Guia de conceitos básicos

AWS Management Console

Versão 1.0

AWS Management Console: Guia de conceitos básicos

Table of Contents

O que é o AWS Management Console?

AWS Management ConsoleÉ um aplicativo da web que compreende e se refere a uma ampla coleção de consoles de serviço para gerenciar AWS recursos. Quando você faz login pela primeira vez, vê a página inicial do console. A página inicial fornece acesso a todos os consoles de serviço e oferece um único local para acessar as informações necessárias para executar as tarefas da AWS relacionadas. Ele também permite que você personalize a experiência do Console Home adicionando, removendo e reorganizando widgets como Recently visited,AWS Health e muito mais.

> **Note**
>
> A opção de seleção de idioma foi movida para a nova página Unified Settings (Configurações unificadas). Para obter mais informações, consulte Alterar o idioma do AWS Management Console.

Os consoles de serviço individuais, por outro lado, oferecem uma ampla gama de ferramentas para computação em nuvem, bem como informações sobre sua conta e faturamento.

Usar o dispositivo de sua escolha

O AWS Management Console foi projetado para funcionar em tablets e outros tipos de dispositivos:

- O espaço horizontal e vertical foi maximizado para exibir mais conteúdo em sua tela.

- Botões e seletores ficaram maiores para uma melhor experiência de toque.

Também AWS Management Console está disponível como um aplicativo para Android e iOS. Este aplicativo viabiliza tarefas relevantes em dispositivos móveis, sendo um ótimo complemento à experiência completa na Web. Por exemplo, você pode facilmente visualizar e gerenciar suas instâncias existentes do Amazon EC2 e os CloudWatch alarmes da Amazon a partir do seu telefone.

Você pode baixar o aplicativo móvel AWS Console na Amazon Appstore, Google Play ou iTunes.

Configurando o AWS Management Console

Este tópico descreve como configurar suas AWS Management Console e como usar a página Configurações Unificadas para definir padrões que se aplicam a todos os consoles de serviço. Também explica os widgets, um recurso do painel inicial do console que permite adicionar componentes personalizados que rastreiam informações sobre seus AWS serviços e recursos.

Tópicos

Trabalhar com widgets

O painel inicial do console inclui widgets que exibem informações importantes sobre seu AWS ambiente e fornecem atalhos para seus serviços. Você pode personalizar sua experiência adicionando e removendo widgets, reorganizando-os ou alterando seu tamanho.

Como adicionar um widget

1. No canto superior ou inferior direito do painel inicial do console, selecione o botão +Adicionar widgets.
2. Escolha o indicador de arrasto, representado por seis pontos verticais no canto superior esquerdo da barra de título do widget, e arraste-o para o painel inicial do console.

Como remover um widget

1. Selecione as reticências, representadas por três pontos verticais no canto superior direito da barra de título do widget.
2. Selecione Remove widget (Remover widget).

Como reorganizar seus widgets

- Escolha o indicador de arrasto, representado por seis pontos verticais no canto superior esquerdo da barra de título do widget, e arraste-o widget para um novo local no painel inicial do console.

Como redimensionar um widget

- Selecione o ícone de redimensionamento no canto inferior direito do widget e arraste para redimensionar o widget.

Se você quiser começar de novo com a organização e a configuração dos widgets, redefina o painel inicial do console como o layout padrão. Isso vai reverter as alterações no layout do painel inicial do console e restaurar todos os widgets para a localização e o tamanho padrão.

Como redefinir a página como o layout padrão

1. No canto superior direito da página, selecione o botão Restaurar layout padrão.
2. Para confirmar, escolha Redefinir.

> **Note**
>
> Isso reverterá todas as alterações no layout do painel inicial do console.

Como solicitar um novo widget no painel inicial do console

1. No canto inferior esquerdo do painel inicial do console, selecione Quer ver outro widget? Conte-nos!

   Descreva o widget a ser adicionado à página inicial do console.
2. Selecione Enviar.

> **Note**
>
> Suas sugestões são analisadas periodicamente e novos widgets podem ser adicionados em atualizações futuras ao AWS Management Console.

Definir configurações unificadas

Você pode definir configurações e padrões, como exibição, idioma e região, na página Configurações AWS Management Console unificadas. O modo visual e o idioma padrão também podem ser definidos diretamente na barra de navegação. Essas alterações se aplicam a todos os consoles de serviço.

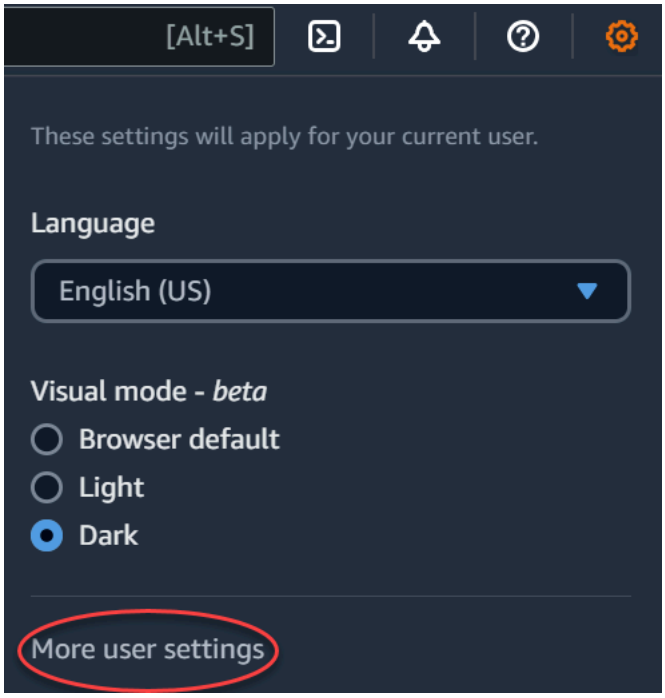
> **Important**
>
> Para garantir que suas configurações, serviços favoritos e serviços visitados recentemente persistam globalmente, esses dados são armazenados em todos Regiões da AWS, incluindo regiões que estão desativadas por padrão. Essas regiões são África (Cidade do Cabo), Ásia-Pacífico (Hong Kong), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Jacarta), Europa (Milão), Europa (Espanha), Europa (Zurique), Oriente Médio (Bahrein) e Oriente Médio (EAU). Você ainda precisa habilitar manualmente uma região para acessá-la e para criar e gerenciar recursos nessa região. Se você não quiser armazenar todos esses dados Regiões da AWS, escolha Redefinir tudo para limpar suas configurações e, em seguida, opte por não lembrar os serviços visitados recentemente no gerenciamento de configurações.

Acessando configurações unificadas

O procedimento a seguir descreve como acessar as Configurações Unificadas.

Para acessar as configurações unificadas

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de engrenagem.
3. Para abrir a página Configurações unificadas, selecione Mais configurações do usuário.



Redefinindo configurações unificadas

Você pode excluir todas as configurações das Configurações Unificadas e restaurar as configurações padrão redefinindo as Configurações Unificadas.

> **Note**
>
> Isso afeta várias áreas AWS, incluindo serviços favoritos na navegação e no menu Serviços, serviços visitados recentemente nos widgets do Console Home e no AWS Console Mobile Application, e todas as configurações que se aplicam aos serviços, como idioma padrão, região padrão e modo visual.

Para redefinir todas as configurações unificadas

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de engrenagem.
3. Abra a página Configurações unificadas escolhendo Mais configurações do usuário.
4. Escolha Redefinir tudo.

Editando configurações unificadas

O procedimento a seguir descreve como editar suas configurações preferidas.

Para editar as configurações unificadas

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de engrenagem.
3. Abra a página Configurações unificadas escolhendo Mais configurações do usuário.
4. Selecione Edite (Edit) próximo às configurações de sua preferência:

   - Localização e região padrão:
     - Idioma permite escolher o idioma padrão para o texto do console.
     - Default Region (Região padrão) permite escolher uma região padrão que se aplica sempre que você faz login. Você pode escolher qualquer uma das regiões disponíveis para a sua conta. Também é possível escolher a última região usada como padrão.

       Para saber mais sobre o roteamento da região no AWS Management Console, consulte Escolher uma região.
   - Exibição:
     - O Visual mode (Modo visual) permite que você defina o console para o modo claro, escuro ou o modo de exibição padrão do navegador.

       O modo escuro é um recurso beta e pode não se aplicar a todos os consoles de serviços da AWS .
     - Exibição da barra de favoritos alterna a exibição da barra Favoritos entre o nome completo do serviço e o respectivo ícone ou apenas o ícone do serviço.
     - Tamanho do ícone da barra de favoritos alterna o tamanho do ícone de serviço na exibição da barra de Favoritos entre pequeno (16 x 16 pixels) e grande (24 x 24 pixels).
   - Settings management: (Gerenciamento de configurações)
     - Lembrar serviços visitados recentemente permite que você escolha se AWS Management Console lembra dos serviços visitados recentemente. Desativar isso também exclui seu histórico de serviços visitados recentemente, para que você não veja mais os serviços visitados recentemente no menu Serviço ou nos widgets do Console Home. AWS Console Mobile Application
5. Escolha Salvar alterações.

Alterar o modo visual do AWS Management Console

Seu modo visual configura o console para o modo claro, escuro ou o modo de exibição padrão do seu navegador.

Como alterar o modo visual na barra de navegação

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de engrenagem.
3. Para o Modo visual, escolha Claro para o modo claro, Escuro para o modo escuro ou Navegador padrão para o modo de exibição padrão do navegador.

Alterando o idioma padrão nas Configurações unificadas

O procedimento a seguir descreve como alterar o idioma padrão usando a barra de navegação.

Como alterar o idioma padrão na barra de navegação

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de engrenagem.
3. Em Idioma, selecione Navegador padrão ou escolha o idioma preferido na lista suspensa.

Escolher uma região

Para muitos serviços, você pode escolher um Região da AWS que especifique onde seus recursos são gerenciados. As regiões são conjuntos de AWS recursos localizados na mesma área geográfica. Você não precisa escolher uma região para AWS Management Consoleou para alguns serviços, como AWS Identity and Access Management. Para saber mais sobre Regiões da AWS, consulte Gerenciar Regiões da AWS na Referência geral da AWS.

Para escolher uma região

1. Faça login no AWS Management Console.
2. Escolha um serviço para acessar o console dele.
3. Na barra de navegação, escolha o nome da região exibida no momento. Depois, escolha a região para a qual pretende alternar.

Para escolher uma região padrão

1. Na barra de navegação, escolha o ícone de configurações e selecione Mais configurações do usuário para navegar pela página Configurações unificadas.
2. Selecione Edit (Editar) próximo a Localization and default Region (Localização e região padrão).
3. Selecione sua região padrão e escolha Salvar configurações. Se não selecionar uma região padrão, a última região que você acessou será usada como padrão.
4. (Opcional) Escolha Ir para a nova região padrão para ir imediatamente para sua nova região padrão.

> **Note**
>
> Se você criou AWS recursos, mas não os vê no console, o console pode estar exibindo recursos de uma região diferente. Alguns recursos (como instâncias do Amazon EC2) são específicos da região em que foram criados. Para visualizá-los, use o seletor de regiões para escolher a região que contém os recursos.

Adição e remoção de favoritos

Para acessar seus serviços usados com frequência mais rapidamente, você pode salvar os consoles de serviço deles em uma lista de favoritos.

Para adicionar um serviço à lista de Favoritos

1. Faça login no AWS Management Console.
2. Selecione o botão Add widgets (Adicionar widgets) no lado superior ou inferior direito da página.
3. No menu Adicionar widgets, selecione Favoritos para adicionar ao console e escolha Adicionar.

   Os Favoritos serão adicionados na parte inferior da página inicial do console. É possível arrastar e soltar os Favoritos selecionando a barra de título na parte superior do widget e, depois, arrastar o widget para um novo local na página.
4. Na barra de navegação, escolha Services (Serviços).
5. Na lista Visitado recentemente ou na lista Todos os serviços, passe o mouse sobre o nome do serviço que deseja adicionar como favorito.
6. Selecione a estrela à esquerda do nome do serviço.

7. Repita as duas etapas anteriores para adicionar mais serviços à sua lista Favorites (Favoritos).

Para remover um serviço da lista de Favoritos

1. Na barra de navegação, escolha Services (Serviços).
2. Execute um destes procedimentos:
   - Na lista Favoritos, passe o mouse sobre o nome de um serviço. Depois, escolha o x à direita do nome do serviço.
   - Na lista Recently visited (Visitados recentemente) ou na lista All services (Todos os serviços), desmarque a estrela próximo ao nome de um serviço que esteja em sua lista Favorites (Favoritos).

Alterar sua senha

Se você for proprietário de uma conta, poderá alterar a senha da AWS conta no AWS Management Console.

Como alterar sua senha do

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o nome da conta.
3. Selecione Security credentials (Credenciais de segurança).
4. As opções exibidas variarão dependendo do seu Conta da AWS tipo. Siga as instruções mostradas no console para alterar a senha.
5. Insira sua senha atual uma vez e a nova senha duas vezes.

   A nova senha deve ter pelo menos oito caracteres e deve incluir o seguinte:

   - Pelo menos um símbolo
   - Pelo menos um número
   - Pelo menos uma letra maiúscula
   - Pelo menos uma letra minúscula
6. Selecione Change Password (Alterar senha) ou Save changes (Salvar alterações).

Alterando o idioma do AWS Management Console

A AWS Console Home experiência inclui a página Configurações unificadas, na qual você pode alterar o idioma padrão AWS dos serviços no AWS Management Console. Você também pode alterar o idioma padrão rapidamente no menu de configurações, que pode ser acessado na barra de navegação. Você pode fazer essa alteração em qualquer lugar no console.

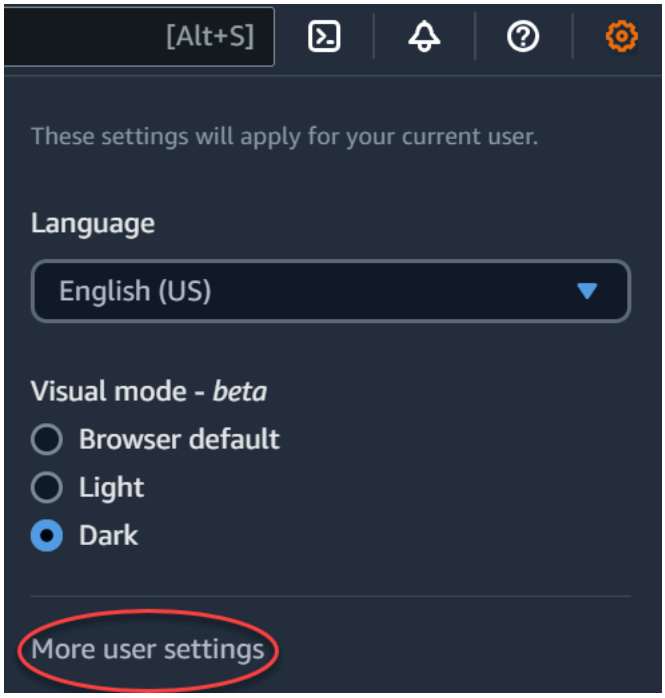
> **Note**
>
> Esse procedimento altera o idioma de todos os consoles, mas não da documentação da AWS . Para alterar o idioma da documentação, use o menu de idiomas no canto superior direito de qualquer página de documentação.

AWS Management Console Atualmente, o suporta os seguintes idiomas:

- Inglês (EUA)
- Inglês (Reino Unido)
- Bahasa Indonésia
- Alemão
- Francês
- Japonês
- Espanhol
- Italiano
- Português
- Coreano
- Chinês (simplificado)
- Chinês (tradicional)

Como alterar o idioma padrão em “Configurações unificadas”

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de configurações.
3. Para abrir a página Configurações unificadas, selecione Mais configurações do usuário.



4. Em Unified Settings (Configurações unificadas), selecione Edit (Editar) próximo a Localization and default Region (Localização e região padrão).
5. Para selecionar o idioma desejado para o console, escolha uma das seguintes opções:

   - Escolha o Padrão do navegador na lista suspensa e selecione Salvar configurações.

     O texto do console para todos os AWS serviços aparece no idioma de sua preferência que você definiu nas configurações do seu navegador.

     > **Note**
     >
     > O navegador padrão só é compatível com os idiomas disponíveis no AWS Management Console.

   - Escolha o idioma preferido na lista suspensa e selecione Salvar configurações.

     O texto do console para todos os AWS serviços aparece em seu idioma preferido.

Como alterar o idioma padrão na barra de navegação

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha o ícone de configurações.

3. Em Idioma, selecione Navegador padrão ou escolha o idioma preferido na lista suspensa.

Conceitos básicos de um serviço

O AWS Management Console fornece várias formas de navegar em consoles de serviços individuais.

Para abrir um console de um serviço

Execute um destes procedimentos:

- Na caixa de pesquisa na barra de navegação, insira todo ou parte do nome do serviço. Em Services (Serviços), escolha o serviço que você deseja na lista de resultados da pesquisa. Para mais informações, consulte Pesquisando produtos, serviços, recursos e muito mais usando a Pesquisa Unificada.
- No widget Recently visited services (Serviços visitados recentemente), escolha o nome de um serviço.
- No widget Recently visited services (Serviços visitados recentemente), escolha View all AWS services (Ver todos os serviços da AWS). Em seguida, na página All AWS services (Todos os serviços da AWS), escolha um nome de serviço.
- Na barra de navegação, escolha Services (Serviços) para abrir uma lista completa de serviços. Em seguida, escolha um serviço em Recently visited (Visitados recentemente) ou All services (Todos os serviços).

Pesquisando produtos, serviços, recursos e muito mais usando a Pesquisa Unificada

A caixa de pesquisa na barra de navegação fornece uma ferramenta de pesquisa unificada para rastrear recursos e serviços da AWS , documentação de serviço e AWS Marketplace. Basta digitar alguns caracteres para ver os resultados de todas essas categorias. Quanto mais caracteres você digitar, mais a pesquisa refinará seus resultados.

Para pesquisar um serviço, recurso, documentação ou AWS Marketplace produto

1. Na caixa de pesquisa na barra de navegação do AWS Management Console, insira todos ou parte dos termos de pesquisa.
2. Realize um dos seguintes procedimentos para refinar sua pesquisa e obter mais detalhes:
   - Para restringir os resultados ao tipo de conteúdo desejado, escolha uma das categorias à esquerda.
   - Para ver mais resultados para uma categoria específica, escolha See all ***n*** results (Ver todos os n resultados) por cada título de categoria. Para retornar à lista de resultados principal, escolha Back (Voltar) no canto superior esquerdo.
   - Para navegar rapidamente para recursos populares de um serviço, pause no nome do serviço nos resultados e escolha um link.
   - Para obter mais detalhes sobre uma documentação ou AWS Marketplace resultado, faça uma pausa no título do resultado.
3. Escolha qualquer link para navegar até o serviço, tópico ou página do AWS Marketplace desejada.

> **Tip**
>
> Você também pode usar o teclado para navegar rapidamente até o resultado da pesquisa superior. Primeiro, pressione Alt+s (Windows) ou Option+s (macOS) para acessar a barra de pesquisa. Em seguida, comece a inserir seu termo de pesquisa. Quando o resultado pretendido aparecer na parte superior da lista, pressione Enter. Por exemplo, para navegar rapidamente para o console do Amazon EC2, insira ec2 e pressione Enter.

Converse com o Amazon Q Developer

O Amazon Q Developer é um assistente de conversação com inteligência artificial generativa (IA) que pode ajudar você a entender, criar, ampliar e operar AWS aplicativos. Você pode fazer qualquer pergunta à Amazon Q AWS, incluindo perguntas sobre AWS arquitetura, seus AWS recursos, melhores práticas, documentação e muito mais. Você também pode criar casos de suporte e receber assistência de um agente ativo. Para obter mais informações, consulte O que é o Amazon Q? no Amazon Q Developer User Guide.

Comece a usar o Amazon Q

Você pode começar a conversar com o Amazon Q nos sites de AWS documentação AWS Management Console, AWS nos sites ou no AWS Console Mobile Application, escolhendo o ícone hexagonal Amazon Q. Para obter mais informações, consulte Comece a usar o Amazon Q Developer no Amazon Q Developer User Guide.

Exemplos de perguntas

A seguir estão alguns exemplos de perguntas que você pode fazer à Amazon Q:

- `How do I get billing support?`
- `How do I create an EC2 instance?`
- `How do I troubleshoot a "Failed to load" error?`
- `How do I close an AWS account?`
- `Can you connect me with a person?`

O que está acontecendo com MyApplications? AWS

O myApplications é uma extensão da página inicial do console que ajuda você a gerenciar e monitorar o custo, a integridade, o procedimento de segurança e a performance das aplicações na AWS. Você pode acessar todos os aplicativos em sua conta, as principais métricas de todos os aplicativos e uma visão geral das métricas e insights de custo, segurança e operações de vários consoles de serviço a partir de uma visualização no AWS Management Console. myApplications inclui o seguinte:

- Widget de aplicações na página inicial do console.
- O myApplications que você pode usar para visualizar os custos dos recursos da aplicação e as descobertas de segurança.
- O painel do myApplications que oferece uma visão das principais métricas da aplicação, como descobertas de custo, performance e segurança.

Atributos do myApplications

- Criar aplicações: crie aplicações e organize os recursos. Seus aplicativos são exibidos automaticamente no MyApplications, para que você possa agir nas APIs AWS Management Console, CLI e SDKs. A infraestrutura como código (IaC) é gerada ao criar uma aplicação e pode ser acessada no painel do myApplication. O IaC pode ser usado em ferramentas de IaC, incluindo AWS CloudFormation o Terraform.
- Acessar as aplicações: é possível acessar rapidamente qualquer uma das aplicações pelo widget myApplications, basta selecioná-las.
- Comparar métricas de aplicações: use o myApplications para comparar as principais métricas de aplicações, como custo dos recursos da aplicação e número de descobertas críticas de segurança de várias aplicações.
- Monitore e gerencie aplicativos — avalie a integridade e o desempenho dos aplicativos usando alarmes, canários e objetivos de nível de serviço Amazon CloudWatch, descobertas e tendências de AWS Security Hub custo de. AWS Cost Explorer Service Você também pode encontrar resumos e otimizações de métricas computacionais e gerenciar a conformidade dos recursos e o status da configuração em. AWS Systems Manager

Serviços relacionados

O myApplications usa os seguintes serviços:

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- Explorador de recursos da AWS
- AWS Security Hub
- Systems Manager
- AWS Service Catalog
- Tags

Acessar o myApplications

É possível acessar o myApplications pelo AWS Management Console selecionando myApplications na barra lateral esquerda.

Definição de preço

MyApplications on AWS é oferecido sem custo adicional. Não há tarifas de configuração nem compromissos antecipados. As cobranças de uso dos recursos e dos serviços subjacentes que o painel do myApplications resume ainda se aplicam às taxas publicadas para esses recursos.

Regiões compatíveis

MyApplications está disponível da seguinte Regiões da AWS forma:

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)

- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Osaka)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Paris)
- Europa (Estocolmo)
- América do Sul (São Paulo)

Regiões de adesão

Regiões de adesão não são habilitadas por padrão. É necessário habilitar manualmente essas regiões para usá-las com o myApplications. Para obter mais informações sobre Regiões da AWS, consulte Gerenciando Regiões da AWS. As seguintes regiões de ativação são compatíveis:

- Africa (Cape Town)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Europa (Milão)
- Europa (Espanha)
- Europa (Zurique)
- Oriente Médio (Barém)

- Oriente Médio (Emirados Árabes Unidos)
- Israel (Tel Aviv)

Conceitos básicos do myApplications

Para começar a criar, monitorar e gerenciar as aplicações no myApplications, siga as etapas a seguir.

Etapa 1: Criar um aplicativo do

Crie um novo aplicativo ou integre um AppRegistry aplicativo existente criado antes de 8 de novembro de 2023 para começar a usar o MyApplications.

Create an application

Para criar um aplicativo.

1. Faça login no AWS Management Console.
2. Na barra lateral esquerda, selecione myApplications.
3. Selecione Create application (Criar aplicativo).
4. Insira o nome de uma aplicação.
5. (Opcional) Insira uma descrição para a aplicação.
6. (Opcional) Adicione tags. Tags são pares de chave-valor aplicados a recursos para armazenar metadados sobre esses recursos.

> **Note**
>
> A tag do AWS aplicativo é aplicada automaticamente aos aplicativos recém-criados e pode ser usada para identificar recursos associados ao seu aplicativo. Para obter mais informações, consulte A tag do AWS aplicativo no Guia AWS Service Catalog AppRegistry do administrador.

7. (Opcional) Adicione grupos de atributos. É possível usar grupos de atributos para armazenar metadados da aplicação.
8. Selecione Next (Próximo).
9. (Opcional) Adicione recursos existentes:

> **Note**
>
> Para pesquisar e adicionar recursos, é necessário ativar Explorador de recursos da AWS. Para obter mais informações, consulte Introdução ao Explorador de recursos da AWS.
> Todos os recursos adicionados são marcados com a tag do AWS aplicativo.

a. Escolha Selecionar recursos.

b. (Opcional) Selecione uma visualização.

c. Procure os recursos. É possível pesquisar por palavra-chave, nome ou tipo, ou escolher um tipo de recurso.

> **Note**
>
> Se você não conseguir encontrar o recurso que está procurando, solucione o problema com Explorador de recursos da AWS. Para obter mais informações, consulte Solução de problemas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de Recursos.

d. Marque a caixa de seleção ao lado dos usuários que você deseja adicionar.

e. Escolha Adicionar.

f. Selecione Next (Próximo).

10. Revise as escolhas.

11. Se estiver associando uma AWS CloudFormation pilha, marque a caixa de seleção na parte inferior da página.

> **Note**
>
> Adicionar uma AWS CloudFormation pilha ao aplicativo requer uma atualização da pilha porque todos os recursos adicionados ao seu aplicativo são marcados com a tag do AWS aplicativo. As configurações manuais realizadas após a última atualização da pilha podem não ser refletidas após essa atualização. Isso pode causar tempo de inatividade ou outros problemas na aplicação. Para obter mais

informações, consulte Atualizar comportamentos de recursos de pilha no Guia do usuário do AWS CloudFormation .

12. Selecione Create application (Criar aplicativo).

Onboard existing application

Para integrar um aplicativo existente AppRegistry

1. Faça login no AWS Management Console.
2. Na barra lateral esquerda, selecione myApplications.
3. Use a barra de pesquisa para encontrar a aplicação.
4. Selecione a aplicação.
5. Selecione Integrar ***nome da aplicação***.
6. Se estiver associando uma CloudFormation pilha, marque a caixa de seleção na caixa de alerta.
7. Selecione Integrar aplicação.

Etapa 2: Visualizar aplicações

É possível visualizar as aplicações em todas as regiões ou em regiões específicas e as respectivas informações relevantes em uma visualização em cartão ou tabela.

Como visualizar aplicações

1. Na barra lateral esquerda, selecione myApplications.
2. Em Regiões, selecione Região atual ou Regiões compatíveis.
3. Para encontrar uma aplicação específica, insira o nome, palavras-chave ou a descrição na barra de pesquisa.
4. (Opcional) A visualização padrão é a visualização em cartão. Para personalizar a página da aplicação:
   a. Selecione o ícone de engrenagem.
   b. (Opcional) Selecione o tamanho da página.
   c. (Opcional) Selecione a visualização em cartão ou tabela.

d. (Opcional) Selecione o tamanho da página.
e. (Opcional) Se estiver usando a visualização em tabela, selecione as propriedades para ela.
f. (Opcional) Alterne quais propriedades da aplicação são visíveis e a ordem em que elas aparecem.
g. Selecione a opção Confirmar.

Gerenciar aplicações

Este tópico aborda como gerenciar as aplicações.

Editar aplicações

A edição do seu aplicativo é aberta AppRegistry para que você possa atualizar sua descrição. Você também pode usar AppRegistry para editar as tags e os grupos de atributos do seu aplicativo.

Como editar uma aplicação

1. Abra a AWS Management Console.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Selecione a aplicação que deseja editar.
4. No painel do myApplication, selecione Ações e, depois, Editar aplicação.
5. Em Editar descrição da aplicação, atualize a descrição e, depois, selecione Salvar alterações.

Como editar tags

- Siga as etapas em Gerenciamento de tags no Guia AWS Service Catalog AppRegistry do administrador.

Como editar grupos de atributos

- Siga as etapas em Edição de grupos de atributos no Guia AWS Service Catalog AppRegistry do administrador.

Excluir aplicações

É possível excluir aplicações, caso elas não sejam mais necessárias.

Como excluir uma aplicação

1. Abra a AWS Management Console.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Selecione a aplicação que você deseja excluir.
4. No painel do myApplications, selecione Ações.
5. Selecione Excluir aplicativo.
6. Escolha Excluir.
7. Confirme a exclusão e selecione Excluir aplicação.

Criar trechos de código

O myApplications cria trechos de código para todas as aplicações. É possível usar trechos de código para adicionar automaticamente recursos recém-criados a uma aplicação usando as ferramentas de Infraestrutura como código (IaC). Todos os recursos adicionados são marcados com a tag do AWS aplicativo para associá-la ao seu aplicativo.

Como criar um trecho de código para a aplicação

1. Abra a AWS Management Console.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Procure e selecione uma aplicação.
4. Escolha Ações.
5. Selecione Obter trecho de código.
6. Selecione um tipo de trecho de código.
7. Selecione Copiar para copiar o código para a área de transferência.
8. Cole o código na ferramenta de IaC.

Gerenciar recursos do

Este tópico aborda como gerenciar os recursos.

Adicionar recursos

Adicionar recursos às aplicações permite agrupá-los e gerenciar a segurança, a performance e a conformidade.

Como adicionar recursos

1. Abra a AWS Management Console.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Procure e selecione uma aplicação.
4. Selecione Gerenciar recursos.
5. Selecione Adicionar recursos.
6. (Opcional) Selecione uma visualização.
7. Procure os recursos. É possível pesquisar por palavra-chave, nome ou tipo, ou escolher um tipo de recurso.

   > **Note**
   >
   > Se você não conseguir encontrar o recurso que está procurando, solucione o problema com Explorador de recursos da AWS. Para obter mais informações, consulte Solução de problemas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de Recursos.

8. Marque a caixa de seleção ao lado dos usuários que você deseja adicionar.
9. Escolha Adicionar.

Remover recursos

É possível remover recursos para dissociá-los da aplicação.

Como remover recursos

1. Abra a AWS Management Console.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Procure e selecione uma aplicação.
4. Selecione Gerenciar recursos.

5. (Opcional) Selecione uma visualização.
6. Procure os recursos. É possível pesquisar por palavra-chave, nome ou tipo, ou escolher um tipo de recurso.

> **Note**
>
> Se você não conseguir encontrar o recurso que está procurando, solucione o problema com Explorador de recursos da AWS. Para obter mais informações, consulte Solução de problemas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de Recursos.

7. Escolha Remover.
8. Confirme que você deseja remover o recurso selecionando Remover recursos.

Painel do myApplications

Cada aplicação criada ou integrada tem o próprio painel do myApplications. O painel MyApplications contém widgets operacionais, de custo e de segurança que revelam insights de vários AWS serviços. Cada widget também pode ser adicionado aos favoritos, reordenado, removido ou redimensionado. Para ter mais informações, consulte Trabalhar com widgets.

Widget de configuração do painel da aplicação

Esse widget contém uma lista de atividades de introdução sugeridas que você pode usar para ajudá-lo a configurar o Serviços da AWS gerenciamento de recursos do aplicativo.

Widget de resumo da aplicação

Esse widget mostra o nome, a descrição e a tag de aplicação da AWS da aplicação. É possível acessar e copiar a tag de aplicação em Infraestrutura como código (IAC) para marcar manualmente os recursos.

Widget de computação

Esse widget exibe informações e métricas dos recursos computacionais que você adiciona à aplicação. Isso inclui o total de alarmes e o total de tipos de recursos computacionais. O widget também mostra gráficos de tendências de métricas de desempenho de recursos Amazon CloudWatch para a utilização da CPU da instância Amazon EC2 e invocações do Lambda.

Configurar o widget de computação

Para preencher dados no widget de computação, configure pelo menos uma instância do Amazon EC2 ou uma função do Lambda para a aplicação. Para obter mais informações, consulte a documentação do Amazon Elastic Compute Cloud e Conceitos básicos do Lambda no Guia do desenvolvedor do AWS Lambda .

Widget de custo e uso

Esse widget mostra dados de AWS custo e uso dos recursos do seu aplicativo. É possível usar esses dados para comparar os custos mensais e visualizar os detalhamentos dos custos por AWS service (Serviço da AWS). Esse widget resume apenas os custos dos recursos marcados com a tag do AWS aplicativo, excluindo impostos, taxas e outros custos compartilhados não diretamente associados a um recurso. Os custos mostrados não são combinados e são atualizados pelo menos uma vez a cada 24 horas. Para obter mais informações, consulte Analyzing your costs with Explorador de recursos da AWS no Guia do usuário do AWS Cost Management .

Configurar o widget de custo e uso

Para configurar o widget Custo e uso, habilite AWS Cost Explorer Service para seu aplicativo e sua conta. Esse serviço é oferecido sem custo adicional e não há taxas de instalação nem compromisso antecipado. Para obter mais informações, consulte Ativar o Cost Explorer no Guia do usuário do AWS Cost Management .

AWS Widget de segurança

Esse widget exibe as descobertas de segurança de AWS Segurança para seu aplicativo. AWS A segurança fornece uma visão abrangente das descobertas de segurança de seu aplicativo em AWS. É possível acessar descobertas prioritárias recentes por gravidade, monitorar o procedimento de segurança, acessar descobertas recentes críticas ou de alta gravidade e obter informações sobre as próximas etapas. Para ter mais informações, consulte AWS Security Hub.

Configurando o widget de AWS segurança

Para configurar o widget de AWS segurança, configure AWS Security Hub seu aplicativo e sua conta. Para obter mais informações, consulte O que é AWS Security Hub? no Guia do AWS Security Hub usuário. Para obter informações sobre preços, consulte Avaliação gratuita, uso e preços do AWS Security Hub no Guia do usuário do AWS Security Hub .

AWS Security Hub requer que você configure o AWS Config Recording. Esse serviço fornece uma visão detalhada dos recursos associados à sua AWS conta. Para obter mais informações, consulte AWS Systems Manager no Guia de Usuário AWS Systems Manager .

DevOps widget

Esse widget mostra informações operacionais para que você possa avaliar a conformidade e tomar medidas para a aplicação. Esses insights incluem:

- Gerenciamento de frota
- Gerenciamento de estados
- Gerenciamento de patches
- Configuração e OpsItems gerenciamento

Configurando o widget DevOps

Para configurar o DevOps widget, habilite-o AWS Systems Manager OpsCenter para seu aplicativo e conta. Para obter mais informações, consulte Introdução ao Systems Manager Explorer e OpsCenter no Guia AWS Systems Manager do Usuário. A ativação OpsCenter permite configurar AWS Config e AWS Systems Manager Explorer fazer com Amazon CloudWatch que seus eventos sejam criados automaticamente OpsItems com base em regras e eventos comumente usados. Para obter mais informações, consulte Configuração OpsCenter no Guia do AWS Systems Manager usuário.

É possível configurar as instâncias para que os agentes do Systems Manager executem e apliquem permissões para permitir a verificação de patches. Para obter mais informações, consulte AWS Systems Manager Quick Setup no Guia do usuário do AWS Systems Manager .

Você também pode configurar a correção automática de instâncias do Amazon EC2 para seu aplicativo AWS Systems Manager configurando o Patch Manager. Para obter mais informações, consulte Usar políticas de patch da Quick Setup no Guia do usuário do AWS Systems Manager .

Para obter informações sobre preços, consulte AWS Systems Manager preços.

Widget de monitoramento e operações

Esse widget mostra:

- Alarmes e alertas referentes aos recursos associados à aplicação

- Objetivos de nível de serviço (SLOs) e métricas da aplicação
- Métricas AWS de sinais de aplicativos disponíveis

Configurar o widget de monitoramento e operações

Para configurar o widget de monitoramento e operações, crie CloudWatch alarmes e canários em sua conta. AWS Para obter mais informações, consulte Como usar CloudWatch alarmes da Amazon e Criar um canário no Guia CloudWatch do usuário da Amazon. Para preços de CloudWatch alarmes e canários sintéticos, consulte os CloudWatch preços da Amazon e o blog de operações e migrações AWS na nuvem, respectivamente.

Para obter mais informações sobre sinais de CloudWatch aplicativos, consulte Habilitar insights de CloudWatch aplicativos da Amazon no Guia CloudWatch do usuário da Amazon.

Widget de tags

Esse widget exibe todas as tags associadas à aplicação. É possível usar esse widget para monitorar e gerenciar os metadados da aplicação (criticidade, ambiente, centro de custos). Para obter mais informações, consulte O que são tags? no AWS whitepaper sobre as melhores práticas para a marcação de AWS recursos.

AWS Management Console Acesso privado

AWS Management Console O Acesso Privado é um recurso de segurança avançado para controlar o acesso ao AWS Management Console. AWS Management Console O acesso privado é útil quando você deseja impedir que os usuários entrem Contas da AWS de forma inesperada na sua rede. Com esse recurso, você pode limitar o acesso AWS Management Console somente a um conjunto específico de dados conhecidos Contas da AWS quando o tráfego se origina de dentro da sua rede.

Tópicos

Compatível Regiões da AWS, consoles de serviço e recursos

AWS Management Console O acesso privado oferece suporte somente a um subconjunto de regiões e AWS serviços. Os consoles de serviço não compatíveis ficarão inativos no AWS Management Console. Além disso, alguns AWS Management Console recursos podem ser desativados ao usar o Acesso AWS Management Console Privado, por exemplo, a seleção da Região Padrão nas Configurações Unificadas.

As seguintes regiões e consoles de serviço são compatíveis.

Regiões compatíveis

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Hyderabad)

- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Seul)
- Asia Pacific (Osaka)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Paris)
- Europa (Estocolmo)
- América do Sul (São Paulo)
- Africa (Cape Town)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Oeste do Canadá (Calgary)
- Europa (Milão)
- Europa (Espanha)
- Europa (Zurique)
- Oriente Médio (Barém)
- Oriente Médio (Emirados Árabes Unidos)
- Israel (Tel Aviv)

Consoles de serviço compatíveis

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service

- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Amazon EMR

- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service for Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Recomendações Estratégicas do AWS Migration Hub
- Amazon MQ
- Analisador de Acesso à Rede
- AWS Network Manager
- OpenSearch Serviço Amazon
- AWS Organizations
- Amazon S3 on Outposts
- Amazon SageMaker Runtime

- Dados SageMaker sintéticos da Amazon
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Configurações unificadas
- IP Address Manager da Amazon VPC

Visão geral dos controles de segurança de acesso AWS Management Console privado

Restrições de conta no AWS Management Console pela rede

AWS Management Console O acesso privado é útil em cenários em que você deseja limitar o acesso ao AWS Management Console da sua rede somente a um conjunto específico de conhecidos Contas da AWS em sua organização. Ao fazer isso, é possível impedir que os usuários façam login em Contas da AWS inesperadas de dentro da sua rede. É possível implementar esses controles usando a política de endpoint da VPC do AWS Management Console . Para ter mais informações, consulte Implementação de políticas de controle de serviços e políticas de endpoint da VPC.

Conectividade da sua rede com a internet

A conectividade com a Internet da sua rede ainda é necessária para acessar os ativos usados pelo AWS Management Console, como conteúdo estático (CSSJavaScript, imagens), e todos Serviços da AWS não habilitados pelo AWS PrivateLink. Para obter uma lista dos domínios de nível superior usados pelo AWS Management Console, consulte. Solução de problemas

> **Note**
>
> Atualmente, o AWS Management Console Private Access não oferece suporte a endpoints como `status.aws.amazon.comhealth.aws.amazon.com`, e. `docs.aws.amazon.com` Você precisará direcionar esses domínios para a internet pública.

Endpoints da VPC e configuração de DNS necessários

AWS Management Console O acesso privado exige os dois VPC endpoints a seguir por região. Substitua *`região`* pelas informações da sua própria região.

1. com.amazonaws. *`region`* .console para AWS Management Console
2. com.amazonaws. *`região`* .signin para Início de Sessão da AWS

> **Note**
>
> Sempre provisione infraestrutura e conectividade de rede à região Leste dos EUA (Norte da Virgínia) (us-east-1), independentemente de outras regiões usadas com o AWS Management Console. É possível usar o AWS Transit Gateway para configurar a conectividade entre o Leste dos EUA (Norte da Virgínia) e todas as outras regiões. Para obter mais informações sobre como usar os gateways de trânsito da VPC, consulte Conceitos básicos dos gateways de trânsito no Guia de gateways de trânsito do Amazon VPC. Você também pode usar o emparelhamento do Amazon VPC. Para obter mais informações, consulte O que é emparelhamento de VPC? no Guia de emparelhamento do Amazon VPC. Para comparar essas opções, consulte Opções de conectividade de Amazon VPC para Amazon VPC no Whitepaper de opções de conectividade do Amazon Virtual Private Cloud.

DNSconfiguração para AWS Management Console e Início de Sessão da AWS

Para rotear o tráfego de rede para os respectivos endpoints da VPC, configure registros DNS na rede pela qual os usuários acessarão o AWS Management Console. Esses registros DNS direcionarão o tráfego do navegador dos usuários para os endpoints da VPC que você criou.

É possível criar uma única zona hospedada. No entanto, endpoints como `health.aws.amazon.com` e `docs.aws.amazon.com` não estarão acessíveis porque eles não têm endpoints da VPC. Você precisará direcionar esses domínios para a internet pública. Recomendamos criar duas zonas hospedadas privadas por região, uma para `signin.aws.amazon.com` e outra para `console.aws.amazon.com` com os seguintes registros de CNAME:

- Registros CNAME regionais (em todas as regiões)
- region.signin.aws.amazon.com apontando para o VPC endpoint na zona de login Início de Sessão da AWS DNS
- region.console.aws.amazon.com apontando para o VPC endpoint na zona do console AWS Management Console DNS
- Registros CNAME sem região apenas para a região Leste dos EUA (Norte da Virgínia). Sempre é necessário configurar a região Leste dos EUA (Norte da Virgínia).
  - signin.aws.amazon.com apontando para o Início de Sessão da AWS VPC endpoint no Leste dos EUA (Norte da Virgínia) (us-east-1)
  - console.aws.amazon.com apontando para o AWS Management Console VPC endpoint no Leste dos EUA (Norte da Virgínia) (us-east-1)

Para obter instruções de como criar um registro CNAME, consulte Trabalhar com registros no Guia do desenvolvedor do Amazon Route 53.

Alguns AWS consoles, incluindo o Amazon S3, usam padrões diferentes para DNS seus nomes. Veja os dois exemplos a seguir:

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

Para poder direcionar esse tráfego para seu AWS Management Console VPC endpoint, você precisa adicionar esses nomes individualmente. Recomendamos que você configure o roteamento de todos os endpoints para oferecer uma experiência totalmente privada. No entanto, isso não é necessário para usar o Acesso AWS Management Console Privado.

Os `json` arquivos a seguir contêm a lista completa de AWS service (Serviço da AWS) s e endpoints de console a serem configurados por região. Use o campo `PrivateIpv4DnsNames` abaixo do endpoint `com.amazonaws.`*`region`*`.console` para os nomes de DNS.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> Essa lista é atualizada a cada mês à medida que adicionamos mais endpoints ao escopo do Acesso Privado do AWS Management Console . Para manter as zonas hospedadas privadas atualizadas, extraia periodicamente a lista de arquivos anterior.

Se você usa o Route 53 para configurar o DNS, acesse https://console.aws.amazon.com/route53/v2/hostedzones# para verificar a configuração de DNS. Para cada zona hospedada privada no Route 53, verifique se os conjuntos de registros a seguir estão presentes.

- console.aws.amazon.com
- signin.aws.amazon.com
- region.console.aws.amazon.com
- region.signin.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com
- Registros adicionais presentes nos arquivos JSON listados anteriormente

Endpoints de VPC e DNS configuração para serviços AWS

As AWS Management Console chamadas são feitas Serviços da AWS por meio de uma combinação de solicitações diretas do navegador e solicitações que são enviadas por proxy por servidores da web. Para direcionar esse tráfego para seu AWS Management Console VPC endpoint, você deve adicionar o VPC endpoint e configurá-lo para cada serviço dependente. DNS AWS

Os json arquivos a seguir AWS PrivateLink listam os arquivos suportados Serviços da AWS que estão disponíveis para você usar. Se um serviço não se integrar ao AWS PrivateLink, ele não será incluído nesses arquivos.

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

Use o campo `ServiceName` do endpoint da VPC do serviço correspondente para adicionar à VPC.

> **Note**
>
> Atualizamos essa lista todos os meses à medida que adicionamos suporte para acesso AWS Management Console privado a mais consoles de serviço. Para se manter atualizado, extraia periodicamente a lista de arquivos anterior e atualize os endpoints da VPC.

Implementação de políticas de controle de serviços e políticas de endpoint da VPC

Você pode usar políticas de controle de serviço (SCPs) e políticas de VPC endpoint para acesso privado AWS Management Console para limitar o conjunto de contas que têm permissão para AWS Management Console usá-las de dentro de sua VPC e de suas redes locais conectadas.

Usando o acesso AWS Management Console privado com políticas AWS Organizations de controle de serviços

Se sua AWS organização estiver usando uma política de controle de serviços (SCP) que permite serviços específicos, você deve adicionar `signin:*` às ações permitidas. Essa permissão é necessária porque o login em um endpoint VPC AWS Management Console de acesso privado executa uma autorização do IAM que o SCP bloqueia sem a permissão. Como exemplo, a política de controle de serviços a seguir permite que o Amazon EC2 e CloudWatch os serviços sejam usados na organização, inclusive quando eles são acessados usando um endpoint de acesso AWS Management Console privado.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

Para ter mais informações sobre SCPs, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .

Permitir o AWS Management Console uso somente para contas e organizações esperadas (identidades confiáveis)

AWS Management Console e Início de Sessão da AWS ofereça suporte a uma política de VPC endpoint que controla especificamente a identidade da conta conectada.

Ao contrário de outras políticas de endpoint da VPC, a política é avaliada antes da autenticação. Como resultado, ele controla especificamente o login e o uso somente da sessão autenticada, e não as ações AWS específicas do serviço que a sessão realiza. Por exemplo, quando a sessão acessa um console de AWS serviço, como o console do Amazon EC2, essas políticas de VPC endpoint não serão avaliadas em relação às ações do Amazon EC2 que são tomadas para exibir essa página. Em vez disso, você pode usar as políticas do IAM associadas ao IAM Principal conectado para controlar sua permissão para AWS ações de serviço.

> **Note**
>
> As políticas de VPC endpoints para e AWS Management Console SignIn VPC endpoints oferecem suporte apenas a um subconjunto limitado de formulações de políticas. Cada `Principal` e `Resource` deve ser definido como `*` e `Action` deve ser `*` ou `signin:*`. Você controla o acesso aos endpoints da VPC usando as chaves de condição `aws:PrincipalOrgId` e `aws:PrincipalAccount`.

As políticas a seguir são recomendadas para os endpoints do console e da SignIn VPC.

Essa política de VPC endpoint permite o login na AWS organização especificada e bloqueia o login Contas da AWS em qualquer outra conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

Essa política de VPC endpoint limita o login a uma lista específica Contas da AWS e bloqueia o login em qualquer outra conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

As políticas que limitam Contas da AWS nossa organização nos endpoints VPC de login AWS Management Console e login são avaliadas no momento do login e são reavaliadas periodicamente para as sessões existentes.

Implementar políticas baseadas em identidade e outros tipos de políticas

Você gerencia o acesso AWS criando políticas e anexando-as às identidades do IAM (usuários, grupos de usuários ou funções) ou AWS recursos. Esta página descreve como as políticas funcionam quando usadas em conjunto com o Acesso AWS Management Console Privado.

Chaves de contexto de condição AWS global suportadas

AWS Management Console O acesso privado não oferece suporte `aws:SourceVpce` a chaves de contexto de condição `aws:VpcSourceIp` AWS global. Em vez disso, é possível usar a condição `aws:SourceVpc` do IAM nas políticas ao utilizar o Acesso Privado ao AWS Management Console .

Como o AWS Management Console Private Access funciona com a AWS: SourceVpc

Esta seção descreve os vários caminhos de rede que as solicitações geradas por você AWS Management Console podem seguir Serviços da AWS. Em geral, os consoles de AWS serviço são implementados com uma combinação de solicitações diretas do navegador e solicitações enviadas por proxy pelos servidores da AWS Management Console web para. Serviços da AWS Essas implementações estão sujeitas a alterações sem aviso prévio. Se seus requisitos de segurança incluírem acesso ao Serviços da AWS uso de VPC endpoints, recomendamos que você configure VPC endpoints para todos os serviços que você pretende usar da VPC, seja diretamente ou por meio de acesso privado. AWS Management Console Além disso, você deve usar a condição `aws:SourceVpc` do IAM em suas políticas em vez de `aws:SourceVpce` valores específicos com o recurso de acesso AWS Management Console privado. Esta seção fornece detalhes sobre como os diferentes caminhos de rede funcionam.

Depois que um usuário faz login no AWS Management Console, ele faz solicitações Serviços da AWS por meio de uma combinação de solicitações diretas do navegador e solicitações que são enviadas por proxy de servidores AWS Management Console web para AWS servidores. Por exemplo, as solicitações de dados CloudWatch gráficos são feitas diretamente do navegador. Já algumas solicitações do console de AWS serviço, como o Amazon S3, são enviadas por proxy pelo servidor web para o Amazon S3.

Para solicitações diretas do navegador, usar o Acesso AWS Management Console Privado não muda nada. Como antes, a solicitação chega ao serviço por meio de qualquer caminho de rede que a VPC tenha configurado para alcançar monitoring.region.amazonaws.com. Se a VPC estiver configurada com um VPC endpoint paracom.amazonaws.region.monitoring, a solicitação chegará por meio CloudWatch desse VPC endpoint. CloudWatch Se não houver um VPC endpoint para CloudWatch, a solicitação chegará CloudWatch ao seu endpoint público, por meio de um Internet Gateway na VPC. As solicitações recebidas CloudWatch por meio do CloudWatch VPC endpoint terão as condições do IAM `aws:SourceVpc` e serão `aws:SourceVpce` definidas com seus respectivos valores. Aqueles que CloudWatch acessarem seu endpoint público terão `aws:SourceIp` definido o endereço IP de origem da solicitação. Para obter mais informações sobre essas chaves de condição do IAM, consulte Chaves de condição globais no Guia do usuário do IAM.

Para solicitações que são enviadas por proxy pelo servidor AWS Management Console web, como a solicitação que o console do Amazon S3 faz para listar seus buckets quando você visita o console do Amazon S3, o caminho da rede é diferente. Essas solicitações não são iniciadas pela VPC e, portanto, não usam o endpoint da VPC que você pode ter configurado na VPC para esse serviço.

Mesmo que você tenha um endpoint da VPC para o Amazon S3 nesse caso, a solicitação da sessão ao Amazon S3 para listar os buckets não usa o endpoint da VPC do Amazon S3. No entanto, quando você usa o acesso AWS Management Console privado com serviços compatíveis, essas solicitações (por exemplo, para o Amazon S3) incluirão a chave de `aws:SourceVpc` condição no contexto da solicitação. A chave de `aws:SourceVpc` condição será definida como a ID da VPC em que seus endpoints de acesso AWS Management Console privado para login e console são implantados. Portanto, se você estiver usando restrições `aws:SourceVpc` nas políticas baseadas em identidade, deverá adicionar o ID dessa VPC que hospeda os endpoints de login e console do Acesso Privado ao AWS Management Console . A condição `aws:SourceVpce` será definida para os respectivos IDs de endpoint da VPC de login ou console.

> **Note**
>
> Se os usuários precisarem acessar os consoles de serviço que não são compatíveis com o Acesso Privado ao AWS Management Console , você deverá incluir uma lista dos endereços de rede pública esperados (como o intervalo de rede on-premises) usando a chave de condição `aws:SourceIP` nas políticas baseadas na identidade dos usuários.

Como os diferentes caminhos de rede são refletidos em CloudTrail

Os diferentes caminhos de rede usados pelas solicitações geradas por você AWS Management Console são refletidos no histórico de CloudTrail eventos.

Para solicitações diretas do navegador, usar o Acesso AWS Management Console Privado não muda nada. CloudTrail os eventos incluirão detalhes sobre a conexão, como o ID do VPC endpoint que foi usado para fazer a chamada da API de serviço.

Para solicitações que são enviadas por proxy pelo servidor AWS Management Console web, os CloudTrail eventos não incluirão detalhes relacionados à VPC. No entanto, Início de Sessão da AWS as solicitações iniciais para estabelecer a sessão do navegador, como o tipo de `AwsConsoleSignIn` evento, incluirão o ID do Início de Sessão da AWS VPC endpoint nos detalhes do evento.

Experimente o acesso AWS Management Console privado

Esta seção descreve como configurar e testar o Acesso AWS Management Console Privado em uma nova conta.

AWS Management Console O acesso privado é um recurso de segurança avançado e requer conhecimento prévio sobre redes e configuração de VPCs. Este tópico descreve como você pode experimentar o Acesso Privado ao AWS Management Console sem uma infraestrutura em escala completa.

Tópicos

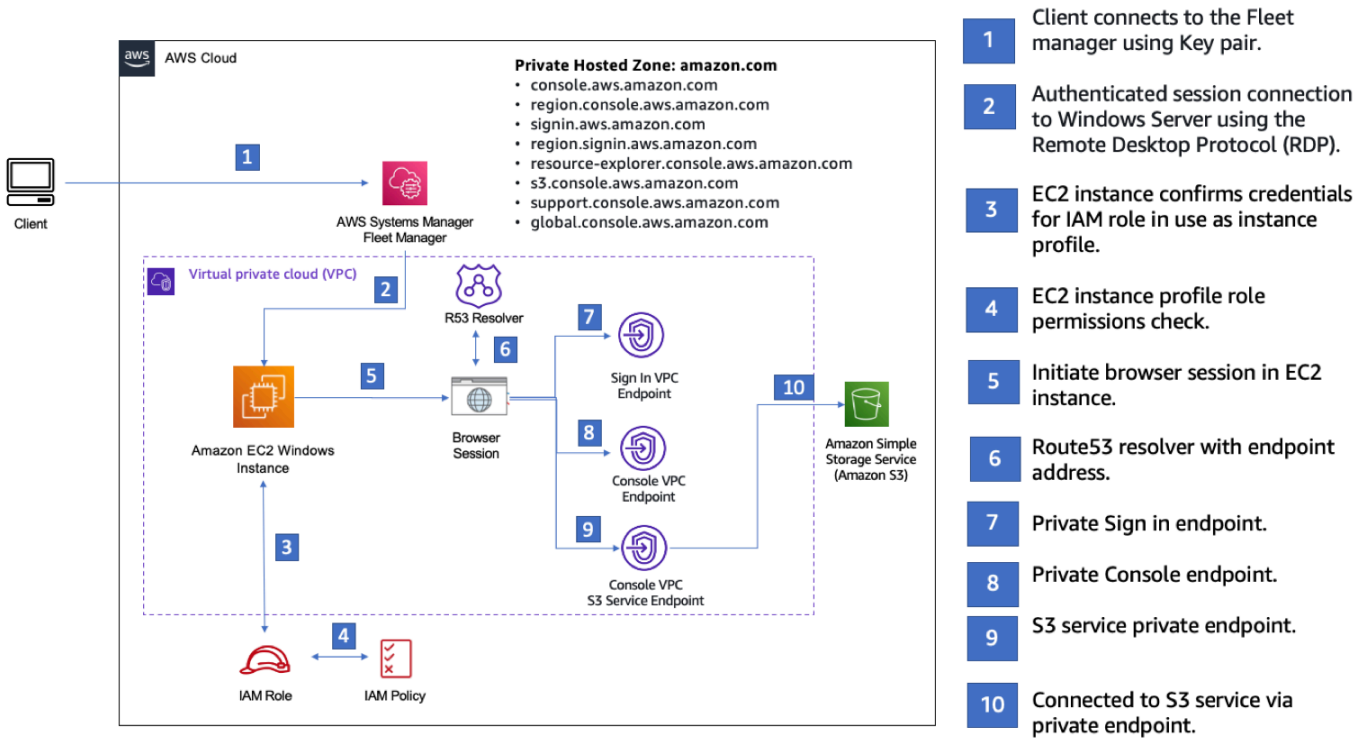
- Configuração de teste com o Amazon EC2
- Configuração de teste com a Amazon WorkSpaces
- Testar a configuração da VPC com políticas do IAM

Configuração de teste com o Amazon EC2

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação escalável na Nuvem Amazon Web Services. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento. Nessa configuração, usamos o Fleet Manager, um recurso do AWS Systems Manager, para estabelecer uma conexão com uma instância do Windows do Amazon EC2 usando o Remote Desktop Protocol (RDP).

Este guia demonstra um ambiente de teste para configurar e experimentar uma conexão de acesso AWS Management Console privado ao Amazon Simple Storage Service a partir de uma instância do Amazon EC2. Este tutorial é usado AWS CloudFormation para criar e configurar a configuração de rede a ser usada pelo Amazon EC2 para visualizar esse recurso.

O diagrama a seguir descreve o fluxo de trabalho para acessar uma configuração do Acesso Privado ao AWS Management Console por meio do Amazon EC2. Mostra como um usuário está conectado ao Amazon S3 usando um endpoint privado.



Copie o AWS CloudFormation modelo a seguir e salve-o em um arquivo que você usará na etapa três do procedimento Para configurar uma rede.

> **Note**
>
> Este AWS CloudFormation modelo usa configurações que atualmente não são suportadas na região de Israel (Tel Aviv).

AWS Management Console Modelo do Amazon AWS CloudFormation EC2 para ambiente de acesso privado

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC
```

```
  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.medium'


Resources:
```

```
#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 2
```

```
        - Fn::GetAZs: ""

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment
```

```
  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
```

```
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock
```

```
  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
```

```
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC
```

```
#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
          -
            Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

  Ec2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
       - !Ref Ec2InstanceRole

  EC2WinInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestWindowsAmiId
      IamInstanceProfile: !Ref Ec2InstanceProfile
      KeyName: !Ref Ec2KeyPair
      InstanceType:
        Ref: InstanceTypeParameter
      SubnetId: !Ref PrivateSubnetA
      SecurityGroupIds:
        - Ref: EC2SecurityGroup
      BlockDeviceMappings:
        - DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
      Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```

Para configurar uma rede

1. Faça login na conta de gerenciamento da organização e abra o console do AWS CloudFormation.
2. Selecione Criar pilha.

3. Escolha With new resources (standard) (Com novos recursos [padrão]). Faça upload do arquivo de AWS CloudFormation modelo que você criou anteriormente e escolha Avançar.
4. Insira um nome para a pilha, por exemplo **`PrivateConsoleNetworkForS3`**, e escolha Próximo.
5. Em VPC e sub-redes, insira os intervalos CIDR de IP de sua preferência ou use os valores padrão fornecidos. Se você usar os valores padrão, verifique se eles não se sobrepõem aos recursos de VPC existentes no seu. Conta da AWS
6. Para o KeyPair parâmetro Ec2, selecione um dos pares de chaves existentes do Amazon EC2 em sua conta. Se você ainda não tiver um par de chaves do Amazon EC2, deverá criar um antes de passar para a próxima etapa. Para obter mais informações, consulte Criar um par de chaves usando o Amazon EC2 no Guia do usuário do Amazon EC2.
7. Selecione Criar pilha.
8. Depois que a pilha for criada, escolha a guia Recursos para ver os recursos que foram criados.

Para se conectar à instância do Amazon EC2

1. Faça login na conta de gerenciamento da organização e abra o console do Amazon EC2.
2. No painel de navegação, escolha Instâncias.
3. Na página Instâncias, selecione a instância de teste do Console VPCE que foi criada pelo AWS CloudFormation modelo. Depois, escolha Conectar.

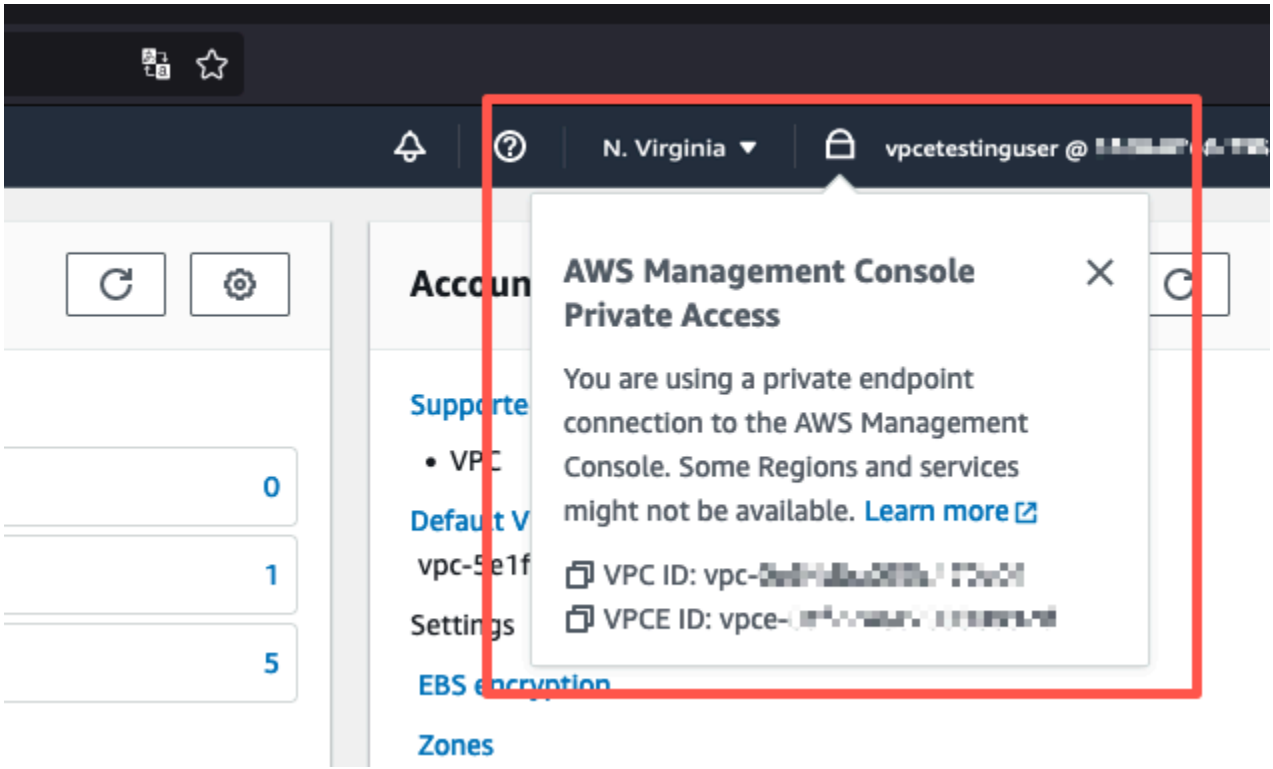
> **Note**
>
> Este exemplo usa o Fleet Manager, um recurso do AWS Systems Manager Explorer, para se conectar ao seu Windows Server. Pode levar alguns minutos até a conexão ser iniciada.

4. Na página Conectar-se à instância, escolha Cliente RDP e Conectar-se usando o Fleet Manager.
5. Escolha Fleet Manager: área de trabalho remota.
6. Para obter a senha administrativa para a instância do Amazon EC2 e acessar o Windows Desktop usando a interface web, use a chave privada associada ao par de chaves do Amazon EC2 que você usou ao AWS CloudFormation criar o modelo.
7. Na instância Windows do Amazon EC2, abra o AWS Management Console no navegador.

8. Depois de fazer login com suas AWS credenciais, abra o console do Amazon S3 e verifique se você está conectado AWS Management Console usando o Private Access.

Para testar a configuração do Acesso AWS Management Console Privado

1. Faça login na conta de gerenciamento da organização e abra o console do Amazon S3.
2. Selecione o ícone de cadeado na barra de navegação para ver o endpoint da VPC em uso. A captura de tela a seguir mostra a localização do ícone de cadeado e as informações da VPC.



Configuração de teste com a Amazon WorkSpaces

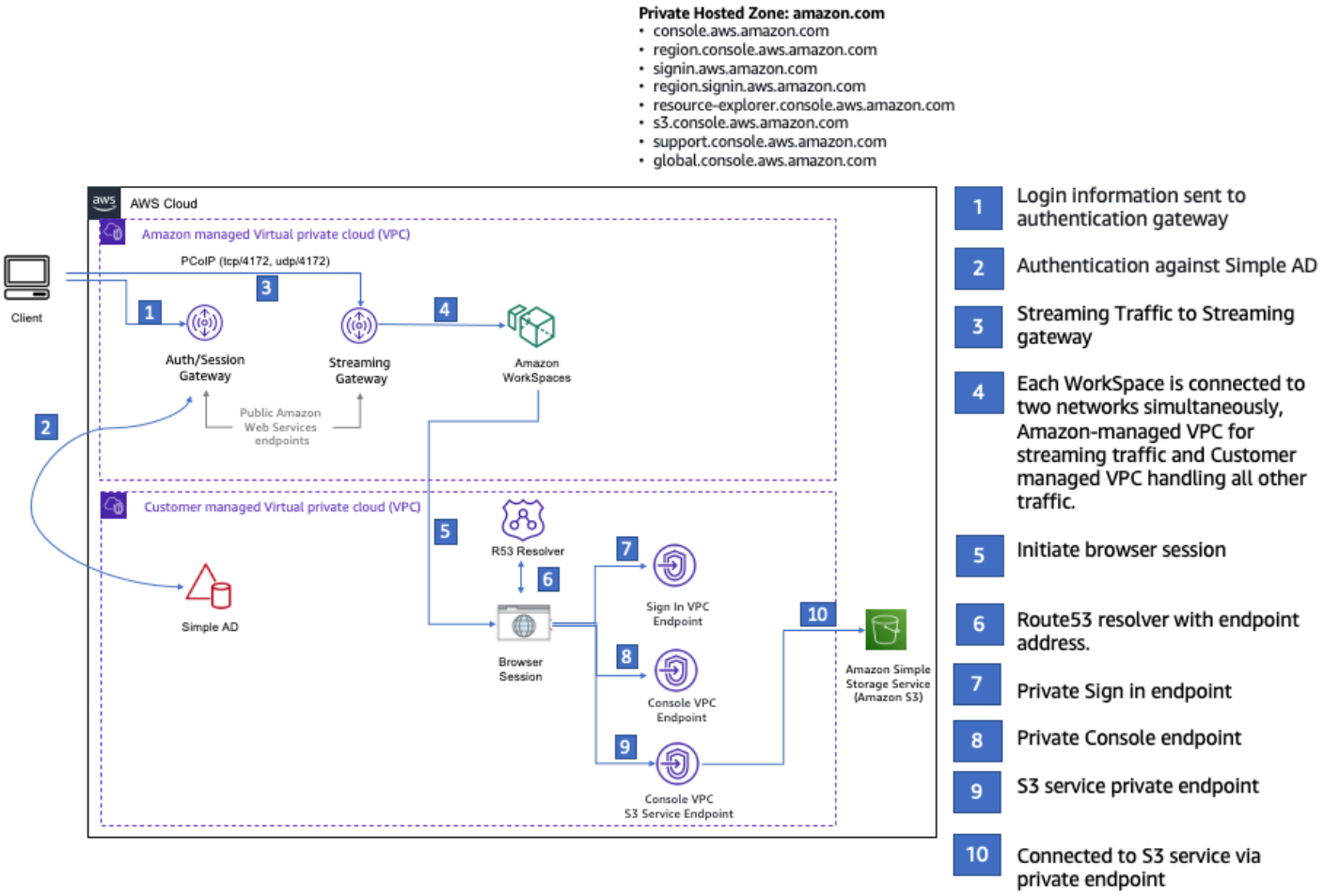
A Amazon WorkSpaces permite que você provisione desktops virtuais baseados em nuvem Windows, Amazon Linux ou Ubuntu Linux para seus usuários, conhecidos como. WorkSpaces Você pode rapidamente adicionar ou remover usuários à medida que suas necessidades mudarem. Os usuários podem acessar suas áreas de trabalho virtuais de vários dispositivos ou navegadores da web. Para saber mais sobre isso WorkSpaces, consulte o Guia de WorkSpaces administração da Amazon.

O exemplo nesta seção descreve um ambiente de teste no qual um ambiente de usuário usa um navegador da Web em execução em um WorkSpace para entrar no AWS Management Console

Private Access. Depois, o usuário acessa o console do Amazon Simple Storage Service. WorkSpace O objetivo é simular a experiência de um usuário corporativo com um laptop em uma rede conectada ao VPC, acessando o pelo AWS Management Console navegador.

Este tutorial é usado AWS CloudFormation para criar e configurar a configuração de rede e um Active Directory simples a ser usado, WorkSpaces juntamente com instruções passo a passo para configurar um WorkSpace usando AWS Management Console o.

O diagrama a seguir descreve o fluxo de trabalho para usar um WorkSpace para testar uma configuração de acesso AWS Management Console privado. Mostra a relação entre um cliente WorkSpace, uma VPC gerenciada pela Amazon e uma VPC gerenciada pelo cliente.



Copie o AWS CloudFormation modelo a seguir e salve-o em um arquivo que você usará na etapa 3 do procedimento para configurar uma rede.

AWS Management ConsoleAWS CloudFormation Modelo de ambiente de acesso privado

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
```

```
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
```

```
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
```

```
                zoneId_to_zoneName(event, context)
            else:
                no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

##########################
# Route Tables
##########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
```

```
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
```

```
# SECURITY GROUPS
#########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
```

```
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleS3ProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 's3.console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

##########################
```

```
# WORKSPACE RESOURCES
########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC


Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory
```

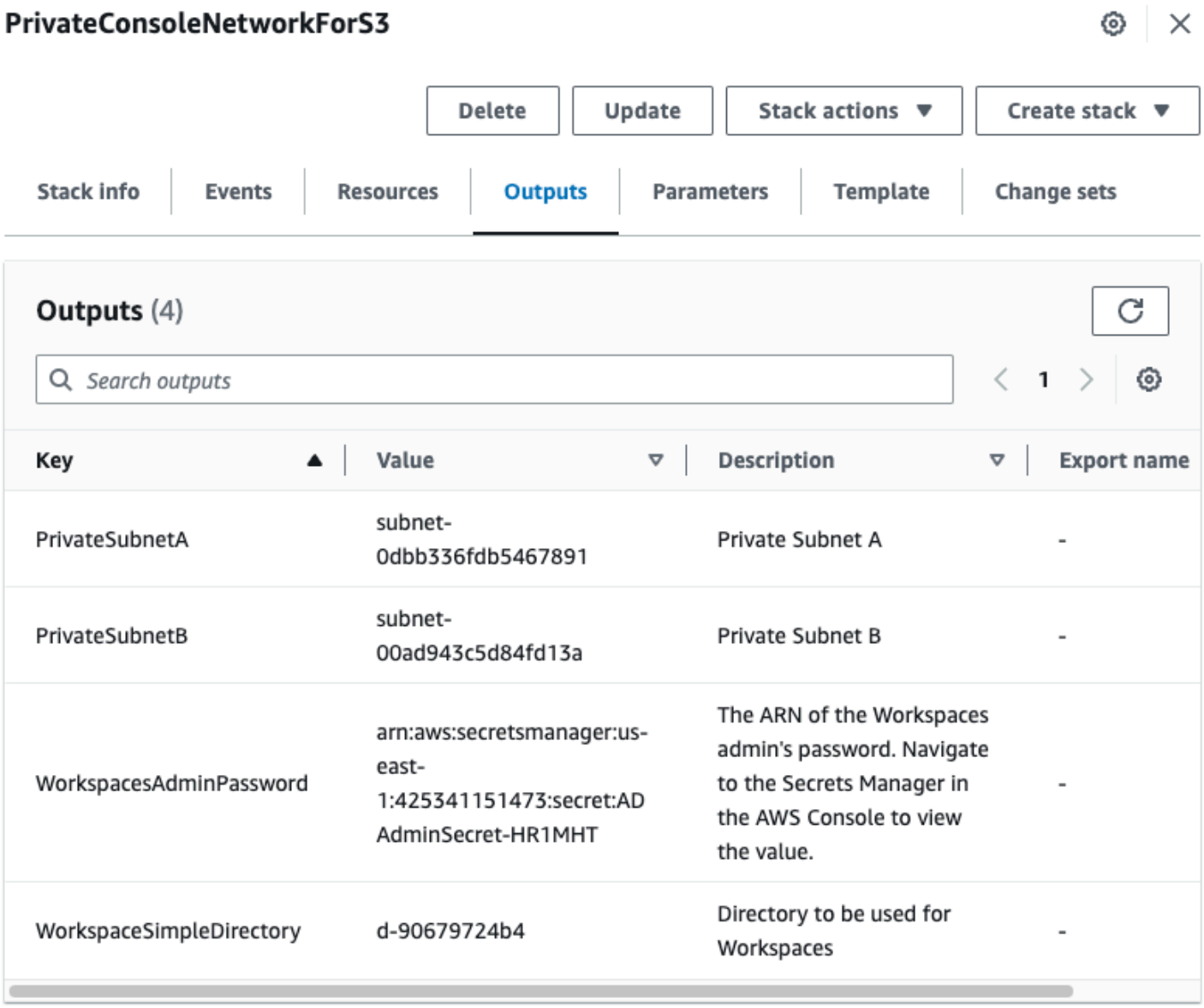
```
  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **Note**
>
> Essa configuração de teste foi projetada para ser executada na região Leste dos EUA (Norte da Virgínia) (us-east-1).

Para configurar uma rede

1. Faça login na conta de gerenciamento da organização e abra o console do AWS CloudFormation.
2. Selecione Criar pilha.
3. Escolha With new resources (standard) (Com novos recursos [padrão]). Faça upload do arquivo de AWS CloudFormation modelo que você criou anteriormente e escolha Avançar.
4. Insira um nome para a pilha, por exemplo **`PrivateConsoleNetworkForS3`**, e escolha Próximo.
5. Em VPC e sub-redes, insira os intervalos CIDR de IP de sua preferência ou use os valores padrão fornecidos. Se você usar os valores padrão, verifique se eles não se sobrepõem aos recursos de VPC existentes no seu. Conta da AWS
6. Selecione Criar pilha.
7. Depois que a pilha for criada, escolha a guia Recursos para ver os recursos que foram criados.
8. Escolha a guia Saídas para visualizar os valores das sub-redes privadas e do Workspace Simple Directory. Anote esses valores, pois você os usará na etapa quatro do próximo procedimento para criar e configurar um WorkSpace.

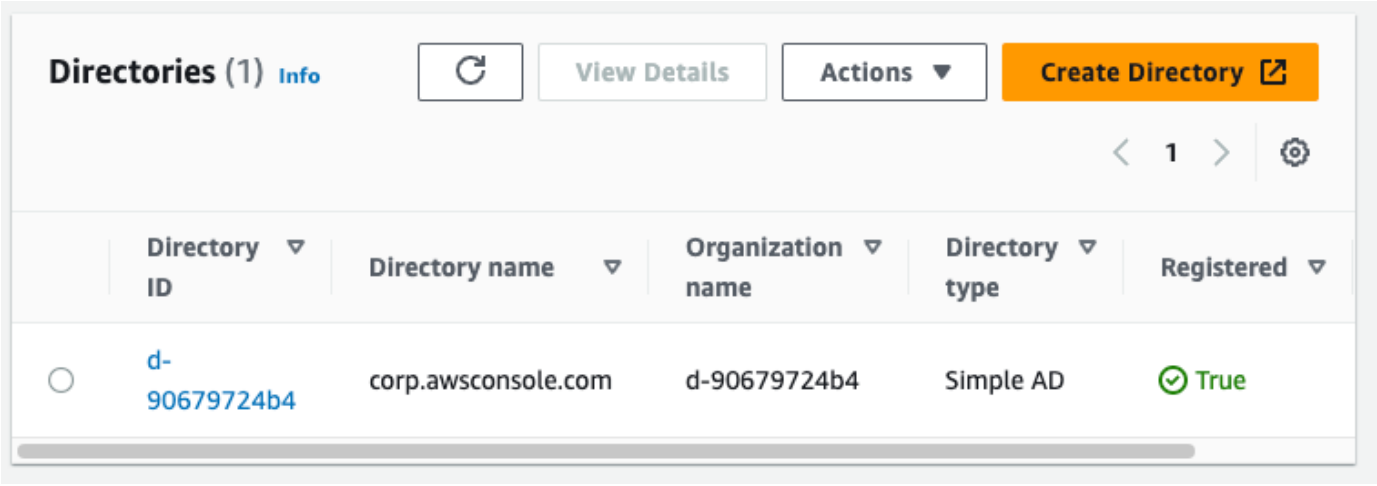
A captura de tela a seguir mostra a visualização da guia Saídas exibindo os valores das sub-redes privadas e do Workspace Simple Directory.



Agora que você criou sua rede, use os procedimentos a seguir para criar e acessar um WorkSpace.

Para criar um WorkSpace

1. Abra o console de WorkSpaces .
2. No painel de navegação, selecionar Diretórios.
3. Na página Diretórios, verifique se o status do diretório é Ativo. A captura de tela a seguir mostra uma página de Diretórios com um diretório ativo.



4. Para usar um diretório em WorkSpaces, você deve registrá-lo. No painel de navegação, escolha e, em seguida WorkSpaces, escolha Criar WorkSpaces.
5. Em Selecionar um diretório, escolha o diretório criado pelo AWS CloudFormation no procedimento anterior. No menu Ações, selecione Registrar.
6. Para a seleção da sub-rede, selecione as duas sub-redes privadas anotadas na etapa nove do procedimento anterior.
7. Selecione Habilitar permissões de autoatendimento e escolha Registrar.
8. Depois que o diretório for registrado, continue criando WorkSpace o. Selecione o diretório registrado e escolha Próximo.
9. Na página Criar usuários, escolha Criar usuário adicional. Digite seu nome e e-mail para permitir que você use WorkSpace o. Verifique se o endereço de e-mail é válido, pois as informações de WorkSpace login são enviadas para esse endereço de e-mail.
10. Selecione Next (Próximo).
11. Na página Identificar usuários, selecione o usuário que você criou na etapa nove e escolha Próximo.
12. Na página Selecionar pacote, escolha Padrão com Amazon Linux 2 e selecione Próximo.
13. Use as configurações padrão para o modo de execução e a personalização do usuário e, depois, escolha Criar espaço de trabalho. O `Pending` status WorkSpace começa e muda para cerca `Available` de 20 minutos.
14. Quando o WorkSpace estiver disponível, você receberá um e-mail com instruções para acessá-lo no endereço de e-mail fornecido na etapa nove.

Depois de entrar no seu WorkSpace, você pode testar se está acessando usando seu Acesso AWS Management Console Privado.

Para acessar um WorkSpace

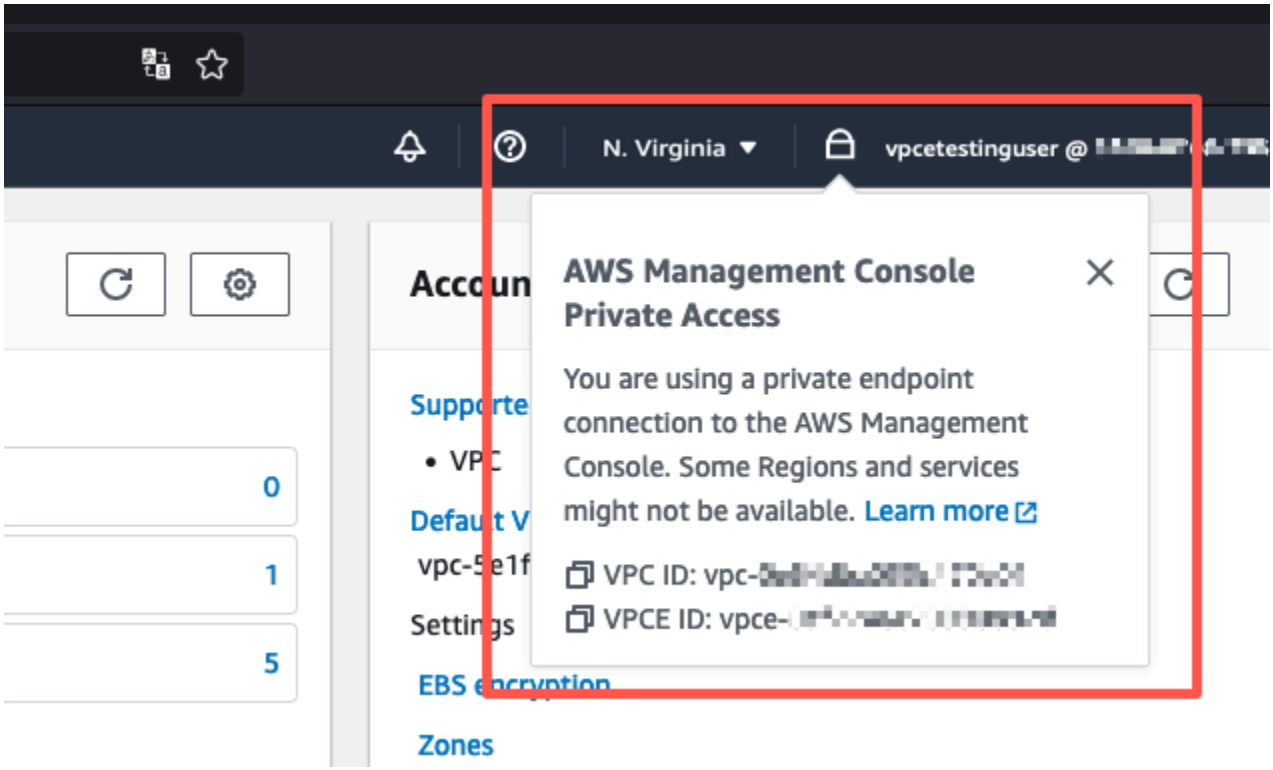
1. Abra o e-mail que você recebeu na etapa 14 do procedimento anterior.
2. No e-mail, escolha o link exclusivo fornecido para configurar seu perfil e baixar o WorkSpaces cliente.
3. Defina a senha.
4. Baixe o cliente de sua escolha.
5. Instale e inicie o cliente. Insira o código de registro fornecido no e-mail e escolha Registrar.
6. Faça login na Amazon WorkSpaces usando as credenciais que você criou na etapa três.

Para testar a configuração do Acesso AWS Management Console Privado

1. Do seu WorkSpace, abra seu navegador. Depois, navegue até o AWS Management Console e faça login usando suas credenciais.

   > **Note**
   >
   > Se você estiver usando o Firefox como navegador, verifique se a opção Ativar DNS por HTTPS está desativada nas configurações do navegador.

2. Abra o console do Amazon S3, onde você pode verificar se está conectado usando o acesso AWS Management Console privado.
3. Selecione o ícone de cadeado na barra de navegação para ver a VPC e o endpoint da VPC em uso. A captura de tela a seguir mostra a localização do ícone de cadeado e as informações da VPC.



Testar a configuração da VPC com políticas do IAM

Você pode testar ainda mais sua VPC que você configurou com o Amazon EC2 WorkSpaces ou implantando políticas do IAM que restringem o acesso.

A política a seguir negará acesso ao Amazon S3, a menos que esteja usando a VPC especificada.

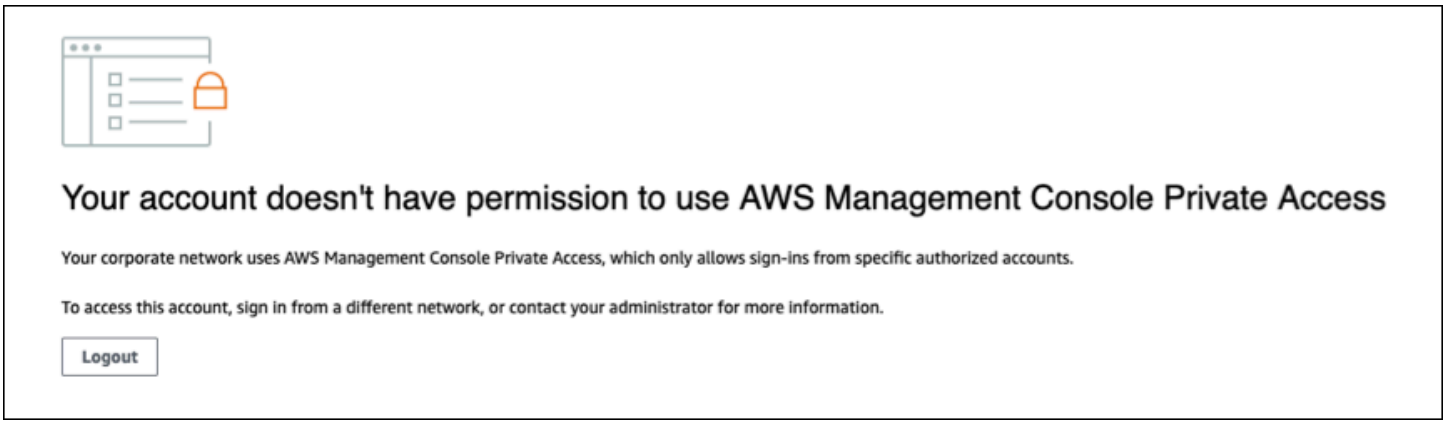
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
```

```
        }
    ]
}
```

A política a seguir limita o login em Conta da AWS IDs selecionadas usando uma política de acesso AWS Management Console privado para o endpoint de login.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

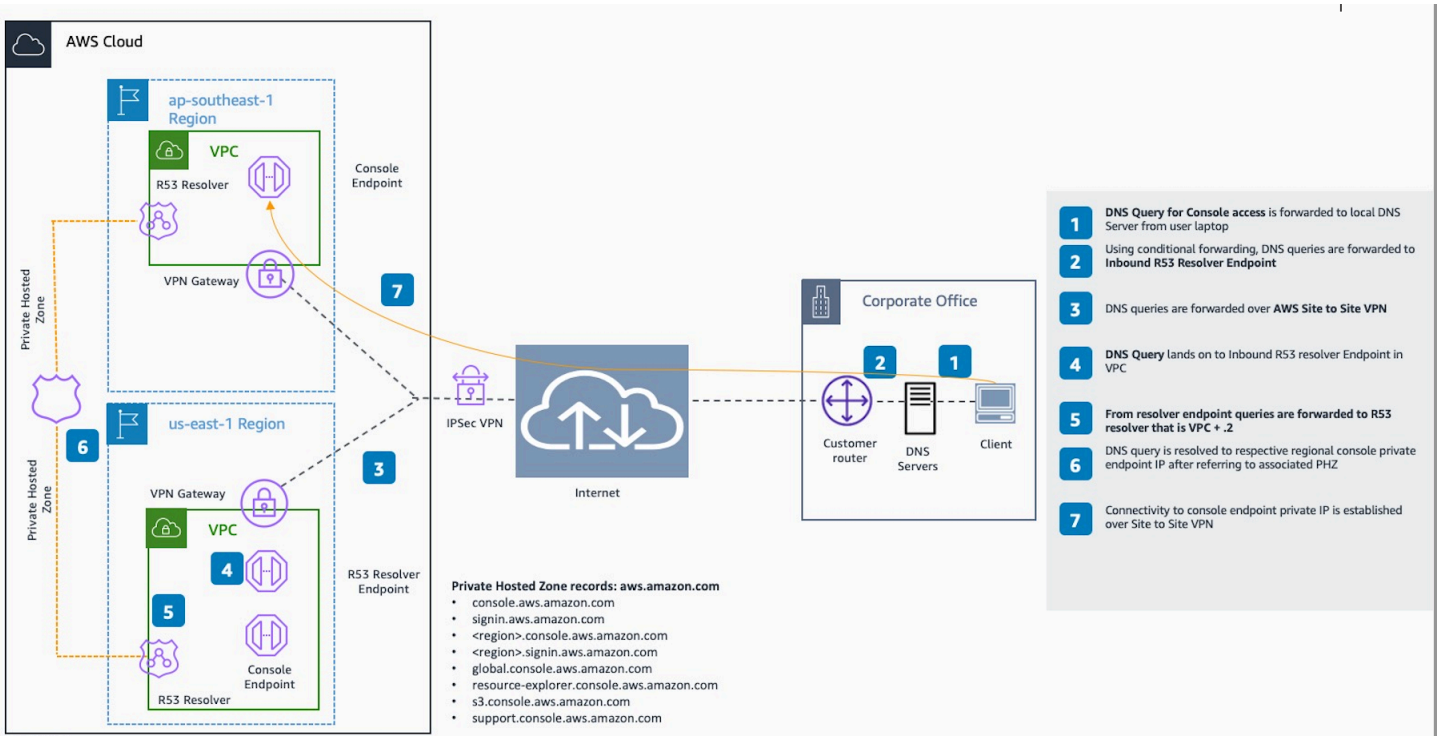
Se você se conectar com uma identidade que não pertence à sua conta, a página de erro a seguir será exibida.



Arquitetura de referência

Para se conectar de forma AWS Management Console privada ao Private Access a partir de uma rede local, você pode aproveitar a opção de conexão AWS Site-to-Site VPN com o AWS Virtual Private Gateway (VGW). AWS Site-to-Site VPN permite o acesso à sua rede remota a partir da sua VPC criando uma conexão e configurando o roteamento para passar o tráfego pela conexão. Para obter mais informações, consulte O que é VPN AWS Site-to-Site no Guia do usuário da VPN Site-to-SiteAWS . AWS O Virtual Private Gateway (VGW) é um serviço regional altamente disponível que atua como um gateway entre uma VPC e a rede local.

AWS Site-to-Site VPN ao AWS Virtual Private Gateway (VGW)



Um componente essencial nesse projeto de arquitetura de referência é Amazon Route 53 Resolver, especificamente, o resolvedor de entrada. Quando você o configura na VPC em que os endpoints de acesso AWS Management Console privado são criados, os endpoints do resolvedor (interfaces de rede) são criados nas sub-redes especificadas. Os endereços IP deles podem então ser referenciados em encaminhadores condicionais nos servidores DNS on-premises, para permitir a consulta de registros em uma zona hospedada privada. Quando os clientes locais se conectam ao AWS Management Console, eles são roteados para os IPs AWS Management Console privados dos endpoints de acesso privado.

Antes de configurar a conexão com o endpoint de acesso AWS Management Console privado, conclua as etapas de pré-requisitos para configurar os endpoints de acesso AWS Management Console privado em todas as regiões em que você deseja acessar AWS Management Console, bem como na região Leste dos EUA (Norte da Virgínia) e configurar a zona hospedada privada.

Iniciar o AWS CloudShell na barra de ferramentas do console

O AWS CloudShell é um shell pré-autenticado baseado em navegador que pode ser iniciado diretamente do AWS Management Console na barra de ferramentas do console. Você pode executar comandos da AWS CLI de serviços usando o shell de sua preferência (Bash, PowerShell ou Z shell).

É possível iniciar o CloudShell pela Console Toolbar usando um dos métodos a seguir:

- Escolha o ícone do CloudShell na parte inferior esquerda do console.
- Clique no ícone do CloudShell na barra de navegação do console.

Para ter mais informações sobre esse serviço, consulte o Guia do usuário do AWS CloudShell.

Para ter informações sobre as Regiões da AWS onde o AWS CloudShell está disponível, consulte a Lista de serviços regionais da AWS. A seleção da região do console está sincronizada com a Região do CloudShell. Se o CloudShell não estiver disponível em uma região selecionada, ele operará na Região mais próxima.

Obter informações de faturamento

Se você tiver as permissões necessárias, é possível obter informações sobre suas cobranças da AWS no console.

Para obter as informações de faturamento

1. Na barra de navegação, selecione o nome da conta.
2. Selecione Billing Dashboard (Painel de faturamento).
3. Use o painel do AWS Billing and Cost Management para encontrar um resumo e um detalhamento de seus gastos mensais. Para saber mais, consulte o Manual do usuário do AWS Billing.

Usar o Markdown no console

Alguns serviços do AWS Management Console, como o Amazon CloudWatch, oferecem suporte ao uso do Markdown em determinados campos. Este tópico explica os tipos de formatação de Markdown compatíveis com o console.

Conteúdo

Parágrafos, espaçamento entre linhas e linhas horizontais

Os parágrafos são separados por uma linha em branco. Para garantir que a linha em branco entre os parágrafos seja renderizada quando for convertida em HTML, adicione uma nova linha com um espaço não separável (` `) e, depois, uma linha em branco. Repita esse par de linhas para inserir várias linhas em branco uma após a outra, como no exemplo a seguir:

```
 

 
```

Para criar uma regra horizontal que separa os parágrafos, adicione uma nova linha com três hifens seguidos: `---`

```
Previous paragraph.
---
Next paragraph.
```

Para criar um bloco de texto com tipo de espaçamento uniforme, adicione uma linha com três acentos graves (`). Insira o texto a ser exibido no tipo de espaçamento uniforme. Depois, adicione

outra nova linha com três acentos graves. O exemplo a seguir mostra o texto que será formatado para o tipo de espaçamento uniforme quando exibido:

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

Títulos

Para criar cabeçalhos, use o sinal de libra (#). Um sinal de libra e um espaço indicam um cabeçalho de nível superior. Dois sinais de libras criam um cabeçalho de segundo nível e três sinais de libras criam um cabeçalho de terceiro nível. Os exemplos a seguir mostram um cabeçalho de nível superior, segundo nível e terceiro nível:

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

Formatação de texto

Para formatar o texto como itálico, cerque-o com sublinhados (_) ou asteriscos (*).

```
*This text appears in italics.*
```

Para formatar o texto como negrito, cerque-o com dois sublinhados ou dois asteriscos em cada lado.

```
**This text appears in bold.**
```

Para formatar o texto como tachado, cerque–o com dois sinais de til (~).

```
~~This text appears in strikethrough.~~
```

Links

Para adicionar um hiperlink de texto, insira o texto do link entre colchetes ([ ]), seguido pelo URL completo entre parênteses (( )), como no exemplo a seguir:

```
Choose [link_text](http://my.example.com).
```

Listas

Para formatar linhas como parte de uma lista com marcadores, adicione-as em linhas separadas que começam com um único asterisco (*) e, depois, um espaço, como no exemplo a seguir:

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

Para formatar linhas como parte de uma lista numerada, adicione-as em linhas separadas que começam com um número, um ponto (.) e um espaço, como no exemplo a seguir:

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

Tabelas e botões (CloudWatch painéis)

CloudWatch Os widgets de texto dos painéis oferecem suporte a tabelas e botões Markdown.

Para criar uma tabela, separe as colunas usando barras verticais (|) e as linhas usando novas linhas. Para tornar a primeira linha um cabeçalho, insira uma linha entre ela (linha de cabeçalho) e a primeira linha de valores. Depois, adicione pelo menos três hifens (-) para cada coluna na tabela. Separe as colunas usando barras verticais. O exemplo a seguir mostra o Markdown para uma tabela com duas colunas, uma linha de cabeçalho e duas linhas de dados:

```
Table | Header
----|-----
Amazon Web Services | AWS
```

```
1 | 2
```

O texto de Markdown no exemplo anterior cria a seguinte tabela:

Tabela	Cabeçalho
Amazon Web Services	AWS
1	2

Em um widget de texto CloudWatch do painel, você também pode formatar um hiperlink para que apareça como um botão. Para criar um botão, use `[button:`*`Button text`*`]`, seguido pelo URL completo entre parênteses (( )), como no exemplo a seguir:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

Solução de problemas

Consulte esta seção para encontrar soluções para problemas comuns com AWS Management Console o.

Você também pode diagnosticar e solucionar erros comuns em alguns AWS serviços usando o Amazon Q Developer. Para obter mais informações, consulte Diagnosticar erros comuns no console com o Amazon Q Developer no Amazon Q Developer User Guide.

Tópicos

A página não está sendo carregada corretamente.

- Se esse problema ocorrer apenas ocasionalmente, verifique a conexão com a Internet. Tente se conectar por meio de uma rede diferente, com ou sem uma VPN, ou tente usar um navegador da Web diferente.
- Se todos os usuários afetados forem da mesma equipe, pode ser um problema de privacidade na extensão do navegador ou no firewall de segurança. Extensões de privacidade do navegador e firewalls de segurança podem bloquear o acesso aos domínios usados pelo. AWS Management Console Tente desativar essas extensões ou ajustar as configurações do firewall. Para verificar problemas com a conexão, abra as ferramentas de desenvolvedor do navegador (Chrome, Firefox) e inspecione os erros na guia Console. O AWS Management Console usa sufixos de domínios, incluindo a lista a seguir. Essa lista não é exaustiva e pode mudar com o tempo. Os sufixos desses domínios não são usados exclusivamente pela AWS.
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com

- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

> **Warning**
>
> Desde 31 de julho de 2022, AWS não é mais compatível com o Internet Explorer 11. Recomendamos que você use o AWS Management Console com outros navegadores compatíveis. Para obter mais informações, consulte o Blog de notícias da AWS.

Meu navegador exibe um erro de “acesso negado” ao se conectar ao AWS Management Console

Alterações recentes feitas no console podem afetar seu acesso se você estiver usando todos os itens a seguir:

- Um navegador de dentro de uma VPC.
- Endpoints de VPC.
- Políticas do IAM que contêm uma chave de condição `aws:SourceIp` global.

No console, acesse a página de políticas do IAM. Recomendamos que você revise as políticas do IAM que contêm uma chave de condição `aws:SourceIp` global e adicione uma `aws:SourceVpc` chave.

Como alternativa, você pode considerar a integração ao recurso de acesso AWS Management Console privado para acessá-lo AWS Management Console por meio de um VPC endpoint e `aws:SourceVpc` usar as condições em suas políticas. Para ter mais informações, consulte AWS Management Console Acesso privado.

Meu navegador exibe erros de tempo limite ao se conectar ao AWS Management Console

Se houver uma interrupção do serviço em seu padrão Região da AWS, seu navegador poderá exibir um erro 504 Gateway Timeout ao tentar se conectar ao. AWS Management Console Para fazer login em uma região diferente, especifique um endpoint regional alternativo na URL. AWS Management Console Por exemplo, se houver uma interrupção na região `us-west-1` (Norte da Califórnia), para acessar a região `us-west-2` (Oregon), use o seguinte modelo:

```
https://region-code.console.aws.amazon.com
```

Para ter informações, consulte Endpoints de serviço do AWS Management Console na Referência geral da AWS.

Para ver o status de tudo Serviços da AWS, incluindo o AWS Management Console, consulte AWS Health Dashboard.

Quero alterar o idioma do AWS Management Console , mas não consigo encontrar o menu de seleção de idiomas na parte inferior da página.

O menu de seleção de idioma foi movido para a nova página Unified Settings (Configurações unificadas). Para alterar o idioma do AWS Management Console, navegue até a página Configurações Unificadas e escolha o idioma do console.

Para obter mais informações, consulte Alterar o idioma do AWS Management Console.

Histórico do documento

A tabela a seguir descreve alterações importantes no Guia de conceitos básicos do AWS Management Console , a partir de março de 2021.

Alteração	Descrição	Data
Converse com Amazon Q	Uma nova página de configurações detalhando como os usuários podem fazer AWS perguntas ao Amazon Q Developer. Para obter mais informações, consulte Converse com o Amazon Q Developer.	29 de maio de 2024
Meus aplicativos	Uma nova página que apresenta MyApplications. Para obter mais informações, consulte What is MyApplications on AWS? .	29 de novembro de 2023
Definir configurações unificadas	Uma nova página de configurações para definir configurações e padrões que se aplicam ao usuário atual, incluindo idioma e região. Para obter mais informações, consulte Definir configurações unificadas.	6 de abril de 2022
Nova AWS Console Home interface de usuário	Nova AWS Console Home interface de usuário, que inclui widgets para exibir informações importantes de uso e atalhos para AWS serviços. Para obter mais informaçõ	25 de fevereiro de 2022

Alteração	Descrição	Data
	es, consulte Trabalhar com widgets.	
Alterar o idioma do console	Escolha um idioma diferente para o AWS Managemen t Console. Para obter mais informações, consulte Alterar o idioma do AWS Managemen t Console.	1º de abril de 2021
Lançamento CloudShell	Abra AWS CloudShell a partir do AWS Managemen t Console e execute os comandos da AWS CLI. Para obter mais informações, consulte Lançamento AWS CloudShell.	22 de março de 2021

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.