Guia de conceitos básicos

Console de gerenciamento da AWS

Versão 1.0

Console de gerenciamento da AWS: Guia de conceitos básicos

Table of Contents

O que é o Console de gerenciamento da AWS?

O Console de gerenciamento da AWSé um aplicativo baseado na web que contém e fornece acesso centralizado a todos os consoles de AWS serviço individuais. Você pode usar a Navegação Unificada no Console de gerenciamento da AWS para pesquisar serviços, visualizar notificações, acessar AWS CloudShell, acessar informações de conta e cobrança e personalizar as configurações gerais do console. A página inicial do Console de gerenciamento da AWS é chamada AWS Console Home. A partir de AWS Console Home, você pode gerenciar seus AWS aplicativos e acessar todos os outros consoles de serviço individuais. Você também pode personalizar AWS Console Home para mostrar outras informações úteis sobre AWS seus recursos usando widgets. Você pode adicionar, remover e reorganizar widgets como Visitado recentemente, AWS Health e muito mais.

Tópicos

Características do Console de gerenciamento da AWS

As características importantes do Console de gerenciamento da AWS incluem o seguinte:

- Navegar até os consoles de AWS serviço — Você pode usar a Navegação Unificada para acessar os consoles de serviço visitados recentemente, visualizar e adicionar serviços à sua lista de Favoritos, acessar as configurações do console e acessar. Notificações de Usuários da AWS
- Pesquise AWS serviços e outras AWS informações — use a Pesquisa Unificada para pesquisar AWS serviços e recursos e produtos do AWS marketplace.
- Personalizar o console: você pode usar as configurações unificadas para personalizar vários aspectos do Console de gerenciamento da AWS. Isso inclui o idioma, a região padrão e muito mais.
- Executar comandos da CLI — pode ser AWS CloudShell acessado diretamente do console. Você pode usar CloudShell para executar comandos da AWS CLI em seus serviços favoritos.
- Acesse todas as notificações de AWS eventos - Você pode usar o Console de gerenciamento da AWS para acessar as notificações de Notificações de Usuários da AWS AWS Health e.

- Personalizar AWS Console Home — Você pode personalizar completamente sua AWS Console Home experiência usando widgets.
- Crie e gerencie AWS aplicativos — gerencie e monitore o custo, a integridade, a postura de segurança e o desempenho de seus aplicativos usando o MyApplications in. AWS Console Home
- Converse com a Amazon Q — Você pode obter respostas geradas pelo assistente de inteligência artificial (IA) generativa para suas AWS service (Serviço da AWS) perguntas diretamente do console. Você também pode se conectar com um agente ao vivo para obter suporte adicional.
- Controle o acesso à AWS conta em sua rede — Você pode usar o Acesso Console de gerenciamento da AWS Privado para limitar o acesso Console de gerenciamento da AWS a um conjunto específico de AWS contas conhecidas quando o tráfego se origina de dentro da sua rede.

Consoles AWS de serviço individuais no Console de gerenciamento da AWS

Cada AWS serviço tem seu próprio console de serviço individual que você pode acessar no Console de gerenciamento da AWS. As configurações escolhidas nas Configurações Unificadas para o Console de gerenciamento da AWS, como modo visual e idioma padrão, são aplicadas a todos os AWS consoles individuais. AWS os consoles de serviços oferecem uma ampla variedade de ferramentas para computação em nuvem, bem como informações sobre sua conta e sobre seu faturamento. Se você quiser saber mais sobre um serviço específico e seu console, por exemplo, o Amazon Elastic Compute Cloud, navegue até o console usando o Unified Search na barra de Console de gerenciamento da AWS navegação e acesse a EC2 documentação da Amazon no site de AWS documentação.

Ao navegar até o console de um AWS serviço individual, você ainda pode acessar os recursos do Console de gerenciamento da AWS uso da Navegação Unificada na parte superior do console. Você pode deixar comentários sobre o console de um serviço específico navegando até esse console e escolhendo Feedback no rodapé da página.

Acessando o Console de gerenciamento da AWS

Você pode acessar o Console de gerenciamento da AWS em https://console.aws.amazon.com/.

Acessar o Console de gerenciamento da AWS com dispositivos móveis

O Console de gerenciamento da AWS foi projetado para funcionar em tablets e outros tipos de dispositivos móveis:

- 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.

Para acessar o Console de gerenciamento da AWS em um dispositivo móvel, você deve usar o AWS Console Mobile Application. Esse aplicativo está disponível para Android e iOS. O aplicativo móvel do Console viabiliza tarefas relevantes em dispositivos móveis, sendo um ótimo complemento à experiência completa na web. Por exemplo, você pode facilmente visualizar e gerenciar instâncias do Amazon EC2 existentes e alarmes do Amazon CloudWatch em seu telefone. Para obter mais informações, consulte O que é o AWS Console Mobile Application? no Manual do usuário do AWS Console Mobile Application.

Você pode baixar o aplicativo móvel do Console na Amazon Appstore, Google Play ou iOS App Store.

Conceitos básicos de um serviço no Console de gerenciamento da AWS

O Console de gerenciamento da AWS 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 obter mais informações, consulte Pesquisando produtos, serviços, recursos e muito mais usando a Pesquisa Unificada no Console de gerenciamento da AWS.
- No widget Recently visited services (Serviços visitados recentemente), escolha o nome de um serviço.
- No widget Serviços acessados recentemente, escolha Veja todos os serviços da AWS. Depois, na página 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).

Usar a barra de navegação do Console de gerenciamento da AWS por meio da navegação unificada

Este tópico descreve como usar a navegação unificada. A navegação unificada refere-se à barra de navegação que atua como cabeçalho e rodapé do console. Você pode usar a navegação unificada para:

- Pesquisar e acessar serviços, recursos, produtos e muito mais na AWS.
- Inicializar o AWS CloudShell.
- Acessar as notificações da AWS e os eventos do AWS Health.
- Receber suporte de várias fontes de conhecimento da AWS.
- Configurar o Console de gerenciamento da AWS escolhendo o idioma padrão, o modo visual, a região e muito mais.
- Acessar informações sobre conta, organização, cota de serviço e faturamento.

Tópicos

Acessar o menu Serviços no Console de gerenciamento da AWS

Você pode usar o menu de Serviços ao lado da barra de pesquisa para acessar os serviços acessados recentemente, visualizar a lista de Favoritos e visualizar todos os serviços da AWS.

Também é possível escolher um tipo de serviço para visualizar os serviços por tipo, por exemplo, Analytics ou Integração de aplicações.

O procedimento a seguir descreve como acessar o menu Serviços.

Como acessar o menu Serviços

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. (Opcional) Escolha Acesso recente para visualizar os serviços e as aplicações com os quais você interagiu recentemente.
4. (Opcional) Escolha Favoritos para ver a lista de favoritos.
5. (Opcional) Escolha Todas as aplicações para visualizar suas aplicações em myApplications.
6. (Opcional) Escolha Todos os serviços para ver uma lista de todos os serviços da AWS em ordem alfabética.
7. (Opcional) Escolha um tipo de serviço para ver os serviços da AWS por tipo.

Pesquisando produtos, serviços, recursos e muito mais usando a Pesquisa Unificada no Console de gerenciamento da AWS

A caixa de pesquisa na barra de navegação fornece uma ferramenta de pesquisa unificada para encontrar AWS serviços e recursos, documentação de serviços, AWS Marketplace produtos e muito mais. Basta inserir alguns caracteres ou uma pergunta para começar a gerar resultados de todos os tipos de conteúdo disponíveis. Cada palavra inserida refina ainda mais os resultados. Os tipos de conteúdo disponíveis incluem:

- Services
- Recursos
- Documentos
- Blogs
- Artigos da base de conhecimento
- Eventos
- Tutoriais
- Marketplace

- Recursos

> **Note**
>
> Você pode realizar uma pesquisa focada para filtrar os resultados da pesquisa e mostrar somente recursos. Para realizar uma pesquisa focada, insira `/Resources` no início da consulta na barra de pesquisa e escolha /Recursos no menu suspenso. Depois, insira o restante da consulta.

Tópicos

Pesquisando AWS produtos no Console de gerenciamento da AWS

O procedimento a seguir detalha como pesquisar AWS produtos usando a ferramenta de pesquisa.

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

1. Na caixa de pesquisa da barra de navegação do Console de gerenciamento da AWS, insira sua consulta.
2. Escolha qualquer link para navegar até o destino desejado.

> **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.

Refinando sua pesquisa no Console de gerenciamento da AWS

Você pode refinar a pesquisa por tipo de conteúdo e ver informações adicionais sobre os resultados da pesquisa.

Como refinar a pesquisa para um tipo de conteúdo específico

1. Na caixa de pesquisa da barra de navegação do Console de gerenciamento da AWS, insira sua consulta.
2. Escolha um dos tipos de conteúdo ao lado dos resultados da pesquisa.
3. (Opcional) Para ver todos os resultados de uma categoria específica:
   - Escolha Mostrar mais. Uma nova guia será aberta mostrando os resultados.
4. (Opcional) Para ver informações adicionais sobre os resultados da pesquisa:
   a. Nos resultados da pesquisa, passe o cursor sobre um resultado da pesquisa.
   b. Veja as informações adicionais disponíveis.

Visualizando os recursos de um serviço no Console de gerenciamento da AWS

Você pode visualizar os recursos de um serviço nos resultados da pesquisa.

Como visualizar os recursos de um serviço

1. Na caixa de pesquisa da barra de navegação do Console de gerenciamento da AWS, insira sua consulta.
2. Nos resultados da pesquisa, passe o cursor sobre um serviço em Serviços.
3. Escolha um dos links em Principais recursos.

Iniciando a AWS CloudShell partir da barra de navegação no Console de gerenciamento da AWS

AWS CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente da barra de navegação. Console de gerenciamento da AWS Você pode executar AWS CLI comandos em serviços usando seu shell preferido (shell Bash ou Z). PowerShell

Você pode iniciar a CloudShell partir do Console de gerenciamento da AWS usando um dos dois métodos a seguir:

- Escolha o CloudShell ícone no rodapé do console.
- Escolha o CloudShell ícone na barra de navegação do console.

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

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

Acessar notificações da AWS e eventos do Health

Você pode acessar algumas de suas notificações da AWS e visualizar eventos do Health na barra de navegação. Você também pode acessar o Notificações de Usuários da AWS para ver todas as suas notificações da AWS e o AWS Health Dashboard na barra de navegação.

Para ter mais informações, consulte What is Notificações de Usuários da AWS? no Guia do usuário do Notificações de Usuários da AWS e O que é o AWS Health? no Guia do usuário do AWS Health.

O procedimento a seguir descreve como acessar as informações de seus eventos da AWS.

Como acessar as informações de seus eventos da AWS

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o ícone de sino.
3. Veja as notificações e os eventos do Health.
4. (Opcional) Escolha Ver todas as notificações para navegar até o console do Notificações de Usuários.
5. (Opcional) Escolha Veja todos os eventos de integridade para navegar até o console do AWS Health.

Obter suporte

Você pode receber suporte escolhendo o ícone de ponto de interrogação na barra de navegação. No menu de suporte, você pode optar por:

- Navegar até o console de serviço da central de suporte
- Receber ajuda especializada do AWS IQ
- Conferir conhecimento selecionado de artigos da comunidade e do centro de conhecimentos no AWS re:Post
- Acessar a documentação da AWS
- Navegar até os treinamentos da AWS
- Navegar até o centro de recursos de conceitos básicos da AWS
- Deixar feedback a respeito de qualquer console de serviço que você esteja acessando

> **Note**
>
> Isso também pode ser feito escolhendo Feedback no rodapé do console. O título do modal exibido mostra para qual console você está deixando feedback no momento.

Você também pode receber ajuda a qualquer momento no console, entrar em contato com um agente ao vivo e fazer qualquer pergunta sobre a AWS conversando com o AWS Q. Para ter mais informações, consulte ???.

Configurando o Console de gerenciamento da AWS uso de configurações unificadas

Este tópico descreve como configurar você Console de gerenciamento da AWS usando a página Configurações Unificadas para definir padrões que se aplicam a todos os consoles de serviço.

Tópicos

- Alterando o idioma do Console de gerenciamento da AWS

Definindo configurações unificadas no Console de gerenciamento da AWS

Você pode definir configurações e padrões, como exibição, idioma e região, na página Configurações Console de gerenciamento da AWS unificadas. Você pode acessar as configurações unificadas por meio da barra de navegação unificada. 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.

Tópicos

- Acessando as configurações unificadas no Console de gerenciamento da AWS
- Redefinindo as configurações unificadas no Console de gerenciamento da AWS
- Editando configurações unificadas no Console de gerenciamento da AWS
- Alterando o modo visual do Console de gerenciamento da AWS

Acessando as configurações unificadas no Console de gerenciamento da AWS

O procedimento a seguir descreve como acessar as configurações unificadas.

Para acessar as configurações unificadas

1. Faça login no Console de gerenciamento da AWS.

2. Na barra de navegação, escolha o ícone de engrenagem (#).
3. Para abrir a página Configurações unificadas, selecione Ver todas as configurações de usuários.

Redefinindo as configurações unificadas no Console de gerenciamento da AWS

Você pode excluir todas as definições de configurações unificadas e restaurar as configurações comuns 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.

Como redefinir todas as configurações unificadas

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o ícone de engrenagem (#).
3. Abra a página Configurações unificadas, selecione Ver todas as configurações de usuários.
4. Escolha Redefinir tudo.

Editando configurações unificadas no Console de gerenciamento da AWS

O procedimento a seguir descreve como editar suas configurações preferidas.

Como editar as configurações unificadas

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o ícone de engrenagem (#).
3. Abra a página Configurações unificadas, selecione Ver todas as configurações de usuários.
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 Console de gerenciamento da AWS, 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 Console de gerenciamento da AWS 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.

Alterando o modo visual do Console de gerenciamento da AWS

O modo visual permite que você defina o console para os modos claro ou escuro, bem como o modo de exibição padrão do navegador.

Como alterar o modo visual na barra de navegação

1. Faça login no Console de gerenciamento da AWS.
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 Padrão do navegador para o modo de exibição padrão do navegador.

Escolher a 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 Console de gerenciamento da AWSou 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.

> **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.

Tópicos

Escolhendo uma região na barra de navegação no Console de gerenciamento da AWS

O procedimento a seguir detalha como você pode alterar a região na barra de navegação.

Como escolher uma região na barra de navegação

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o nome da região exibida no momento.
3. Escolha uma região para a qual mudar.

Definindo a região padrão no Console de gerenciamento da AWS

O procedimento a seguir detalha como você pode alterar a região padrão na página Configurações unificadas.

Como definir a região padrão

1. Na barra de navegação, escolha o ícone de engrenagem (#).

2. Escolha Ver todas as configurações de usuários para navegar até a página Configurações unificadas.
3. Selecione Edit (Editar) próximo a Localization and default Region (Localização e região padrão).
4. Em Região padrão, escolha uma região.

> **Note**
>
> Se não selecionar uma região padrão, a última região que você acessou será usada como padrão.

5. Escolha Salvar configurações.
6. (Opcional) Escolha Ir para nova região padrão para acessar imediatamente a nova região padrão.

Favoritos no Console de gerenciamento da AWS

Para acessar seus serviços e aplicações usados com frequência mais rapidamente, você pode salvar os consoles de serviço em uma lista de Favoritos. Você pode adicionar e remover usuários usando o Console de gerenciamento da AWS. Quando você adiciona um serviço ou uma aplicação aos seus Favoritos, ele aparece na barra rápida de Favoritos.

Tópicos

Adicionando favoritos no Console de gerenciamento da AWS

É possível adicionar serviços e aplicações aos seus favoritos no menu Serviços e no menu Acesso recente. Você também pode adicionar serviços aos seus favoritos na página de resultados da pesquisa na caixa de pesquisa. Os serviços e as aplicações que você adiciona aos seus favoritos aparecem na barra rápida de Favoritos.

Tópicos

- Adicionar serviços aos seus favoritos no Console de gerenciamento da AWS
- Adicionar aplicativos aos seus favoritos no Console de gerenciamento da AWS

Barra rápida de favoritos na Console de gerenciamento da AWS

A barra rápida de favoritos aparece quando você tem pelo menos um AWS serviço ou aplicativo adicionado aos seus favoritos. A barra rápida de favoritos está localizada após a barra de navegação e é visível em todos os consoles de AWS serviço, para que você possa acessar rapidamente seus serviços e aplicativos favoritos. Você pode reorganizar a ordem dos serviços e das aplicações na barra rápida de favoritos arrastando um serviço ou uma aplicação para a esquerda ou para a direita.

Adicionar serviços aos seus favoritos no Console de gerenciamento da AWS

Você pode adicionar serviços aos seus favoritos no menu Serviços ou na página de resultados da pesquisa na caixa de pesquisa.

Services menu

Como adicionar favoritos no menu Serviços

1. Abra a Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. (Opcional) Adicione um serviço acessado recentemente aos seus favoritos:
   a. Em Visitado recentemente, passe o cursor sobre um serviço.
   b. Selecione a estrela ao lado do nome do serviço.
4. Selecione Todos os serviços.
5. Passe o cursor sobre o serviço escolhido.
6. Selecione a estrela ao lado do nome do serviço.

Search box

Como adicionar favoritos pela caixa de pesquisa

1. Abra a Console de gerenciamento da AWS.
2. Insira o nome de um serviço na caixa de pesquisa.
3. Na página de resultados da pesquisa, selecione a estrela ao lado do nome do serviço.

> **Note**
>
> Depois de adicionar um serviço aos favoritos, ele será adicionado à barra rápida de favoritos após a barra de navegação.

Adicionar aplicativos aos seus favoritos no Console de gerenciamento da AWS

É possível adicionar aplicações aos seus favoritos no menu Serviços.

Como adicionar favoritos no menu Serviços

1. Abra a Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. (Opcional) Adicione uma aplicação acessada recentemente aos seus favoritos:
   a. Em Acesso recente, passe o cursor sobre uma aplicação.
   b. Selecione a estrela ao lado do nome da aplicação.
4. Selecione Aplicações.
5. Passe o cursor sobre a aplicação escolhida.
6. Selecione a estrela ao lado do nome da aplicação.

> **Note**
>
> Depois de adicionar uma aplicação aos favoritos, ele será adicionado à barra rápida de favoritos após a barra de navegação.

Acessando favoritos no Console de gerenciamento da AWS

Você pode acessar serviços e aplicações adicionados aos seus favoritos no menu Serviços, na barra rápida de favoritos e no widget Favoritos.

Services menu

Como acessar favoritos no menu Serviços

1. Abra a Console de gerenciamento da AWS.

2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. Escolha Favoritos.
4. Visualize os serviços e as aplicações que você adicionou aos favoritos.
5. (Opcional) Visualize recursos de aplicações:
    a. Selecione uma aplicação.
    b. (Opcional) Selecione uma exibição.
    c. Visualize seus recursos.
    d. (Opcional) Selecione um filtro. É possível filtrar seus recursos por Propriedades ou por Tags. Consulte mais informações em Referência de sintaxe de consultas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de recursos da AWS .
    e. (Opcional) Selecione um recurso para visualizá-lo no console de serviço relevante.

> **Tip**
>
> Você pode continuar navegando pelos recursos de onde parou, escolhendo Serviços (⁝⁝⁝). Seus filtros de pesquisa aplicados também são mantidos.

Favorites quickbar

Como acessar seus favoritos na barra rápida de favoritos

1. Abra a Console de gerenciamento da AWS.
2. Visualize os serviços e as aplicações na barra rápida de favoritos.

Favorites widget

Como acessar seus favoritos no widget Favoritos

1. Abra a Console de gerenciamento da AWS.
2. (Opcional) Adicione o widget Favoritos se você ainda não o tiver:
    a. Escolha o botão + Adicionar widgets na página inicial do console.
    b. No menu Adicionar widgets, arraste o widget Favoritos usando o ícone ⁝⁝ e coloque-o na página inicial do console.

3. Visualize os serviços e as aplicações no widget Favoritos.

Para ter mais informações sobre widgets, consulte the section called “Trabalhar com widgets”.

Removendo favoritos no Console de gerenciamento da AWS

É possível remover serviços e aplicações dos seus favoritos usando o menu Serviços. Você também pode remover serviços usando a página de resultados da pesquisa na barra de pesquisa.

Services menu

Como remover favoritos do menu Serviços

1. Abra a Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços.
3. Escolha Favoritos.
4. Desmarque a estrela ao lado do nome do serviço ou da aplicação.

Search box

> **Note**
>
> No momento, só é possível remover serviços usando a página de resultados da pesquisa na barra de pesquisa.

Como remover favoritos da caixa de pesquisa

1. Abra a Console de gerenciamento da AWS.
2. Insira o nome de um serviço na caixa de pesquisa.
3. Na página de resultados da pesquisa, desmarque a estrela ao lado do nome do serviço.

Alterando sua senha no Console de gerenciamento da AWS

Talvez você consiga alterar sua senha pelo Console de gerenciamento da AWS dependendo do seu tipo de usuário e das respectivas permissões. O tópico a seguir descreve como alterar a senha para cada tipo de usuário.

Tópicos

Usuários root no Console de gerenciamento da AWS

Os usuários-raiz podem alterar as respectivas senhas diretamente do Console de gerenciamento da AWS. Um usuário root é o proprietário da conta com acesso completo a todos os AWS serviços e recursos. Você é o usuário raiz se tiver criado a AWS conta e fizer login usando o e-mail e a senha do usuário raiz. Para ter mais informações, consulte Root user no Guia do usuário do Centro de Identidade do AWS IAM .

Como alterar a senha sendo usuário-raiz

1. Faça login no Console de gerenciamento da AWS.
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).

Usuários do IAM no Console de gerenciamento da AWS

Os usuários do IAM podem alterar suas senhas de Console de gerenciamento da AWS acordo com suas permissões. Caso contrário, eles devem usar um portal de AWS acesso. Um usuário do IAM

é uma identidade em sua AWS conta que recebe permissões personalizadas específicas. Você é um usuário do IAM se não criou a AWS conta e seu administrador ou funcionário do suporte técnico forneceu suas credenciais de login que incluem um ID ou alias da AWS conta, um nome de usuário e uma senha do IAM. Para ter mais informações, consulte IAM user no Guia do usuário do Início de Sessão da AWS .

Se você tiver permissões da política AWS: permite que os usuários do IAM alterem suas próprias senhas do console na página Credenciais de segurança, poderá alterar a senha pelo console. Para ter mais informações, consulte Como um usuário do IAM altera a própria senha no Guia do usuário do AWS Identity and Access Management .

Se você não tiver as permissões necessárias para alterar sua senha, Console de gerenciamento da AWS consulte Redefinir sua senha de Centro de Identidade do AWS IAM usuário no Guia do Centro de Identidade do AWS IAM usuário.

Usuários do IAM Identity Center no Console de gerenciamento da AWS

Centro de Identidade do AWS IAM os usuários devem alterar sua senha em um portal de AWS acesso. Para obter mais informações, consulte Redefinir sua senha de Centro de Identidade do AWS IAM usuário no Guia do Centro de Identidade do AWS IAM usuário.

Um usuário do IAM Identity Center é um usuário cuja AWS conta faz parte AWS Organizations e faz login por meio do portal de AWS acesso com uma URL exclusiva. Esses usuários podem ser criados diretamente no Centro de Identidade do IAM, no Active Directory ou em outro provedor de identidades externo. Para ter mais informações, consulte Centro de Identidade do AWS IAM user no Guia do usuário do Início de Sessão da AWS .

Identidades federadas no Console de gerenciamento da AWS

Os usuários de identidade federada devem alterar sua senha em um portal de AWS acesso. Para obter mais informações, consulte Redefinir sua senha de Centro de Identidade do AWS IAM usuário no Guia do Centro de Identidade do AWS IAM usuário.

Os usuários com identidade federada fazem login usando um provedor de identidades (IdP) externo. Você é uma identidade federada se:

- Acesse sua AWS conta ou recursos com credenciais de terceiros, como Login with Amazon, Facebook ou Google.
- Use as mesmas credenciais para entrar nos sistemas e AWS serviços corporativos e use um portal personalizado da empresa para entrar. AWS

Para ter mais informações, consulte Federated identity no Guia do usuário do Início de Sessão da AWS .

Alterando o idioma do Console de gerenciamento da AWS

A AWS Console Home experiência inclui a página Configurações unificadas, na qual você pode alterar o idioma padrão AWS dos serviços no Console de gerenciamento da AWS. Você também pode alterar o idioma padrão rapidamente no menu de configurações na barra de navegação.

> **Note**
>
> Os procedimentos a seguir alteram o idioma de todos os consoles de serviço da AWS , 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.

Tópicos

Idiomas compatíveis

Console de gerenciamento da AWS Atualmente, o suporta os seguintes idiomas:

- Inglês (EUA)
- Inglês (Reino Unido)
- Bahasa Indonésia
- Alemã
- Espanhola
- Francesa
- Japonesa
- Italiana

- Portuguesa
- Coreana
- Chinês (simplificado)
- Chinês (tradicional)
- Turca

Alterando o idioma padrão na barra de navegação no Console de gerenciamento da AWS

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

Como alterar o idioma padrão na barra de navegação

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

Alterando o idioma padrão por meio de Configurações unificadas no Console de gerenciamento da AWS

O procedimento a seguir detalha como alterar o idioma padrão na página Configurações unificadas.

Como alterar o idioma padrão em “Configurações unificadas”

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o ícone de engrenagem (#).
3. Para abrir a página Configurações unificadas, selecione Ver todas as configurações de usuários.
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 Console de gerenciamento da AWS.

- 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.

Acessando sua AWS conta, organização, cota de serviço e informações de cobrança no Console de gerenciamento da AWS

Se você tiver as permissões necessárias, poderá acessar informações sobre sua AWS conta, cotas de serviço, organização e informações de cobrança no console.

> **Note**
>
> O Console de gerenciamento da AWS único fornece acesso à conta, organização, cota de serviço e informações de cobrança. Esses serviços têm consoles próprios. Para obter mais informações, consulte o seguinte:
>
> - Gerencie sua AWS conta no Guia AWS Gerenciamento de contas de referência.
> - O que AWS Organizationsé no Guia do AWS Organizations usuário.
> - What is Service Quotas? no Guia do usuário do Service Quotas.
> - Usando a página Gerenciamento de Faturamento e Custos da AWS inicial do Guia do usuário AWS de faturamento.

> **Tip**
>
> Você também pode encontrar mais informações sobre qualquer um desses tópicos perguntando ao Amazon Q. Para ter mais informações, consulte Chat with Amazon Q Developer.

Tópicos

Acessando as informações da conta no Console de gerenciamento da AWS

Se você tiver as permissões necessárias, poderá acessar informações sobre sua AWS conta no console.

Como acessar as informações da conta

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, selecione o nome da conta.
3. Escolha Conta.
4. Veja as informações da sua conta.

> **Note**
>
> Se você quiser fechar sua AWS conta, consulte Fechar uma AWS conta no Guia de AWS Gerenciamento de contas referência.

Acessando as informações da organização no Console de gerenciamento da AWS

Se você tiver as permissões necessárias, poderá acessar informações sobre suas AWS organizações no console.

Como acessar as informações da organização

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, selecione o nome da conta.
3. Escolha Organizações.
4. Visualize as informações da organização.

Acessando as informações da cota de serviço no Console de gerenciamento da AWS

Se você tiver as permissões necessárias, poderá acessar informações sobre as cotas de serviço no console.

Como acessar as informações das cotas de serviço

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, selecione o nome da conta.
3. Escolha Service Quotas.
4. Visualize e gerencie as informações das cotas de serviço.

Acessando informações de cobrança no Console de gerenciamento da AWS

Se você tiver as permissões necessárias, poderá acessar informações sobre suas AWS cobranças no console.

Como acessar as informações de faturamento

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, selecione o nome da conta.
3. Escolha Gerenciamento de cobrança e custos.
4. Use o Gerenciamento de Faturamento e Custos da AWS painel para encontrar um resumo e um detalhamento de seus gastos mensais.

Fazer login em várias contas

Você pode fazer login com até cinco identidades diferentes simultaneamente em um único navegador da Web no Console de gerenciamento da AWS. Elas podem ser qualquer combinação de perfis-raiz, perfis do IAM ou perfis federados em contas diferentes ou na mesma conta. Cada identidade na qual você faz login abre sua própria instância do Console de gerenciamento da AWS em uma nova guia.

Quando você habilita o suporte multissessão, o URL do console contém um subdomínio (por exemplo, `https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`). Atualize seus favoritos e os links do console.

> **Note**
>
> Você deve optar pelo suporte multissessão escolhendo Ativar multissessão no menu da conta do Console de gerenciamento da AWS, ou escolhendo Habilitar multissessão em https://console.aws.amazon.com/. Você pode optar desabilitar o suporte multissessão a qualquer momento escolhendo Desabilitar multissessão em https://console.aws.amazon.com/ ou limpando os cookies do navegador. A aceitação é específica do navegador.

Como fazer login em várias identidades

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, escolha o nome da conta.
3. Escolha Adicionar sessão e escolha Fazer login. Uma nova guia será aberta para você fazer login.

   > **Note**
   >
   > Consulte mais informações sobre como fazer login como usuário do IAM ou usuário-raiz em Fazer login no Console de gerenciamento da AWS no Guia do usuário de Login da AWS.

4. Insira suas credenciais.
5. Escolha Logon. As cargas do Console de gerenciamento da AWS nessa guia são a identidade da AWS escolhida.
6. (Opcional) Como fazer federação em perfis adicionais

   a. No portal de acesso do Centro de Identidade do AWS IAM ou no portal de autenticação única (SSO), faça login no perfil adicional.

   b. No Console de gerenciamento da AWS, escolha o nome da conta.

   c. Visualize as sessões adicionais que você pode escolher.

Ações Recomendadas pela AWS no Console de gerenciamento da AWS

As Ações Recomendadas pela AWS ajudam a trabalhar com mais eficiência no Console de gerenciamento da AWS fornecendo sugestões contextuais para concluir tarefas e implementar as práticas recomendadas. Quando há recomendações relevantes disponíveis, aparece um botão dinâmico que você pode usar para agir rapidamente com relação a essas sugestões.

> **Note**
>
> As Ações Recomendadas pela AWS analisam o estado do recurso para fornecer sugestões, mas não processam os dados do usuário.

Tópicos

Recursos das Ações Recomendadas pela AWS

- Recomendações de ação: receba sugestões relevantes com base no estado dos recursos, nas práticas recomendadas e nos padrões de uso comuns
- Ações com um clique: conclua as ações recomendadas diretamente pelas mensagens de sucesso ou visualizações de recursos
- Painel lateral direito integrado: acesse um painel lateral integrado para implementar sugestões sem interromper o fluxo de trabalho
- Suporte a vários serviços: receba recomendações em vários serviços da AWS

Usar ações recomendadas

Como usar ações recomendadas

1. Faça login no Console de gerenciamento da AWS

2. Procure o botão # Ações recomendadas.

> **Note**
>
> O botão de ações recomendadas pode aparecer em qualquer lugar do Console de gerenciamento da AWS e só pode ser acessado quando há ações recomendadas disponíveis.

3. Selecione o botão para visualizar as ações disponíveis.
4. Execute recomendações diretamente ou pelo painel lateral.

Registrando chamadas da API de ações AWS recomendadas usando AWS CloudTrail

AWS As ações recomendadas AWS CloudTrailsão integradas a um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura todas as chamadas de API para ações AWS recomendadas como eventos. As chamadas capturadas incluem chamadas de Console de gerenciamento da AWS e chamadas de código para as operações da API de ações AWS recomendadas. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita às Ações AWS Recomendadas, o endereço IP a partir do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

AWS Eventos de gerenciamento de ações recomendados em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

AWS As Ações Recomendadas registram todas as operações do plano de controle das Ações AWS Recomendadas como eventos de gerenciamento.

AWS Exemplos de eventos de ações recomendadas

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra um CloudTrail evento que demonstra a operação.


```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
```

```
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```


Para obter informações sobre o conteúdo do CloudTrail registro, consulte o conteúdo do CloudTrail registro no Guia AWS CloudTrail do usuário.

Usando AWS Console Home no Console de gerenciamento da AWS

Este tópico descreve como usar AWS Console Home, inclusive como personalizar a página inicial do console. Console Home é a página inicial do Console de gerenciamento da AWS. Na primeira vez que fizer login no console, você acessará a página inicial do console. Você pode personalizar a página inicial do console usando widgets e aplicações. Os widgets permitem que você adicione componentes personalizados que rastreiam informações sobre seus AWS serviços e recursos. Os aplicativos permitem que você agrupe seus AWS recursos e metadados. Você pode gerenciar as aplicações usando myApplications. Você também pode usar o Console Home para ver uma lista de todos os AWS serviços e conversar com o Amazon Q.

Tópicos

Visualizando todos os AWS serviços em AWS Console Home

Você pode ver uma lista de todos os AWS serviços e acessar seus consoles na Página inicial do console.

Para acessar uma lista completa de AWS serviços

1. Faça login no Console de gerenciamento da AWS.
2. Expanda o menu da página inicial do console escolhendo o ícone de hambúrguer (☰).
3. Selecione Todos os serviços.
4. Selecione um AWS serviço para navegar até seu console.

Trabalhando com widgets em AWS Console Home

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.

Gerenciar widgets

Para gerenciar os widgets, você pode realizar ações de adição, remoção, reorganização e redimensionamento. Os widgets padrão podem ser removidos e adicionados novamente. Você também pode restaurar o layout padrão da página inicial do console e solicitar novos widgets.

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 da página inicial do console.

Como remover um widget

1. Selecione o ícone de reticências, representado 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 da página 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 Console de gerenciamento da AWS.

Em que está MyApplications? AWS Console Home

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. As aplicações permitem o agrupamento de recursos e metadados. 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 Console de gerenciamento da AWS. 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.

Tópicos

Atributos do myApplications

- Criar aplicações: crie aplicações e organize os recursos. Seus aplicativos são exibidos automaticamente no MyApplications, para que você possa agir na Console de gerenciamento da AWS, APIs, 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.
- Acessar os recursos: é possível visualizar rapidamente os recursos da aplicação no menu Serviços selecionando a aplicação. Ao selecionar um recurso, você vai diretamente ao console do serviço em questão. Seu lugar na tabela de recursos é salvo, para que você possa continuar navegando a qualquer momento no menu Serviços.
- 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 CSPM 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 CSPM
- Systems Manager
- AWS Service Catalog
- Tags

Acessar o myApplications

É possível acessar o myApplications pelo Console de gerenciamento da AWS selecionando myApplications na barra lateral esquerda.

Preços

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 com myApplications

MyApplications está disponível da seguinte Regiões da AWS forma:

- Leste dos EUA (Ohio)
- Leste dos EUA (Norte 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 (Bahrein)
- Oriente Médio (Emirados Árabes Unidos)

- Israel (Tel Aviv)

Aplicações em myApplications

As aplicações permitem que você agrupe recursos e metadados. Você pode criar, integrar, visualizar, editar e excluir aplicações para gerenciá-las. Também é possível criar trechos de código para adicionar automaticamente novos recursos a uma aplicação.

> **Note**
>
> Você também pode adicionar aplicações aos seus Favoritos para facilitar o acesso. Para obter mais informações, consulte ???.

Tópicos

Criar aplicações em myApplications

Você pode criar uma aplicação ou the section called “Integrar aplicações” criadas antes de 8 de novembro de 2023 para começar a usar a extensão myApplications. Ao criar uma aplicação, você pode adicionar recursos pesquisando-os e selecionando-os ou usando etiquetas existentes.

Criar uma nova aplicação

1. Faça login no Console de gerenciamento da AWS.
2. Expanda a barra lateral esquerda e escolha myApplications.
3. Selecione 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. 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. Escolha Próximo.
9. (Opcional) Adicione recursos:

   Search and select resources

   > **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.

   Como adicionar recursos usando a pesquisa

   1. Escolha Pesquisar e selecionar recursos.
   2. Escolha Selecionar recursos.
   3. (Opcional) Selecione uma visualização.
   4. 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.

5. Marque a caixa de seleção ao lado dos usuários que você deseja adicionar.
6. Escolha Adicionar.
7. Escolha Próximo.
8. Revise as escolhas.

Automatically add resources using tags

Ao criar uma aplicação, você pode integrar recursos em massa especificando um par de chave/valor de etiqueta existente. Com esse método, aplica AWS automaticamente a `awsApplication` tag a todos os recursos marcados com o par de valores-chave especificado e cria uma sincronização de tags para os recursos do aplicativo por padrão. Com a sincronização de etiquetas ativada, todos os recursos marcados com o par de chave/valor de etiqueta especificado são adicionados automaticamente à aplicação. Para ter informações sobre como resolver erros de sincronização de etiquetas, consulte the section called “Resolver erros de sincronização de etiquetas em myApplications”.

> **Note**
>
> Adicionar recursos a um aplicativo usando tags requer permissões para criar um AppRegistry aplicativo, agrupar e desagrupar recursos e marcar e desmarcar recursos. Você pode adicionar a política `ResourceGroupsTaggingAPITagUntagSupportedResources` AWS gerenciada do Resource Groups ou criar e manter sua própria política personalizada. As seguintes permissões devem ser adicionadas à declaração de política de um usuário no IAM:
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

Como adicionar recursos usando etiquetas existentes

1. Escolha Adicione recursos automaticamente usando etiquetas.
2. Selecione a chave e o valor de uma etiqueta existente:

   a. Selecione o Perfil usado para marcar recursos. Para obter mais informações, consulte as permissões necessárias de sincronização de tags no AWS Service Catalog AppRegistry Administrator Guide.

   b. Selecione uma Chave de tag.

   c. Selecione um Valor de tag.

   d. (Opcional) Escolha Visualizar recursos para visualizar quais recursos estão marcados com o par de chave/valor da etiqueta.

   e. Confira e aceite o aviso Reconheço que o recurso Eventos do Ciclo de Vida do Grupo será habilitado para criar uma sincronização de etiquetas. O GLE AWS permite observar alterações nos recursos marcados com seu par de valores-chave.
3. Escolha Próximo.
4. Analise os detalhes da aplicação, o par de chave/valor da etiqueta selecionada e a pré-visualização dos recursos que serão adicionados à aplicação.

> **Note**
>
> Por padrão, criar uma aplicação usando um par de chave/valor de etiqueta existente cria uma sincronização de etiquetas. Após a configuração, a sincronização de etiquetas também gerencia continuamente os recursos da aplicação, adicionando ou removendo recursos à medida que são marcados ou desmarcados com o par de chave/valor especificado. Você pode gerenciar a sincronização de etiquetas na página Gerenciar recursos da aplicação.

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

> **Note**
>
> Adicionar uma 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 CloudFormation .

11. Selecione Criar aplicativo.

Integre AppRegistry aplicativos existentes em MyApplications

Você pode integrar um AppRegistry aplicativo existente criado antes de 8 de novembro de 2023 para começar a usar o MyApplications.

Para integrar um aplicativo existente AppRegistry

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

Visualizar aplicações em myApplications

Agora, você pode visualizar as aplicações em myApplications ou no menu de Serviços. Se estiver visualizando seus aplicativos em MyApplications, você poderá visualizá-los em todas as Regiões da AWS informações específicas Regiões da AWS e suas informações relevantes em uma visualização em cartão ou tabela.

> **Note**
>
> Você também pode visualizar as aplicações adicionados aos seus Favoritos no menu de favoritos. Para obter mais informações, consulte Favoritos no Console de gerenciamento da AWS.

myApplications

Como visualizar aplicações em myApplications

1. Abra a Console de gerenciamento da AWS.
2. Na barra lateral esquerda, selecione myApplications.
3. Em Regiões, selecione Região atual ou Regiões compatíveis.
4. Para encontrar uma aplicação específica, insira o nome, palavras-chave ou a descrição na barra de pesquisa.
5. (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. Escolha Confirmar.

Services menu

Como visualizar aplicações no menu Serviços

1. Abra a Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. Selecione Todas as aplicações.
4. Selecione uma aplicação.
5. (Opcional) Selecione uma exibição.
6. (Opcional) Selecione um filtro. É possível filtrar seus recursos por Propriedades ou por Tags. Consulte mais informações em Referência de sintaxe de consultas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de recursos da AWS .
7. (Opcional) Selecione um recurso para visualizá-lo no console de serviço relevante.

> **Tip**
>
> Você pode continuar navegando pelos recursos de onde parou, escolhendo Serviços (⁝⁝⁝). Seus filtros de pesquisa aplicados também são mantidos.

Editar aplicações em myApplications

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 Console de gerenciamento da AWS.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Selecione a aplicação que deseja editar.
4. No painel da extensão myApplications, selecione Ações e Editar aplicação.
5. Em Editar aplicação, faça as alterações desejadas na descrição, nas etiquetas e nos grupos de atributos da aplicação.

   > **Note**
   >
   > Para obter mais informações sobre o gerenciamento de tags e grupos de atributos, consulte Gerenciamento de tags e Edição de grupos de atributos no Guia AWS Service Catalog AppRegistry do administrador.

6. Selecione Atualizar.

Excluir aplicações em myApplications

É possível excluir aplicações, caso elas não sejam mais necessárias. Antes de excluir um aplicativo, certifique-se de remover todos os compartilhamentos de recursos e grupos de atributos associados que não foram criados por um AWS serviço.

> **Note**
>
> A exclusão de uma aplicação não afeta seus recursos. Os recursos marcados com a tag do AWS aplicativo permanecerão marcados.

Como excluir uma aplicação do

1. Abra a Console de gerenciamento da AWS.
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. Confirme a exclusão e escolha Excluir.

Criar trechos de código em myApplications

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 Console de gerenciamento da AWS.
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.

Recursos em myApplications

Em AWS, um recurso é uma entidade com a qual você pode trabalhar. Os exemplos incluem uma instância do Amazon EC2, uma AWS CloudFormation pilha ou um bucket do Amazon S3. Você pode gerenciar recursos em myApplications adicionando e removendo-os das aplicações.

Tópicos

Adicionar recursos em myApplications

Adicionar recursos às aplicações permite agrupá-los e gerenciar a segurança, a performance e a conformidade. Para adicionar recursos às aplicações existentes, você pode pesquisá-los e selecioná-los ou usar etiquetas existentes e executar uma sincronização de etiquetas.

Search and select resources

Como pesquisar e selecionar recursos

1. Abra a Console de gerenciamento da AWS.
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.

Automatically add resources using tags

Ao criar uma aplicação, você pode integrar recursos em massa especificando um par de chave/valor de etiqueta existente. Com esse método, aplica AWS automaticamente a `awsApplication` tag a todos os recursos e cria uma sincronização de tags para os recursos do aplicativo por padrão. Com a sincronização de etiquetas ativada, todos os recursos marcados com o par de chave/valor de etiqueta especificado são adicionados automaticamente à aplicação.

Como adicionar recursos usando etiquetas existentes

1. Abra a Console de gerenciamento da AWS.
2. Na barra lateral esquerda do console, selecione myApplications.
3. Selecione Gerenciar recursos.
4. Escolha Criar sincronização de tags.
5. Selecione a chave e o valor de uma etiqueta existente:
    a. Selecione o Perfil usado para marcar recursos. Para obter mais informações, consulte Permissões necessárias para tarefas de sincronização de tags no AWS Service Catalog AppRegistry Administrator Guide.
    b. Selecione uma Chave de tag.
    c. Selecione um Valor de tag.
    d. Confira e aceite o aviso Reconheço que o recurso Eventos do Ciclo de Vida do Grupo será habilitado para criar uma sincronização de etiquetas. O GLE AWS permite observar alterações nos recursos marcados com seu par de valores-chave.
6. Escolha Criar sincronização de tags.

Resolver erros de sincronização de etiquetas em myApplications

Esta seção descreve erros comuns de sincronização de etiquetas e como resolvê-los. Depois de tentar resolver o erro, você pode repetir a tarefa de sincronização de etiquetas que falhou.

- Permissões insuficientes: você não tem as permissões mínimas necessárias para iniciar, atualizar ou cancelar a sincronização de etiquetas. Consulte Tag-sync required permissions para ter mais

informações. Depois de garantir que o perfil especificado para realizar a sincronização de etiquetas tem as permissões mínimas necessárias, tente novamente a tarefa de sincronização de etiquetas que falhou.

- Já existe: já existe uma tarefa com esse par de chave/valor de etiqueta para essa aplicação. Uma aplicação pode oferecer suporte a mais de uma sincronização de etiquetas, mas cada sincronização de etiquetas deve ter um par de chave/valor de etiqueta diferente. Depois de especificar outro par de chave/valor de etiqueta, repita a tarefa de sincronização de etiquetas que falhou.
- Limite máximo atingido: você atingiu o máximo de 100 tarefas de sincronização de etiquetas por conta, em todas as aplicações.

Remover recursos em myApplications

É possível remover recursos para dissociá-los da aplicação.

Como remover recursos

1. Abra a Console de gerenciamento da AWS.
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.

Como visualizar recursos em myApplications

Agora, você pode visualizar recursos das aplicações em myApplications e no menu de Serviços.

myApplications

Como visualizar recursos em myApplications

1. Abra a Console de gerenciamento da AWS.
2. Expanda a barra lateral esquerda e escolha myApplications.
3. Selecione uma aplicação.
4. No widget Recursos, visualize seus recursos.

Services menu

Como visualizar aplicações no menu Serviços

1. Abra a Console de gerenciamento da AWS.
2. Na barra de navegação, escolha Serviços (⁝⁝⁝).
3. Selecione Todas as aplicações.
4. Selecione uma aplicação.
5. (Opcional) Selecione uma exibição.
6. (Opcional) Selecione um filtro. É possível filtrar seus recursos por Propriedades ou por Tags. Consulte mais informações em Referência de sintaxe de consultas de pesquisa do Explorador de Recursos no Guia do usuário do Explorador de recursos da AWS .
7. (Opcional) Selecione um recurso para visualizá-lo no console de serviço relevante.

> **Tip**
>
> Você pode continuar navegando pelos recursos de onde parou, escolhendo Serviços (⁝⁝⁝). Seus filtros de pesquisa aplicados também são mantidos.

Painel de controle MyApplications em AWS Console Home

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 obter mais informações, consulte Trabalhando com widgets em AWS Console Home.

Tópicos

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. FOr para obter mais informações, consulte Analisando seus custos Explorador de recursos da AWS no Guia AWS Cost Management do usuário.

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 obter mais informações, consulte AWS Security Hub CSPM.

Configurando o widget de AWS segurança

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

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

AWS Widget de resiliência

Esse widget exibe detalhes de resiliência do AWS Resilience Hub para seus aplicativos. Depois de iniciar uma avaliação, o AWS Resiliency Hub analisa a postura de resiliência de seus aplicativos avaliando seus recursos em relação a uma política de resiliência predefinida. Você pode acessar várias métricas, como pontuação de resiliência, violações de políticas, desvios de políticas, desvios de recursos e histórico de pontuação de resiliência. As aplicações são avaliadas diariamente para rastreamento aprimorado, mas você pode desabilitar esse recurso a qualquer momento. Para obter mais informações, consulte AWS Resilience Hub. Para obter informações sobre preços, consulte AWS Resilience Hub preços.

Configurando o widget de AWS resiliência

Para configurar o widget AWS de resiliência, adicione um aplicativo. Para obter mais informações, consulte O que é AWS Resilience Hub? no Guia do AWS Resilience Hub usuário.

Widget de recursos

Esse widget usa o AWS Resource Explorer para mostrar os recursos que você adicionou ao seu aplicativo em uma visualização. Você também pode usar esse widget para pesquisar ou filtrar seus recursos usando metadados de recursos, como nomes, tags e. IDs Para ter mais informações, consulte AWS Resource Explorer.

Configurar o widget de recursos

Para configurar o widget de recursos, faça a integração com o Explorador de Recursos. Para ter mais informações, consulte Getting started with Resource Explorer no Guia do usuário do Explorador de Recursos da AWS .

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 (SLOs) e métricas do nível de serviço do aplicativo
- 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 Ativar sinais 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.

Conversar com o Amazon Q Developer no AWS Console Home

O Amazon Q Developer é um assistente conversacional baseado em inteligência artificial (IA) generativa que pode ajudar você a entender, criar, estender e operar aplicações da AWS. Você pode fazer qualquer pergunta ao Amazon Q sobre a AWS, incluindo perguntas sobre arquitetura da AWS, recursos da AWS, práticas recomendadas, documentação e muito mais. Você também pode criar casos de suporte e receber assistência de um agente ao vivo. Para ter mais informações, consulte What is Amazon Q? no Guia do usuário do Amazon Q Developer.

Começar a usar o Amazon Q

Você pode começar a conversar com o Amazon Q no Console de gerenciamento da AWS, nos sites de documentação da AWS, nos sites da AWS ou no aplicativo móvel do Console da AWS, escolhendo o ícone hexagonal do Amazon Q. Para ter mais informações, consulte Get started with Amazon Q Developer no Guia do usuário do Amazon Q Developer.

Exemplos de perguntas

Veja alguns exemplos de perguntas que você pode fazer ao 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?`

Console de gerenciamento da AWS Acesso privado

Console de gerenciamento da AWS O Acesso Privado é um recurso de segurança avançado para controlar o acesso ao Console de gerenciamento da AWS. O Acesso Privado ao Console é útil quando você deseja impedir que os usuários façam login de forma inesperada em Contas da AWS de dentro da sua rede. Com esse recurso, você pode limitar o acesso Console de gerenciamento da AWS somente a um conjunto específico de dados conhecidos Contas da AWS quando o tráfego se origina de dentro da sua rede. O acesso privado do console também é útil quando você deseja garantir que todas as chamadas do Console de gerenciamento da AWS para sejam Serviços da AWS originadas de sua rede e de contas permitidas.

Tópicos

Compatível Regiões da AWS, consoles de serviço e recursos para acesso privado

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

As seguintes regiões e consoles de serviço são compatíveis.

Regiões aceitas

- Leste dos EUA (Ohio)
- Leste dos EUA (Norte 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 (Malásia)
- Ásia-Pacífico (Tailândia)
- 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)
- México (Centro)
- Europa (Milão)
- Europa (Espanha)
- Europa (Zurique)
- Oriente Médio (Bahrein)
- Oriente Médio (Emirados Árabes Unidos)

- Israel (Tel Aviv)

Consoles de serviço compatíveis

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- Gerenciamento de Faturamento e Custos da AWS
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer

- AWS Console Home
- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- 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
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- GameLift Servidores Amazon
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station

- Amazon GuardDuty
- Centro de Identidade do AWS IAM
- 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 Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- 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 Firewall
- AWS Network Manager
- OpenSearch Serviço Amazon
- AWS Organizations
- Autoridade de Certificação Privada da AWS
- Public Health Dashboard
- Amazon Rekognition

- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups e editor de tags
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver Firewall DNS
- Amazon S3 on Outposts
- Amazon SageMaker
- Amazon SageMaker Runtime
- Dados sintéticos da Amazon SageMaker AI
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- Suporte
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- Configurações unificadas
- IP Address Manager da Amazon VPC
- Amazon Virtual Private Cloud

- Cliente Amazon WorkSpaces Thin

Visão geral dos controles de segurança de acesso Console de gerenciamento da AWS privado

Restrições de conta na Console de gerenciamento da AWS da sua rede

Console de gerenciamento da AWS O acesso privado é útil em cenários em que você deseja limitar o acesso ao Console de gerenciamento da AWS 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 Console de gerenciamento da AWS . Para obter 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 Console de gerenciamento da AWS, 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 Console de gerenciamento da AWS, consulte. Solução de problemas

> **Note**
>
> Atualmente, o Console de gerenciamento da AWS 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

Console de gerenciamento da AWS O acesso privado exige os dois VPC endpoints a seguir por região. *`region`*Substitua por suas próprias informações de região.

1. com.amazonaws. *`region`*.console para Console de gerenciamento da AWS
2. com.amazonaws. *`region`*.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 Console de gerenciamento da AWS. 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 as opções de conectividade da Amazon VPC-to-Amazon VPC no whitepaper Opções de conectividade da Amazon Virtual Private Cloud.

Tópicos

DNSconfiguração para Console de gerenciamento da AWS 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 Console de gerenciamento da AWS. 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:

- fazer login
  - *`region`*.signin.aws.amazon.com apontando para o Início de Sessão da AWS VPC endpoint na zona de login onde está a região desejada DNS *`region`*

- signin.aws.amazon.com apontando para o endpoint VPC de AWS login no Leste dos EUA (Norte da Virgínia) (us-east-1)

- Console
  - *region*.console.aws.amazon.com apontando para o Console de gerenciamento da AWS VPC endpoint na zona do console onde está a região desejada DNS *region*
  - *. *region*.console.aws.amazon.com apontando para o Console de gerenciamento da AWS VPC endpoint na zona do console onde está a região desejada DNS *region*
  - *. *region*.console.aws.amazon.com apontando para o VPC endpoint na zona do console Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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-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 Console de gerenciamento da AWS . Para manter as zonas hospedadas privadas atualizadas, extraia periodicamente a lista de arquivos anterior.

Se você usa o Route 53 para configurar seuDNS, acesse https://console.aws.amazon.com/route53/ v2/hostedzones# para verificar a configuração. 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*.console.aws.amazon.com
- *. *region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- Registros adicionais presentes nos arquivos JSON listados anteriormente

Endpoints de VPC e DNS configuração para AWS serviços no Console de gerenciamento da AWS

As Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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-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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS privado para limitar o conjunto de contas que têm permissão para usá-las de dentro Console de gerenciamento da AWS de sua VPC e de suas redes locais conectadas.

Tópicos

Usando o acesso Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS privado.

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

```
  "Resource": "*"
}
```

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

Permitir o Console de gerenciamento da AWS uso somente para contas e organizações esperadas (identidades confiáveis)

Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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.

JSON

```
{
  "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.

JSON

```
{
  "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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS Privado.

Chaves de contexto de condição AWS global suportadas

Console de gerenciamento da AWS 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 Console de gerenciamento da AWS .

Como o Console de gerenciamento da AWS Private Access funciona com a AWS: SourceVpc

Esta seção descreve os vários caminhos de rede que as solicitações geradas por você Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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. Console de gerenciamento da AWS 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 Console de gerenciamento da AWS privado. Esta seção fornece detalhes sobre como os diferentes caminhos de rede funcionam.

Depois que um usuário faz login no Console de gerenciamento da AWS, 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS . A `aws:SourceVpce` condição será definida para o respectivo endpoint VPC de login ou console. IDs

> **Note**
>
> Se os usuários precisarem acessar os consoles de serviço que não são compatíveis com o Acesso Privado ao Console de gerenciamento da AWS , 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 Console de gerenciamento da AWS são refletidos no histórico de CloudTrail eventos.

Para solicitações diretas do navegador, usar o Acesso Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS privado

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

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

Tópicos

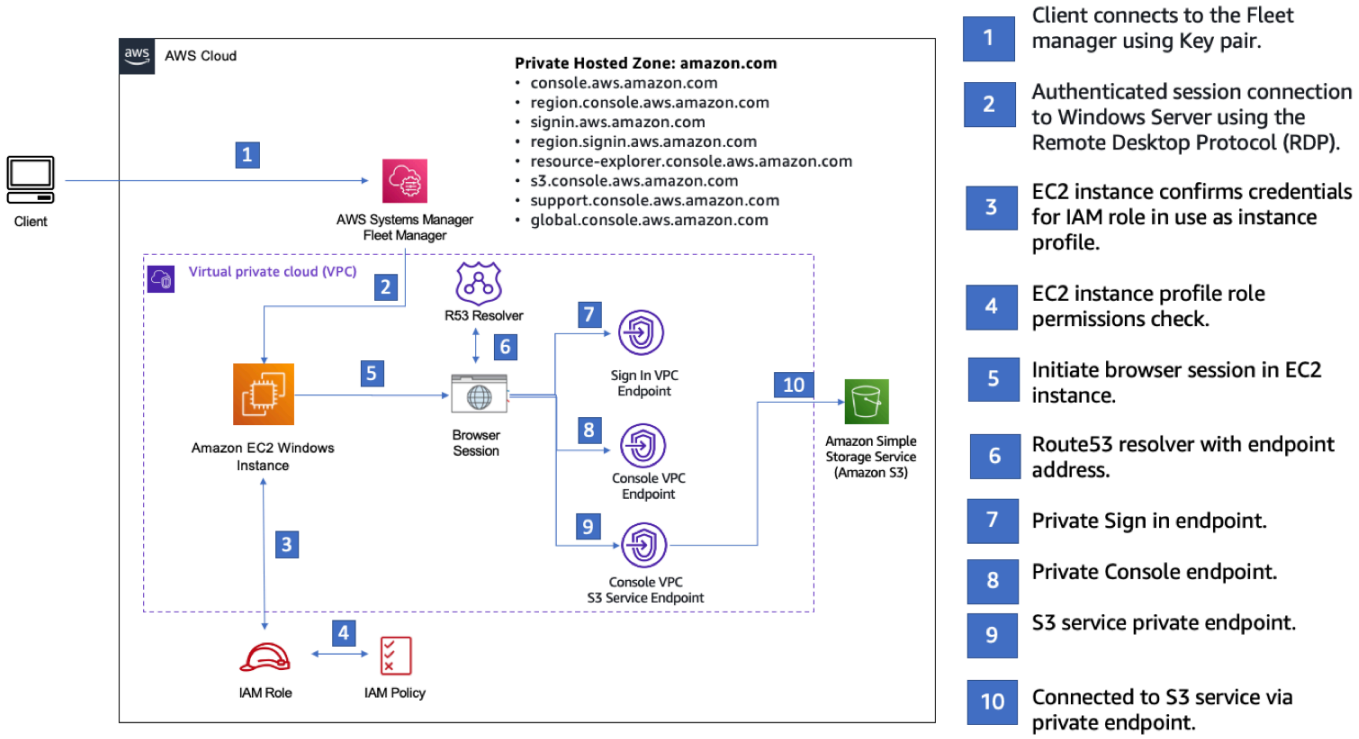
- Configuração de teste com o Amazon EC2
- Configuração de teste com a Amazon WorkSpaces
- Testar a configuração da VPC com políticas do IAM

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 Console de gerenciamento da AWS privado ao Amazon Simple Storage Service a partir de uma instância do Amazon EC2. Este tutorial é usado 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 Console de gerenciamento da AWS por meio do Amazon EC2. Mostra como um usuário está conectado ao Amazon S3 usando um endpoint privado.



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

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

Console de gerenciamento da AWS Modelo do Amazon 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: 't3.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

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "*.widget.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

 ConsoleRecordRegionalMultiSession:
   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 CloudFormation.
2. Selecione Criar pilha.
3. Escolha With new resources (standard) (Com novos recursos [padrão]). Faça upload do arquivo de 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 ter 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

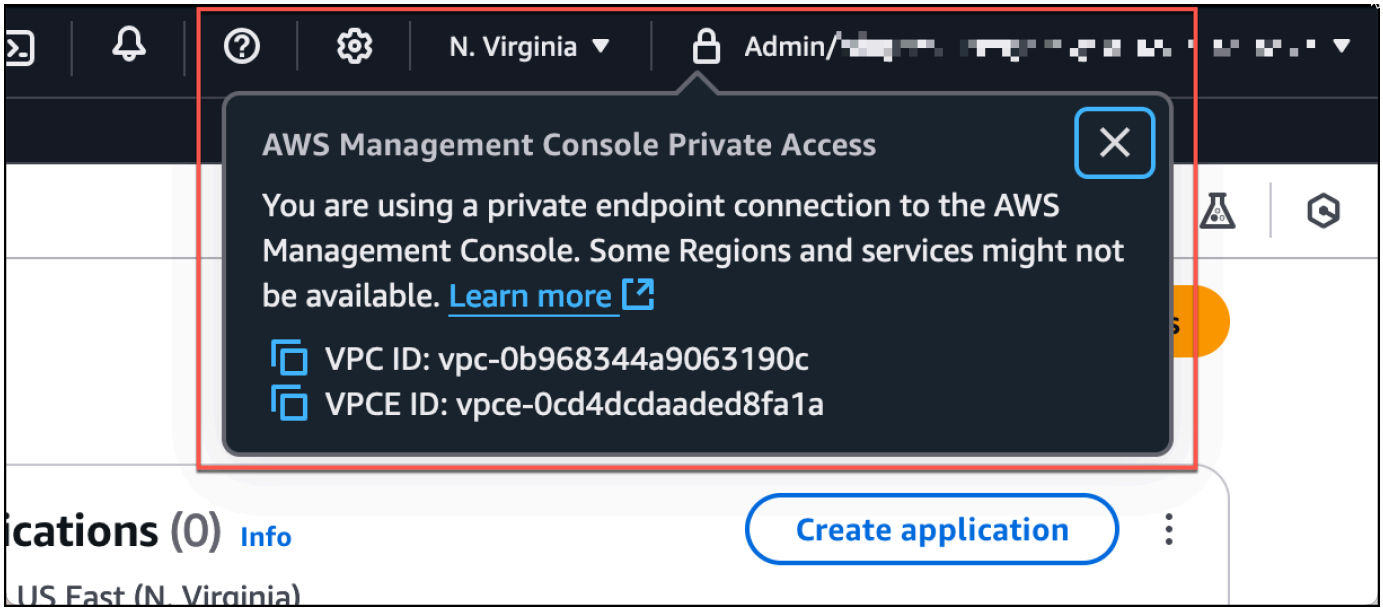
1. Faça login na conta de gerenciamento da organização e abra o console do Amazon EC2.
2. No painel de navegação, escolha Instâncias.
3. Na página Instâncias, selecione a instância de teste do Console VPCE que foi criada pelo CloudFormation modelo. Depois, escolha Conectar.

> **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 CloudFormation criar o modelo.
7. Na instância Windows do Amazon EC2, abra o Console de gerenciamento da AWS no navegador.
8. Depois de fazer login com suas AWS credenciais, abra o console do Amazon S3 e verifique se você está conectado Console de gerenciamento da AWS usando o Private Access.

Para testar a configuração do Acesso Console de gerenciamento da AWS 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.



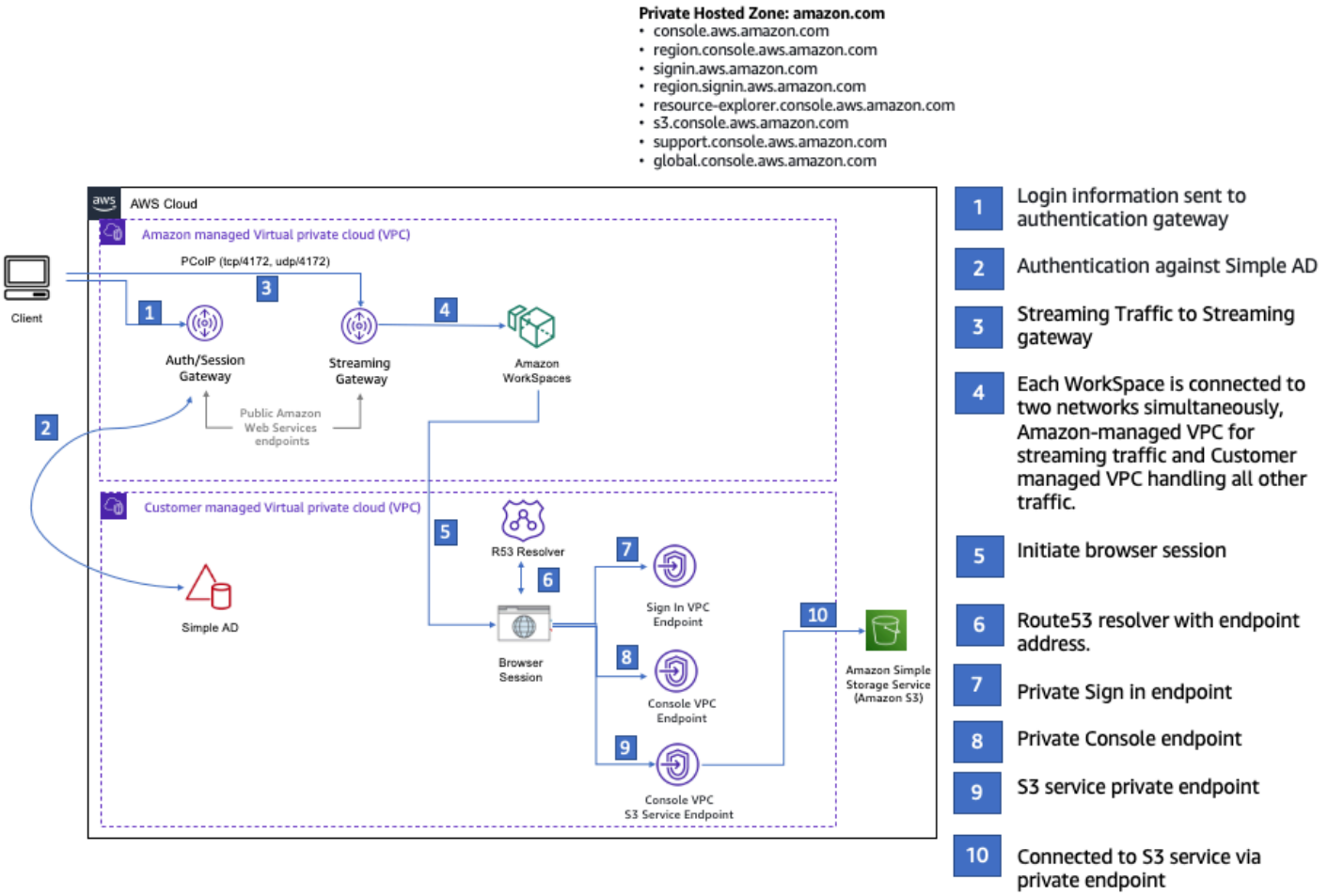
Configuração de teste com a Amazon WorkSpaces

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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS o.

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



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

Console de gerenciamento da AWS 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

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# 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

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref "ConsoleHostedZone"
      Name: "*.widget.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

  ConsoleRecordRegionalMultiSession:
    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: !Ref DSAdminPasswordResourceName
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    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
```

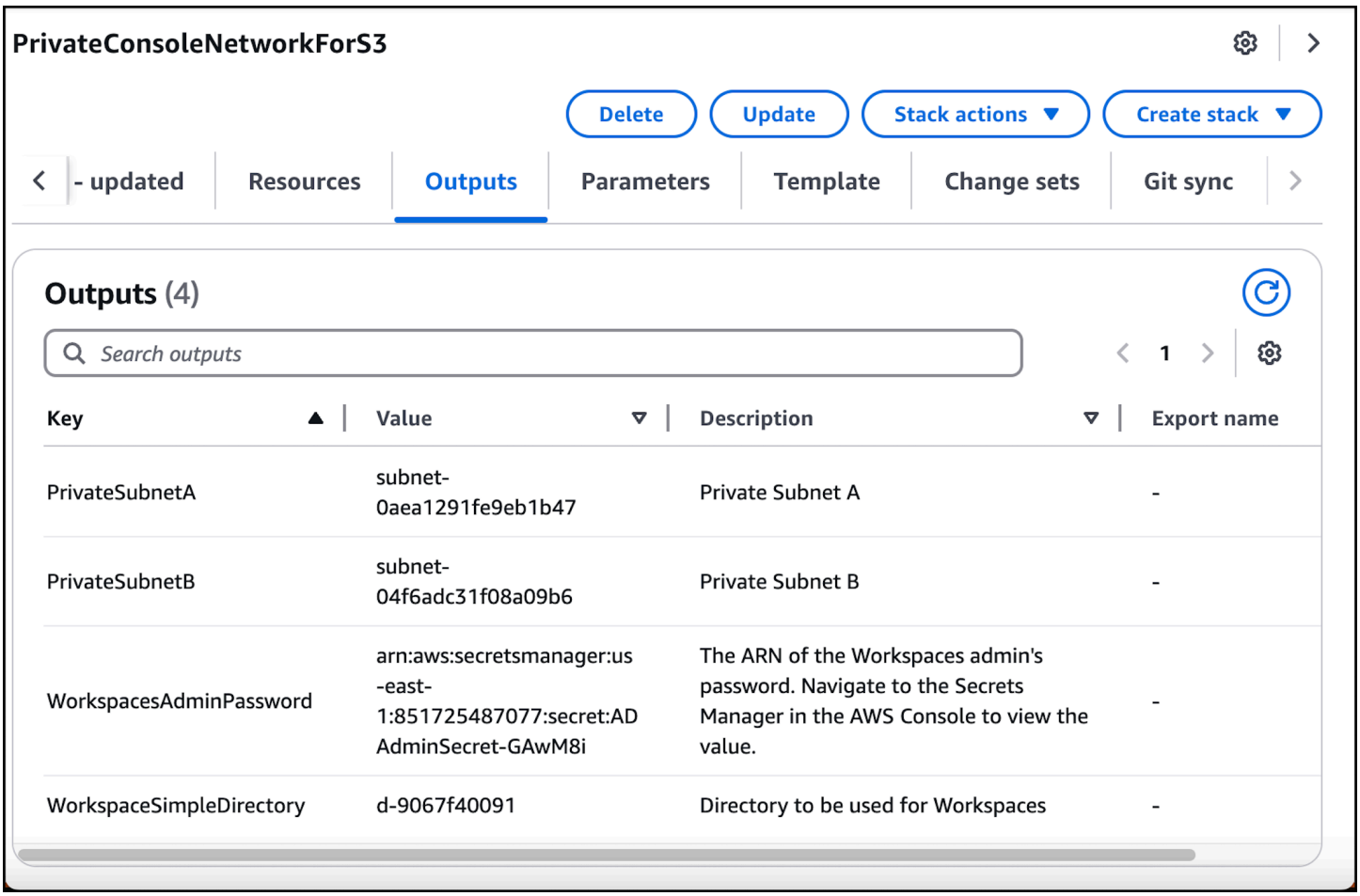
> **Note**
>
> Essa configuração de teste foi projetada para ser executada na região Leste dos EUA (Norte da Virgínia) (us-east-1).

Para configurar uma rede

1. Faça login na conta de gerenciamento da organização e abra o console do CloudFormation.
2. Selecione Criar pilha.
3. Escolha With new resources (standard) (Com novos recursos [padrão]). Faça upload do arquivo de 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.

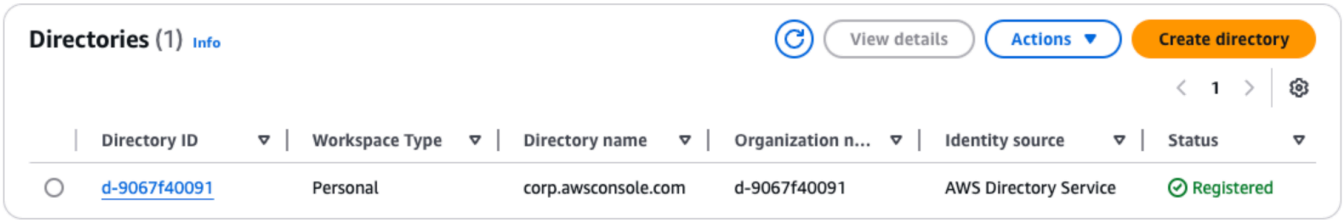
A captura de tela a seguir mostra a visualização da guia Saídas exibindo os valores das sub-redes privadas e do Workspace Simple Directory.



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 do 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 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. Escolha 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 Console de gerenciamento da AWS Privado.

Para acessar um WorkSpace

1. Abra o e-mail que você recebeu na etapa 14 do procedimento anterior.

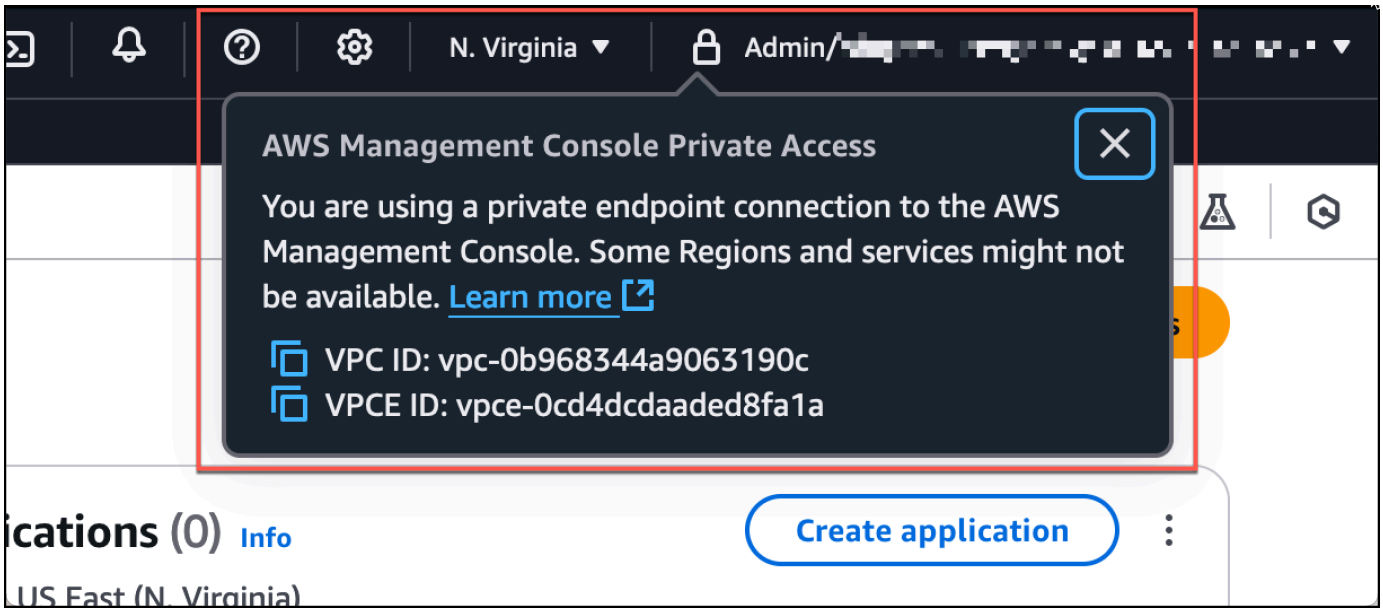
2. No e-mail, escolha o link exclusivo fornecido para configurar seu perfil e baixar o WorkSpaces cliente.
3. Defina a senha.
4. Baixe o cliente de sua escolha.
5. Instale e inicie o cliente. Insira o código de registro fornecido no e-mail e escolha Registrar.
6. Faça login na Amazon WorkSpaces usando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

Para testar a configuração do Acesso Console de gerenciamento da AWS Privado

1. Do seu WorkSpace, abra seu navegador. Depois, navegue até o Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

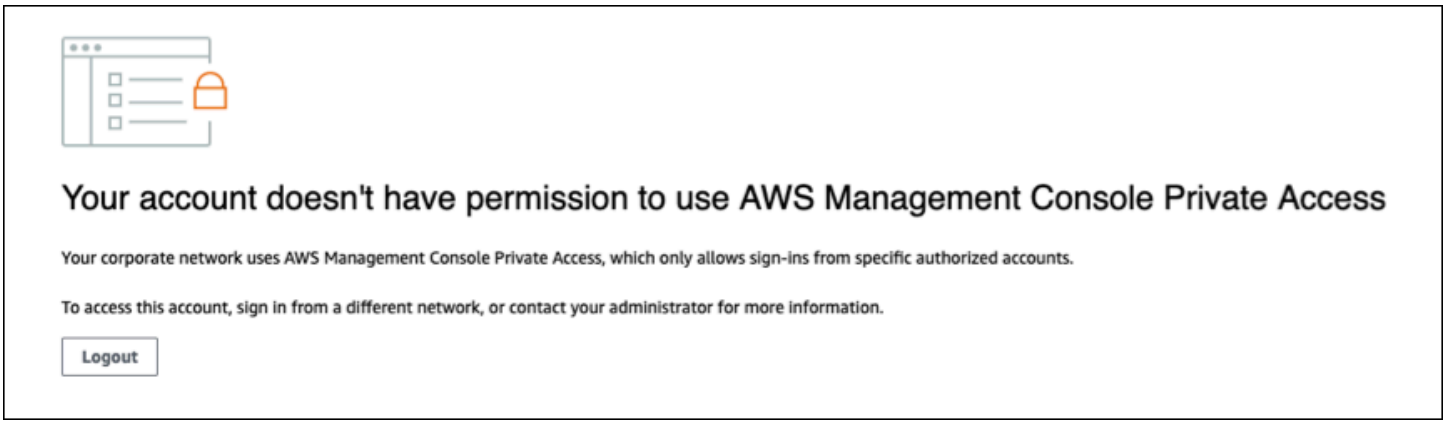
A política a seguir limita o login aos selecionados Conta da AWS IDs usando uma política de acesso Console de gerenciamento da AWS privado para o endpoint de login.

JSON

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

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

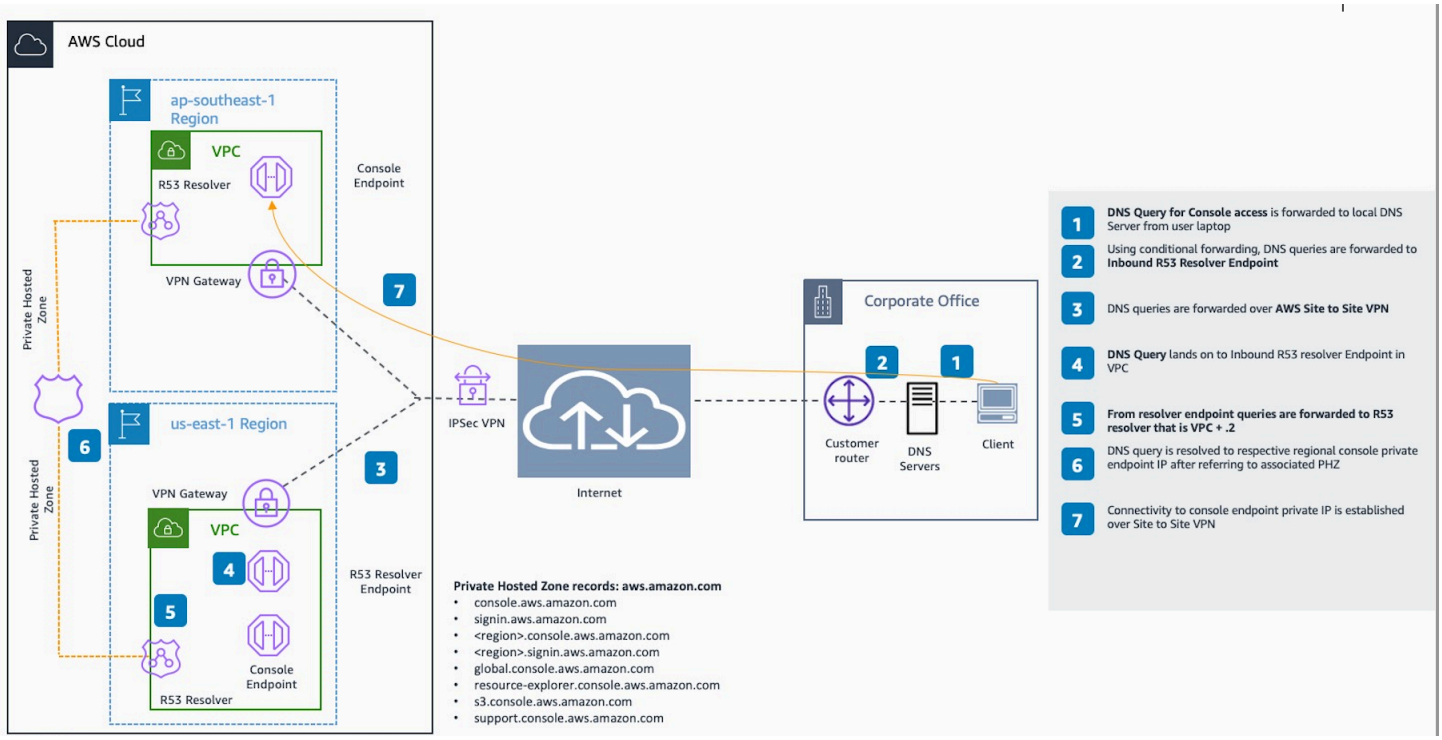
Se você se conectar com uma identidade que não pertence à sua conta, a página de erro a seguir será exibida.



Arquitetura de referência

Para se conectar de forma Console de gerenciamento da AWS 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 AWS VPN Site-to-Site no Guia do Usuário da VPN.AWS Site-to-Site 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS, eles são roteados para a área Console de gerenciamento da AWS privada dos endpoints de acesso privado. IPs

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

AWS Personalização da experiência do usuário (UXC)

AWS A personalização da experiência do usuário permite que você personalize suas AWS interfaces para atender às suas necessidades específicas e melhorar a eficiência. Atualmente, o UXC oferece um recurso de personalização de cores da conta para administradores de contas. Esse recurso permite que os administradores definam uma cor para uma conta, dependendo do agrupamento necessário. Por exemplo, um administrador pode atribuir vermelho a todas as contas de produção, amarelo a todas as contas de teste e verde a todas as contas de desenvolvedor. Os benefícios da personalização de cores de conta incluem:

- Identificar visualmente os tipos de conta com rapidez
- Reduzir os riscos de fazer alterações em contas erradas
- Agrupar contas semelhantes (de produção, teste, desenvolvimento)

Como acessar o User Experience Customization

É possível acessar o UXC na página da conta no Console de gerenciamento da AWS. Consulte mais informações sobre como acessar essa página em ???.

Introdução à personalização da experiência AWS do usuário

Os administradores podem definir cores para AWS contas diferentes. As cores de conta tornam mais fácil distinguir as contas que estão conectadas no momento. As organizações podem usar cores de conta para distinguir entre diferentes tipos de contas, por exemplo, usar verde para contas de desenvolvimento, amarelo para contas de teste e vermelho para contas de produção.

> **Note**
>
> Recursos essenciais para o Console de gerenciamento da AWS, como a personalização da experiência AWS do usuário e o Amazon Q, exigem permissões apropriadas do IAM. AWS CloudShell AWS as políticas gerenciadas fornecem uma maneira conveniente de conceder essas permissões aos usuários e funções usados no Console de gerenciamento da AWS. As seguintes políticas gerenciadas estão disponíveis para uso:
>
> - `AWSManagementConsoleBasicUserAccess`
>   - Para usuários não administrativos

- Concede acesso aos recursos básicos do console
- `AWSManagementConsoleAdministratorAccess`
  - Para usuários administrativos
  - Fornece acesso a Console de gerenciamento da AWS recursos essenciais
  - Permite que os administradores configurem e personalizem o Console de gerenciamento da AWS para outras identidades

Para obter mais informações, consulte ???.

Como definir cor de uma conta

1. Faça login no Console de gerenciamento da AWS.
2. Na barra de navegação, selecione o nome da conta.
3. Escolha Conta.
4. Em Configurações de exibição da conta, escolha uma cor.
5. Selecione Atualizar.

Referência da API

A Referência da API de Personalização da Experiência AWS do Usuário fornece descrições, parâmetros de solicitação da API e a resposta JSON para cada uma das ações da API de Personalização da Experiência AWS do Usuário.

Tópicos

Ações

As ações a seguir são compatíveis:

- ???
- ???

- ???

GetAccountColor

Obtém a cor associada à conta.

Sintaxe da solicitação

```
GET /v1/account-color HTTP/1.1
```

Essa solicitação não usa parâmetros de URI nem inclui corpo.

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
    "color": "string"
}
```

Elementos de resposta

color

A cor associada à conta.

Tipo: string

Valores válidos: none | pink | purple | darkBlue | lightBlue | teal | green | yellow | orange | red

Erros

Consulte informações sobre os erros comuns de todas as ações em Erros comuns.

AccessDeniedException

O usuário não tem acesso suficiente para executar esta ação.

Código de status HTTP: 403

InternalServerException

Erro inesperado durante o processamento da solicitação.

Código de status HTTP: 500

ThrottlingException

A solicitação foi negada devido ao controle de utilização da solicitação.

Código de status HTTP: 429

ValidationException

Essa exceção é lançada quando o evento de notificação falha na validação.

Código de status HTTP: 400

DeleteAccountColor

Exclui a configuração de cor da conta.

Sintaxe da solicitação

```
DELETE /v1/account-color HTTP/1.1
```

Parâmetros da solicitação

Essa operação não usa parâmetros de solicitação.

Corpo da Solicitação

Essa operação não tem um corpo de solicitação.

Corpo da resposta

Essa operação não retorna um corpo de resposta.

Erros

Consulte informações sobre os erros comuns de todas as ações em Erros comuns.

AccessDeniedException

O usuário não tem acesso suficiente para executar esta ação.

Código de status HTTP: 403

InternalServerException

Erro inesperado durante o processamento da solicitação.

Código de status HTTP: 500

ThrottlingException

A solicitação foi negada devido ao controle de utilização da solicitação.

Código de status HTTP: 429

ValidationException

Essa exceção é lançada quando o evento de notificação falha na validação.

Código de status HTTP: 400

PutAccountColor

Define a cor associada à conta.

Sintaxe da solicitação

```
PUT /v1/account-color HTTP/1.1
```

Corpo da Solicitação

```
Content-type: application/json

{
   "color": "string"
}
```

Sintaxe da resposta

```
HTTP/1.1 200
Content-type: application/json

{
    "color": "string"
```

```
}
```

Elementos de resposta

color

A cor associada à conta.

Tipo: string

Valores válidos: none | pink | purple | darkBlue | lightBlue | teal | green | yellow | orange | red

Erros

Consulte informações sobre os erros comuns de todas as ações em Erros comuns.

AccessDeniedException

O usuário não tem acesso suficiente para executar esta ação.

Código de status HTTP: 403

InternalServerException

Erro inesperado durante o processamento da solicitação.

Código de status HTTP: 500

ThrottlingException

A solicitação foi negada devido ao controle de utilização da solicitação.

Código de status HTTP: 429

ValidationException

Essa exceção é lançada quando o evento de notificação falha na validação.

Código de status HTTP: 400

Erros comuns

Os erros a seguir são comuns às ações de API de todos os AWS serviços. Consulte os erros específicos de uma ação de API na documentação sobre a ação em questão.

AccessDeniedException

Você não tem acesso suficiente para executar essa ação.

Código de status HTTP: 403

Para obter mais informações, consulte Solução de problemas de erros de acesso negado.

ExpiredTokenException

O token de segurança incluído na solicitação está expirado.

Código de status HTTP: 403

IncompleteSignature

A assinatura da solicitação não está em conformidade com os AWS padrões.

Código de status HTTP: 403

InternalFailure

O processamento da solicitação falhou por causa de um erro, uma exceção ou uma falha desconhecida.

Código de status HTTP: 500

MalformedHttpRequestException

Há problemas com a solicitação no nível HTTP. Por exemplo, não conseguimos descompactar o corpo de acordo com o algoritmo de descompactação especificado pela codificação de conteúdo.

Código de status HTTP: 400

NotAuthorized

Você não tem permissão para realizar esta ação.

Código de status HTTP: 401

OptInRequired

O ID da chave de AWS acesso precisa de uma assinatura para o serviço.

Código de status HTTP: 403

RequestAbortedException

A solicitação foi anulada antes que uma resposta fosse enviada de volta (por exemplo, o cliente fechou a conexão).

Código de status HTTP: 400

RequestEntityTooLargeException

Há problemas com a solicitação no nível HTTP. A entidade de solicitação é muito grande.

Código de status HTTP: 413

RequestExpired

A solicitação chegou ao serviço mais de 15 minutos após o carimbo de data na solicitação ou mais de 15 minutos após a data de expiração da solicitação (como para pré-assinada URLs), ou o carimbo de data na solicitação é mais de 15 minutos no futuro.

Código de status HTTP: 400

RequestTimeoutException

Há problemas com a solicitação no nível HTTP. A leitura da solicitação atingiu o tempo limite.

Código de status HTTP: 408

ServiceUnavailable

Falha na solicitação devido a um erro temporário do servidor.

Código de status HTTP: 503

ThrottlingException

A solicitação foi negada devido à limitação da solicitação.

Código de status HTTP: 400

UnrecognizedClientException

O certificado X.509 ou ID da chave de AWS acesso fornecido não existe em nossos registros.

Código de status HTTP: 403

UnknownOperationException

A ação ou operação solicitada é inválida. Verifique se a ação foi digitada corretamente.

Código de status HTTP: 404

ValidationError

A entrada não satisfaz as restrições especificadas por um AWS serviço.

Código de status HTTP: 400

Registrando chamadas da API de personalização da experiência do AWS usuário usando AWS CloudTrail

AWS A personalização da experiência do usuário é integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura todas as chamadas de API para UXC como eventos. As chamadas capturadas incluem as aquelas do UXC console e chamadas de código para operações de API do UXC. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à UXC, o endereço IP a partir do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

Eventos de gerenciamento de UXC em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

AWS A personalização da experiência do usuário registra todas as operações do plano de controle UXC como eventos de gerenciamento. Para obter uma lista das operações do plano de controle da Personalização da Experiência AWS do Usuário nas quais o UXC se registra CloudTrail, consulte a Referência da API de Personalização da Experiência AWS do Usuário.

Exemplos de evento do UXC

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra um CloudTrail evento que demonstra a operação.


```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
```

```
  "eventType" : "AwsApiCall",
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```

Para obter informações sobre o conteúdo do CloudTrail registro, consulte o conteúdo do CloudTrail registro no Guia AWS CloudTrail do usuário.

AWS políticas gerenciadas para o Console de gerenciamento da AWS

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para saber mais, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

AWS política gerenciada: AWSManagement ConsoleBasicUserAccess

Você pode anexar `AWSManagementConsoleBasicUserAccess` aos seus usuários, grupos e funções.

Essa política concede as permissões necessárias para usuários não administrativos do Console de gerenciamento da AWS. Isso inclui recursos como descoberta de recursos, notificações, acesso ao shell baseado em navegador e navegação personalizada.

Detalhes das permissões

Esse `AWSManagementConsoleBasicUserAccess` é agrupado nos seguintes conjuntos de permissões:

- `cloudshell`— permite que os diretores tenham acesso total aos AWS CloudShell recursos, incluindo criação de ambiente, gerenciamento de sessões e execução de comandos.
- `ec2`: permite que as entidades principais descrevam as regiões habilitadas para a conta na Navegação Unificada.
- `notifications`— Permite que os diretores obtenham eventos de Notificações de Usuários da AWS.
- `q`: permite que as entidades principais conversem com o Amazon Q Developer.
- `resource-explorer-2`— Permite que os diretores pesquisem e descubram AWS recursos usando a Pesquisa Unificada.
- `uxc`— Permite que os diretores leiam as configurações de personalização da experiência AWS do usuário.
- `action-recommendations`— Permite que os diretores recebam recomendações de ações contextuais.
- `account`— permite que os diretores recuperem informações sobre a conta especificada, incluindo nome da conta, ID da conta e data e hora de criação da conta.

Para visualizar as permissões para esta política, consulte AWSManagementConsoleBasicUserAccess na Referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AWSManagement ConsoleAdministratorAccess

Você pode anexar `AWSManagementConsoleAdministratorAccess` aos seus usuários, grupos e funções.

Essa política concede acesso total para configurar e personalizar o Console de gerenciamento da AWS. Ela permite que os administradores definam as cores de contas, habilitem notificações

de usuários e configurem a descoberta de recursos. Também inclui permissões da política gerenciada `AWSManagementConsoleBasicUserAccess`, que são essenciais para usuários não administrativos do Console de gerenciamento da AWS.

Detalhes das permissões

Esse `AWSManagementConsoleAdministratorAccess` é agrupado nos seguintes conjuntos de permissões:

- `cloudshell`— permite que os diretores tenham acesso total aos AWS CloudShell recursos, incluindo criação de ambiente, gerenciamento de sessões e execução de comandos.
- `ec2`: permite que as entidades principais descrevam as regiões habilitadas para a conta na Navegação Unificada.
- `notifications`: permite que as entidades principais acessem e atualizem configurações de notificação, eventos e status de aceitação de recursos.
- `q`: permite que as entidades principais conversem com o Amazon Q Developer para suporte assistido por IA.
- `resource-explorer-2`— Permite que os diretores pesquisem e descubram AWS recursos usando a Pesquisa Unificada.
- `uxc`— Permite que os diretores tenham acesso total às configurações de personalização da experiência AWS do usuário.
- `action-recommendations`— Permite que os diretores recebam recomendações de ações contextuais.
- `account`— permite que os diretores recuperem informações sobre a conta especificada, incluindo nome da conta, ID da conta e data e hora de criação da conta.

Para visualizar as permissões para esta política, consulte AWSManagementConsoleAdministratorAccess na Referência de políticas gerenciadas pela AWS .

Console de gerenciamento da AWS atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas Console de gerenciamento da AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do Console de gerenciamento da AWS documento.

Alteração	Descrição	Data
AWSManagementConsoleBasicUserAccess: política atualizada	Política atualizada para adicionar permissões para permitir que os usuários vejam as informações da conta e recebam recomendações de ações enquanto navegam no Console de gerenciamento da AWS.	9 de dezembro de 2025
AWSManagementConsoleAdministratorAccess: política atualizada	Política atualizada para adicionar permissões para permitir que os usuários vejam as informações da conta e recebam recomendações de ações enquanto navegam no Console de gerenciamento da AWS.	9 de dezembro de 2025
AWSManagementConsoleBasicUserAccess – Nova política	Foi adicionada uma nova política AWS gerenciada que concede as permissões necessárias para Console de gerenciamento da AWS navegação básica, visualização de cores da conta e descoberta de recursos.	14 de agosto de 2025
AWSManagementConsoleAdministratorAccess – Nova política	Foi adicionada uma nova política AWS gerenciada que fornece acesso total para	14 de agosto de 2025

Alteração	Descrição	Data
	configurar e personalizar Console de gerenciamento da AWS o.	
Console de gerenciamento da AWS começou a rastrear as alterações	Console de gerenciamento da AWS começou a rastrear as mudanças em suas políticas AWS gerenciadas.	14 de agosto de 2025

Usar o Markdown no console

Alguns serviços do Console de gerenciamento da AWS, 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 Console de gerenciamento da AWS o.

Você também pode diagnosticar e solucionar erros comuns em alguns AWS serviços usando o Amazon Q Developer. Para ter mais informações, consulte Diagnose common errors in the console with Amazon Q Developer no Guia do usuário do Amazon Q Developer.

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, ou com ou sem uma VPN, ou tente usar outro navegador da web.
- Se todos os usuários afetados forem da mesma equipe, poderá se tratar de um problema na extensão de privacidade para navegadores ou no firewall de segurança. Extensões de privacidade para navegadores ou firewalls de segurança podem bloquear o acesso aos domínios usados pelo Console de gerenciamento da AWS. 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS

Alterações recentes feitas no console poderão afetar o acesso se todas as condições a seguir forem atendidas:

- Você acessa Console de gerenciamento da AWS de uma rede configurada para alcançar endpoints de AWS serviço por meio de VPC endpoints.
- Você restringe o acesso aos AWS serviços usando uma chave `aws:SourceIp` de condição `aws:SourceVpc` global em suas políticas do IAM.

Recomendamos que você revise as políticas do IAM que contêm a chave de condição global `aws:SourceIp` ou `aws:SourceVpc`. Aplique `aws:SourceIp` e `aws:SourceVpc` sempre que aplicável.

Alguns Console de gerenciamento da AWS recursos usam domínios de pilha dupla que oferecem suporte a conexões e ambas. IPv4 IPv6 Se sua política do IAM restringir o acesso usando `aws:SourceIp` apenas blocos IPv4 CIDR, as solicitações poderão falhar quando seu sistema operacional preferir IPv6 conexões (ou vice-versa). Para evitar isso, inclua ambos os blocos IPv4 e

IPv6 CIDR em sua `aws:SourceIp` condição. Para obter mais informações, consulte aws: SourceIp no Guia AWS Identity and Access Management do usuário.

Você também pode integrar o recurso de acesso Console de gerenciamento da AWS privado para acessá-lo Console de gerenciamento da AWS por meio de um VPC endpoint e `aws:SourceVpc` usar as condições em suas políticas. Para saber mais, consulte:

- Console de gerenciamento da AWS Acesso privado
- the section called “Como o Console de gerenciamento da AWS Private Access funciona com a AWS: SourceVpc”
- the section called “Chaves de contexto de condição AWS global suportadas”

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

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. Console de gerenciamento da AWS Para fazer login em uma região diferente, especifique um endpoint regional alternativo na URL. Console de gerenciamento da AWS 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.console.aws.amazon.com
```

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

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

Quero alterar o idioma do, Console de gerenciamento da AWS mas não consigo encontrar o menu de seleção de idioma 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 Console de gerenciamento da AWS, navegue até a página Configurações Unificadas e escolha o idioma do console.

Para obter mais informações, consulte Alterar o idioma do Console de gerenciamento da AWS.

Histórico do documento

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

Alteração	Descrição	Data
Página adicionada	Nova página adicionad a para explicar as ações recomendadas. Para obter mais informações, consulte ???.	15.º de outubro de 2025
Novas políticas gerenciadas pela AWS	Adição de duas novas políticas às permissões de escopo para usar, configurar e personalizar o Console de gerenciamento da AWS. • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	14 de agosto de 2025
User Experience Customizations (UXC)	Novo serviço disponível.	14 de agosto de 2025
Página atualizada	Agora, você pode visualizar as aplicações em myApplications no menu de Serviços. Para obter mais informações, consulte ???.	29 de julho de 2025
Página adicionada	Nova página adicionada para explicar o recurso de multisessão. Para obter mais informações, consulte ???.	06 de dezembro de 2024

Alteração	Descrição	Data
Página atualizada	Atualização da página de alteração da senha. Para obter mais informações, consulte ???.	18 de junho de 2024
Novas páginas adicionadas	Adição de novas páginas para descrever como acessar o menu Serviços e as notificaç ões de eventos da AWS. Para obter mais informações, consulte ??? e ???.	18 de junho de 2024
Página atualizada	Atualização da página “What is the Console de gerenciam ento da AWS?”. Para obter mais informações, consulte ???.	18 de junho de 2024
Obter suporte	Uma nova página foi adicionada para descrever como obter suporte. Para obter mais informações, consulte ???.	18 de junho de 2024
Navegação unificada e AWS Console Home	Adição de novas páginas para descrever como trabalhar com o console. Para obter mais informações, consulte ??? e ???.	18 de junho de 2024

Alteração	Descrição	Data
Conversar com o Amazon Q	Nova página de configurações detalhando como os usuários podem fazer perguntas sobre a AWS ao Amazon Q Developer. Para ter mais informações, consulte Chat with Amazon Q Developer.	29 de maio de 2024
myApplications	Nova página que apresenta myApplications. Para ter 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 interface de usuário do AWS Console Home	Nova interface de usuário do AWS Console Home, que inclui widgets para exibir informações de uso importantes e atalhos para serviços da AWS. Para obter mais informações, consulte Trabalhar com widgets.	25 de fevereiro de 2022

Alteração	Descrição	Data
Alterar o idioma do console	Escolha um idioma diferente para o Console de gerenciamento da AWS. Para obter mais informações, consulte Alterar o idioma do Console de gerenciamento da AWS.	1.º de abril de 2021
Iniciar o CloudShell	Abra o AWS CloudShell pelo Console de gerenciamento da AWS e execute os comandos da AWS CLI. Para obter mais informações, consulte Iniciar o AWS CloudShell.	22 de março de 2021

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.