Instalar um agente no local

NetApp Console setup and administration

NetApp
February 11, 2026

Índice

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 .

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

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

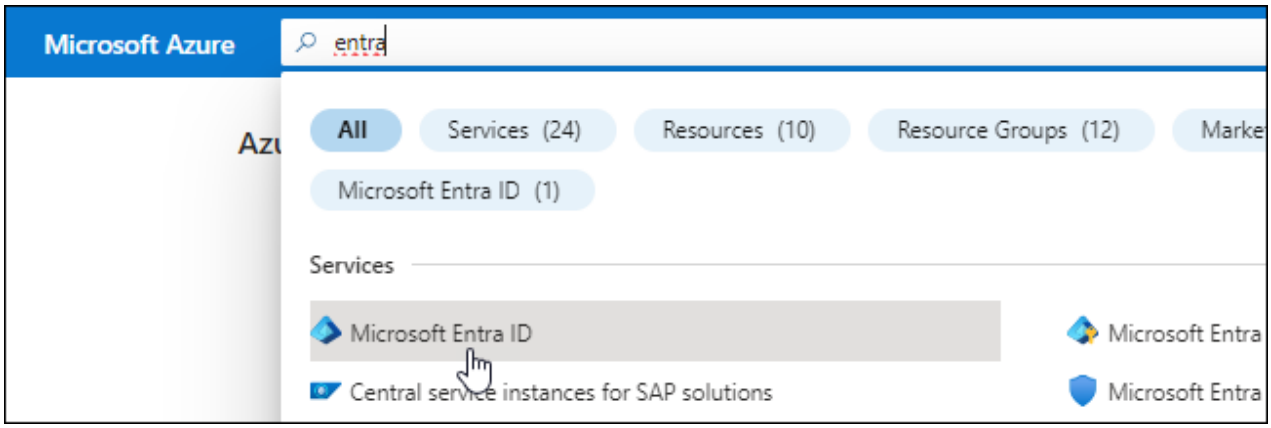
Quando o agente do Console é instalado no local, você precisa fornecer ao agente do Console permissões do Azure configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

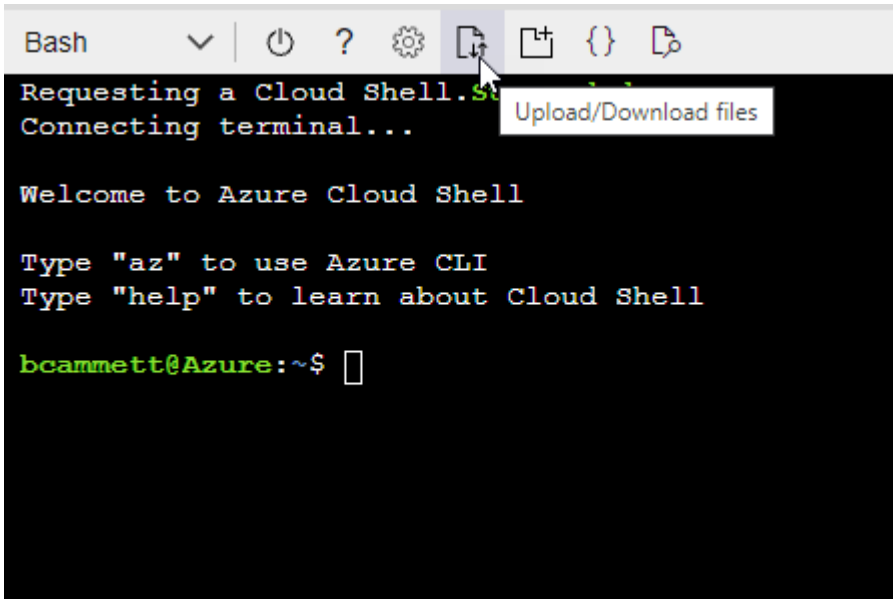
      Exemplo

```
"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:

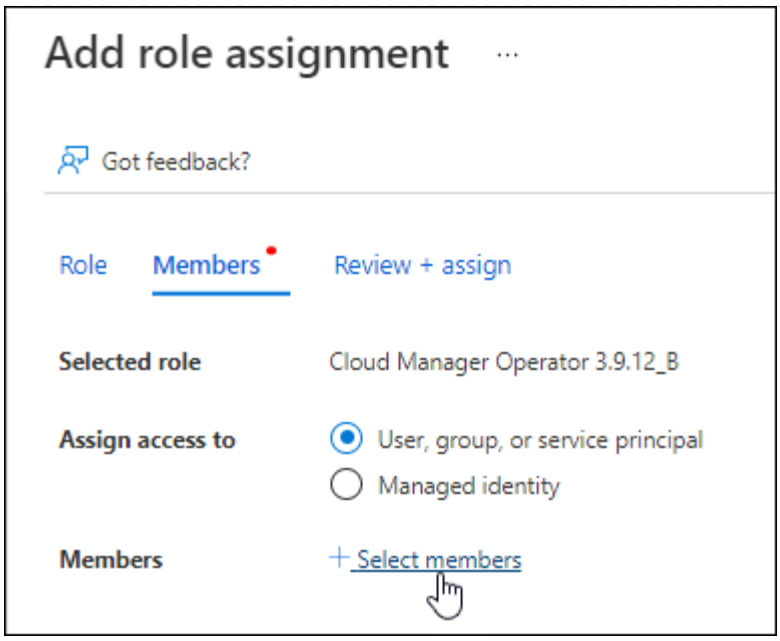
```
az role definition create --role-definition agent_Policy.json
```

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:

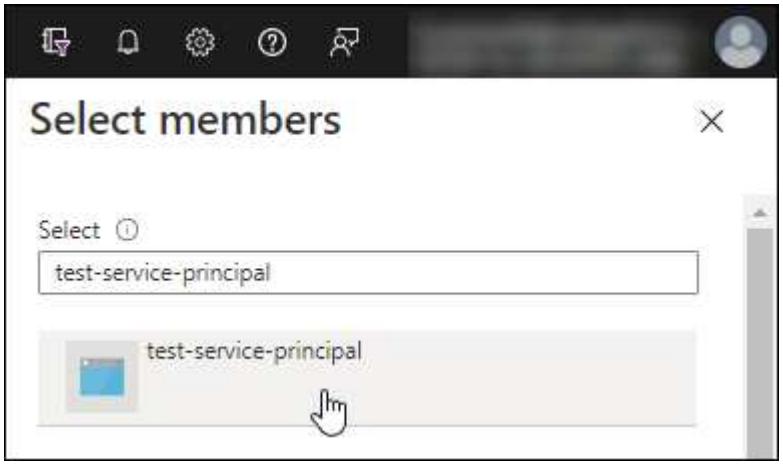
   a. No portal do Azure, abra o serviço **Assinaturas**.
   b. Selecione a assinatura.
   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.
   e. Na aba **Membros**, complete 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**.

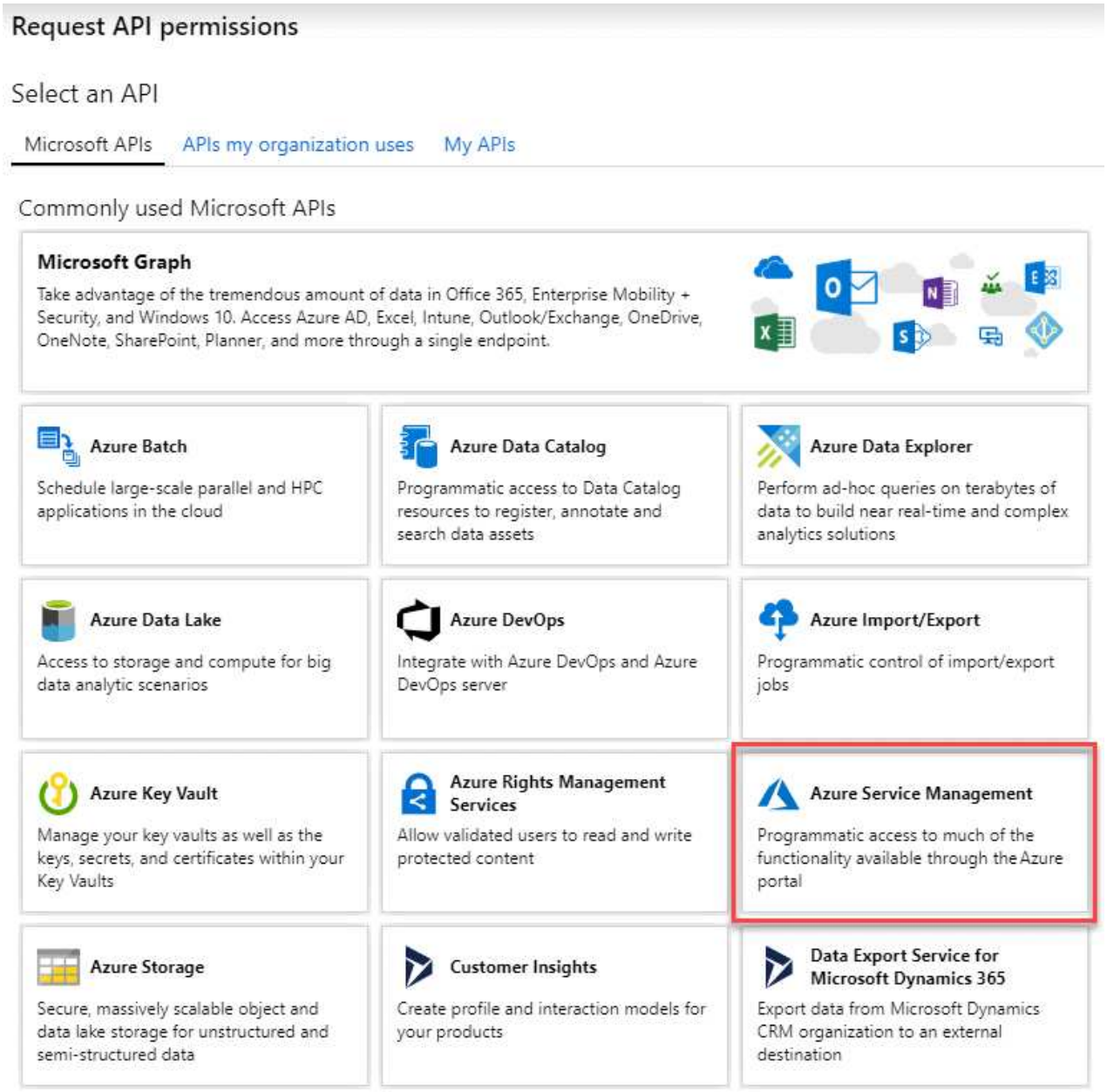
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

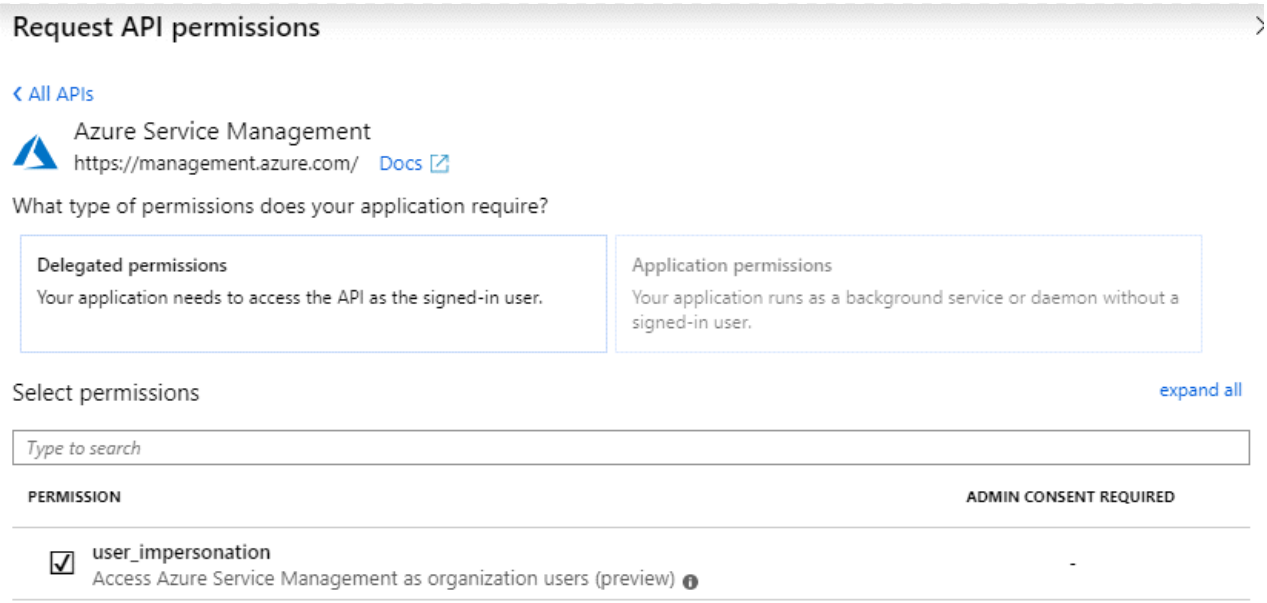
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

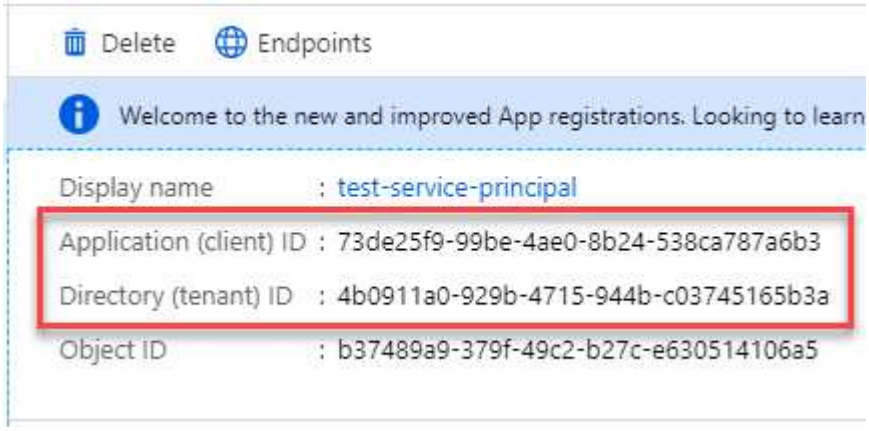


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

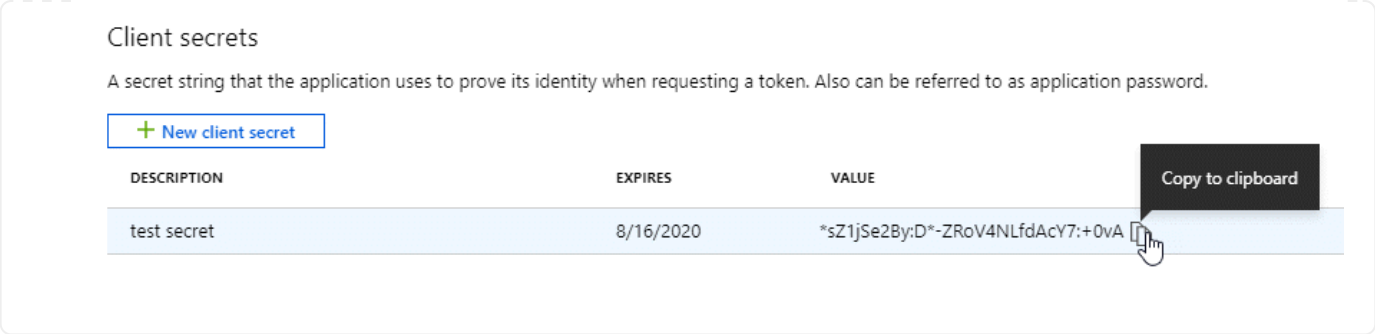
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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 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
```

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

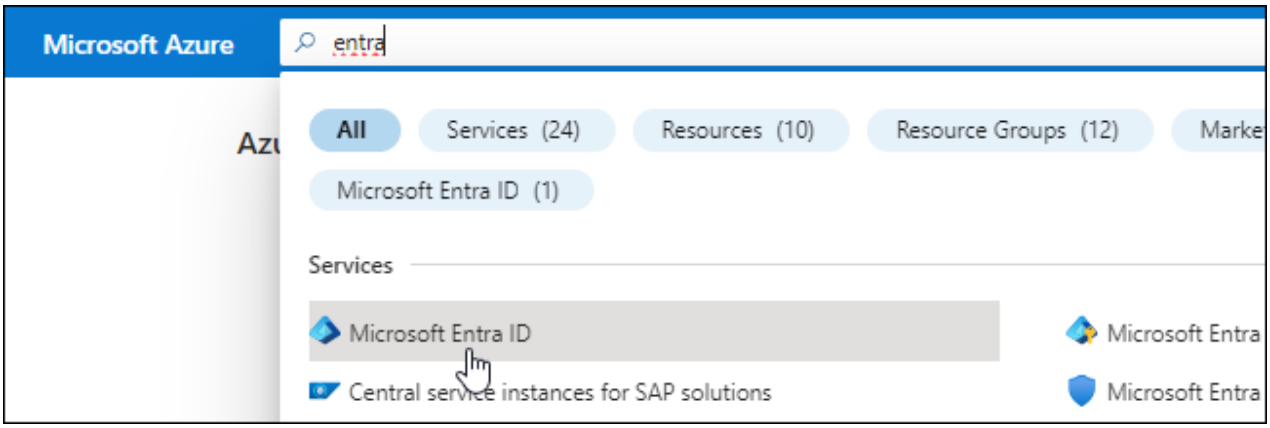
Quando o agente do Console estiver instalado no local, você precisará conceder permissões do Azure ao agente do Console configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

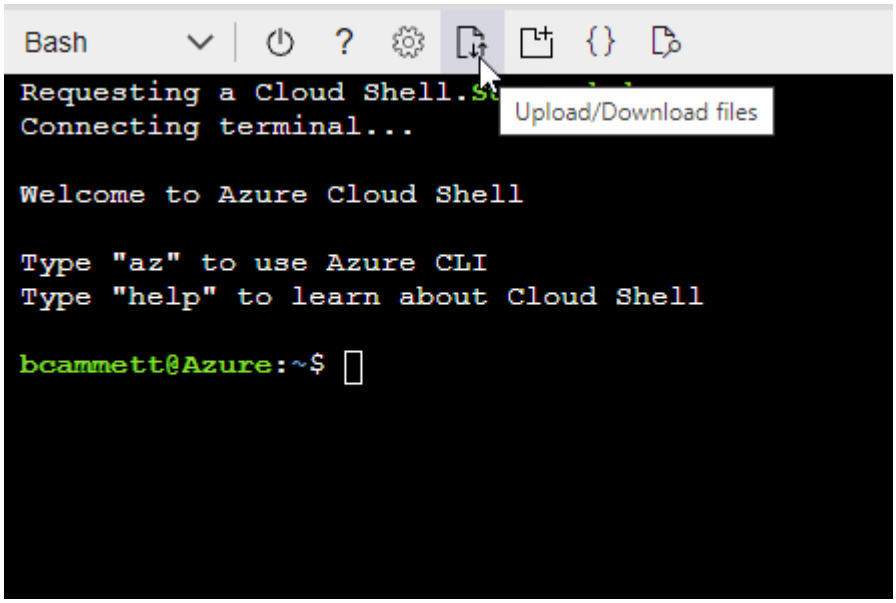
      Exemplo

```
"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**.

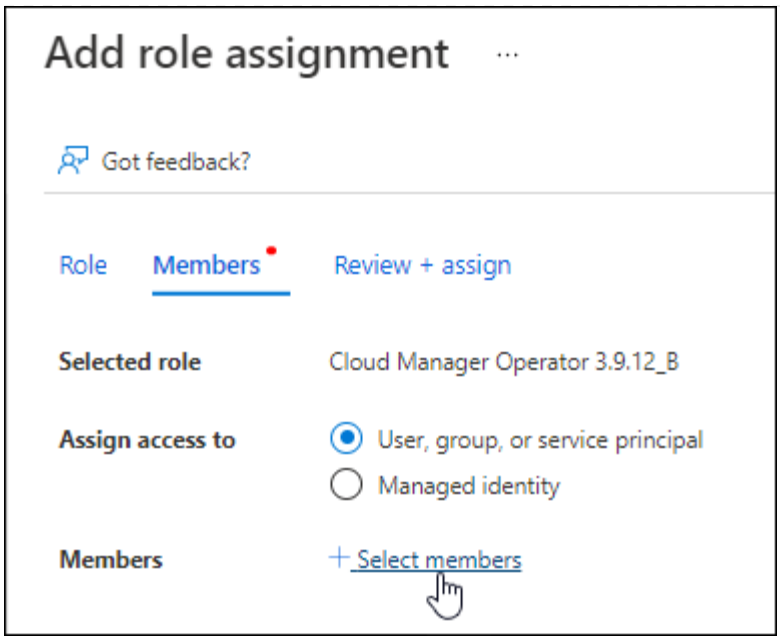
   b. Selecione a assinatura.

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

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

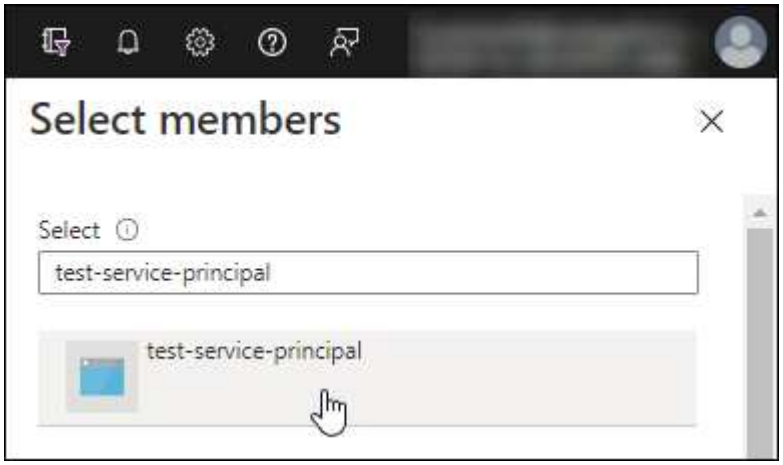
   e. Na aba **Membros**, complete os seguintes passos:

   - 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**.

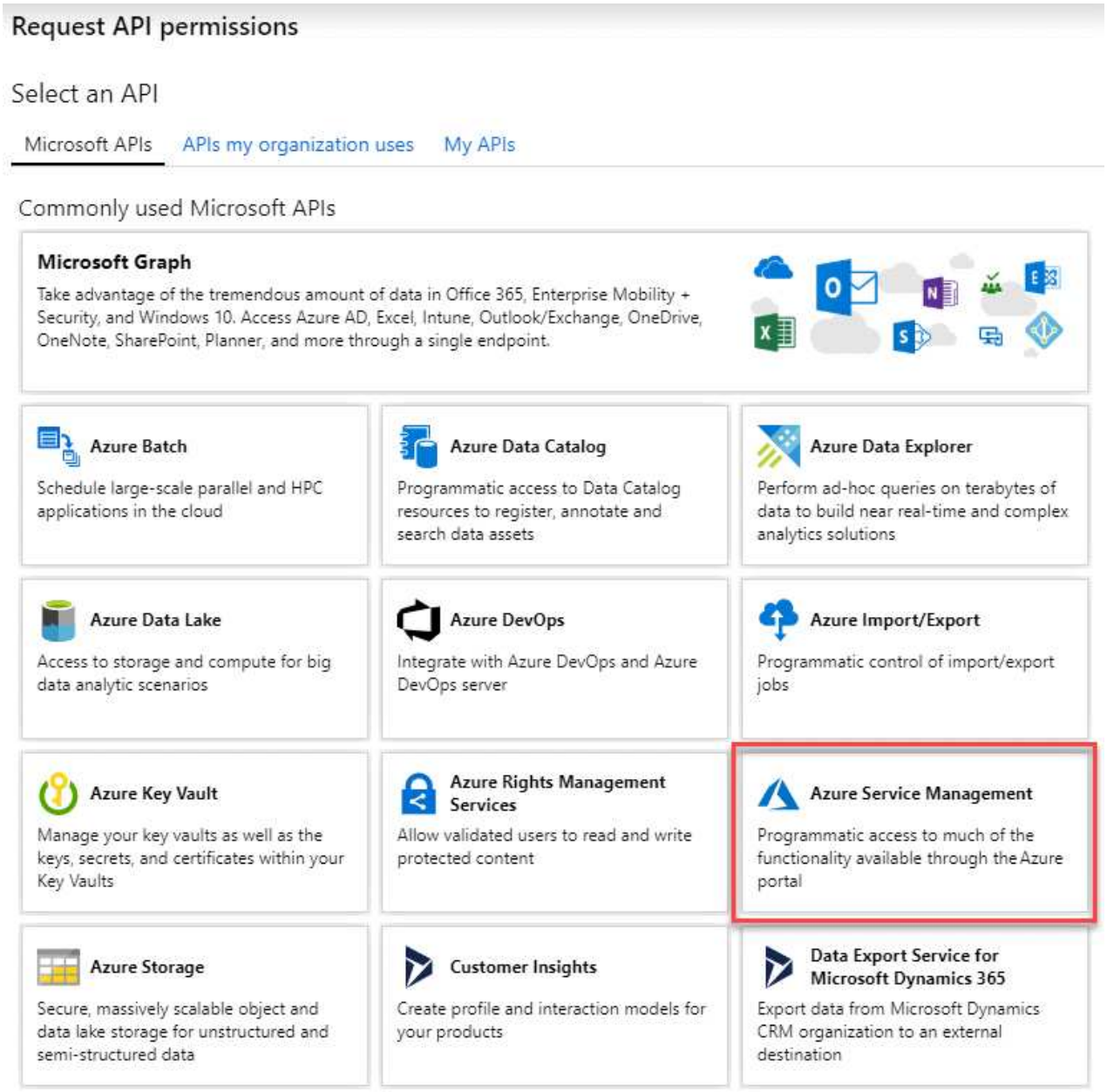
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

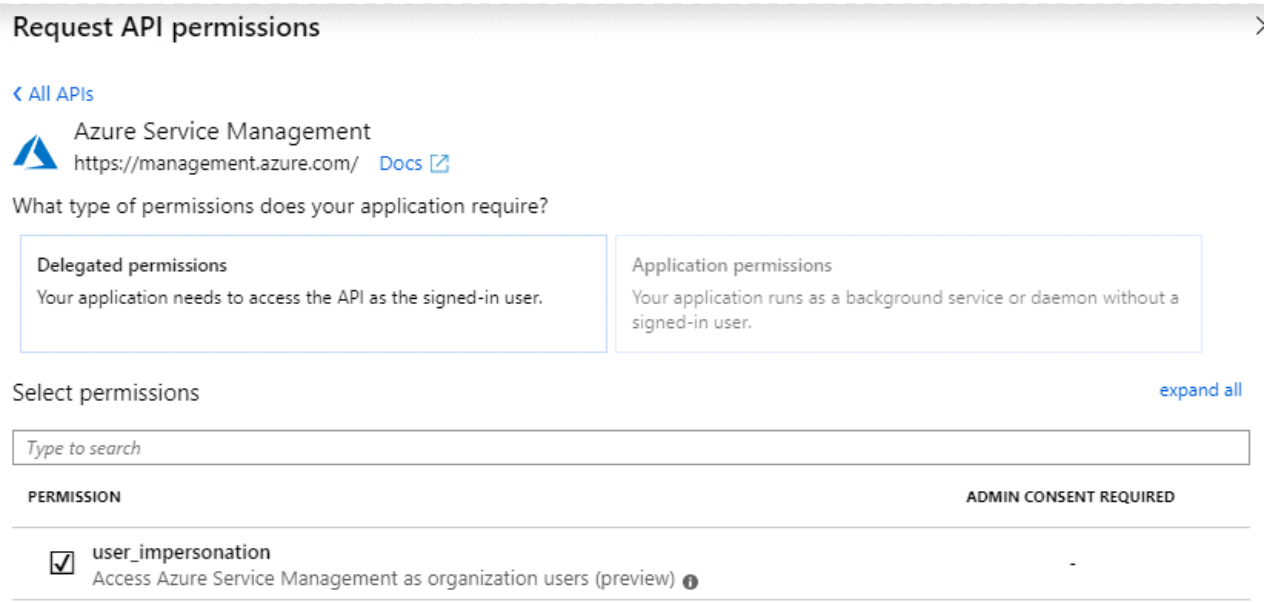
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

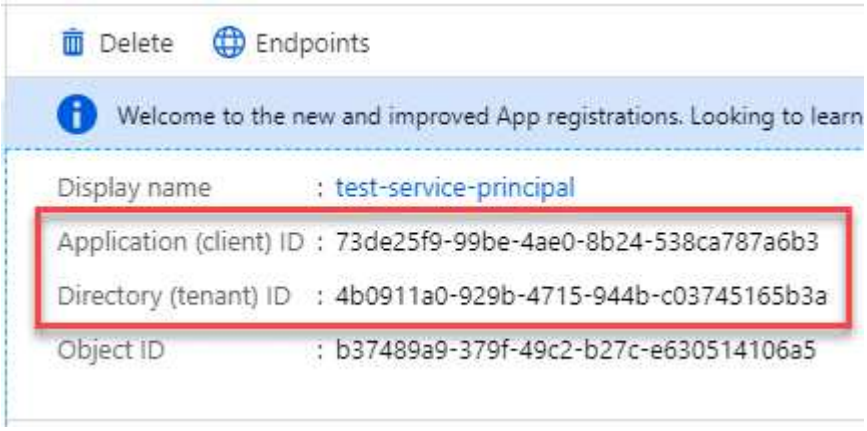


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

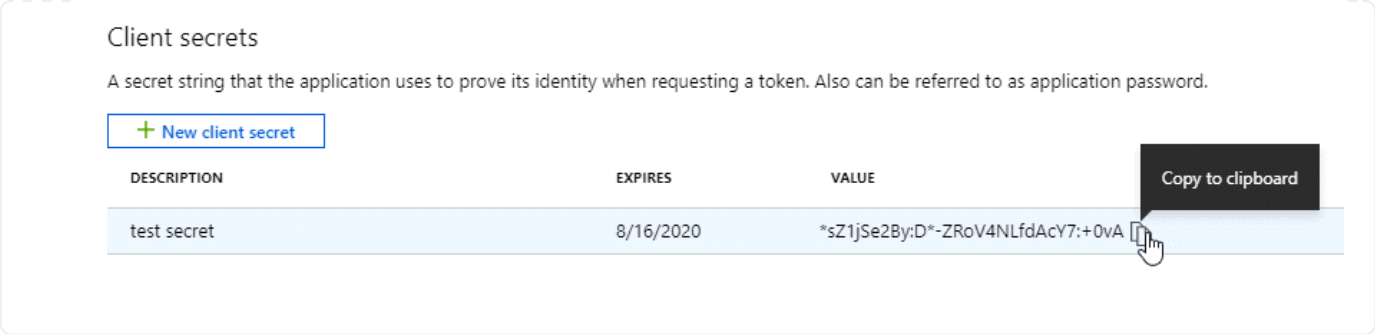
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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

Informações sobre direitos autorais

Informações sobre marcas comerciais