Administrar e monitorar

NetApp Console setup and administration

NetApp
January 27, 2026

Índice

Administrar e monitorar

Associar contas de suporte da NetApp

Gerenciar credenciais NSS associadas ao NetApp Console

Associe uma conta do NetApp Support Site à sua organização do Console para habilitar fluxos de trabalho importantes para gerenciamento de armazenamento. Essas credenciais do NSS estão associadas a toda a organização.

O Console também suporta a associação de uma conta NSS por conta de usuário. "Aprenda a gerenciar credenciais em nível de usuário" .

Visão geral

É necessário associar as credenciais do site de suporte da NetApp ao número de série específico da sua conta do Console para habilitar as seguintes tarefas:

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer sua conta NSS para que o Console possa carregar sua chave de licença e habilitar a assinatura para o período que você comprou. Isso inclui atualizações automáticas para renovações de prazo.

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso

  É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

Essas credenciais estão associadas ao número de série específico da sua conta do Console. Os usuários podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

Adicionar uma conta NSS

Você pode adicionar e gerenciar suas contas do Site de Suporte NetApp para uso com o Console no Painel de Suporte do Console.

Depois de adicionar sua conta NSS, o Console usa essas informações para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

Você pode associar várias contas NSS à sua organização; no entanto, não é possível ter contas de clientes e contas de parceiros na mesma organização.

A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.

3. Selecione **Adicionar conta NSS**.
4. Selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.
5. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp .

   Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

   Este é um ID gerado pelo sistema que mapeia para seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no ••• menu.

     Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

O que vem a seguir?

Os usuários agora podem selecionar a conta ao criar novos sistemas Cloud Volumes ONTAP e ao registrar sistemas Cloud Volumes ONTAP existentes.

- "Lançamento do Cloud Volumes ONTAP na AWS"
- "Iniciando o Cloud Volumes ONTAP no Azure"
- "Lançamento do Cloud Volumes ONTAP no Google Cloud"
- "Registrando sistemas de pagamento conforme o uso"

Atualizar credenciais NSS

Por motivos de segurança, você deve atualizar suas credenciais do NSS a cada 90 dias. Você será notificado no centro de notificações do Console se sua credencial NSS tiver expirado. "Saiba mais sobre o Centro de Notificações" .

Credenciais expiradas podem interromper o seguinte, mas não estão limitadas a:

- Atualizações de licença, o que significa que você não poderá aproveitar a capacidade recém-adquirida.
- Capacidade de enviar e rastrear casos de suporte.

Além disso, você pode atualizar as credenciais do NSS associadas à sua organização se quiser alterar a conta do NSS associada à sua organização. Por exemplo, se a pessoa associada à sua conta NSS saiu da sua empresa.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja atualizar, selecione ••• e então selecione **Atualizar credenciais**.
4. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

   A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação relacionados a suporte e licenciamento.

5. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp .

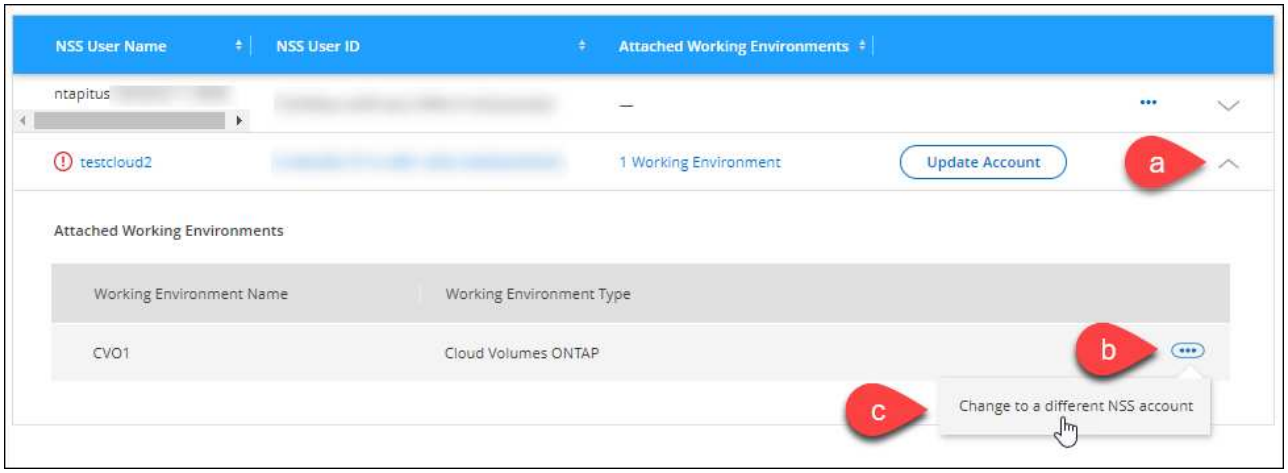
Anexar um sistema a uma conta NSS diferente

Se sua organização tiver várias contas do NetApp Support Site, você poderá alterar qual conta está associada a um sistema Cloud Volumes ONTAP .

Primeiro você deve associar a conta ao Console.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Conclua as seguintes etapas para alterar a conta NSS:
   a. Expanda a linha da conta do site de suporte da NetApp à qual o sistema está atualmente associado.
   b. Para o sistema cuja associação você deseja alterar, selecione •••
   c. Selecione **Alterar para uma conta NSS diferente**.



   d. Selecione a conta e depois selecione **Salvar**.

Exibir o endereço de e-mail de uma conta NSS

Por segurança, o endereço de e-mail associado a uma conta NSS não é exibido por padrão. Você pode visualizar o endereço de e-mail e o nome de usuário associado a uma conta NSS.

Quando você acessa a página Gerenciamento do NSS, o Console gera um token para cada conta na tabela. Esse token inclui informações sobre o endereço de e-mail associado. O token é removido quando você sai da página. As informações nunca são armazenadas em cache, o que ajuda a proteger sua privacidade.

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja atualizar, selecione ••• e então selecione **Exibir endereço de e-mail**. Você pode usar o botão copiar para copiar o endereço de e-mail.

Remover uma conta NSS

Exclua todas as contas NSS que você não deseja mais usar com o Console.

Não é possível excluir uma conta que esteja atualmente associada a um sistema Cloud Volumes ONTAP . Primeiro você precisaanexar esses sistemas a uma conta NSS diferente .

Passos

1. Em **Administração > Suporte**.
2. Selecione **Gerenciamento NSS**.
3. Para a conta NSS que você deseja excluir, selecione ••• e então selecione **Excluir**.
4. Selecione **Excluir** para confirmar.

Gerenciar credenciais associadas ao seu login do NetApp Console

Dependendo das ações que você realizou no Console, você pode ter associado credenciais do ONTAP e credenciais do NetApp Support Site (NSS) ao seu login de usuário. Você pode visualizar e gerenciar essas credenciais depois de associá-las. Por exemplo, se você alterar a senha dessas credenciais, será necessário atualizar a senha no Console.

Credenciais ONTAP

Os usuários precisam de credenciais de administrador do ONTAP para descobrir clusters do ONTAP no Console. No entanto, o acesso ao ONTAP System Manager depende se você está ou não usando um agente de console.

Sem um agente de console

Os usuários são solicitados a inserir suas credenciais do ONTAP para acessar o ONTAP System Manager para o cluster. Os usuários podem optar por salvar essas credenciais no Console, o que significa que não serão solicitados a inseri-las toda vez. As credenciais do usuário são visíveis apenas para o respectivo usuário e podem ser gerenciadas na página Credenciais do usuário.

Com um agente de console

Por padrão, os usuários não são solicitados a inserir suas credenciais do ONTAP para acessar o ONTAP System Manager. No entanto, um administrador do Console (com a função de administrador da organização) pode configurar o Console para solicitar que os usuários insiram suas credenciais do ONTAP . Quando essa configuração estiver habilitada, os usuários precisarão inserir suas credenciais do ONTAP sempre.

"Saber mais."

Credenciais NSS

As credenciais do NSS associadas ao seu login no NetApp Console permitem o registro de suporte, o gerenciamento de casos e o acesso ao Digital Advisor.

- Ao acessar **Suporte > Recursos** e se registrar para obter suporte, você será solicitado a associar as credenciais do NSS ao seu login.

  Isso registra sua organização ou conta para suporte e ativa o direito ao suporte. Somente um usuário em sua organização deve associar uma conta do NetApp Support Site ao seu login para se registrar para suporte e ativar o direito ao suporte. Após a conclusão, a página **Recursos** mostrará que sua conta está

registrada para suporte.

"Aprenda como se registrar para receber suporte"

- Ao acessar **Administração > Suporte > Gerenciamento de casos**, você será solicitado a inserir suas credenciais do NSS, caso ainda não tenha feito isso. Esta página permite que você crie e gerencie os casos de suporte associados à sua conta NSS e à sua empresa.
- Ao acessar o Digital Advisor no Console, você será solicitado a efetuar login no Digital Advisor inserindo suas credenciais do NSS.

Observe o seguinte sobre a conta NSS associada ao seu login:

- A conta é gerenciada no nível do usuário, o que significa que ela não pode ser visualizada por outros usuários que efetuam login.
- Só pode haver uma conta NSS associada ao Digital Advisor e ao gerenciamento de casos de suporte por usuário.
- Se você estiver tentando associar uma conta do NetApp Support Site a um sistema Cloud Volumes ONTAP , só poderá escolher entre as contas NSS que foram adicionadas à organização da qual você é membro.

  As credenciais no nível da conta NSS são diferentes da conta NSS associada ao seu login. As credenciais de nível de conta do NSS permitem que você implante o Cloud Volumes ONTAP com BYOL, registre sistemas PAYGO e atualize seu software.

  "Saiba mais sobre como usar credenciais NSS com sua organização ou conta do NetApp Console" .

Gerencie suas credenciais de usuário

Gerencie suas credenciais de usuário atualizando o nome de usuário e a senha ou excluindo as credenciais.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais do usuário**.
3. Se você ainda não tiver nenhuma credencial de usuário, poderá selecionar **Adicionar credenciais NSS** para adicionar sua conta do Site de Suporte NetApp .
4. Gerencie as credenciais existentes escolhendo as seguintes opções no menu Ações:
   - **Atualizar credenciais**: Atualize o nome de usuário e a senha da conta.
   - **Excluir credenciais**: Remova a conta NSS associada ao seu login do Console.

Agentes de console

Saiba mais sobre os agentes do NetApp Console

Você usa um agente do Console para conectar o NetApp Console à sua infraestrutura e orquestrar com segurança soluções de armazenamento em ambientes AWS, Azure, Google Cloud ou locais, além de usar serviços de proteção de dados.

Um agente de console permite que você:

- Orquestre tarefas de gerenciamento de armazenamento a partir do NetApp Console , como provisionamento do Cloud Volumes ONTAP, configuração de volumes de armazenamento, uso de classificação de dados e muito mais.
- Autentique-se usando as funções IAM do seu provedor de nuvem para integração de faturamento de assinaturas.
- Utilize serviços de dados avançados (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience e NetApp Cloud Tiering).
- Utilize o console no modo restrito.

Se você não precisa de orquestração avançada ou proteção de dados, pode gerenciar centralmente clusters ONTAP locais e serviços de armazenamento nativos da nuvem sem implantar um agente. Ferramentas de monitoramento e mobilidade de dados também estão disponíveis.

A tabela a seguir mostra quais recursos e serviços você pode usar com e sem um agente do Console.

	Disponível com agente	**Disponível sem agente**
Sistemas de armazenamento suportados:		
Amazon FSx para ONTAP	Sim (recursos de descoberta e gerenciamento)	Sim (somente descoberta)
Armazenamento Amazon S3	Sim	Não
Armazenamento de Blobs do Azure	Sim	Sim
Azure NetApp Files	Sim	Sim
Cloud Volumes ONTAP	Sim	Não
Sistemas da série E	Sim	Não
Google Cloud NetApp Volumes	Sim	Sim
Buckets de armazenamento do Google Cloud	Sim	Não
Sistemas StorageGRID	Sim	Não
Cluster ONTAP local (gerenciamento e descoberta avançados)	Sim (gestão e descoberta avançadas)	Não (apenas descoberta básica)
Serviços de gestão de armazenamento disponíveis:		
Alertas	Sim	Não
Centro de automação	Sim	Sim

	Disponível com agente	Disponível sem agente
Digital Advisor (Active IQ)	Sim	Não
Gerenciamento de licenças e assinaturas	Sim	Não
Eficiência econômica	Sim	Não
Métricas do painel da página inicial	Sim[2]	Não
Planejamento do ciclo de vida	Sim	Não[1]
Sustentabilidade	Sim	Não
Atualizações de software	Sim	Sim
Cargas de trabalho da NetApp	Sim	Sim
Serviços de dados disponíveis:		
NetApp Backup and Recovery	Sim	Não
Classificação de Dados	Sim	Não
NetApp Cloud Tiering	Sim	Não
NetApp Copy and Sync	Sim	Não
NetApp Disaster Recovery	Sim	Não
NetApp Ransomware Resilience	Sim	Não
NetApp Volume Caching	Sim	Não

[1] É possível visualizar o planejamento do ciclo de vida sem um agente do console, mas um agente do console é necessário para iniciar ações.

[2] Métricas precisas na página inicial exigem agentes de console com tamanho e configuração adequados.

Os agentes do console devem estar operacionais o tempo todo

Os agentes de console são uma parte fundamental do NetApp Console. É sua responsabilidade (o cliente) garantir que os agentes relevantes estejam sempre ativos, operacionais e acessíveis. O Console pode lidar com pequenas interrupções do agente, mas você deve corrigir falhas de infraestrutura rapidamente.

Esta documentação é regida pelo CLUF. Operar o produto fora da documentação pode afetar sua funcionalidade e seus direitos de EULA.

Locais suportados

Você pode instalar agentes nos seguintes locais:

- Serviços Web da Amazon
- Microsoft Azure

  Implante um agente de console no Azure na mesma região que os sistemas Cloud Volumes ONTAP que ele gerencia. Alternativamente, implante-o no "Par de regiões do Azure" . Isso garante que uma conexão do Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas. "Saiba como o Cloud Volumes ONTAP usa um Azure Private Link"

- Google Cloud

  Para usar o Console e os serviços de dados com o Google Cloud, implante seu agente no Google Cloud.

- Nas suas instalações

Comunicação com provedores de nuvem

O agente usa TLS 1.3 para todas as comunicações com AWS, Azure e Google Cloud.

Modo restrito

Para usar o Console no modo restrito, instale um agente do Console e acesse a interface do Console que está sendo executada localmente no agente do Console.

"Saiba mais sobre os modos de implantação do NetApp Console" .

Como instalar um agente de console

Você pode instalar um agente do Console diretamente do Console, do marketplace do seu provedor de nuvem ou instalando manualmente o software no seu próprio host Linux ou no seu ambiente VCenter.

- "Saiba mais sobre os modos de implantação do NetApp Console"
- "Comece a usar o NetApp Console no modo padrão"
- "Comece a usar o NetApp Console no modo restrito"

Permissões do provedor de nuvem

Você precisa de permissões específicas para criar o agente do Console diretamente do NetApp Console e outro conjunto de permissões para o próprio agente do Console. Se você criar o agente do Console na AWS ou no Azure diretamente do Console, o Console criará o agente do Console com as permissões necessárias.

Ao usar o Console no modo padrão, a maneira como você fornece permissões depende de como você planeja criar o agente do Console.

Para saber como configurar permissões, consulte o seguinte:

- Modo padrão
  - "Opções de instalação do agente na AWS"
  - "Opções de instalação do agente no Azure"

    - "Opções de instalação do agente no Google Cloud"
    - "Configurar permissões de nuvem para implantações locais"
- "Configurar permissões para o modo restrito"

Para visualizar as permissões exatas que o agente do Console precisa para operações diárias, consulte as seguintes páginas:

- "Aprenda como o agente do Console usa as permissões da AWS"
- "Aprenda como o agente do Console usa as permissões do Azure"
- "Saiba como o agente do Console usa as permissões do Google Cloud"

É sua responsabilidade atualizar as políticas do agente do Console à medida que novas permissões são adicionadas em versões subsequentes. As notas de versão listam novas permissões.

Atualizações de agentes

A NetApp atualiza o software do agente mensalmente para adicionar recursos e melhorar a estabilidade. Alguns recursos do Console, como o Cloud Volumes ONTAP e o gerenciamento de cluster ONTAP local, dependem da versão e das configurações do agente do Console.

Ao instalar o agente na nuvem, o agente do Console é atualizado automaticamente, desde que tenha acesso à internet.

Manutenção de sistema operacional e VM

Manter o sistema operacional no host do agente do Console é responsabilidade sua (do cliente). Por exemplo, você (cliente) deve aplicar atualizações de segurança ao sistema operacional no host do agente do Console seguindo os procedimentos padrão da sua empresa para distribuição do sistema operacional.

Observe que você (cliente) não precisa interromper nenhum serviço no host do Console Gent ao aplicar pequenas atualizações de segurança.

Se você (cliente) precisar parar e iniciar a VM do agente do Console, faça isso no console do seu provedor de nuvem ou usando os procedimentos padrão para gerenciamento local.

O agente do Console deve estar operacional o tempo todo .

Vários sistemas e agentes

Um agente pode gerenciar vários sistemas e dar suporte a serviços de dados no Console. Você pode usar um único agente para gerenciar vários sistemas com base no tamanho da implantação e nos serviços de dados que você usa.

Para implantações em larga escala, trabalhe com seu representante da NetApp para dimensionar seu ambiente. Entre em contato com o Suporte da NetApp se tiver problemas.

Aqui estão alguns exemplos de implantações de agentes:

- Você tem um ambiente multicloud (por exemplo, AWS e Azure) e prefere ter um agente na AWS e outro no Azure. Cada um gerencia os sistemas Cloud Volumes ONTAP em execução nesses ambientes.
- Um provedor de serviços pode usar uma organização do Console para fornecer serviços aos seus clientes, enquanto usa outra organização para fornecer recuperação de desastres para uma de suas unidades de negócios. Cada organização precisa de seu próprio agente.

Implantar um agente de console

AWS

Opções de instalação do agente de console na AWS

Existem algumas maneiras diferentes de criar um agente de console na AWS. Diretamente do NetApp Console é a maneira mais comum.

As seguintes opções de instalação estão disponíveis:

- "Crie o agente do Console diretamente do Console"(esta é a opção padrão)

  Esta ação inicia uma instância do EC2 executando o Linux e o software do agente do Console em uma VPC de sua escolha.

- "Crie um agente de console no AWS Marketplace"

  Esta ação também inicia uma instância do EC2 executando o Linux e o software do agente do Console, mas a implantação é iniciada diretamente do AWS Marketplace, e não do Console.

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao Console as permissões necessárias para autenticar e gerenciar recursos na AWS.

Crie um agente de console na AWS a partir do NetApp Console

Você pode criar um agente de console na AWS diretamente do NetApp Console. Antes de criar um agente do Console na AWS a partir do Console, você precisa configurar sua rede e preparar as permissões da AWS.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede para implantar um agente de console na AWS

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos e processos na sua nuvem híbrida.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Você precisará implementar esse requisito de rede depois de criar o agente do Console.

Etapa 2: configurar permissões da AWS para o agente do Console

O Console precisa ser autenticado na AWS antes de poder implantar o agente do Console na sua VPC. Você pode escolher um destes métodos de autenticação:

- Deixe o Console assumir uma função do IAM que tenha as permissões necessárias
- Forneça uma chave de acesso e uma chave secreta da AWS para um usuário do IAM que tenha as permissões necessárias

Com qualquer uma das opções, o primeiro passo é criar uma política de IAM. Esta política contém apenas as permissões necessárias para iniciar o agente do Console na AWS a partir do Console.

Se necessário, você pode restringir a política do IAM usando o IAM `Condition` elemento. "Documentação da AWS: Elemento Condition"

Passos

1. Acesse o console do AWS IAM.
2. Selecione **Políticas > Criar política**.
3. Selecione **JSON**.
4. Copie e cole a seguinte política:

   Esta política contém apenas as permissões necessárias para iniciar o agente do Console na AWS a partir do Console. Quando o Console cria o agente do Console, ele aplica um novo conjunto de permissões ao agente do Console que permite que o agente do Console gerencie recursos da AWS. "Exibir permissões necessárias para o próprio agente do Console".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
```

```
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Selecione **Avançar** e adicione tags, se necessário.
6. Selecione **Avançar** e insira um nome e uma descrição.
7. Selecione **Criar política**.
8. Anexe a política a uma função do IAM que o Console pode assumir ou a um usuário do IAM para que você possa fornecer chaves de acesso ao Console:
   - (Opção 1) Configure uma função do IAM que o Console pode assumir:
     i. Acesse o console do AWS IAM na conta de destino.
     ii. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.
     iii. Em **Tipo de entidade confiável**, selecione **Conta AWS**.
     iv. Selecione **Outra conta AWS** e insira o ID da conta SaaS do Console: 952013314444
     v. Selecione a política que você criou na seção anterior.
     vi. Depois de criar a função, copie o ARN da função para poder colá-lo no Console ao criar o agente do Console.
   - (Opção 2) Configure permissões para um usuário do IAM para que você possa fornecer chaves de acesso ao Console:
     i. No console do AWS IAM, selecione **Usuários** e, em seguida, selecione o nome do usuário.
     ii. Selecione **Adicionar permissões > Anexar políticas existentes diretamente**.
     iii. Selecione a política que você criou.
     iv. Selecione **Avançar** e depois selecione **Adicionar permissões**.

v. Certifique-se de ter a chave de acesso e a chave secreta para o usuário do IAM.

Resultado

Agora você deve ter uma função do IAM que tenha as permissões necessárias ou um usuário do IAM que tenha as permissões necessárias. Ao criar o agente do Console a partir do Console, você pode fornecer informações sobre a função ou as chaves de acesso.

Etapa 3: Criar o agente do Console

Crie o agente do Console diretamente do console baseado na Web.

Sobre esta tarefa

- A criação do agente do Console a partir do Console implanta uma instância do EC2 na AWS usando uma configuração padrão. Não mude para uma instância EC2 menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .
- Quando o Console cria o agente do Console, ele cria uma função do IAM e um perfil para o agente. Esta função inclui permissões que permitem ao agente do Console gerenciar recursos da AWS. Garanta que a função seja atualizada conforme novas permissões forem adicionadas em versões futuras. "Saiba mais sobre a política do IAM para o agente do Console".

Antes de começar

Você deve ter o seguinte:

- Um método de autenticação da AWS: uma função do IAM ou chaves de acesso para um usuário do IAM com as permissões necessárias.
- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Um par de chaves para a instância EC2.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.
- Configurar"requisitos de rede" .
- Configurar"Permissões da AWS" .

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > AWS**
3. Siga as etapas do assistente para criar o agente do Console:
4. Na página **Introdução** é fornecida uma visão geral do processo
5. Na página **Credenciais da AWS**, especifique sua região da AWS e escolha um método de autenticação, que pode ser uma função do IAM que o Console pode assumir ou uma chave de acesso e uma chave secreta da AWS.

Se você escolher **Assumir função**, poderá criar o primeiro conjunto de credenciais no assistente de implantação do agente do Console. Qualquer conjunto adicional de credenciais deve ser criado na página Credenciais. Eles estarão disponíveis no assistente em uma lista suspensa. "Aprenda como adicionar credenciais adicionais" .

6. Na página **Detalhes**, forneça detalhes sobre o agente do Console.
   - Digite um nome.

- Adicione tags personalizadas (metadados).
- Escolha se deseja que o Console crie uma nova função que tenha as permissões necessárias ou se deseja selecionar uma função existente que você configurou com"as permissões necessárias" .
- Escolha se deseja criptografar os discos EBS do agente do Console. Você tem a opção de usar a chave de criptografia padrão ou usar uma chave personalizada.

7. Na página **Rede**, especifique uma VPC, uma sub-rede e um par de chaves para o agente, escolha se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.

   Certifique-se de ter o par de chaves correto para acessar a máquina virtual do agente do Console. Sem um par de chaves, você não pode acessá-lo.

8. Na página **Grupo de segurança**, escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

   "Exibir regras de grupo de segurança para AWS" .

9. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

   Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

10. Selecione **Adicionar**.

    O Console implanta o agente em cerca de 10 minutos. Permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso no Console.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na página **Sistemas**. "Aprenda a gerenciar buckets do S3 no NetApp Console"

Crie um agente de console no AWS Marketplace

Você cria um agente de console na AWS diretamente do AWS Marketplace. Para criar um agente do Console no AWS Marketplace, você precisa configurar sua rede, preparar as permissões da AWS, revisar os requisitos da instância e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede do agente do Console atenda aos seguintes requisitos para gerenciar recursos de nuvem híbrida.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Implemente esse acesso à rede depois de criar o agente do Console.

Etapa 2: configurar permissões da AWS

Para se preparar para uma implantação de mercado, crie políticas do IAM na AWS e anexe-as a uma função do IAM. Ao criar o agente do Console no AWS Marketplace, você será solicitado a selecionar essa função do IAM.

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:
   a. Selecione **Políticas > Criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .
   c. Conclua as etapas restantes para criar a política.

      Talvez seja necessário criar uma segunda política com base nos serviços de dados da NetApp que você planeja usar. Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .
3. Crie uma função do IAM:
   a. Selecione **Funções > Criar função**.
   b. Selecione **Serviço AWS > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

Resultado

Agora você tem uma função do IAM que pode ser associada à instância do EC2 durante a implantação no AWS Marketplace.

Etapa 3: Revisar os requisitos da instância

Ao criar o agente do Console, você precisa escolher um tipo de instância do EC2 que atenda aos seguintes requisitos.

CPU

8 núcleos ou 8 vCPUs

BATER
32 GB

Tipo de instância AWS EC2
Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda t3.2xlarge.

Etapa 4: criar o agente do console

Crie o agente do Console diretamente do AWS Marketplace.

Sobre esta tarefa

A criação do agente do Console no AWS Marketplace implanta uma instância do EC2 na AWS usando uma configuração padrão. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Uma função do IAM com uma política anexada que inclui as permissões necessárias para o agente do Console.
- Permissões para assinar e cancelar a assinatura do AWS Marketplace para seu usuário do IAM.
- Uma compreensão dos requisitos de CPU e RAM para a instância.
- Um par de chaves para a instância EC2.

Passos

1. Vá para o "Listagem do agente do NetApp Console no AWS Marketplace"
2. Na página Marketplace, selecione **Continuar assinando**.
3. Para assinar o software, selecione **Aceitar Termos**.

   O processo de assinatura pode levar alguns minutos.

4. Após a conclusão do processo de assinatura, selecione **Continuar para configuração**.
5. Na página **Configurar este software**, certifique-se de ter selecionado a região correta e selecione **Continuar para iniciar**.
6. Na página **Iniciar este software**, em **Escolher ação**, selecione **Iniciar pelo EC2** e depois selecione **Iniciar**.

   Use o Console do EC2 para iniciar a instância e anexar uma função do IAM. Isso não é possível com a ação **Iniciar do site**.

7. Siga as instruções para configurar e implantar a instância:

   - **Nome e tags**: Insira um nome e tags para a instância.
   - **Imagens de aplicativos e sistemas operacionais**: pule esta seção. O agente do console AMI já está selecionado.
   - **Tipo de instância**: Dependendo da disponibilidade da região, escolha um tipo de instância que atenda aos requisitos de RAM e CPU (t3.2xlarge é pré-selecionado e recomendado).
   - **Par de chaves (login)**: Selecione o par de chaves que você deseja usar para se conectar com segurança à instância.

- **Configurações de rede**: edite as configurações de rede conforme necessário:
  - Escolha a VPC e a sub-rede desejadas.
  - Especifique se a instância deve ter um endereço IP público.
  - Especifique as configurações do grupo de segurança que habilitam os métodos de conexão necessários para a instância do agente do Console: SSH, HTTP e HTTPS.

    "Exibir regras de grupo de segurança para AWS" .
- **Configurar armazenamento**: Mantenha o tamanho e o tipo de disco padrão para o volume raiz.

  Se você quiser habilitar a criptografia do Amazon EBS no volume raiz, selecione **Avançado**, expanda **Volume 1**, selecione **Criptografado** e escolha uma chave KMS.
- **Detalhes avançados**: Em **Perfil de instância do IAM**, escolha a função do IAM que inclui as permissões necessárias para o agente do Console.
- **Resumo**: Revise o resumo e selecione **Iniciar instância**.

  A AWS inicia o agente do Console com as configurações especificadas, e o agente do Console é executado em cerca de dez minutos.

  Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."

8. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e a URL do agente do Console.
9. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Mantenha o modo restrito desabilitado para usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend do Console. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

   d. Selecione **Vamos começar**.

Resultado

O agente do Console agora está instalado e configurado com sua organização do Console.

Abra um navegador da web e vá para o "NetApp Console" para começar a usar o agente do Console com o Console.

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um ambiente de trabalho do Amazon S3 aparecer automaticamente na página **Sistemas**. "Aprenda a gerenciar buckets do S3 no NetApp Console"

Instalar manualmente o agente do Console na AWS

Você pode instalar manualmente um agente do Console em um host Linux em execução

na AWS. Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões da AWS, instalar o agente do Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

Certifique-se de que o host que executa o software do agente do Console atenda aos requisitos de sistema operacional, RAM e portas.

> O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console requer um host dedicado. Qualquer arquitetura é suportada, desde que atenda a estes requisitos de tamanho:

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB é recomendado para o host, com os seguintes requisitos de partição:
  - `/opt`: 120 GiB de espaço devem estar disponíveis

    O agente usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

  - `/var`: 40 GiB de espaço devem estar disponíveis

    O agente do console requer este espaço em `/var` Porque o Podman ou o Docker são projetados para criar contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório e `/var/lib/docker` para Docker. Montagens externas ou links simbólicos não funcionam neste espaço.

Tipo de instância AWS EC2

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda t3.2xlarge.

Hipervisor

É necessário um hipervisor bare metal ou hospedado certificado para executar um sistema operacional compatível.

Requisitos do sistema operacional e do contêiner

O agente do Console é compatível com os seguintes sistemas operacionais ao usar o Console no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o agente.

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Red Hat Enterprise Linux		9,6 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	4.0.0 ou posterior com o Console no modo padrão ou no modo restrito.	Podman versão 5.4.0 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo		9.1 a 9.4 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.9.4 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo		8,6 a 8,10 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.6.1 ou 4.9.4 com podman-compose 1.0.6. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo	Ubuntu		24,04 LTS	3.9.45 ou posterior com o NetApp Console no modo padrão ou restrito
Docker Engine 23.06 para 28.0.0.	Não suportado		22,04 LTS	3.9.50 ou posterior

Par de chaves

Ao criar o agente do Console, você precisará selecionar um par de chaves EC2 para usar com a instância.

Limite de salto de resposta PUT ao usar IMDSv2

Se o IMDSv2 estiver ativado (o padrão para novas instâncias EC2), defina o limite de saltos de resposta PUT para 3. Caso contrário, o sistema exibirá um erro de inicialização da interface do usuário durante a configuração do agente.

- "Exigir o uso do IMDSv2 em instâncias do Amazon EC2"
- "Documentação da AWS: Alterar o limite de salto de resposta PUT"

Etapa 2: instalar o Podman ou o Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine é necessário antes de instalar o agente.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas .

- O Docker Engine é necessário para o Ubuntu.

  Veja as versões suportadas do Docker Engine .

Exemplo 1. Passos

Podman

Siga estas etapas para instalar e configurar o Podman:

- Habilite e inicie o serviço podman.socket
- Instalar python3
- Instale o pacote podman-compose versão 1.0.6
- Adicione podman-compose à variável de ambiente PATH
- Se estiver usando o Red Hat Enterprise Linux, verifique se sua versão do Podman está usando o DNS Netavark Aardvark em vez do CNI

Ajuste a porta aardvark-dns (padrão: 53) após instalar o agente para evitar conflitos de porta DNS. Siga as instruções para configurar a porta.

Passos

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   Você pode obter o Podman nos repositórios oficiais do Red Hat Enterprise Linux.

   a. Para Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   c. Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

3. Habilite e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ele ainda não estiver disponível no seu sistema.

   Esta etapa é necessária porque o podman-compose está disponível no repositório Extra Packages for Enterprise Linux (EPEL).

6. Se estiver usando o Red Hat Enterprise 9:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Instale o pacote podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se estiver usando o Red Hat Enterprise Linux 8:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Instale o pacote podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   Usando o `dnf install` O comando atende ao requisito de adicionar podman-compose à variável de ambiente PATH. O comando de instalação adiciona podman-compose a /usr/bin, que já está incluído no `secure_path` opção no host.

   c. Se estiver usando o Red Hat Enterprise Linux 8, verifique se sua versão do Podman está usando o NetAvark com o DNS Aardvark em vez do CNI.

i. Verifique se o seu networkBackend está definido como CNI executando o seguinte comando:

```
podman info | grep networkBackend
```

ii. Se o networkBackend estiver definido como `CNI` , você precisará alterá-lo para `netavark` .

iii. Instalar `netavark` e `aardvark-dns` usando o seguinte comando:

```
dnf install aardvark-dns netavark
```

iv. Abra o `/etc/containers/containers.conf` arquivo e modifique a opção network_backend para usar "netavark" em vez de "cni".

Se `/etc/containers/containers.conf` não existe, faça as alterações de configuração para `/usr/share/containers/containers.conf` .

v. Reinicie o podman.

```
systemctl restart podman
```

vi. Confirme se networkBackend foi alterado para "netavark" usando o seguinte comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga a documentação do Docker para instalar o Docker Engine.

Passos

1. "Ver instruções de instalação do Docker"

   Siga as etapas para instalar uma versão compatível do Docker Engine. Não instale a versão mais recente, pois ela não é suportada pelo Console.

2. Verifique se o Docker está habilitado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Etapa 3: configurar a rede

Certifique-se de que a localização da rede atenda aos seguintes requisitos para que o agente do Console possa gerenciar recursos em sua nuvem híbrida.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .

Pontos finais	Propósito
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Etapa 4: configurar permissões da AWS para o console

Conceda permissões da AWS ao NetApp Console usando uma destas opções:

- Opção 1: Crie políticas do IAM e anexe-as a uma função do IAM que você pode associar à instância do EC2.
- Opção 2: forneça ao Console a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

Siga as etapas para preparar permissões para o Console.

Função IAM

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:
   a. Selecione **Políticas > Criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços de dados da NetApp que você planeja usar, pode ser necessário criar uma segunda política. Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .
3. Crie uma função do IAM:
   a. Selecione **Funções > Criar função**.
   b. Selecione **Serviço AWS > EC2**.
   c. Adicione permissões anexando a política que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

Resultado

Agora você tem uma função do IAM que pode ser associada à instância do EC2 após instalar o agente do Console.

Chave de acesso AWS

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:
   a. Selecione **Políticas > Criar política**.
   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .
   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços de dados da NetApp que você planeja usar, pode ser necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .
3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o usuário tenha uma chave de acesso que você possa adicionar ao NetApp Console após instalar o agente do Console.

Resultado

Agora você tem um usuário do IAM que tem as permissões necessárias e uma chave de acesso que você pode fornecer ao Console.

Etapa 5: instalar o agente do console

Após concluir os pré-requisitos, instale manualmente o software em seu host Linux.

Antes de começar

Você deve ter o seguinte:

- Privilégios de root para instalar o agente do Console.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do agente do Console.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy de interceptação.

> Não é possível definir um certificado para um servidor proxy transparente ao instalar manualmente o agente do Console. Se precisar definir um certificado para um servidor proxy transparente, você deverá usar o Console de Manutenção após a instalação. Saiba mais sobre o"Console de manutenção do agente" .

Sobre esta tarefa

Após a instalação, o agente do Console se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Baixe o software do agente do Console e copie-o para o host Linux. Você pode baixá-lo tanto do NetApp Console quanto do site de suporte da NetApp .
   - NetApp Console: Acesse **Agentes > Gerenciamento > Implantar agente > Local > Instalação manual**.

     Escolha baixar os arquivos de instalação do agente ou um URL para os arquivos.

   - Site de suporte da NetApp (necessário caso você ainda não tenha acesso ao Console) "Site de suporte da NetApp" ,
3. Atribua permissões para executar o script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

Onde <versão> é a versão do agente do Console que você baixou.

4. Se estiver instalando em um ambiente de nuvem governamental, desative as verificações de configuração."Aprenda como desabilitar verificações de configuração para instalações manuais."
5. Execute o script de instalação.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Você precisará adicionar informações de proxy se sua rede exigir um proxy para acesso à internet. Você pode adicionar um proxy explícito durante a instalação. Os parâmetros `--proxy` e `--cacert` são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy explícito, precisará inserir os parâmetros conforme mostrado.

Se você deseja configurar um proxy transparente, pode fazê-lo após a instalação. "Saiba mais sobre o console de manutenção do agente."

+

Aqui está um exemplo de configuração de um servidor proxy explícito com um certificado assinado por uma CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` configura o agente do Console para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

+ * http://endereço:porta * http://nome-do-usuário:senha@endereço:porta * http://nome-do-domínio%92nome-do-usuário:senha@endereço:porta * https://endereço:porta * https://nome-do-usuário:senha@endereço:porta * https://nome-do-domínio%92nome-do-usuário:senha@endereço:porta

+ Observe o seguinte:

+ **O usuário pode ser um usuário local ou um usuário de domínio.** Para um usuário de domínio, você deve usar o código ASCII para uma \ conforme mostrado acima. **O agente do Console não oferece suporte a nomes de usuário ou senhas que incluam o caractere @.** Se a senha incluir algum dos seguintes caracteres especiais, você deve escapar esse caractere especial adicionando uma barra invertida antes dele: & ou !

+ Por exemplo:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Se você usou o Podman, precisará ajustar a porta aardvark-dns.

a. SSH para a máquina virtual do agente do Console.

b. Abra o arquivo podman */usr/share/containers/containers.conf* e modifique a porta escolhida para o serviço DNS do Aardvark. Por exemplo, altere para 54.

```
vi /usr/share/containers/containers.conf
```

Por exemplo:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. Reinicie a máquina virtual do agente do Console.

2. Aguarde a conclusão da instalação.

No final da instalação, o serviço do agente do Console (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

https://ipaddress

2. Após efetuar login, configure o agente do Console:

a. Especifique a organização a ser associada ao agente do Console.

b. Digite um nome para o sistema.

c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

d. Selecione **Vamos começar**.

Se você tiver buckets do Amazon S3 na mesma conta da AWS onde criou o agente do Console, verá um sistema de armazenamento do Amazon S3 aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar buckets S3 no NetApp ConsoleP"

Etapa 6: fornecer permissões ao NetApp Console

Após instalar o agente do Console, forneça as permissões da AWS que você configurou para que o agente do Console possa gerenciar seus dados e infraestrutura de armazenamento na AWS.

Função IAM

Anexe a função IAM que você criou à instância EC2 do agente do console.

Passos

1. Acesse o console do Amazon EC2.
2. Selecione **Instâncias**.
3. Selecione a instância do agente do Console.
4. Selecione **Ações > Segurança > Modificar função do IAM**.
5. Selecione a função do IAM e selecione **Atualizar função do IAM**.

Vá para o "NetApp Console" para começar a usar o agente do Console.

Chave de acesso AWS

Forneça ao Console a chave de acesso da AWS para um usuário do IAM que tenha as permissões necessárias.

Passos

1. Certifique-se de que o agente correto do Console esteja selecionado no Console.
2. Selecione **Administração > Credenciais**.
3. Selecione **Credenciais da organização**.
4. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione *Amazon Web Services > Agente.
   b. **Definir credenciais**: insira uma chave de acesso e uma chave secreta da AWS.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Vá para o "NetApp Console" para começar a usar o agente do Console.

Azul

Opções de instalação do agente de console no Azure

Existem algumas maneiras diferentes de criar um agente de console no Azure. Diretamente do NetApp Console é a maneira mais comum.

As seguintes opções de instalação estão disponíveis:

- "Crie um agente de console diretamente do NetApp Console"(esta é a opção padrão)

  Esta ação inicia uma VM executando Linux e o software do agente do Console em uma VNet de sua escolha.

- "Crie um agente de console no Azure Marketplace"

  Esta ação também inicia uma VM executando Linux e o software do agente do Console, mas a implantação é iniciada diretamente do Azure Marketplace, e não do Console.

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao agente do Console as permissões necessárias para autenticar e gerenciar recursos no Azure.

Criar um agente de console no Azure a partir do NetApp Console

Para criar um agente do Console no Azure a partir do NetApp Console, você precisa configurar sua rede, preparar as permissões do Azure e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos de nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito garante que uma conexão do Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um Azure Private Link"

VNet e sub-rede

Ao criar o agente do Console, você precisa especificar a VNet e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Você precisa implementar esse requisito de rede depois de criar o agente do Console.

Etapa 2: criar uma política de implantação do agente do console (função personalizada)

Você precisa criar uma função personalizada que tenha permissões para implantar o agente do Console no Azure.

Crie uma função personalizada do Azure que você pode atribuir à sua conta do Azure ou a uma entidade de serviço do Microsoft Entra. O Console é autenticado com o Azure e usa essas permissões para criar o agente do Console em seu nome.

O Console implanta a VM do agente do Console no Azure, habilita um "identidade gerenciada atribuída pelo sistema" , cria a função necessária e a atribui à VM. "Revise como o Console usa as permissões" .

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

Passos

1. Copie as permissões necessárias para uma nova função personalizada no Azure e salve-as em um arquivo JSON.

   Esta função personalizada contém apenas as permissões necessárias para iniciar a VM do agente do Console no Azure a partir do Console. Não use esta política para outras situações. Quando o Console cria o agente do Console, ele aplica um novo conjunto de permissões à VM do agente do Console que permite que o agente do Console gerencie recursos do Azure.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
```

```
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
```

```
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. Modifique o JSON adicionando sua ID de assinatura do Azure ao escopo atribuível.

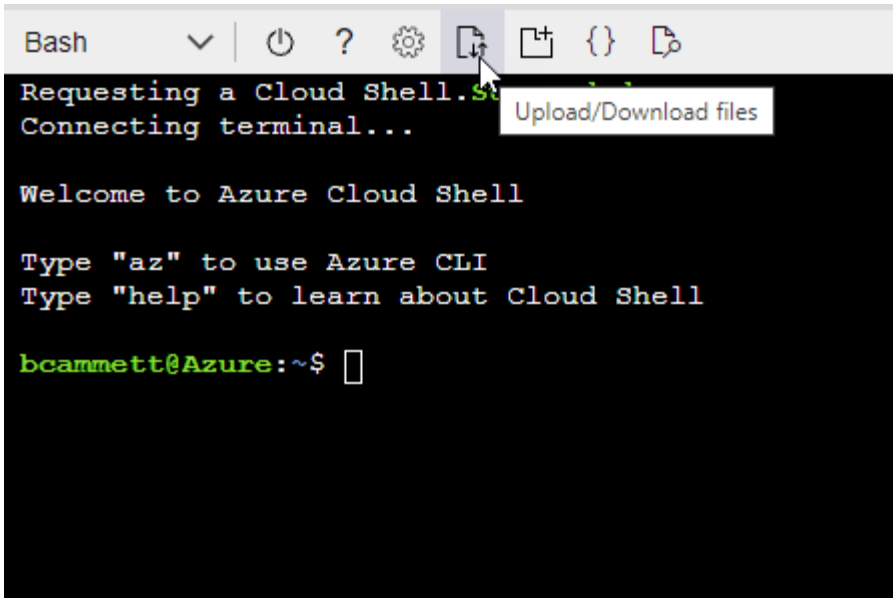
   Exemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Começar "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.



c. Digite o seguinte comando da CLI do Azure:

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

Agora você tem uma função personalizada chamada *Azure SetupAsService*. Você pode aplicar essa função personalizada à sua conta de usuário ou a uma entidade de serviço.

Etapa 3: Configurar autenticação

Ao criar o agente do Console a partir do Console, você precisa fornecer um login que permita que o Console se autentique com o Azure e implante a VM. Você tem duas opções:

1. Sign in com sua conta do Azure quando solicitado. Esta conta deve ter permissões específicas do Azure. Esta é a opção padrão.
2. Forneça detalhes sobre uma entidade de serviço do Microsoft Entra. Este principal de serviço também requer permissões específicas.

Siga as etapas para preparar um desses métodos de autenticação para uso com o Console.

Conta do Azure

Atribua a função personalizada ao usuário que implantará o agente do Console a partir do Console.

Passos

1. No portal do Azure, abra o serviço **Assinaturas** e selecione a assinatura do usuário.
2. Clique em **Controle de acesso (IAM)**.
3. Clique em **Adicionar** > **Adicionar atribuição de função** e adicione as permissões:
   a. Selecione a função **Azure SetupAsService** e clique em **Avançar**.

      Azure SetupAsService é o nome padrão fornecido na política de implantação do agente do Console para o Azure. Se você escolheu um nome diferente para a função, selecione esse nome.

   b. Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
   c. Clique em **Selecionar membros**, escolha sua conta de usuário e clique em **Selecionar**.
   d. Clique em **Avançar**.
   e. Clique em **Revisar + atribuir**.

Diretor de serviço

Em vez de fazer login com sua conta do Azure, você pode fornecer ao Console as credenciais de uma entidade de serviço do Azure que tenha as permissões necessárias.

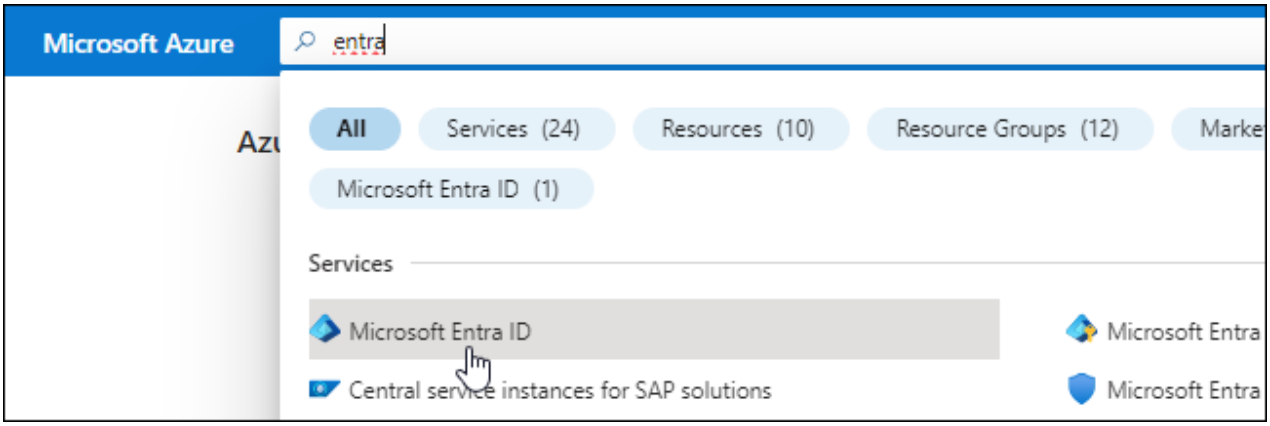
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.

5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Digite um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
   - **URI de redirecionamento**: Você pode deixar este campo em branco.
6. Selecione **Registrar**.

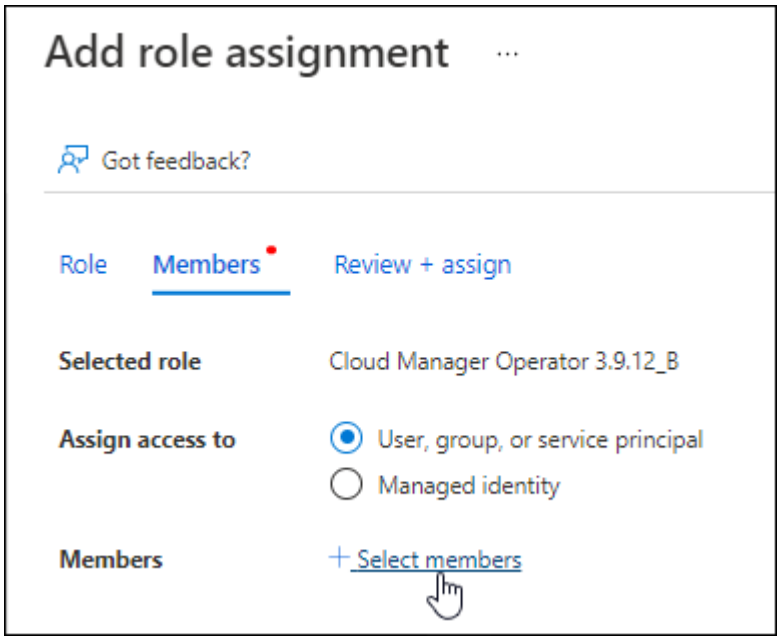
   Você criou o aplicativo AD e a entidade de serviço.

Atribuir a função personalizada ao aplicativo

1. No portal do Azure, abra o serviço **Assinaturas**.
2. Selecione a assinatura.
3. Clique em **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
4. Na guia **Função**, selecione a função **Operador de console** e clique em **Avançar**.
5. Na aba **Membros**, complete os seguintes passos:

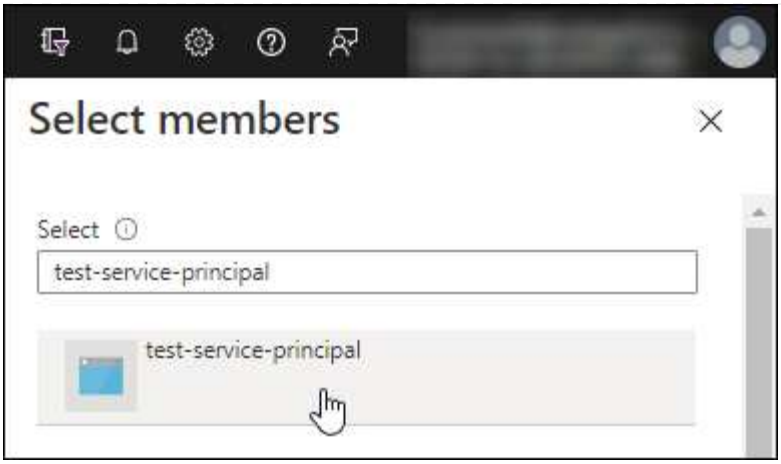
   a. Mantenha **Usuário, grupo ou entidade de serviço** selecionado.

   b. Clique em **Selecionar membros**.



   c. Pesquise o nome do aplicativo.

   Aqui está um exemplo:



a. Selecione o aplicativo e clique em **Selecionar**.

b. Clique em **Avançar**.

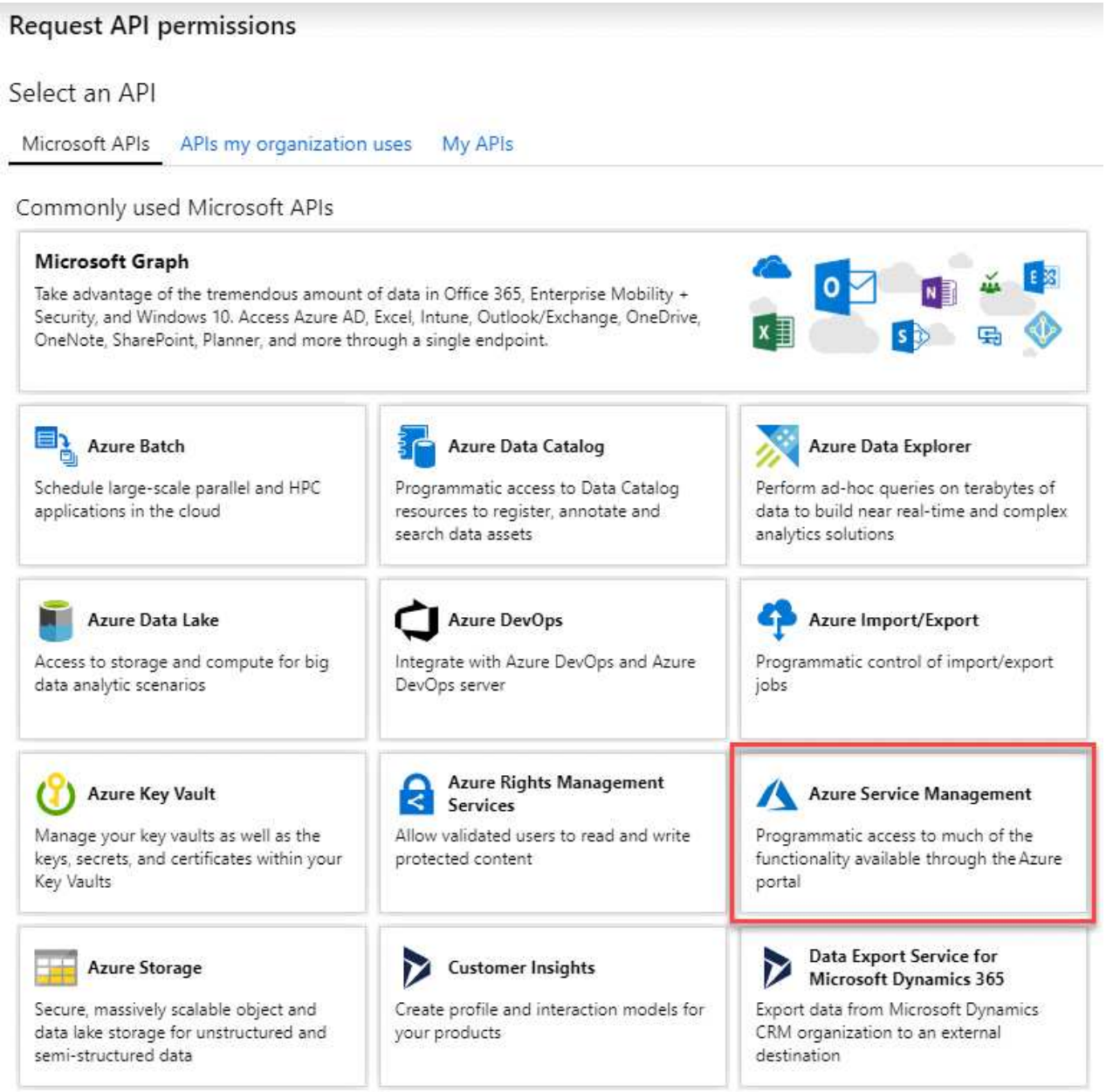
6. Clique em **Revisar + atribuir**.

   O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

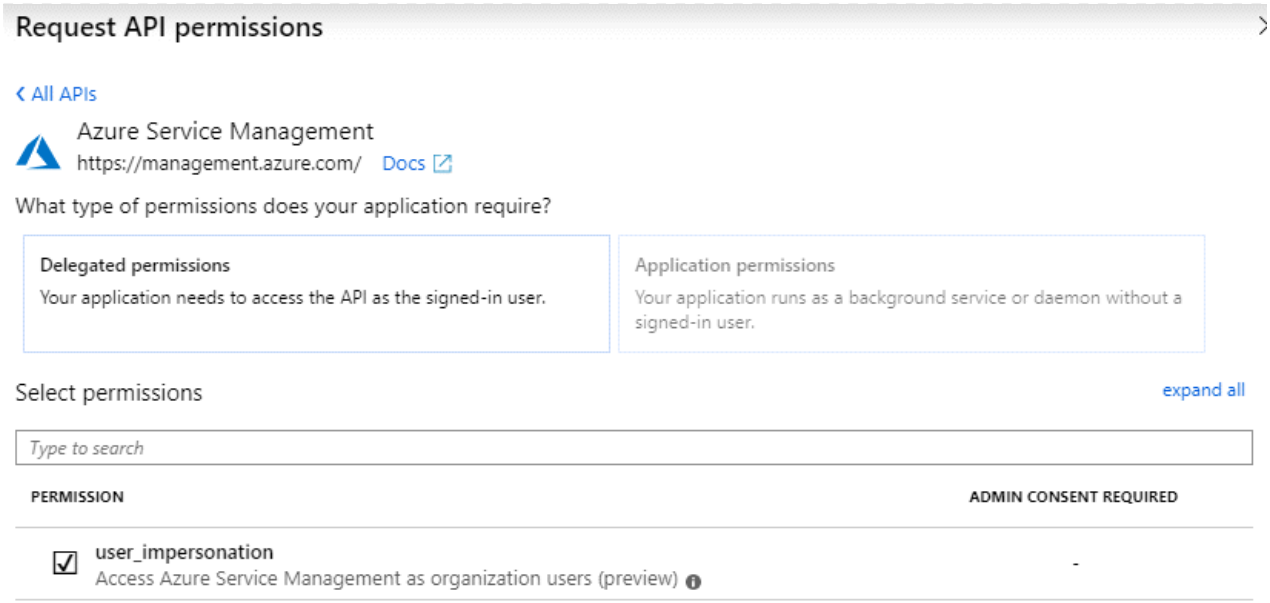
   Se você quiser gerenciar recursos em várias assinaturas do Azure, deverá vincular a entidade de serviço a cada uma dessas assinaturas. Por exemplo, o Console permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.
3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

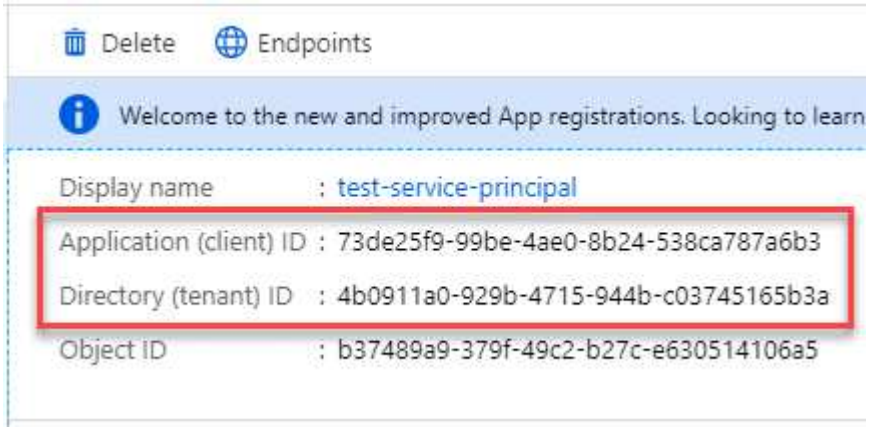


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



Obtenha o ID do aplicativo e o ID do diretório para o aplicativo

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.

Resultado

Seu principal serviço agora está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no Console ao criar o agente do Console.

Etapa 4: criar o agente do console

Crie o agente do Console diretamente do NetApp Console.

Sobre esta tarefa

- A criação do agente do Console a partir do Console implanta uma máquina virtual no Azure usando uma configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .
- Quando o Console implanta o agente do Console, ele cria uma função personalizada e a atribui à VM do agente do Console. Esta função inclui permissões que permitem ao agente do Console gerenciar recursos do Azure. Você precisa garantir que a função seja mantida atualizada à medida que novas permissões forem adicionadas em versões subsequentes. "Saiba mais sobre a função personalizada do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- Uma assinatura do Azure.
- Uma VNet e uma sub-rede na região do Azure de sua escolha.
- Detalhes sobre um servidor proxy, caso sua organização exija um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do agente do Console. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como se conectar a uma VM Linux no Azure"

- Se você não quiser que o Console crie automaticamente uma função do Azure para o agente do Console, será necessário criar sua própria"usando a política nesta página" .

  Essas permissões são para o próprio agente do Console. É um conjunto diferente de permissões do que você configurou anteriormente para implantar a VM do agente do Console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > Azure**
3. Na página **Revisão**, revise os requisitos para implantar um agente. Esses requisitos também estão detalhados acima nesta página.
4. Na página **Autenticação de Máquina Virtual**, selecione a opção de autenticação que corresponde à forma como você configura as permissões do Azure:

   - Selecione **Fazer login** para fazer login na sua conta da Microsoft, que deve ter as permissões necessárias.

     O formulário é de propriedade e hospedado pela Microsoft. Suas credenciais não são fornecidas à NetApp.

     Se você já estiver conectado a uma conta do Azure, o Console usará essa conta automaticamente. Se você tiver várias contas, talvez seja necessário sair primeiro para garantir que está usando a conta correta.

   - Selecione **Principal do serviço do Active Directory** para inserir informações sobre o principal do serviço do Microsoft Entra que concede as permissões necessárias:
     - ID do aplicativo (cliente)
     - ID do diretório (inquilino)
     - Segredo do cliente

   Aprenda como obter esses valores para um principal de serviço .

5. Na página **Autenticação de Máquina Virtual**, escolha uma assinatura do Azure, um local, um novo grupo de recursos ou um grupo de recursos existente e, em seguida, escolha um método de autenticação para a máquina virtual do agente do Console que você está criando.

   O método de autenticação para a máquina virtual pode ser uma senha ou uma chave pública SSH.

   "Saiba mais sobre como se conectar a uma VM Linux no Azure"

6. Na página **Detalhes**, insira um nome para o agente, especifique as tags e escolha se deseja que o Console crie uma nova função com as permissões necessárias ou se deseja selecionar uma função existente configurada com"as permissões necessárias" .

   Observe que você pode escolher as assinaturas do Azure associadas a essa função. Cada assinatura escolhida fornece ao agente do Console permissões para gerenciar recursos nessa assinatura (por exemplo, Cloud Volumes ONTAP).

7. Na página **Rede**, escolha uma VNet e uma sub-rede, se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
   - Na página **Grupo de segurança**, escolha se deseja criar um novo grupo de segurança ou se deseja selecionar um grupo de segurança existente que permita as regras de entrada e saída necessárias.

     "Exibir regras de grupo de segurança para o Azure" .

8. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide

os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

9. Selecione **Adicionar**.

   O Console prepara o agente em cerca de 10 minutos. Permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso no Console.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver o armazenamento de Blobs do Azure na mesma conta do Azure onde criou o agente do Console, verá o armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no NetApp Console"

Crie um agente de console no Azure Marketplace

Você pode criar um agente de console no Azure diretamente do Azure Marketplace. Para criar um agente do Console no Azure Marketplace, você precisa configurar sua rede, preparar as permissões do Azure, revisar os requisitos da instância e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Análise"Limitações do agente do console" .

Etapa 1: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console atenda aos seguintes requisitos. Esses requisitos permitem que o agente do Console gerencie recursos na sua nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito garante que uma conexão do Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um Azure Private Link"

VNet e sub-rede

Ao criar o agente do Console, você precisa especificar a VNet e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Implemente os requisitos de rede após criar o agente do Console.

Etapa 2: Revisar os requisitos da VM

Ao criar o agente do Console, escolha um tipo de máquina virtual que atenda aos seguintes requisitos.

CPU

8 núcleos ou 8 vCPUs

BATER

32 GB

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda Standard_D8s_v3.

Etapa 3: Configurar permissões

Você pode fornecer permissões das seguintes maneiras:

- Opção 1: atribuir uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída pelo sistema.
- Opção 2: forneça ao Console as credenciais para uma entidade de serviço do Azure que tenha as permissões necessárias.

Siga estas etapas para configurar permissões para o Console.

Função personalizada

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

Passos

1. Se você estiver planejando instalar manualmente o software em seu próprio host, habilite uma identidade gerenciada atribuída pelo sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configurar identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do"permissões de função personalizadas para o Conector" e salvá-los em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID de cada assinatura do Azure que deseja usar com o NetApp Console.

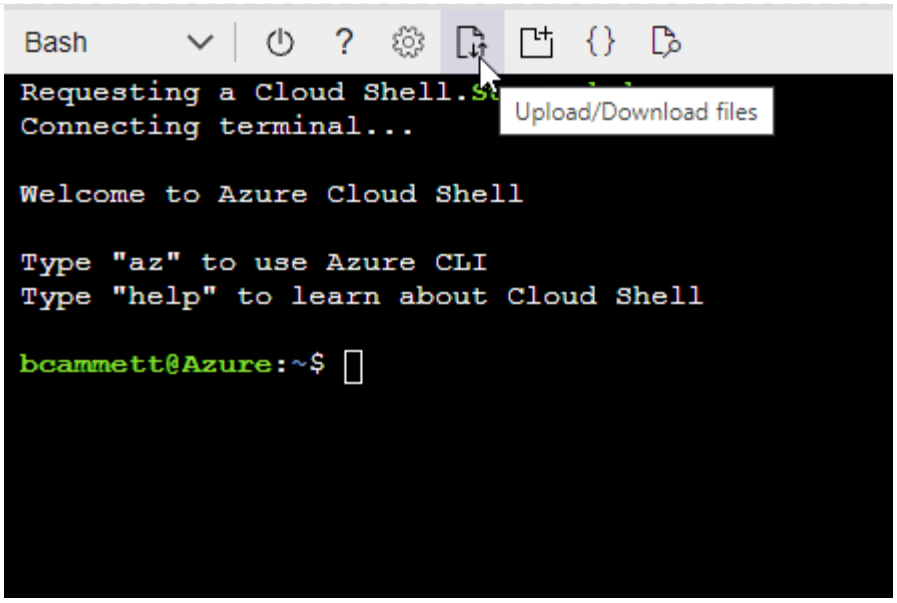
   Exemplo

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Começar "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.



c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition agent_Policy.json
```

Diretor de serviço

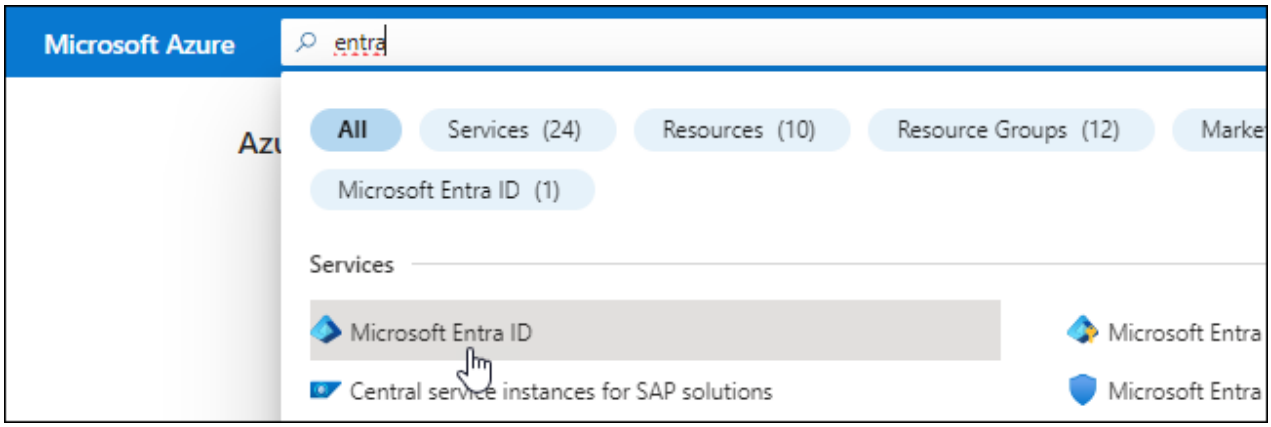
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.
5. Especifique detalhes sobre o aplicativo:

- **Nome**: Digite um nome para o aplicativo.
- **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
- **URI de redirecionamento**: Você pode deixar este campo em branco.

6. Selecione **Registrar**.

Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo a uma função

1. Crie uma função personalizada:

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

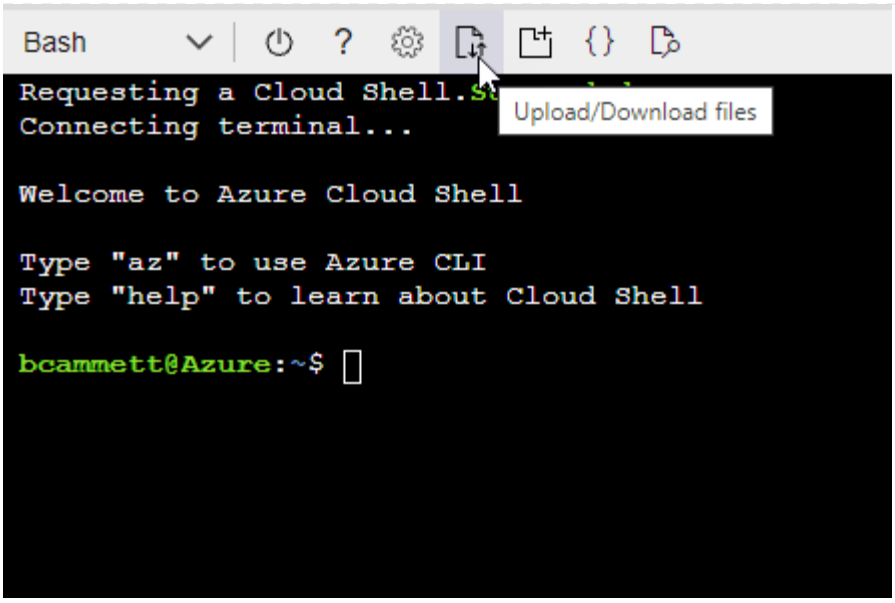
Exemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Começar "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.



- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

   a. No portal do Azure, abra o serviço **Assinaturas**.

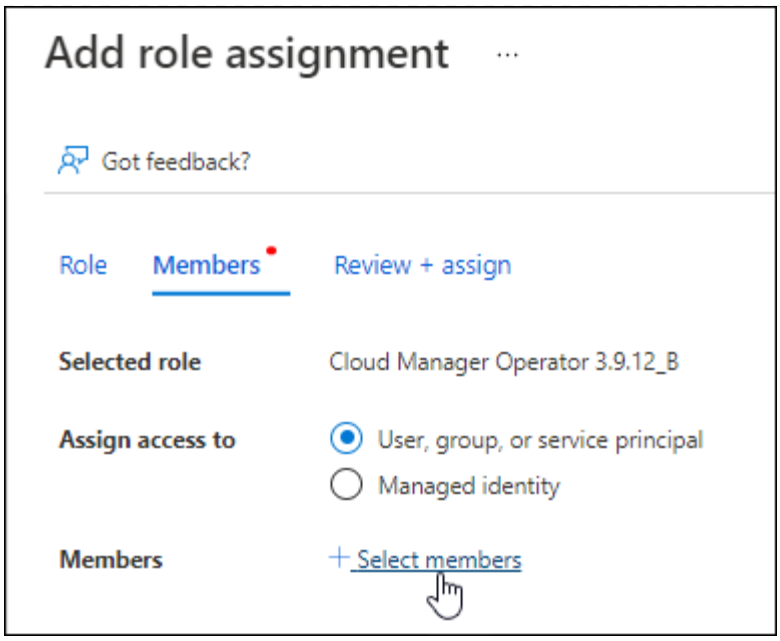
   b. Selecione a assinatura.

   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.

   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

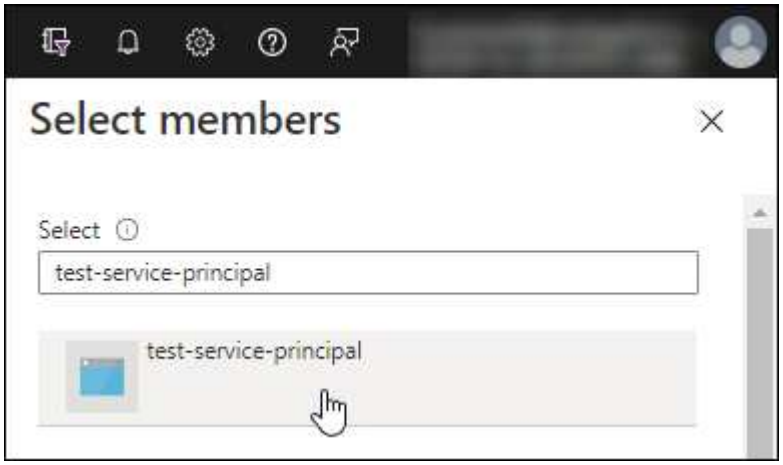
   e. Na aba **Membros**, complete os seguintes passos:

      - Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
      - Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

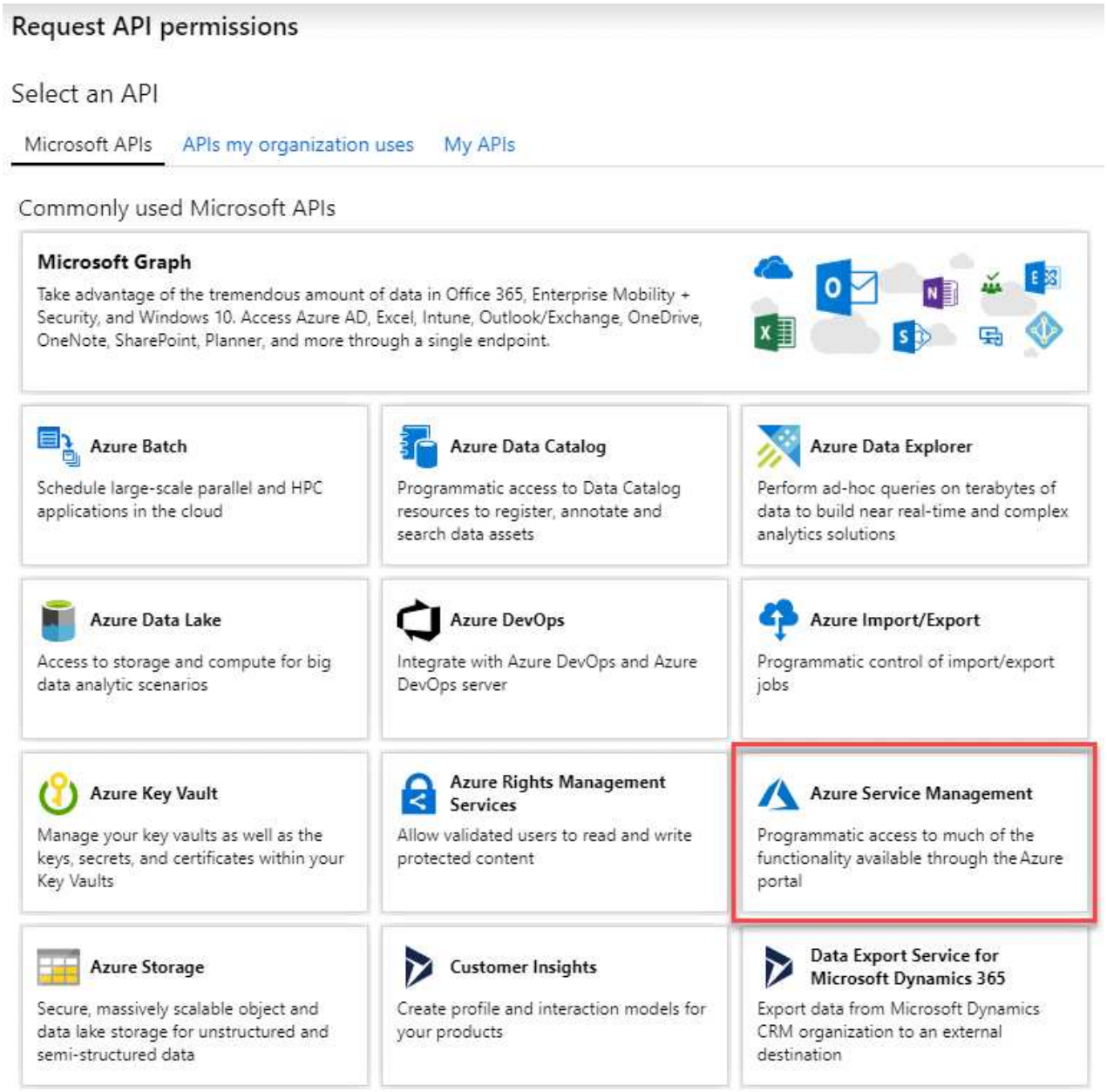
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

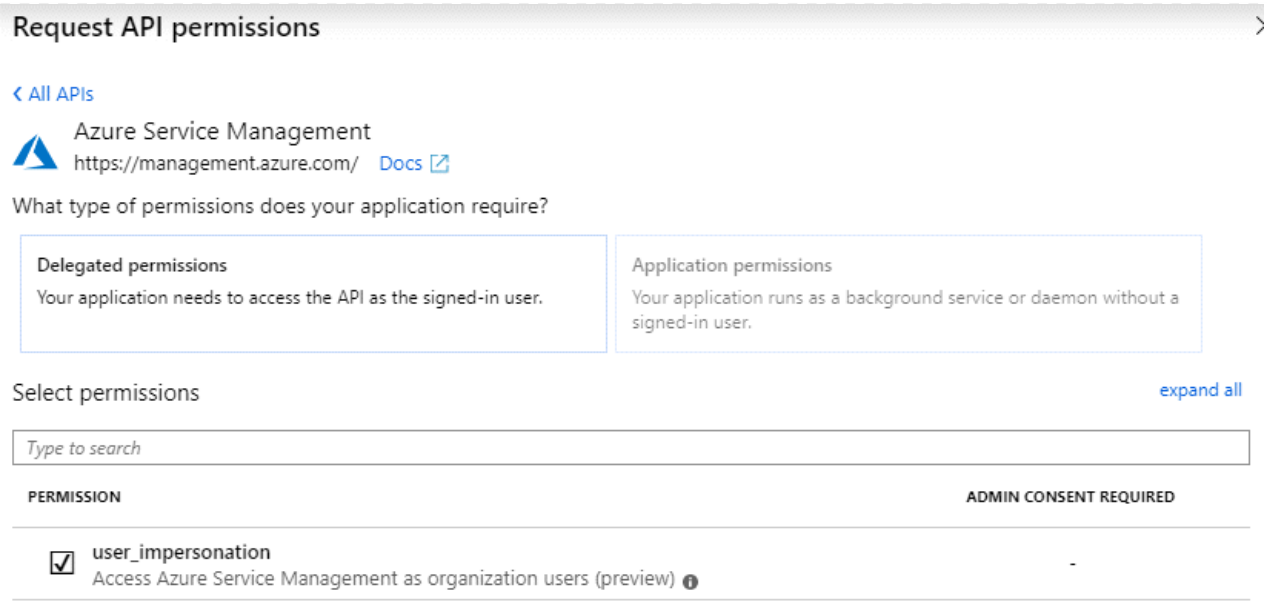
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.

3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

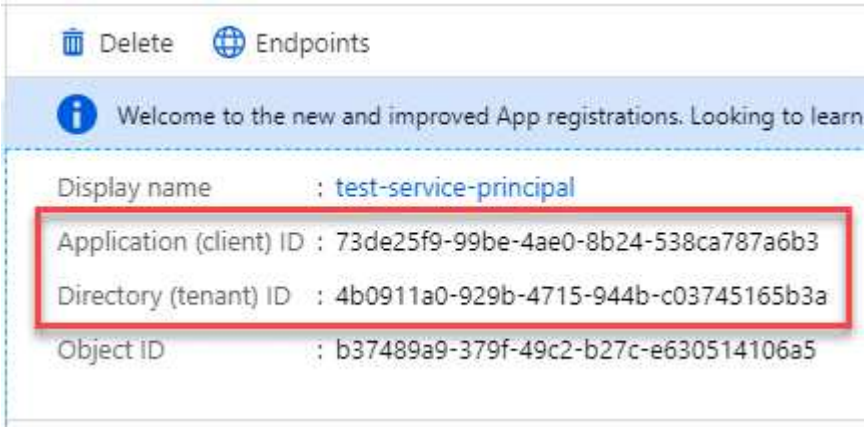


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



Obtenha o ID do aplicativo e o ID do diretório para o aplicativo

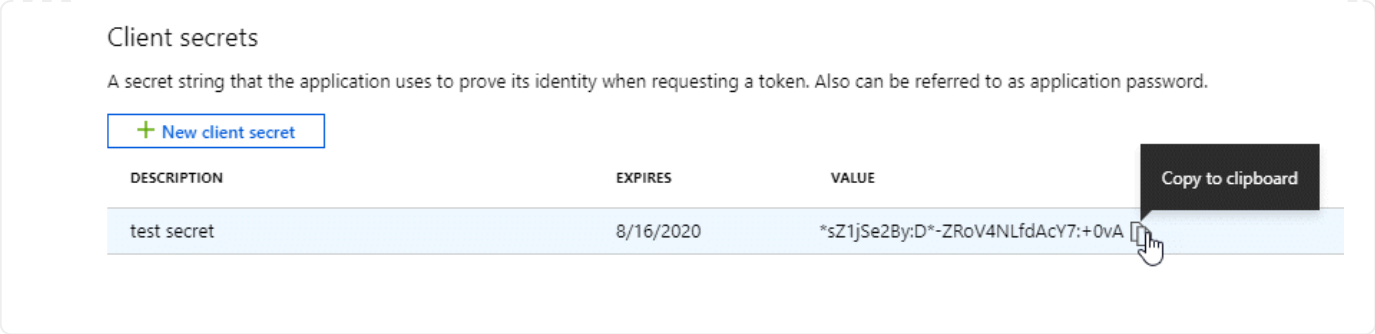
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.



Etapa 4: criar o agente do console

Inicie o agente do Console diretamente do Azure Marketplace.

Sobre esta tarefa

A criação do agente do Console no Azure Marketplace configura uma máquina virtual com uma configuração padrão. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- Uma assinatura do Azure.
- Uma VNet e uma sub-rede na região do Azure de sua escolha.
- Detalhes sobre um servidor proxy, caso sua organização exija um proxy para todo o tráfego de saída da Internet:
  - Endereço IP
  - Credenciais
  - Certificado HTTPS
- Uma chave pública SSH, se você quiser usar esse método de autenticação para a máquina virtual do agente do Console. A outra opção para o método de autenticação é usar uma senha.

  "Saiba mais sobre como se conectar a uma VM Linux no Azure"

- Se você não quiser que o Console crie automaticamente uma função do Azure para o agente do Console, será necessário criar sua própria"usando a política nesta página" .

  Essas permissões são para a própria instância do agente do Console. É um conjunto diferente de permissões do que você configurou anteriormente para implantar a VM do agente do Console.

Passos

1. Acesse a página da VM do agente do NetApp Console no Azure Marketplace.

   "Página do Azure Marketplace para regiões comerciais"

2. Selecione **Obter agora** e depois selecione **Continuar**.
3. No portal do Azure, selecione **Criar** e siga as etapas para configurar a máquina virtual.

   Observe o seguinte ao configurar a VM:

   - **Tamanho da VM**: escolha um tamanho de VM que atenda aos requisitos de CPU e RAM.

Recomendamos Standard_D8s_v3.

- **Discos**: O agente do Console pode ter desempenho ideal com discos HDD ou SSD.
- **Grupo de segurança de rede**: O agente do Console requer conexões de entrada usando SSH, HTTP e HTTPS.

  "Exibir regras de grupo de segurança para o Azure" .

- Identidade*: Em **Gerenciamento**, selecione **Ativar identidade gerenciada atribuída pelo sistema**.

  Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual do agente do Console se identifique no Microsoft Entra ID sem fornecer nenhuma credencial. "Saiba mais sobre identidades gerenciadas para recursos do Azure" .

4. Na página **Revisar + criar**, revise suas seleções e selecione **Criar** para iniciar a implantação.

   O Azure implanta a máquina virtual com as configurações especificadas. Você deverá ver a máquina virtual e o software do agente do console em execução em cerca de dez minutos.

   Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."

5. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

6. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Mantenha o modo restrito desabilitado para usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend do Console. Se for esse o caso,"siga os passos para começar a usar o Console no modo restrito" .

   d. Selecione **Vamos começar**.

Resultado

Agora você instalou o agente do Console e o configurou com sua organização do Console.

Se você tiver armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o agente do Console, verá um sistema de armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no Console"

Etapa 5: fornecer permissões ao agente do Console

Agora que você criou o agente do Console, precisa fornecer a ele as permissões que configurou anteriormente. Fornecer as permissões permite que o agente do Console gerencie seus dados e infraestrutura de armazenamento no Azure.

Função personalizada

Acesse o portal do Azure e atribua a função personalizada do Azure à máquina virtual do agente do Console para uma ou mais assinaturas.

Passos

1. No Portal do Azure, abra o serviço **Assinaturas** e selecione sua assinatura.

   É importante atribuir a função do serviço **Assinaturas** porque isso especifica o escopo da atribuição de função no nível da assinatura. O *escopo* define o conjunto de recursos aos quais o acesso se aplica. Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações no NetApp Console será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do RBAC do Azure"

2. Selecione **Controle de acesso (IAM)** > **Adicionar** > **Adicionar atribuição de função**.
3. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

   Operador do console é o nome padrão fornecido na política. Se você escolheu um nome diferente para a função, selecione esse nome.

4. Na aba **Membros**, complete os seguintes passos:
   a. Atribuir acesso a uma **Identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do agente do Console foi criada, em **Identidade gerenciada**, escolha **Máquina virtual** e selecione a máquina virtual do agente do Console.
   c. Selecione **Selecionar**.
   d. Selecione **Avançar**.
   e. Selecione **Revisar + atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, alterne para essa assinatura e repita essas etapas.

O que vem a seguir?

Vá para o "NetApp Console" para começar a usar o agente do Console.

Diretor de serviço

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
   b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
      - ID do aplicativo (cliente)
      - ID do diretório (inquilino)
      - Segredo do cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

O Console agora tem as permissões necessárias para executar ações no Azure em seu nome.

Instalar manualmente o agente do Console no Azure

Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões do Azure, instalar o agente do Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

O software do agente do Console deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta e assim por diante.

> O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console requer um host dedicado. Qualquer arquitetura é suportada, desde que atenda a estes requisitos de tamanho:

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB é recomendado para o host, com os seguintes requisitos de partição:
  - `/opt`: 120 GiB de espaço devem estar disponíveis

    O agente usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

  - `/var`: 40 GiB de espaço devem estar disponíveis

    O agente do console requer este espaço em `/var` Porque o Podman ou o Docker são projetados para criar contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório e `/var/lib/docker` para Docker. Montagens externas ou links simbólicos não funcionam neste espaço.

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda Standard_D8s_v3.

Hipervisor

É necessário um hipervisor bare metal ou hospedado certificado para executar um sistema operacional compatível.

Requisitos do sistema operacional e do contêiner

O agente do Console é compatível com os seguintes sistemas operacionais ao usar o Console no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o agente.

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Red Hat Enterprise Linux		9,6 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	4.0.0 ou posterior com o Console no modo padrão ou no modo restrito.	Podman versão 5.4.0 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo		9.1 a 9.4 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.9.4 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo		8,6 a 8,10 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.6.1 ou 4.9.4 com podman-compose 1.0.6. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo	Ubuntu		24,04 LTS	3.9.45 ou posterior com o NetApp Console no modo padrão ou restrito
Docker Engine 23.06 para 28.0.0.	Não suportado		22,04 LTS	3.9.50 ou posterior

Etapa 2: instalar o Podman ou o Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine é necessário antes de instalar o agente.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas .

- O Docker Engine é necessário para o Ubuntu.

  Veja as versões suportadas do Docker Engine .

Exemplo 2. Passos

Podman

Siga estas etapas para instalar e configurar o Podman:

- Habilite e inicie o serviço podman.socket
- Instalar python3
- Instale o pacote podman-compose versão 1.0.6
- Adicione podman-compose à variável de ambiente PATH
- Se estiver usando o Red Hat Enterprise Linux, verifique se sua versão do Podman está usando o DNS Netavark Aardvark em vez do CNI

Ajuste a porta aardvark-dns (padrão: 53) após instalar o agente para evitar conflitos de porta DNS. Siga as instruções para configurar a porta.

Passos

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   Você pode obter o Podman nos repositórios oficiais do Red Hat Enterprise Linux.

   a. Para Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   c. Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

3. Habilite e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ele ainda não estiver disponível no seu sistema.

   Esta etapa é necessária porque o podman-compose está disponível no repositório Extra Packages for Enterprise Linux (EPEL).

6. Se estiver usando o Red Hat Enterprise 9:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Instale o pacote podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se estiver usando o Red Hat Enterprise Linux 8:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Instale o pacote podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   Usando o `dnf install` O comando atende ao requisito de adicionar podman-compose à variável de ambiente PATH. O comando de instalação adiciona podman-compose a /usr/bin, que já está incluído no `secure_path` opção no host.

   c. Se estiver usando o Red Hat Enterprise Linux 8, verifique se sua versão do Podman está usando o NetAvark com o DNS Aardvark em vez do CNI.

i. Verifique se o seu networkBackend está definido como CNI executando o seguinte comando:

```
podman info | grep networkBackend
```

ii. Se o networkBackend estiver definido como `CNI` , você precisará alterá-lo para `netavark` .

iii. Instalar `netavark` e `aardvark-dns` usando o seguinte comando:

```
dnf install aardvark-dns netavark
```

iv. Abra o `/etc/containers/containers.conf` arquivo e modifique a opção network_backend para usar "netavark" em vez de "cni".

Se `/etc/containers/containers.conf` não existe, faça as alterações de configuração para `/usr/share/containers/containers.conf` .

v. Reinicie o podman.

```
systemctl restart podman
```

vi. Confirme se networkBackend foi alterado para "netavark" usando o seguinte comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga a documentação do Docker para instalar o Docker Engine.

Passos

1. "Ver instruções de instalação do Docker"

   Siga as etapas para instalar uma versão compatível do Docker Engine. Não instale a versão mais recente, pois ela não é suportada pelo Console.

2. Verifique se o Docker está habilitado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Etapa 3: configurar a rede

Certifique-se de que o local de rede onde você planeja instalar o agente do Console suporte os seguintes requisitos. Atender a esses requisitos permite que o agente do Console gerencie recursos e processos dentro do seu ambiente de nuvem híbrida.

Região Azure

Se você usar o Cloud Volumes ONTAP, o agente do Console deverá ser implantado na mesma região do Azure que os sistemas Cloud Volumes ONTAP que ele gerencia ou no "Par de regiões do Azure" para os sistemas Cloud Volumes ONTAP . Esse requisito garante que uma conexão do Azure Private Link seja usada entre o Cloud Volumes ONTAP e suas contas de armazenamento associadas.

"Saiba como o Cloud Volumes ONTAP usa um Azure Private Link"

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.

Pontos finais	Propósito
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP

- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Etapa 4: configurar permissões de implantação do agente do console

Você precisa fornecer permissões do Azure ao agente do Console usando uma das seguintes opções:

- Opção 1: atribuir uma função personalizada à VM do Azure usando uma identidade gerenciada atribuída pelo sistema.
- Opção 2: forneça ao agente do Console as credenciais para uma entidade de serviço do Azure que tenha as permissões necessárias.

Siga as etapas para preparar permissões para o agente do Console.

Criar uma função personalizada para implantação do agente do Console

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

Passos

1. Se você estiver planejando instalar manualmente o software em seu próprio host, habilite uma identidade gerenciada atribuída pelo sistema na VM para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

   "Documentação do Microsoft Azure: Configurar identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

2. Copie o conteúdo do"permissões de função personalizadas para o Conector" e salvá-los em um arquivo JSON.
3. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

   Você deve adicionar o ID de cada assinatura do Azure que deseja usar com o NetApp Console.

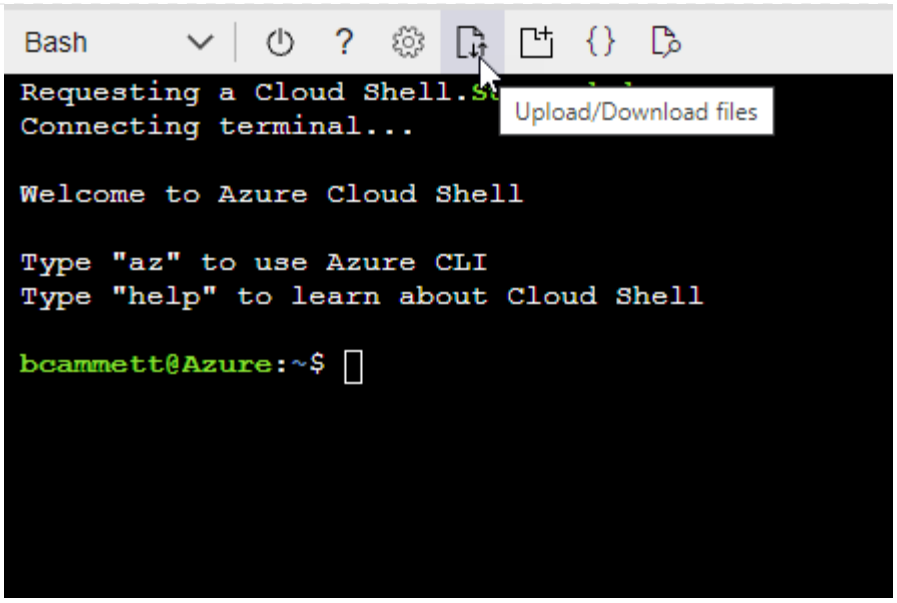
   Exemplo

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

4. Use o arquivo JSON para criar uma função personalizada no Azure.

   As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

   a. Começar "Azure Cloud Shell" e escolha o ambiente Bash.
   b. Carregue o arquivo JSON.



c. Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition agent_Policy.json
```

Diretor de serviço

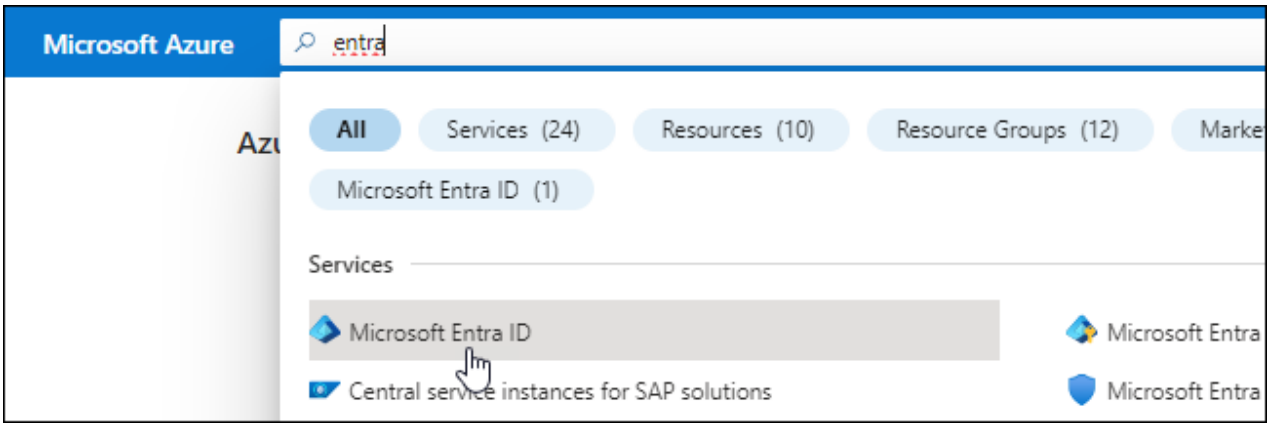
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o agente do Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.
5. Especifique detalhes sobre o aplicativo:

- **Nome**: Digite um nome para o aplicativo.
- **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
- **URI de redirecionamento**: Você pode deixar este campo em branco.

6. Selecione **Registrar**.

Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo a uma função

1. Crie uma função personalizada:

Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

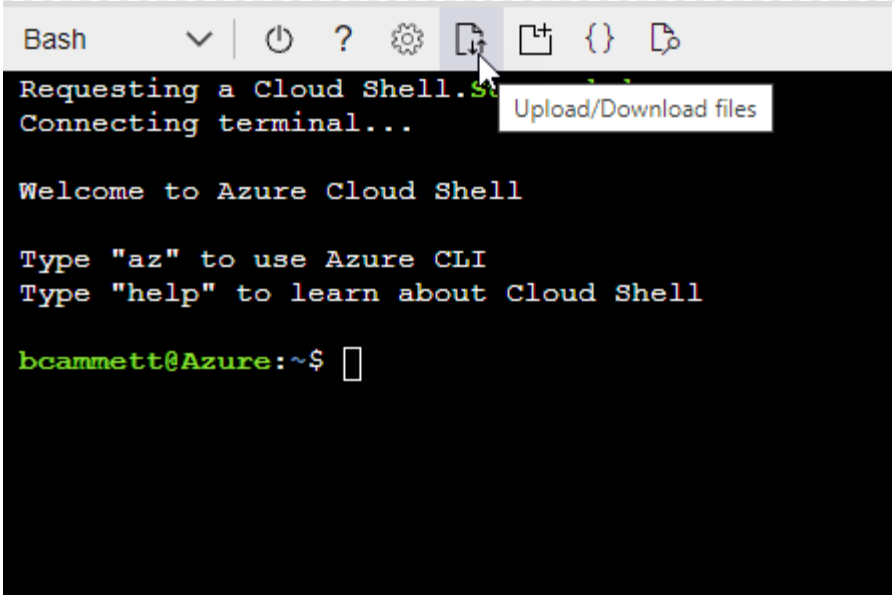
Exemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Começar "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.



- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

   a. No portal do Azure, abra o serviço **Assinaturas**.

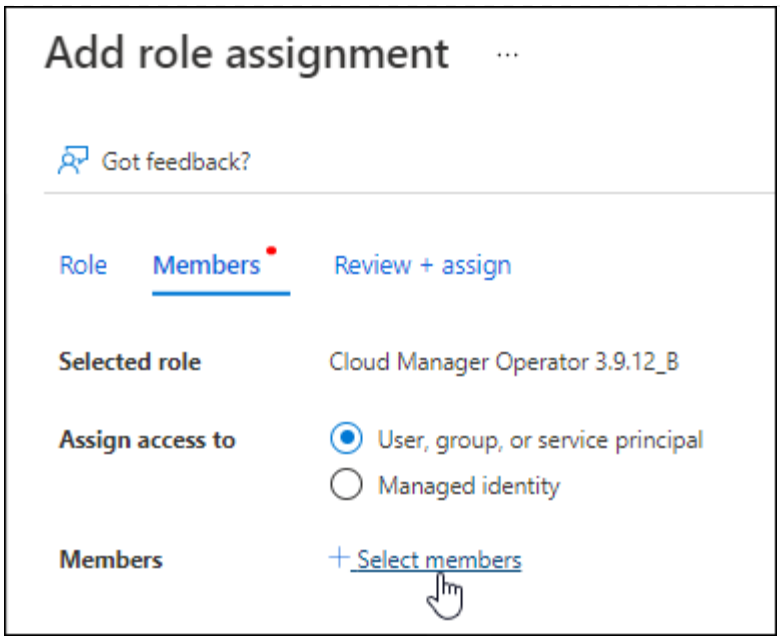
   b. Selecione a assinatura.

   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.

   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

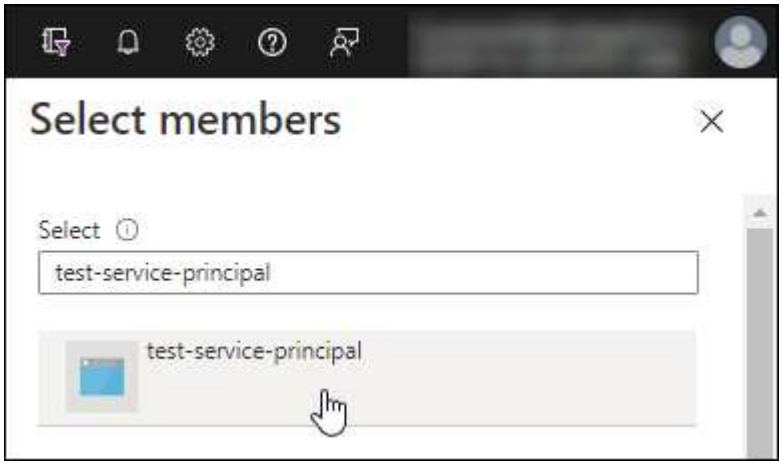
   e. Na aba **Membros**, complete os seguintes passos:

      - Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
      - Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

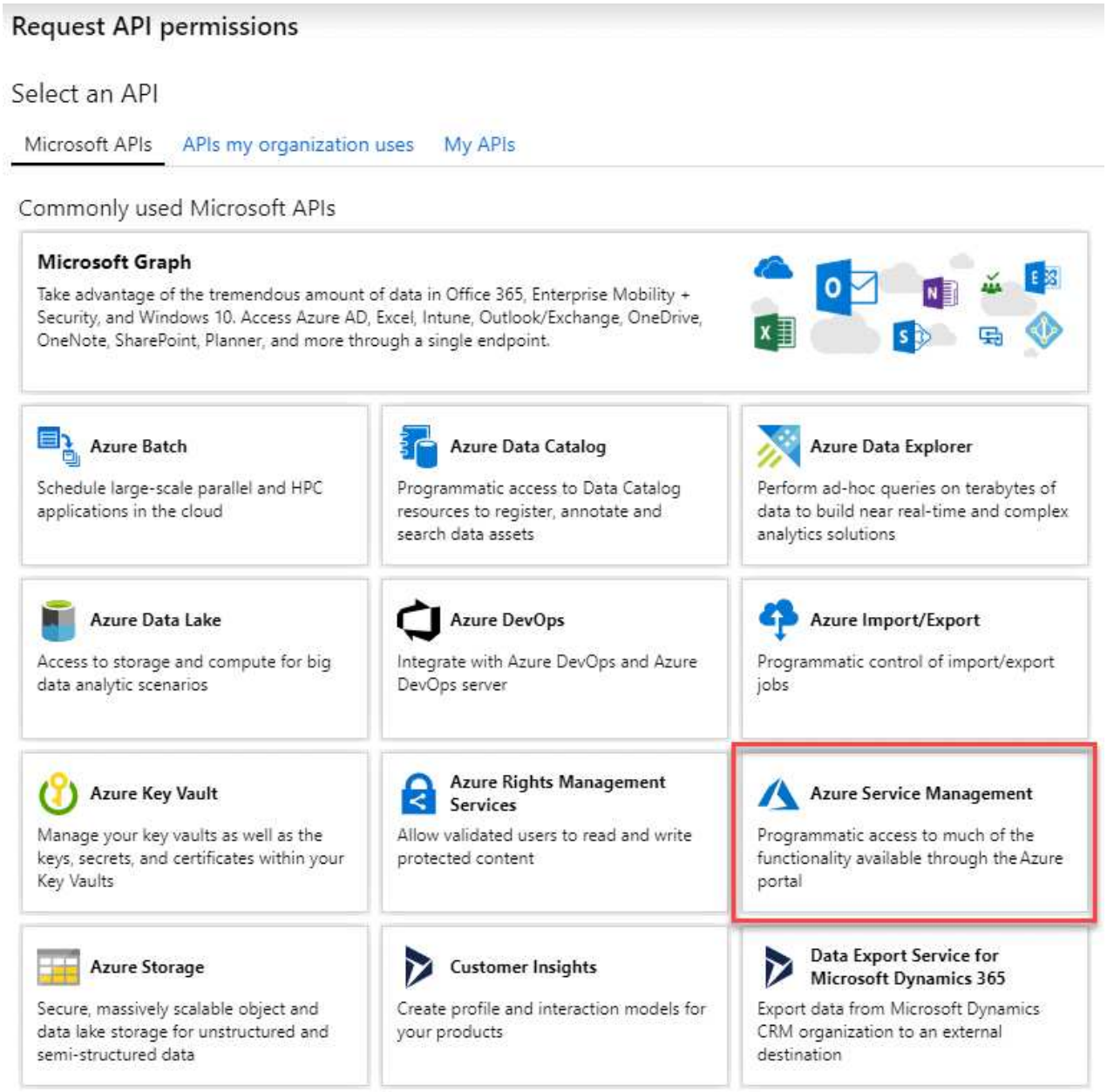
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

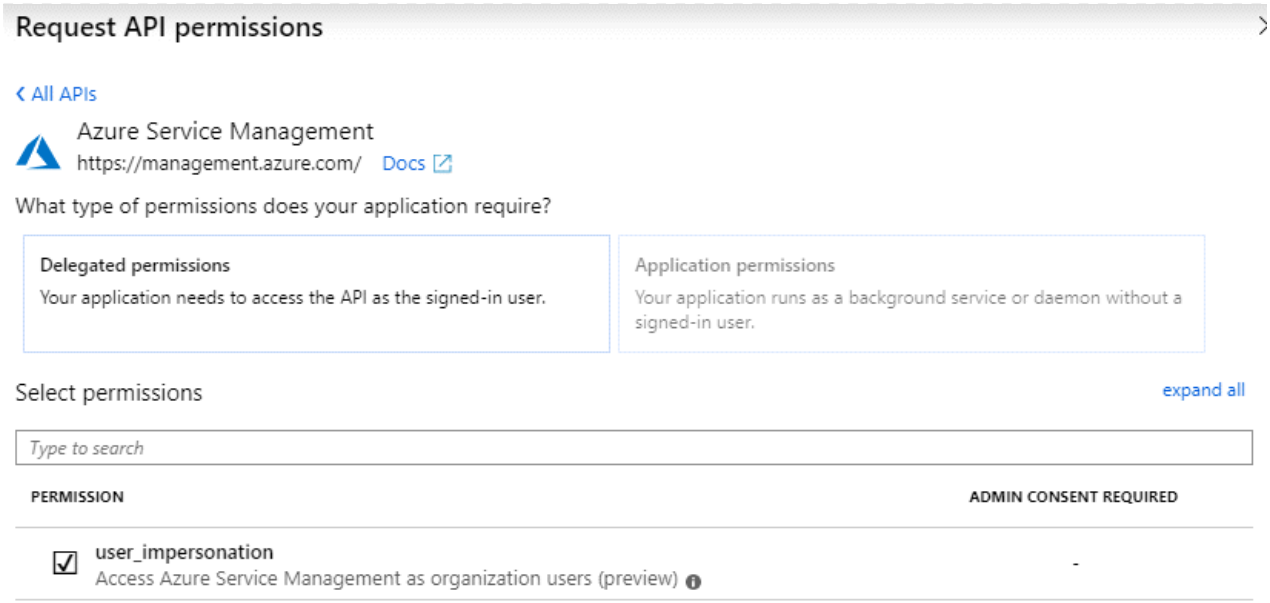
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.

3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

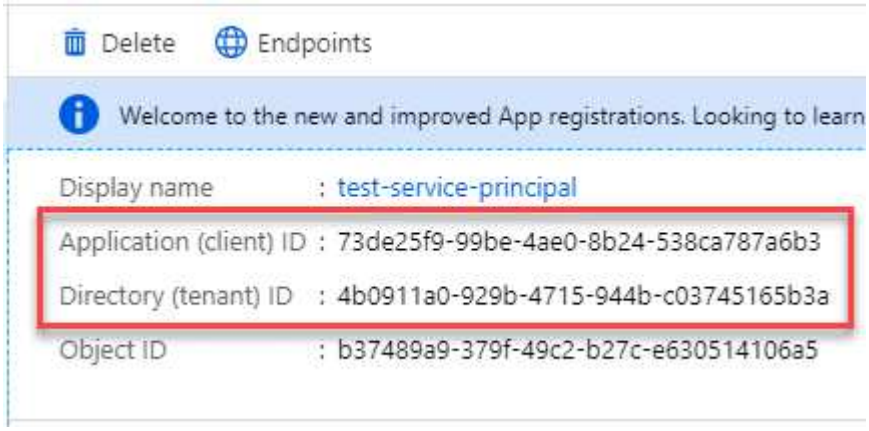


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



Obtenha o ID do aplicativo e o ID do diretório para o aplicativo

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.

Resultado

Seu principal serviço agora está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no Console ao adicionar uma conta do Azure.

Etapa 5: instalar o agente do console

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software no seu próprio host Linux.

Antes de começar

Você deve ter o seguinte:

- Privilégios de root para instalar o agente do Console.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do agente do Console.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy de interceptação.

> Não é possível definir um certificado para um servidor proxy transparente ao instalar manualmente o agente do Console. Se precisar definir um certificado para um servidor proxy transparente, você deverá usar o Console de Manutenção após a instalação. Saiba mais sobre o"Console de manutenção do agente" .

- Uma identidade gerenciada habilitada na VM no Azure para que você possa fornecer as permissões necessárias do Azure por meio de uma função personalizada.

  "Documentação do Microsoft Azure: Configurar identidades gerenciadas para recursos do Azure em uma VM usando o portal do Azure"

Sobre esta tarefa

Após a instalação, o agente do Console se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

```
unset http_proxy
unset https_proxy
```

Se você não remover essas variáveis do sistema, a instalação falhará.

2. Baixe o software do agente do Console e copie-o para o host Linux. Você pode baixá-lo tanto do NetApp Console quanto do site de suporte da NetApp .
   - NetApp Console: Acesse **Agentes > Gerenciamento > Implantar agente > Local > Instalação manual**.

     Escolha baixar os arquivos de instalação do agente ou um URL para os arquivos.

   - Site de suporte da NetApp (necessário caso você ainda não tenha acesso ao Console) "Site de suporte da NetApp" ,
3. Atribua permissões para executar o script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

Onde <versão> é a versão do agente do Console que você baixou.

4. Se estiver instalando em um ambiente de nuvem governamental, desative as verificações de configuração."Aprenda como desabilitar verificações de configuração para instalações manuais."
5. Execute o script de instalação.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Você precisará adicionar informações de proxy se sua rede exigir um proxy para acesso à internet. Você pode adicionar um proxy explícito durante a instalação. Os parâmetros `--proxy` e `--cacert` são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy explícito, precisará inserir os parâmetros conforme mostrado.

Se você deseja configurar um proxy transparente, pode fazê-lo após a instalação. "Saiba mais sobre o console de manutenção do agente."

+

Aqui está um exemplo de configuração de um servidor proxy explícito com um certificado assinado por uma CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` configura o agente do Console para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

+ * http://endereço:porta * http://nome-do-usuário:senha@endereço:porta * http://nome-do-domínio%92nome-do-usuário:senha@endereço:porta * https://endereço:porta * https://nome-do-usuário:senha@endereço:porta * https://nome-do-domínio%92nome-do-usuário:senha@endereço:porta

+ Observe o seguinte:

+ **O usuário pode ser um usuário local ou um usuário de domínio.** Para um usuário de domínio, você deve usar o código ASCII para uma \ conforme mostrado acima. **O agente do Console não oferece suporte a nomes de usuário ou senhas que incluam o caractere @.** Se a senha incluir algum dos seguintes caracteres especiais, você deve escapar esse caractere especial adicionando uma barra invertida antes dele: & ou !

+ Por exemplo:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Se você usou o Podman, precisará ajustar a porta aardvark-dns.

   a. SSH para a máquina virtual do agente do Console.

   b. Abra o arquivo podman */usr/share/containers/containers.conf* e modifique a porta escolhida para o serviço DNS do Aardvark. Por exemplo, altere para 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

      Por exemplo:

   ```
   # Port to use for dns forwarding daemon with netavark in rootful bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services should
   # run on the machine.
   #
   dns_bind_port = 54
   ```

   a. Reinicie a máquina virtual do agente do Console.

2. Aguarde a conclusão da instalação.

   No final da instalação, o serviço do agente do Console (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

   Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

https://ipaddress

2. Após efetuar login, configure o agente do Console:
   a. Especifique a organização a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

   d. Selecione **Vamos começar**.

Se você tiver armazenamento de Blobs do Azure na mesma assinatura do Azure em que criou o agente do Console, verá um sistema de armazenamento de Blobs do Azure aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o armazenamento de Blobs do Azure no NetApp Console"

Etapa 6: fornecer permissões ao NetApp Console

Agora que você instalou o agente do Console, precisa fornecer a ele as permissões do Azure que você configurou anteriormente. Fornecer as permissões permite que o Console gerencie seus dados e infraestrutura de armazenamento no Azure.

Função personalizada

Acesse o portal do Azure e atribua a função personalizada do Azure à máquina virtual do agente do Console para uma ou mais assinaturas.

Passos

1. No Portal do Azure, abra o serviço **Assinaturas** e selecione sua assinatura.

   É importante atribuir a função do serviço **Assinaturas** porque isso especifica o escopo da atribuição de função no nível da assinatura. O *escopo* define o conjunto de recursos aos quais o acesso se aplica. Se você especificar um escopo em um nível diferente (por exemplo, no nível da máquina virtual), sua capacidade de concluir ações no NetApp Console será afetada.

   "Documentação do Microsoft Azure: Entenda o escopo do RBAC do Azure"

2. Selecione **Controle de acesso (IAM)** > **Adicionar** > **Adicionar atribuição de função**.
3. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

   Operador do console é o nome padrão fornecido na política. Se você escolheu um nome diferente para a função, selecione esse nome.

4. Na aba **Membros**, complete os seguintes passos:
   a. Atribuir acesso a uma **Identidade gerenciada**.
   b. Selecione **Selecionar membros**, selecione a assinatura na qual a máquina virtual do agente do Console foi criada, em **Identidade gerenciada**, escolha **Máquina virtual** e selecione a máquina virtual do agente do Console.
   c. Selecione **Selecionar**.
   d. Selecione **Avançar**.
   e. Selecione **Revisar + atribuir**.
   f. Se você quiser gerenciar recursos em assinaturas adicionais do Azure, alterne para essa assinatura e repita essas etapas.

O que vem a seguir?

Vá para o "NetApp Console" para começar a usar o agente do Console.

Diretor de serviço

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
   b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
      - ID do aplicativo (cliente)
      - ID do diretório (inquilino)
      - Segredo do cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

O agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome.

Google Cloud

Opções de instalação do agente de console no Google Cloud

Existem algumas maneiras diferentes de criar um agente do Console no Google Cloud. Diretamente do NetApp Console é a maneira mais comum.

As seguintes opções de instalação estão disponíveis:

- "Crie o agente do Console diretamente do Console"(esta é a opção padrão)

  Esta ação inicia uma instância de VM executando Linux e o software do agente do Console em uma VPC de sua escolha.

- "Crie o agente do Console usando a plataforma Google"

  Esta ação também inicia uma instância de VM executando o Linux e o software do agente do Console, mas a implantação é iniciada diretamente do Google Cloud, e não do Console.

- "Baixe e instale manualmente o software em seu próprio host Linux"

A opção de instalação escolhida afeta a maneira como você se prepara para a instalação. Isso inclui como você fornece ao Console as permissões necessárias para autenticar e gerenciar recursos no Google Cloud.

Crie um agente de console no Google Cloud a partir do NetApp Console

Você pode criar um agente do Console no Google Cloud a partir do Console. Você precisa configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Configure a rede para garantir que o agente do Console possa gerenciar recursos, com conexões a redes de destino e acesso de saída à Internet.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	Para gerenciar recursos no Google Cloud.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Implemente este requisito de rede após criar o agente do Console.

Etapa 2: configurar permissões para criar o agente do Console

Antes de poder implantar um agente do Console a partir do Console, você precisa configurar permissões para o usuário da Plataforma Google que implanta a VM do agente do Console.

Passos

1. Crie uma função personalizada na plataforma Google:

   a. Crie um arquivo YAML que inclua as seguintes permissões:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
```

```
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
```

```
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. No Google Cloud, ative o Cloud Shell.

c. Faça upload do arquivo YAML que inclui as permissões necessárias.

d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

O exemplo a seguir cria uma função chamada "agentDeployment" no nível do projeto:

gcloud iam roles create connectorDeployment --project=myproject --file=agent-deployment.yaml

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Atribua esta função personalizada ao usuário que implantará o agente do Console a partir do Console ou usando o gcloud.

"Documentação do Google Cloud: Conceder uma única função"

Etapa 3: Crie uma conta de serviço do Google Cloud para usar com o agente.

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .

b. No Google Cloud, ative o Cloud Shell.
c. Faça upload do arquivo YAML que inclui as permissões necessárias.
d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

   O exemplo a seguir cria uma função chamada "agente" no nível do projeto:

   ```
   gcloud iam roles create connector --project=myproject --file=agent.yaml
   ```

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:
   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.
   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.
   c. Selecione a função que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

      "Documentação do Google Cloud: Criação de uma conta de serviço"

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP .
   b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.
      - Insira o e-mail da conta de serviço do agente do Console.
      - Selecione a função personalizada do agente do Console.
      - Selecione **Salvar**.

   Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 4: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 5: habilitar as APIs do Google Cloud

Você deve habilitar várias APIs do Google Cloud antes de implantar o agente do Console e o Cloud Volumes ONTAP.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - API do Cloud Infrastructure Manager
   - API do Gerenciador de Implantação em Nuvem V2
   - API de registro em nuvem
   - API do Gerenciador de Recursos de Nuvem
   - API do mecanismo de computação
   - API de gerenciamento de identidade e acesso (IAM)
   - API do Serviço de Gerenciamento de Chaves em Nuvem (KMS)

     (Obrigatório somente se você estiver planejando usar o NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 6: Criar o agente do Console

Crie um agente do Console diretamente do Console.

A criação do agente do Console implanta uma instância de máquina virtual no Google Cloud usando uma configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .

Ao implantar um agente no Google Cloud, o agente cria um bucket para armazenar os arquivos de implantação.

Antes de começar

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o agente do Console e uma conta de serviço para a VM do agente do Console.
- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > Google Cloud**
3. Na página **Implantando um agente**, revise os detalhes sobre o que você precisará. Você tem duas

opções:

a. Selecione **Continuar** para se preparar para a implantação usando o guia do produto. Cada etapa do guia do produto inclui as informações contidas nesta página da documentação.

b. Selecione **Ir para a implantação** se você já se preparou seguindo as etapas desta página.

4. Siga as etapas do assistente para criar o agente do Console:

   - Se solicitado, faça login na sua conta do Google, que deve ter as permissões necessárias para criar a instância da máquina virtual.

     O formulário é de propriedade e hospedado pelo Google. Suas credenciais não são fornecidas à NetApp.

   - **Detalhes**: Insira um nome para a instância da máquina virtual, especifique tags, selecione um projeto e, em seguida, selecione a conta de serviço que tem as permissões necessárias (consulte a seção acima para obter detalhes).
   - **Localização**: especifique uma região, zona, VPC e sub-rede para a instância.
   - **Rede**: Escolha se deseja habilitar um endereço IP público e, opcionalmente, especifique uma configuração de proxy.
   - **Tags de rede**: adicione uma tag de rede à instância do agente do Console se estiver usando um proxy transparente. As tags de rede devem começar com uma letra minúscula e podem conter letras minúsculas, números e hifens. As tags devem terminar com uma letra minúscula ou um número. Por exemplo, você pode usar a tag "console-agent-proxy".
   - **Política de firewall**: escolha se deseja criar uma nova política de firewall ou selecionar uma política de firewall existente que permita as regras de entrada e saída necessárias.

     "Regras de firewall no Google Cloud"

5. Revise suas seleções para verificar se sua configuração está correta.

   a. A caixa de seleção **Validar configuração do agente** é marcada por padrão para que o Console valide os requisitos de conectividade de rede quando você implantar. Se o Console não conseguir implantar o agente, ele fornecerá um relatório para ajudar você a solucionar o problema. Se a implantação for bem-sucedida, nenhum relatório será fornecido.

   Se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, desmarque a caixa de seleção para pular a verificação de validação.

6. Selecione **Adicionar**.

   O agente estará pronto em aproximadamente 10 minutos; permaneça na página até que o processo seja concluído.

Resultado

Após a conclusão do processo, o agente do Console estará disponível para uso.

Se a implantação falhar, você poderá baixar um relatório e logs do Console para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o agente do

Console, verá um sistema do Google Cloud Storage aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o Google Cloud Storage pelo Console"

Crie um agente de console do Google Cloud

Para criar um agente do Console no Google Cloud usando o Google Cloud, você precisa configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud e, em seguida, criar o agente do Console.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: configurar a rede

Configure a rede para permitir que o agente do Console gerencie recursos e se conecte às redes de destino e à Internet.

VPC e sub-rede

Ao criar o agente do Console, você precisa especificar a VPC e a sub-rede onde ele deve residir.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	Para gerenciar recursos no Google Cloud.

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Endpoints contatados do console NetApp

À medida que você usa o NetApp Console baseado na Web fornecido pela camada SaaS, ele entra em contato com vários endpoints para concluir tarefas de gerenciamento de dados. Isso inclui endpoints que são contatados para implantar o agente do Console a partir do Console.

"Exibir a lista de endpoints contatados pelo console do NetApp" .

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Implemente este requisito de rede após criar o agente do Console.

Etapa 2: configurar permissões para criar o agente do Console

Configure permissões para o usuário do Google Cloud implantar a VM do agente do Console do Google Cloud.

Passos

1. Crie uma função personalizada na plataforma Google:

   a. Crie um arquivo YAML que inclua as seguintes permissões:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. No Google Cloud, ative o Cloud Shell.

c. Faça upload do arquivo YAML que inclui as permissões necessárias.

d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

O exemplo a seguir cria uma função chamada "connectorDeployment" no nível do projeto:

gcloud iam roles criar connectorDeployment --project=myproject --file=connector-deployment.yaml

"Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Atribua esta função personalizada ao usuário que implanta o agente do Console do Google Cloud.

   "Documentação do Google Cloud: Conceder uma única função"

Etapa 3: Configurar permissões para as operações do agente do Console

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .
   b. No Google Cloud, ative o Cloud Shell.
   c. Faça upload do arquivo YAML que inclui as permissões necessárias.
   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

      O exemplo a seguir cria uma função chamada "agente" no nível do projeto:

      ```
      gcloud iam roles create connector --project=myproject --file=agent.yaml
      ```

   "Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:
   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.
   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.
   c. Selecione a função que você acabou de criar.
   d. Conclua as etapas restantes para criar a função.

      "Documentação do Google Cloud: Criação de uma conta de serviço"

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP .
   b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.

- Insira o e-mail da conta de serviço do agente do Console.
- Selecione a função personalizada do agente do Console.
- Selecione **Salvar**.

Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 4: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 5: habilitar as APIs do Google Cloud

Habilite várias APIs do Google Cloud antes de implantar o agente do Console e o Cloud Volumes ONTAP.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - API do Cloud Infrastructure Manager
   - API do Gerenciador de Implantação em Nuvem V2
   - API de registro em nuvem
   - API do Gerenciador de Recursos de Nuvem
   - API do mecanismo de computação
   - API de gerenciamento de identidade e acesso (IAM)
   - API do Serviço de Gerenciamento de Chaves em Nuvem (KMS)

     (Obrigatório somente se você estiver planejando usar o NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 6: Criar o agente do Console

Crie um agente do Console usando o Google Cloud.

A criação do agente do Console implanta uma instância de VM no Google Cloud com a configuração padrão. Não mude para uma instância de VM menor com menos CPUs ou menos RAM depois de criar o agente do Console. "Saiba mais sobre a configuração padrão do agente do Console" .

Antes de começar

Você deve ter o seguinte:

- As permissões necessárias do Google Cloud para criar o agente do Console e uma conta de serviço para a VM do agente do Console.
- Uma VPC e uma sub-rede que atendem aos requisitos de rede.
- Uma compreensão dos requisitos da instância de VM.
  - **CPU**: 8 núcleos ou 8 vCPUs
  - **RAM**: 32 GB
  - **Tipo de máquina**: Recomendamos n2-standard-8.

    O agente do Console é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível com recursos de VM protegida.

Passos

1. Faça login no Google Cloud SDK usando seu método preferido.

Este exemplo usa um shell local com o gcloud SDK instalado, mas você também pode usar o Google Cloud Shell.

Para obter mais informações sobre o Google Cloud SDK, visite o"Página de documentação do Google Cloud SDK" .

2. Verifique se você está conectado como um usuário que possui as permissões necessárias definidas na seção acima:

```
gcloud auth list
```

A saída deve mostrar o seguinte, onde * a conta de usuário é a conta de usuário desejada para efetuar login:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. Execute o `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nome da instância
O nome da instância desejada para a instância da VM.

projeto
(Opcional) O projeto onde você deseja implantar a VM.

conta de serviço
A conta de serviço especificada na saída da etapa 2.

zona
A zona onde você deseja implantar a VM

sem endereço
(Opcional) Nenhum endereço IP externo é usado (você precisa de um NAT ou proxy na nuvem para rotear o tráfego para a Internet pública)

tag de rede
(Opcional) Adicione marcação de rede para vincular uma regra de firewall usando tags à instância do agente do Console

caminho de rede
(Opcional) Adicione o nome da rede na qual implantar o agente do Console (para uma VPC compartilhada, você precisa do caminho completo)

caminho de sub-rede
(Opcional) Adicione o nome da sub-rede para implantar o agente do Console (para uma VPC compartilhada, você precisa do caminho completo)

kms-chave-caminho
(Opcional) Adicione uma chave KMS para criptografar os discos do agente do Console (as permissões do IAM também precisam ser aplicadas)

Para mais informações sobre essas bandeiras, visite o"Documentação do SDK de computação do Google Cloud" .

Executar o comando implanta o agente do Console. A instância do agente do Console e o software devem estar em execução em aproximadamente cinco minutos.

4. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

5. Após efetuar login, configure o agente do Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.

      "Aprenda sobre gerenciamento de identidade e acesso" .

   b. Digite um nome para o sistema.

Resultado

O agente do Console agora está instalado e configurado com sua organização do Console.

Abra um navegador da web e vá para o "NetApp Console" para começar a usar o agente do Console.

Instalar manualmente o agente do Console no Google Cloud

Para instalar manualmente o agente do Console no seu próprio host Linux, você precisa revisar os requisitos do host, configurar sua rede, preparar as permissões do Google Cloud, habilitar as APIs do Google Cloud, instalar o Console e, em seguida, fornecer as permissões que você preparou.

Antes de começar

- Você deveria ter um"compreensão dos agentes do Console" .
- Você deve revisar"Limitações do agente do console" .

Etapa 1: Revise os requisitos do host

O software do agente do Console deve ser executado em um host que atenda aos requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta e assim por diante.

> O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console requer um host dedicado. Qualquer arquitetura é suportada, desde que atenda a estes requisitos de tamanho:

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB é recomendado para o host, com os seguintes requisitos de partição:
  - `/opt`: 120 GiB de espaço devem estar disponíveis

    O agente usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

  - `/var`: 40 GiB de espaço devem estar disponíveis

    O agente do console requer este espaço em `/var` Porque o Podman ou o Docker são projetados para criar contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório e `/var/lib/docker` para Docker. Montagens externas ou links simbólicos não funcionam neste espaço.

Tipo de máquina do Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda o n2-standard-8.

O agente do Console é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindada"

Hipervisor

É necessário um hipervisor bare metal ou hospedado certificado para executar um sistema operacional compatível.

Requisitos do sistema operacional e do contêiner

O agente do Console é compatível com os seguintes sistemas operacionais ao usar o Console no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o agente.

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Red Hat Enterprise Linux		9,6 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	4.0.0 ou posterior com o Console no modo padrão ou no modo restrito.	Podman versão 5.4.0 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo		9.1 a 9.4 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.9.4 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo		8,6 a 8,10 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.6.1 ou 4.9.4 com podman-compose 1.0.6. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo	Ubuntu		24,04 LTS	3.9.45 ou posterior com o NetApp Console no modo padrão ou restrito
Docker Engine 23.06 para 28.0.0.	Não suportado		22,04 LTS	3.9.50 ou posterior

Tipo de máquina do Google Cloud

Um tipo de instância que atende aos requisitos de CPU e RAM. A NetApp recomenda o n2-standard-8.

O agente do Console é compatível com o Google Cloud em uma instância de VM com um sistema operacional compatível "Recursos de VM blindada"

Etapa 2: instalar o Podman ou o Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine é necessário antes de instalar o agente.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas .

- O Docker Engine é necessário para o Ubuntu.

  Veja as versões suportadas do Docker Engine .

Exemplo 3. Passos

Podman

Siga estas etapas para instalar e configurar o Podman:

- Habilite e inicie o serviço podman.socket
- Instalar python3
- Instale o pacote podman-compose versão 1.0.6
- Adicione podman-compose à variável de ambiente PATH
- Se estiver usando o Red Hat Enterprise Linux, verifique se sua versão do Podman está usando o DNS Netavark Aardvark em vez do CNI

Ajuste a porta aardvark-dns (padrão: 53) após instalar o agente para evitar conflitos de porta DNS. Siga as instruções para configurar a porta.

Passos

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   Você pode obter o Podman nos repositórios oficiais do Red Hat Enterprise Linux.

   a. Para Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   c. Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

3. Habilite e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ele ainda não estiver disponível no seu sistema.

   Esta etapa é necessária porque o podman-compose está disponível no repositório Extra Packages for Enterprise Linux (EPEL).

6. Se estiver usando o Red Hat Enterprise 9:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Instale o pacote podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se estiver usando o Red Hat Enterprise Linux 8:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Instale o pacote podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   Usando o `dnf install` O comando atende ao requisito de adicionar podman-compose à variável de ambiente PATH. O comando de instalação adiciona podman-compose a /usr/bin, que já está incluído no `secure_path` opção no host.

   c. Se estiver usando o Red Hat Enterprise Linux 8, verifique se sua versão do Podman está usando o NetAvark com o DNS Aardvark em vez do CNI.

i. Verifique se o seu networkBackend está definido como CNI executando o seguinte comando:

```
podman info | grep networkBackend
```

ii. Se o networkBackend estiver definido como `CNI` , você precisará alterá-lo para `netavark` .

iii. Instalar `netavark` e `aardvark-dns` usando o seguinte comando:

```
dnf install aardvark-dns netavark
```

iv. Abra o `/etc/containers/containers.conf` arquivo e modifique a opção network_backend para usar "netavark" em vez de "cni".

Se `/etc/containers/containers.conf` não existe, faça as alterações de configuração para `/usr/share/containers/containers.conf` .

v. Reinicie o podman.

```
systemctl restart podman
```

vi. Confirme se networkBackend foi alterado para "netavark" usando o seguinte comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga a documentação do Docker para instalar o Docker Engine.

Passos

1. "Ver instruções de instalação do Docker"

   Siga as etapas para instalar uma versão compatível do Docker Engine. Não instale a versão mais recente, pois ela não é suportada pelo Console.

2. Verifique se o Docker está habilitado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Etapa 3: configurar a rede

Configure sua rede para que o agente do Console possa gerenciar recursos e processos dentro do seu ambiente de nuvem híbrida. Por exemplo, você precisa garantir que as conexões estejam disponíveis para as redes de destino e que o acesso de saída à Internet esteja disponível.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	Para gerenciar recursos no Google Cloud.
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.

Pontos finais	Propósito
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

  Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Etapa 4: configurar permissões para o agente do Console

Uma conta de serviço do Google Cloud é necessária para fornecer ao agente do Console as permissões necessárias para que o Console gerencie recursos no Google Cloud. Ao criar o agente do Console, você precisará associar essa conta de serviço à VM do agente do Console.

É sua responsabilidade atualizar a função personalizada à medida que novas permissões são adicionadas em versões subsequentes. Se novas permissões forem necessárias, elas serão listadas nas notas de versão.

Passos

1. Crie uma função personalizada no Google Cloud:

   a. Crie um arquivo YAML que inclua o conteúdo do"permissões de conta de serviço para o agente do Console" .

   b. No Google Cloud, ative o Cloud Shell.

   c. Faça upload do arquivo YAML que inclui as permissões necessárias.

   d. Crie uma função personalizada usando o `gcloud iam roles create` comando.

      O exemplo a seguir cria uma função chamada "agente" no nível do projeto:

      ```
      gcloud iam roles create connector --project=myproject --file=agent.yaml
      ```

   "Documentação do Google Cloud: Criação e gerenciamento de funções personalizadas"

2. Crie uma conta de serviço no Google Cloud e atribua a função à conta de serviço:

   a. No serviço IAM e Admin, selecione **Contas de serviço > Criar conta de serviço**.

   b. Insira os detalhes da conta de serviço e selecione **Criar e continuar**.

   c. Selecione a função que você acabou de criar.

   d. Conclua as etapas restantes para criar a função.

      "Documentação do Google Cloud: Criação de uma conta de serviço"

3. Se você planeja implantar sistemas Cloud Volumes ONTAP em projetos diferentes daquele em que o agente do Console reside, será necessário fornecer à conta de serviço do agente do Console acesso a esses projetos.

   Por exemplo, digamos que o agente do Console esteja no projeto 1 e você queira criar sistemas Cloud Volumes ONTAP no projeto 2. Você precisará conceder acesso à conta de serviço no projeto 2.

   a. No serviço IAM e Admin, selecione o projeto do Google Cloud onde você deseja criar sistemas Cloud Volumes ONTAP .
   b. Na página **IAM**, selecione **Conceder acesso** e forneça os detalhes necessários.
      - Insira o e-mail da conta de serviço do agente do Console.
      - Selecione a função personalizada do agente do Console.
      - Selecione **Salvar**.

   Para mais detalhes, consulte "Documentação do Google Cloud"

Etapa 5: configurar permissões de VPC compartilhadas

Se você estiver usando uma VPC compartilhada para implantar recursos em um projeto de serviço, precisará preparar suas permissões.

Esta tabela é para referência e seu ambiente deve refletir a tabela de permissões quando a configuração do IAM estiver concluída.

Exibir permissões de VPC compartilhadas

Identidade	Criador	Hospedado em	Permissões do projeto de serviço	Permissões do projeto host	Propósito
Conta do Google para implantar o agente	Personalizado	Projeto de Serviço	"Política de implantação do agente"	compute.networkUser	Implantando o agente no projeto de serviço
conta de serviço do agente	Personalizado	Projeto de serviço	"Política de conta de serviço do agente"	compute.networkUser gerenciador de implantação.editor	Implantando e mantendo o Cloud Volumes ONTAP e serviços no projeto de serviço
Conta de serviço Cloud Volumes ONTAP	Personalizado	Projeto de serviço	membro storage.admin: conta de serviço do NetApp Console como serviceAccount.user	N / D	(Opcional) Para NetApp Cloud Tiering e NetApp Backup and Recovery
Agente de serviço de APIs do Google	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Interage com as APIs do Google Cloud em nome da implantação. Permite que o Console use a rede compartilhada.
Conta de serviço padrão do Google Compute Engine	Google Cloud	Projeto de serviço	(Padrão) Editor	compute.networkUser	Implanta instâncias do Google Cloud e infraestrutura de computação em nome da implantação. Permite que o Console use a rede compartilhada.

Observações:

1. deploymentmanager.editor só é necessário no projeto host se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. O NetApp Console cria uma implantação no projeto host que contém a regra de firewall VPC0 se nenhuma regra for especificada.
2. firewall.create e firewall.delete só são necessários se você não estiver passando regras de firewall para a implantação e optar por deixar que o Console as crie para você. Essas permissões residem no arquivo .yaml da conta do Console. Se você estiver implantando um par de HA usando uma VPC compartilhada, essas permissões serão usadas para criar as regras de firewall para VPC1, 2 e 3. Para todas as outras implantações, essas permissões também serão usadas para criar regras para VPC0.
3. Para Cloud Tiering, a conta de serviço de hierarquização deve ter a função serviceAccount.user na conta de serviço, não apenas no nível do projeto. Atualmente, se você atribuir serviceAccount.user

no nível do projeto, as permissões não serão exibidas quando você consultar a conta de serviço com getIAMPolicy.

Etapa 6: habilitar as APIs do Google Cloud

Diversas APIs do Google Cloud precisam ser ativadas antes que você possa implantar um agente do Console no Google Cloud.

Etapa

1. Ative as seguintes APIs do Google Cloud no seu projeto:
   - API do Cloud Infrastructure Manager
   - API do Gerenciador de Implantação em Nuvem V2
   - API de registro em nuvem
   - API do Gerenciador de Recursos de Nuvem
   - API do mecanismo de computação
   - API de gerenciamento de identidade e acesso (IAM)
   - API do Serviço de Gerenciamento de Chaves em Nuvem (KMS)

     (Obrigatório somente se você estiver planejando usar o NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))

"Documentação do Google Cloud: Habilitando APIs"

Etapa 7: instalar o agente do console

Após a conclusão dos pré-requisitos, você pode instalar manualmente o software no seu próprio host Linux.

Ao implantar um agente, o sistema também cria um bucket do Google Cloud para armazenar os arquivos de implantação.

Antes de começar

Você deve ter o seguinte:

- Privilégios de root para instalar o agente do Console.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do agente do Console.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy de interceptação.

> Não é possível definir um certificado para um servidor proxy transparente ao instalar manualmente o agente do Console. Se precisar definir um certificado para um servidor proxy transparente, você deverá usar o Console de Manutenção após a instalação. Saiba mais sobre o"Console de manutenção do agente" .

Sobre esta tarefa

Após a instalação, o agente do Console se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Baixe o software do agente do Console e copie-o para o host Linux. Você pode baixá-lo tanto do NetApp Console quanto do site de suporte da NetApp .
   - NetApp Console: Acesse **Agentes > Gerenciamento > Implantar agente > Local > Instalação manual**.

     Escolha baixar os arquivos de instalação do agente ou um URL para os arquivos.

   - Site de suporte da NetApp (necessário caso você ainda não tenha acesso ao Console) "Site de suporte da NetApp" ,

3. Atribua permissões para executar o script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Onde <versão> é a versão do agente do Console que você baixou.

4. Se estiver instalando em um ambiente de nuvem governamental, desative as verificações de configuração."Aprenda como desabilitar verificações de configuração para instalações manuais."

5. Execute o script de instalação.

   ```
   ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
   server> --cacert <path and file name of a CA-signed certificate>
   ```

   Você precisará adicionar informações de proxy se sua rede exigir um proxy para acesso à internet. Você pode adicionar um proxy explícito durante a instalação. Os parâmetros `--proxy` e `--cacert` são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy explícito, precisará inserir os parâmetros conforme mostrado.

   Se você deseja configurar um proxy transparente, pode fazê-lo após a instalação. "Saiba mais sobre o console de manutenção do agente."

+

Aqui está um exemplo de configuração de um servidor proxy explícito com um certificado assinado por uma CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` configura o agente do Console para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

+ * http://endereço:porta * http://nome-do-usuário:senha@endereço:porta * http://nome-do-domínio%92nome-do-usuário:senha@endereço:porta * https://endereço:porta * https://nome-do-usuário:senha@endereço:porta * https://nome-do-domínio%92nome-do-usuário:senha@endereço:porta

+ Observe o seguinte:

+ **O usuário pode ser um usuário local ou um usuário de domínio.** Para um usuário de domínio, você deve usar o código ASCII para uma \ conforme mostrado acima. **O agente do Console não oferece suporte a nomes de usuário ou senhas que incluam o caractere @.** Se a senha incluir algum dos seguintes caracteres especiais, você deve escapar esse caractere especial adicionando uma barra invertida antes dele: & ou !

+ Por exemplo:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Se você usou o Podman, precisará ajustar a porta aardvark-dns.
   a. SSH para a máquina virtual do agente do Console.
   b. Abra o arquivo podman */usr/share/containers/containers.conf* e modifique a porta escolhida para o serviço DNS do Aardvark. Por exemplo, altere para 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

      Por exemplo:

      ```
      # Port to use for dns forwarding daemon with netavark in rootful bridge
      # mode and dns enabled.
      # Using an alternate port might be useful if other DNS services should
      # run on the machine.
      #
      dns_bind_port = 54
      ```

   a. Reinicie a máquina virtual do agente do Console.
2. Aguarde a conclusão da instalação.

   No final da instalação, o serviço do agente do Console (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

Se a instalação falhar, você pode visualizar o relatório e os logs da instalação para ajudar a corrigir os problemas."Aprenda a solucionar problemas de instalação."

1. Abra um navegador da Web em um host que tenha uma conexão com a máquina virtual do agente do Console e insira o seguinte URL:

   https://ipaddress

2. Após efetuar login, configure o agente do Console:

   a. Especifique a organização a ser associada ao agente do Console.

   b. Digite um nome para o sistema.

   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      Você deve manter o modo restrito desabilitado porque estas etapas descrevem como usar o Console no modo padrão. Você deve habilitar o modo restrito somente se tiver um ambiente seguro e quiser desconectar esta conta dos serviços de backend. Se for esse o caso,"siga as etapas para começar a usar o NetApp Console no modo restrito" .

   d. Selecione **Vamos começar**.

   Se a instalação falhar, você poderá visualizar logs e um relatório para ajudar a solucionar problemas."Aprenda a solucionar problemas de instalação."

Se você tiver buckets do Google Cloud Storage na mesma conta do Google Cloud onde criou o agente do Console, verá um sistema do Google Cloud Storage aparecer na página **Sistemas** automaticamente. "Aprenda a gerenciar o Google Cloud Storage no NetApp Console"

Etapa 8: fornecer permissões ao agente do console

Você precisa fornecer ao agente do Console as permissões do Google Cloud que você configurou anteriormente. Fornecer as permissões permite que o agente do Console gerencie seus dados e infraestrutura de armazenamento no Google Cloud.

Passos

1. Acesse o portal do Google Cloud e atribua a conta de serviço à instância de VM do agente do Console.

   "Documentação do Google Cloud: Alterando a conta de serviço e os escopos de acesso de uma instância"

2. Se você quiser gerenciar recursos em outros projetos do Google Cloud, conceda acesso adicionando a conta de serviço com a função de agente do Console a esse projeto. Você precisará repetir esta etapa para cada projeto.

Instalar um agente no local

Instalar manualmente um agente do Console no local

Instale um agente do Console no local, faça login e configure-o para funcionar com sua organização do Console.

Se você for um usuário do VMWare, poderá usar um OVA para instalar um agente de console no seu VCenter."Saiba mais sobre como instalar um agente em um VCenter."

Antes de instalar, você precisará garantir que seu host (VM ou host Linux) atenda aos requisitos e que o agente do Console terá acesso de saída à Internet, bem como às redes de destino. Se você planeja usar serviços de dados NetApp ou opções de armazenamento em nuvem, como o Cloud Volumes ONTAP, será necessário criar credenciais no seu provedor de nuvem para adicionar ao Console, para que o agente do Console possa executar ações na nuvem em seu nome.

Preparar para instalar o agente do Console

Antes de instalar um agente do Console, você deve garantir que tenha uma máquina host que atenda aos requisitos de instalação. Você também precisará trabalhar com seu administrador de rede para garantir que o agente do Console tenha acesso de saída aos endpoints necessários e conexões às redes de destino.

Revisar os requisitos do host do agente do console

Execute o agente do Console em um host x86 que atenda aos requisitos de sistema operacional, RAM e porta. Certifique-se de que seu host atenda a esses requisitos antes de instalar o agente do Console.

O agente do Console reserva o intervalo de UID e GID de 19000 a 19200. Este intervalo é fixo e não pode ser modificado. Se algum software de terceiros no seu host estiver usando UIDs ou GIDs dentro desse intervalo, a instalação do agente falhará. A NetApp recomenda usar um host livre de software de terceiros para evitar conflitos.

Host dedicado

O agente do Console requer um host dedicado. Qualquer arquitetura é suportada, desde que atenda a estes requisitos de tamanho:

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB é recomendado para o host, com os seguintes requisitos de partição:
  - `/opt`: 120 GiB de espaço devem estar disponíveis

    O agente usa `/opt` para instalar o `/opt/application/netapp` diretório e seu conteúdo.

  - `/var`: 40 GiB de espaço devem estar disponíveis

    O agente do console requer este espaço em `/var` Porque o Podman ou o Docker são projetados para criar contêineres dentro deste diretório. Especificamente, eles criarão contêineres no `/var/lib/containers/storage` diretório e `/var/lib/docker` para Docker. Montagens externas ou links simbólicos não funcionam neste espaço.

Hipervisor

É necessário um hipervisor bare metal ou hospedado certificado para executar um sistema operacional compatível.

Requisitos do sistema operacional e do contêiner

O agente do Console é compatível com os seguintes sistemas operacionais ao usar o Console no modo padrão ou no modo restrito. Uma ferramenta de orquestração de contêineres é necessária antes de instalar o agente.

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Red Hat Enterprise Linux		9,6 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	4.0.0 ou posterior com o Console no modo padrão ou no modo restrito.	Podman versão 5.4.0 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo		9.1 a 9.4 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.9.4 com podman-compose 1.5.0. Ver requisitos de configuração do Podman .

Sistema operacional	Versões de SO suportadas	Versões de agentes suportadas	Ferramenta de contêiner necessária	SELinux
Suportado no modo de imposição ou no modo permissivo		8,6 a 8,10 • Somente versões em inglês. • O host deve ser registrado no Red Hat Subscription Management. Se não estiver registrado, o host não poderá acessar os repositórios para atualizar o software de terceiros necessário durante a instalação do agente.	3.9.50 ou posterior com o Console no modo padrão ou modo restrito	Podman versão 4.6.1 ou 4.9.4 com podman-compose 1.0.6. Ver requisitos de configuração do Podman .
Suportado no modo de imposição ou no modo permissivo	Ubuntu		24,04 LTS	3.9.45 ou posterior com o NetApp Console no modo padrão ou restrito
Docker Engine 23.06 para 28.0.0.	Não suportado		22,04 LTS	3.9.50 ou posterior

Configurar acesso à rede para o agente do Console

Configure o acesso à rede para garantir que o agente do Console possa gerenciar recursos. Ele precisa de conexões para redes de destino e acesso de saída à Internet para endpoints específicos.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso

diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

> Um agente do Console instalado em suas instalações não pode gerenciar recursos no Google Cloud. Se você quiser gerenciar recursos do Google Cloud, precisará instalar um agente no Google Cloud.

AWS

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes endpoints da AWS para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados na AWS.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.

Pontos finais	Propósito
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Azul

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes pontos de extremidade do Azure para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados no Azure.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Criar permissões de nuvem do agente do Console para AWS ou Azure

Se você quiser usar os serviços de dados da NetApp na AWS ou no Azure com um agente do Console local, será necessário configurar permissões no seu provedor de nuvem e adicionar as credenciais ao agente do Console após instalá-lo.

Você deve instalar o agente do Console no Google Cloud para gerenciar quaisquer recursos que residam lá.

AWS

Quando o agente do Console é instalado no local, você precisa fornecer ao Console permissões da AWS adicionando chaves de acesso para um usuário do IAM que tenha as permissões necessárias.

Você deve usar este método de autenticação se o agente do Console estiver instalado no local. Você não pode usar uma função do IAM.

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:

   a. Selecione **Políticas > Criar política**.

   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .

   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços de dados da NetApp que você planeja usar, pode ser necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .

3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o usuário tenha uma chave de acesso que você possa adicionar ao NetApp Console após instalar o agente do Console.

Resultado

Agora você deve ter chaves de acesso para um usuário do IAM que tenha as permissões necessárias. Depois de instalar o agente do Console, associe essas credenciais ao agente do Console do Console.

Azul

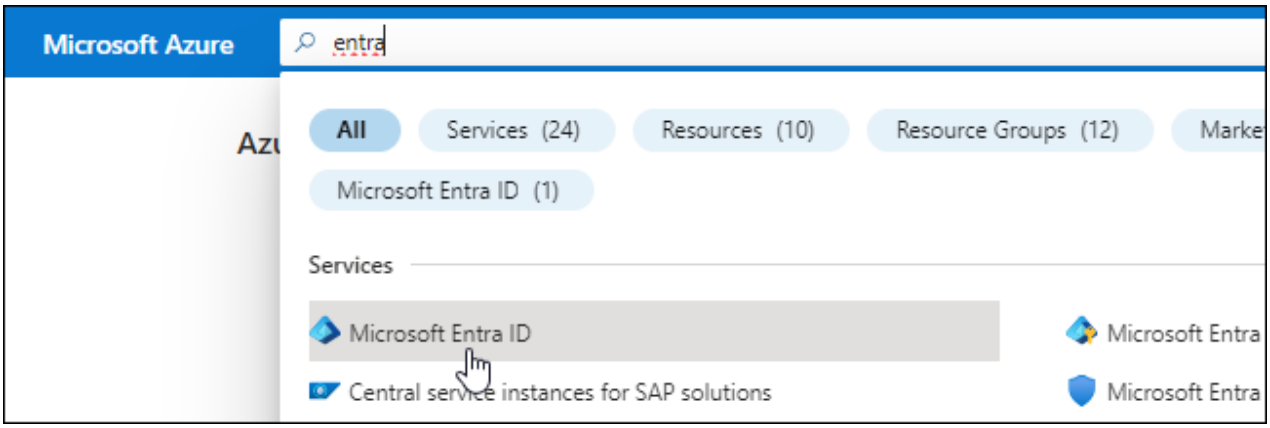
Quando o agente do Console é instalado no local, você precisa fornecer ao agente do Console permissões do Azure configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Digite um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
   - **URI de redirecionamento**: Você pode deixar este campo em branco.
6. Selecione **Registrar**.

   Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo a uma função

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

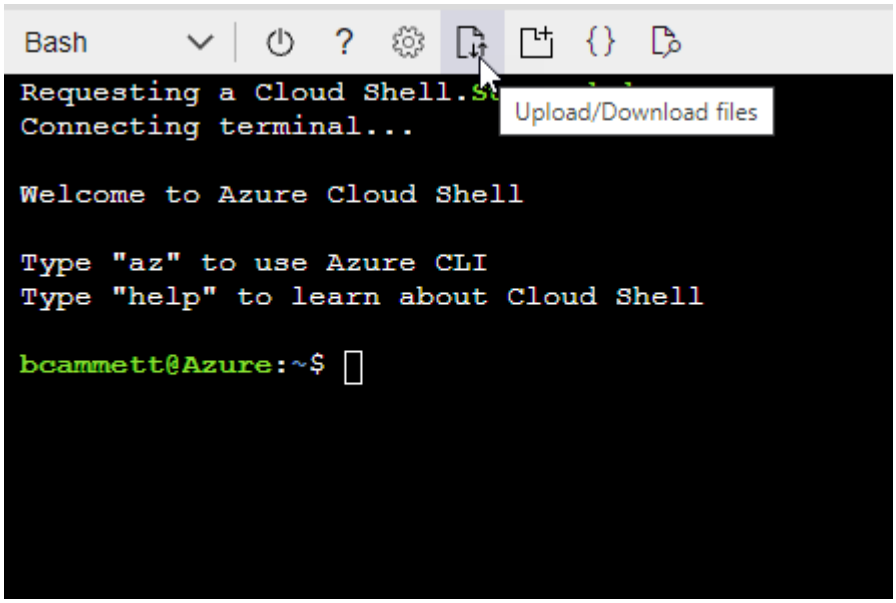
      Exemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Começar "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.



- Use a CLI do Azure para criar a função personalizada:

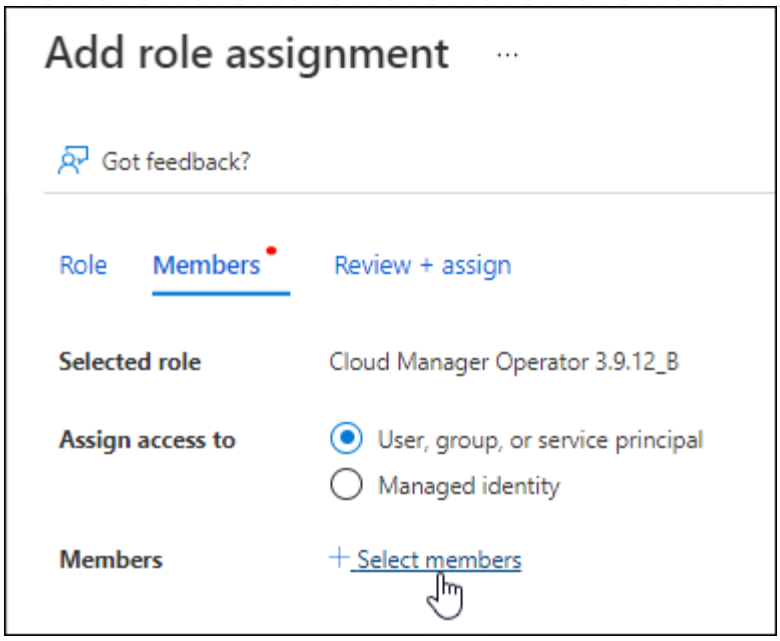
```
az role definition create --role-definition agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

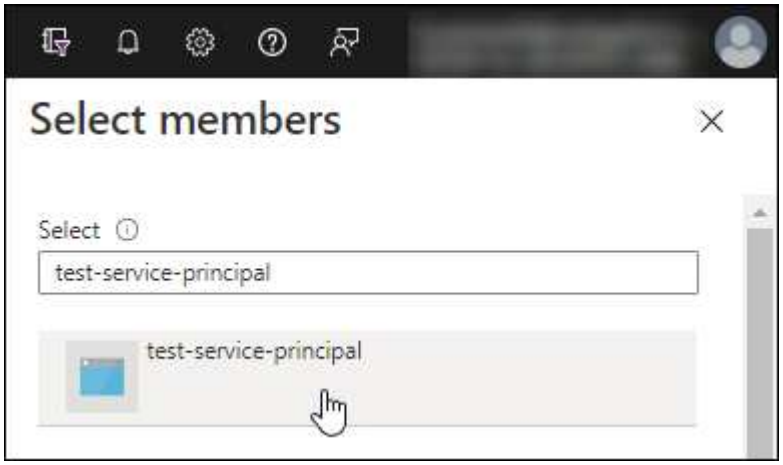
   a. No portal do Azure, abra o serviço **Assinaturas**.
   b. Selecione a assinatura.
   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.
   e. Na aba **Membros**, complete os seguintes passos:

      - Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
      - Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

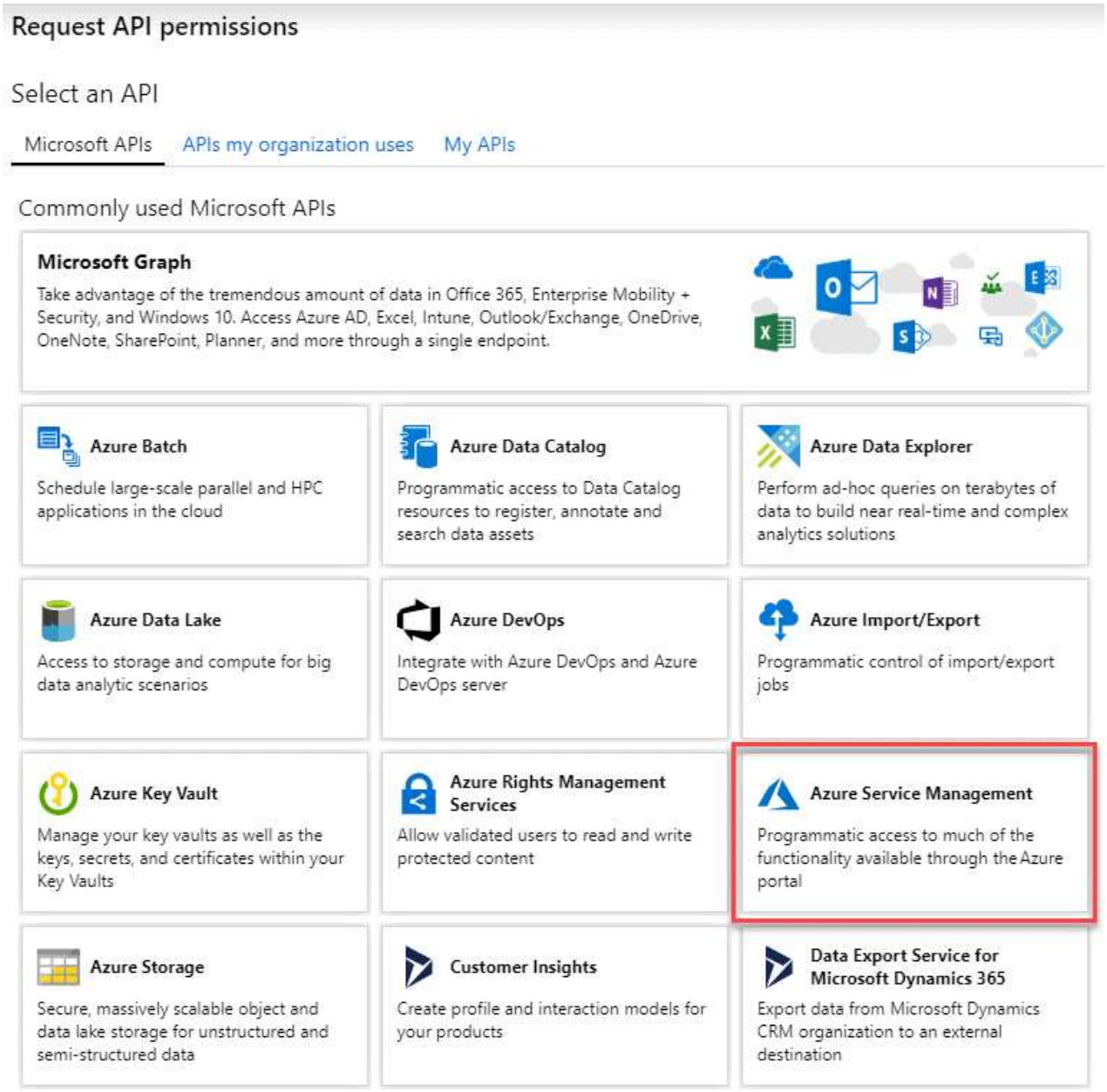
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

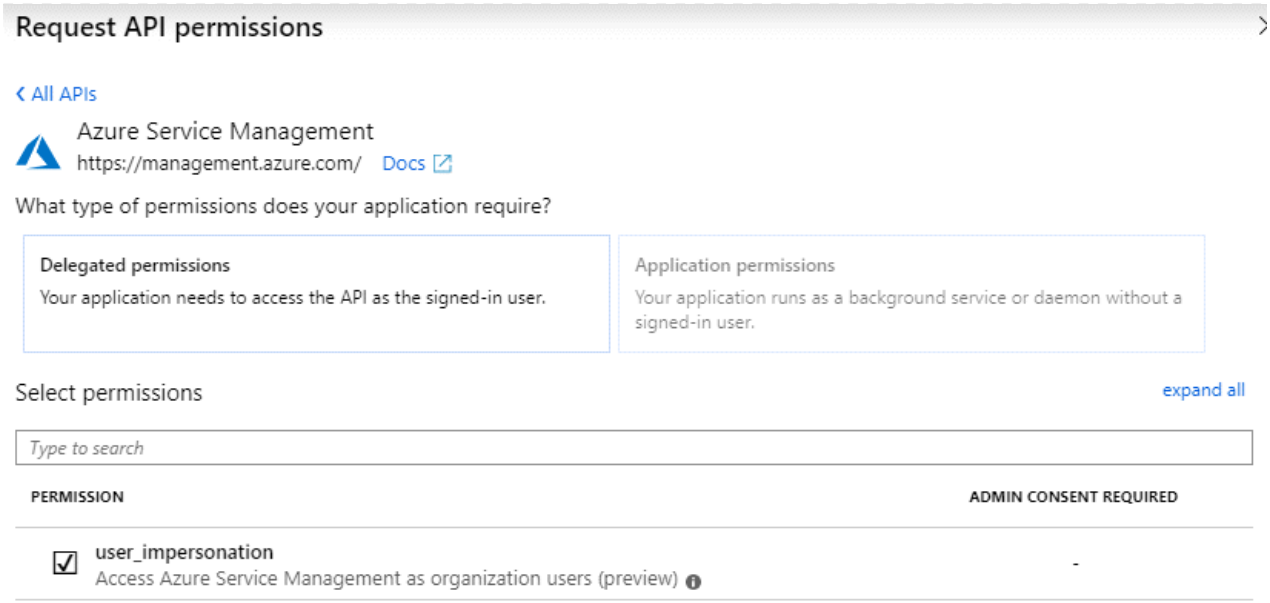
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.

3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

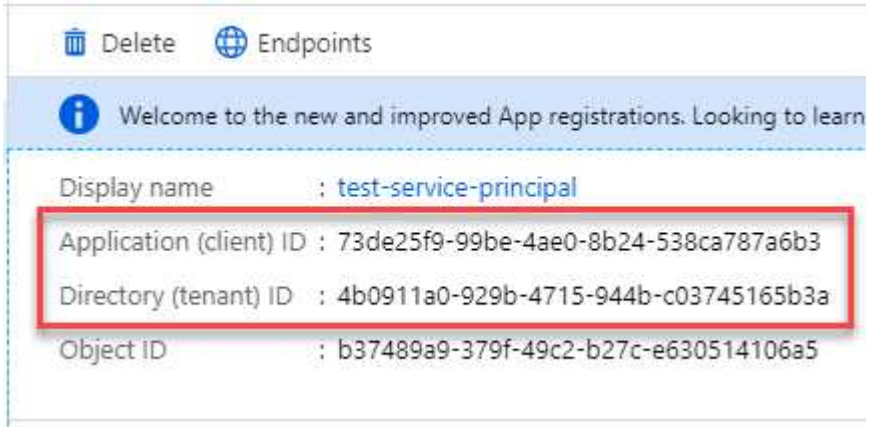


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



Obtenha o ID do aplicativo e o ID do diretório para o aplicativo

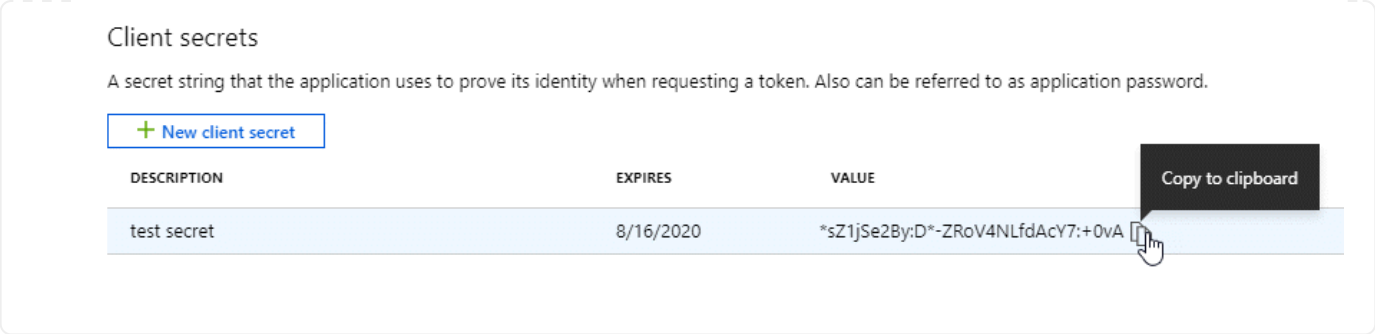
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.



Instalar manualmente um agente do Console

Ao instalar manualmente um agente do Console, você precisa preparar o ambiente da sua máquina para que ele atenda aos requisitos. Você precisará de uma máquina Linux e instalar o Podman ou o Docker, dependendo do seu sistema operacional Linux.

Instalar Podman ou Docker Engine

Dependendo do seu sistema operacional, o Podman ou o Docker Engine é necessário antes de instalar o agente.

- O Podman é necessário para o Red Hat Enterprise Linux 8 e 9.

  Veja as versões do Podman suportadas .

- O Docker Engine é necessário para o Ubuntu.

  Veja as versões suportadas do Docker Engine .

Exemplo 4. Passos

Podman

Siga estas etapas para instalar e configurar o Podman:

- Habilite e inicie o serviço podman.socket
- Instalar python3
- Instale o pacote podman-compose versão 1.0.6
- Adicione podman-compose à variável de ambiente PATH
- Se estiver usando o Red Hat Enterprise Linux, verifique se sua versão do Podman está usando o DNS Netavark Aardvark em vez do CNI

Ajuste a porta aardvark-dns (padrão: 53) após instalar o agente para evitar conflitos de porta DNS. Siga as instruções para configurar a porta.

Passos

1. Remova o pacote podman-docker se ele estiver instalado no host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale o Podman.

   Você pode obter o Podman nos repositórios oficiais do Red Hat Enterprise Linux.

   a. Para Red Hat Enterprise Linux 9,6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

   c. Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<version>
   ```

   Onde <versão> é a versão suportada do Podman que você está instalando. Veja as versões do Podman suportadas .

3. Habilite e inicie o serviço podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale o pacote do repositório EPEL se ele ainda não estiver disponível no seu sistema.

   Esta etapa é necessária porque o podman-compose está disponível no repositório Extra Packages for Enterprise Linux (EPEL).

6. Se estiver usando o Red Hat Enterprise 9:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Instale o pacote podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Se estiver usando o Red Hat Enterprise Linux 8:

   a. Instale o pacote do repositório EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Instale o pacote podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   Usando o `dnf install` O comando atende ao requisito de adicionar podman-compose à variável de ambiente PATH. O comando de instalação adiciona podman-compose a /usr/bin, que já está incluído no `secure_path` opção no host.

   c. Se estiver usando o Red Hat Enterprise Linux 8, verifique se sua versão do Podman está usando o NetAvark com o DNS Aardvark em vez do CNI.

i. Verifique se o seu networkBackend está definido como CNI executando o seguinte comando:

```
podman info | grep networkBackend
```

ii. Se o networkBackend estiver definido como `CNI` , você precisará alterá-lo para `netavark` .

iii. Instalar `netavark` e `aardvark-dns` usando o seguinte comando:

```
dnf install aardvark-dns netavark
```

iv. Abra o `/etc/containers/containers.conf` arquivo e modifique a opção network_backend para usar "netavark" em vez de "cni".

Se `/etc/containers/containers.conf` não existe, faça as alterações de configuração para `/usr/share/containers/containers.conf` .

v. Reinicie o podman.

```
systemctl restart podman
```

vi. Confirme se networkBackend foi alterado para "netavark" usando o seguinte comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga a documentação do Docker para instalar o Docker Engine.

Passos

1. "Ver instruções de instalação do Docker"

   Siga as etapas para instalar uma versão compatível do Docker Engine. Não instale a versão mais recente, pois ela não é suportada pelo Console.

2. Verifique se o Docker está habilitado e em execução.

```
sudo systemctl enable docker && sudo systemctl start docker
```

Instalar o agente do Console manualmente

Baixe e instale o software do agente do Console em um host Linux existente no local.

Antes de começar

Você deve ter o seguinte:

- Privilégios de root para instalar o agente do Console.
- Detalhes sobre um servidor proxy, caso um proxy seja necessário para acesso à Internet a partir do agente do Console.

  Você tem a opção de configurar um servidor proxy após a instalação, mas isso requer a reinicialização do agente do Console.

- Um certificado assinado pela CA, se o servidor proxy usar HTTPS ou se o proxy for um proxy de interceptação.

> Não é possível definir um certificado para um servidor proxy transparente ao instalar manualmente o agente do Console. Se precisar definir um certificado para um servidor proxy transparente, você deverá usar o Console de Manutenção após a instalação. Saiba mais sobre o"Console de manutenção do agente" .

Sobre esta tarefa

Após a instalação, o agente do Console se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Se as variáveis de sistema *http_proxy* ou *https_proxy* estiverem definidas no host, remova-as:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Se você não remover essas variáveis do sistema, a instalação falhará.

2. Baixe o software do agente do Console e copie-o para o host Linux. Você pode baixá-lo tanto do NetApp Console quanto do site de suporte da NetApp .
   - NetApp Console: Acesse **Agentes > Gerenciamento > Implantar agente > Local > Instalação manual**.

     Escolha baixar os arquivos de instalação do agente ou um URL para os arquivos.

   - Site de suporte da NetApp (necessário caso você ainda não tenha acesso ao Console) "Site de suporte da NetApp" ,
3. Atribua permissões para executar o script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Onde <versão> é a versão do agente do Console que você baixou.

4. Se estiver instalando em um ambiente de nuvem governamental, desative as verificações de configuração."Aprenda como desabilitar verificações de configuração para instalações manuais."
5. Execute o script de instalação.

```
./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Você precisará adicionar informações de proxy se sua rede exigir um proxy para acesso à internet. Você pode adicionar um proxy explícito durante a instalação. Os parâmetros `--proxy` e `--cacert` são opcionais e você não será solicitado a adicioná-los. Se você tiver um servidor proxy explícito, precisará inserir os parâmetros conforme mostrado.

Se você deseja configurar um proxy transparente, pode fazê-lo após a instalação. "Saiba mais sobre o console de manutenção do agente."

+

Aqui está um exemplo de configuração de um servidor proxy explícito com um certificado assinado por uma CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` configura o agente do Console para usar um servidor proxy HTTP ou HTTPS usando um dos seguintes formatos:

+ * http://endereço:porta * http://nome-do-usuário:senha@endereço:porta * http://nome-do-domínio%92nome-do-usuário:senha@endereço:porta * https://endereço:porta * https://nome-do-usuário:senha@endereço:porta * https://nome-do-domínio%92nome-do-usuário:senha@endereço:porta

+ Observe o seguinte:

+ **O usuário pode ser um usuário local ou um usuário de domínio.** Para um usuário de domínio, você deve usar o código ASCII para uma \ conforme mostrado acima. **O agente do Console não oferece suporte a nomes de usuário ou senhas que incluam o caractere @.** Se a senha incluir algum dos seguintes caracteres especiais, você deve escapar esse caractere especial adicionando uma barra invertida antes dele: & ou !

+ Por exemplo:

+ http://bxpproxyuser:netapp1\!@address:3128

1. Se você usou o Podman, precisará ajustar a porta aardvark-dns.

   a. SSH para a máquina virtual do agente do Console.

   b. Abra o arquivo podman */usr/share/containers/containers.conf* e modifique a porta escolhida para o serviço DNS do Aardvark. Por exemplo, altere para 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

Por exemplo:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. Reinicie a máquina virtual do agente do Console.

O que vem a seguir?

Você precisará registrar o agente do Console no NetApp Console.

Registre o agente do Console com o NetApp Console

Efetue login no Console e associe o agente do Console à sua organização. A forma como você efetua login depende do modo em que você está usando o Console. Se você estiver usando o Console no modo padrão, faça login pelo site do SaaS. Se estiver usando o Console no modo restrito, faça login localmente no host do agente do Console.

Passos

1. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

2. Cadastre-se ou faça login.
3. Após efetuar login, configure o Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      O modo restrito não é suportado quando o agente do Console é instalado no local.

   d. Selecione **Vamos começar**.

Forneça credenciais do provedor de nuvem ao NetApp Console

Depois de instalar e configurar o agente do Console, adicione suas credenciais de nuvem para que o agente do Console tenha as permissões necessárias para executar ações na AWS ou no Azure.

AWS

Antes de começar

Se você acabou de criar essas credenciais da AWS, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione **Adicionar credenciais** e siga as etapas do assistente.
    a. **Localização das credenciais**: Selecione *Amazon Web Services > Agente.
    b. **Definir credenciais**: insira uma chave de acesso e uma chave secreta da AWS.
    c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
    d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Agora você pode ir para o "NetApp Console" para começar a usar o agente do Console.

Azul

Antes de começar

Se você acabou de criar essas credenciais do Azure, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais do agente do Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
    a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
    b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
        - ID do aplicativo (cliente)
        - ID do diretório (inquilino)
        - Segredo do cliente
    c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
    d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

O agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome. Agora você pode ir para o "NetApp Console" para começar a usar o agente do Console.

Instalar um agente de console no local usando o VCenter

Se você for um usuário do VMWare, poderá usar um OVA para instalar um agente de console no seu VCenter. O download ou URL do OVA está disponível no NetApp Console.

Ao instalar um agente do Console com suas ferramentas do VCenter, você pode usar o console da Web da VM para executar tarefas de manutenção."Saiba mais sobre o console da VM para o agente."

Preparar para instalar o agente do Console

Antes da instalação, certifique-se de que o host da VM atenda aos requisitos e que o agente do Console possa acessar a Internet e as redes de destino. Para usar os serviços de dados do NetApp ou o Cloud Volumes ONTAP, crie credenciais do provedor de nuvem para que o agente do Console execute ações em seu nome.

Revisar os requisitos do host do agente do console

Certifique-se de que sua máquina host atenda aos requisitos de instalação antes de instalar o agente do Console.

- CPU: 8 núcleos ou 8 vCPUs
- RAM: 32 GB
- Espaço em disco: 165 GB (provisionamento denso)
- vSphere 7.0 ou superior
- Host ESXi 7.03 ou superior

Instale o agente em um ambiente vCenter em vez de diretamente em um host ESXi.

Configurar acesso à rede para o agente do Console

Trabalhe com seu administrador de rede para garantir que o agente do Console tenha acesso de saída aos endpoints necessários e conexões com redes de destino.

Conexões com redes de destino

O agente do Console requer uma conexão de rede com o local onde você planeja criar e gerenciar sistemas. Por exemplo, a rede onde você planeja criar sistemas Cloud Volumes ONTAP ou um sistema de armazenamento em seu ambiente local.

Acesso de saída à Internet

O local de rede onde você implanta o agente do Console deve ter uma conexão de saída com a Internet para entrar em contato com endpoints específicos.

Endpoints contatados de computadores ao usar o NetApp Console baseado na Web

Os computadores que acessam o Console a partir de um navegador da web devem ter a capacidade de contatar vários terminais. Você precisará usar o Console para configurar o agente do Console e para o uso diário do Console.

"Preparar a rede para o console NetApp" .

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Não é possível gerenciar recursos no Google Cloud com um agente do Console instalado em suas instalações. Para gerenciar recursos do Google Cloud, instale um agente no Google Cloud.

AWS

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes endpoints da AWS para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados na AWS.

Endpoints contatados pelo agente do Console

O agente do Console requer acesso de saída à Internet para entrar em contato com os seguintes endpoints para gerenciar recursos e processos dentro do seu ambiente de nuvem pública para operações diárias.

Os endpoints listados abaixo são todos entradas CNAME.

Pontos finais	Propósito
Serviços da AWS (amazonaws.com): • CloudFormation • Nuvem de Computação Elástica (EC2) • Gerenciamento de Identidade e Acesso (IAM) • Serviço de Gerenciamento de Chaves (KMS) • Serviço de Token de Segurança (STS) • Serviço de Armazenamento Simples (S3)	Para gerenciar recursos da AWS. O ponto de extremidade depende da sua região da AWS. "Consulte a documentação da AWS para obter detalhes"
Amazon FSX para NetApp ONTAP: • api.workloads.netapp.com	O console baseado na web contata este endpoint para interagir com as APIs do Workload Factory, a fim de gerenciar e operar cargas de trabalho baseadas no FSx para ONTAP .
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.

Pontos finais	Propósito
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Azul

Quando o agente do Console é instalado no local, ele precisa de acesso à rede para os seguintes pontos de extremidade do Azure para gerenciar sistemas NetApp (como o Cloud Volumes ONTAP) implantados no Azure.

Pontos finais	Propósito
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para gerenciar recursos em regiões públicas do Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para gerenciar recursos nas regiões do Azure China.

Pontos finais	Propósito
\ https://mysupport.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp .
\ https://signin.b2c.netapp.com	Para atualizar as credenciais do NetApp Support Site (NSS) ou adicionar novas credenciais do NSS ao NetApp Console.
\ https://support.netapp.com	Para obter informações de licenciamento e enviar mensagens do AutoSupport para o suporte da NetApp , bem como receber atualizações de software para o Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Para fornecer recursos e serviços no NetApp Console.

Pontos finais	Propósito
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obter imagens para atualizações do agente do Console. • Quando você implanta um novo agente, a verificação de validação testa a conectividade com os endpoints atuais. Se você usar"pontos finais anteriores" , a verificação de validação falha. Para evitar essa falha, pule a verificação de validação. Embora os endpoints anteriores ainda sejam suportados, a NetApp recomenda atualizar suas regras de firewall para os endpoints atuais o mais rápido possível. "Aprenda como atualizar sua lista de endpoints" . • Quando você atualiza os endpoints atuais no seu firewall, seus agentes existentes continuarão funcionando.

Servidor proxy

O NetApp oferece suporte a configurações de proxy explícitas e transparentes. Se você estiver usando um proxy transparente, você só precisa fornecer o certificado para o servidor proxy. Se estiver usando um proxy explícito, você também precisará do endereço IP e das credenciais.

- Endereço IP
- Credenciais
- Certificado HTTPS

Portos

Não há tráfego de entrada para o agente do Console, a menos que você o inicie ou se ele for usado como um proxy para enviar mensagens do AutoSupport do Cloud Volumes ONTAP para o Suporte da NetApp .

- HTTP (80) e HTTPS (443) fornecem acesso à interface de usuário local, que você usará em raras circunstâncias.
- SSH (22) só é necessário se você precisar se conectar ao host para solução de problemas.
- Conexões de entrada pela porta 3128 serão necessárias se você implantar sistemas Cloud Volumes ONTAP em uma sub-rede onde uma conexão de saída com a Internet não esteja disponível.

Se os sistemas Cloud Volumes ONTAP não tiverem uma conexão de saída com a Internet para enviar mensagens do AutoSupport , o Console configurará automaticamente esses sistemas para usar um servidor proxy incluído no agente do Console. O único requisito é garantir que o grupo de segurança do agente do Console permita conexões de entrada pela porta 3128. Você precisará abrir esta porta depois de implantar o agente do Console.

Habilitar NTP

Se você planeja usar o NetApp Data Classification para verificar suas fontes de dados corporativos, habilite um serviço Network Time Protocol (NTP) no agente do Console e no sistema NetApp Data Classification para que o horário seja sincronizado entre os sistemas. "Saiba mais sobre a classificação de dados da NetApp"

Criar permissões de nuvem do agente do Console para AWS ou Azure

Se você quiser usar os serviços de dados do NetApp na AWS ou no Azure com um agente do Console local, precisará configurar permissões no seu provedor de nuvem para poder adicionar as credenciais ao agente do Console após instalá-lo.

Não é possível gerenciar recursos no Google Cloud com um agente do Console instalado em suas instalações. Se você quiser gerenciar recursos do Google Cloud, precisará instalar um agente no Google Cloud.

AWS

Para agentes do Console locais, forneça permissões da AWS adicionando chaves de acesso de usuário do IAM.

Use chaves de acesso de usuário do IAM para agentes do Console locais; funções do IAM não são suportadas para agentes do Console locais.

Passos

1. Faça login no console da AWS e navegue até o serviço IAM.
2. Crie uma política:

   a. Selecione **Políticas > Criar política**.

   b. Selecione **JSON** e copie e cole o conteúdo do"Política do IAM para o agente do Console" .

   c. Conclua as etapas restantes para criar a política.

      Dependendo dos serviços de dados da NetApp que você planeja usar, pode ser necessário criar uma segunda política.

   Para regiões padrão, as permissões são distribuídas em duas políticas. Duas políticas são necessárias devido ao limite máximo de tamanho de caracteres para políticas gerenciadas na AWS. "Saiba mais sobre as políticas do IAM para o agente do Console" .

3. Anexe as políticas a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"
4. Certifique-se de que o usuário tenha uma chave de acesso que você possa adicionar ao NetApp Console após instalar o agente do Console.

Resultado

Agora você deve ter chaves de acesso de usuário do IAM com as permissões necessárias. Depois de instalar o agente do Console, associe essas credenciais ao agente do Console no Console.

Azul

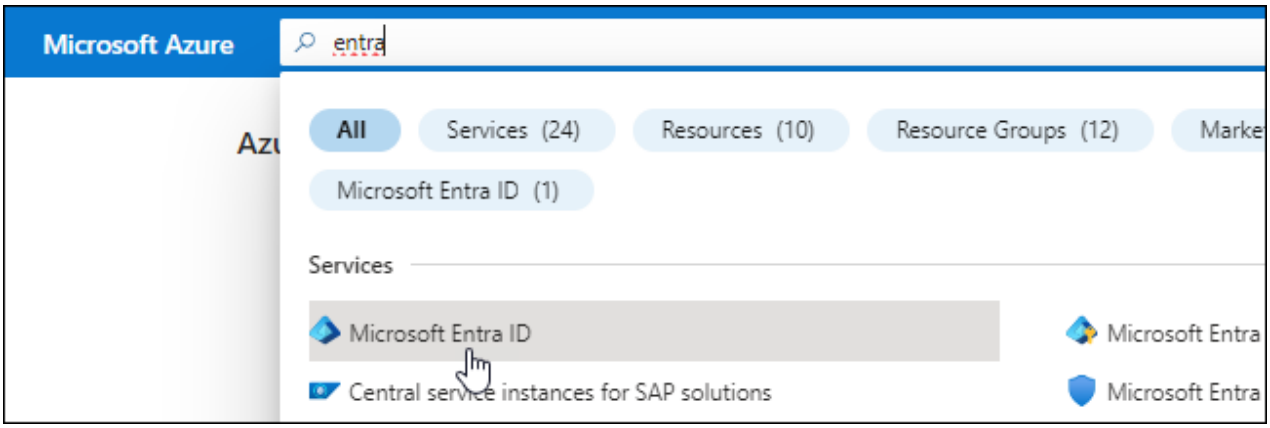
Quando o agente do Console estiver instalado no local, você precisará conceder permissões do Azure ao agente do Console configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

Crie um aplicativo Microsoft Entra para controle de acesso baseado em função

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Digite um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
   - **URI de redirecionamento**: Você pode deixar este campo em branco.
6. Selecione **Registrar**.

   Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo a uma função

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

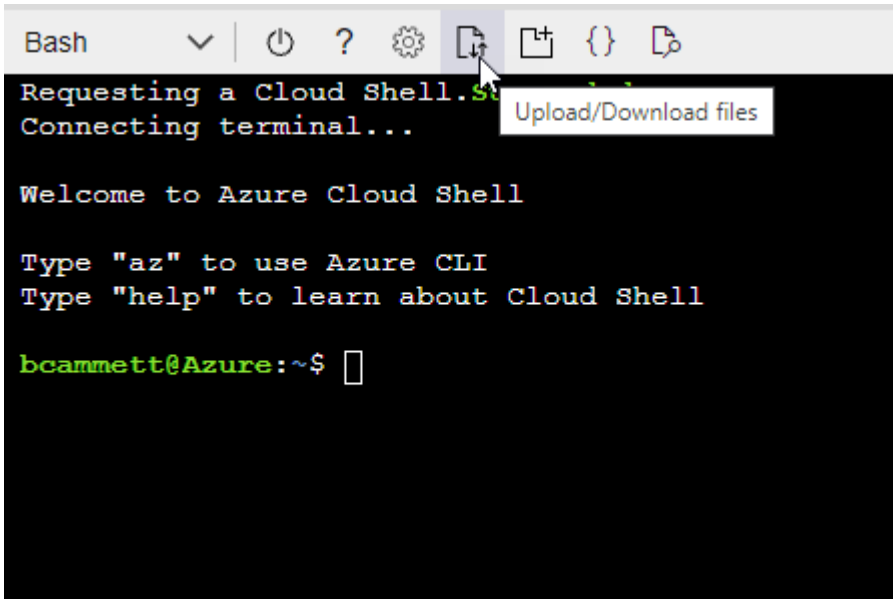
      Exemplo

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ]
      ```

   c. Use o arquivo JSON para criar uma função personalizada no Azure.

      As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Começar "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.



- Use a CLI do Azure para criar a função personalizada:

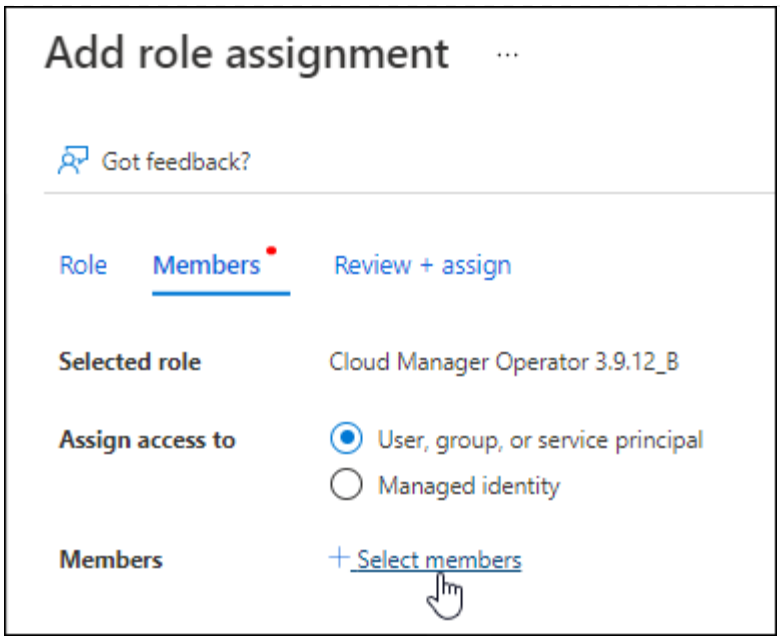
```
az role definition create --role-definition agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

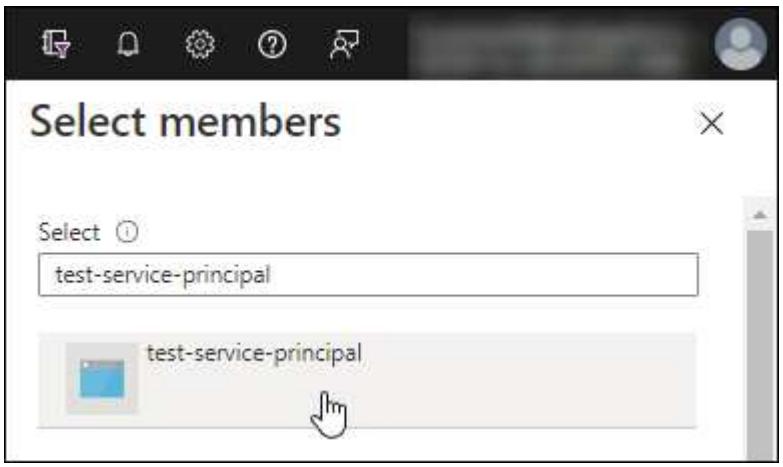
   a. No portal do Azure, abra o serviço **Assinaturas**.
   b. Selecione a assinatura.
   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.
   e. Na aba **Membros**, complete os seguintes passos:

      - Mantenha **Usuário, grupo ou entidade de serviço** selecionado.
      - Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

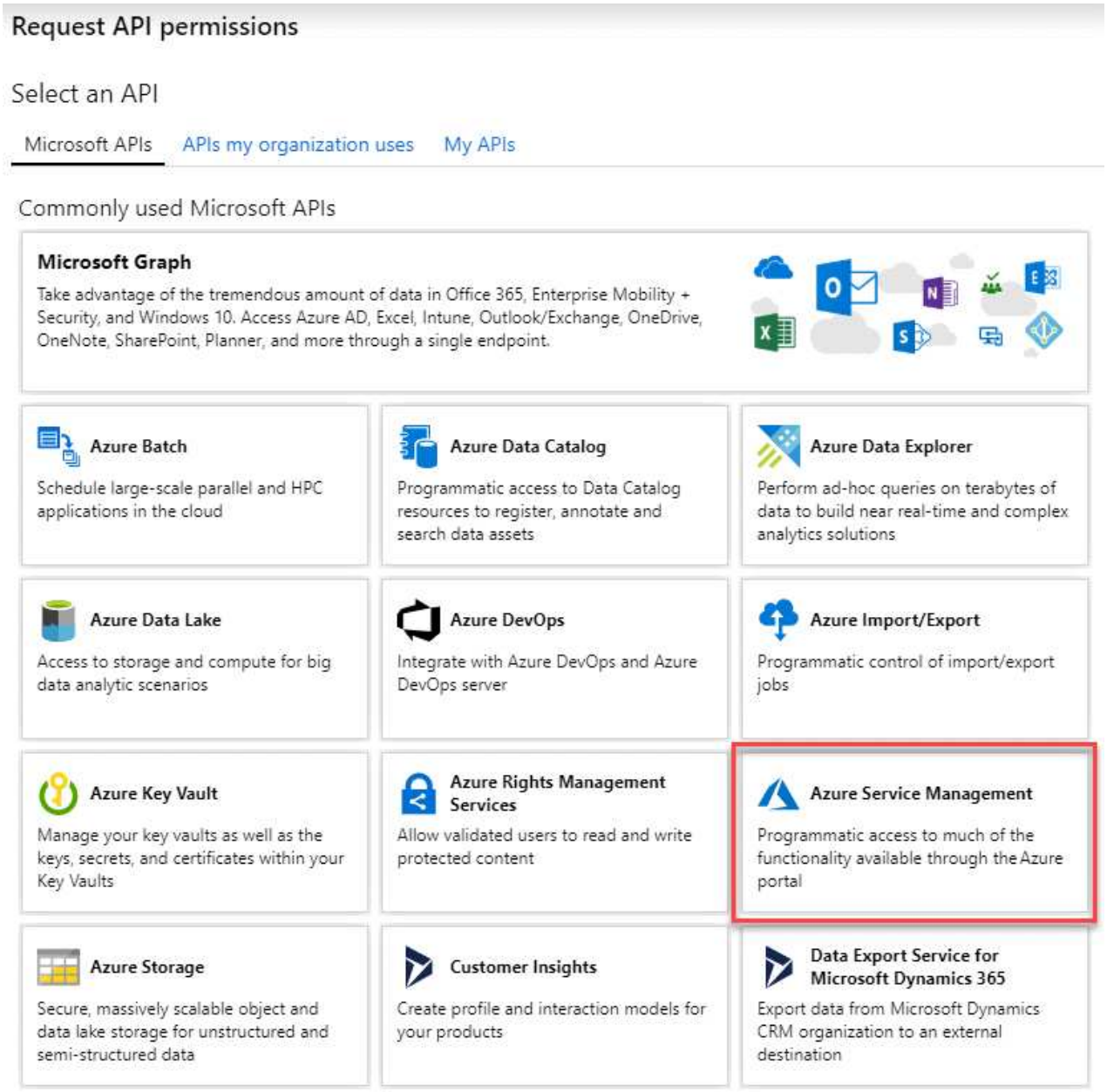
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

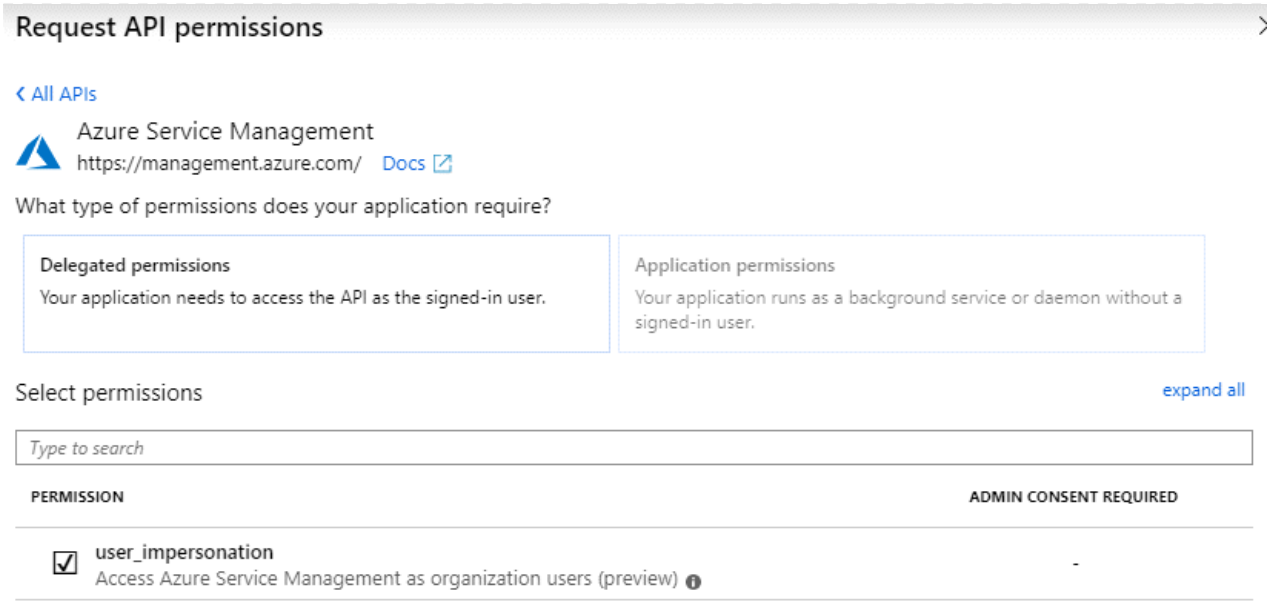
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.

3. Em **APIs da Microsoft**, selecione **Azure Service Management**.

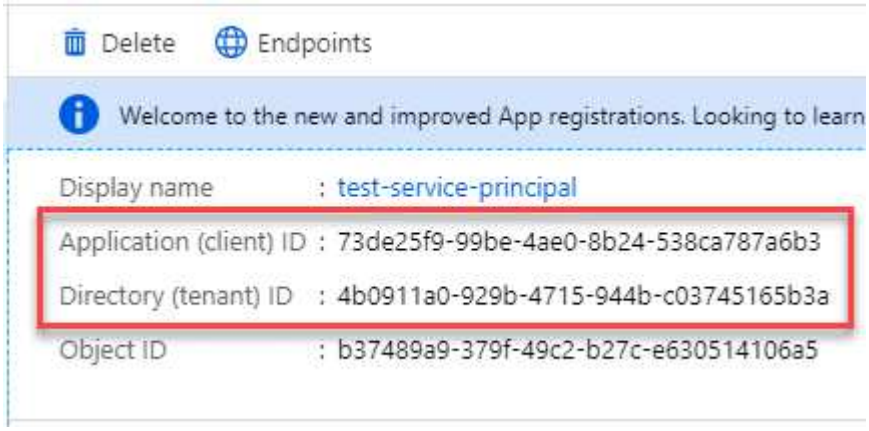


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



Obtenha o ID do aplicativo e o ID do diretório para o aplicativo

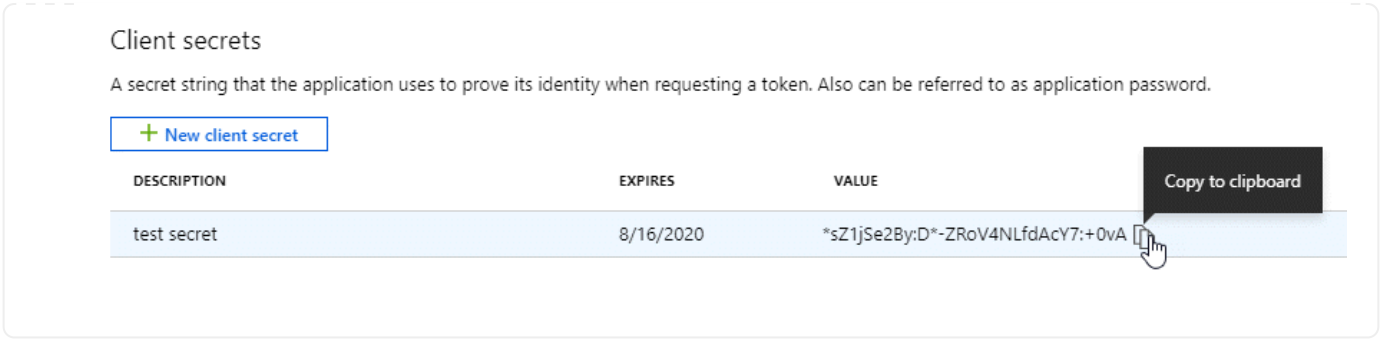
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

1. Abra o serviço **Microsoft Entra ID**.
2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.



Instale um agente de console no seu ambiente VCenter

A NetApp oferece suporte à instalação do agente do Console no seu ambiente VCenter. O arquivo OVA inclui uma imagem de VM pré-configurada que você pode implantar no seu ambiente VMware. Um download de arquivo ou implantação de URL está disponível diretamente no NetApp Console. Inclui o software do agente do Console e um certificado autoassinado.

Baixe o OVA ou copie o URL

Baixe o OVA ou copie o URL do OVA diretamente do NetApp Console.

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione **Implantar agente > No local**.
3. Selecione **Com OVA**.
4. Escolha entre baixar o OVA ou copiar o URL para usar no VCenter.

Implante o agente no seu VCenter

Efetue login no seu ambiente VCenter para implantar o agente.

Passos

1. Carregue o certificado autoassinado nos seus certificados confiáveis se o seu ambiente exigir. Você substitui este certificado após a instalação."Aprenda como substituir o certificado autoassinado."
2. Implante o OVA da biblioteca de conteúdo ou do sistema local.

Do sistema local	Da biblioteca de conteúdo
a. Clique com o botão direito e selecione **Implantar modelo OVF…**. b. Escolha o arquivo OVA na URL ou navegue até seu local e selecione **Avançar**.	a. Acesse sua biblioteca de conteúdo e selecione o agente OVA do Console. b. Selecione **Ações** > **Nova VM deste modelo**

3. Conclua o assistente Implantar modelo OVF para implantar o agente do Console.
4. Selecione um nome e uma pasta para a VM e selecione **Avançar**.
5. Selecione um recurso de computação e, em seguida, selecione **Avançar**.
6. Revise os detalhes do modelo e selecione **Avançar**.
7. Aceite o contrato de licença e selecione **Avançar**.
8. Escolha o tipo de configuração de proxy que você deseja usar: proxy explícito, proxy transparente ou nenhum proxy.
9. Selecione o armazenamento de dados onde você deseja implantar a VM e selecione **Avançar**. Certifique-

se de que ele atenda aos requisitos do host.

10. Selecione a rede à qual você deseja conectar a VM e selecione **Avançar**. Certifique-se de que a rede seja IPv4 e tenha acesso de saída à Internet para os terminais necessários.
11. na janela **Personalizar modelo**, preencha os seguintes campos:
    - **Informações de proxy**
      - Se você selecionou proxy explícito, insira o nome do host ou endereço IP do servidor proxy e o número da porta, bem como o nome de usuário e a senha.
      - Se você selecionou proxy transparente, carregue o respectivo certificado.
    - **Configuração da Máquina Virtual**
      - **Ignorar verificação de configuração**: esta caixa de seleção fica desmarcada por padrão, o que significa que o agente executa uma verificação de configuração para validar o acesso à rede.
        - A NetApp recomenda deixar esta caixa desmarcada para que a instalação inclua uma verificação de configuração do agente. A verificação de configuração valida se o agente tem acesso de rede aos terminais necessários. Se a implantação falhar devido a problemas de conectividade, você poderá acessar o relatório de validação e os logs do host do agente. Em alguns casos, se você tiver certeza de que o agente tem acesso à rede, você pode optar por pular a verificação. Por exemplo, se você ainda estiver usando o"pontos finais anteriores" usado para atualizações de agentes, a validação falha com um erro. Para evitar isso, marque a caixa de seleção para instalar sem uma verificação de validação. "Aprenda como atualizar sua lista de endpoints" .
      - **Senha de manutenção**: Defina a senha para o `maint` usuário que permite acesso ao console de manutenção do agente.
      - **Servidores NTP**: especifique um ou mais servidores NTP para sincronização de horário.
      - **Nome do host**: define o nome do host para esta VM. Não deve incluir o domínio de pesquisa. Por exemplo, um FQDN de console10.searchdomain.company.com deve ser inserido como console10.
      - **DNS primário**: especifique o servidor DNS primário a ser usado para resolução de nomes.
      - **DNS secundário**: especifique o servidor DNS secundário a ser usado para resolução de nomes.
      - Domínios de pesquisa: especifique o nome do domínio de pesquisa a ser usado ao resolver o nome do host. Por exemplo, se o FQDN for console10.searchdomain.company.com, insira searchdomain.company.com.
      - **Endereço IPv4**: O endereço IP mapeado para o nome do host.
      - **Máscara de sub-rede IPv4**: A máscara de sub-rede para o endereço IPv4.
      - **Endereço de gateway IPv4**: O endereço de gateway para o endereço IPv4.
12. Selecione **Avançar**.
13. Revise os detalhes na janela **Pronto para concluir** e selecione **Concluir**.

    A barra de tarefas do vSphere mostra o progresso conforme o agente do Console é implantado.

14. Ligue a VM.

> Se a implantação falhar, você poderá acessar o relatório de validação e os logs do host do agente."Aprenda a solucionar problemas de instalação."

Registre o agente do Console com o NetApp Console

Efetue login no Console e associe o agente do Console à sua organização. A forma como você efetua login depende do modo em que você está usando o Console. Se você estiver usando o Console no modo padrão, faça login pelo site do SaaS. Se você estiver usando o Console no modo restrito ou privado, faça login localmente no host do agente do Console.

Passos

1. Abra um navegador da Web e insira o URL do host do agente do Console:

   O URL do host do console pode ser um host local, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o agente do Console estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do agente do Console.

2. Cadastre-se ou faça login.
3. Após efetuar login, configure o Console:
   a. Especifique a organização do Console a ser associada ao agente do Console.
   b. Digite um nome para o sistema.
   c. Em **Você está executando em um ambiente seguro?** mantenha o modo restrito desabilitado.

      O modo restrito não é suportado quando o agente do Console é instalado no local.

   d. Selecione **Vamos começar**.

Adicionar credenciais do provedor de nuvem ao Console

Depois de instalar e configurar o agente do Console, adicione suas credenciais de nuvem para que o agente do Console tenha as permissões necessárias para executar ações na AWS ou no Azure.

AWS

Antes de começar

Se você acabou de criar essas credenciais da AWS, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione **Adicionar credenciais** e siga as etapas do assistente.
    a. **Localização das credenciais**: Selecione *Amazon Web Services > Agente.
    b. **Definir credenciais**: insira uma chave de acesso e uma chave secreta da AWS.
    c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
    d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Agora você pode ir para o "NetApp Console" para começar a usar o agente do Console.

Azul

Antes de começar

Se você acabou de criar essas credenciais do Azure, elas podem levar alguns minutos para ficarem disponíveis. Aguarde alguns minutos antes de adicionar as credenciais do agente do Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
    a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
    b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
        - ID do aplicativo (cliente)
        - ID do diretório (inquilino)
        - Segredo do cliente
    c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
    d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

O agente do Console agora tem as permissões necessárias para executar ações no Azure em seu nome. Agora você pode ir para o "NetApp Console" para começar a usar o agente do Console.

Portas para o agente do Console local

O agente do Console usa portas *de entrada* quando instalado manualmente em um host Linux local. Consulte essas portas para fins de planejamento.

Essas regras de entrada se aplicam a todos os modos de implantação do NetApp Console .

Protocolo	Porta	Propósito
HTTP	80	• Fornece acesso HTTP dos navegadores da web do cliente para a interface do usuário local • Usado durante o processo de atualização do Cloud Volumes ONTAP
HTTPS	443	Fornece acesso HTTPS dos navegadores da web do cliente para a interface do usuário local

Manter agentes do console

Manter um host VCenter ou ESXi para o agente do Console

Você pode fazer alterações no seu host VCenter ou ESXi existente depois de implantar o agente do Console. Por exemplo, você pode aumentar a CPU ou a RAM da instância da VM que hospeda o agente do Console.

Execute estas tarefas de manutenção usando o console da Web da VM:

- Aumentar o tamanho do disco
- Reinicie o agente
- Atualizar rotas estáticas
- Atualizar domínios de pesquisa

Limitações

A atualização do agente pelo console ainda não é suportada. Além disso, você só pode visualizar informações sobre o endereço IP, DNS e gateways.

Acesse o console de manutenção da VM

Você pode acessar o Console de manutenção a partir do cliente VSphere.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.

Alterar a senha do usuário de manutenção

Você pode alterar a senha para o `maint` usuário.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.

2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `1` para ver o `System Configuration` menu.
6. Digitar `1` para alterar a senha do usuário de manutenção e seguir as instruções na tela.

Aumente a CPU ou a RAM da instância da VM

Você pode aumentar a CPU ou a RAM da instância da VM que hospeda o agente do Console.

Edite as configurações da instância da VM no seu host VCenter ou ESXi e use o Console de manutenção para aplicar as alterações.

Etapas no cliente VSphere

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Clique com o botão direito do mouse na instância da VM e selecione **Editar configurações**.
4. Aumente o espaço do disco rígido usado para /opt ou a partição /var.
   a. Selecione **Disco Rígido 2** para aumentar o espaço no disco rígido usado para /opt.
   b. Selecione **Disco Rígido 3** para aumentar o espaço no disco rígido usado para /var.
5. Salve suas alterações.

Etapas no console de manutenção

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `1 to view the `System Configuration` menu.
6. Digitar `2` e siga as instruções na tela. O console procura novas configurações e aumenta o tamanho das partições.

Exibir configurações de rede para a VM do agente

Visualize as configurações de rede da VM do agente no cliente VSphere para confirmar ou solucionar problemas de rede. Você só pode visualizar (não atualizar) as seguintes configurações de rede: endereço IP e detalhes de DNS.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.

4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2` para ver o `Network Configuration` menu.
6. Digite um número entre 1 e 6 para visualizar as configurações de rede correspondentes.

Atualizar as rotas estáticas para a VM do agente

Adicione, atualize ou remova rotas estáticas para a VM do agente, conforme necessário.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2` para ver o `Network Configuration` menu.
6. Digitar `7` para atualizar rotas estáticas e seguir as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digitar `9` para confirmar suas alterações.

Atualizar as configurações de pesquisa de domínio para a VM do agente

Você pode atualizar as configurações do domínio de pesquisa para a VM do agente.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `2`` para ver o `Network Configuration` menu.
6. Digitar `8` para atualizar as configurações de pesquisa de domínio e seguir as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digitar `9` para confirmar suas alterações.

Acesse as ferramentas de diagnóstico do agente

Acesse ferramentas de diagnóstico para solucionar problemas com o agente do Console. O Suporte da NetApp pode solicitar que você faça isso ao solucionar problemas.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `3` para visualizar o menu Suporte e Diagnóstico.
6. Digitar `1` para acessar as ferramentas de diagnóstico e seguir as instruções na tela. + Por exemplo, você pode verificar se todos os serviços do agente estão em execução. "Verifique o status do agente do Console" .

Acesse as ferramentas de diagnóstico do agente remotamente

Você pode acessar ferramentas de diagnóstico remotamente com uma ferramenta como o Putty. Habilite o acesso SSH à VM do agente atribuindo uma senha de uso único.

O acesso SSH habilita recursos avançados do terminal, como copiar e colar.

Passos

1. Abra o cliente VSphere e faça login no seu VCenter.
2. Selecione a instância da VM que hospeda o agente do Console.
3. Selecione **Iniciar Console Web**.
4. Efetue login na instância da VM usando o nome de usuário e a senha que você especificou quando criou a instância da VM. O nome de usuário é `maint` e a senha é aquela que você especificou quando criou a instância da VM.
5. Digitar `3` para ver o `Support and Diagnostics` menu.
6. Digitar `2` para acessar as ferramentas de diagnóstico e seguir as instruções na tela para configurar uma senha de uso único que expira em 24 horas.
7. Use uma ferramenta SSH como o Putty para se conectar à VM do agente usando o nome de usuário `diag` e a senha de uso único que você configurou.

Instalar um certificado assinado por CA para acesso ao console baseado na web

Quando você usa o NetApp Console no modo restrito, a interface do usuário pode ser acessada na máquina virtual do agente do Console implantada na sua região de nuvem ou no local. Por padrão, o Console usa um certificado SSL autoassinado para fornecer acesso HTTPS seguro ao console baseado na Web em execução no agente do Console.

Se exigido pela sua empresa, você pode instalar um certificado assinado por uma autoridade de certificação (CA), que fornece melhor proteção de segurança do que um certificado autoassinado. Após instalar o certificado, o Console usa o certificado assinado pela CA quando os usuários acessam o console baseado na Web.

Instalar um certificado HTTPS

Instale um certificado assinado por uma CA para acesso seguro ao console baseado na Web em execução no

agente do Console.

Sobre esta tarefa

Você pode instalar o certificado usando uma das seguintes opções:

- Gere uma solicitação de assinatura de certificado (CSR) no Console, envie a solicitação de certificado para uma CA e instale o certificado assinado pela CA no agente do Console.

  O par de chaves que o Console usa para gerar o CSR é armazenado internamente no agente do Console. O Console recupera automaticamente o mesmo par de chaves (chave privada) quando você instala o certificado no agente do Console.

- Instale um certificado assinado pela CA que você já tenha.

  Com esta opção, o CSR não é gerado pelo Console. Você gera o CSR separadamente e armazena a chave privada externamente. Você fornece a chave privada ao Console quando instala o certificado.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Configuração HTTPS**.

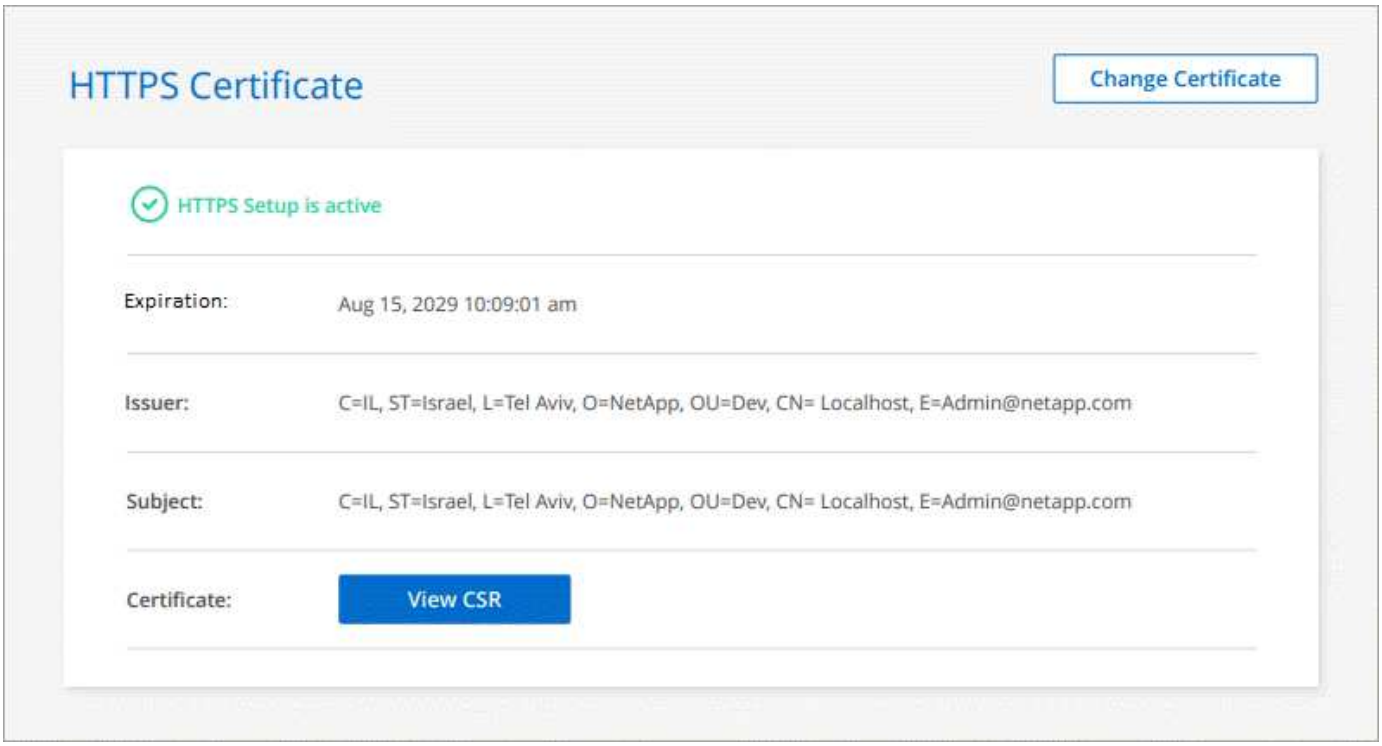
   O agente do Console precisa estar conectado para que você possa editá-lo.

3. Na página Configuração de HTTPS, instale um certificado gerando uma solicitação de assinatura de certificado (CSR) ou instalando seu próprio certificado assinado pela CA:

Opção	Descrição
Gerar um CSR	a. Insira o nome do host ou DNS do host do agente do Console (seu Nome Comum) e selecione **Gerar CSR**. O Console exibe uma solicitação de assinatura de certificado. b. Use o CSR para enviar uma solicitação de certificado SSL a uma CA. O certificado deve usar o formato X.509 codificado em Base 64 do Privacy Enhanced Mail (PEM). c. Carregue o arquivo de certificado e selecione **Instalar**.
Instale seu próprio certificado assinado pela CA	a. Selecione **Instalar certificado assinado pela CA**. b. Carregue o arquivo de certificado e a chave privada e selecione **Instalar**. O certificado deve usar o formato X.509 codificado em Base 64 do Privacy Enhanced Mail (PEM).

Resultado

O agente do Console agora usa o certificado assinado pela CA para fornecer acesso HTTPS seguro. A imagem a seguir mostra um agente configurado para acesso seguro:



Renovar o certificado HTTPS do Console

Você deve renovar o certificado HTTPS do agente antes que ele expire para garantir acesso seguro. Se você não renovar o certificado antes que ele expire, um aviso será exibido quando os usuários acessarem o console da web usando HTTPS.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Configuração HTTPS**.

   Detalhes sobre o certificado são exibidos, incluindo a data de validade.

3. Selecione **Alterar certificado** e siga as etapas para gerar um CSR ou instalar seu próprio certificado assinado pela CA.

Configurar um agente de console para usar um servidor proxy

Se suas políticas corporativas exigirem que você use um servidor proxy para todas as comunicações com a Internet, será necessário configurar seus agentes para usar esse servidor proxy. Se você não configurou um agente do Console para usar um servidor proxy durante a instalação, poderá configurá-lo para usar esse servidor proxy a qualquer momento.

O servidor proxy do agente permite acesso de saída à Internet sem um IP público ou gateway NAT. O servidor proxy fornece conectividade de saída somente para o agente do Console, não para sistemas Cloud Volumes ONTAP .

Se os sistemas Cloud Volumes ONTAP não tiverem acesso de saída à Internet, o Console os configurará para usar o servidor proxy do agente do Console. Você deve garantir que o grupo de segurança do agente do

Console permita conexões de entrada pela porta 3128. Abra esta porta após implantar o agente do Console.

Se o próprio agente do Console não tiver uma conexão de saída com a Internet, os sistemas Cloud Volumes ONTAP não poderão usar o servidor proxy configurado.

Configurações suportadas

- Servidores proxy transparentes são suportados por agentes que atendem sistemas Cloud Volumes ONTAP . Se você usar serviços de dados da NetApp com o Cloud Volumes ONTAP, crie um agente dedicado para o Cloud Volumes ONTAP onde você pode usar um servidor proxy transparente.
- Servidores proxy explícitos são suportados por todos os agentes, incluindo aqueles que gerenciam sistemas Cloud Volumes ONTAP e aqueles que gerenciam serviços de dados NetApp .
- HTTP e HTTPS.
- O servidor proxy pode residir na nuvem ou na sua rede.

> Depois de configurar um proxy, você não poderá alterar o tipo de proxy. Se precisar alterar o tipo de proxy, remova o agente do Console e adicione um novo agente com o novo tipo de proxy.

Habilitar um proxy explícito em um agente do Console

Quando você configura um agente do Console para usar um servidor proxy, esse agente e os sistemas Cloud Volumes ONTAP que ele gerencia (incluindo quaisquer mediadores de HA) usam o servidor proxy.

Esta operação reinicia o agente do Console. Verifique se o agente do Console está ocioso antes de prosseguir.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Selecione **Configuração de proxy HTTP**.
4. Selecione **Proxy explícito** no campo Tipo de configuração.
5. Selecione **Ativar proxy**.
6. Especifique o servidor usando a sintaxe http://address:port ou https://address:port
7. Especifique um nome de usuário e uma senha se a autenticação básica for necessária para o servidor.

   Observe o seguinte:

   - O usuário pode ser um usuário local ou de domínio.
   - Para um usuário de domínio, você deve inserir o código ASCII para \ da seguinte forma: nome-de-domínio%92nome-de-usuário

     Por exemplo: netapp%92proxy

   - O Console não suporta senhas que incluem o caractere @.

8. Selecione **Salvar**.

Habilitar um proxy transparente para um agente do Console

Somente o Cloud Volumes ONTAP oferece suporte ao uso de um proxy transparente no agente do Console. Se você usar serviços de dados da NetApp além do Cloud Volumes ONTAP, crie um agente separado para usar em serviços de dados ou para usar no Cloud Volumes ONTAP.

Antes de habilitar um proxy transparente, certifique-se de que os seguintes requisitos sejam atendidos:

- O agente é instalado na mesma rede que o servidor proxy transparente.
- A inspeção TLS está habilitada no servidor proxy.
- Você tem um certificado no formato PEM que corresponde ao usado no servidor proxy transparente.
- Não use o agente do Console para nenhum serviço de dados da NetApp além do Cloud Volumes ONTAP.

Para configurar um agente existente para usar um servidor proxy transparente, use a ferramenta de manutenção do agente do Console, disponível por meio da linha de comando no host do agente do Console.

Quando você configura um servidor proxy, o agente do Console é reiniciado. Verifique se o agente do Console está ocioso antes de prosseguir.

Passos

Certifique-se de ter um arquivo de certificado no formato PEM para o servidor proxy. Se você não tiver um certificado, entre em contato com o administrador da rede para obtê-lo.

1. Abra uma interface de linha de comando no host do agente do Console.
2. Navegue até o diretório da ferramenta de manutenção do agente do Console: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Execute o seguinte comando para habilitar o proxy transparente, onde `/home/ubuntu/<certificate-file>.pem` é o diretório e o arquivo de certificado de nome que você tem para o servidor proxy:

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   Certifique-se de que o arquivo de certificado esteja no formato PEM e resida no mesmo diretório que o comando ou especifique o caminho completo para o arquivo de certificado.

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Modifique o proxy transparente para o agente do Console

Você pode atualizar o servidor proxy transparente existente de um agente do Console usando o `proxy update` comando ou remova o servidor proxy transparente usando o `proxy remove` comando. Para obter mais informações, consulte a documentação."Console de manutenção do agente" .

> Depois de configurar um proxy, você não poderá alterar o tipo de proxy. Se precisar alterar o tipo de proxy, remova o agente do Console e adicione um novo agente com o novo tipo de proxy.

Atualize o proxy do agente do Console se ele perder o acesso à Internet

Se a configuração de proxy da sua rede mudar, seu agente poderá perder o acesso à Internet. Por exemplo, se alguém alterar a senha do servidor proxy ou atualizar o certificado. Nesse caso, você precisará acessar a interface do usuário diretamente do host do agente do Console e atualizar as configurações. Certifique-se de ter acesso à rede do host do agente do Console e de poder efetuar login no Console.

Habilitar tráfego direto da API

Se você configurou um agente do Console para usar um servidor proxy, pode habilitar o tráfego direto da API no agente do Console para enviar chamadas de API diretamente aos serviços do provedor de nuvem sem passar pelo proxy. Agentes executados na AWS, Azure ou Google Cloud são compatíveis com essa opção.

Se você desabilitar o Azure Private Links com o Cloud Volumes ONTAP e usar pontos de extremidade de serviço, habilite o tráfego de API direto. Caso contrário, o tráfego não será roteado corretamente.

"Saiba mais sobre como usar um Azure Private Link ou pontos de extremidade de serviço com o Cloud Volumes ONTAP"

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Selecione **Suporte ao tráfego direto da API**.
4. Marque a caixa de seleção para habilitar a opção e selecione **Salvar**.

Solucionar problemas do agente do console

Para solucionar problemas com um agente do Console, você pode verificar os problemas sozinho ou trabalhar com o Suporte da NetApp , que pode solicitar o ID do seu sistema, a versão do agente ou as mensagens mais recentes do AutoSupport .

Se você tiver uma conta no site de suporte da NetApp , também poderá visualizar o"Base de conhecimento da NetApp ."

Mensagens de erro comuns e soluções

Esta tabela lista mensagens de erro comuns e mostra como corrigi-las:

Mensagem de erro	Explicação	O que fazer
Não é possível carregar a interface do usuário do agente do console	A instalação do agente falhou	• Verifique se o serviço Service Manager está ativo. • Verifique se todos os contêineres estão em execução. • Certifique-se de que seu firewall permite acesso ao serviço na porta 8888. • Se você ainda tiver problemas, entre em contato com o suporte.
Não é possível acessar a interface do usuário do agente NetApp	Esta mensagem aparece ao tentar acessar o endereço IP de um agente. O agente pode falhar ao inicializar se não tiver o acesso correto à rede ou se estiver instável.	• Conecte-se ao agente do Console. • Verifique se o serviço Service Manager • Verifique se o agente tem o acesso à rede necessário."Saiba mais sobre os pontos de extremidade de acesso à rede necessários."
Não é possível carregar as configurações do agente	O Console exibe esta mensagem quando você tenta acessar a página de configurações do Agente.	• Verifique se o contêiner OCCM está em execução e funcionando. • Se o problema persistir, entre em contato com o suporte.
Não é possível carregar informações de suporte para o agente.	Esta mensagem é exibida se o agente não conseguir acessar sua conta de suporte.	• Verifique se o agente tem acesso de saída aos endpoints necessários."Saiba mais sobre os pontos de extremidade de acesso à rede necessários."

Verifique o status do agente do Console

Use um dos seguintes comandos para verificar seu agente do Console. Todos os serviços devem ter o status *Em execução*. Se esse não for o caso, entre em contato com o suporte da NetApp .

Para obter informações mais detalhadas sobre como acessar o diagnóstico do agente do Console, consulte os seguintes tópicos:

- "Verifique o status do agente do console (para implantações de host Linux)"
- "Verifique o status do agente do console (para implantações do VCenter)"

Docker (para implantações do Ubuntu e VCenter)

```
docker ps -a
```

Podman (para implantações do RedHat Enterprise Linux)

```
podman ps -a
```

Ver a versão do agente do Console

Visualize a versão do agente do Console para confirmar a atualização ou compartilhe-a com seu representante da NetApp .

Passos

1. Selecione **Administração > Suporte > Agentes**.

   O Console exibe a versão no topo da página.

Verificar acesso à rede

Certifique-se de que o agente do Console tenha o acesso à rede necessário."Saiba mais sobre os pontos de acesso de rede necessários."

Execute verificações de configuração no agente do console.

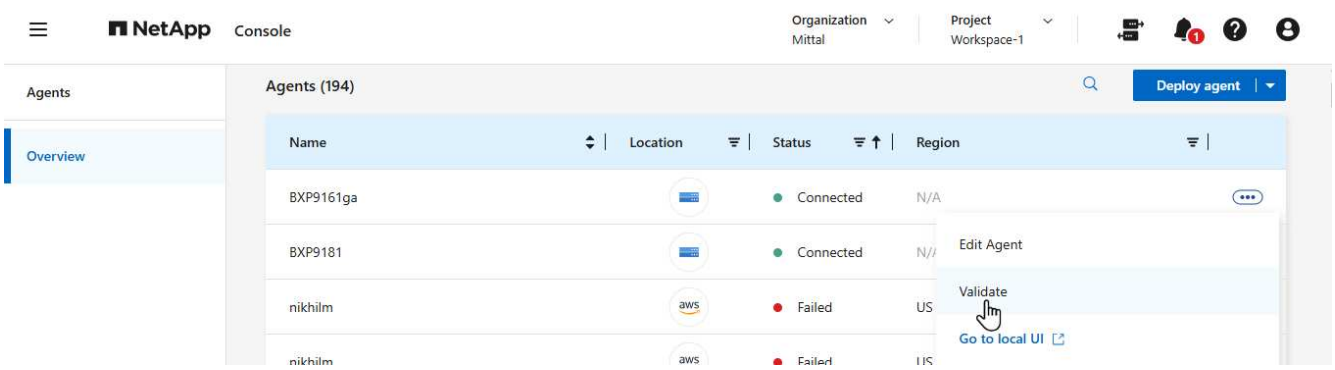
Execute verificações de configuração nos agentes do Console a partir do Console ou do console de manutenção do agente para garantir que estejam conectados.

Você também pode executar verificações de configuração usando o console de manutenção do agente."Saiba mais sobre como usar o comando `config-checker validate`."

Você só pode validar agentes que tenham o status **Conectado**.

Etapas a partir do console

1. Selecione **Administração > Agentes**.
2. Selecione o menu de ações do agente do Console que deseja verificar e escolha **Validar**.



A validação pode levar até 15 minutos. Os resultados serão mostrados quando o processo estiver concluído.

Problemas de instalação do agente do console

Se a instalação falhar, visualize o relatório e os logs para resolver os problemas.

Você também pode acessar o relatório de validação no formato JSON e os logs de configuração diretamente do host do agente do Console nos seguintes diretórios:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Para novas implantações de agentes, a NetApp verifica os seguintes endpoints:"listados aqui" . Esta verificação de configuração falhará com um erro se você estiver usando os endpoints anteriores usados para atualizações,"listados aqui" . A NetApp recomenda atualizar suas regras de firewall para permitir acesso aos endpoints atuais e bloquear o acesso aos endpoints anteriores o mais breve possível."Aprenda a atualizar sua rede" .
- Se você atualizar os endpoints no seu firewall, seus agentes existentes continuarão funcionando.

Desabilitar verificações de configuração para instalações manuais

Pode haver momentos em que você precise desabilitar as verificações de configuração que verificam a conectividade de saída durante a instalação. Por exemplo, ao instalar manualmente um agente no seu ambiente de Nuvem Governamental, você precisa desativar as verificações de configuração, caso contrário, a instalação falhará.

Passos

Você desabilita a verificação de configuração definindo o sinalizador *skipConfigCheck* no arquivo *com/opt/application/netapp/service-manager-2/config.json*. Por padrão, esse sinalizador é definido como falso e a verificação de configuração verifica o acesso de saída do agente. Defina este sinalizador como verdadeiro para desabilitar a verificação. Familiarize-se com a sintaxe JSON antes de concluir esta etapa.

Para reativar a verificação de configuração, siga estas etapas e defina o sinalizador *skipConfigCheck* como falso.

Passos

1. Acesse o host do agente do Console como root ou com privilégios sudo.
2. Crie uma cópia de backup do arquivo */opt/application/netapp/service-manager-2/config.json* para garantir que você possa reverter suas alterações.
3. Pare o serviço do gerenciador de serviços 2 executando o seguinte comando:

```
systemctl stop netapp-service-manager.service
```

1. Edite o arquivo */opt/application/netapp/service-manager-2/config.json* e altere o valor do sinalizador *skipConfigCheck* para true.

```
"skipConfigCheck": true
```

2. Salve seu arquivo.
3. Reinicie o serviço do gerenciador de serviços 2 executando o seguinte comando:

```
systemctl restart netapp-service-manager.service
```

Trabalhe com o suporte da NetApp

Se você não conseguiu resolver os problemas com seu agente do Console, entre em contato com o Suporte da NetApp . O suporte da NetApp pode solicitar o ID do agente do Console ou que você envie os logs do agente do Console, caso eles ainda não os tenham.

Encontre o ID do agente do console

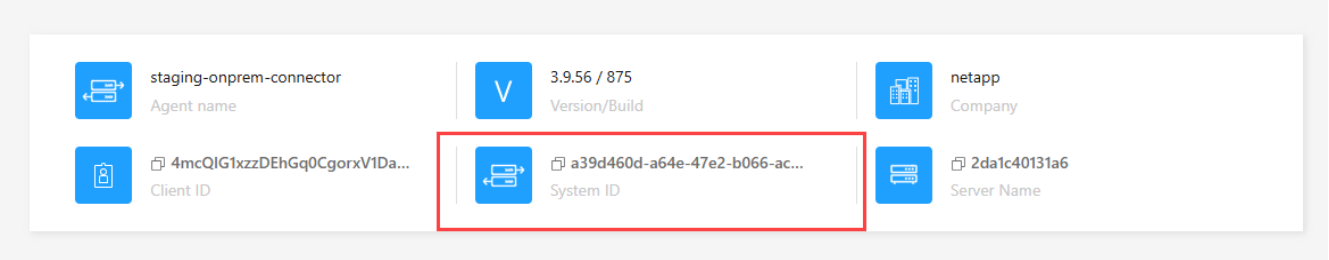
Para ajudar você a começar, você pode precisar do ID do sistema do seu agente do Console. O ID normalmente é usado para fins de licenciamento e solução de problemas.

Passos

1. Selecione **Administração > Suporte > Agentes**.

   Você pode encontrar o ID do sistema no topo da página.

   Exemplo

2. Passe o mouse e clique no ID para copiá-lo.

Baixe ou envie uma mensagem de AutoSupport

Se você estiver tendo problemas, a NetApp pode solicitar que você envie uma mensagem de AutoSupport para o suporte da NetApp para fins de solução de problemas.

O NetApp Console leva até cinco horas para enviar mensagens de AutoSupport devido ao balanceamento de carga. Para comunicação urgente, baixe o arquivo e envie-o manualmente.

Passos

1. Selecione **Administração > Suporte > Agentes**.
2. Dependendo de como você precisa enviar as informações para o suporte da NetApp , escolha uma das seguintes opções:
   a. Selecione a opção para baixar a mensagem do AutoSupport para sua máquina local. Você pode então enviá-lo ao Suporte da NetApp usando um método de sua preferência.
   b. Selecione **Enviar AutoSupport** para enviar a mensagem diretamente ao Suporte da NetApp .

Corrigir falhas de download ao usar um gateway NAT do Google Cloud

O agente do Console baixa automaticamente as atualizações de software para o Cloud Volumes ONTAP. Sua

configuração pode causar falha no download se ele usar um gateway NAT do Google Cloud. Você pode corrigir esse problema limitando o número de partes em que a imagem do software é dividida. Esta etapa deve ser concluída usando a API.

Etapa

1. Envie uma solicitação PUT para /occm/config com o seguinte JSON como corpo:

```
{
  "maxDownloadSessions": 32
}
```

   O valor para *maxDownloadSessions* pode ser 1 ou qualquer número inteiro maior que 1. Se o valor for 1, a imagem baixada não será dividida.

   Observe que 32 é um valor de exemplo. O valor depende da sua configuração NAT e do número de sessões simultâneas.

"Saiba mais sobre a chamada de API /occm/config"

Obtenha ajuda na Base de conhecimento da NetApp

"Veja as informações de solução de problemas criadas pela equipe de suporte da NetApp" .

Desinstalar e remover um agente do Console

Desinstale o agente do Console para solucionar problemas ou removê-lo permanentemente do host. As etapas que você precisa usar dependem do modo de implantação que você está usando. Depois de remover um agente do Console do seu ambiente, você pode removê-lo do Console.

"Saiba mais sobre os modos de implantação do NetApp Console" .

Desinstale o agente ao usar o modo padrão ou restrito

Se você estiver usando o modo padrão ou o modo restrito (em outras palavras, o host do agente tem conectividade de saída), siga as etapas abaixo para desinstalar o agente.

Passos

1. Conecte-se à VM Linux para o agente.
2. No host Linux, execute o script de desinstalação:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent executa o script sem solicitar sua confirmação.

Remover agentes do Console do Console

Se você excluiu uma máquina virtual de agente ou desinstalou o agente, deverá removê-la da lista de agentes no Console. Após excluir uma máquina virtual do agente ou desinstalar o software do agente, o agente exibirá o status **Desconectado** no Console.

Observe o seguinte sobre a remoção de um agente do Console:

- Esta ação não exclui a máquina virtual.
- Esta ação não pode ser revertida: depois de remover um agente do Console, você não poderá adicioná-lo novamente.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ações para um agente desconectado e selecione **Remover agente**.
3. Digite o nome do agente para confirmar e selecione **Remover**.

Gerenciar credenciais de provedores de nuvem

AWS

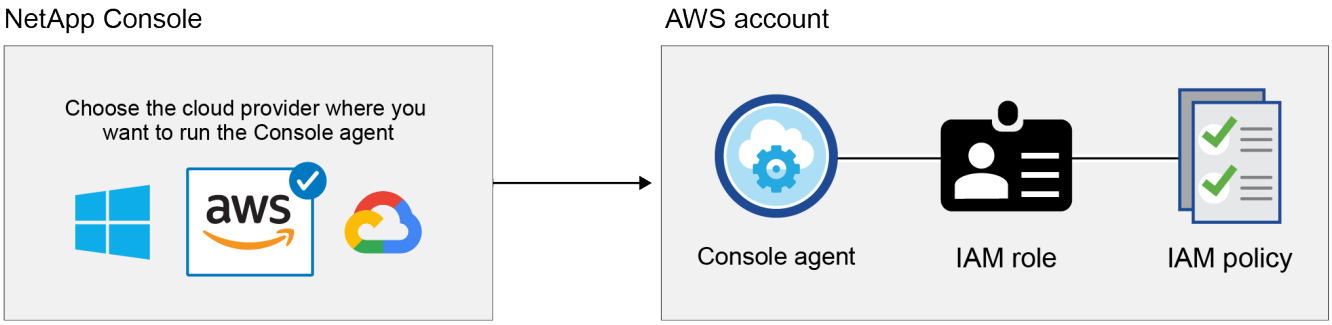
Saiba mais sobre credenciais e permissões da AWS no NetApp Console

Você gerencia as credenciais da AWS e as assinaturas do marketplace diretamente do NetApp Console para garantir a implantação segura do Cloud Volumes ONTAP e de outros serviços de dados, fornecendo as credenciais IAM apropriadas durante a implantação do agente do Console e associando-as às assinaturas do AWS Marketplace para faturamento.

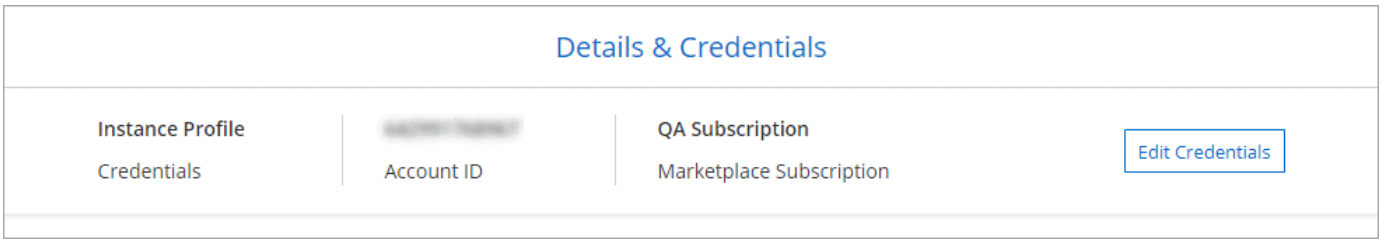
Credenciais iniciais da AWS

Ao implantar um agente do Console a partir do Console, você precisa fornecer o ARN de uma função do IAM ou chaves de acesso para um usuário do IAM. O método de autenticação deve ter permissões para implantar o agente do Console na AWS. As permissões necessárias estão listadas no"Política de implantação de agentes para AWS" .

Quando o Console inicia o agente do Console na AWS, ele cria uma função do IAM e um perfil para o agente. Ele também anexa uma política que fornece ao agente do Console permissões para gerenciar recursos e processos dentro dessa conta da AWS. "Revise como o Agente usa as permissões".



Se você adicionar um novo sistema Cloud Volumes ONTAP , o Console selecionará estas credenciais da AWS por padrão:



Implante todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais da AWS ou adicione credenciais adicionais.

Credenciais adicionais da AWS

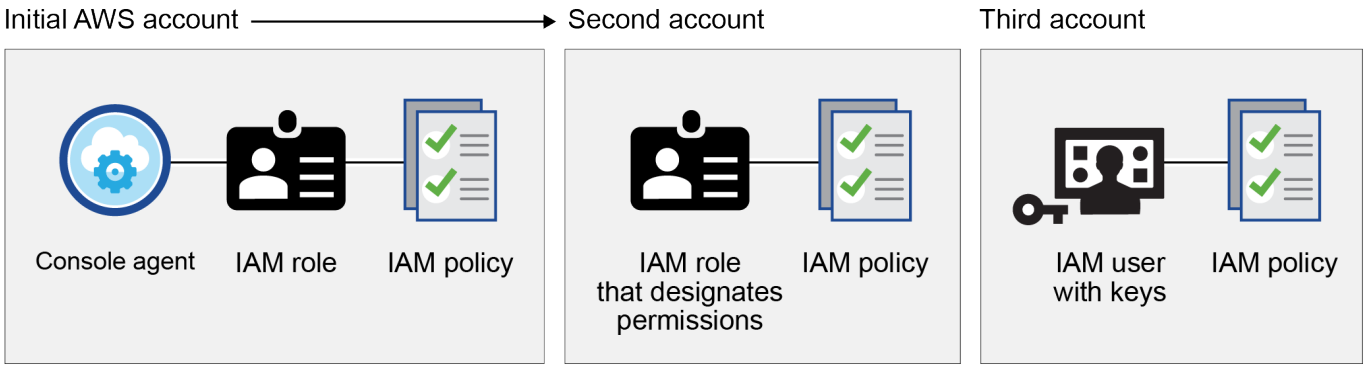
Você pode adicionar credenciais adicionais da AWS ao Console nos seguintes casos:

- Para usar seu agente de console existente com uma conta AWS adicional.
- Para criar um novo agente em uma conta específica da AWS
- Para criar e gerenciar FSx para sistemas de arquivos ONTAP

Revise as seções abaixo para mais detalhes.

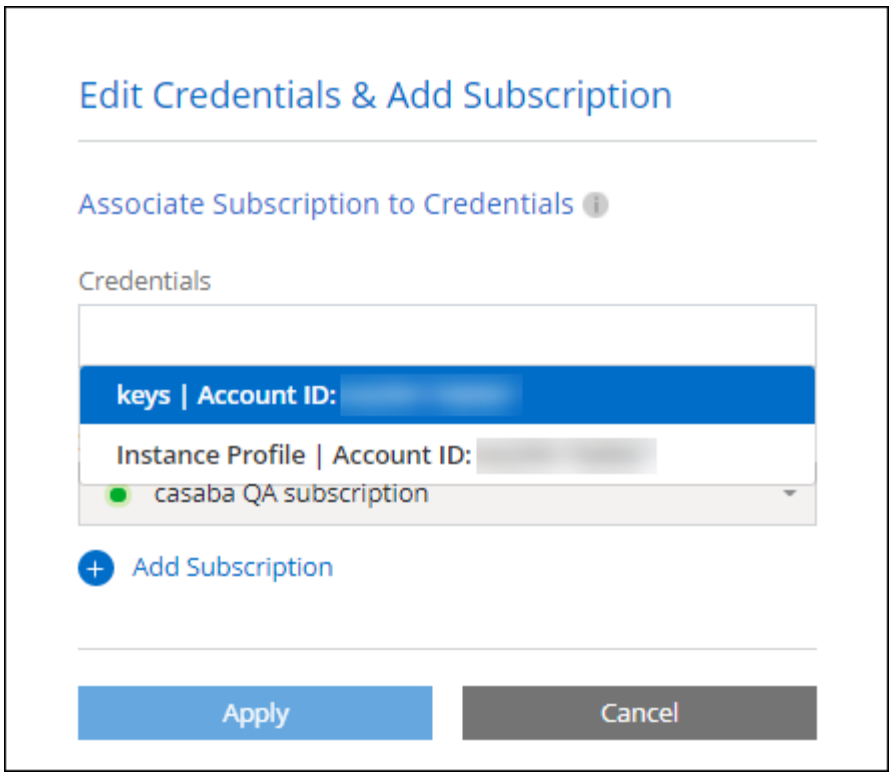
Adicione credenciais da AWS para usar um agente do Console com outra conta da AWS

Para usar o Console com contas AWS adicionais, forneça as chaves da AWS ou o ARN de uma função em uma conta confiável. A imagem a seguir mostra duas contas adicionais, uma fornecendo permissões por meio de uma função do IAM em uma conta confiável e outra por meio das chaves da AWS de um usuário do IAM:



Você adiciona credenciais de conta ao Console especificando o Nome de Recurso da Amazon (ARN) da função do IAM ou as chaves da AWS para o usuário do IAM.

Por exemplo, você pode alternar entre credenciais ao criar um novo sistema Cloud Volumes ONTAP :



"Saiba como adicionar credenciais da AWS a um agente existente."

Adicione credenciais da AWS para criar um agente do Console

Adicionar credenciais da AWS fornece permissões para criar um agente do Console.

"Aprenda como adicionar credenciais da AWS ao Console para criar um agente do Console"

Adicionar credenciais da AWS para FSx para ONTAP

Adicione credenciais da AWS ao Console para fornecer as permissões necessárias para criar e gerenciar um sistema FSx para ONTAP .

"Aprenda como adicionar credenciais da AWS ao Console do Amazon FSx para ONTAP"

Credenciais e assinaturas de mercado

Você deve associar as credenciais adicionadas a um agente do Console a uma assinatura do AWS Marketplace para pagar pelo Cloud Volumes ONTAP por hora (PAYGO) e outros serviços de dados da NetApp ou por meio de um contrato anual. "Aprenda como associar uma assinatura da AWS".

Observe o seguinte sobre credenciais da AWS e assinaturas do marketplace:

- Você pode associar apenas uma assinatura do AWS Marketplace a um conjunto de credenciais da AWS
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Perguntas frequentes

As perguntas a seguir estão relacionadas a credenciais e assinaturas.

Como posso rotacionar minhas credenciais da AWS com segurança?

Conforme descrito nas seções acima, o Console permite que você forneça credenciais da AWS de algumas maneiras: uma função do IAM associada ao agente do Console, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS.

Com as duas primeiras opções, o Console usa o AWS Security Token Service para obter credenciais temporárias que são rotacionadas constantemente. Este processo é a melhor prática – é automático e seguro.

Se você fornecer ao Console chaves de acesso da AWS, deverá rotacionar as chaves atualizando-as no Console em intervalos regulares. Este é um processo completamente manual.

Posso alterar a assinatura do AWS Marketplace para sistemas Cloud Volumes ONTAP ?

Sim, você pode. Quando você altera a assinatura do AWS Marketplace associada a um conjunto de credenciais, todos os sistemas Cloud Volumes ONTAP existentes e novos são cobrados na nova assinatura.

"Aprenda como associar uma assinatura da AWS" .

Posso adicionar várias credenciais da AWS, cada uma com diferentes assinaturas de marketplace?

Todas as credenciais da AWS que pertencem à mesma conta da AWS serão associadas à mesma assinatura do AWS Marketplace.

Se você tiver várias credenciais da AWS que pertencem a diferentes contas da AWS, essas credenciais poderão ser associadas à mesma assinatura do AWS Marketplace ou a assinaturas diferentes.

Posso mover sistemas Cloud Volumes ONTAP existentes para uma conta AWS diferente?

Não, não é possível mover os recursos da AWS associados ao seu sistema Cloud Volumes ONTAP para uma conta diferente da AWS.

Como as credenciais funcionam para implantações de mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o agente do Console, que é do Console. Você também pode implantar um agente na AWS a partir do AWS Marketplace e pode instalar manualmente o software do agente do Console em seu próprio host Linux ou em seu vCenter.

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a função do IAM e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, você não pode configurar uma função do IAM para o Console, mas pode fornecer permissões usando chaves de acesso da AWS.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão
  - "Configurar permissões para uma implantação do AWS Marketplace"
  - "Configurar permissões para implantações locais"
- Modo restrito
  - "Configurar permissões para o modo restrito"

Adicione e gerencie credenciais da AWS para que você implante e gerencie recursos de nuvem em suas contas da AWS a partir do NetApp Console. Se você gerencia várias assinaturas do AWS Marketplace, pode atribuir cada uma delas a diferentes credenciais da AWS na página Credenciais.

Visão geral

Você pode adicionar credenciais da AWS a um agente do Console existente ou diretamente ao Console:

- Adicionar credenciais adicionais da AWS a um agente existente

  Adicione credenciais da AWS a um agente do Console para gerenciar recursos de nuvem. Aprenda como adicionar credenciais da AWS a um agente do Console .

- Adicione credenciais da AWS ao Console para criar um agente do Console

  Adicionar novas credenciais da AWS ao Console fornece as permissões necessárias para criar um agente do Console. Aprenda como adicionar credenciais da AWS ao NetApp Console .

- Adicionar credenciais da AWS ao Console do FSx para ONTAP

  Adicione novas credenciais da AWS ao Console para criar e gerenciar o FSx para ONTAP. "Aprenda a configurar permissões para FSx para ONTAP"

Como rotacionar credenciais

O NetApp Console permite que você forneça credenciais da AWS de algumas maneiras: uma função do IAM associada à instância do agente, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS. "Saiba mais sobre credenciais e permissões da AWS" .

Com as duas primeiras opções, o Console usa o AWS Security Token Service para obter credenciais temporárias que são rotacionadas constantemente. Esse processo é a melhor prática porque é automático e seguro.

Gire manualmente as chaves de acesso da AWS atualizando-as no Console.

Adicionar credenciais adicionais a um agente do Console

Adicione credenciais adicionais da AWS a um agente do Console para que ele tenha as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. Você pode fornecer o ARN de uma função do IAM em outra conta ou fornecer chaves de acesso da AWS.

"Saiba como o NetApp Console usa credenciais e permissões da AWS".

Conceder permissões

Conceda permissões antes de adicionar credenciais da AWS a um agente do Console. As permissões permitem que um agente do Console gerencie recursos e processos dentro dessa conta da AWS. Você pode fornecer as permissões com o ARN de uma função em uma conta confiável ou chaves da AWS.

Se você implantou um agente do Console a partir do Console, ele adicionou automaticamente credenciais da AWS para a conta na qual você implantou um agente do Console. Isso garante que as permissões necessárias estejam em vigor para gerenciar recursos.

Escolhas

- Conceder permissões assumindo uma função do IAM em outra conta
- Conceder permissões fornecendo chaves da AWS

Conceder permissões assumindo uma função do IAM em outra conta

Você pode configurar uma relação de confiança entre a conta de origem da AWS na qual você implantou um agente do Console e outras contas da AWS usando funções do IAM. Em seguida, você forneceria ao Console o ARN das funções do IAM das contas confiáveis.

Se um agente do Console estiver instalado no local, você não poderá usar esse método de autenticação. Você deve usar chaves da AWS.

Passos

1. Acesse o console do IAM na conta de destino na qual você deseja fornecer permissões ao agente do Console.
2. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.

   Não se esqueça de fazer o seguinte:

   - Em **Tipo de entidade confiável**, selecione **Conta AWS**.
   - Selecione **Outra conta da AWS** e insira o ID da conta onde reside uma instância do agente do Console.
   - Crie as políticas necessárias copiando e colando o conteúdo de"as políticas do IAM para um agente do Console" .
3. Copie o ARN da função do IAM para poder colá-lo no Console mais tarde.

Resultado

A conta tem as permissões necessárias. Agora você pode adicionar as credenciais a um agente do Console .

Conceder permissões fornecendo chaves da AWS

Se você quiser fornecer ao Console chaves da AWS para um usuário do IAM, precisará conceder as permissões necessárias a esse usuário. A política do Console IAM define as ações e os recursos da AWS que o Console tem permissão para usar.

Você deve usar este método de autenticação se um agente do Console estiver instalado no local. Você não pode usar uma função do IAM.

Passos

1. No console do IAM, crie políticas copiando e colando o conteúdo de"as políticas do IAM para um agente do Console" .

   "Documentação da AWS: Criando políticas do IAM"
2. Anexe as políticas a uma função do IAM ou a um usuário do IAM.

- "Documentação da AWS: Criando funções do IAM"
- "Documentação da AWS: Adicionando e removendo políticas do IAM"

Adicione as credenciais a um agente existente

Depois de fornecer a uma conta da AWS as permissões necessárias, você pode adicionar as credenciais dessa conta a um agente existente. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta usando o mesmo agente.

Novas credenciais no seu provedor de nuvem podem levar alguns minutos para ficarem disponíveis.

Passos

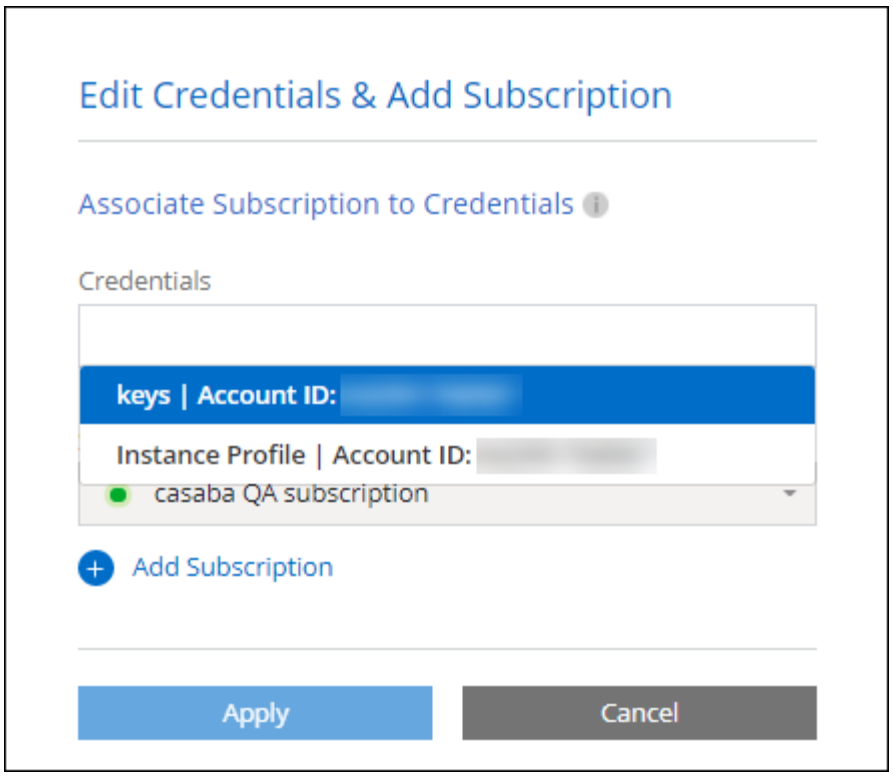
1. Use a barra de navegação superior para selecionar um agente do Console ao qual você deseja adicionar credenciais.
2. Na barra de navegação à esquerda, selecione **Administração > Credenciais**.
3. Na página **Credenciais da organização**, selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Agente**.
   b. **Definir credenciais**: forneça o ARN (Amazon Resource Name) de uma função do IAM confiável ou insira uma chave de acesso e uma chave secreta da AWS.
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.

      Para pagar por serviços por hora (PAYGO) ou com um contrato anual, você deve associar as credenciais da AWS à sua assinatura do AWS Marketplace.

   d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

Agora você pode alternar para um conjunto diferente de credenciais na página Detalhes e credenciais ao adicionar uma assinatura ao Console.



Adicionar credenciais ao Console para criar um agente do Console

Adicione credenciais da AWS fornecendo o ARN de uma função do IAM que concede as permissões necessárias para criar um agente do Console. Você pode escolher essas credenciais ao criar um novo agente.

Configurar a função do IAM

Configure uma função do IAM que permita que a camada de software como serviço (SaaS) do NetApp Console assuma a função.

Passos

1. Acesse o console do IAM na conta de destino.
2. Em Gerenciamento de acesso, selecione **Funções > Criar função** e siga as etapas para criar a função.

   Não se esqueça de fazer o seguinte:

   - Em **Tipo de entidade confiável**, selecione **Conta AWS**.
   - Selecione **Outra conta AWS** e insira o ID do NetApp Console SaaS: 952013314444
   - Especificamente para o Amazon FSx for NetApp ONTAP , edite a política **Relacionamentos de confiança** para incluir "AWS": "arn:aws:iam::952013314444:root".

     Por exemplo, a política deve ficar assim:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Consulte "Documentação do AWS Identity and Access Management (IAM)" para obter mais informações sobre acesso a recursos entre contas no IAM.

- Crie uma política que inclua as permissões necessárias para criar um agente do Console.
  - "Veja as permissões necessárias para o FSx para ONTAP"
  - "Exibir a política de implantação do agente"

3. Copie o ARN da função do IAM para que você possa colá-lo no Console na próxima etapa.

Resultado

A função IAM agora tem as permissões necessárias. Agora você pode adicioná-lo ao Console.

Adicione as credenciais

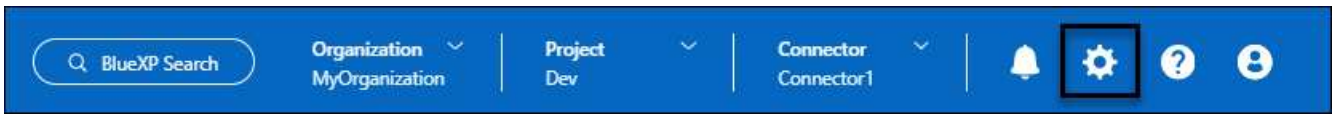
Depois de fornecer à função do IAM as permissões necessárias, adicione o ARN da função ao Console.

Antes de começar

Se você acabou de criar a função do IAM, pode levar alguns minutos até que ela esteja disponível para uso. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Passos

1. Selecione **Administração > Credenciais**.



2. Na página **Credenciais da organização**, selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Amazon Web Services > Console**.
   b. **Definir credenciais**: forneça o ARN (Amazon Resource Name) da função do IAM.
   c. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Adicionar credenciais ao Console do Amazon FSx para ONTAP

Para mais detalhes, consulte o "a documentação do console para Amazon FSx para ONTAP"

Configurar uma assinatura da AWS

Depois de adicionar suas credenciais da AWS, você pode configurar uma assinatura do AWS Marketplace com essas credenciais. A assinatura permite que você pague pelos serviços de dados da NetApp e do Cloud Volumes ONTAP por uma taxa horária (PAYGO) ou usando um contrato anual.

Há dois cenários nos quais você pode configurar uma assinatura do AWS Marketplace depois de já ter adicionado as credenciais:

- Você não configurou uma assinatura quando adicionou as credenciais inicialmente.
- Você deseja alterar a assinatura do AWS Marketplace configurada para as credenciais da AWS.

  Substituir a assinatura atual do marketplace por uma nova assinatura altera a assinatura do marketplace para todos os sistemas Cloud Volumes ONTAP existentes e todos os novos sistemas.

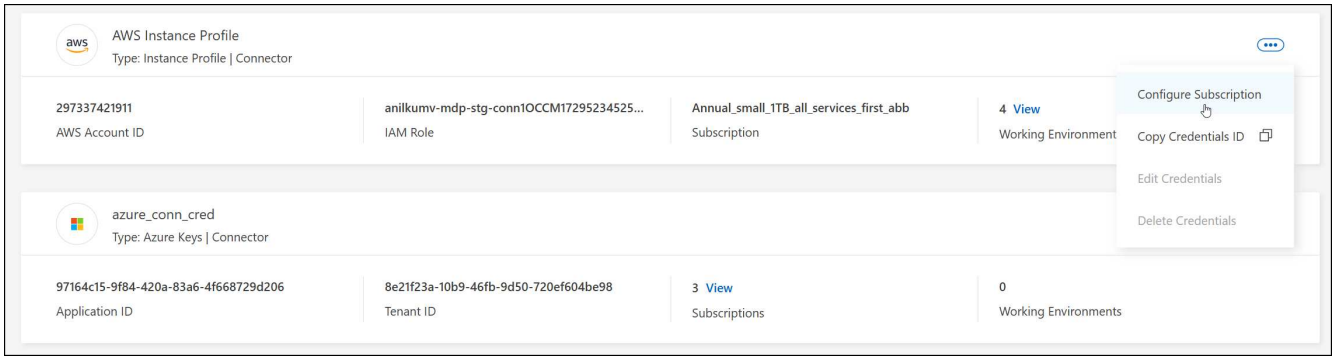
Antes de começar

Você precisa criar um agente do Console antes de poder configurar uma assinatura. "Aprenda a criar um agente de console" .

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais associadas a um agente do Console e selecione **Configurar assinatura**.

   Você deve selecionar credenciais associadas a um agente do Console. Não é possível associar uma assinatura do marketplace a credenciais associadas ao NetApp Console.



4. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e selecione **Configurar**.
5. Para associar as credenciais a uma nova assinatura, selecione **Adicionar assinatura > Continuar** e siga as etapas no AWS Marketplace:

   a. Selecione **Ver opções de compra**.

   b. Selecione **Inscrever-se**.

   c. Selecione **Configurar sua conta**.

Você será redirecionado para o NetApp Console.

d. Na página **Atribuição de Assinatura**:

- Selecione as organizações ou contas do Console às quais você gostaria de associar esta assinatura.
- No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização ou conta por esta nova assinatura.

  O Console substitui a assinatura existente para todas as credenciais na organização ou conta por esta nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

- Selecione **Salvar**.

Associe uma assinatura existente à sua organização

Ao assinar no AWS Marketplace, a última etapa do processo é associar a assinatura à sua organização. Se você não concluiu esta etapa, não poderá usar a assinatura com sua organização.

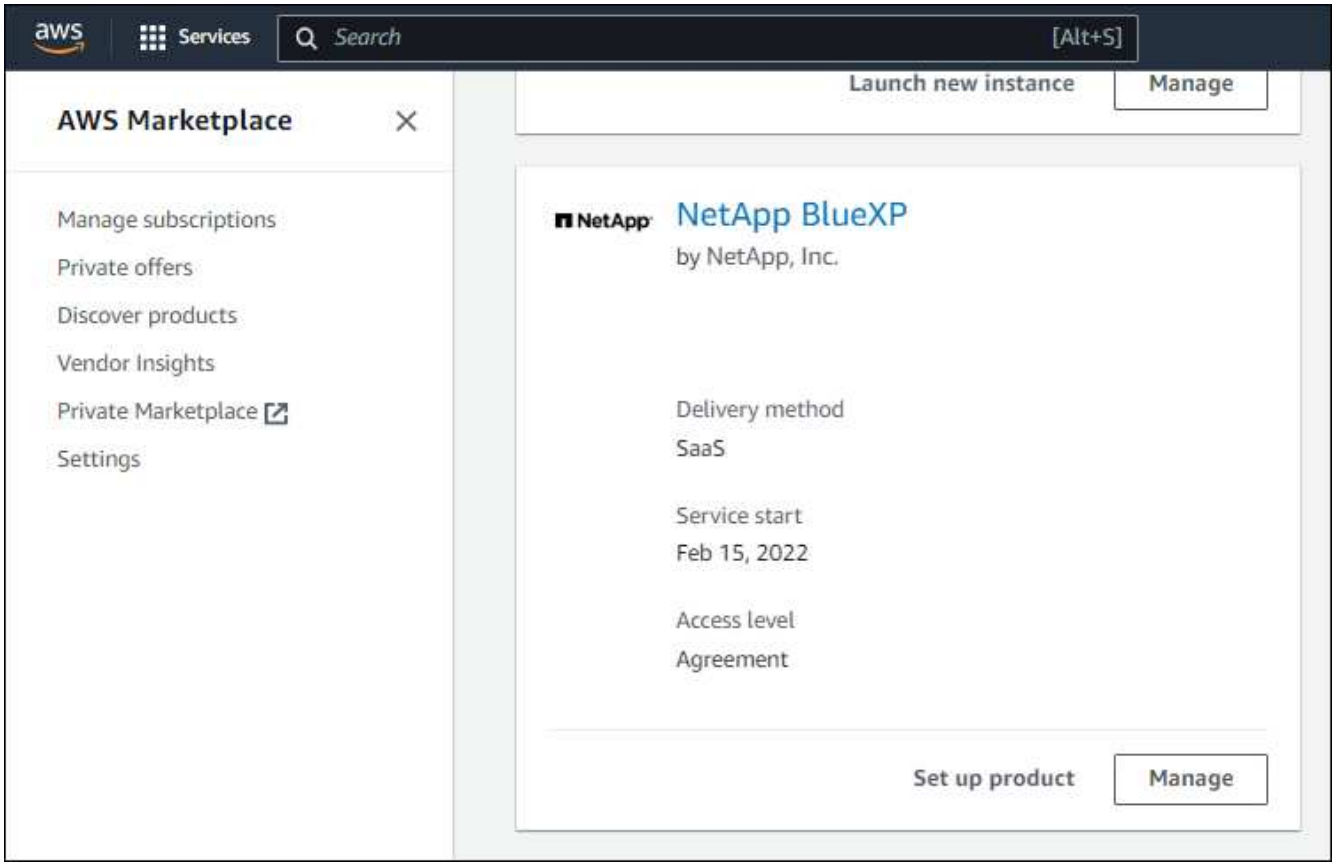
- "Saiba mais sobre os modos de implantação do Console"
- "Saiba mais sobre o gerenciamento de identidade e acesso do Console"

Siga as etapas abaixo se você assinou o NetApp Intelligent Services no AWS Marketplace, mas perdeu a etapa para associar a assinatura à sua conta.

Passos

1. Confirme se você não associou sua assinatura à sua organização do Console.
   a. No menu de navegação, selecione **Administração > Licenses and subscriptions**.
   b. Selecione **Assinaturas**.
   c. Verifique se sua assinatura não aparece.

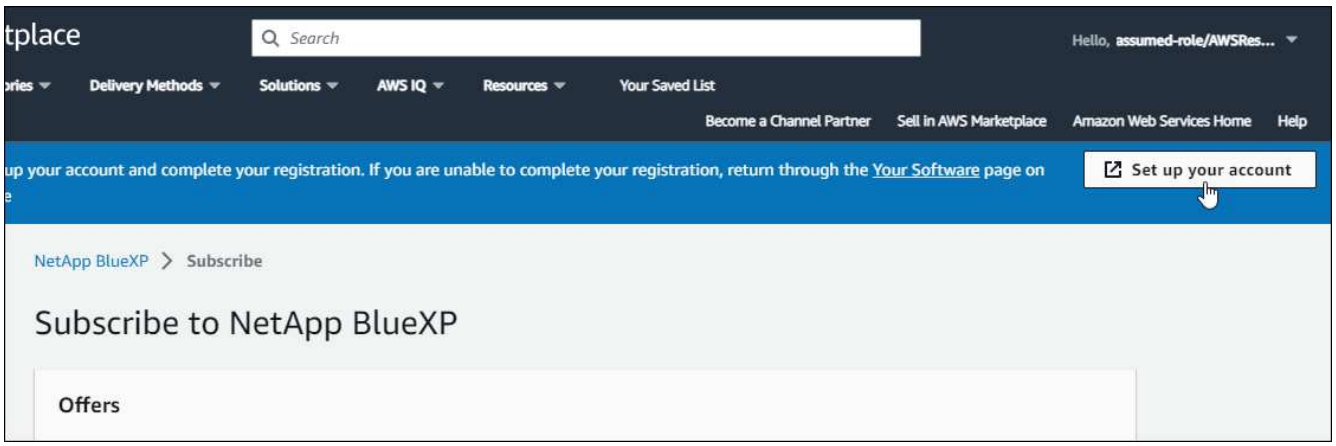
      Você verá apenas as assinaturas associadas à organização ou conta que você está visualizando no momento. Caso não veja sua assinatura, prossiga com os seguintes passos.
2. Efetue login no Console da AWS e navegue até **Assinaturas do AWS Marketplace**.
3. Encontre a assinatura.



4. Selecione **Configurar produto**.

   A página de oferta de assinatura deve ser carregada em uma nova aba ou janela do navegador.

5. Selecione **Configurar sua conta**.



   A página **Atribuição de Assinatura** no netapp.com deve ser carregada em uma nova guia ou janela do navegador.

   Observe que você pode ser solicitado a efetuar login no Console primeiro.

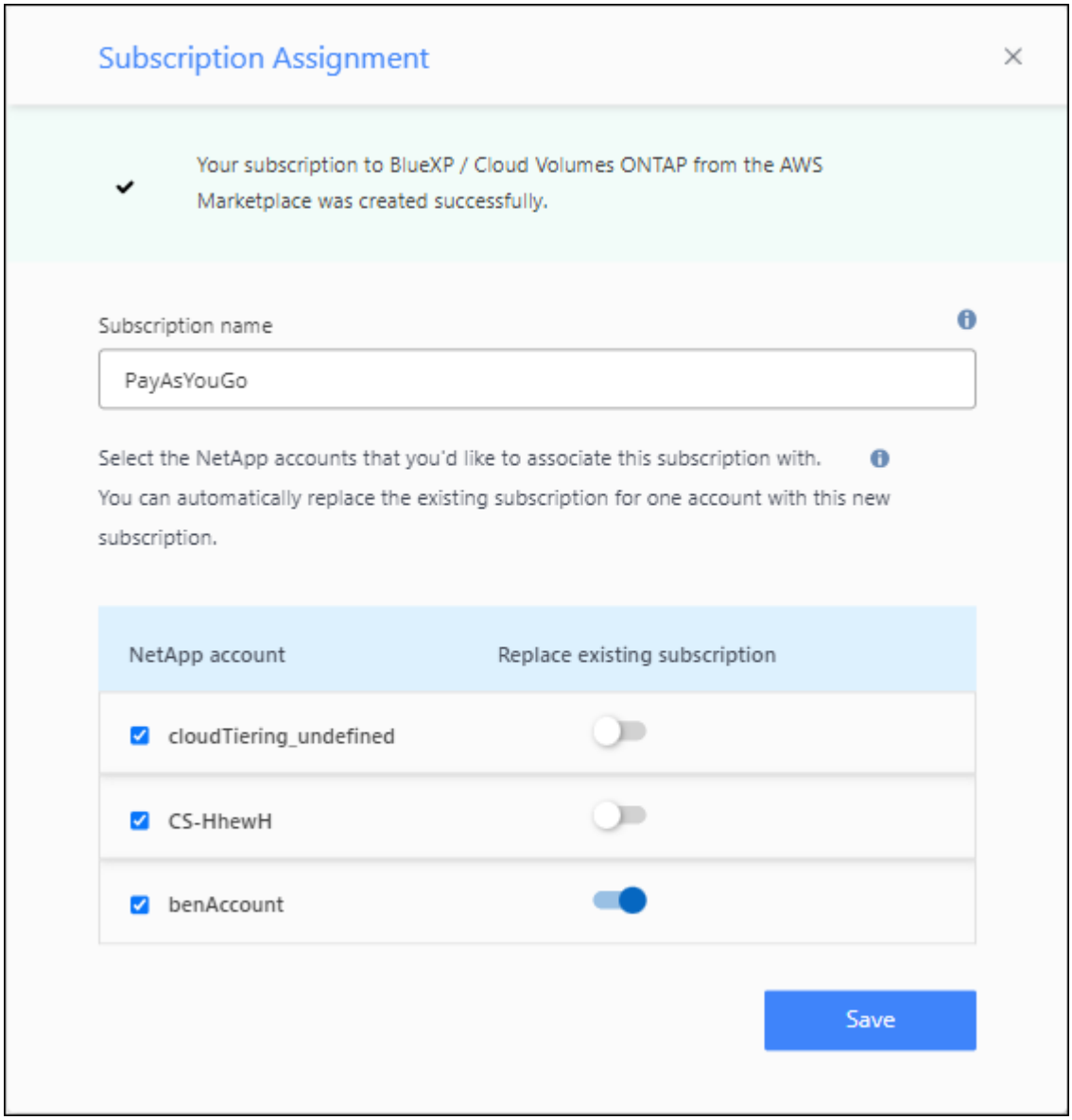
6. Na página **Atribuição de Assinatura**:

   - Selecione as organizações ou contas do Console às quais você gostaria de associar esta assinatura.

- No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização ou conta por esta nova assinatura.

  O Console substitui a assinatura existente para todas as credenciais na organização ou conta por esta nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

  Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

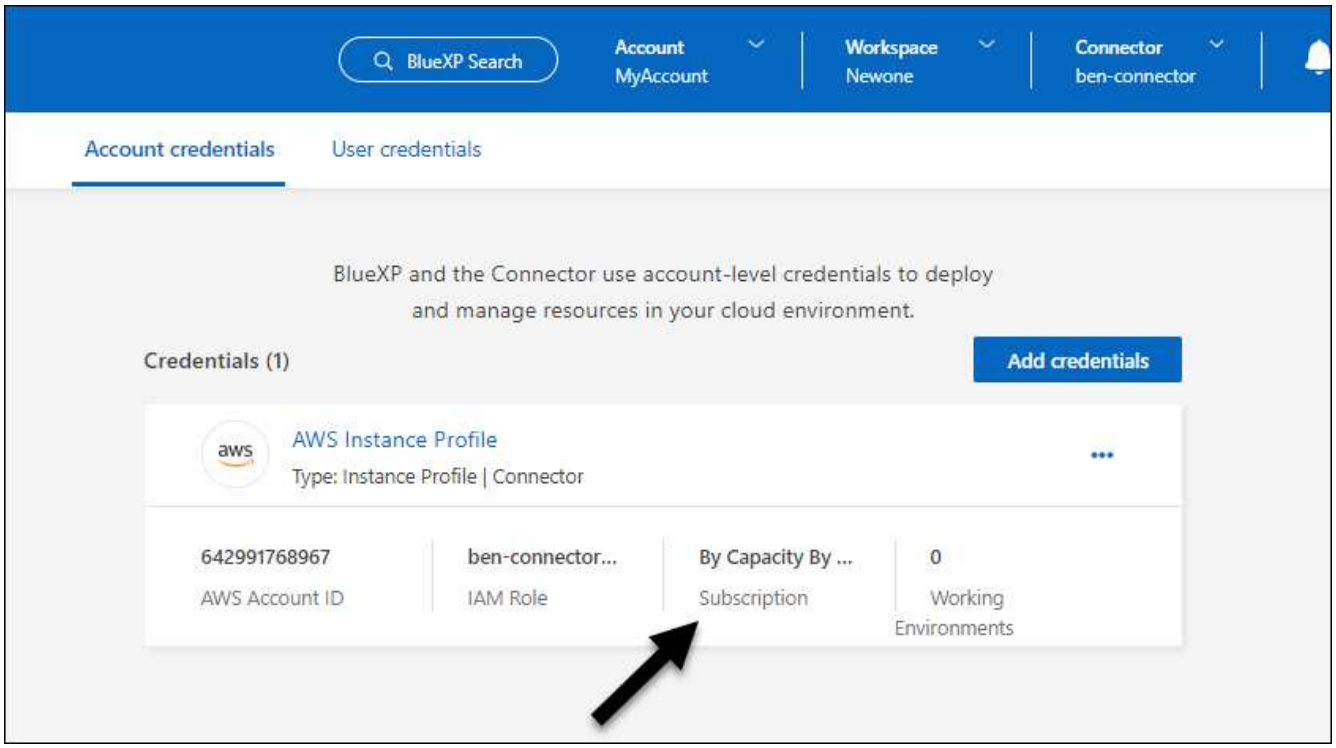


7. Confirme se a assinatura está associada à sua organização.
   a. No menu de navegação, selecione **Administração > Licença e assinaturas**.
   b. Selecione **Assinaturas**.
   c. Verifique se sua assinatura aparece.
8. Confirme se a assinatura está associada às suas credenciais da AWS.

   a. Selecione **Administração > Credenciais**.

b. Na página **Credenciais da organização**, verifique se a assinatura está associada às suas credenciais da AWS.

Aqui está um exemplo.



Editar credenciais

Edite suas credenciais da AWS alterando o tipo de conta (chaves da AWS ou função assumida), editando o nome ou atualizando as próprias credenciais (as chaves ou o ARN da função).

Não é possível editar as credenciais de um perfil de instância associado a uma instância do agente do Console ou a uma instância do Amazon FSx for ONTAP . Você só pode renomear as credenciais de uma instância do FSx for ONTAP .

Passos

1. Selecione **Administração > Credenciais**.
2. Na página **Credenciais da organização**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
3. Faça as alterações necessárias e selecione **Aplicar**.

Excluir credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las. Você só pode excluir credenciais que não estejam associadas a um sistema.

Não é possível excluir as credenciais de um perfil de instância associado a um agente do Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Na página **Credenciais da organização** ou **Credenciais da conta**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
3. Selecione **Excluir** para confirmar.

Azul

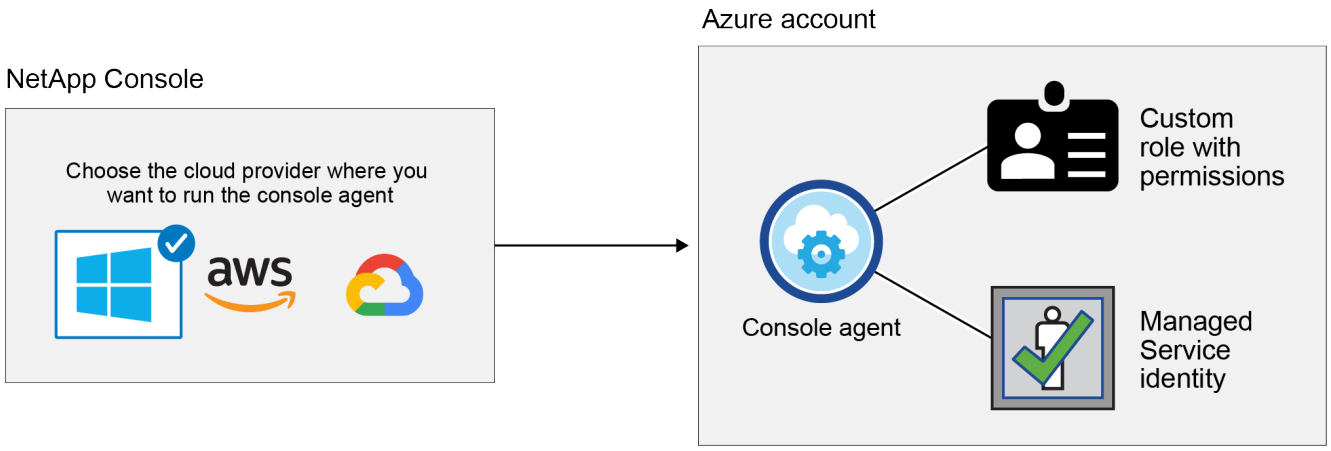
Saiba mais sobre credenciais e permissões do Azure no NetApp Console

Saiba como o NetApp Console usa credenciais do Azure para executar ações em seu nome e como essas credenciais são associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de uma ou mais assinaturas do Azure. Por exemplo, talvez você queira saber quando adicionar credenciais adicionais do Azure ao Console.

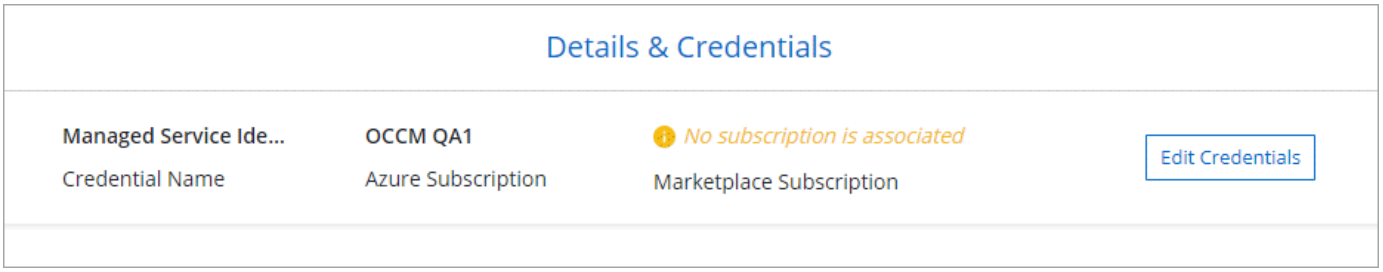
Credenciais iniciais do Azure

Ao implantar um agente do Console a partir do Console, você precisa usar uma conta do Azure ou uma entidade de serviço que tenha permissões para implantar a máquina virtual do agente do Console. As permissões necessárias estão listadas em"Política de implantação de agente para o Azure" .

Quando o Console implanta a máquina virtual do agente do Console no Azure, ele habilita um "identidade gerenciada atribuída pelo sistema" na máquina virtual, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao Console as permissões necessárias para gerenciar recursos e processos dentro dessa assinatura do Azure. "Revise como o Console usa as permissões" .



Se você criar um novo sistema para o Cloud Volumes ONTAP, o Console selecionará estas credenciais do Azure por padrão:



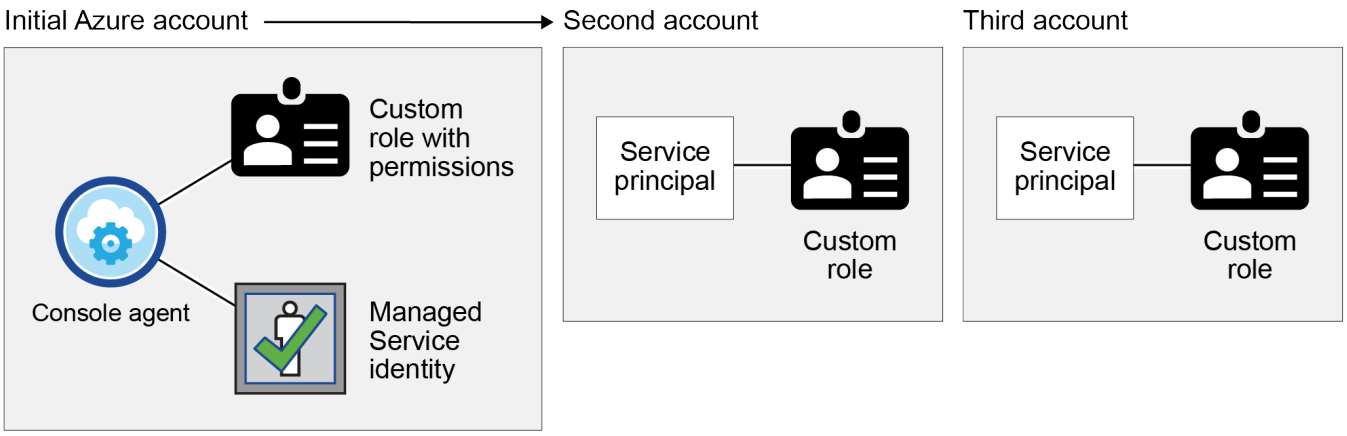
Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais do Azure ou pode adicionar credenciais adicionais.

Assinaturas adicionais do Azure para uma identidade gerenciada

A identidade gerenciada atribuída pelo sistema à VM do agente do Console está associada à assinatura na qual você iniciou o agente do Console. Se você quiser selecionar uma assinatura diferente do Azure, será necessário"associar a identidade gerenciada a essas assinaturas" .

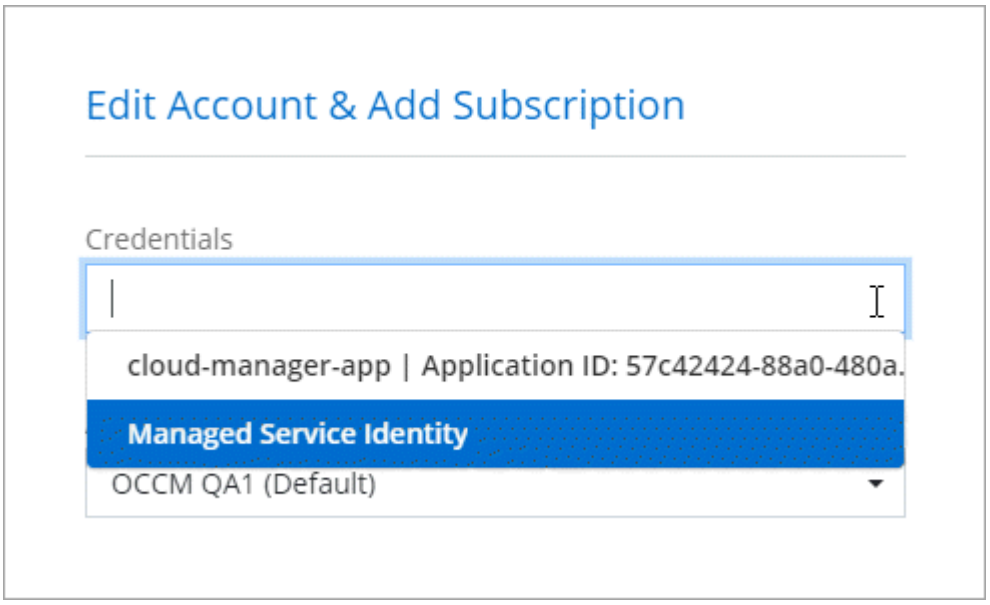
Credenciais adicionais do Azure

Se você quiser usar credenciais diferentes do Azure com o Console, deverá conceder as permissões necessárias por"criando e configurando uma entidade de serviço no Microsoft Entra ID" para cada conta do Azure. A imagem a seguir mostra duas contas adicionais, cada uma configurada com uma entidade de serviço e uma função personalizada que fornece permissões:



Você então"adicione as credenciais da conta ao Console" fornecendo detalhes sobre o principal serviço do AD.

Por exemplo, você pode alternar entre credenciais ao criar um novo sistema Cloud Volumes ONTAP :



Credenciais e assinaturas de mercado

As credenciais que você adiciona a um agente de console devem ser associadas a uma assinatura do Azure Marketplace para que você possa pagar pelo Cloud Volumes ONTAP a uma taxa por hora (PAYGO) ou pelos serviços de dados da NetApp ou por meio de um contrato anual.

"Aprenda como associar uma assinatura do Azure" .

Observe o seguinte sobre credenciais do Azure e assinaturas do marketplace:

- Você pode associar apenas uma assinatura do Azure Marketplace a um conjunto de credenciais do Azure
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Perguntas frequentes

A pergunta a seguir está relacionada a credenciais e assinaturas.

Posso alterar a assinatura do Azure Marketplace para sistemas Cloud Volumes ONTAP ?

Sim, você pode. Quando você altera a assinatura do Azure Marketplace associada a um conjunto de credenciais do Azure, todos os sistemas Cloud Volumes ONTAP existentes e novos serão cobrados pela nova assinatura.

"Aprenda como associar uma assinatura do Azure" .

Posso adicionar várias credenciais do Azure, cada uma com diferentes assinaturas de marketplace?

Todas as credenciais do Azure que pertencem à mesma assinatura do Azure serão associadas à mesma assinatura do Azure Marketplace.

Se você tiver várias credenciais do Azure que pertencem a diferentes assinaturas do Azure, essas credenciais poderão ser associadas à mesma assinatura do Azure Marketplace ou a diferentes assinaturas do marketplace.

Posso mover sistemas Cloud Volumes ONTAP existentes para uma assinatura diferente do Azure?

Não, não é possível mover os recursos do Azure associados ao seu sistema Cloud Volumes ONTAP para uma assinatura diferente do Azure.

Como as credenciais funcionam para implantações de mercado e implantações locais?

As seções acima descrevem o método de implantação recomendado para o agente do Console, que é do Console. Você também pode implantar um agente de console no Azure a partir do Azure Marketplace e instalar o software do agente de console no seu próprio host Linux.

Se você usar o Marketplace, poderá fornecer permissões atribuindo uma função personalizada à VM do agente do Console e a uma identidade gerenciada atribuída pelo sistema, ou poderá usar uma entidade de serviço do Microsoft Entra.

Para implantações locais, você não pode configurar uma identidade gerenciada para o agente do Console, mas pode fornecer permissões usando uma entidade de serviço.

Para saber como configurar permissões, consulte as seguintes páginas:

- Modo padrão
  - "Configurar permissões para uma implantação do Azure Marketplace"
  - "Configurar permissões para implantações locais"
- Modo restrito
  - "Configurar permissões para o modo restrito"

Gerenciar credenciais do Azure e assinaturas do marketplace para o NetApp Console

Adicione e gerencie credenciais do Azure para que o NetApp Console tenha as permissões necessárias para implantar e gerenciar recursos de nuvem em suas assinaturas do Azure. Se você gerencia várias assinaturas do Azure Marketplace, pode atribuir cada uma delas a diferentes credenciais do Azure na página Credenciais.

Visão geral

Há duas maneiras de adicionar assinaturas e credenciais adicionais do Azure no Console.

1. Associe assinaturas adicionais do Azure à identidade gerenciada do Azure.
2. Para implantar o Cloud Volumes ONTAP usando diferentes credenciais do Azure, conceda permissões do Azure usando uma entidade de serviço e adicione suas credenciais ao Console.

Associar assinaturas adicionais do Azure a uma identidade gerenciada

O Console permite que você escolha as credenciais do Azure e a assinatura do Azure nas quais deseja implantar o Cloud Volumes ONTAP. Você não pode selecionar uma assinatura diferente do Azure para o perfil de identidade gerenciado, a menos que associe o "identidade gerenciada" com essas assinaturas.

Sobre esta tarefa

Uma identidade gerenciada é"a conta inicial do Azure" quando você implanta um agente do Console a partir do Console. Quando você implanta o agente do Console, o Console atribui a função de Operador do Console à máquina virtual do agente do Console.

Passos

1. Efetue login no portal do Azure.
2. Abra o serviço **Assinaturas** e selecione a assinatura na qual deseja implantar o Cloud Volumes ONTAP.
3. Selecione **Controle de acesso (IAM)**.
   a. Selecione **Adicionar** > **Adicionar atribuição de função** e adicione as permissões:
      - Selecione a função **Operador de console**.

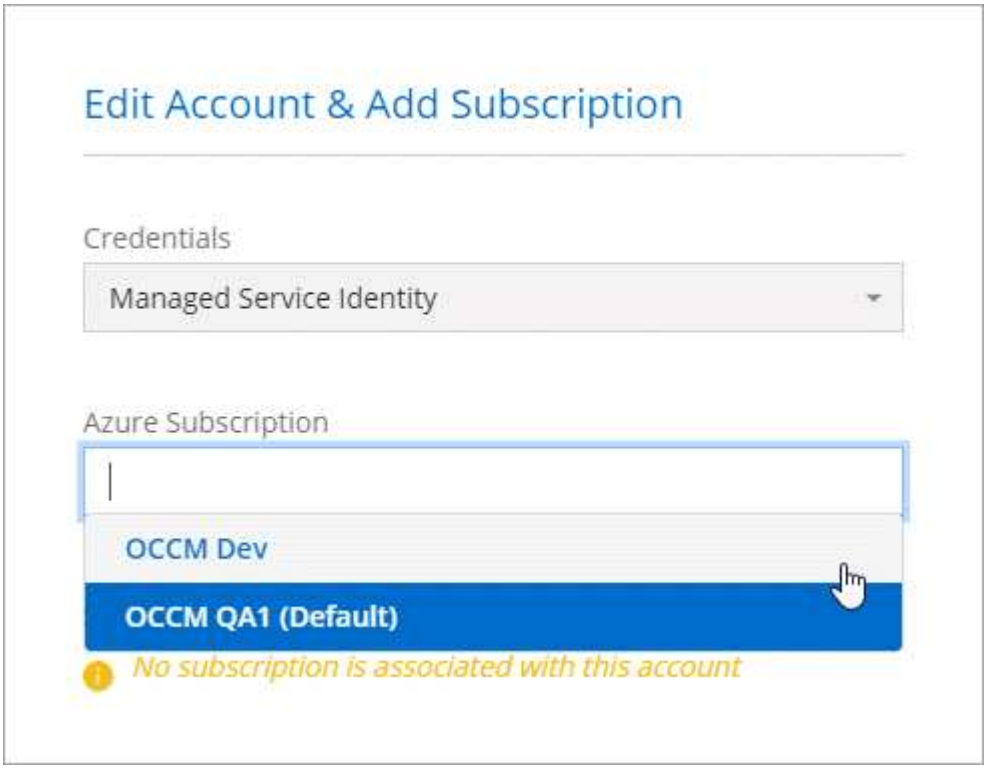
        Operador do console é o nome padrão fornecido em uma política de agente do console. Se você escolheu um nome diferente para a função, selecione esse nome.

      - Atribuir acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual uma máquina virtual do agente do Console foi criada.
      - Selecione uma máquina virtual do agente do Console.
      - Selecione **Salvar**.

4. Repita essas etapas para assinaturas adicionais.

Resultado

Ao criar um novo sistema, agora você pode selecionar entre várias assinaturas do Azure para o perfil de identidade gerenciado.



Adicionar credenciais adicionais do Azure ao NetApp Console

Quando você implanta um agente do Console a partir do Console, o Console habilita uma identidade gerenciada atribuída pelo sistema na máquina virtual que tem as permissões necessárias. O Console seleciona essas credenciais do Azure por padrão quando você cria um novo sistema para o Cloud Volumes ONTAP.

Um conjunto inicial de credenciais não será adicionado se você instalar manualmente um software de agente do Console em um sistema existente. "Saiba mais sobre credenciais e permissões do Azure" .

Se você quiser implantar o Cloud Volumes ONTAP usando credenciais *diferentes* do Azure, deverá conceder as permissões necessárias criando e configurando uma entidade de serviço no Microsoft Entra ID para cada conta do Azure. Você pode então adicionar as novas credenciais ao Console.

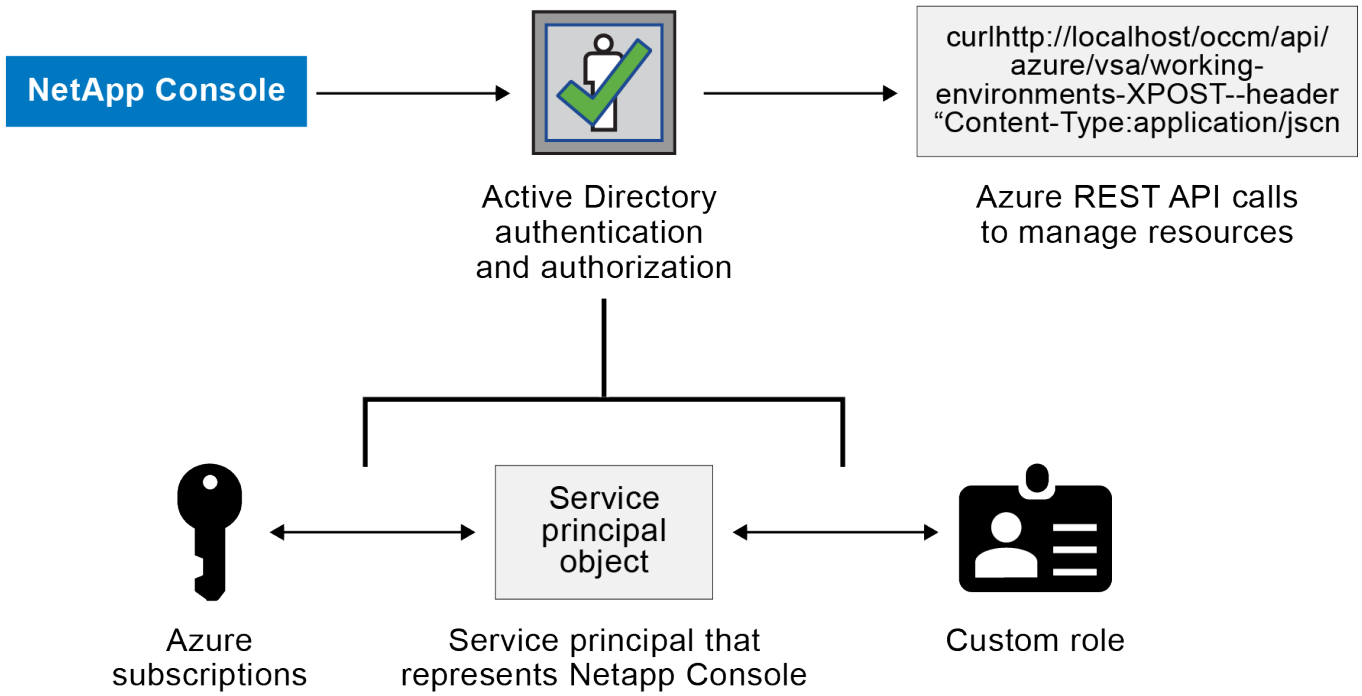
Conceder permissões do Azure usando uma entidade de serviço

O Console precisa de permissões para executar ações no Azure. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o Console.

Sobre esta tarefa

A imagem a seguir mostra como o Console obtém permissões para executar operações no Azure. Um objeto principal de serviço, que está vinculado a uma ou mais assinaturas do Azure, representa o Console no

Microsoft Entra ID e é atribuído a uma função personalizada que concede as permissões necessárias.



Passos

1. Criar um aplicativo Microsoft Entra .
2. Atribuir o aplicativo a uma função .
3. Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure .
4. Obtenha o ID do aplicativo e o ID do diretório .
5. Criar um segredo do cliente .

Criar um aplicativo Microsoft Entra

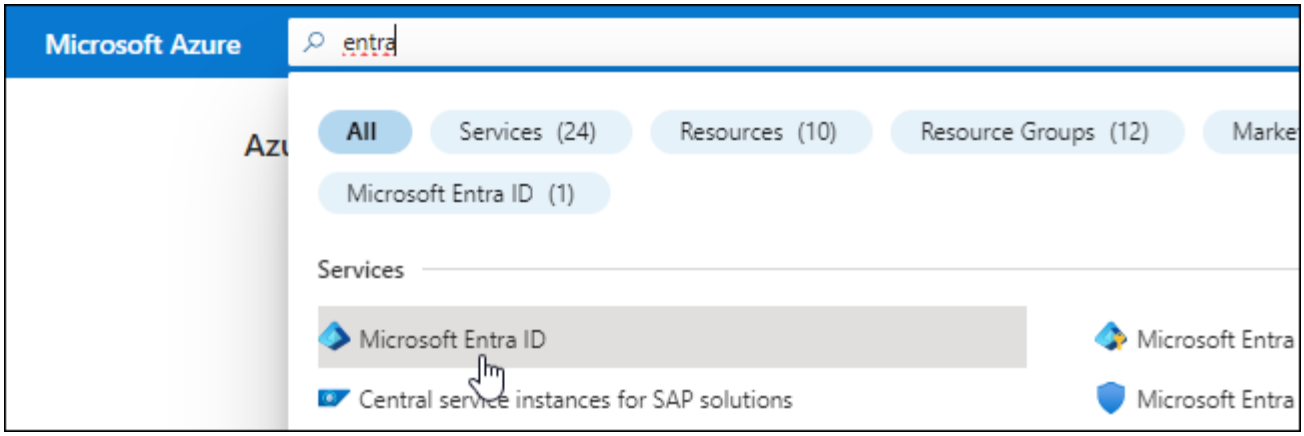
Crie um aplicativo Microsoft Entra e uma entidade de serviço que o Console possa usar para controle de acesso baseado em função.

Passos

1. Verifique se você tem permissões no Azure para criar um aplicativo do Active Directory e atribuir o aplicativo a uma função.

   Para mais detalhes, consulte "Documentação do Microsoft Azure: Permissões necessárias"

2. No portal do Azure, abra o serviço **Microsoft Entra ID**.



3. No menu, selecione **Registros de aplicativos**.
4. Selecione **Novo registro**.
5. Especifique detalhes sobre o aplicativo:
   - **Nome**: Digite um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer um funcionará com o NetApp Console).
   - **URI de redirecionamento**: Você pode deixar este campo em branco.
6. Selecione **Registrar**.

   Você criou o aplicativo AD e a entidade de serviço.

Atribuir o aplicativo a uma função

Você deve vincular a entidade de serviço a uma ou mais assinaturas do Azure e atribuir a ela a função personalizada "Operador do Console" para que o Console tenha permissões no Azure.

Passos

1. Crie uma função personalizada:

   Observe que você pode criar uma função personalizada do Azure usando o portal do Azure, o Azure PowerShell, a CLI do Azure ou a API REST. As etapas a seguir mostram como criar a função usando a CLI do Azure. Se preferir usar um método diferente, consulte "Documentação do Azure"

   a. Copie o conteúdo do"permissões de função personalizadas para o agente do Console" e salvá-los em um arquivo JSON.

   b. Modifique o arquivo JSON adicionando IDs de assinatura do Azure ao escopo atribuível.

      Você deve adicionar o ID de cada assinatura do Azure a partir da qual os usuários criarão sistemas Cloud Volumes ONTAP .

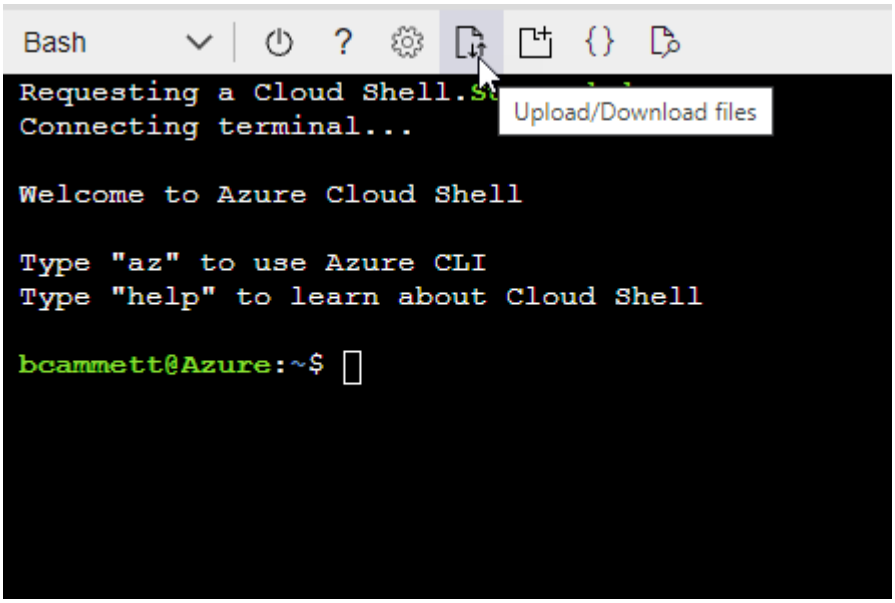
      Exemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. Use o arquivo JSON para criar uma função personalizada no Azure.

As etapas a seguir descrevem como criar a função usando o Bash no Azure Cloud Shell.

- Começar "Azure Cloud Shell" e escolha o ambiente Bash.
- Carregue o arquivo JSON.



- Use a CLI do Azure para criar a função personalizada:

```
az role definition create --role-definition agent_Policy.json
```

Agora você deve ter uma função personalizada chamada Operador do Console que pode ser atribuída à máquina virtual do agente do Console.

2. Atribuir o aplicativo à função:

a. No portal do Azure, abra o serviço **Assinaturas**.

b. Selecione a assinatura.

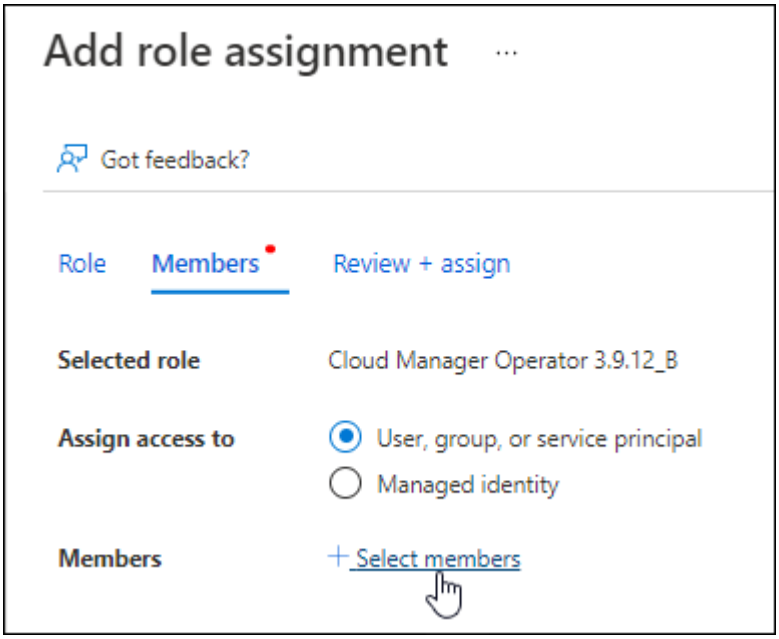
c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.

d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.

e. Na aba **Membros**, complete os seguintes passos:

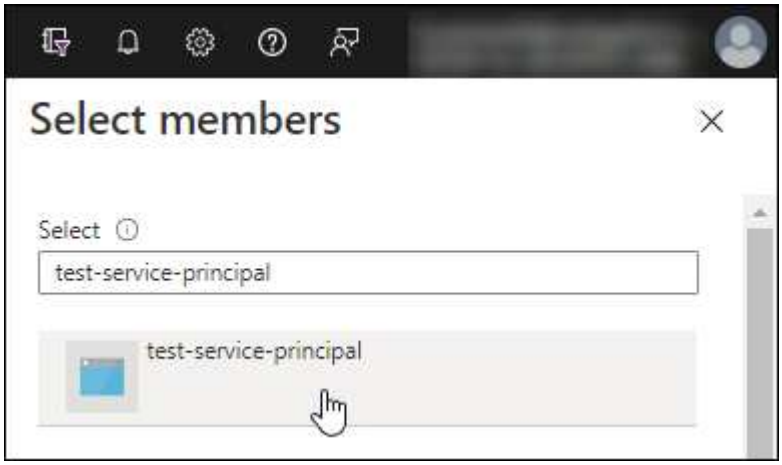
- Mantenha **Usuário, grupo ou entidade de serviço** selecionado.

- Selecione **Selecionar membros**.



- Pesquise o nome do aplicativo.

  Aqui está um exemplo:



- Selecione o aplicativo e selecione **Selecionar**.
- Selecione **Avançar**.

f. Selecione **Revisar + atribuir**.

   O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

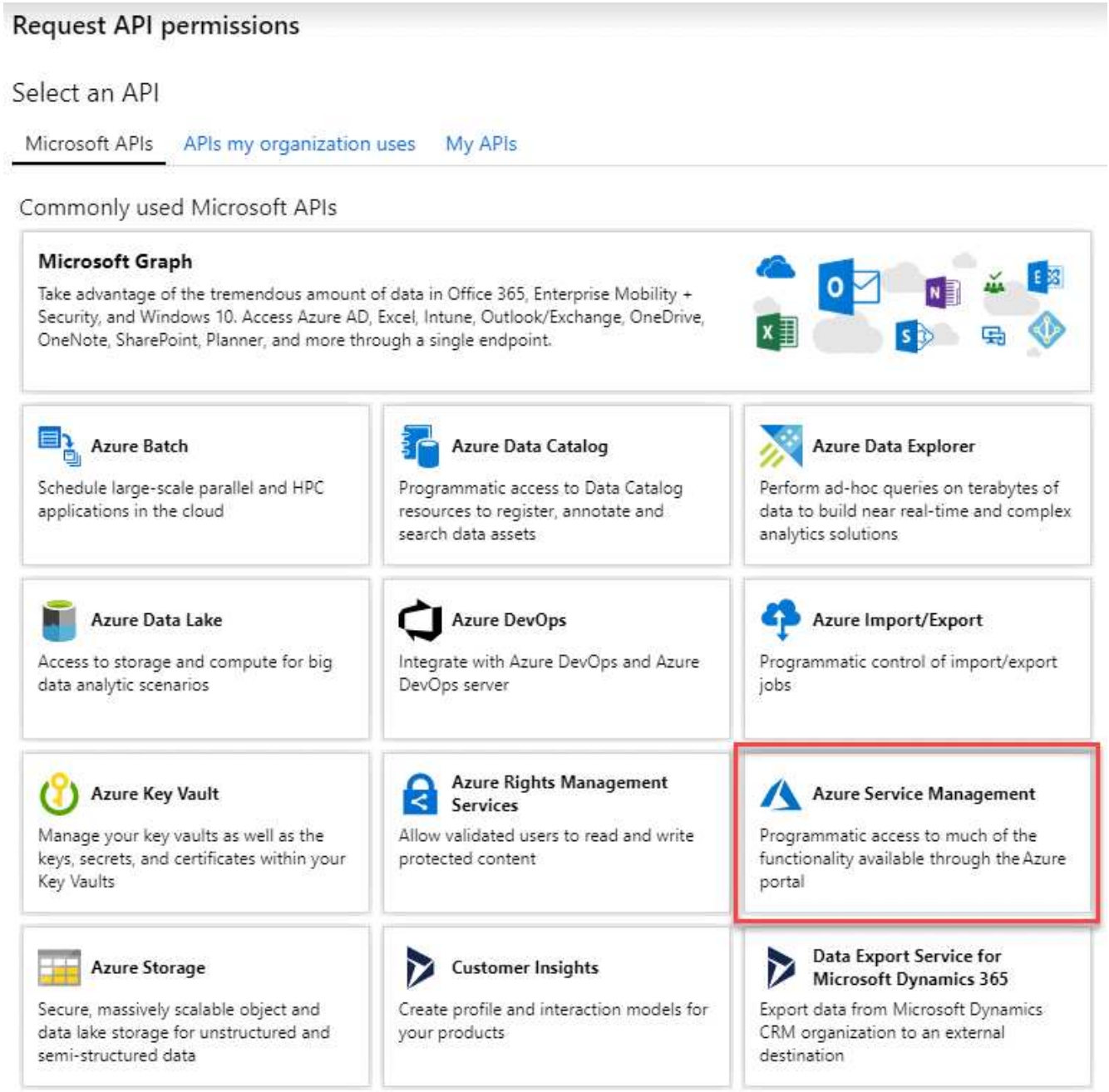
Se você quiser implantar o Cloud Volumes ONTAP de várias assinaturas do Azure, será necessário vincular a entidade de serviço a cada uma dessas assinaturas. No NetApp Console, você pode selecionar a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

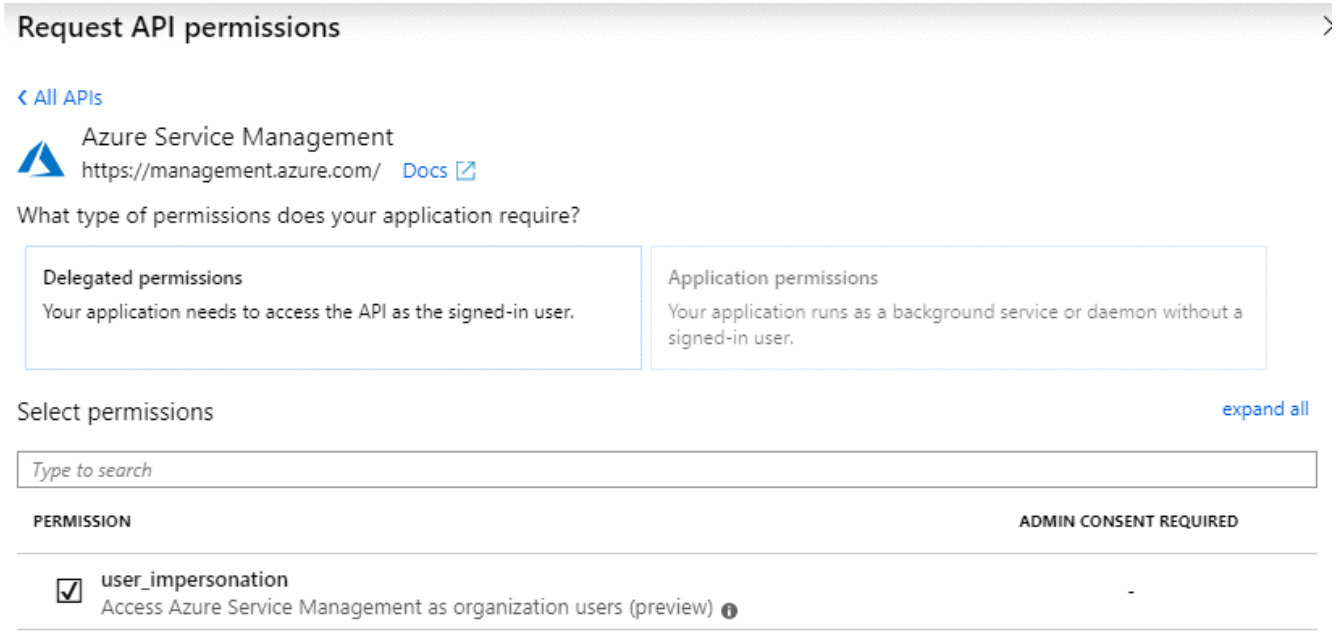
Você deve atribuir permissões "API de Gerenciamento de Serviços do Windows Azure" à entidade de serviço.

Passos

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Selecione **Permissões de API > Adicionar uma permissão**.
3. Em **APIs da Microsoft**, selecione **Azure Service Management**.



4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.

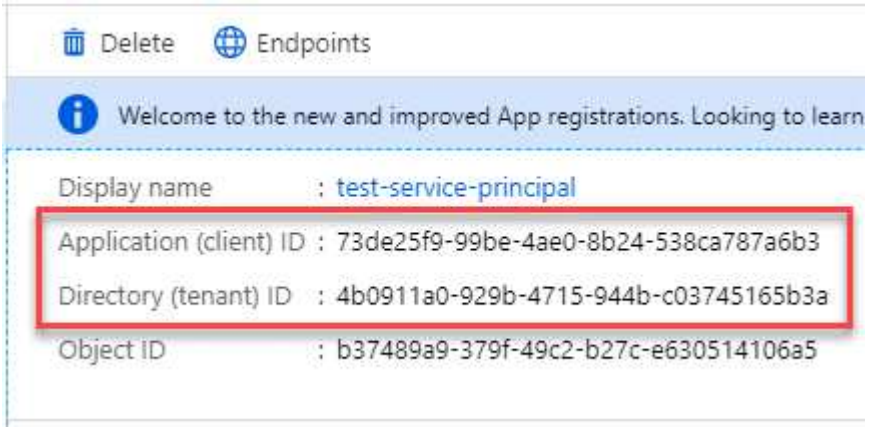


Obtenha o ID do aplicativo e o ID do diretório

Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Passos

1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Ao adicionar a conta do Azure ao Console, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Console usa os IDs para fazer login programaticamente.

Criar um segredo do cliente

Crie um segredo do cliente e forneça seu valor ao Console para autenticação com o Microsoft Entra ID.

Passos

1. Abra o serviço **Microsoft Entra ID**.

2. Selecione **Registros de aplicativos** e selecione seu aplicativo.
3. Selecione **Certificados e segredos > Novo segredo do cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Selecione **Adicionar**.
6. Copie o valor do segredo do cliente.

Resultado

Seu principal serviço agora está configurado e você deve ter copiado o ID do aplicativo (cliente), o ID do diretório (locatário) e o valor do segredo do cliente. Você precisa inserir essas informações no Console ao adicionar uma conta do Azure.

Adicione as credenciais ao Console

Depois de fornecer uma conta do Azure com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Console. Concluir esta etapa permite que você inicie o Cloud Volumes ONTAP usando diferentes credenciais do Azure.

Antes de começar

Se você acabou de criar essas credenciais no seu provedor de nuvem, pode levar alguns minutos até que elas estejam disponíveis para uso. Aguarde alguns minutos antes de adicionar as credenciais ao Console.

Antes de começar

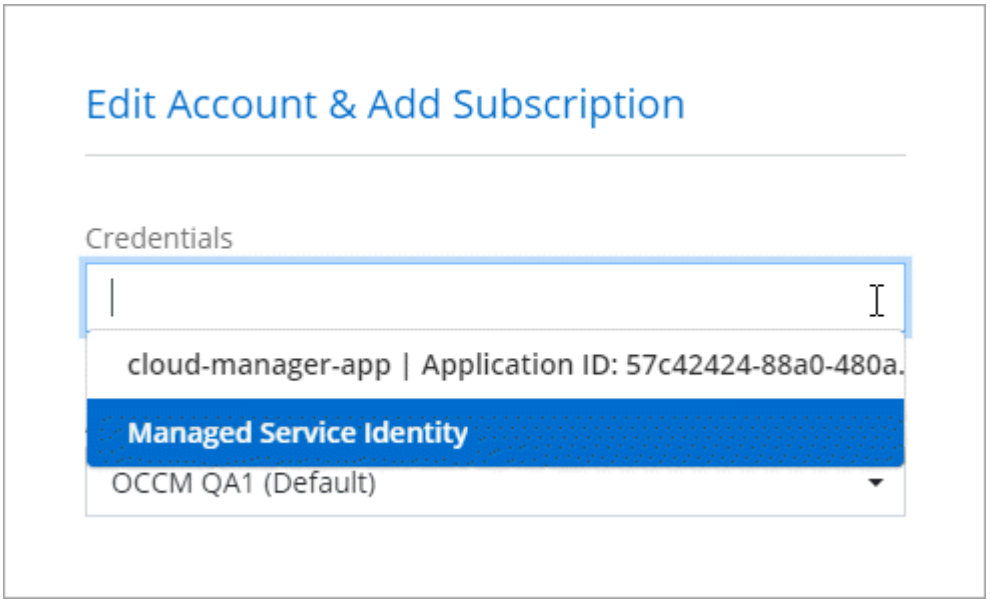
Você precisa criar um agente do Console antes de poder alterar as configurações do Console. "Aprenda a criar um agente de console" .

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Adicionar credenciais** e siga as etapas do assistente.
   a. **Localização das credenciais**: Selecione **Microsoft Azure > Agente**.
   b. **Definir credenciais**: insira informações sobre a entidade de serviço do Microsoft Entra que concede as permissões necessárias:
      - ID do aplicativo (cliente)
      - ID do diretório (inquilino)
      - Segredo do cliente
   c. **Assinatura do Marketplace**: Associe uma assinatura do Marketplace a essas credenciais assinando agora ou selecionando uma assinatura existente.
   d. **Revisar**: Confirme os detalhes sobre as novas credenciais e selecione **Adicionar**.

Resultado

Você pode alternar para um conjunto diferente de credenciais na página Detalhes e Credenciais "ao adicionar um sistema ao Console"



Gerenciar credenciais existentes

Gerencie as credenciais do Azure que você já adicionou ao Console associando uma assinatura do Marketplace, editando credenciais e excluindo-as.

Associar uma assinatura do Azure Marketplace às credenciais

Depois de adicionar suas credenciais do Azure ao Console, você pode associar uma assinatura do Azure Marketplace a essas credenciais. Você pode usar a assinatura para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e acessar os serviços de dados da NetApp .

Há dois cenários nos quais você pode associar uma assinatura do Azure Marketplace depois de já ter adicionado as credenciais ao Console:

- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Console.
- Você deseja alterar a assinatura do Azure Marketplace associada às credenciais do Azure.

  A substituição da assinatura atual do marketplace a atualiza para sistemas Cloud Volumes ONTAP existentes e novos.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais associadas a um agente do Console e selecione **Configurar assinatura**.

   Você deve selecionar credenciais associadas a um agente do Console. Não é possível associar uma assinatura do marketplace a credenciais associadas ao NetApp Console.

4. Para associar as credenciais a uma assinatura existente, selecione a assinatura na lista suspensa e

selecione **Configurar**.

5. Para associar as credenciais a uma nova assinatura, selecione **Adicionar Assinatura > Continuar** e siga as etapas no Azure Marketplace:

   a. Se solicitado, faça login na sua conta do Azure.

   b. Selecione **Inscrever-se**.

   c. Preencha o formulário e selecione **Inscrever-se**.

   d. Após a conclusão do processo de assinatura, selecione **Configurar conta agora**.

      Você será redirecionado para o NetApp Console.

   e. Na página **Atribuição de Assinatura**:

      - Selecione as organizações ou contas do Console às quais você gostaria de associar esta assinatura.
      - No campo **Substituir assinatura existente**, escolha se deseja substituir automaticamente a assinatura existente de uma organização ou conta por esta nova assinatura.

        O Console substitui a assinatura existente para todas as credenciais na organização ou conta por esta nova assinatura. Se um conjunto de credenciais nunca foi associado a uma assinatura, essa nova assinatura não será associada a essas credenciais.

   Para todas as outras organizações ou contas, você precisará associar manualmente a assinatura repetindo essas etapas.

   ◦ Selecione **Salvar**.

Editar credenciais

Edite suas credenciais do Azure no Console. Por exemplo, você pode atualizar o segredo do cliente se um novo segredo tiver sido criado para o aplicativo principal do serviço.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Selecione o menu de ação para um conjunto de credenciais e, em seguida, selecione **Editar credenciais**.
4. Faça as alterações necessárias e selecione **Aplicar**.

Excluir credenciais

Se você não precisar mais de um conjunto de credenciais, poderá excluí-las. Você só pode excluir credenciais que não estejam associadas a um sistema.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais da organização**.
3. Na página **Credenciais da organização**, selecione o menu de ações para um conjunto de credenciais e, em seguida, selecione **Excluir credenciais**.
4. Selecione **Excluir** para confirmar.

Google Cloud

Saiba mais sobre projetos e permissões do Google Cloud

Saiba como o NetApp Console usa as credenciais do Google Cloud para executar ações em seu nome e como essas credenciais são associadas às assinaturas do marketplace. Entender esses detalhes pode ser útil ao gerenciar as credenciais de um ou mais projetos do Google Cloud. Por exemplo, talvez você queira saber mais sobre a conta de serviço associada à VM do agente do Console.

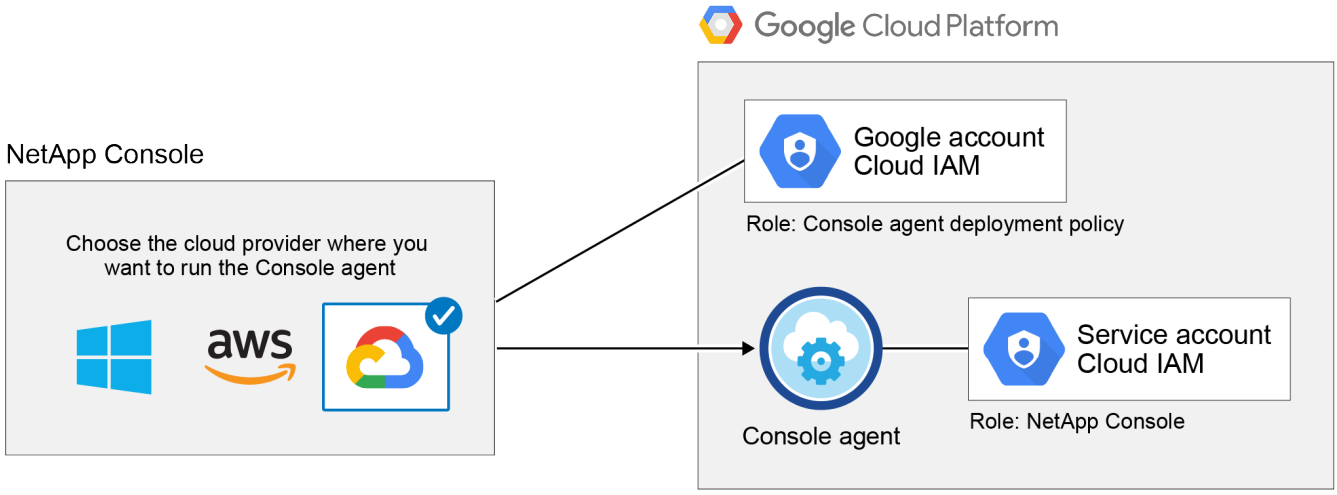
Projeto e permissões para o NetApp Console

Antes de usar o Console para gerenciar recursos no seu projeto do Google Cloud, você deve primeiro implantar um agente do Console. O agente não pode estar sendo executado em suas instalações ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de você implantar um agente do Console diretamente do Console:

1. Você precisa implantar um agente do Console usando uma conta do Google que tenha permissões para iniciar o agente do Console a partir do Console.
2. Ao implantar o agente do Console, você será solicitado a selecionar um "conta de serviço" para o agente O Console obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP , gerenciar backups usando o backup e a recuperação do NetApp e muito mais. As permissões são fornecidas anexando uma função personalizada à conta de serviço.

A imagem a seguir descreve os requisitos de permissão descritos nos números 1 e 2 acima:



Para saber como configurar permissões, consulte as seguintes páginas:

- "Configurar permissões do Google Cloud para o modo padrão"
- "Configurar permissões para o modo restrito"

Credenciais e assinaturas de mercado

Quando você implanta um agente do Console no Google Cloud, o Console cria um conjunto padrão de credenciais para a conta de serviço do Google Cloud no projeto em que o agente do Console reside. Essas

credenciais devem estar associadas a uma assinatura do Google Cloud Marketplace para que você possa pagar pelos serviços de dados do Cloud Volumes ONTAP e do NetApp .

"Aprenda como associar uma assinatura do Google Cloud Marketplace" .

Observe o seguinte sobre credenciais do Google Cloud e assinaturas do marketplace:

- Apenas um conjunto de credenciais do Google Cloud pode ser associado a um agente do Console
- Você pode associar apenas uma assinatura do Google Cloud Marketplace às credenciais
- Você pode substituir uma assinatura de mercado existente por uma nova assinatura

Projeto para Cloud Volumes ONTAP

O Cloud Volumes ONTAP pode residir no mesmo projeto que o agente do Console ou em um projeto diferente. Para implantar o Cloud Volumes ONTAP em um projeto diferente, você precisa primeiro adicionar a conta de serviço e a função do agente do Console a esse projeto.

- "Aprenda a configurar a conta de serviço"
- "Aprenda a implantar o Cloud Volumes ONTAP no Google Cloud e selecione um projeto"

Gerenciar permissões do agente do Console para implantações do Google Cloud

Ocasionalmente, a NetApp atualiza as permissões necessárias para a conta de serviço usada pelo agente do Console quando ele é implantado no Google Cloud.

"Verifique a lista de permissões do Google necessárias".

Use o Console do Google Cloud para atualizar a função do IAM atribuída à conta de serviço para corresponder ao novo conjunto de permissões.

"Documentação do Google Cloud: Editar uma função personalizada"

Gerenciamento de identidade e acesso

Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console

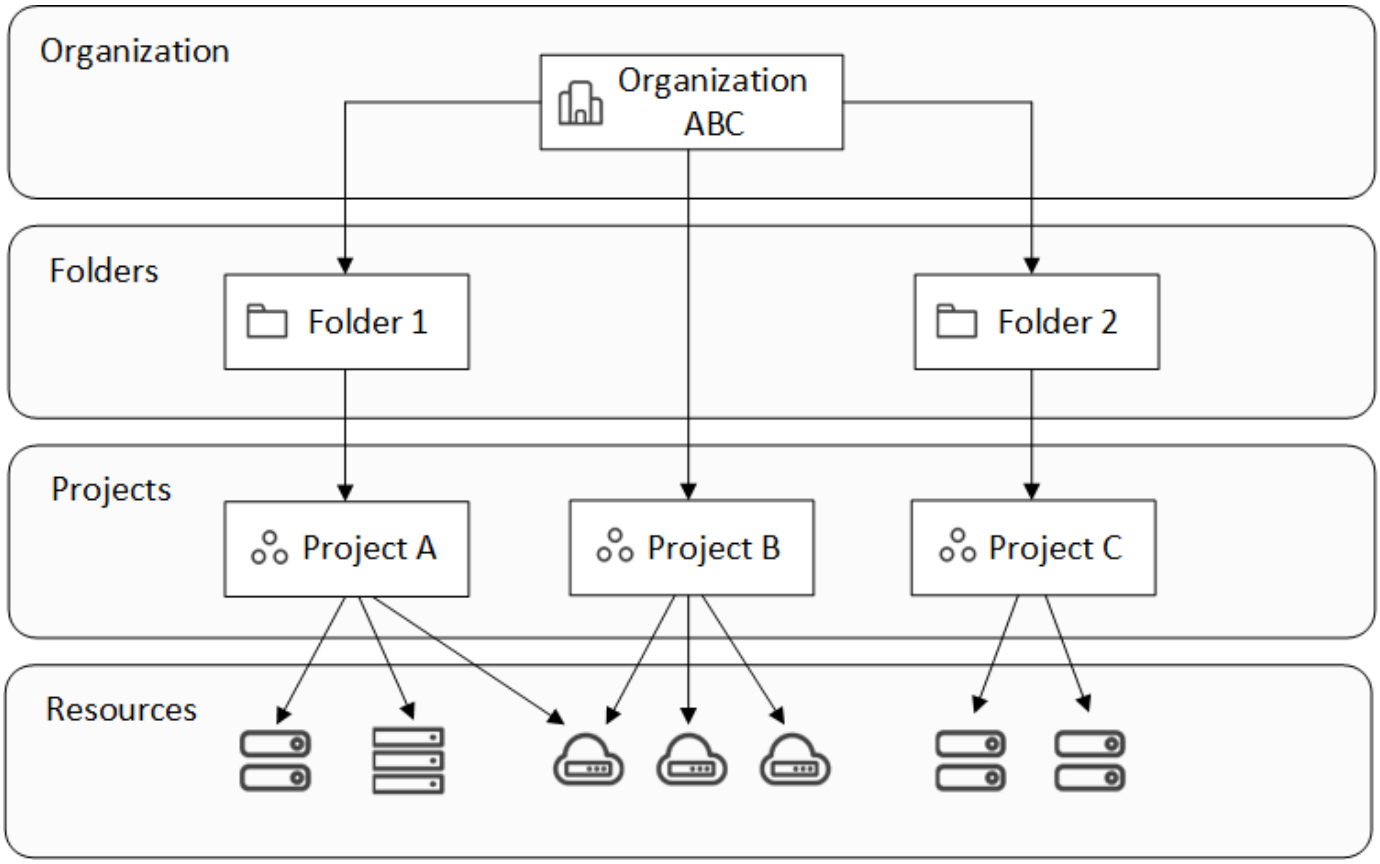
Utilize o Gerenciamento de Identidade e Acesso (IAM) do NetApp Console para organizar seus recursos NetApp e controlar o acesso de acordo com a estrutura da sua empresa — por local, departamento ou projeto.

Os recursos são organizados hierarquicamente: a organização está no topo, seguida pelas pastas (que podem conter outras pastas ou projetos) e, em seguida, pelos projetos, que contêm sistemas de armazenamento, cargas de trabalho e agentes.

Atribua permissões de controle de acesso baseado em funções (RBAC) aos membros no nível da organização, pasta ou projeto para garantir que os usuários tenham o acesso apropriado aos recursos.

Você precisa ter as funções de *Superadministrador*, *Administrador da organização* ou *Administrador de pasta ou projeto* para gerenciar o IAM no NetApp Console.

A imagem a seguir ilustra essa hierarquia em um nível básico.



]

Componentes de gerenciamento de identidade e acesso

No NetApp Console, você organiza seus recursos de armazenamento usando três componentes principais: componentes organizacionais, componentes de recursos e componentes de acesso do usuário.

Projetos e pastas dentro da sua organização

Dentro da sua estrutura IAM, você trabalha com três componentes organizacionais: organizações, projetos e pastas. Você pode conceder acesso aos usuários atribuindo-lhes funções em qualquer um desses níveis.

Organização

Uma *organização* é o nível superior do sistema Console IAM e normalmente representa sua empresa. Sua organização consiste em pastas, projetos, membros, funções e recursos. Os agentes estão associados a projetos específicos na organização.

Projetos

Um *projeto* é usado para fornecer acesso a um recurso de armazenamento. Você precisa atribuir recursos ao projeto antes que alguém possa acessá-los. Você pode atribuir vários recursos a um único projeto e também pode ter vários projetos. Em seguida, você atribui permissões de usuário ao projeto para dar a eles acesso aos recursos contidos nele.

Por exemplo, você pode associar um sistema ONTAP local a um único projeto ou a todos os projetos da sua organização, dependendo das suas necessidades.

"Aprenda como adicionar projetos à sua organização."

Pastas

Agrupe projetos relacionados em *pastas* para organizá-los por local, unidade ou negócio. Não é possível associar recursos diretamente a pastas, mas atribuir uma função a um usuário no nível da pasta dá a ele acesso a todos os projetos dessa pasta.

"Aprenda como adicionar pastas à sua organização."

Recursos

Os recursos incluem sistemas de armazenamento, assinaturas do Keystone , bem como agentes do Console.

+ Você precisa associar um recurso a um projeto antes que alguém possa acessá-lo.

+

Por exemplo, você pode associar um sistema Cloud Volumes ONTAP a um projeto ou a todos os projetos da sua organização. A forma como você associa um recurso depende das necessidades da sua organização.

+

"Aprenda como associar recursos a projetos."

Sistemas de armazenamento e assinaturas Keystone

Os sistemas de armazenamento são os principais recursos que você gerencia no NetApp Console. O NetApp Console oferece suporte ao gerenciamento de sistemas de armazenamento locais e em nuvem. Você precisa adicionar um sistema de armazenamento a um projeto antes que alguém possa acessá-lo.

Os sistemas de armazenamento são associados automaticamente ao projeto em que são adicionados, mas você também pode associá-los a outros projetos ou pastas na página **Recursos**.

As assinaturas do Keystone também são recursos que você pode associar a projetos para conceder aos usuários acesso à assinatura no NetApp Console.

Agentes de console

Os administradores da organização criam agentes do Console para gerenciar sistemas de armazenamento e habilitar os serviços de dados da NetApp . Inicialmente, os agentes são vinculados ao projeto em que são criados, mas os administradores podem adicioná-los a outros projetos ou pastas na página Agentes.

Associar um agente a um projeto permite o gerenciamento de recursos nesse projeto, enquanto associar um agente a uma pasta permite que os administradores da pasta ou do projeto decidam quais projetos devem usar o agente. Os agentes devem estar vinculados a projetos específicos para fornecerem capacidades de gestão.

"Aprenda como associar agentes a projetos."

Membros e funções

Membros

Os membros da sua organização são contas de usuário ou contas de serviço. Uma conta de serviço normalmente é usada por um aplicativo para concluir tarefas específicas sem intervenção humana.

Você precisa adicionar membros à sua organização depois que eles se inscreverem no NetApp Console. Depois de adicionados, você pode atribuir funções a eles para fornecer acesso a recursos. Você pode adicionar contas de serviço manualmente no Console ou automatizar a criação e o gerenciamento delas por meio da API IAM do NetApp Console .

"Aprenda como adicionar membros à sua organização."

Funções de acesso

O Console fornece funções de acesso que você pode atribuir aos membros da sua organização.

Ao associar um membro a uma função, você pode conceder essa função para toda a organização, uma pasta específica ou um projeto específico. A função que você selecionar concede permissões a um membro para acessar os recursos na parte selecionada da hierarquia.

O NetApp Console oferece funções granulares que seguem o princípio do "privilégio mínimo", o que significa que as funções de acesso são projetadas para conceder aos usuários acesso somente ao que eles precisam.

Isso significa que os usuários podem ter várias funções atribuídas a eles à medida que suas responsabilidades aumentam.

"Saiba mais sobre funções de acesso" .

Exemplos de estratégia IAM

Estratégia para pequenas organizações

Para organizações com menos de 50 usuários e gerenciamento de armazenamento centralizado, considere uma abordagem simplificada usando as funções de Superadministrador e Supervisualizador.

Exemplo: ABC Corporation (equipe de 5 pessoas)

- **Estrutura:** Organização única com 3 projetos (Produção, Desenvolvimento, Backup)
- **Funções:**
  - 2 membros seniores: Função de **Superadministrador** com acesso administrativo completo.
  - 3 membros da equipe: Função de **Supervisor** para monitoramento sem direitos de modificação.
- **Estratégia de agente:** Um único agente associado a todos os projetos para acesso a recursos compartilhados.
- **Benefícios:** Administração simplificada, complexidade de funções reduzida, adequado para equipes que necessitam de amplo acesso.

Estratégia empresarial multirregional

Para grandes organizações com operações regionais e equipes especializadas, implemente uma abordagem hierárquica com pastas representando limites geográficos ou de unidades de negócios.

Exemplo: Corporação XYZ (empresa multinacional)

- **Estrutura:** Organização > Pastas regionais (América do Norte, Europa, Ásia-Pacífico) > Pastas de projetos por região
- **Funções da plataforma:**
  - 1 **Administração organizacional**: Supervisão global e gestão de políticas
  - 3 **Administradores de pastas ou projetos**: Controle regional (um por região)
  - 1 **Administração da Federação**: Integração do provedor de identidade corporativa
- **Funções de armazenamento por região:**

    - 9 **Administrador de armazenamento**: Descobrir e gerenciar sistemas de armazenamento em regiões atribuídas.
    - 2 **Visualizador de armazenamento**: Monitore os recursos de armazenamento em diferentes regiões.
    - 1 **Especialista em integridade do sistema**: Gerencie a integridade do armazenamento sem modificações no sistema
- **Funções do serviço de dados:**
    - **Administrador de Backup e Recuperação**: Cobrança por projeto, com base nas responsabilidades de backup.
    - **Administrador de Resiliência a Ransomware**: Monitoramento da equipe de segurança em todos os projetos
- **Estratégia de agentes:** Agentes regionais associados a projetos geográficos relevantes.
- **Benefícios:** Segurança reforçada por meio da segregação de funções, autonomia regional e conformidade com as regulamentações locais.

Estratégia de especialização departamental

Para organizações com equipes especializadas que necessitam de acesso a serviços de dados específicos, utilize atribuições de funções direcionadas com base nas responsabilidades funcionais.

Exemplo: TechCorp (empresa de tecnologia de médio porte)

- **Estrutura:** Organização > Pastas de departamento (TI, Segurança, Desenvolvimento) > Recursos específicos do projeto
- **Funções especializadas:**
    - Equipe de segurança: funções de **Administrador de Resiliência a Ransomware** e **Visualizador de Classificações**.
    - Equipe de backup: **Superadministrador de backup e recuperação** para operações de backup abrangentes.
    - Equipe de desenvolvimento: **Administrador de armazenamento** para gerenciamento de ambiente de teste
    - Equipe de Compliance: **Analista de suporte operacional** para monitoramento e gerenciamento de casos de suporte.
- **Estratégia de agentes:** Agentes vinculados a projetos departamentais com base na propriedade dos recursos.
- **Benefícios:** Controle de acesso personalizado, maior eficiência operacional e responsabilidade clara por tarefas especializadas.

Próximos passos com o IAM no NetApp Console

- "Introdução ao IAM no NetApp Console"
- "Monitorar ou auditar a atividade do IAM"
- "Saiba mais sobre a API para NetApp Console IAM"

Comece a usar identidade e acesso no NetApp Console

Ao se inscrever no NetApp Console, você será solicitado a criar uma nova organização.

A organização inclui um membro (um administrador da organização) e um projeto padrão. Para configurar o gerenciamento de identidade e acesso (IAM) para atender às suas necessidades comerciais, você precisará personalizar a hierarquia da sua organização, adicionar membros adicionais, adicionar ou descobrir recursos e associar esses recursos à sua hierarquia.

Você precisa das permissões de **Administrador da organização** ou **Superadministrador** para gerenciar a identidade e o acesso da sua organização. Com as permissões de **Administrador de pasta ou projeto**, você só pode gerenciar as pastas e os projetos aos quais tem acesso.

Siga estas etapas para configurar uma nova organização. A ordem pode variar de acordo com as necessidades da sua organização.

1 Edite o projeto padrão ou adicione-o à hierarquia da sua organização

Use o projeto padrão ou crie projetos e pastas adicionais que correspondam à hierarquia da sua empresa.

"Aprenda a organizar seus recursos com pastas e projetos" .

2 Associe membros à sua organização

Após os usuários se inscreverem no NetApp Console, você deve adicioná-los explicitamente à sua organização do Console. Você também tem a opção de adicionar contas de serviço à sua organização.

"Aprenda a gerenciar membros e suas permissões" .

3 Adicionar ou descobrir recursos

Adicione ou descubra recursos (sistemas) ao Console. Os membros da organização gerenciam sistemas de dentro de um projeto.

Aprenda como criar ou descobrir recursos:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemas da série E"
- "Clusters ONTAP locais"
- "StorageGRID"

4 Associar recursos a projetos adicionais

Adicionar ou descobrir um sistema no Console associa automaticamente o recurso ao projeto selecionado no momento. Para disponibilizar esse recurso para outro projeto na sua organização, associe-o ao respectivo projeto. Se um agente do Console for usado para gerenciar o recurso, associe o agente do Console ao respectivo projeto.

- "Aprenda a gerenciar a hierarquia de recursos da sua organização" .

- "Aprenda como associar um agente do Console a uma pasta ou projeto" .

Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso no NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Configure a organização do seu console.

Adicione pastas e projetos à sua organização do NetApp Console.

Adicione pastas e projetos para que correspondam à estrutura da sua empresa. Depois de criar pastas e projetos, você pode associar recursos a eles e gerenciar o acesso dos membros a esses projetos.

O Console cria automaticamente um projeto para você quando você cria uma nova organização. A maioria das organizações precisa de mais de um projeto, além de pastas para manter tudo organizado. "Saiba mais sobre a hierarquia de recursos no NetApp Console.".

Utilizando pastas e projetos para organizar recursos

No NetApp Console, uma organização contém pastas e projetos que ajudam você a organizar seus recursos. As pastas ajudam a agrupar projetos relacionados, e os projetos ajudam a gerenciar recursos e o acesso de membros.

Pastas

As pastas ajudam você a organizar projetos relacionados. Você pode criar pastas aninhadas para representar diferentes níveis da estrutura da sua organização. Por exemplo, você pode criar uma pasta de nível superior para cada unidade de negócios e, em seguida, criar subpastas para diferentes equipes dentro dessa unidade de negócios. Em seguida, você cria projetos dentro de pastas.

As pastas também permitem gerenciar o acesso de membros de forma mais eficiente, utilizando a herança de funções. Ao atribuir funções aos membros no nível da pasta, eles herdam as permissões para todos os projetos e pastas filhos.

As pastas são uma ferramenta organizacional e não são visíveis para membros que não possuem permissões do IAM, como administrador da organização, administrador de pasta ou projeto, ou superadministrador. Os membros têm acesso a projetos, não a pastas.

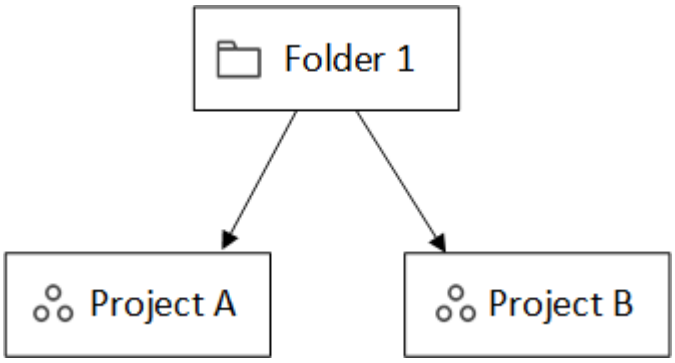
Os administradores da organização podem delegar responsabilidades administrativas criando pastas. Após criar uma pasta, um administrador da organização pode atribuir a um membro as funções de administrador da pasta ou do projeto para pastas específicas. Esses membros podem então gerenciar todos os projetos dentro dessa pasta sem ter acesso a toda a organização.

As pastas podem ter outras pastas ou projetos como filhos, mas não podem ter recursos diretamente associados a elas. Os recursos devem estar associados a um projeto.

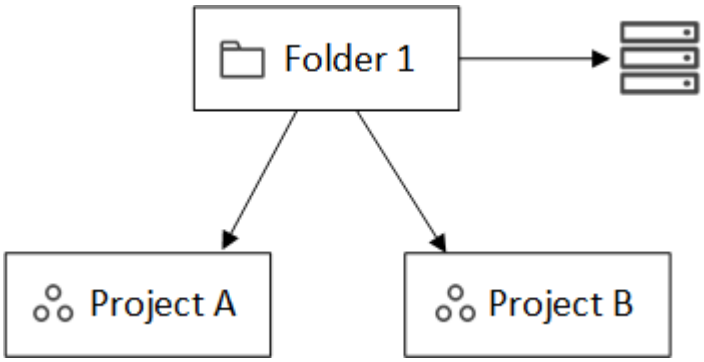
Quando associar um recurso a uma pasta

Um *Administrador da organização* pode associar um recurso a uma pasta para que um *Administrador de pasta ou projeto* possa vinculá-lo aos projetos apropriados na pasta.

Por exemplo, digamos que você tenha uma pasta que contém dois projetos:

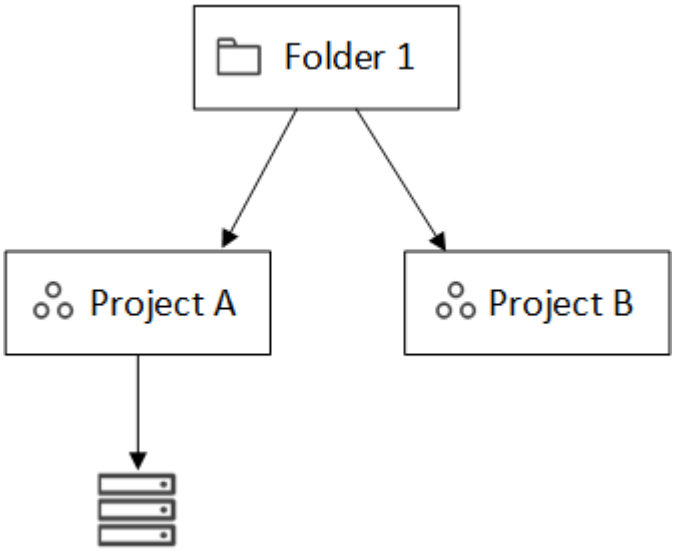


O *Administrador da organização* pode associar um recurso à pasta:



Associar um recurso a uma pasta não o torna acessível a todos os projetos; somente o *administrador da pasta ou do projeto* pode vê-lo. O *administrador de pasta ou projeto* decide quais projetos podem acessá-lo e associa o recurso aos projetos apropriados.

Neste exemplo, o administrador associa o recurso ao Projeto A:



Membros que têm permissões para o projeto A agora podem acessar o recurso.

Projetos

Associe recursos a projetos para permitir que os membros os gerenciem. Os recursos devem ser associados a um projeto para fins de gerenciamento e acesso do usuário.

Uma organização pode ter um ou vários projetos. Um projeto pode estar diretamente subordinado à organização ou dentro de uma pasta. Se um agente for usado para descobrir recursos dentro de um projeto, você também deverá associar o agente a esse projeto.

Os usuários navegam entre os projetos atribuídos na página **Sistemas** para gerenciar os recursos associados a cada projeto.

Adicionar uma pasta ou projeto

Adicione projetos para gerenciar recursos e pastas para agrupar projetos relacionados. Ao criar uma nova organização, o Console inclui um projeto.

Você pode criar até sete níveis de pastas e projetos na estrutura de recursos da sua organização. Crie pastas aninhadas para organizar seus recursos conforme necessário.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organização**.
3. Na página **Organização**, selecione **Adicionar pasta ou projeto**.
4. Selecione **Pasta** ou **Projeto**.
5. Insira os detalhes da pasta ou do projeto:
   - **Nome e localização**: Insira um nome e escolha uma localização para a pasta ou projeto. Você pode colocar pastas ou projetos dentro da organização ou em outra pasta.
   - **Recursos**: Selecione os recursos que deseja associar a esta pasta ou projeto. Se você ainda não adicionou sistemas de armazenamento ao Console, poderá fazer isso mais tarde.

     Os membros não podem acessar os recursos em uma pasta até que esses recursos sejam atribuídos a um projeto. Utilize pastas para armazenar recursos temporariamente até que você crie os projetos necessários. Isso pode ajudar o administrador da organização a delegar a alocação de recursos a um administrador de pasta ou projeto, que então atribui recursos aos projetos dentro da pasta.

   - **Acesso**: Selecione **Adicionar um membro** para atribuir acesso e uma função. Você pode adicionar ou remover membros do projeto ou da pasta a qualquer momento.

     "Saiba mais sobre funções de acesso" .
6. Selecione **Adicionar**.

Renomear uma pasta ou projeto

Renomeie uma pasta ou projeto conforme necessário. A mudança de nome não afeta os recursos associados nem o acesso dos membros.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, insira um novo nome e selecione **Aplicar**.

Excluir uma pasta ou projeto

Exclua pastas e projetos que você não precisa mais, como após uma reestruturação da equipe ou a conclusão de um projeto.

Antes de excluir uma pasta ou projeto, certifique-se de que ele não contenha nenhum recurso. Aprenda como remover recursos.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Excluir**.
2. Confirme que deseja excluir a pasta ou o projeto.

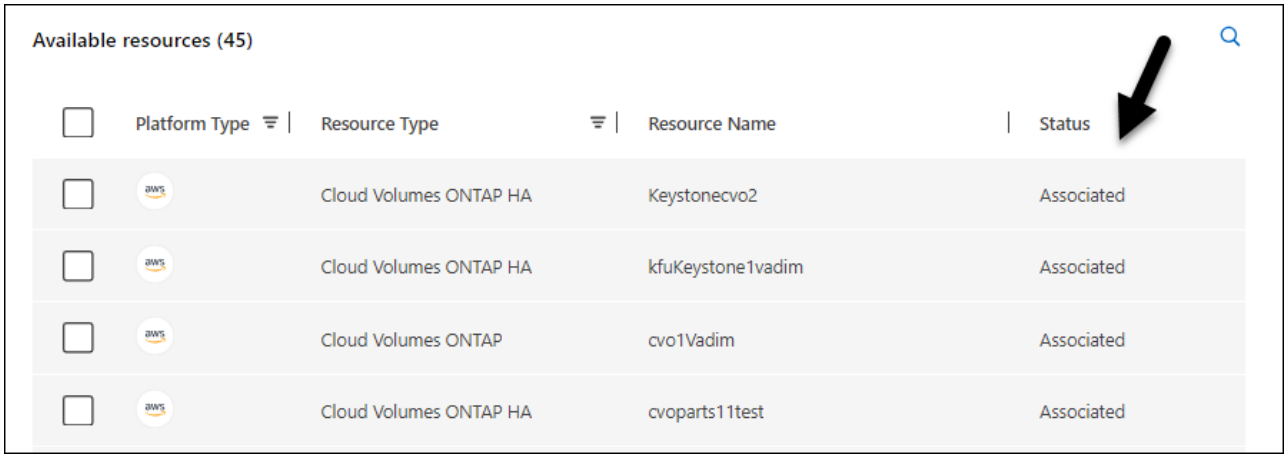
Visualizar os recursos associados a uma pasta ou projeto

Veja quais recursos e membros estão associados a uma pasta ou projeto.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.

2. Na página **Editar**, você pode visualizar detalhes sobre a pasta ou projeto selecionado expandindo as seções **Recursos** ou **Acesso**.
   - Selecione **Recursos** para visualizar os recursos associados. Na tabela, a coluna **Status** identifica os recursos associados à pasta ou ao projeto.



Alterar os recursos associados a uma pasta ou projeto

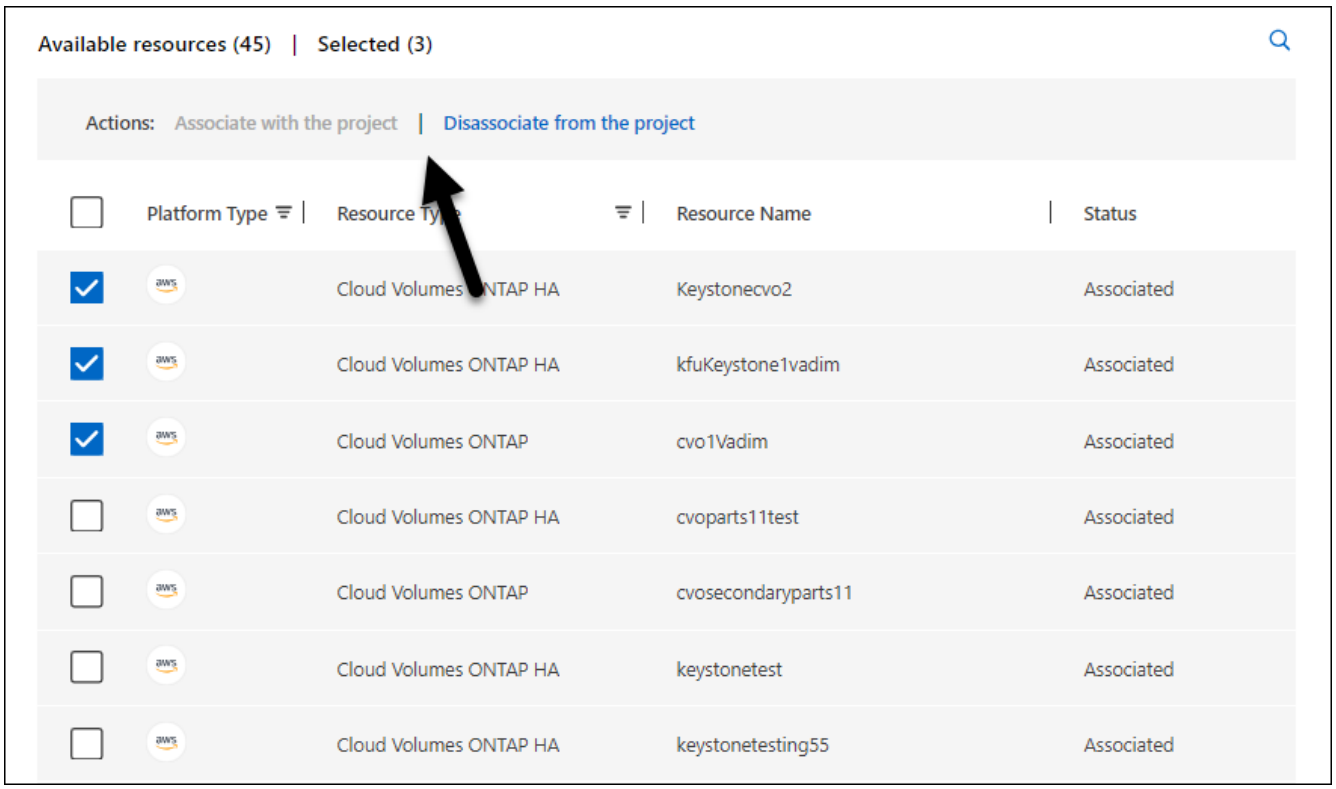
Você pode alterar os recursos associados a uma pasta ou projeto conforme as necessidades da sua organização mudam.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Recursos**.

   Na tabela, a coluna **Status** identifica os recursos associados à pasta ou ao projeto.

3. Selecione os recursos que você gostaria de associar ou desassociar.
4. Com base nos recursos que você selecionou, escolha **Associar-se ao projeto** ou **Desassociar-se do projeto**.



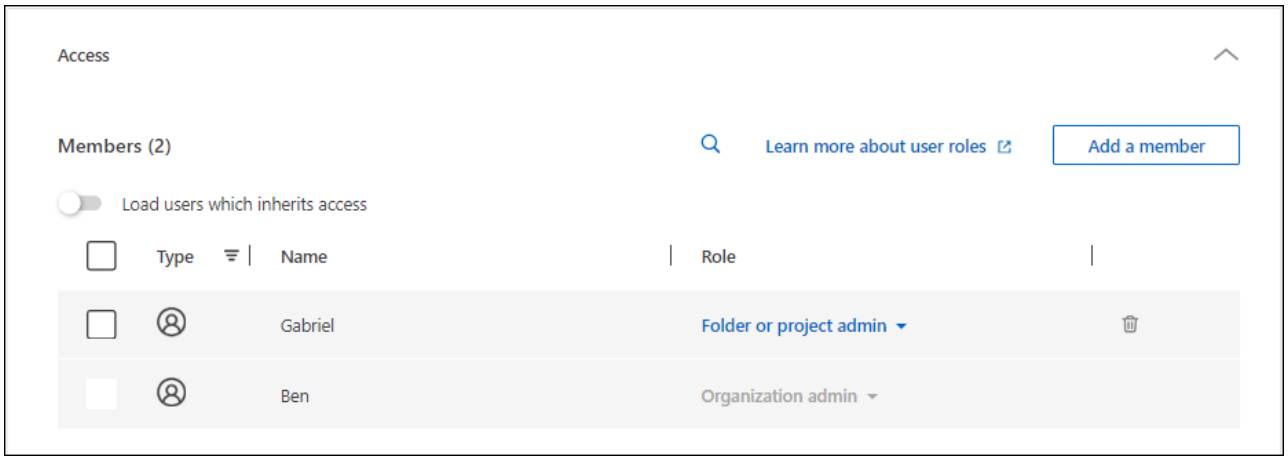
5. Selecione **Aplicar**.

Ver membros associados a uma pasta ou projeto

Você pode visualizar os membros associados a uma pasta ou projeto na página **Organização**.

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Acesso** para visualizar a lista de membros que têm acesso à pasta ou projeto selecionado.
   - Selecione **Acesso** para visualizar os membros que têm acesso à pasta ou ao projeto.



Modificar o acesso de membros a uma pasta ou projeto

Modifique o acesso dos membros para controlar o acesso aos recursos. Lembre-se de que as funções atribuídas no nível da pasta são herdadas por todos os projetos e pastas filhos.

Não é possível alterar o acesso de membros em níveis inferiores se ele for herdado do nível da pasta ou da organização. Altere a permissão do membro no nível hierárquico superior para modificar o acesso. Alternativamente, você pode "gerenciar permissões na página de membros".

Passos

1. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione ••• e então selecione **Editar pasta** ou **Editar projeto**.
2. Na página **Editar**, selecione **Acesso** para visualizar a lista de membros que têm acesso à pasta ou projeto selecionado.
3. Modificar acesso de membro:
   - **Adicionar um membro**: Selecione o membro que você gostaria de adicionar à pasta ou projeto e atribua uma função a ele.
   - **Alterar a função de um membro**: Para qualquer membro com uma função diferente de Administrador da Organização, selecione a função existente e escolha uma nova função.
   - **Remover acesso de membro**: Para membros que têm uma função definida na pasta ou projeto que você está visualizando, você pode remover o acesso deles.
4. Selecione **Aplicar**.

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API de identidade e acesso"

Adicione recursos a pastas e projetos no NetApp Console.

Controle o acesso dos usuários aos recursos adicionando-os a projetos e pastas na sua organização do NetApp Console . Conceder acesso aos usuários no nível do projeto.

Um *recurso* é uma entidade da qual o Console tem conhecimento, como um recurso de armazenamento, um agente do Console ou uma carga de trabalho de Backup e Recuperação.

Você pode visualizar e gerenciar recursos na página **Recursos** do Console.

Tipos de recursos do console

Você pode associar vários tipos de recursos a projetos na sua organização do NetApp Console :

Recursos de armazenamento

Os recursos de armazenamento são o tipo de recurso mais comum em sua organização e representam sistemas de armazenamento locais e em nuvem. Ao adicionar um sistema de armazenamento ao Console, você pode adicioná-lo a uma pasta ou projeto. Até então, o Console o marca como não descoberto e não o exibe na página **Recursos**.

Agentes de console

Se você utilizou um agente de console para descobrir sistemas de armazenamento, adicione o agente à mesma pasta ou projeto. Isso permite que os usuários executem funções habilitadas por agente, como serviços de dados ou gerenciamento de armazenamento nativo do Console. Você pode adicionar agentes a pastas ou projetos na página **Agentes** do Console. "Aprenda como associar um agente do Console a uma pasta ou projeto".

Assinaturas Keystone

Se a sua organização possui assinaturas do Keystone , você pode visualizá-las na página **Recursos**. Você pode associar assinaturas do Keystone a pastas ou projetos para fornecer acesso a membros que tenham permissões para essas pastas ou projetos.

Visualize os recursos em sua organização

Você pode visualizar recursos descobertos e não descobertos associados à sua organização. O sistema localiza recursos de armazenamento e os marca como não descobertos até que você os adicione ao Console.

> O Console exclui os recursos do Amazon FSx for NetApp ONTAP da página Recursos porque os usuários não podem associá-los a uma função. Você pode visualizar esses recursos na página **Sistemas** ou em Cargas de Trabalho.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Recursos**.
3. Selecione **Pesquisa e filtragem avançadas**.
4. Utilize as opções disponíveis para encontrar um recurso:
   - **Pesquisar por nome do recurso**: Insira uma sequência de texto e selecione **Adicionar**.
   - **Plataforma**: Selecione uma ou mais plataformas, como Amazon Web Services.
   - **Recursos**: Selecione um ou mais recursos, como Cloud Volumes ONTAP.
   - **Organização, pasta ou projeto**: Selecione a organização inteira, uma pasta específica ou um projeto específico.
5. Selecione **Pesquisar**.

Associar um recurso a pastas e projetos

Associe um recurso a uma pasta ou projeto para torná-lo disponível aos membros que têm permissões para essa pasta ou projeto.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Associar a pastas ou projetos**.
2. Selecione uma pasta ou projeto e então selecione **Aceitar**.
3. Para associar uma pasta ou projeto adicional, selecione **Adicionar pasta ou projeto** e depois selecione a pasta ou projeto.

   Observe que você só pode selecionar pastas e projetos para os quais você tem permissões de administrador.

4. Selecione **Associar recursos**.
   - Se você associou o recurso a projetos, os membros que têm permissões para esses projetos agora poderão acessar o recurso no Console.
   - Se você associou o recurso a uma pasta, um *administrador de pasta ou projeto* agora pode acessar o recurso e associá-lo a um projeto dentro da pasta. "Aprenda a associar um recurso a uma pasta".

Depois que você terminar

Se você descobrir um recurso usando um agente do Console, associe o agente do Console ao projeto para conceder acesso. Caso contrário, o agente do Console e seu recurso associado não poderão ser acessados por membros sem a função *Administrador da organização*.

"Aprenda como associar um agente do Console a uma pasta ou projeto".

Visualizar as pastas e projetos associados a um recurso

Você pode visualizar as pastas e os projetos associados a um recurso específico.

Se você precisar descobrir quais membros da organização têm acesso ao recurso, você pode"visualizar os membros que têm acesso às pastas e projetos associados ao recurso" .

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Ver detalhes**.

O exemplo a seguir mostra um recurso associado a um projeto.

Para ver quais membros da organização têm acesso ao recurso,"Veja os membros com acesso às pastas e projetos associados." .

Remover um recurso de uma pasta ou projeto

Para remover um recurso de uma pasta ou projeto, remova a sua associação. Isso impede que os membros gerenciem o recurso nessa pasta ou projeto.

> Para remover um recurso detectado de toda a organização, acesse a página **Sistemas** e remova o sistema.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e então selecione **Ver detalhes**.
2. Para remover um recurso de uma pasta ou projeto, selecione 🗑 ao lado da pasta ou do projeto.
3. Selecione **Excluir** para remover a associação.

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece a usar identidade e acesso no NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Associar um agente do Console a outras pastas e projetos

Associe agentes do Console a projetos específicos para permitir o gerenciamento de recursos e o acesso a serviços de dados. Os recursos descobertos por meio de um agente do Console exigem que tanto o recurso quanto o agente estejam associados aos mesmos projetos respectivos para que a equipe tenha acesso.

Os superadministradores e administradores da organização podem criar agentes e associar qualquer agente a qualquer projeto ou pasta. Os administradores de pastas ou projetos só podem associar agentes existentes a pastas e projetos para os quais possuem permissões. "Saiba mais sobre as ações que um *administrador de pasta ou projeto* pode concluir".

Passos

1. Selecione **Administração > Identidade e acesso** > **Agentes**.
2. Na tabela, encontre o agente do Console que você deseja associar.

   Use a pesquisa acima da tabela para encontrar um agente específico do Console ou filtre a tabela por hierarquia de recursos.

3. Para visualizar as pastas e projetos vinculados ao agente do Console, selecione ••• e então selecione **Ver detalhes**.

   A página exibe detalhes sobre as pastas e projetos associados ao agente do Console.

4. Selecione **Associar à pasta ou projeto**.
5. Selecione uma pasta ou projeto e então selecione **Aceitar**.
6. Para associar o agente do Console a uma pasta ou projeto adicional, selecione **Adicionar uma pasta ou projeto** e, em seguida, selecione a pasta ou projeto.
7. Selecione **Agente Associado**.

Depois que você terminar

Associe os recursos do agente do Console às mesmas pastas e projetos da página **Recursos**.

"Aprenda a associar um recurso a pastas e projetos" .

Informações relacionadas

- "Saiba mais sobre os agentes do NetApp Console"
- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API para gerenciamento de identidade e acesso"

Adicione usuários à sua organização do Console.

Adicionar usuários a uma organização do NetApp Console

No Console, você concede aos usuários acesso a projetos ou pastas de acordo com uma função de acesso. Uma *função de acesso* contém um conjunto de permissões que permite a um membro (usuário ou conta de serviço) executar ações específicas no nível atribuído da hierarquia de recursos.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e projetos que eles administram). "Saiba mais sobre funções de acesso".

Entenda como o acesso é concedido no NetApp Console.

O NetApp Console utiliza o controle de acesso baseado em funções (RBAC) para gerenciar permissões. Atribua funções aos usuários individualmente ou por meio de grupos federados. Cada função define as ações permitidas para recursos específicos.

Observe o seguinte sobre como conceder acesso no NetApp Console:

- Todos os usuários devem primeiro se cadastrar no NetApp Console antes de obterem acesso aos recursos.
- Você deve atribuir explicitamente uma função a cada usuário no Console antes que ele possa acessar os recursos, mesmo que seja membro de um grupo federado ao qual já tenha sido atribuída uma função.
- Você pode adicionar contas de serviço diretamente do Console e atribuir funções a elas.

Adicionar membros à sua organização

O NetApp Console suporta três tipos de membros: contas de usuário, contas de serviço e grupos federados.

Os usuários precisam se cadastrar no NetApp Console antes que você possa adicioná-los e atribuir uma função, mesmo que estejam em um grupo federado. Crie contas de serviço diretamente no Console.

Todos os membros devem ter pelo menos uma função explicitamente atribuída a eles para poderem acessar os recursos.

Ao adicionar um membro, escolha o nível de recurso (organização, pasta ou projeto) e atribua uma ou mais funções com as permissões necessárias.

Adicionar um usuário

Os usuários se cadastram no NetApp Console, mas um administrador da organização, pasta ou projeto precisa adicioná-los à organização, pasta ou projeto para que possam acessar os recursos.

Antes de começar:

O usuário já deve ter se cadastrado no NetApp Console. Se eles ainda não se inscreveram, oriente-os a… "Inscreva-se no NetApp Console."

> Se você estiver adicionando um usuário que faz parte de um grupo federado, certifique-se de que ele já tenha se cadastrado no NetApp Console e que uma função tenha sido explicitamente atribuída a ele no Console. A NetApp recomenda atribuir uma função de acesso mínima, como a de visualizador da organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Para **Tipo de membro**, mantenha **Usuário** selecionado.
5. Em **E-mail do usuário**, insira o endereço de e-mail do usuário associado ao login que ele criou.
6. Use a seção **Selecione uma organização, pasta ou projeto** para escolher o nível da hierarquia de recursos para o qual o membro deve ter permissões.

   Observe o seguinte:

   - Você pode selecionar apenas as pastas e os projetos para os quais você tem permissão.
   - Ao selecionar uma organização ou pasta, você concede ao membro permissões para acessar todo o seu conteúdo.
   - Você só pode atribuir a função **Administrador da organização** no nível da organização.
7. **Selecione uma categoria** e depois selecione uma **Função** que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .
8. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione uma função.
9. Selecione **Adicionar**.

   O console envia instruções ao usuário por e-mail.

Adicionar uma conta de serviço

As contas de serviço permitem automatizar tarefas e conectar-se com segurança às APIs do Console. Escolha um ID e um segredo do cliente para configurações simples ou um JWT (JSON Web Token) para maior segurança em ambientes automatizados ou nativos da nuvem. Selecione o método que atenda aos seus requisitos de segurança.

Antes de começar:

Para autenticação JWT, prepare sua chave pública ou certificado.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Para **Tipo de membro**, selecione **Conta de serviço**.
5. Insira um nome para a conta de serviço.
6. Para usar a autenticação JWT, selecione **Usar autenticação JWT com chave privada** e carregue sua chave ou certificado RSA público. Ignore se estiver usando ID e segredo do cliente.

   Seu certificado X.509. Deve estar no formato PEM, CRT ou CER.

   a. Configure notificações de expiração para o seu certificado. Escolha entre sete dias ou 30 dias. As notificações de expiração são enviadas por e-mail e exibidas no Console para usuários com a função de Superadministrador ou Administrador da Organização.
7. Use a seção **Selecione uma organização, pasta ou projeto** para escolher o nível da hierarquia de recursos para o qual o membro deve ter permissões.

   Observe o seguinte:

   ◦ Você só pode selecionar pastas e projetos para os quais você tem permissão.
   ◦ Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   ◦ Você só pode atribuir a função **Administrador da organização** no nível da organização.
8. Selecione uma **Categoria** e, em seguida, selecione uma **Função** que conceda ao membro permissões para os recursos na organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .
9. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione uma função.
10. Se você não escolheu usar a autenticação JWT, baixe ou copie o ID do cliente e o segredo do cliente.

    O Console exibe o segredo do cliente apenas uma vez. Faça uma cópia segura; você poderá recriá-la mais tarde, caso a perca.
11. Se você escolheu a autenticação JWT, baixe ou copie o ID do cliente e o público-alvo do JWT. O Console exibe essas informações apenas uma vez e não permite que você as recupere posteriormente.
12. Selecione **Fechar**.

Adicione um grupo federado à sua organização.

Você pode adicionar um grupo federado do seu provedor de identidade (IdP) à sua organização e atribuir a ele uma ou mais funções. Os membros do grupo federado herdam as funções que você atribui ao grupo no Console.

Antes de atribuir uma função a um grupo federado, certifique-se do seguinte:

- Configure a federação entre seu IdP e o Console. "Aprenda como configurar a federação."
- O grupo já deve existir no seu IdP e ter recebido acesso ao Console.
- Os usuários pertencentes ao grupo já devem ter se cadastrado no NetApp Console e ter recebido uma

função explicitamente atribuída no Console. A NetApp recomenda atribuir uma função de acesso mínima, como a de visualizador da organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione **Adicionar um membro**.
4. Em **Tipo de membro**, selecione **Grupo federado**.
5. Selecione a federação à qual o grupo pertence.
6. Em **Nome do grupo**, insira o nome exato do grupo em seu IdP.
7. Use a seção **Selecione uma organização, pasta ou projeto** para escolher o nível da hierarquia de recursos para o qual o membro deve ter permissões.

   Observe o seguinte:

   - Você só pode selecionar pastas e projetos para os quais você tem permissão.
   - Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função **Administrador da organização** no nível da organização.
8. Selecione uma **Categoria** e, em seguida, selecione uma **Função** que conceda ao membro permissões para os recursos na organização, pasta ou projeto que você selecionou.

   "Saiba mais sobre funções de acesso" .
9. Para conceder acesso a mais pastas, projetos ou funções, selecione **Adicionar função**, escolha a categoria de pasta, projeto ou função e selecione uma função.

Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso no NetApp Console"
- "Comece com identidade e acesso"
- "Funções de acesso ao NetApp Console"
- "Saiba mais sobre a API para identidade e acesso"

Gerenciar o acesso e a segurança do usuário

Saiba mais sobre o controle de acesso baseado em função (RBAC) do NetApp Console .

Gerencie o acesso de usuários ao NetApp Console com controle de acesso baseado em funções (RBAC), atribuindo funções predefinidas no nível da organização, pasta ou projeto. Cada função concede permissões específicas que definem quais ações os usuários podem executar dentro do escopo atribuído.

A NetApp projeta funções de console com privilégios mínimos, de forma que cada função inclua apenas as permissões necessárias para suas tarefas. Essa abordagem aumenta a segurança ao limitar o acesso apenas ao que cada membro precisa.

Depois de organizar os recursos em pastas e projetos, atribua aos membros da organização uma ou mais funções para pastas ou projetos específicos, permitindo que eles executem apenas suas responsabilidades.

Por exemplo, você pode atribuir a um membro a função de administrador de Resiliência a Ransomware para um nível de projeto específico, permitindo que ele execute operações de Resiliência a Ransomware para recursos dentro desse projeto, sem conceder a ele acesso mais amplo a toda a organização. Esse mesmo usuário pode receber a função para vários projetos dentro da sua organização.

Você pode atribuir aos usuários várias funções para o mesmo escopo ou para escopos diferentes, dependendo de suas responsabilidades. Por exemplo, uma organização menor pode ter o mesmo usuário gerenciando as tarefas de Resiliência a Ransomware e Backup e Recuperação no nível organizacional, enquanto uma organização maior pode ter usuários diferentes atribuídos a cada função no nível do projeto.

Tipos de membros da organização Console

Existem três tipos de membros em uma organização do NetApp Console : * *Contas de usuário*: Usuários individuais que fazem login no NetApp Console para gerenciar recursos. Os usuários precisam se cadastrar no NetApp Console antes de serem adicionados a uma organização. * *Contas de serviço*: Contas não humanas usadas por aplicativos ou serviços para interagir com o NetApp Console por meio de APIs. Você pode adicionar contas de serviço diretamente à sua organização do Console. * *Grupos federados*: Grupos sincronizados do seu provedor de identidade (IdP) que permitem gerenciar o acesso de vários usuários coletivamente. Cada usuário dentro de um grupo federado deve ter se cadastrado no NetApp Console e ter sido adicionado à sua organização com uma função de acesso antes de poder acessar os recursos concedidos ao grupo.

"Aprenda como adicionar membros à sua organização."

Funções predefinidas no NetApp Console

O NetApp Console inclui funções predefinidas que você pode atribuir aos membros da organização. Cada função inclui permissões que especificam quais ações um membro pode realizar dentro do seu escopo atribuído (organização, pasta ou projeto).

As funções do NetApp Console utilizam princípios de privilégio mínimo, garantindo que os membros tenham apenas as permissões necessárias para suas tarefas, e categorizam as funções pelo tipo de acesso que fornecem:

- Funções da plataforma: Conceder permissões de administração do console
- Funções de serviços de dados: Conceder permissões para gerenciar serviços de dados específicos, como Resiliência a Ransomware e Backup e Recuperação.
- Funções do aplicativo: Conceder permissões para gerenciar o armazenamento, bem como auditar eventos e alertas do Console.

Você pode atribuir várias funções a um membro com base em suas responsabilidades. Por exemplo, você pode atribuir a um membro tanto a função de administrador de Resiliência a Ransomware quanto a função de administrador de Backup e Recuperação para um projeto específico.

"Saiba mais sobre as funções predefinidas disponíveis no NetApp Console.".

Gerencie o acesso de membros no NetApp Console.

Gerencie o acesso de membros na sua organização do Console. Atribua funções para definir permissões. Remover membros quando eles saírem.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e

projetos que eles administram). Link:reference-iam-predefined-roles.html[Saiba mais sobre funções de acesso].

Você pode atribuir funções de acesso por projeto ou pasta. Por exemplo, atribua uma função a um usuário para dois projetos específicos ou atribua a função no nível da pasta para conceder a um usuário a função de administrador de Resiliência a Ransomware para todos os projetos em uma pasta.

Adicione suas pastas e projetos antes de atribuir acesso aos usuários. "Aprenda como adicionar pastas e projetos."

Entenda como o acesso é concedido no NetApp Console.

O NetApp Console utiliza um modelo de controle de acesso baseado em funções (RBAC) para gerenciar as permissões de usuário. Você pode atribuir funções predefinidas aos membros individualmente ou por meio de grupos federados. Você pode adicionar e atribuir funções a contas de serviço, bem como a grupos federados. Cada função define quais ações um membro pode executar nos recursos associados.

Observe o seguinte sobre como conceder acesso no NetApp Console:

- Todos os usuários devem primeiro se cadastrar no NetApp Console antes de obterem acesso aos recursos.
- Você deve atribuir explicitamente uma função a cada usuário no Console antes que ele possa acessar os recursos, mesmo que seja membro de um grupo federado ao qual já tenha sido atribuída uma função.
- Você pode adicionar contas de serviço diretamente do Console e atribuir funções a elas.

Utilizando a herança de funções

Ao atribuir uma função no nível da organização, pasta ou projeto no NetApp Console, essa função é automaticamente herdada por todos os recursos dentro do escopo selecionado. Por exemplo, as funções em nível de pasta aplicam-se a todos os projetos contidos nela, enquanto as funções em nível de projeto aplicam-se a todos os recursos dentro desse projeto.

Ver membros da organização

Para entender quais recursos e permissões estão disponíveis para um membro, você pode visualizar as funções atribuídas ao membro em diferentes níveis da hierarquia de recursos da sua organização."Aprenda a usar funções para controlar o acesso aos recursos do Console."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.

   A tabela **Membros** lista os membros da sua organização.

3. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.

Exibir funções atribuídas a um membro

Você pode verificar quais funções estão atribuídas a eles atualmente.

Se você tiver a função de *Administrador de pasta ou projeto*, a página exibirá todos os membros da organização. No entanto, você só pode visualizar e gerenciar permissões de membros para as pastas e projetos para os quais você tem permissões. "Saiba mais sobre as ações que um *administrador de pasta ou*

projeto pode concluir" .

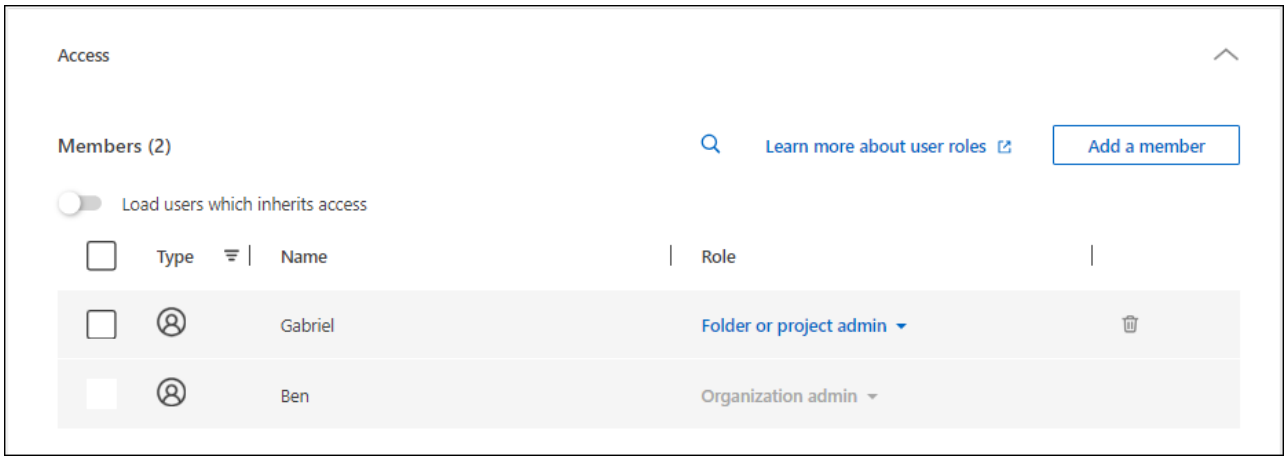
1. Na página **Membros**, navegue até um membro na tabela e selecione ••• Em seguida, selecione **Ver detalhes**.
2. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja visualizar a função atribuída ao membro e selecione **Exibir** na coluna **Função**.

Ver membros associados a uma pasta ou projeto

Você pode visualizar os membros que têm acesso a uma pasta ou projeto específico.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organização**.
3. Na página **Organização**, navegue até um projeto ou pasta na tabela, selecione••• e então selecione **Editar pasta** ou **Editar projeto**.
   - Selecione **Acesso** para visualizar os membros que têm acesso à pasta ou ao projeto.



Atribuir ou modificar o acesso de membros

Depois que um usuário se cadastra no NetApp Console, você pode adicioná-lo à sua organização e atribuir-lhe uma função para fornecer acesso aos recursos. "Aprenda como adicionar membros à sua organização."

Você pode ajustar o acesso de um membro adicionando ou removendo funções conforme necessário.

Adicionar uma função de acesso a um membro

Normalmente, você atribui uma função ao adicionar um membro à sua organização, mas pode atualizá-la a qualquer momento removendo ou adicionando funções.

Você pode atribuir a um usuário uma função de acesso para sua organização, pasta ou projeto.

Os membros podem desempenhar múltiplas funções dentro do mesmo projeto e em projetos diferentes. Por exemplo, organizações menores podem atribuir todas as funções de acesso disponíveis ao mesmo usuário, enquanto organizações maiores podem ter usuários que realizam tarefas mais especializadas. Alternativamente, você também pode atribuir a função de administrador de Resiliência a Ransomware a um usuário no nível da organização. Nesse exemplo, o usuário seria capaz de executar tarefas de resiliência a ransomware em todos os projetos da sua organização.

Sua estratégia de função de acesso deve estar alinhada à maneira como você organizou seus recursos do NetApp .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
4. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
5. Para adicionar uma função, conclua as etapas na caixa de diálogo:
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside na organização ou pasta.
   - **Selecione uma categoria**: Escolha uma categoria de função. "Saiba mais sobre funções de acesso" .
   - Selecione uma **Função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.
   - **Adicionar função**: se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização, selecione **Adicionar função**, especifique outra pasta, projeto ou categoria de função e, em seguida, selecione uma categoria de função e uma função correspondente.
6. Selecione **Adicionar novas funções**.

Alterar a função atribuída a um membro

Alterar as funções de um membro para atualizar o seu acesso.

> ⓘ Os usuários devem ter pelo menos uma função atribuída a eles. Não é possível remover todas as funções de um usuário. Se precisar remover todas as funções, você deverá excluir o usuário da sua organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
5. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a este membro.
6. Você pode alterar uma função existente para um membro ou remover uma função.
   a. Para alterar a função de um membro, selecione **Alterar** ao lado da função que deseja alterar. Você só pode alterar uma função para uma função dentro da mesma categoria de função. Por exemplo, você pode mudar de uma função de serviço de dados para outra. Confirme a alteração.
   b. Para remover a função de um membro, selecione 🗑 Ao lado da função, clique para remover a respectiva função do membro. Você precisará confirmar a remoção.

Remover um membro da sua organização

Remova um membro se ele deixar sua organização.

Ao remover um membro, o sistema revoga suas permissões de Console, mas mantém suas contas de Console e do Site de Suporte da NetApp .

Membros federados

- Os usuários federados perdem automaticamente o acesso ao NetApp Console quando são removidos do seu IdP. Mas você ainda deve removê-los da sua organização no Console para manter sua lista de membros atualizada.
- Se você remover um usuário de um grupo federado em seu IdP, ele perderá o acesso ao Console associado a esse grupo. No entanto, eles ainda mantêm qualquer acesso associado a uma função explícita atribuída a eles no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Selecione uma das guias de membros: **Usuários**, **Contas de serviço** ou **Grupos federados**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• então selecione **Excluir usuário**.
5. Confirme que você deseja remover o membro da sua organização.

Segurança do usuário

Proteja o acesso dos usuários à sua organização NetApp Console gerenciando as configurações de segurança dos membros. Você pode redefinir senhas de usuários, gerenciar a autenticação multifator (MFA) e recriar credenciais de contas de serviço.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou projeto (para pastas e projetos que eles administram). Link:reference-iam-predefined-roles.html[Saiba mais sobre funções de acesso].

Redefinir senhas de usuários (somente usuários locais)

Os administradores da organização não podem redefinir as senhas dos usuários locais. No entanto, eles podem instruir os usuários a redefinirem suas próprias senhas.

Instrua o usuário a redefinir sua senha na página de login do Console, selecionando **Esqueceu sua senha?**.

Essa opção não está disponível para usuários em uma organização federada.

Gerenciar a autenticação multifator (MFA) de um usuário

Se um usuário perder o acesso ao seu dispositivo MFA, você poderá remover ou desabilitar a configuração do MFA.

A autenticação multifator está disponível apenas para usuários locais. Usuários federados não podem ativar a autenticação multifator (MFA).

Os usuários deverão configurar a autenticação multifator (MFA) novamente ao fazerem login após a remoção. Caso o usuário perca temporariamente o acesso ao seu dispositivo MFA, ele poderá usar o código de recuperação salvo para fazer login.

Caso não tenham o código de recuperação, desative temporariamente o MFA para permitir o login. Quando você desabilita o MFA para um usuário, ele é desabilitado por apenas oito horas e depois reabilitado automaticamente. O usuário tem direito a apenas um login durante esse período, sem MFA. Após as oito horas, o usuário deve usar o MFA para efetuar login.

Para gerenciar a autenticação multifator de um usuário, você deve ter um endereço de e-mail no mesmo domínio que o usuário afetado.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.

   A tabela **Membros** lista os membros da sua organização.

3. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Gerenciar autenticação multifator**.
4. Escolha se deseja remover ou desabilitar a configuração MFA do usuário.

Recriar as credenciais para uma conta de serviço

Você pode criar novas credenciais para um serviço caso as perca ou precise atualizá-las.

A criação de novas credenciais exclui as antigas. Você não pode usar as credenciais antigas.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Membros**.
3. Na tabela **Membros**, navegue até uma conta de serviço, selecione ••• e então selecione **Recriar segredos**.
4. Selecione **Recriar**.
5. Baixe ou copie o ID do cliente e o segredo do cliente.

   O Console exibe o segredo do cliente apenas uma vez. Certifique-se de copiar ou baixar o arquivo e armazená-lo em local seguro.

Funções de acesso ao NetApp Console

Saiba mais sobre as funções de acesso do NetApp Console

O gerenciamento de identidade e acesso (IAM) no NetApp Console fornece funções predefinidas que você pode atribuir aos membros da sua organização em diferentes níveis da hierarquia de recursos. Antes de atribuir essas funções, você deve entender as permissões que cada função inclui. As funções se enquadram nas seguintes categorias: plataforma, aplicativo e serviço de dados.

Funções da plataforma

As funções da plataforma concedem permissões de administração do NetApp Console , incluindo atribuição de funções e gerenciamento de usuários. O Console tem várias funções de plataforma.

Função da plataforma	Responsabilidades
"Administrador da organização"	Permite que um usuário tenha acesso irrestrito a todos os projetos e pastas dentro de uma organização, adicione membros a qualquer projeto ou pasta, bem como execute qualquer tarefa e use qualquer serviço de dados que não tenha uma função explícita associada a ele. Usuários com essa função gerenciam sua organização criando pastas e projetos, atribuindo funções, adicionando usuários e gerenciando sistemas, se tiverem as credenciais adequadas. Esta é a única função de acesso que pode criar agentes do Console.
"Administrador de pasta ou projeto"	Permite ao usuário acesso irrestrito aos projetos e pastas atribuídos. Podem adicionar membros às pastas ou projetos que gerenciam, bem como executar qualquer tarefa e usar qualquer serviço de dados ou aplicativo em recursos dentro da pasta ou projeto que lhes foi atribuído. Administradores de pastas ou projetos não podem criar agentes do Console.
"Administrador da Federação"	Permite que um usuário crie e gerencie federações com o Console, o que permite logon único (SSO).
"Visualizador da Federação"	Permite que um usuário visualize federações existentes com o Console. Não é possível criar ou gerenciar federações.
"Administrador de parceria"	Permite que um usuário crie e gerencie parcerias.
"Visualizador de parceria"	Permite que um usuário visualize parcerias existentes. Não é possível criar ou gerenciar parcerias.
"Superadministrador"	Dá ao usuário um subconjunto de funções de administrador. Esta função foi projetada para organizações menores que podem não precisar distribuir responsabilidades do Console entre vários usuários.
"Super visualizador"	Dá ao usuário um subconjunto de funções de visualizador. Esta função foi projetada para organizações menores que podem não precisar distribuir responsabilidades do Console entre vários usuários.

Funções de aplicação

A seguir está uma lista de funções na categoria de aplicação. Cada função concede permissões específicas dentro de seu escopo designado. Usuários sem a função de aplicativo ou plataforma necessária não podem acessar o respectivo aplicativo.

Função de aplicação	Responsabilidades
"Administrador do Google Cloud NetApp Volumes"	Usuários com a função Google Cloud NetApp Volumes podem descobrir e gerenciar o Google Cloud NetApp Volumes.
"Visualizador de Google Cloud NetApp Volumes"	Usuários com a função de usuário Google Cloud NetApp Volumes podem visualizar os Google Cloud NetApp Volumes.

Função de aplicação	Responsabilidades
"Administrador Keystone"	Usuários com a função de administrador do Keystone podem criar solicitações de serviço. Permite que os usuários monitorem e visualizem o uso, os recursos e os detalhes administrativos dentro do locatário do Keystone que estão acessando.
"Visualizador Keystone"	Usuários com a função de visualizador do Keystone NÃO PODEM criar solicitações de serviço. Permite que os usuários monitorem e visualizem o consumo, os ativos e as informações administrativas dentro do locatário do Keystone que estão acessando.
Função de configuração do Mediador ONTAP	Contas de serviço com a função de configuração do ONTAP Mediator podem criar solicitações de serviço. Esta função é necessária em uma conta de serviço para configurar uma instância do"Mediador de Nuvem ONTAP" .
"Analista de suporte operacional"	Fornece acesso a alertas e ferramentas de monitoramento e capacidade de inserir e gerenciar casos de suporte.
"Administrador de armazenamento"	Administre funções de governança e integridade de armazenamento, descubra recursos de armazenamento e modifique e exclua sistemas existentes.
"Visualizador de armazenamento"	Visualize as funções de governança e integridade do armazenamento, bem como visualize os recursos de armazenamento descobertos anteriormente. Não é possível descobrir, modificar ou excluir sistemas de armazenamento existentes.
"Especialista em saúde do sistema"	Administrar funções de armazenamento, saúde e governança, todas as permissões do administrador de armazenamento, exceto não poder modificar ou excluir sistemas existentes.

Funções de serviço de dados

A seguir está uma lista de funções na categoria de serviço de dados. Cada função concede permissões específicas dentro de seu escopo designado. Usuários que não tenham a função de serviço de dados necessária ou uma função de plataforma não poderão acessar o serviço de dados.

Função de serviço de dados	Responsabilidades
"Superadministrador de Backup e Recuperação"	Execute qualquer ação no NetApp Backup and Recovery.
"Administrador de backup e recuperação"	Faça backups em snapshots locais, replique para armazenamento secundário e faça backup no armazenamento de objetos.
"Administração de restauração de backup e recuperação"	Restaure cargas de trabalho no Backup e Recuperação.
"Administrador clone de backup e recuperação"	Clone aplicativos e dados no Backup e Recuperação.
"Visualizador de backup e recuperação"	Ver informações de backup e recuperação.
"Administrador de recuperação de desastres"	Execute quaisquer ações no serviço NetApp Disaster Recovery .

Função de serviço de dados	Responsabilidades
"Administrador de failover de recuperação de desastres"	Execute failover e migrações.
"Administrador do aplicativo de recuperação de desastres"	Crie planos de replicação, altere planos de replicação e inicie failovers de teste.
"Visualizador de recuperação de desastres"	Ver apenas informações.
Visualizador de classificação	Permite que os usuários visualizem os resultados da verificação de NetApp Data Classification . Usuários com essa função podem visualizar informações de conformidade e gerar relatórios para recursos aos quais têm permissão de acesso. Esses usuários não podem habilitar ou desabilitar a verificação de volumes, buckets ou esquemas de banco de dados. A classificação não possui função administrativa.
"Administrador de resiliência de ransomware"	Gerencie ações nas guias Proteger, Alertas, Recuperar, Configurações e Relatórios do NetApp Ransomware Resilience.
"Visualizador de resiliência de ransomware"	Visualize dados de carga de trabalho, visualize dados de alerta, baixe dados de recuperação e baixe relatórios no Ransomware Resilience.
"Comportamento do usuário de resiliência ao ransomware"	Configure, gerencie e visualize a detecção, os alertas e o monitoramento de comportamento suspeito do usuário no Ransomware Resilience.
"Visualizador de comportamento do usuário de resiliência de ransomware"	Veja alertas e insights sobre comportamento suspeito de usuários no Ransomware Resilience.
Administrador do SnapCenter	Oferece a capacidade de fazer backup de instantâneos de clusters ONTAP locais usando o NetApp Backup and Recovery para aplicativos. Um membro com essa função pode concluir as seguintes ações: * Concluir qualquer ação em Backup e recuperação > Aplicativos * Gerenciar todos os sistemas nos projetos e pastas para os quais eles têm permissões * Usar todos os serviços do NetApp Console O SnapCenter não tem uma função de visualizador.

Links relacionados

- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console"
- "Comece a usar o NetApp Console IAM"
- "Gerenciar membros do NetApp Console e suas permissões"
- "Saiba mais sobre a API para NetApp Console IAM"

Funções de acesso à plataforma do NetApp Console

Atribua funções de plataforma aos usuários para conceder permissões para gerenciar o NetApp Console, atribuir funções, adicionar usuários, criar agentes do Console e gerenciar federações.

Exemplo de funções organizacionais para uma grande organização multinacional

A XYZ Corporation organiza o acesso ao armazenamento de dados por região — América do Norte, Europa e Ásia-Pacífico — fornecendo controle regional com supervisão centralizada.

O **administrador da organização** no Console da XYZ Corporation cria uma organização inicial e pastas separadas para cada região. O **administrador de pasta ou projeto** de cada região organiza projetos (com recursos associados) dentro da pasta da região.

Administradores regionais com a função **Administrador de pasta ou projeto** gerenciam ativamente suas pastas adicionando recursos e usuários. Esses administradores regionais também podem adicionar, remover ou renomear pastas e projetos que gerenciam. O **administrador da organização** herda permissões para quaisquer novos recursos, mantendo a visibilidade do uso do armazenamento em toda a organização.

Dentro da mesma organização, um usuário recebe a função **Administrador da federação** para gerenciar a federação da organização com seu IdP corporativo. Este usuário pode adicionar ou remover organizações federadas, mas não pode gerenciar usuários ou recursos dentro da organização. O **Administrador da organização** atribui a um usuário a função **Visualizador da federação** para verificar o status da federação e visualizar organizações federadas.

As tabelas a seguir indicam as ações que cada função da plataforma Console pode executar.

Funções de administração da organização

Tarefa	Administrador da organização	Administrador de pasta ou projeto
Criar agentes	Sim	Não
Criar, modificar ou excluir sistemas do Console (adicionar ou descobrir sistemas)	Sim	Sim
Crie pastas e projetos, incluindo exclusão	Sim	Não
Renomear pastas e projetos existentes	Sim	Sim
Atribuir funções e adicionar usuários	Sim	Sim
Associar recursos a pastas e projetos	Sim	Sim
Associar agentes a pastas e projetos	Sim	Não
Remover agentes de pastas e projetos	Sim	Não
Gerenciar agentes (editar certificados, configurações e assim por diante)	Sim	Não
Gerenciar credenciais em Administração > Credenciais	Sim	Sim
Criar, gerenciar e visualizar federações	Sim	Não
Registre-se para obter suporte e envie casos por meio do Console	Sim	Sim
Use serviços de dados que não estejam associados a uma função de acesso explícita	Sim	Sim
Ver a página de auditoria e notificações	Sim	Sim

Funções da Federação

Tarefa	Administrador da Federação	Visualizador da Federação
Criar uma federação	Sim	Não
Verificar um domínio	Sim	Não
Adicionar um domínio a uma federação	Sim	Não
Desabilitar e excluir federações	Sim	Não
Federações de teste	Sim	Não
Ver federações e seus detalhes	Sim	Sim

Funções de parceria

Tarefa	Administrador de parceria	Visualizador de parceria
Pode criar uma parceria	Sim	Não
Atribuir funções aos membros parceiros	Sim	Não
Pode adicionar membros a uma parceria	Sim	Não
Pode visualizar detalhes da parceria da organização	Sim	Sim

Funções de superadministrador e visualizador

A função **Superadministrador** fornece acesso total para gerenciar recursos do Console, armazenamento e serviços de dados. Essa função é adequada para aqueles que supervisionam a administração e a governança. Em contraste, a função **Super visualizador** oferece acesso somente leitura, ideal para auditores ou partes interessadas que precisam de visibilidade sem fazer alterações.

As organizações devem usar o acesso de **Superadministrador** com moderação para minimizar os riscos de segurança e se alinhar ao princípio do menor privilégio. A maioria das organizações deve atribuir funções refinadas com apenas as permissões necessárias para reduzir riscos e melhorar a capacidade de auditoria.

Exemplo para super funções

A ABC Corporation tem uma pequena equipe de cinco pessoas que utiliza o NetApp Console para serviços de dados e gerenciamento de armazenamento. Em vez de distribuir várias funções, eles atribuem a função de **Superadministrador** a dois membros seniores da equipe que lidam com todas as tarefas administrativas, incluindo gerenciamento de usuários e configuração de recursos. Os três membros restantes da equipe recebem a função de **Supervisualizador**, o que lhes permite monitorar a integridade do armazenamento e o status do serviço de dados sem a capacidade de modificar as configurações.

Papel	Funções herdadas
Superadministrador	• Administrador da organização • Administrador de pasta ou projeto • Administrador da Federação • Administrador de parceria • Administrador de resiliência de ransomware • Administrador de recuperação de desastres • Superadministrador de backup • Administrador de armazenamento • Administrador Keystone • Administrador do Google Cloud NetApp Volumes
Super visualizador	• Visualizador de organização • Visualizador da Federação • Visualizador de parceria • Visualizador de resiliência de ransomware • Visualizador de recuperação de desastres • Visualizador de backup • Visualizador de armazenamento • Visualizador Keystone • Visualizador de Google Cloud NetApp Volumes

Funções de aplicação

Funções do Google Cloud NetApp Volumes no NetApp Console

Você pode atribuir a seguinte função aos usuários para fornecer a eles acesso ao Google Cloud NetApp Volumes no NetApp Console.

O Google Cloud NetApp Volumes usa a seguinte função:

- * Administrador do Google Cloud NetApp Volumes *: Descubra e gerencie o Google Cloud NetApp Volumes no Console.
- *Visualizador de Google Cloud NetApp Volumes *: Visualize os Google Cloud NetApp Volumes no

Console.

Funções de acesso Keystone no NetApp Console

As funções do Keystone fornecem acesso aos painéis do Keystone e permitem que os usuários visualizem e gerenciem sua assinatura do Keystone . Há duas funções do Keystone : administrador do Keystone e visualizador do Keystone . A principal diferença entre as duas funções são as ações que elas podem realizar no Keystone. A função de administrador do Keystone é a única função que tem permissão para criar solicitações de serviço ou modificar assinaturas.

Exemplo de funções Keystone no NetApp Console

A XYZ Corporation tem quatro engenheiros de armazenamento de diferentes departamentos que visualizam as informações de assinatura do Keystone . Embora todos esses usuários precisem monitorar a assinatura do Keystone , somente o líder da equipe tem permissão para fazer solicitações de serviço. Três membros da equipe recebem a função de *visualizador do Keystone *, enquanto o líder da equipe recebe a função de *administrador do Keystone * para que haja um ponto de controle sobre as solicitações de serviço da empresa.

A tabela a seguir indica as ações que cada função Keystone pode executar.

Recurso e ação	Administrador Keystone	Visualizador Keystone
Visualize as seguintes guias: Assinatura, Ativos, Monitor e Administração	Sim	Sim
* Página de assinatura do Keystone *:		
Ver assinaturas	Sim	Sim
Alterar ou renovar assinaturas	Sim	Não
* Página de ativos do Keystone *:		
Ver ativos	Sim	Sim
Gerenciar ativos	Sim	Não
* Página de alertas do Keystone *:		
Ver alertas	Sim	Sim
Gerenciar alertas	Sim	Não
Crie alertas para si mesmo	Sim	Sim
* Licenses and subscriptions*:		
Pode visualizar licenças e assinaturas	Sim	Sim
*Página de relatórios do Keystone *:		

Recurso e ação	Administrador Keystone	Visualizador Keystone
Baixar relatórios	Sim	Sim
Gerenciar relatórios	Sim	Sim
Crie relatórios para si mesmo	Sim	Sim
Solicitações de serviço:		
Criar solicitações de serviço	Sim	Não
Visualizar solicitações de serviço criadas por qualquer usuário dentro da organização	Sim	Sim

Função de acesso de analista de suporte operacional para o NetApp Console

Você pode atribuir a função de analista de suporte operacional aos usuários para conceder a eles acesso a alertas e monitoramento. Usuários com essa função também podem abrir casos de suporte.

Analista de suporte operacional

Tarefa	Pode executar
Gerencie suas próprias credenciais de usuário em Configurações > Credenciais	Sim
Ver recursos descobertos	Sim
Registre-se para obter suporte e envie casos por meio do Console	Sim
Ver a página de auditoria e notificações	Sim
Visualizar, baixar e configurar alertas	Sim

Funções de acesso de armazenamento para o NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso aos recursos de gerenciamento de armazenamento no NetApp Console. Você pode atribuir aos usuários uma função administrativa para gerenciar o armazenamento ou uma função de visualizador para monitoramento.

Essas funções não estão disponíveis na API de parceria do NetApp Console .

Os administradores podem atribuir funções de armazenamento aos usuários para os seguintes recursos e funcionalidades de armazenamento:

Recursos de armazenamento:

- Clusters ONTAP locais
- StorageGRID
- Série E

Serviços e recursos do console:

- Consultor digital
- Atualizações de software
- Planejamento do ciclo de vida
- Sustentabilidade

Exemplo de funções de armazenamento no NetApp Console

A XYZ Corporation, uma empresa multinacional, tem uma grande equipe de engenheiros e administradores de armazenamento. Eles permitem que essa equipe gerencie ativos de armazenamento para suas regiões, ao mesmo tempo em que limitam o acesso às principais tarefas do Console, como gerenciamento de usuários, criação de agentes e gerenciamento de licenças.

Em uma equipe de 12 pessoas, dois usuários recebem a função **Visualizador de armazenamento**, que lhes permite monitorar os recursos de armazenamento associados aos projetos do Console aos quais estão atribuídos. Os nove restantes recebem a função de **Administrador de armazenamento**, que inclui a capacidade de gerenciar atualizações de software, acessar o ONTAP System Manager por meio do Console, bem como descobrir recursos de armazenamento (adicionar sistemas). Uma pessoa na equipe recebe a função de **Especialista em integridade do sistema** para que possa gerenciar a integridade dos recursos de armazenamento em sua região, mas não modificar ou excluir nenhum sistema. Essa pessoa também pode executar atualizações de software nos recursos de armazenamento para projetos aos quais ela foi atribuída.

A organização tem dois usuários adicionais com a função **Administrador da organização** que podem gerenciar todos os aspectos do Console, incluindo gerenciamento de usuários, criação de agentes e gerenciamento de licenças, bem como vários usuários com a função **Administrador de pasta ou projeto** que podem executar tarefas de administração do Console para as pastas e projetos aos quais estão atribuídos.

A tabela a seguir mostra as ações que cada função de armazenamento executa.

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Gerenciamento de Armazenamento:			
Descubra novos recursos (crie sistemas)	Sim	Sim	Não
Ver sistemas descobertos	Sim	Sim	Não
Excluir sistemas do Console	Sim	Não	Não
Modificar sistemas	Sim	Não	Não
Criar agentes	Não	Não	Não
Consultor digital			

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Ver todas as páginas e funções	Sim	Sim	Sim
* Licenses and subscriptions*			
Ver todas as páginas e funções	Não	Não	Não
Atualizações de software			
Ver página de destino e recomendações	Sim	Sim	Sim
Revise as recomendações de versões potenciais e os principais benefícios	Sim	Sim	Sim
Exibir detalhes de atualização para um cluster	Sim	Sim	Sim
Execute verificações de pré-atualização e baixe o plano de atualização	Sim	Sim	Sim
Instalar atualizações de software	Sim	Sim	Não
Planejamento do ciclo de vida			
Revisar status de planejamento de capacidade	Sim	Sim	Sim
Escolha a próxima ação (melhor prática, nível)	Sim	Não	Não
Coloque dados frios em camadas no armazenamento em nuvem e libere espaço de armazenamento	Sim	Sim	Não
Configurar lembretes	Sim	Sim	Sim
Sustentabilidade			
Ver painel e recomendações	Sim	Sim	Sim
Baixar dados do relatório	Sim	Sim	Sim
Editar porcentagem de mitigação de carbono	Sim	Sim	Não
Recomendações de correção	Sim	Sim	Não
Adiar recomendações	Sim	Sim	Não
Acesso do gerente do sistema			
Pode inserir credenciais	Sim	Sim	Não

Recurso e ação	Administrador de armazenamento	Especialista em saúde do sistema	Visualizador de armazenamento
Credenciais			
Credenciais do usuário	Sim	Sim	Não

Funções de serviços de dados

Funções de NetApp Backup and Recovery no NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso ao NetApp Backup and Recovery no Console. As funções de backup e recuperação oferecem a flexibilidade de atribuir aos usuários uma função específica para as tarefas que eles precisam realizar na sua organização. A maneira como você atribui funções depende das suas próprias práticas de negócios e gerenciamento de armazenamento.

O serviço usa as seguintes funções específicas do NetApp Backup and Recovery.

- **Superadministrador de Backup e Recuperação**: Execute qualquer ação no NetApp Backup and Recovery.
- **Administrador de backup e recuperação**: execute backups em instantâneos locais, replique para armazenamento secundário e faça backup em ações de armazenamento de objetos no NetApp Backup and Recovery.
- **Administrador de restauração de backup e recuperação**: restaure cargas de trabalho usando o NetApp Backup and Recovery.
- **Administrador de Clone de Backup e Recuperação**: Clone aplicativos e dados usando o NetApp Backup and Recovery.
- **Visualizador de backup e recuperação**: visualize informações no NetApp Backup and Recovery, mas não execute nenhuma ação.

Para obter detalhes sobre todas as funções de acesso do NetApp Console , consulte "a documentação de configuração e administração do Console" .

Funções usadas para ações comuns

A tabela a seguir indica as ações que cada função do NetApp Backup and Recovery pode executar para todas as cargas de trabalho.

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Adicionar, editar ou excluir hosts	Sim	Não	Não	Não	Não
Instalar plugins	Sim	Não	Não	Não	Não

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Adicionar credenciais (host, instância, vCenter)	Sim	Não	Não	Não	Não
Ver painel e todas as guias	Sim	Sim	Sim	Sim	Sim
Iniciar teste gratuito	Sim	Não	Não	Não	Não
Iniciar descoberta de cargas de trabalho	Não	Sim	Sim	Sim	Não
Ver informações da licença	Sim	Sim	Sim	Sim	Sim
Ativar licença	Sim	Não	Não	Não	Não
Ver hosts	Sim	Sim	Sim	Sim	Sim
Horários:					
Ativar agendamentos	Sim	Sim	Sim	Sim	Não
Suspender horários	Sim	Sim	Sim	Sim	Não
Políticas e proteção:					
Ver planos de proteção	Sim	Sim	Sim	Sim	Sim
Criar, modificar ou excluir planos de proteção	Sim	Sim	Não	Não	Não
Restaurar cargas de trabalho	Sim	Não	Sim	Não	Não
Criar, dividir ou excluir clones	Sim	Não	Não	Sim	Não
Criar, modificar ou excluir política	Sim	Sim	Não	Não	Não
Relatórios:					
Ver relatórios	Sim	Sim	Sim	Sim	Sim
Criar relatórios	Sim	Sim	Sim	Sim	Não

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Administrador clone de backup e recuperação	Visualizador de backup e recuperação
Excluir relatórios	Sim	Não	Não	Não	Não
Importar do SnapCenter e gerenciar host:					
Exibir dados importados do SnapCenter	Sim	Sim	Sim	Sim	Sim
Importar dados do SnapCenter	Sim	Sim	Não	Não	Não
Gerenciar (migrar) host	Sim	Sim	Não	Não	Não
Configurar definições:					
Configurar diretório de log	Sim	Sim	Sim	Não	Não
Associar ou remover credenciais de instância	Sim	Sim	Sim	Não	Não
Baldes:					
Ver baldes	Sim	Sim	Sim	Sim	Sim
Criar, editar ou excluir bucket	Sim	Sim	Não	Não	Não

Funções usadas para ações específicas da carga de trabalho

A tabela a seguir indica as ações que cada função do NetApp Backup and Recovery pode executar para cargas de trabalho específicas.

Cargas de trabalho do Kubernetes

Esta tabela indica as ações que cada função do NetApp Backup and Recovery pode executar para ações específicas de cargas de trabalho do Kubernetes.

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Exibir clusters, namespaces, classes de armazenamento e recursos de API	Sim	Sim	Sim	Sim

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Adicionar novos clusters do Kubernetes	Sim	Sim	Não	Não
Atualizar configurações de cluster	Sim	Não	Não	Não
Remover clusters do gerenciamento	Sim	Não	Não	Não
Ver aplicações	Sim	Sim	Sim	Sim
Criar e definir novos aplicativos	Sim	Sim	Não	Não
Atualizar configurações do aplicativo	Sim	Sim	Não	Não
Remover aplicativos do gerenciamento	Sim	Sim	Não	Não
Exibir recursos protegidos e status de backup	Sim	Sim	Sim	Sim
Crie backups e proteja aplicativos com políticas	Sim	Sim	Não	Não
Desproteja aplicativos e exclua backups	Sim	Sim	Não	Não
Exibir pontos de recuperação e resultados do visualizador de recursos	Sim	Sim	Sim	Sim
Restaurar aplicativos de pontos de recuperação	Sim	Não	Sim	Não
Ver políticas de backup do Kubernetes	Sim	Sim	Sim	Sim
Criar políticas de backup do Kubernetes	Sim	Sim	Sim	Não
Atualizar políticas de backup	Sim	Sim	Sim	Não
Excluir políticas de backup	Sim	Sim	Sim	Não
Exibir ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Sim

Recurso e ação	Superadministrador de Backup e Recuperação	Administrador de backup e recuperação	Administração de restauração de backup e recuperação	Visualizador de backup e recuperação
Crie ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não
Atualizar ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não
Excluir ganchos de execução e fontes de ganchos	Sim	Sim	Sim	Não
Exibir modelos de ganchos de execução	Sim	Sim	Sim	Sim
Criar modelos de gancho de execução	Sim	Sim	Sim	Não
Atualizar modelos de gancho de execução	Sim	Sim	Sim	Não
Excluir modelos de gancho de execução	Sim	Sim	Sim	Não
Visualizar resumo da carga de trabalho e painéis analíticos	Sim	Sim	Sim	Sim
Exibir buckets e destinos de armazenamento do StorageGRID	Sim	Sim	Sim	Sim

Funções de NetApp Disaster Recovery no NetApp Console

Você pode atribuir as seguintes funções aos usuários para fornecer a eles acesso ao NetApp Disaster Recovery no Console. As funções de Recuperação de Desastres oferecem a flexibilidade de atribuir aos usuários uma função específica para as tarefas que eles precisam realizar na sua organização. A maneira como você atribui funções depende das suas próprias práticas de negócios e gerenciamento de armazenamento.

A recuperação de desastres utiliza as seguintes funções:

- **Administrador de recuperação de desastres**: Execute quaisquer ações.
- **Administrador de failover de recuperação de desastres**: Executa failover e migrações.
- **Administrador do aplicativo de recuperação de desastres**: Crie planos de replicação. Modificar planos de replicação. Iniciar failovers de teste.
- **Visualizador de recuperação de desastres**: Visualize somente informações.

A tabela a seguir indica as ações que cada função pode executar.

Recurso e ação	Administrador de recuperação de desastres	Administrador de failover de recuperação de desastres	Administrador do aplicativo de recuperação de desastres	Visualizador de recuperação de desastres
Ver painel e todas as guias	Sim	Sim	Sim	Sim
Iniciar teste gratuito	Sim	Não	Não	Não
Iniciar descoberta de cargas de trabalho	Sim	Não	Não	Não
Ver informações da licença	Sim	Sim	Sim	Sim
Ativar licença	Sim	Não	Sim	Não
Na aba Sites:				
Ver sites	Sim	Sim	Sim	Sim
Adicionar, modificar ou excluir sites	Sim	Não	Não	Não
Na aba Planos de replicação:				
Ver planos de replicação	Sim	Sim	Sim	Sim
Ver detalhes do plano de replicação	Sim	Sim	Sim	Sim
Criar ou modificar planos de replicação	Sim	Sim	Sim	Não
Criar relatórios	Sim	Não	Não	Não
Ver instantâneos	Sim	Sim	Sim	Sim
Executar testes de failover	Sim	Sim	Sim	Não
Executar failovers	Sim	Sim	Não	Não
Executar failbacks	Sim	Sim	Não	Não
Executar migrações	Sim	Sim	Não	Não
Na aba Grupos de recursos:				
Exibir grupos de recursos	Sim	Sim	Sim	Sim
Criar, modificar ou excluir grupos de recursos	Sim	Não	Sim	Não

Recurso e ação	Administrador de recuperação de desastres	Administrador de failover de recuperação de desastres	Administrador do aplicativo de recuperação de desastres	Visualizador de recuperação de desastres
Na aba Monitoramento de Tarefas:				
Ver empregos	Sim	Não	Sim	Sim
Cancelar trabalhos	Sim	Sim	Sim	Não

Funções de acesso de resiliência contra ransomware para o NetApp Console

As funções de resiliência contra ransomware fornecem aos usuários acesso ao NetApp Ransomware Resilience. O Ransomware Resilience oferece suporte às seguintes funções:

Funções de base

- Administrador de resiliência contra ransomware - Configurar as configurações de resiliência contra ransomware; investigar e responder a alertas de criptografia
- Visualizador de resiliência de ransomware - visualize incidentes de criptografia, relatórios e configurações de descoberta

Funções de atividade de comportamento do usuário"Detecção de atividade suspeita do usuário" Os alertas fornecem visibilidade de dados como eventos de atividade de arquivo; esses alertas incluem nomes de arquivos e ações de arquivo (como Ler, Gravar, Excluir, Renomear) executadas pelo usuário. Para limitar a visibilidade desses dados, somente usuários com essas funções podem gerenciar ou visualizar esses alertas.

- Administrador de comportamento do usuário de resiliência contra ransomware - Ative a detecção de atividades suspeitas do usuário, investigue e responda a alertas de atividades suspeitas do usuário
- Visualizador de comportamento do usuário do Ransomware Resilience - Visualize alertas de atividades suspeitas do usuário

> As funções de comportamento do usuário não são funções autônomas; elas foram projetadas para serem adicionadas às funções de administrador ou visualizador do Ransomware Resilience. Para mais informações, consulte Funções de comportamento do usuário.

Consulte as tabelas a seguir para obter descrições detalhadas de cada função.

Funções de base

A tabela a seguir descreve as ações disponíveis para as funções de administrador e visualizador do Ransomware Resilience.

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
Ver painel e todas as guias	Sim	Sim

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
No painel, atualize o status da recomendação	Sim	Não
Iniciar teste gratuito	Sim	Não
Iniciar descoberta de cargas de trabalho	Sim	Não
Iniciar a redescoberta das cargas de trabalho	Sim	Não
Na aba Proteger:		
Adicionar, modificar ou excluir planos de proteção para políticas de *criptografia*	Sim	Não
Proteja as cargas de trabalho	Sim	Não
Identifique a exposição a dados sensíveis com a Classificação de Dados	Sim	Não
Listar planos de proteção e detalhes	Sim	Sim
Grupos de proteção de lista	Sim	Sim
Ver detalhes do grupo de proteção	Sim	Sim
Criar, editar ou excluir grupos de proteção	Sim	Não
Baixar dados	Sim	Sim
Na aba Alertas:		
Exibir alertas de criptografia e detalhes de alertas	Sim	Sim
Editar status do incidente de criptografia	Sim	Não
Marcar alerta de criptografia para recuperação	Sim	Não
Ver detalhes do incidente de criptografia	Sim	Sim
Descartar ou resolver incidentes de criptografia	Sim	Não
Obtenha a lista completa de arquivos afetados no evento de criptografia	Sim	Não
Baixar dados de alertas de eventos de criptografia	Sim	Sim

Recurso e ação	Administrador de resiliência de ransomware	Visualizador de resiliência de ransomware
Bloquear usuário (com configuração do agente de segurança de carga de trabalho)	Sim	Não
Na aba Recuperar:		
Baixar arquivos afetados pelo evento de criptografia	Sim	Não
Restaurar carga de trabalho do evento de criptografia	Sim	Não
Baixar dados de recuperação do evento de criptografia	Sim	Sim
Baixar relatórios do evento de criptografia	Sim	Sim
Na aba Configurações:		
Adicionar ou modificar destinos de backup	Sim	Não
Listar destinos de backup	Sim	Sim
Exibir alvos SIEM conectados	Sim	Sim
Adicionar ou modificar alvos SIEM	Sim	Não
Configurar exercício de prontidão	Sim	Não
Iniciar, redefinir ou editar o exercício de prontidão	Sim	Não
Revisar o status do exercício de prontidão	Sim	Sim
Atualizar configuração de descoberta	Sim	Não
Exibir configuração de descoberta	Sim	Sim
Na aba Relatórios:		
Baixar relatórios	Sim	Sim

Funções de comportamento do usuário

Para configurar configurações de comportamento suspeito do usuário e responder a alertas, um usuário deve ter a função de administrador de comportamento do usuário de resiliência ao ransomware. Para visualizar apenas alertas de comportamento suspeito do usuário, o usuário deve ter a função de visualizador de comportamento do usuário do Ransomware Resilience.

As funções de comportamento do usuário devem ser conferidas aos usuários com privilégios de administrador ou visualizador do Ransomware Resilience existentes que precisam de acesso a"configurações e alertas de

atividades suspeitas do usuário" . Um usuário com a função de administrador de Resiliência contra Ransomware, por exemplo, deve receber a função de administrador de comportamento de usuário de Resiliência contra Ransomware para configurar agentes de atividade do usuário e bloquear ou desbloquear usuários. A função de administrador de comportamento do usuário de Resiliência contra Ransomware não deve ser conferida a um visualizador de Resiliência contra Ransomware.

Para ativar a detecção de atividades suspeitas do usuário, você deve ter a função de administrador da Organização do Console.

A tabela a seguir descreve as ações disponíveis para as funções de administrador e visualizador do comportamento do usuário do Ransomware Resilience.

Recurso e ação	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Na aba Configurações:		
Criar, modificar ou excluir agente de atividade do usuário	Sim	Não
Criar ou excluir conector de diretório de usuário	Sim	Não
Pausar ou retomar o coletor de dados	Sim	Não
Execute um exercício de preparação para violação de dados	Sim	Não
Na aba Proteger:		
Adicionar, modificar ou excluir planos de proteção para políticas de *comportamento suspeito do usuário*	Sim	Não
Na aba Alertas:		
Ver alertas de atividade do usuário e detalhes do alerta	Sim	Sim
Editar status do incidente de atividade do usuário	Sim	Não
Marcar alerta de atividade do usuário para recuperação	Sim	Não
Ver detalhes do incidente de atividade do usuário	Sim	Sim
Descartar ou resolver incidentes de atividade do usuário	Sim	Não
Obtenha a lista completa de arquivos afetados por usuários suspeitos	Sim	Sim
Baixar dados de alertas de eventos de atividade do usuário	Sim	Sim
Bloquear ou desbloquear usuário	Sim	Não

Recurso e ação	Comportamento do usuário de resiliência ao ransomware	Visualizador de comportamento do usuário de resiliência de ransomware
Na aba Recuperar:		
Baixar arquivos impactados para evento de atividade do usuário	Sim	Não
Restaurar carga de trabalho do evento de atividade do usuário	Sim	Não
Baixar dados de recuperação do evento de atividade do usuário	Sim	Sim
Baixar relatórios de eventos de atividade do usuário	Sim	Sim

API de identidade e acesso

IDs de organização e projeto

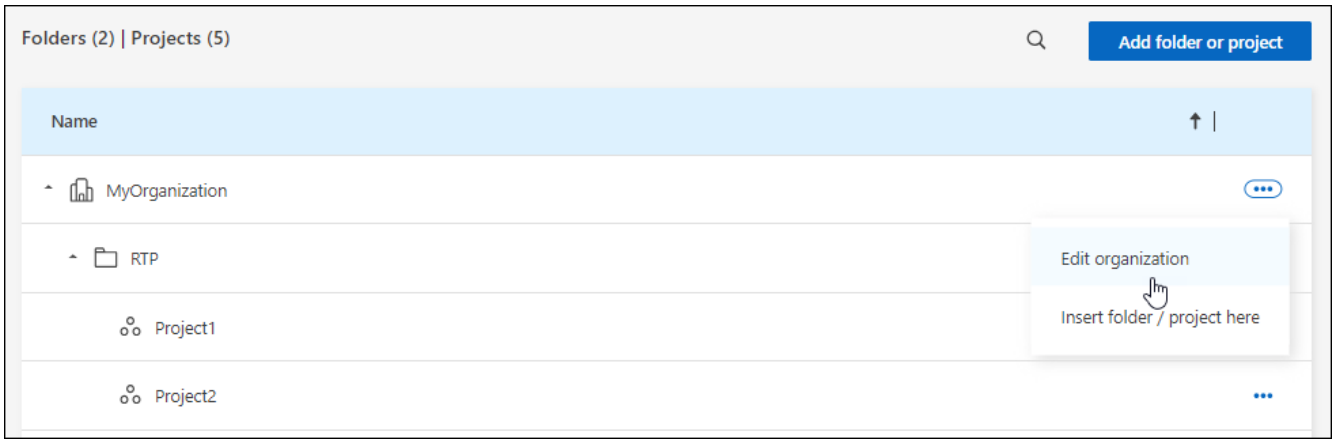
Sua organização do NetApp Console tem um nome e um ID. Você pode escolher um nome para sua organização para ajudar a identificá-la. Também pode ser necessário recuperar o ID da organização para determinadas integrações.

Renomeie sua organização

Você pode renomear sua organização. Isso é útil se você apoia mais do que uma organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organização**.
3. Na página **Organização**, navegue até a primeira linha da tabela e selecione ••• e então selecione **Editar organização**.



4. Digite um novo nome para a organização e selecione **Aplicar**.

Obter o ID da organização

O ID da organização é usado para determinadas integrações com o Console.

Você pode visualizar o ID da organização na página Organizações e copiá-lo para a área de transferência conforme suas necessidades.

Passos

1. Selecione **Administração > Identidade e acesso** > **Organização**.
2. Na página **Organização**, procure o ID da sua organização na barra de resumo e copie-o para a área de transferência. Você pode salvar isso para usar mais tarde ou copiá-lo diretamente para onde precisar usá-lo.

Obter o ID de um projeto

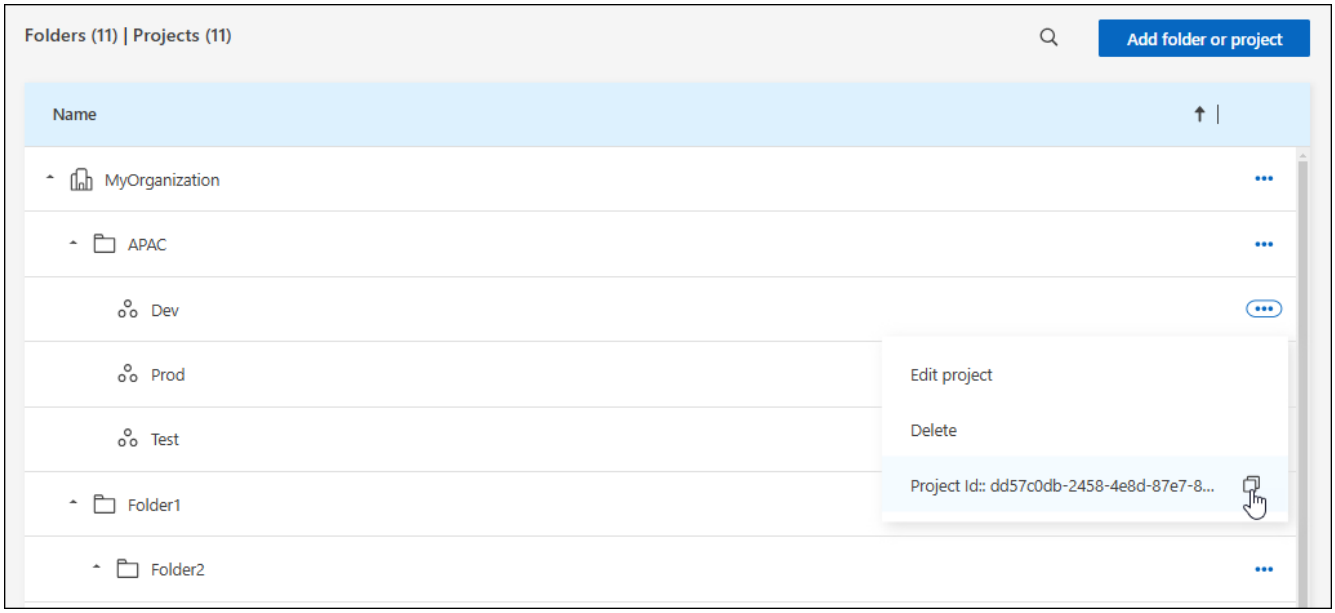
Você precisará obter o ID de um projeto se estiver usando a API. Por exemplo, ao criar um sistema Cloud Volumes ONTAP .

Passos

1. Na página **Organização**, navegue até um projeto na tabela e selecione •••

   O ID do projeto é exibido.

2. Para copiar o ID, selecione o botão copiar.



Informações relacionadas

- "Aprenda sobre gerenciamento de identidade e acesso"
- "Comece com identidade e acesso"
- "Saiba mais sobre a API para identidade e acesso"

Segurança e conformidade

Federação de identidade

Habilitar logon único usando federação de identidade com o NetApp Console

O logon único (federação) simplifica o processo de login e aumenta a segurança, permitindo que os usuários façam login no NetApp Console usando suas credenciais corporativas. Você pode habilitar o logon único (SSO) com seu provedor de identidade (IdP) ou com o site de suporte da NetApp .

Função necessária

Administrador da organização, administrador da federação, visualizador da federação."Saiba mais sobre funções de acesso."

Federação de identidade com o site de suporte da NetApp

A federação com o site de suporte da NetApp permite que os usuários façam login no Console, no Active IQ Digital Advisor e em outros aplicativos associados usando as mesmas credenciais.

> Se você se federar com o Site de Suporte da NetApp , não poderá se federar também com seu provedor de gerenciamento de identidade corporativa. Escolha o que funciona melhor para sua organização.

Passos

1. Baixe e complete o "Formulário de solicitação de federação da NetApp" .
2. Envie o formulário para o endereço de e-mail especificado no formulário.

   A equipe de suporte da NetApp analisa e processa sua solicitação.

Configure uma conexão federada com seu provedor de identidade

Você pode configurar uma conexão federada com seu provedor de identidade para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu provedor de identidade para confiar na NetApp como provedora de serviços e, em seguida, criar a conexão no Console.

> Se você configurou a federação anteriormente usando o NetApp Cloud Central (um aplicativo externo ao Console), será necessário importar sua federação usando a página Federação para gerenciá-la no Console."Aprenda como importar sua federação."

Provedores de identidade suportados

A NetApp oferece suporte aos seguintes protocolos e provedores de identidade para federação:

Protocolos

- Provedores de identidade de Linguagem de Marcação de Asserção de Segurança (SAML)
- Serviços de Federação do Active Directory (AD FS)

Provedores de identidade

- ID de entrada da Microsoft
- PingFederate

Federação com fluxo de trabalho do NetApp Console

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode federar com seu domínio de e-mail ou com um domínio diferente que você possui. Para federar com um domínio diferente do seu domínio de e-mail, primeiro verifique se você é o proprietário do domínio.

Verifique seu domínio (se não estiver usando seu domínio de e-mail)

Para federar com um domínio diferente do seu domínio de e-mail, verifique se você é o proprietário dele. Você pode federar seu domínio de e-mail sem nenhuma etapa extra.

Configure seu IdP para confiar na NetApp como um provedor de serviços

Configure seu provedor de identidade para confiar no NetApp criando um novo aplicativo e fornecendo detalhes como URL do ACS, ID da entidade ou outras informações de credencial. As informações do provedor de serviços variam de acordo com o provedor de identidade, portanto, consulte a documentação do seu provedor de identidade específico para obter detalhes. Você precisará trabalhar com o administrador do seu IdP para concluir esta etapa.

Crie a conexão federada no Console

Forneça o URL ou arquivo de metadados SAML do seu provedor de identidade para criar a conexão. Essas informações são usadas para estabelecer a relação de confiança entre o Console e seu provedor de identidade. As informações fornecidas dependem do IdP que você está usando. Por exemplo, se estiver usando o Microsoft Entra ID, você precisará fornecer o ID do cliente, o segredo e o domínio.

Teste sua federação no Console

Teste sua conexão federada antes de habilitá-la. Use a opção de teste na página Federação no Console para verificar se o usuário de teste pode ser autenticado com sucesso. Se o teste for bem-sucedido, você poderá habilitar a conexão.

Habilite sua conexão no Console

Depois de habilitar a conexão, os usuários podem efetuar login no Console usando suas credenciais corporativas.

Revise o tópico do seu respectivo protocolo ou IdP para começar:

- "Configurar uma conexão federada com o AD FS"
- "Configurar uma conexão federada com o Microsoft Entra ID"
- "Configurar uma conexão federada com PingFederate"
- "Configurar uma conexão federada com um provedor de identidade SAML"

Verificação de domínio

Verifique o domínio de e-mail para sua conexão federada

Se você quiser federar com um domínio diferente do seu domínio de e-mail, primeiro você deve verificar se é o proprietário do domínio. Você só pode usar domínios verificados para federação.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Verificar seu domínio envolve adicionar um registro TXT às configurações de DNS do seu domínio. Este registro é usado para provar que você é o proprietário do domínio e permite que o NetApp Console confie no domínio para federação. Talvez seja necessário coordenar com seu administrador de TI ou de rede para concluir esta etapa.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Selecione **Verificar propriedade do domínio**.
5. Digite o domínio que você deseja verificar e selecione **Continuar**.
6. Copie o registro TXT fornecido.
7. Acesse as configurações de DNS do seu domínio e configure o valor TXT que foi fornecido como um registro TXT para seu domínio. Trabalhe com seu administrador de TI ou de rede, se necessário.
8. Após o registro TXT ser adicionado, retorne ao Console e selecione **Verificar**.

Configurar federações

Federar o NetApp Console com os Serviços de Federação do Active Directory (AD FS)

Federe seus Serviços de Federação do Active Directory (AD FS) com o NetApp Console para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login no Console usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

> Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, configure o provedor de identidade para confiar no NetApp Console como um provedor de serviços. Em seguida, crie uma conexão no Console usando a configuração do seu provedor de identidade.

Você pode configurar a federação com seu servidor AD FS para habilitar o logon único (SSO) para o NetApp Console. O processo envolve configurar o AD FS para confiar no Console como um provedor de serviços e,

em seguida, criar a conexão no NetApp Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Serviços de Federação do Active Directory (AD FS)**.
7. Selecione **Avançar**.
8. Crie uma Relying Party Trust no seu servidor AD FS. Você pode usar o PowerShell ou configurá-lo manualmente no seu servidor AD FS. Consulte a documentação do AD FS para obter detalhes sobre como criar uma confiança de terceira parte confiável.
   a. Crie a confiança usando o PowerShell usando o seguinte script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. Como alternativa, você pode criar a confiança manualmente no console de gerenciamento do AD FS. Use os seguintes valores do NetApp Console ao criar a confiança:
      - Ao criar o Relying Trust Identifier, use o valor **YOUR_TENANT**: `netapp-cloud-account`
      - Ao selecionar **Habilitar suporte para WS-Federation**, use o valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`
   c. Depois de criar a confiança, copie o URL de metadados do seu servidor AD FS ou baixe o arquivo de metadados da federação. Você precisará deste URL ou arquivo para concluir a conexão no Console.

   A NetApp recomenda usar o URL de metadados para permitir que o NetApp Console recupere automaticamente a configuração mais recente do AD FS. Se você baixar o arquivo de metadados da federação, precisará atualizá-lo manualmente no NetApp Console sempre que houver alterações na configuração do AD FS.
9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com o AD FS.
    a. Insira o **URL do AD FS** que você copiou do seu servidor AD FS na etapa anterior ou carregue o arquivo de metadados da federação que você baixou do seu servidor AD FS.
11. Selecione **Criar conexão**. A criação da conexão pode levar alguns segundos.

12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

    Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

14. No Console, selecione **Avançar** para revisar a página de resumo.
15. Configure as notificações.

    Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

16. Analise os detalhes da federação e selecione **Ativar federação**.
17. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federar NetApp Console com Microsoft Entra ID

Federe com seu provedor de IdP do Microsoft Entra ID para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o Microsoft Entra ID para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu ID do Microsoft Entra para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.

Detalhes do domínio

1. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o

domínio associado à conta com a qual você está conectado.

b. Digite o nome da federação que você está configurando.

c. Se você escolher um domínio verificado, selecione o domínio na lista.

2. Selecione **Avançar**.

Método de conexão

1. Para seu método de conexão, escolha **Provedor** e depois selecione **Microsoft Enterprise ID**.
2. Selecione **Avançar**.

Instruções de configuração

1. Configure seu ID Microsoft Entra para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor Microsoft Entra ID.

   a. Use os seguintes valores ao registrar seu aplicativo Microsoft Entra ID para confiar no Console:

      - Para o **URL de redirecionamento**, use `https://services.cloud.netapp.com`
      - Para o **URL de resposta**, use `https://netapp-cloud-account.auth0.com/login/callback`

   b. Crie um segredo do cliente para seu aplicativo Microsoft Entra ID. Você precisará fornecer o ID do cliente, o segredo do cliente e o nome de domínio do Entra ID para concluir a federação.

2. Retorne ao Console e selecione **Avançar** para criar a conexão.

Criar conexão

1. Crie a conexão com o Microsoft Entra ID

   a. Insira o ID do cliente e o segredo do cliente que você criou na etapa anterior.

   b. Digite o nome de domínio do ID do Microsoft Entra.

2. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.

Teste e habilite a conexão

1. Selecione **Avançar**.
2. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

   Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

3. No Console, selecione **Avançar** para revisar a página de resumo.
4. Configure as notificações.

   Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

5. Analise os detalhes da federação e selecione **Ativar federação**.

6. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federar o NetApp Console com o PingFederate

Federe com seu provedor PingFederate IdP para habilitar o logon único (SSO) para o NetApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . A NetApp recomenda escolher um ou outro, mas não ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com o PingFederate para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu servidor PingFederate para confiar no Console como um provedor de serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Provedor** e depois selecione **PingFederate**.
7. Selecione **Avançar**.
8. Configure seu servidor PingFederate para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no seu servidor PingFederate.
   a. Use os seguintes valores ao configurar o PingFederate para confiar no NetApp Console:
      - Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
      - Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
      - Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-pingfederate> é o nome de domínio da federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria

`urn:auth0:netappcloud-account:fed-example-com-pingfederate`.

b. Copie a URL do servidor PingFederate. Você precisará deste URL ao criar a conexão no Console.

c. Baixe o certificado X.509 do seu servidor PingFederate. Ele precisa estar no formato PEM codificado em Base64 (.pem, .crt, .cer).

9. Retorne ao Console e selecione **Avançar** para criar a conexão.
10. Crie a conexão com PingFederate

a. Digite a URL do servidor PingFederate que você copiou na etapa anterior.

b. Carregue o certificado de assinatura X.509. O certificado deve estar no formato PEM, CER ou CRT.

11. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
12. Selecione **Avançar**.
13. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

14. No Console, selecione **Avançar** para revisar a página de resumo.
15. Configure as notificações.

Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

16. Analise os detalhes da federação e selecione **Ativar federação**.
17. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Federe com um provedor de identidade SAML

Federe com seu provedor SAML 2.0 IdP para habilitar o logon único (SSO) para o NEtApp Console. Isso permite que os usuários façam login usando suas credenciais corporativas.

Função necessária

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você pode federar com seu IdP corporativo ou com o site de suporte da NetApp . Você não pode federar com ambos.

O NetApp oferece suporte somente a SSO iniciado pelo provedor de serviços (iniciado pelo SP). Primeiro, você precisa configurar o provedor de identidade para confiar na NetApp como provedora de serviços. Em seguida, você pode criar uma conexão no Console que usa a configuração do provedor de identidade.

Você pode configurar uma conexão federada com seu provedor SAML 2.0 para habilitar o logon único (SSO) para o Console. O processo envolve configurar seu provedor para confiar na NetApp como provedora de

serviços e, em seguida, criar a conexão no Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Federação** para visualizar a página **Federações**.
3. Selecione **Configurar nova federação**.
4. Insira os detalhes do seu domínio:
   a. Escolha se deseja usar um domínio verificado ou seu domínio de e-mail. O domínio de e-mail é o domínio associado à conta com a qual você está conectado.
   b. Digite o nome da federação que você está configurando.
   c. Se você escolher um domínio verificado, selecione o domínio na lista.
5. Selecione **Avançar**.
6. Para seu método de conexão, escolha **Protocolo** e depois selecione **Provedor de identidade SAML**.
7. Selecione **Avançar**.
8. Configure seu provedor de identidade SAML para confiar na NetApp como provedora de serviços. Você precisa executar esta etapa no servidor do seu provedor SAML.
   a. Certifique-se de que seu IdP tenha o atributo `email` definido como o endereço de e-mail do usuário. Isso é necessário para que o Console identifique os usuários corretamente:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Use os seguintes valores ao registrar seu aplicativo SAML no Console:
   - Para o **URL de resposta** ou **URL do serviço de consumidor de declaração (ACS)**, use `https://netapp-cloud-account.auth0.com/login/callback`
   - Para o **URL de logout**, use `https://netapp-cloud-account.auth0.com/logout`
   - Para **ID do público/entidade**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` onde <fed-domain-name-saml> é o nome de domínio que você deseja usar para federação. Por exemplo, se o seu domínio for `example.com` , o ID do público/entidade seria `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Depois de criar a confiança, copie os seguintes valores do servidor do seu provedor SAML:
   - URL de login
   - URL de saída (opcional)
3. Baixe o certificado X.509 do servidor do seu provedor SAML. Precisa estar no formato PEM, CER ou CRT.

a. Retorne ao Console e selecione **Avançar** para criar a conexão.

b. Crie a conexão com SAML.

4. Digite o **URL de login** do seu servidor SAML.
5. Faça upload do certificado X.509 que você baixou do servidor do seu provedor SAML.
6. Opcionalmente, insira o **URL de saída** do seu servidor SAML.
   a. Selecione **Criar conexão**. O sistema cria a conexão em poucos segundos.
   b. Selecione **Avançar**.
   c. Selecione **Testar conexão** para testar sua conexão. Você será direcionado para uma página de login para seu servidor IdP. Faça login com suas credenciais do IdP. Após efetuar o login, volte ao Console para ativar a conexão.

      Ao usar o Console no modo restrito, copie o URL para uma janela anônima do navegador ou para um navegador separado para fazer login no seu IdP.

   d. No Console, selecione **Avançar** para revisar a página de resumo.
   e. Configure as notificações.

      Escolha entre sete dias ou 30 dias. O sistema envia notificações de expiração por e-mail e as exibe no Console para qualquer usuário com as seguintes funções: Superadministrador, Administrador da organização, Administrador da federação e Visualizador da federação.

   f. Analise os detalhes da federação e selecione **Ativar federação**.
   g. Selecione **Concluir** para finalizar o processo.

Após habilitar a federação, os usuários fazem login no NetApp Console usando suas credenciais corporativas.

Gerenciar federações

Gerenciar federações no NetApp Console

Você pode gerenciar sua federação no NetApp Console. Você pode desativá-lo, atualizar credenciais expiradas e também desativá-lo caso não precise mais dele.

Funções necessárias

A função de administrador da Federação é necessária para criar e gerenciar federações. O visualizador da Federação pode visualizar a página da Federação."Saiba mais sobre funções de acesso."

Você também pode adicionar um domínio verificado adicional a uma federação existente, o que permite usar vários domínios para sua conexão federada.

- Se você configurou a federação usando o NetApp Cloud Central, importe-a por meio da página **Federação** para gerenciá-la no Console."Aprenda como importar sua federação"
- Na página de Auditoria, você pode visualizar eventos de gerenciamento de federação, como ativação, desativação e atualização de federações. "Saiba mais sobre o monitoramento de operações no NetApp Console."

Habilitar uma federação

Se você criou uma federação, mas ela não está habilitada, você pode habilitá-la na página **Federação**. Habilitar uma federação permite que usuários associados à federação façam login no Console usando suas credenciais corporativas. Crie e teste a federação com sucesso antes de habilitá-la.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ••• ao lado da federação que você deseja habilitar e selecione **Habilitar**.

Adicionar um domínio verificado a uma federação existente

Você pode adicionar um domínio verificado a uma federação existente no Console para usar vários domínios com o mesmo provedor de identidade (IdP).

Você já deve ter verificado o domínio no Console antes de poder adicioná-lo a uma federação. Se você ainda não verificou o domínio, pode fazê-lo seguindo as etapas em"Verifique seu domínio no Console" .

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ⋮ ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Atualizar domínios**. A caixa de diálogo **Atualizar domínios** exibe o domínio já associado a esta federação.
4. Selecione um domínio verificado na lista de domínios disponíveis.
5. Selecione **Atualizar**. Novos usuários de domínio podem obter acesso ao Console federado em 30 segundos.

Atualizando uma conexão federada que está expirando

Você pode atualizar os detalhes de uma federação no Console. Por exemplo, você precisará atualizar a federação se as credenciais, como um certificado ou segredo do cliente, expirarem. Quando necessário, atualize a data de notificação para lembrá-lo de atualizar a conexão antes que ela expire.

ⓘ Atualize o Console antes de atualizar seu IdP para evitar problemas de login. Permaneça conectado ao Console durante o processo.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações (três pontos verticais) ao lado da federação que você deseja atualizar e selecione **Atualizar federação**.
4. Atualize os detalhes da federação conforme necessário.
5. Selecione **Atualizar**.

Testar uma federação existente

Teste a conexão de uma federação existente para verificar se ela funciona. Isso pode ajudar você a identificar quaisquer problemas com a federação e solucioná-los.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ⋮ ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Testar conexão**.
4. Selecione **Testar**. O sistema solicita que você faça login com suas credenciais corporativas. Se a conexão for bem-sucedida, você será redirecionado para o NetApp Console. Se a conexão falhar, você verá uma mensagem de erro indicando o problema com a federação.
5. Selecione **Concluído** para retornar à aba **Federação**.

Desabilitar uma federação

Se você não precisar mais de uma federação, poderá desativá-la. Isso impede que usuários associados à federação façam login no Console usando suas credenciais corporativas. Você pode reativar a federação mais tarde, se necessário.

Desabilite uma federação antes de excluí-la, como ao desativar o IdP ou descontinuar a federação. Isso permite que você o reative mais tarde, se necessário.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione o menu de ações ⋮ ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Desativar**.

Excluir uma federação

Se você não precisar mais de uma federação, poderá excluí-la. Isso remove a federação e impede que qualquer usuário associado a ela faça login no Console usando suas credenciais corporativas. Por exemplo, se o IdP estiver sendo desativado ou se a federação não for mais necessária.

Não é possível recuperar uma federação após excluí-la. Você deve criar uma nova federação.

ⓘ Você deve desabilitar uma federação antes de poder excluí-la. Não é possível recuperar uma federação após excluí-la.

Passos

1. Selecione **Administração > Identidade e acesso** .
2. Selecione **Federações** para visualizar a página **Federações**.
3. Selecione o menu de ações ⋮ ao lado da federação à qual você deseja adicionar um domínio verificado e selecione **Excluir**.

Importe sua federação para o NetApp Console

Se você tiver configurado anteriormente a federação por meio do NetApp Cloud Central

(um aplicativo externo ao NetApp Console), a página Federação solicitará que você importe sua conexão federada existente para o Console para que você possa gerenciá-la na nova interface. Você pode então aproveitar os aprimoramentos mais recentes sem precisar recriar sua conexão federada.

Depois de importar sua federação existente, você pode gerenciá-la na página **Federações** ."Saiba mais sobre como gerenciar federações."

Função necessária

Administrador da organização ou administrador da federação."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Federação**.
3. Selecione **Importar Federação**.

Aplicar permissões ONTAP para o ONTAP Advanced View (ONTAP System Manager)

Por padrão, as credenciais do agente do Console permitem que os usuários acessem o Advanced View (ONTAP System Manager). Em vez disso, você pode solicitar aos usuários suas credenciais ONTAP . Isso garante que as permissões ONTAP de um usuário sejam aplicadas quando ele trabalha com clusters ONTAP nos clusters Cloud Volumes ONTAP e ONTAP locais.

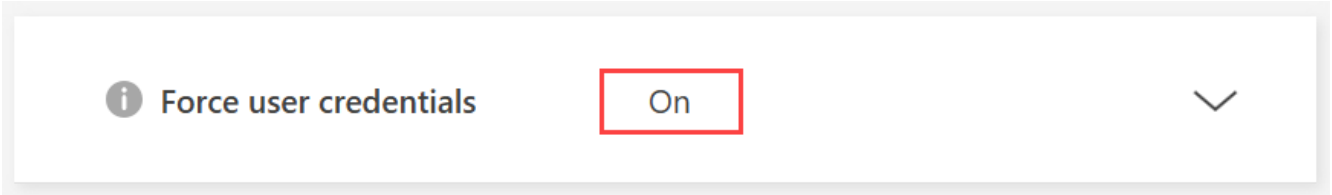
Você deve ter a função de administrador da organização para editar as configurações do agente do console.

Passos

1. Selecione **Administração > Agentes**.
2. Na página **Visão geral**, selecione o menu de ação para um agente do Console e selecione **Editar agente**.

   O agente do Console deve estar ativo para editá-lo.

3. Expanda a opção **Forçar credenciais**.
4. Marque a caixa de seleção para habilitar a opção **Forçar credenciais** e selecione **Salvar**.
5. Verifique se a opção **Forçar credenciais** está habilitada.



Ativar o modo somente leitura para uma organização do NetApp Console

Como medida de segurança, você pode ativar o modo somente leitura para sua organização do NetApp Console . No modo somente leitura, os usuários podem visualizar recursos e configurações, mas não podem fazer alterações.

No modo somente leitura, os usuários com funções de administrador precisam elevar manualmente suas permissões para fazer alterações, o que garante que as alterações sejam intencionais.

Funções de acesso necessárias

Superadministrador ou administrador da organização.

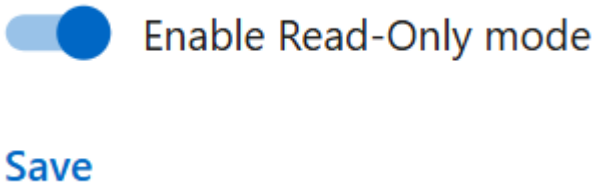
Ative o modo somente leitura para sua organização do Console.

Ative o modo somente leitura para restringir as alterações na sua organização do Console. Todos os usuários ainda podem visualizar os recursos. Usuários com funções de administrador não podem executar nenhuma ação no Console sem elevar manualmente suas permissões.

Quando o modo somente leitura está ativado, os usuários veem um banner que os notifica de que a organização está em modo somente leitura. Os usuários devem acessar as Configurações do usuário para elevar seu nível de privilégio.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Na guia **Organizações**, selecione **Editar configurações da organização** para a organização que você deseja definir como somente leitura.
3. Na seção **Modo somente leitura**, ative o modo somente leitura movendo a chave para a posição **Ligado** e, em seguida, selecione **Salvar**.



Cadastre-se no NetApp Console como administrador inicial da organização.

Se sua empresa não possui uma organização NetApp Console , inscreva-se para criar uma. O primeiro usuário é o administrador e gerencia as contas e permissões. Você poderá atualizar as funções e adicionar administradores posteriormente.

Passos

1. Abra um navegador da web e vá para o "NetApp Console"
2. Se você possui uma conta no site de suporte da NetApp , insira o endereço de e-mail associado à sua conta diretamente na página de **login**.

   O Console realiza o seu cadastro como parte deste login inicial, utilizando as suas credenciais do Site de Suporte da NetApp .

3. Se você quiser se inscrever criando um login no Console, selecione **Inscrever-se**.
   a. Na página **Inscreva-se**, insira as informações necessárias e selecione **Avançar**.

      Somente caracteres em inglês são permitidos no formulário de inscrição.

   b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.

      Verifique seu endereço de e-mail para concluir o cadastro.

4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Na página **Boas-vindas**, crie uma organização.
6. Selecione **Vamos começar**.

+ Se você for um administrador iniciante, siga o processo guiado para adicionar armazenamento, criar um agente do Console e muito mais. "Aprenda a usar o Assistente do Console."

Próximos passos

Como administrador, após concluir as etapas incluídas no Assistente do Console, você deve planejar sua estratégia de identidade e acesso, adicionar usuários à sua organização e atribuir funções. "Saiba mais sobre gerenciamento de identidade e acesso para o NetApp Console."

Cadastre-se ou faça login no NetApp Console se já existir uma organização.

Se sua empresa já possui uma organização NetApp Console , inscreva-se ou faça login para acessá-la. O método de cadastro ou login depende se sua empresa utiliza federação de identidades ou possui credenciais do site de suporte da NetApp . Caso contrário, crie um login no NetApp Console .

Passos

1. Abra um navegador da web e vá para o "NetApp Console"
2. Se você possui uma conta no site de suporte da NetApp ou se sua empresa configurou o login único (SSO), insira seu endereço de e-mail associado ou suas credenciais de SSO na página **Entrar**. Siga as instruções para concluir o login.

   Em ambos os casos, você se inscreve no Console como parte desse login inicial.

3. Se você quiser se inscrever criando um login no Console, selecione **Inscrever-se**.
   a. Na página **Inscreva-se**, insira as informações necessárias e selecione **Avançar**.

      Somente caracteres em inglês são permitidos no formulário de inscrição.

   b. Verifique sua caixa de entrada para ver se recebeu um e-mail da NetApp com instruções para verificar seu endereço de e-mail.

      Verifique seu endereço de e-mail para concluir o cadastro.

4. Após efetuar o login, revise e aceite o Contrato de Licença do Usuário Final.
5. Se o sistema solicitar que você crie uma organização, feche a caixa de diálogo e informe um administrador do Console para que ele possa adicioná-lo à sua organização do Console e conceder-lhe acesso. "Aprenda como entrar em contato com um administrador da organização."

Próximos passos

Após receber acesso à sua organização, você poderá começar a gerenciar o armazenamento e usar os serviços de dados que lhe forem atribuídos.

Gerenciar parcerias organizacionais

Parcerias no NetApp Console

A criação de parcerias entre organizações no NetApp Console permite que os parceiros gerenciem recursos da NetApp com segurança, ultrapassando as fronteiras organizacionais, simplificando a colaboração e aprimorando a segurança.

Funções necessárias

Administrador de parceria"Saiba mais sobre funções de acesso."

As parcerias permitem o gerenciamento seguro de recursos da NetApp em todas as organizações usando relacionamentos baseados em funções no Console. A organização iniciadora concede acesso aos seus recursos, enquanto a organização aceitante fornece os usuários ou contas de serviço aos quais será concedido acesso. As parcerias são estabelecidas por meio de um fluxo de trabalho de autoatendimento, dando à organização iniciadora controle total sobre quais recursos são compartilhados, quais funções são atribuídas e a capacidade de integrar, gerenciar ou revogar o acesso do parceiro conforme necessário.

Os clientes podem autorizar MSPs ou revendedores a gerenciar ambientes NetApp sem precisar de configurações complicadas. Os clientes podem controlar quais clusters os parceiros podem acessar e quais funções eles têm, e podem revogar o acesso a qualquer momento para manter a segurança e a conformidade.

Como parceiro, você obtém visibilidade e controle centralizados em todos os ambientes do cliente. Você pode facilmente mudar para a organização de um cliente para gerenciar recursos, executar serviços de dados e monitorar a integridade dentro de limites definidos, reduzindo ferramentas personalizadas e garantindo o alinhamento com as políticas de cada cliente.

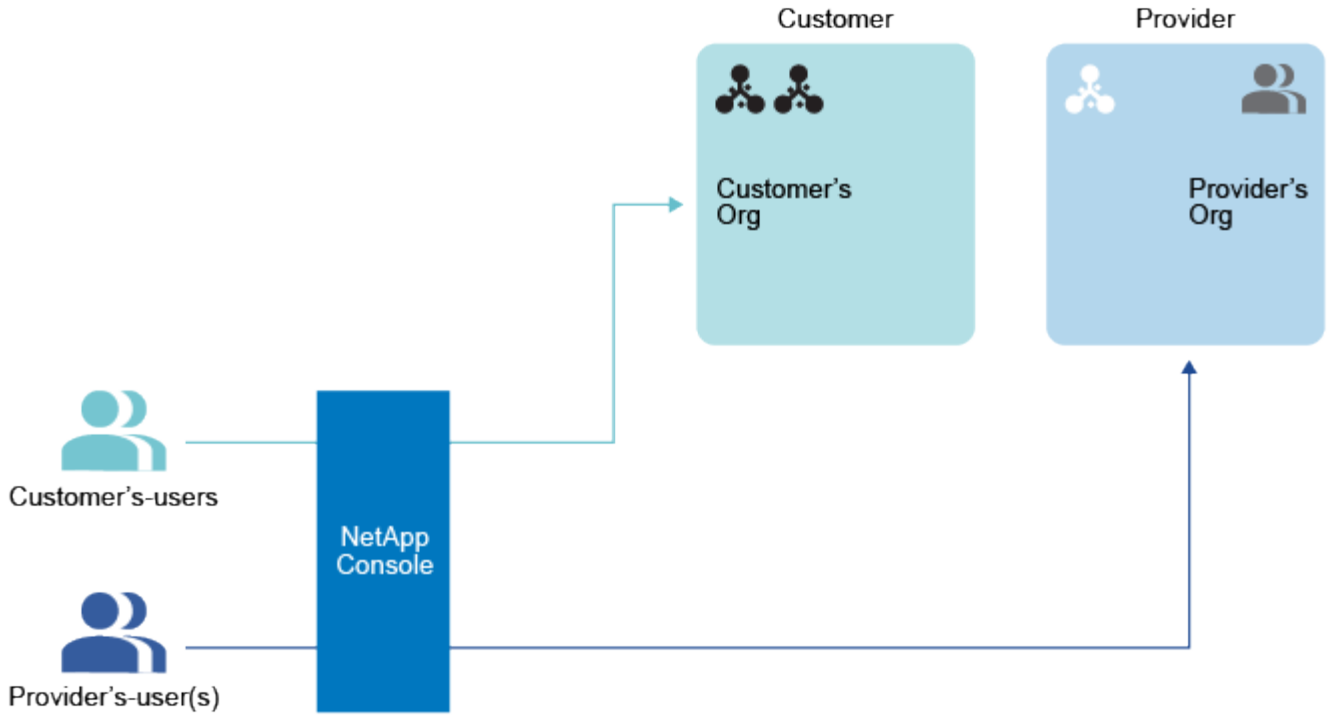
1. **Atribuir a um ou mais usuários a função de administrador de parceria**

Atribua a um ou mais usuários nas organizações iniciadora e receptora a função de administrador de parceria para criar e gerenciar parcerias. Você pode atribuir a função de visualizador de parceria a usuários que precisam apenas visualizar parcerias, e não gerenciá-las.

2. **Compartilhe o ID da sua organização com a organização iniciadora**

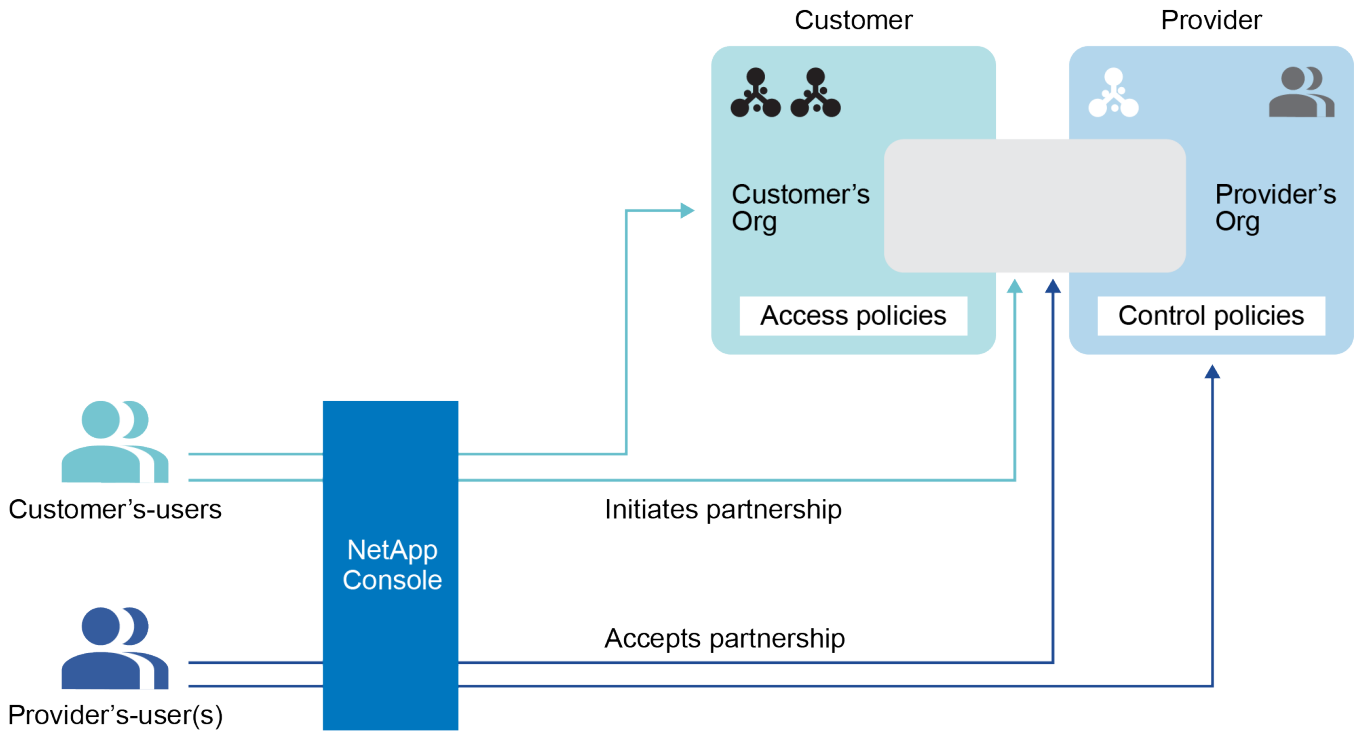
Para iniciar uma parceria, o iniciador deve saber o ID da organização alvo. Somente a respectiva organização pode acessar este ID da organização. Compartilhe-o diretamente com a organização iniciadora fora do NetApp Console por e-mail ou outro método.

A organização iniciadora é a organização que concede acesso aos seus recursos.



3 Iniciar a parceria dentro do NetApp Console

A organização que inicia a parceria o faz no NetApp Console enviando uma solicitação de parceria.



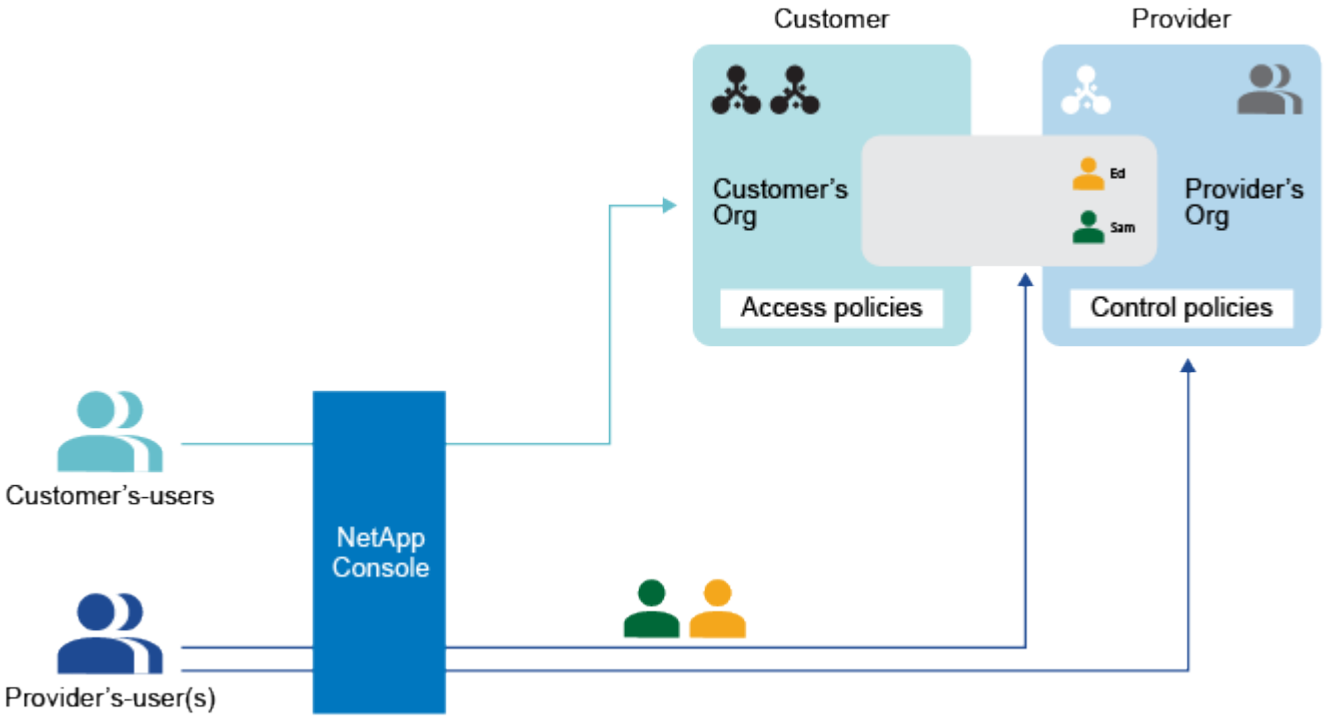
4 Aprovar a parceria

A organização receptora deve aceitar a solicitação.

A organização receptora é a organização que está recebendo acesso aos recursos.

5 Atribuir usuários à parceria

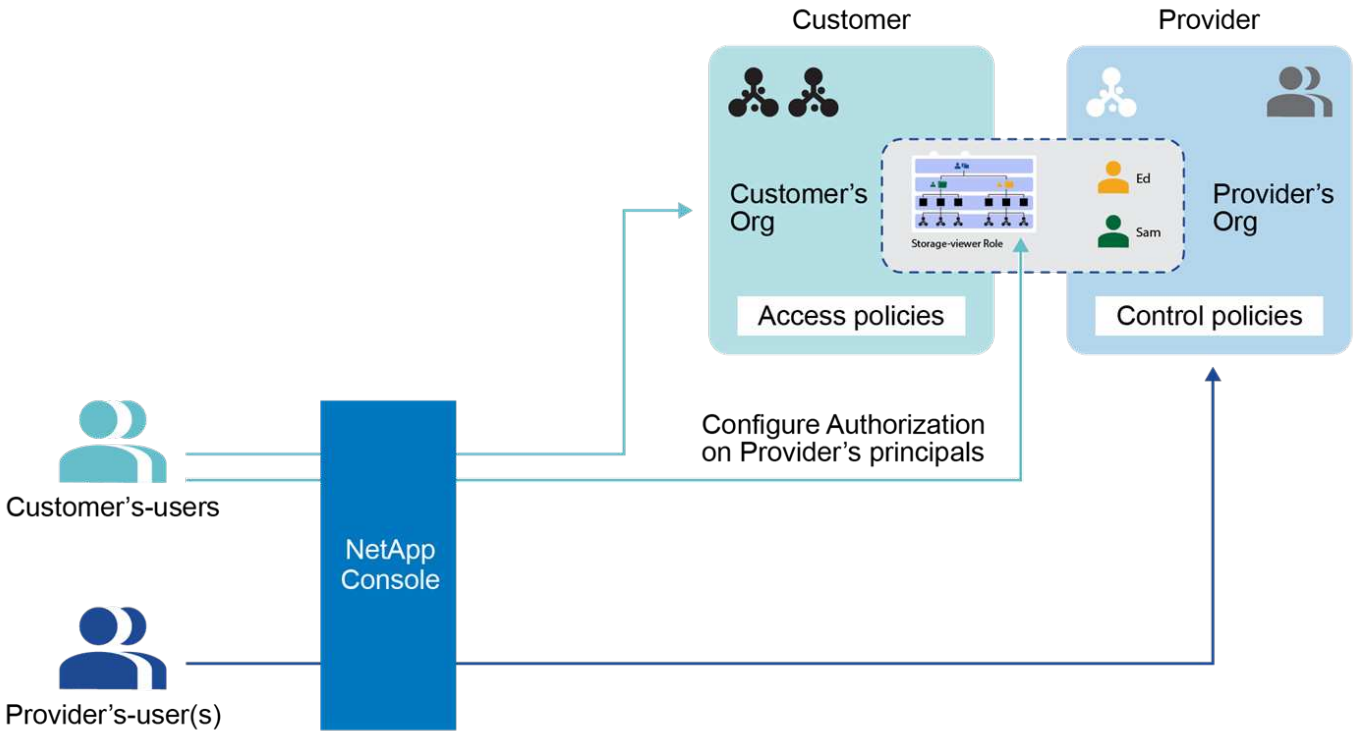
A organização receptora atribui usuários ou contas de serviço específicos da sua organização à parceria. A organização iniciadora atribui funções a esses usuários.



6 Conceder aos usuários atribuídos acesso aos recursos

Se você for a organização iniciadora, poderá conceder acesso a recursos específicos aos usuários que foram atribuídos à parceria. Você pode revogar o acesso a qualquer momento.

Você faz isso atribuindo funções para projetos ou pastas específicos dentro da sua organização.



Gerenciar parcerias no NetApp Console

Crie parcerias para estabelecer conexões seguras e gerenciadas entre sua organização e parceiros confiáveis para gerenciamento colaborativo de recursos do NetApp .

As parcerias permitem que você gerencie com segurança os recursos do NetApp em todos os limites com relacionamentos baseados em funções no Console. A organização iniciadora concede acesso aos seus recursos, enquanto a organização aceitante fornece os usuários ou contas de serviço aos quais será concedido acesso. As parcerias são estabelecidas por meio de um fluxo de trabalho de autoatendimento, dando à organização iniciadora controle total sobre quais recursos são compartilhados, quais funções são atribuídas e a capacidade de integrar, gerenciar ou revogar o acesso do parceiro conforme necessário.

Funções necessárias

A função **Administrador de parceria** é necessária para criar e gerenciar parcerias. O **Visualizador de Parcerias** pode visualizar a página Parcerias."Saiba mais sobre funções de acesso."

Iniciar uma parceria organizacional

Você pode solicitar uma parceria com outra organização se souber o ID da organização. A organização receptora aprova a solicitação antes que a parceria possa prosseguir.

Antes de começar, certifique-se de ter o ID da organização parceira e de que você recebeu a função de **Administrador da parceria**.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione a aba **Parcerias**.
3. Selecione **Adicionar parceria**.

4. Na caixa de diálogo **Criar parceria**, insira o ID da organização parceira do parceiro solicitado e selecione **Adicionar**.

   A solicitação de parceria é enviada à organização parceira para aprovação. Você pode visualizar o status da solicitação de parceria na página **Parcerias**.

Aprovar uma parceria organizacional

Uma solicitação de parceria de organização deve ser aceita pela organização receptora antes que a parceria possa prosseguir. Você deve ter a função **Administrador de parceria** para aprovar e gerenciar parcerias.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Navegue até a parceria recebida que deseja aprovar e selecione ••• e então selecione **Aprovar**.
5. Revise os detalhes da parceria, incluindo o nome e o ID da organização que solicitou a parceria e selecione **Avançar.**
6. Opcionalmente, adicione membros da organização à parceria e selecione **Aplicar**.

   Você pode adicionar membros adicionais por meio da página **Parceria** a qualquer momento.

   Todos os membros que você adicionar ficarão visíveis na organização do parceiro, onde o parceiro poderá atribuí-los aos recursos.

Resultado

A parceria que você aprovou agora mostra o status **Estabelecida**. Usuários com as funções **Administrador de parceria** ou **Visualizador de parceria** em qualquer organização podem visualizar a parceria.

Ver status da parceria

Veja o status das suas parcerias.

Função necessária

Administrador de parceria, visualizador de parceria."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parcerias iniciadas** ou **Parcerias recebidas**.
4. Revise a tabela respectiva que exibe as parcerias e seus status.

Desabilitar uma parceria de organização

Você deve ser membro da organização iniciadora para desabilitar uma parceria. Desabilitar uma parceria revoga imediatamente o acesso a quaisquer recursos na sua organização que foram compartilhados com a organização parceira.

Função necessária

Administração de parcerias."Saiba mais sobre funções de acesso."

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parcerias iniciadas**.
4. Revise a tabela respectiva que exibe as parcerias e seus status.
5. Navegue até a parceria iniciada que deseja desabilitar e selecione ••• e então selecione **Desativar**.

Gerenciar membros de uma organização parceira

Você pode adicionar usuários a uma parceria adicionando-os à organização parceira. Depois de adicionar usuários, a organização parceira é responsável por atribuir a eles funções para recursos específicos em sua organização.

Funções necessárias

A função **Administrador de parceria** é necessária para criar e gerenciar parcerias. O **Visualizador de Parcerias** pode visualizar a página Parcerias."Saiba mais sobre funções de acesso."

Você pode remover usuários de uma parceria a qualquer momento. Remover um usuário de uma parceria revoga imediatamente seu acesso a quaisquer recursos na organização parceira.

Adicionar membros a uma parceria

Ao adicionar membros a uma parceria, o **administrador da parceria** da organização parceira deve atribuir a eles funções para recursos específicos na organização antes que eles possam acessá-los.

Depois de adicionar membros a uma parceria, os membros são exibidos como membros na organização parceira, onde o parceiro pode atribuí-los aos recursos.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja incluir como membros e selecione **Adicionar membros**.
5. Escolha um ou mais membros para adicionar à parceria e selecione **Adicionar**.

Remover membros de uma parceria

Você pode remover membros de uma parceria a qualquer momento. Remover um usuário de uma parceria revoga imediatamente seu acesso a quaisquer recursos na organização parceira.

Se você quiser ajustar a função de um membro ou os recursos que ele pode acessar, o administrador da Parceria da organização parceira deverá fazer essas alterações.

Passos

1. Selecione **Administração > Identidade e acesso**.

2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Selecione o menu de ações ••• ao lado do membro que você deseja remover e selecione **Remover associação**.
5. Confirme a ação selecionando **Remover** na caixa de diálogo.

Exibir informações de função de um usuário

Você pode visualizar a função que foi atribuída a um usuário e os recursos associados.

Você não pode alterar a função associada a um usuário. Se você tiver dúvidas sobre os recursos ou a função fornecida, entre em contato com o administrador da organização parceira.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria recebida**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
5. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja visualizar a função atribuída ao membro e selecione o número na coluna **Função**.

Fornecer acesso a recursos para usuários de parceria

Você pode conceder acesso a usuários de parceria atribuindo a eles funções específicas para pastas e projetos dentro da sua organização.

Funções necessárias

Administração de parcerias."Saiba mais sobre funções de acesso."

Uma organização parceira deve primeiro adicionar membros à parceria antes que você possa atribuir a eles funções para recursos em sua organização."Aprenda como adicionar membros a uma parceria."

Entenda as funções dos usuários da parceria

Você pode gerenciar funções para membros de organizações parceiras da mesma forma que faz para as suas. No entanto, nem todas as funções estão disponíveis para usuários de parceria. Em particular, você não pode conceder aos usuários parceiros uma função que permita atualizações de software. A atualização do software ONTAP geralmente requer acesso direto à rede.

Você pode atribuir as seguintes funções aos usuários parceiros:

- "Administrador da organização"
- "Administrador de pasta ou projeto"
- "Administrador da Federação"
- "Visualizador da Federação"
- "Administrador de backup e recuperação"
- "Visualizador de backup"

- "Restaurar administrador"
- "Clonar administrador"
- "Administrador de recuperação de desastres"
- "Administrador de failover de recuperação de desastres"
- "Administrador do aplicativo de recuperação de desastres"
- "Visualizador de recuperação de desastres"
- "Analista de suporte de operações"
- "Visualizador de classificação"

"Saiba mais sobre funções predefinidas"

Adicionar uma função a um usuário parceiro

Você fornece acesso aos recursos da sua organização adicionando uma função a um membro. Ao atribuir uma função, você especifica um recurso e uma função. Você pode atribuir mais de uma função a um usuário.

Por exemplo, se você tivesse dois projetos e quisesse que o mesmo usuário tivesse a função de administrador de backup e recuperação para ambos, seria necessário fornecer a função ao usuário para cada projeto. Da mesma forma, se você quisesse fornecer a um usuário duas funções diferentes para o mesmo projeto, seria necessário atribuir cada função separadamente.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria iniciada**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja visualizar e selecione **Ver detalhes**.

   A lista **Membros** exibe os membros que a organização parceira adicionou à parceria.

5. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
6. Para adicionar uma função, conclua as etapas na caixa de diálogo:
   - **Selecione uma organização, pasta ou projeto**: Escolha o nível da hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que reside na organização ou pasta.

   - **Selecione uma categoria**: Escolha uma categoria de função. "Saiba mais sobre funções de acesso" .
   - Selecione uma **Função**: Escolha uma função que forneça ao membro permissões para os recursos associados à organização, pasta ou projeto que você selecionou.
   - **Adicionar função**: se você quiser fornecer acesso a pastas ou projetos adicionais dentro da sua organização, selecione **Adicionar função**, especifique outra pasta, projeto ou categoria de função e, em seguida, selecione uma categoria de função e uma função correspondente.
7. Selecione **Adicionar novas funções**.

Alterar ou remover uma função de um usuário parceiro

Você pode alterar ou remover uma função que atribuiu a um membro de uma organização parceira.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Parcerias**.
3. Selecione a aba **Parceria iniciada**.
4. Selecione o menu de ações ••• ao lado da parceria estabelecida que você deseja visualizar e selecione **Ver detalhes**.

   A lista **Membros** exibe os membros que a organização parceira adicionou à parceria.

5. Na página **Membros**, navegue até um membro na tabela, selecione ••• e então selecione **Ver detalhes**.
6. Na tabela, expanda a linha respectiva da organização, pasta ou projeto onde você deseja alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a este membro.
7. Você pode alterar uma função existente para um membro ou remover uma função.
   a. Para alterar a função de um membro, selecione **Alterar** ao lado da função que deseja alterar. Você só pode alterar uma função para uma função dentro da mesma categoria de função. Por exemplo, você pode mudar de uma função de serviço de dados para outra. Confirme a alteração.
   b. Para remover a função de um membro, selecione 🗑 Ao lado da função, clique para remover a respectiva função do membro. Você precisará confirmar a remoção.

Trabalhar em uma organização parceira

Depois de receber uma função em uma organização parceira, você pode alternar para essa organização e executar ações para as quais tem permissão.

Use o menu Organização para alternar entre suas organizações e quaisquer organizações parceiras às quais você tenha acesso."Saiba mais sobre como mudar de organização e projeto."

Você poderá ver os recursos que foram compartilhados com você na organização parceira e executar ações com base na função que foi atribuída a você. Trabalhe com seu administrador de parceria para garantir que você tenha a função apropriada para os recursos que precisa acessar.

Monitorar as operações do NetApp Console

Você pode monitorar o status das operações que o Console está executando para ver se há algum problema que precisa ser resolvido. Você pode visualizar o status na página Auditoria, na Central de Notificações ou receber notificações por e-mail.

A tabela destaca os recursos da página Auditoria e do Centro de Notificações comparando-os.

Central de Notificações	Página de auditoria
Mostra status de alto nível para eventos e ações	Fornece detalhes de cada evento ou ação para investigação posterior

Central de Notificações	Página de auditoria
Mostra o status da sessão de login atual (as informações não aparecem na Central de Notificações depois que você faz logoff)	Mantém o status do último mês
Mostra apenas ações iniciadas na interface do usuário	Mostra todas as ações da IU ou APIs
Mostra ações iniciadas pelo usuário	Mostra todas as ações, sejam elas iniciadas pelo usuário ou pelo sistema
Filtrar resultados por importância	Filtrar por serviço, ação, usuário, status e muito mais
Oferece a capacidade de enviar notificações por e-mail aos usuários e a outras pessoas	Sem capacidade de e-mail

Auditar a atividade do usuário na página Auditoria

Use a página Auditoria para identificar quem executou uma ação ou seu status.

A página Auditoria mostra as ações que os usuários concluíram para gerenciar sua organização ou conta. Isso inclui ações de gerenciamento, como associação de usuários, criação de sistemas, criação de agentes e muito mais.

Você também pode verificar quem adicionou um membro a uma organização ou se um projeto foi excluído com sucesso.

Passos

1. Selecione **Administração > Auditoria**.
2. Use os filtros acima da tabela para alterar quais ações serão exibidas na tabela.

   Por exemplo, você pode usar o filtro **Serviço** para mostrar ações relacionadas a um serviço específico ou pode usar o filtro **Usuário** para mostrar ações relacionadas a uma conta de usuário específica.

Baixe os logs de auditoria da página Auditoria

Você pode baixar os logs de auditoria da página Auditoria para um arquivo CSV. Isso permite que você mantenha um registro das ações que os usuários realizam na sua organização. O arquivo CSV inclui todas as colunas no arquivo CSV baixado, independentemente dos filtros ou colunas exibidas na página Auditoria.

Passos

1. Na página **Auditoria**, selecione o ícone de download no canto superior direito da tabela.

Monitore atividades usando o Centro de Notificações

As notificações rastreiam as operações do Console para confirmar o sucesso. Eles permitem que você visualize o status de muitas ações do Console que você iniciou durante sua sessão de login atual. Nem todos os serviços do Console reportam informações ao Centro de Notificações.

Você pode exibir as notificações selecionando o sino de notificação () na barra de menu. A cor da pequena bolha no sino indica o nível de gravidade mais alto que está ativo. Então, se você vir uma bolha vermelha, significa que há uma notificação importante que você deve consultar.

Você também pode configurar o Console para enviar certos tipos de notificações por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conectado ao sistema. Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema. Veja comodefinir configurações de notificação por e-mail .

Comparando o Centro de Notificações com alertas

O Centro de Notificações permite que você visualize o status das operações iniciadas e configure notificações de alerta para determinados tipos de atividades do sistema. Enquanto isso, os alertas permitem que você visualize problemas ou riscos potenciais no seu ambiente de armazenamento ONTAP relacionados à capacidade, disponibilidade, desempenho, proteção e segurança.

"Saiba mais sobre os alertas do NetApp Console"

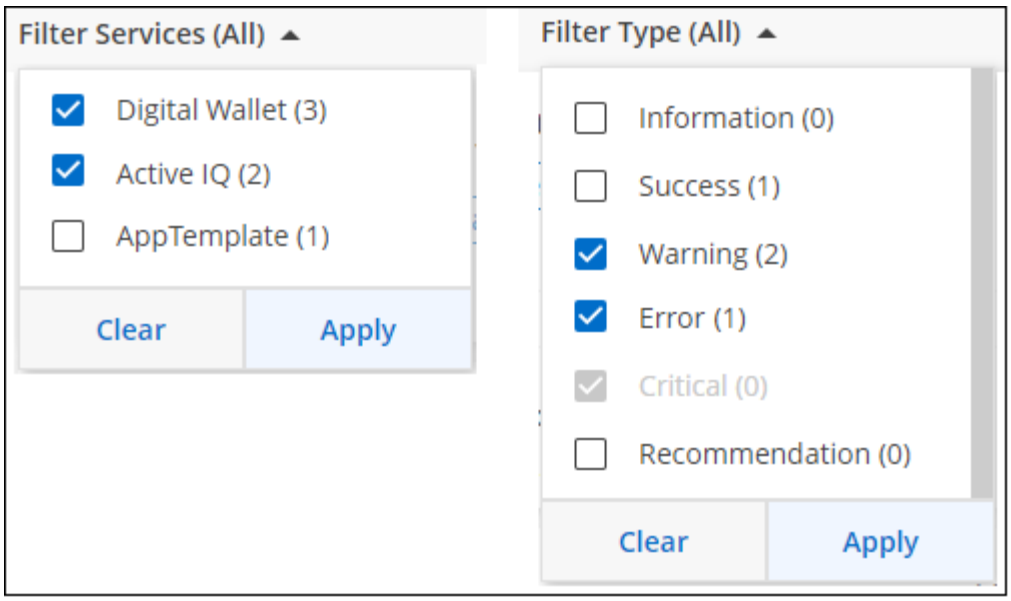
Tipos de notificação

O Console classifica as notificações nas seguintes categorias:

Tipo de notificação	Descrição
Crítico	Ocorreu um problema que pode levar à interrupção do serviço se uma ação corretiva não for tomada imediatamente.
Erro	Uma ação ou processo terminou em falha ou pode levar à falha se medidas corretivas não forem tomadas.
Aviso	Um problema que você deve estar ciente para garantir que ele não atinja a gravidade crítica. Notificações dessa gravidade não causam interrupção do serviço e pode não ser necessária ação corretiva imediata.
Recomendação	Uma recomendação do sistema para que você tome uma ação para melhorar o sistema ou um determinado serviço; por exemplo: economia de custos, sugestão de novos serviços, configuração de segurança recomendada, etc.
Informação	Uma mensagem que fornece informações adicionais sobre uma ação ou processo.
Sucesso	Uma ação ou processo concluído com sucesso.

Filtrar notificações

Por padrão, você verá todas as notificações ativas na Central de Notificações. Você pode filtrar as notificações que vê para mostrar apenas aquelas que são importantes para você. Você pode filtrar por "Serviço" e por "Tipo" de notificação.



Por exemplo, se você quiser ver apenas notificações de "Erro" e "Aviso" para operações do Console, selecione essas entradas e você verá apenas esses tipos de notificações.

Descartar notificações

Você pode remover notificações da página se não precisar mais vê-las. Você pode descartar notificações individualmente ou todas de uma vez.

Para descartar todas as notificações, na Central de Notificações, selecione ⋮ e selecione **Descartar tudo**.

Para descartar notificações individuais, passe o cursor sobre a notificação e selecione **Descartar**.

Definir configurações de notificação por e-mail

Você pode enviar tipos específicos de notificações por e-mail para ser informado sobre atividades importantes do sistema, mesmo quando não estiver conectado. Os e-mails podem ser enviados a qualquer usuário que faça parte da sua organização ou conta, ou a qualquer outro destinatário que precise estar ciente de certos tipos de atividade do sistema.

- O Console envia notificações por e-mail para o agente, licenças e assinaturas, NetApp Copy and Sync e NetApp Backup and Recovery.
- O envio de notificações por e-mail não é suportado quando o agente do Console está instalado em um site sem acesso à Internet.

Os filtros definidos na Central de Notificações não determinam os tipos de notificações que você recebe por e-mail. Por padrão, qualquer administrador da organização receberá e-mails para todas as notificações "Críticas" e "Recomendações". Essas notificações são válidas para todos os serviços. Você não pode optar por receber notificações apenas para determinados serviços, por exemplo, agentes ou NetApp Backup and Recovery.

Todos os outros usuários e destinatários estão configurados para não receber nenhum e-mail de notificação. Portanto, você precisará configurar as definições de notificação para quaisquer usuários adicionais.

Você deve ter a função de administrador da organização para personalizar as configurações de notificações.

Passos

1. Selecione **Administração > Configurações de notificações**.
2. Selecione **Usuários da organização** ou **Destinatários adicionais**.

   A página **Destinatários adicionais** permite que você configure o Console para notificar pessoas que são membros da sua organização do Console.

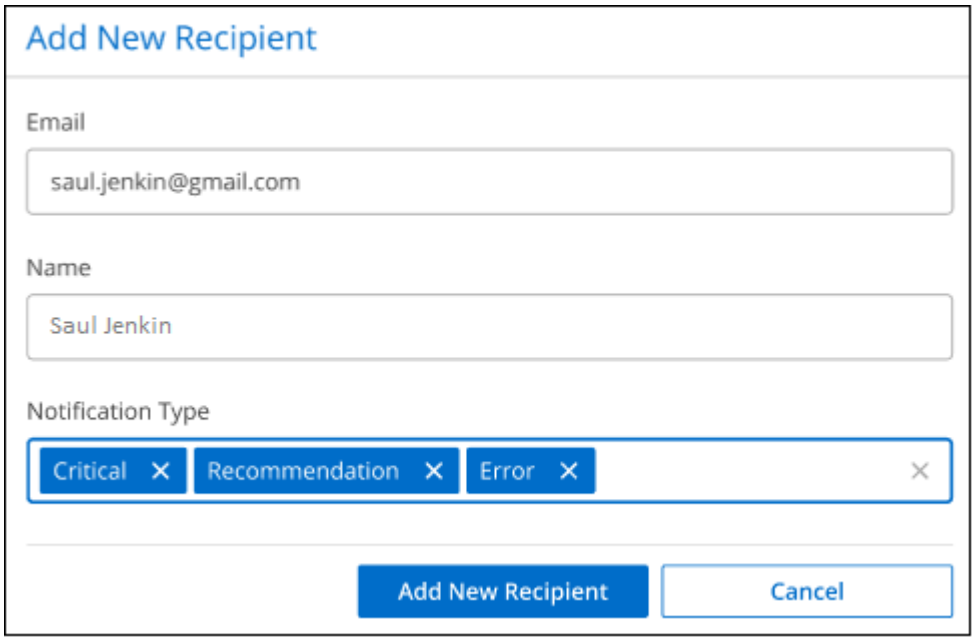
3. Selecione um usuário ou vários usuários na página *Usuários da organização* ou na página *Destinatários adicionais* e escolha o tipo de notificação a ser enviada:
   - Para fazer alterações para um único usuário, selecione o menu na coluna Notificações desse usuário, marque os tipos de Notificações a serem enviadas e selecione **Aplicar**.
   - Para fazer alterações para vários usuários, marque a caixa de cada usuário, selecione **Gerenciar notificações por e-mail**, marque os tipos de notificações a serem enviadas e selecione **Aplicar**.

Adicionar destinatários de e-mail adicionais

Os usuários que aparecem na página *Usuários da organização* são preenchidos automaticamente a partir dos usuários da sua organização ou conta. Você pode adicionar endereços de e-mail na página *Destinatários adicionais* para outras pessoas ou grupos que não têm acesso ao Console, mas que precisam ser notificados sobre determinados tipos de alertas e notificações.

Passos

1. Na página **Configurações de notificações**, selecione **Adicionar novos destinatários**.



2. Digite o nome, endereço de e-mail, selecione os tipos de notificações que o destinatário receberá e selecione **Adicionar novo destinatário**.

Informações sobre direitos autorais

Informações sobre marcas comerciais