se você não encontrar o orçamento que acabou de criar, selecione o botão de atualização ao lado da lista suspensa.

   Para obter informações sobre opções avançadas, consulteAdicionar um modelo de lançamento.
4. Selecione Enviar.

Adicionar ou remover tags de um projeto

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

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

Exibir sistemas de arquivos associados a um projeto

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

Adicionar um modelo de lançamento

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

Adicionar políticas

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

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

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

Adição de grupos de segurança

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

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

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

Adicionar scripts de lançamento

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

Executar script quando a VDI é iniciada

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

Executar script quando o VDI estiver configurado

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

Os scripts oferecem suporte às seguintes opções:

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

Para Argumentos, forneça quaisquer argumentos separados por uma vírgula.

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. Permissões de gerenciamento de sessão de VDI que consistem em “Criar sessão”, que permite que um usuário designado crie uma sessão de VDI 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

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.

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.

Permissões de gerenciamento de sessão VDI

Crie uma sessão.

Controla se um usuário tem permissão ou não para iniciar sua própria sessão de VDI na página Meus desktops virtuais. Desative isso para negar aos usuários não administradores a capacidade de iniciar suas próprias sessões de VDI. Os usuários sempre podem parar e encerrar suas próprias sessões de VDI.

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 sessões de VDI 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 administrador do RES, 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 Política de permissão no painel de navegação esquerdo. Nessa página, você pode criar, atualizar, listar, visualizar e excluir perfis de permissão.

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.

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

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.

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.

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.

Perfis de permissões padrão

Cada projeto RES 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 ou sem essa permissão.	X	X	
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 ambientais

Os limites do ambiente permitem que os administradores do Research and Engineering Studio (RES) configurem permissões que entrarão em vigor globalmente para todos os usuários. Isso inclui permissões como permissões do Navegador de Arquivos e SSH, Permissões da área de trabalho e configurações avançadas da área de trabalho.

Configurando o acesso ao navegador de arquivos

Os administradores do RES 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 o acesso SSH

Os administradores podem ativar ou desativar o SSH para o ambiente RES na seção Limites do ambiente. O acesso SSH ao VDIs é facilitado por meio de um host bastion. Quando você ativa essa opção, o RES implanta um bastion host e torna a página de instruções de acesso SSH visível para os usuários. Quando você desativa a opção, o RES desativa o acesso SSH, encerra o bastion host e remove a página de instruções de acesso SSH para os usuários. Essa opção está desativada por padrão.

> **Note**
>
> Quando o RES implanta um bastion host, ele adiciona uma EC2 instância da `t3.medium` Amazon à sua AWS conta. Você é responsável por todas as cobranças associadas a essa instância. Consulte a página de EC2 preços da Amazon para obter mais informações.

Para habilitar o acesso SSH

1. No console RES, no painel de navegação esquerdo, escolha Gerenciamento de ambiente e, em seguida, Política de permissão. Em Limites do ambiente, selecione a opção de acesso SSH.

2. Aguarde até que o acesso SSH seja ativado.

3. Depois que o host Bastion é adicionado, o acesso SSH é ativado.

   A página de instruções de acesso SSH é visível para os usuários no painel de navegação esquerdo.

Para desativar o acesso SSH

1. No console RES, no painel de navegação esquerdo, escolha Gerenciamento de ambiente e, em seguida, Política de permissão. Em Limites do ambiente, selecione a opção de acesso SSH.

2. Aguarde até que o acesso SSH seja desativado.

3. Quando o processo estiver concluído, o acesso SSH será desativado.

Configurando as permissões da área de trabalho

Os administradores podem ativar ou desativar as permissões da área de trabalho para gerenciar globalmente a funcionalidade de VDI de todos os proprietários da sessão. 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 ative essa permissão de área de trabalho novamente, a permissão no perfil de compartilhamento de área de trabalho 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.

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.

Sistemas de arquivos

Na página Sistemas de arquivos, você pode:

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

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. VDIs VDIs montará o sistema de arquivos no ponto de montagem selecionado durante a integração de um sistema de arquivos.

4. Selecione Enviar.

Gerenciamento de snapshots

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

Na página de gerenciamento de snapshots, você pode:

1. Visualize todos os instantâneos criados e seus status.
2. Crie um instantâneo. Antes de criar um snapshot, você precisará criar um bucket com as permissões apropriadas.
3. Visualize todos os instantâneos aplicados e 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:
   - *111122223333*-> seu ID AWS da conta
   - *{RES_ENVIRONMENT_NAME}*-> nome do seu ambiente RES
   - *us-east-1*-> sua AWS região
   - *amzn-s3-demo-bucket*-> nome do seu bucket S3

> **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.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-us-east-1}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
```

```
}
```

Para criar o instantâneo:

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

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

Aplicar um instantâneo

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

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

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

Se o novo ambiente não for o esperado ou falhar, você poderá verificar os CloudWatch registros encontrados no grupo de registros `/res-<env-name>/cluster-manager` para obter detalhes.

Cada registro terá a tag [aplicar instantâneo]. Depois de aplicar um snapshot, você pode verificar seu status na the section called “Gerenciamento de snapshots” 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:

   - *111122223333*-> seu ID AWS da conta
   - *{RES_ENVIRONMENT_NAME}*-> nome do seu ambiente RES
   - *us-east-1*-> sua AWS região
   - *amzn-s3-demo-bucket*-> nome do seu bucket S3

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-us-east-1}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
```

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

Para aplicar um instantâneo:

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

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

Buckets do Amazon S3

O Research and Engineering Studio (RES) suporta a montagem de buckets do Amazon S3 em instâncias de infraestrutura de desktop virtual (VDI) Linux. Os administradores do RES podem integrar buckets do S3 ao RES, 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 S3 ao 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 de VPC

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

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.
4. No lado esquerdo, escolha Variáveis de ambiente para visualizar essa seção.
5. Escolha Editar e adicione a seguinte nova variável de ambiente à função:

- Chave: `AWS_STS_REGIONAL_ENDPOINTS`
- Valor: `regional`

6. Escolha Salvar.

Adicionar um bucket Amazon S3

Para adicionar um bucket S3 ao seu ambiente RES:

1. Escolha Add bucket (Adicionar bucket).
2. Insira os detalhes do bucket, como nome do bucket, ARN e ponto de montagem.

> **Important**
>
> - O ARN do bucket, o ponto de montagem e o modo fornecidos não podem ser alterados após a criação.
> - O ARN do bucket 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 um ARN de função do IAM para montar os buckets para acesso entre contas. Siga as etapas Acesso ao bucket entre contas para criar a função do IAM 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 sessões de VDI existentes de um projeto. Somente as sessões iniciadas após o projeto ter sido associado ao bucket montarão o bucket.
6. Selecione Enviar.

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 sessões de VDI 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.

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 o RES.
> - A remoção de um bucket fará com que as sessões de VDI 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 S3 ao RES, 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)` for selecionado, o isolamento de dados será imposto com base no prefixo do ARN do bucket (Amazon Resource Name). Por exemplo, se um administrador adicionar um bucket ao RES usando o ARN `arn:aws:s3:::`*`bucket-name/example-data/`* e associar esse bucket 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 ARN do bucket, todo o bucket 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 ARN do bucket, 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

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 bucket ao RES usando o ARN `arn:aws:s3:::`*`bucket-name`* `No custom prefix` selecionado e associar esse bucket ao Projeto A e ao Projeto B, os usuários que iniciarem a VDIs partir do Projeto A e do Projeto B terão acesso irrestrito de leitura e gravação ao bucket.

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 usando o ARN `arn:aws:s3:::bucket-name` com `/%p` selecionado e um ponto de montagem de`/bucket`, e associar esse bucket ao Projeto A e ao Projeto B, o usuário A no Projeto A poderá gravar um arquivo no. `/bucket` O usuário B no Projeto A também pode ver o arquivo no qual o usuário A escreveu`/bucket`. No entanto, se o usuário B iniciar uma VDI no Projeto B e examinar`/bucket`, ele não verá 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 usando o ARN `arn:aws:s3:::bucket-name` com `/%p/%u` selecionado e um ponto de montagem de. `/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`/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

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

Etapa 1: Crie uma função do IAM na conta na qual o RES está implantado (isso será chamado de Conta A):

1. Faça login no console AWS de gerenciamento da conta RES que precisa acessar o bucket do S3 (Conta A).
2. Abra o console do IAM:

a. Navegue até o painel do IAM.

b. No painel de navegação, selecione Políticas.

3. Crie uma política:

a. Escolha Criar política.

b. Selecione a guia JSON.

c. Cole a seguinte política JSON (*amzn-s3-demo-bucket*substitua pelo nome do bucket do S3 localizado na Conta B):

JSON

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

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 console do IAM:

a. Navegue até o painel do IAM.

b. No painel de navegação, selecione Perfis.

6. Crie uma função:

a. Selecione Criar perfil.

b. Escolha Política de confiança personalizada como o tipo de entidade confiável.

c. Cole a seguinte política JSON (*111122223333*substitua pelo ID da conta real da Conta A, *<ENVIRONMENT_NAME>* pelo nome do ambiente da implantação do RES e *us-east-1* pela AWS região em que o RES é implantado):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-us-east-1"
            },
            "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 função do IAM no RES:

a. Copie o ARN da função do IAM que você criou.

b. Faça login no console RES.

c. No painel de navegação esquerdo, escolha S3 Bucket.

d. Escolha Adicionar bucket e preencha o formulário com o ARN do bucket S3 entre contas.

e. Escolha o menu suspenso Configurações avançadas - opcional.

f. Insira o ARN da função no campo ARN da função do IAM.

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 à função do IAM da Conta A acesso ao bucket (*111122223333*substitua pelo ID real da conta A e *amzn-s3-demo-bucket* pelo nome do bucket S3):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

c. Escolha Salvar.

Evitando a exfiltração de dados em uma VPC privada

Para evitar que os usuários extraiam dados de buckets seguros do S3 para seus próprios buckets do S3 em suas contas, você pode anexar um VPC endpoint para proteger sua VPC privada. 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 console da Amazon VPC:
   a. Faça login no AWS Management Console.
   b. Abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/
2. Crie um VPC Endpoint para 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, insira `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 a VPC em que você deseja criar o endpoint.

b. Para sub-redes, selecione as duas sub-redes privadas usadas para as sub-redes VDI durante a implantação.

c. Em Habilitar nome DNS, verifique se a opção está marcada. Isso permite que o nome do host DNS 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 em sua conta ou em uma conta específica. Aqui está um exemplo de política (*amzn-s3-demo-bucket*substitua pelo nome do bucket do S3 *111122223333* e *444455556666* pela AWS conta apropriada IDs que você deseja acessar):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",
                        "444455556666"
                    ]
                }
            }
        }
    ]
}
```

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 console da VPC.
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 bucket não consegue ser montado em uma VDI

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

1. Verifique os registros do VDI:

a. Faça login no console AWS de gerenciamento.
b. Abra o EC2 console e navegue até Instâncias.
c. Selecione a instância de VDI que você executou.
d. Conecte-se à 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 API Gateway 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*<stack-name>*-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<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 função do IAM 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` `<filesystem_id>` substituindo pelo valor do sistema de arquivos que precisa ser modificado.

5. Execute a verificação:

   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 o ARN correto da função do IAM.

   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 o ARN correto da função do IAM.

   c. Escolha Salvar para adicionar o item.

7. Reinicie as instâncias de VDI:

   Reinicialize a instância para garantir VDIs que os ARN afetados pela função incorreta do IAM sejam montados 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 função do IAM 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

Acesso a SSH

Para usar o SSH para acessar o bastion host:

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

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 com suporte

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

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

Tópicos

Inicie um novo desktop

1. No menu, escolha Meus desktops virtuais.
2. Escolha Iniciar nova área de trabalho virtual.

3. Insira os detalhes do seu novo desktop.
4. Selecione Enviar.

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

Acesse sua área de trabalho

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

Web connection

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

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

DCV connection

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

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

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

Controle o estado do seu desktop

Para controlar o estado da sua área de trabalho:

1. Escolha Ações.

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

   - Interromper

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

     Reinicializa a sessão atual.
   - Encerrar

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

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

Modificar uma área de trabalho virtual

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

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

   a. Escolha Ações.

   b. Escolha o estado da área de trabalho virtual.

   c. Escolha Parar.

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

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

   a. Escolha Ações.

   b. Escolha o estado da área de trabalho virtual.

   c. Escolha Iniciar.

Recuperar informações da sessão

1. Escolha Ações.

2. Escolha Mostrar informações.

Agende desktops virtuais

Por padrão, os desktops virtuais não têm uma agenda e permanecerão ativos até que você interrompa ou encerre a sessão. Os desktops também param se estiverem ociosos para evitar

paradas acidentais. Um estado ocioso é determinado pela ausência de conexão ativa e pelo uso da CPU abaixo de 15% por pelo menos 15 minutos. Você pode configurar um agendamento para iniciar e parar automaticamente sua área de trabalho.

1. Escolha Ações.

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

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 a utilização da CPU abaixo do limite expirarão.
2. Limite de utilização da CPU: 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.

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.

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

1. Na 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, consultethe 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 entrar por meio de um navegador da web ou DCV. Para se conectar, siga as instruções emAcesse sua área de trabalho.

Navegador de arquivos

O navegador de arquivos permite que você acesse sistemas de arquivos por meio do portal da web. Você pode gerenciar todos os arquivos disponíveis que você tem permissão para acessar no sistema

de arquivos subjacente. O armazenamento de back-end (Amazon EFS) está disponível para todos os nós Linux. Para nós Linux e Windows, o FSx 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)

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)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)

Solução de problemas

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

Tópicos

Conteúdo detalhado:

- (2024.08) Os desktops virtuais falham ao montar o bucket read/write Amazon S3 com ARN do bucket raiz e prefixo personalizado
- (2024.06) A aplicação do instantâneo falha quando o nome do grupo AD contém espaços
- (2024.04-2024.04.02) Limite de permissão do IAM fornecido não anexado à função das instâncias de 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 na exclusão de RES em GovCloud
- (2024.04 - 2024.04.02) O desktop virtual Linux pode ficar preso no status “RETOMANDO” na reinicialização
- (2024.04.02 e anteriores) Falha ao sincronizar usuários do AD cujo atributo SAMAccount Name 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 com RES durante a sincronização do AD
- (2024.06 e anteriores) CVE-2024-6387, Regre, Vulnerabilidade de segurança no Ubuntu SSHion RHEL9 VDIs

Depuração e monitoramento gerais

Esta seção contém informações sobre onde as informações podem ser encontradas no 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
  - Hosts de infraestrutura
  - Hosts de infraestrutura e desktops virtuais
  - Hosts em um estado encerrado
  - Comandos úteis relacionados ao Active Directory (AD) para referência
- Depuração DCV do Windows

- Encontre informações sobre a versão do Amazon DCV

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 (EC2 instâncias da Amazon)

Existem arquivos de log nas EC2 instâncias da Amazon em uso pelo RES. O SSM Session Manager 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/sssd/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

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

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

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 certificado NICE DCV 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 das strings error e 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.

Pilhas RES:

- <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>-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 o RES UIs indicar 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 do ASG relacionado para determinar se as instâncias da EC2 Amazon estão circulando.

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 SSM Session para abrir uma sessão em uma instância em

execução desse tipo e examinar os arquivos de log na instância para determinar uma causa antes que a instância seja marcada como não íntegra e encerrada pelo ASG.

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

Aparência típica EC2 do console Amazon

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

Hosts de infraestrutura

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

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 indicados 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.

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.

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>
```

Depuração DCV 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 versão do Amazon DCV

O Amazon DCV é utilizado para sessões de desktop virtual. AWS Amazon DCV. Os exemplos a seguir mostram como determinar a versão do software DCV 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 depois de instalar o 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 no parâmetro de bloco CIDR durante a criação do ambiente
  - CloudFormation falha na criação da pilha durante a criação do ambiente
  - A criação da pilha de recursos externos (demo) 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

Problemas de instalação

Tópicos

.....

Quero configurar domínios personalizados depois de instalar o 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 externo RES 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 SSL/TLS certificado padrão 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) do 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 nome DNS do balanceador de carga externo do laboratório. `<env-name>-external-alb`
4. Se o SSO já estiver configurado no ambiente, reconfigure o SSO com as mesmas entradas que você usou inicialmente no botão Configurações gerais > Provedor de identidade > Login único > Status > Editar no portal web RES.

Adicione certificados ao VDIs

1. Conceda permissão ao aplicativo RES 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 “dcv_connection_gateway”.
   c. `vdc.dcv_connection_gateway.certificate.provided`Defina como Verdadeiro.
   d. Atualize o valor de`vdc.dcv_connection_gateway.certificate.custom_dns_name`. Esse é o nome de domínio personalizado para acesso à VDI.
   e. Atualize o valor de`vdc.dcv_connection_gateway.certificate.certificate_secret_arn`. Esse é o ARN do segredo que contém o conteúdo do certificado.
   f. Atualize o valor de`vdc.dcv_connection_gateway.certificate.private_key_secret_arn`. Esse é o ARN do 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 ambiente RES. 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 contêm 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 de subdomínio Route53 correspondente que você criou para seus desktops virtuais para apontar para o nome DNS 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 a VPC, as sub-redes públicas e privadas e outros parâmetros selecionados foram criados pela pilha.

   Se algum dos parâmetros estiver incorreto, talvez seja necessário excluir e reimplantar o ambiente RES. Para 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 com SSM na instância em execução do controlador vdc.

2. Executar `sudo su -`.
3. Executar `systemctl status sssd`.

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

Registro de erros do SSM

Para resolver o problema:

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

O problema pode 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 pilha RES.
   - directoryservice.ldap_connection_uri
   - serviço de diretório.ldap_base
   - directoryservice.users.ou

- directoryservice.groups.ou
- directoryservice.sudoers.ou
- directoryservice.computers.ou
- nome do serviço de diretório.name

2. Atualize todos os valores incorretos na tabela do DynamoDB. A tabela é encontrada no console do DynamoDB em Tabelas. O nome da tabela deve ser`<stack name>.cluster-settings`.
3. Depois de atualizar a tabela, exclua o cluster-manager e o vdc-controller que estão executando as instâncias do ambiente no momento. O Auto Scaling iniciará novas instâncias usando os valores mais recentes da tabela do DynamoDB.

Causa raiz 2: nome de ServiceAccount usuário incorreto inserido

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

1. No AWS console, abra o Secrets Manager.
2. Pesquise por `directoryserviceServiceAccountUsername`. O segredo deveria ser`<stack name>-directoryservice-ServiceAccountUsername`.
3. Abra o segredo para ver a página de detalhes. Em Valor secreto, escolha Recuperar valor secreto e escolha Texto sem formatação.
4. Se o valor tiver sido atualizado, exclua as instâncias cluster-manager e vdc-controller do ambiente atualmente em execução. O escalonamento automático iniciará novas instâncias usando o valor mais recente do Secrets Manager.

Causa raiz 3: ServiceAccount senha incorreta inserida

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

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

4. Se você esqueceu a senha ou não tem certeza se a senha digitada está correta, você pode redefinir a senha no Active Directory e no Secrets Manager.

   a. Para redefinir a senha em AWS Managed Microsoft AD:

      i. Abra o AWS console e vá para AWS Directory Service.

      ii. Selecione o ID do diretório para seu diretório RES e escolha Ações.

      iii. 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. Escolha 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 o`vdcdcvhostsecuritygroup`, isso pode ser devido a uma EC2 instância da Amazon que foi executada em uma sub-rede ou grupo de segurança criado pelo RES 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 no parâmetro de bloco CIDR durante a criação do ambiente

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

Exemplo de erro:

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

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

.....

CloudFormation falha na criação da pilha durante a criação do ambiente

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

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

.....

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

Se a criação da pilha do ambiente de demonstração falhar com o seguinte erro, pode ser devido à ocorrência inesperada de 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 RunCommand/Automation execução do SSM, verifique se a execução de um documento SSM 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 instâncias RES pelo menos 15 minutos após o lançamento.

.....

Problemas de gerenciamento de identidade

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

- the section called “Configurando o SSO com o IAM Identity Center”
- the section called “Configurando seu provedor de identidade para 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 passe uma função para o RES.

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 usuário do IAM 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 organização podem usar para acessar seus recursos. É possível 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 Como fornecer acesso a um usuário do IAM em outra AWS conta que você possui no Guia do usuário do IAM.
- 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 usuário do IAM.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Como fornecer acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.

- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as funções do IAM diferem das políticas baseadas em recursos no Guia do usuário do IAM.

.....

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

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

Para verificar os registros:

1. Abra o console de CloudWatch .
2. Em Grupos de registros, encontre o grupo chamado/*<environment-name>*/cluster-manager.
3. Abra o grupo de registros para pesquisar erros nos fluxos de registros.

Para verificar as configurações:

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

.....

Erro “Usuário não encontrado” ao tentar fazer login

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

- Se o usuário não estiver presente no RES e você o tiver adicionado recentemente ao AD
  - É possível que o usuário ainda não esteja sincronizado com o RES. O RES sincroniza de hora em hora, então talvez seja necessário esperar e verificar se o usuário foi adicionado após a próxima sincronização. Para sincronizar imediatamente, siga as etapas emUsuário adicionado no Active Directory, mas ausente do RES.
- Se o usuário estiver presente no RES:
  1. Certifique-se de que o mapeamento de atributos esteja configurado corretamente. Para obter mais informações, consulte Configurando seu provedor de identidade para login único (SSO).
  2. Certifique-se de que o assunto do SAML e o e-mail do SAML sejam mapeados para o endereço de e-mail do usuário.

.....

Usuário adicionado no Active Directory, mas ausente do RES

> **Note**
>
> Esta seção se aplica ao RES 2024.10 e versões anteriores. Para RES 2024.12 e versões posteriores, consulte. Como executar manualmente a sincronização (versão 2024.12 e posterior)

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

Inicie o processo de sincronização manualmente:

1. Abra o console do Amazon SQS.

2. Em Filas, selecione<environment-name>-cluster-manager-tasks.fifo.
3. Escolha Enviar e receber mensagens.
4. Em Corpo da mensagem, insira:

   { "name": "adsync.sync-from-ad", "payload": {} }
5. Em ID do grupo de mensagens, digite: **adsync.sync-from-ad**
6. Em ID de desduplicação de mensagens, insira uma sequência de caracteres alfanumérica aleatória. Essa entrada deve ser diferente de todas as chamadas 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 o limite de resultados de pesquisa ldap do seu IDP.

.....

Armazenamento

Tópicos

- Não consigo me conectar a partir read/write de hosts VDI
- Eu criei o Amazon FSx for NetApp ONTAP a partir do RES, mas ele não se juntou ao meu domínio

.....

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

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

Amazon EFS

1. Acesse o console do Amazon EFS.
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 os hosts VDI.

Amazon FSx ONTAP

1. Acesse o FSx console da Amazon.
2. Verifique se o status está disponível.
3. Se o status não estiver disponível, aguarde antes de iniciar os hosts VDI.

.....

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

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

- Tráfego NFS (porta: 2049) dos hosts Linux VDC

- Tráfego SMB (porta: 445) dos hosts VDC do Windows

.....

Não consigo me conectar a partir read/write de hosts VDI

O ONTAP suporta os estilos de segurança UNIX, NTFS e MIXED para os volumes. Os estilos de segurança determinam o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e qual tipo de cliente pode modificar essas permissões.

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

Exemplos de casos de uso de tratamento de permissões

Usando o volume no estilo UNIX 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 read/write permissões `<group-ID>` totais no `/<project-name>` diretório:

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

Usando o volume no estilo NTFS 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 ControlChange`, ou `Read` para `Allow` ou`Deny`:

Se o volume for usado por clientes Linux e Windows, precisamos configurar um mapeamento de nomes no SVM que associará qualquer nome de usuário Linux ao mesmo nome de usuário com o formato de nome de domínio NetBIOS 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 o Amazon FSx for NetApp ONTAP a partir do RES, mas ele não se juntou ao meu domínio

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

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

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 nome DNS SMB 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. Os novos hosts VDI que usam o sistema de arquivos agora poderão montar o SVM e o sistema de arquivos unidos ao domínio.

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

.....

Snapshots

Tópicos

.....

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 do 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 ExportStatus várias tabelas é CONCLUÍDO. 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 mude para CONCLUÍDO em 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

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:

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

Se uma conexão de desktop for fechada ou você não puder mais se conectar a ela, o problema pode ser devido à falha da EC2 instância Amazon subjacente ou a 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 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 DCV Session, 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 servidor DCV 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 SSM Session Manager 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.

.....

VDIs preso no estado de aprovisionamento

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 ID da AMI 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 nem as ferramentas necessárias. Os arquivos de log na instância, como `/root/bootstrap/logs/` em uma instância Linux, podem conter informações úteis sobre isso. AMIs IDs retirados do AWS Marketplace podem não funcionar para instâncias de desktop RES. Eles precisam de testes para confirmar se são compatíveis.

- Os scripts de dados do usuário não são executados quando a instância de desktop virtual do Windows é iniciada a partir de uma AMI personalizada.

  Por padrão, os scripts de dados do usuário são executados uma vez quando uma EC2 instância da Amazon é iniciada. Se você criar uma AMI a partir de uma instância de desktop virtual existente, depois registrar uma pilha de software na 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 usada para criar a AMI e execute o seguinte comando:

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

  Em seguida, crie uma nova AMI a partir da instância. Você pode usar a nova 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 terá o mesmo problema novamente ao iniciar outra área de trabalho virtual a partir da AMI configurada incorretamente.

.....

VDIs entrar em estado de erro após o lançamento

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

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

1. A versão RES implantada é 2024.01 ou superior.
2. Durante a implantação da pilha RES, o atributo for `EnableLdapIDMapping` foi definido como. `True`

3. O sistema de arquivos inicial especificado durante a implantação da pilha RES foi usado na versão anterior ao 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 os usuários da tabela DDB 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. Reinicialize a instância VDI no `Error` estado a partir da página da web do RES. Valide se o VDI faz a 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 na junção do módulo AD/eVDI e mostra Failed API Health Check
- 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”
- Problemas de opções de DHCP com a configuração external/customer do AD
- 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 pelo RES têm tags que são usadas como parte das políticas de controle de acesso do IAM 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 na junção do módulo AD/eVDI e mostra Failed API Health Check

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

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: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - Você pode acessar o ServiceAccount nome de usuário fornecido durante a implantação do RES 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, certifique-se de que o usuário ServiceAccount "" tenha 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 assinante do SQS 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 o RES não tenha sido configurado corretamente para o AD em uso. Um exemplo pode ser que o

`ServiceAccountCredentialsSecretArn` parâmetro usado na criação do BI/RES 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 após ter feito login com sucesso via SSO.

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

.....

Problemas de opções de DHCP com a configuração external/customer do AD

Se você encontrar um erro informando `"The connection has been closed. Transport error"` sobre os desktops virtuais do Windows ao usar o RES com seu próprio Active Directory, verifique o CloudWatch log da dcv-connection-gateway Amazon em busca de algo semelhante ao seguinte:

```
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 AD para suas opções de DHCP para sua própria VPC, você precisará:

1. Adicione o AmazonProvided DNS aos dois controladores IPs de domínio.
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, porque RES/DCV procura ip-10-0-x-xx.ec2.internal hostname.

.....

Erro do Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Ao usar o navegador Firefox, você pode encontrar a mensagem de erro do tipo MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING ao tentar se conectar a uma área de trabalho virtual.

A causa é que o servidor web RES está configurado com TLS + Stapling On, mas não está respondendo com Stapling Validation (consulte 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 registros de VDI
- Baixando registros de EC2 instâncias Linux
- Baixando registros de EC2 instâncias do Windows
- Coletando registros do ECS para o erro WaitCondition

.....

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 no 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. Acesse o console do IAM 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` Escolher`CloudFormation`.

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

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 console do IAM 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 registros de VDI

Identifique a EC2 instância correspondente da Amazon

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

Colete registros de VDI 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 instância VDI da Amazon EC2 .

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

Coletar registros de VDI 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 na EC2 instância da VDI.

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 registros de VDI.

.....

Baixando registros de VDI

1. Atualize a função do IAM da EC2 instância de VDI para permitir o acesso ao S3.
2. Acesse o EC2 console e selecione sua instância de VDI.
3. Selecione a função do IAM que ele 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 tipo de VDI para baixar os registros. O nome do módulo seria o nome da instância.
   a. Baixando registros de EC2 instâncias Linuxpara Linux.
   b. Baixando registros de EC2 instâncias do Windowspara Windows.
7. Por fim, edite a função para remover a `AmazonS3FullAccess` política.

> **Note**
>
> Todos VDIs usam a mesma função do IAM, 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 registros do ECS para o erro WaitCondition

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

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 do Active Directory Service
3. Acesse o EC2 console e encerre a instância do gerenciador de cluster. As regras do Auto Scaling acionarão automaticamente a implantação de uma nova instância.

.....

O keycloak da pilha de demonstração não está funcionando

Problema

Se o servidor do keycloak travou e, quando você reiniciou o servidor, o IP da instância mudou, isso pode ter resultado na quebra do keycloak — a página de login do seu portal RES falha ao carregar ou fica presa em um estado de carregamento que nunca é resolvido.

Mitigação

Você precisará excluir a infraestrutura existente e reimplantar a pilha do Keycloak para restaurar o Keycloak a um estado saudável. Siga estas etapas:

1. Acesse o Cloudformation. Você deve ver duas pilhas relacionadas ao keycloak lá:
   - `<env-name>-RESSsoKeycloak-<random characters>`(Pilha 1)

     `<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-*`(Pilha 2)
2. Exclua Stack1. Se solicitado a excluir a pilha aninhada, selecione Sim para excluir a pilha aninhada.

   Certifique-se de que a pilha tenha sido completamente excluída.
3. Baixe o modelo de pilha RES SSO Keycloak aqui.
4. Implante essa pilha manualmente com exatamente os mesmos valores de parâmetros da pilha excluída. Implante-o a partir do CloudFormation console acessando Criar pilha → Com novos

recursos (padrão) → Escolha um modelo existente → Carregar um arquivo de modelo. Preencha os parâmetros necessários usando as mesmas entradas da pilha excluída. Você pode encontrar essas entradas na sua pilha excluída alterando o filtro no CloudFormation console e acessando a guia Parâmetros. Certifique-se de que o nome do ambiente, o key pair e outros parâmetros correspondam aos parâmetros originais da pilha.

5. Depois que a pilha for implantada, seu ambiente estará pronto para ser usado novamente. Você pode encontrá-los ApplicationUrl na guia Saídas da pilha implantada.

.....

Problemas conhecidos

Problemas conhecidos 2024.x

.....

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

Descrição do bug

O Research and Engineering Studio 2024.08 não consegue montar buckets read/write S3 em uma instância de infraestrutura de desktop virtual (VDI) ao usar um ARN de bucket raiz (ou seja,`arn:aws:s3:::example-bucket`) e um prefixo personalizado (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
- buckets de leitura/gravação com um prefixo como parte do ARN do bucket (ou seja,`arn:aws:s3:::example-bucket/example-folder-prefix`) e prefixo personalizado (nome do projeto ou nome do projeto e nome do usuário)
- buckets de leitura/gravação com um ARN do bucket raiz, mas sem prefixo personalizado

Depois de provisionar uma instância de VDI, o diretório de montagem especificado para esse bucket do S3 não terá o bucket montado. Embora o diretório de montagem na 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 ambiente RES:

   a. O patch só se aplica ao RES 2024.08.

   b. O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.

   c. Configure a AWS CLI para a conta e a região em que o RES é implantado e certifique-se de ter permissões do Amazon S3 para gravar no bucket criado pelo 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 de patch 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 ambiente RES 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 configurações de VPC privadas, se você ainda não tiver feito isso, para a `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` função, certifique-se de adicionar o nome `AWS_STS_REGIONAL_ENDPOINTS` e o valor `Environment variable` de. `regional` Consulte Pré-requisitos do bucket Amazon S3 para implantações isoladas de VPC para obter 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 grupo que terá os buckets read/write S3 com ARN do bucket raiz e prefixo personalizado montados corretamente.

.....

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

Problema

O RES 2024.06 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 do fato de o RES aceitar apenas nomes de grupos que atendam aos seguintes requisitos:

- Ele só pode conter letras ASCII minúsculas e maiúsculas, 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 de patch 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 <environment-name> pelo nome do seu ambiente RES:

a. O patch só se aplica ao RES 2024.06

b. O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.

c. Configure a AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo 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 de patch 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 letras ASCII minúsculas e maiúsculas, dígitos, traço (-), ponto (.), sublinhado (_) e espaços com um comprimento total entre 1 e 30, inclusive.

.....

(2024.04-2024.04.02) Limite de permissão do IAM fornecido não anexado à função das instâncias de 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 parâmetro IAMPermission Boundary 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 ao 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 CLI (v2), Python 3.9.16 ou superior e Boto3.

   c. Configure a AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo 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 de patch e o arquivo de patch são baixados. Execute o seguinte comando de patch, `<environment-name>` substituindo-o pelo nome do seu ambiente RES:

```
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 a partir do 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 criar desktops virtuais (VDIs) em RES com configurações específicas. Cada AMI tem uma ID associada que difere por região. A ID da AMI configurada no RES para iniciar instâncias Windows Nvidia em ap-southeast-2 (Sydney) está incorreta no momento.

O AMI-ID `ami-0e190f8939a996caf` para esse tipo de configuração de instância está listado incorretamente em ap-southeast-2 (Sydney). Em vez disso, o ID da AMI `ami-027cf6e71e2e442f4` deve ser usado.

Os usuários receberão o seguinte erro ao tentarem iniciar uma instância com a `ami-0e190f8939a996caf` AMI padrão.

```
An error occured (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 o RES na região ap-southeast-2.
- Execute uma instância usando a pilha de software padrão Windows-NVIDIA (ID AMI). `ami-0e190f8939a996caf`

Versões afetadas

Todas as versões do RES 2024.04.02 ou anteriores são afetadas

Mitigação

A seguinte mitigação foi testada na versão 2024.01.01 do RES:

- Registre uma nova pilha de software com as seguintes configurações
  - ID da AMI: `ami-027cf6e71e2e442f4`
  - Sistema operacional: Windows
  - Fabricante da GPU: NVIDIA
  - Min. Tamanho de armazenamento (GB): 30
  - Min. MEMÓRIA RAM (GB): 4
- Use essa pilha de software para iniciar instâncias Windows-NVIDIA

.....

(2024.04 e 2024.04.01) Falha na exclusão de RES em GovCloud

O problema

Durante o fluxo de trabalho de exclusão do RES, 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 versão padrão da AWS CLI entre Commercial e GovCloud regiões, a `update_user_pool` chamada no Lambda falhará nas regiões. GovCloud

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

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

Etapas para reproduzir o bug:

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

Versões afetadas

RES versões 2024.04 e 2024.04.01

Mitigação

A seguinte mitigação foi testada na versão 2024.04 do RES:

- 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 pilha RES -> deixe o recurso do instalador do Retain DESMARCADO -> Excluir.

.....

(2024.04 - 2024.04.02) O desktop virtual Linux pode ficar preso no status “RETOMANDO” na reinicialização

O problema

Os desktops virtuais Linux podem ficar presos no status “RETOMANDO” ao serem reiniciados após uma parada manual ou programada.

Depois que a instância é reinicializada, o AWS Systems Manager não executa nenhum comando remoto para criar uma nova sessão DCV 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 “RETOMANDO”:

1. SSH na instância problemática 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 ao RES 2024.04.02.
> - O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.
> - Configure a AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo 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 de patch e o arquivo de patch são baixados. Execute o seguinte comando de patch, `<environment-name>` substituindo-o pelo nome do seu ambiente RES e `<aws-region>` pela região em que o 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 seguintes comandos, `<environment-name>` substituindo-os pelo nome do seu ambiente RES:

```
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 atributo SAMAccount Name inclui letras maiúsculas ou caracteres especiais

O problema

O RES não sincroniza os usuários do AD após a configuração do SSO 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 do fato de o RES aceitar apenas um SAMAccount nome de usuário que atenda aos seguintes requisitos:

- Ele só pode conter letras ASCII 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 ao RES 2024.04.02.
   > - O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.
   > - Configure a AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo 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 de patch e o arquivo de patch são baixados. Execute o seguinte comando de patch, `<environment-name>` substituindo-o pelo nome do seu ambiente RES:

```
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 ambiente RES. Você também pode encerrar a instância a partir do 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 web RES, 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 com RES durante a sincronização do AD

Descrição do bug

Os membros do grupo não sincronizarão adequadamente com o RES se o GroupOU for diferente do UserOU.

O RES cria 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 versões do RES 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 seguintes comandos, `<output-directory>` substituindo-os pelo diretório local em que você gostaria de baixar os arquivos e pela versão do RES que você deseja corrigir: `<res_version>`

   > **Note**
   >
   > - O script de patch requer AWS CLI v2, Python 3.9.16 ou superior e Boto3.

- Configure a AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo RES.
- O patch suporta apenas as versões RES 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.
  - Versão RES: RES 2024.04.02

    Link para download do patch: 2024.04.02_group_member_sync_bug_fix.patch
  - Versão RES: 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 de patch e o arquivo de patch são baixados. Execute o seguinte comando de patch, `<environment-name>` substituindo-o pelo nome do seu ambiente RES:

```
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, Regre, Vulnerabilidade de segurança no Ubuntu SSHion RHEL9 VDIs

Descrição do bug

O CVE-2024-6387, apelidado de regre, foi identificado no servidor OpenSSHSSHion. 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 OpenSSH para comunicações seguras.

Para RES, a configuração padrão é passar do bastion host para SSH em desktops virtuais, e o bastion host não é afetado por essa vulnerabilidade. No entanto, a AMI (Amazon Machine Image) padrão que fornecemos RHEL9 e o Ubuntu2024 VDIs (Virtual Desktop Infrastructure) em TODAS as versões do RES utilizam uma versão do OpenSSH 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 versões do RES 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 extraídos usando o respectivo gerenciador de pacotes da plataforma.

Se você já RHEL9 tem um Ubuntu VDIs, recomendamos seguir as VDIs instruções do PATCH EXISTING abaixo. Para corrigir o futuro VDIs, recomendamos seguir as VDIs instruções do PATCH

FUTURE. Essas instruções descrevem como executar um script para aplicar a atualização da plataforma em seu VDIs.

PATCH EXISTENTE VDIs

1. Execute o seguinte comando que corrigirá todo o Ubuntu existente e RHEL9 VDIs:

   a. O script de patch requer AWS CLI v2.

   b. Configure a AWS CLI para a conta e a região em que o RES está implantado e verifique se você tem 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 mensagem de SUCESSO.

FUTURO DO PATCH 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 ao RES 2024.06.
   > - O script de patch requer AWS CLI (v2), Python 3.9.16 ou superior e Boto3.
   > - Configure sua cópia da AWS CLI para a conta e a região em que o RES está implantado e certifique-se de ter permissões do S3 para gravar no bucket criado pelo 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 suportado nas versões 2024.06 e posteriores do RES. Para corrigir o futuro VDIs em ambientes RES com versões anteriores a 2024.06, primeiro atualize o ambiente RES 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 fazer login remotamente em EC2 instâncias da Amazon sem RDP e sem a necessidade de licenças RDP. 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 das perguntas frequentes.

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas AWS atuais de produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. AWS as responsabilidades e obrigações para com seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum acordo entre AWS e seus clientes.

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

Revisões

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

Data	Alteração
Dezembro de 2024	• Versão de lançamento 2024.12 Seções adicionadas — • Sincronização do Active Directory. • Configurando as permissões da área de trabalho. • Configurando o acesso ao navegador de arquivos. • Configurando o acesso SSH. • Configurando usuários do Amazon Cognito. Seções alteradas — • Limites ambientais. • Configurar uma VPC privada (opcional).
Outubro de 2024	• Versão de lançamento 2024.10: suporte adicionado para — • Limites ambientais. • Perfis de compartilhamento de desktop. • Parada automática da interface de desktop virtual.
Agosto de 2024	• Versão de lançamento 2024.08: suporte adicionado para — • montagem de buckets do Amazon S3 em instâncias de infraestrutura de desktop virtual (VDI) Linux. Consulte Buckets do Amazon S3.

Data	Alteração
	• 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	• 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 prontos para RES e de lançamento de projetos AMIs
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.