Implantar um agente de console

NetApp Console setup and administration

NetApp
February 11, 2026

Índice

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.

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.

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"

Pontos finais	Propósito
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.

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.

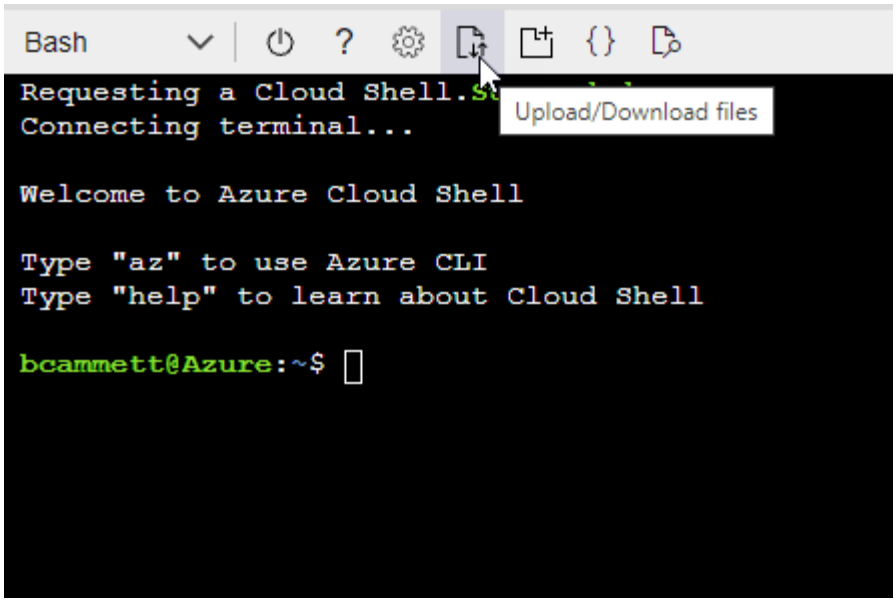
   Exemplo

```
"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.

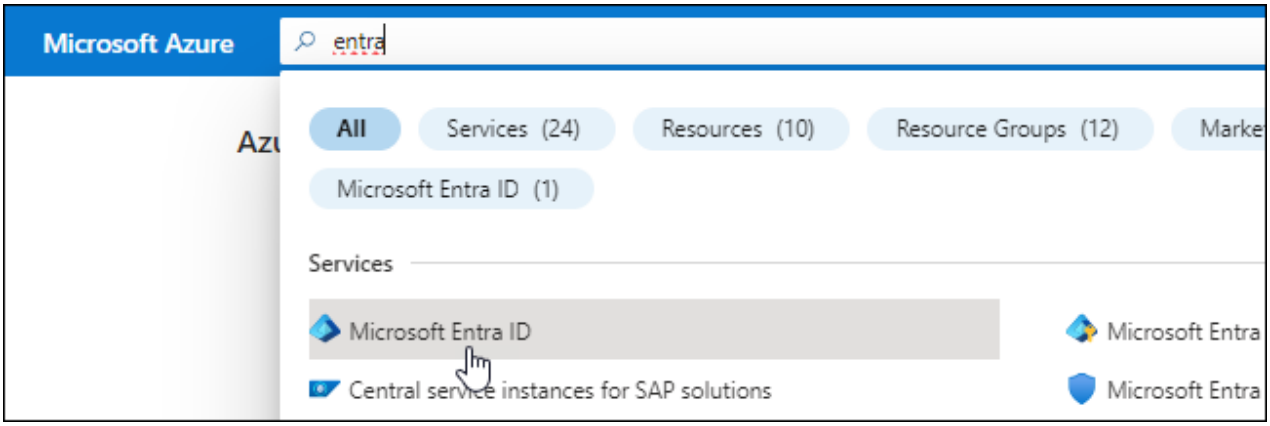
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

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**.

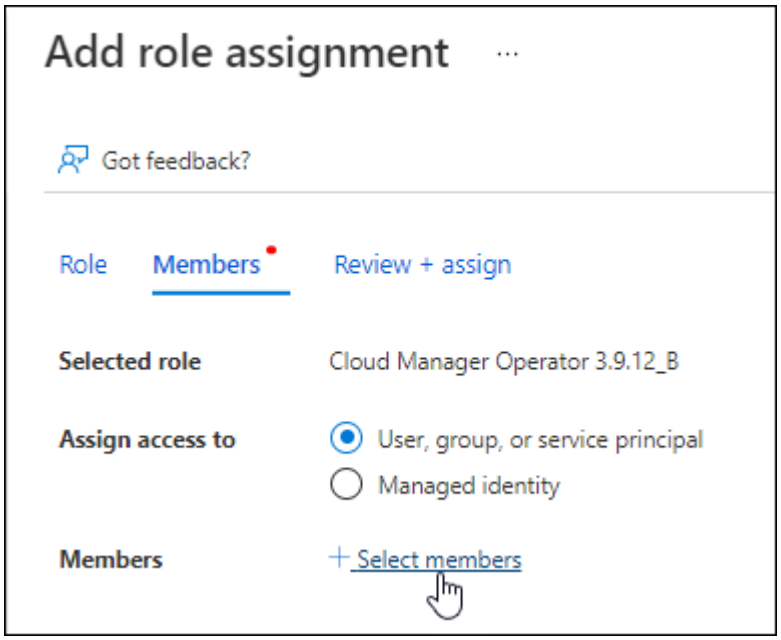
   Você criou o aplicativo AD e a entidade de serviço.

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:

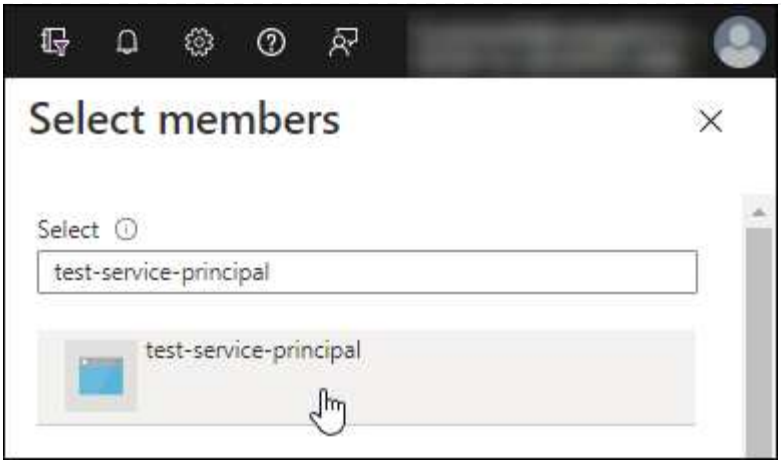
   a. Mantenha **Usuário, grupo ou entidade de serviço** selecionado.

   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**.

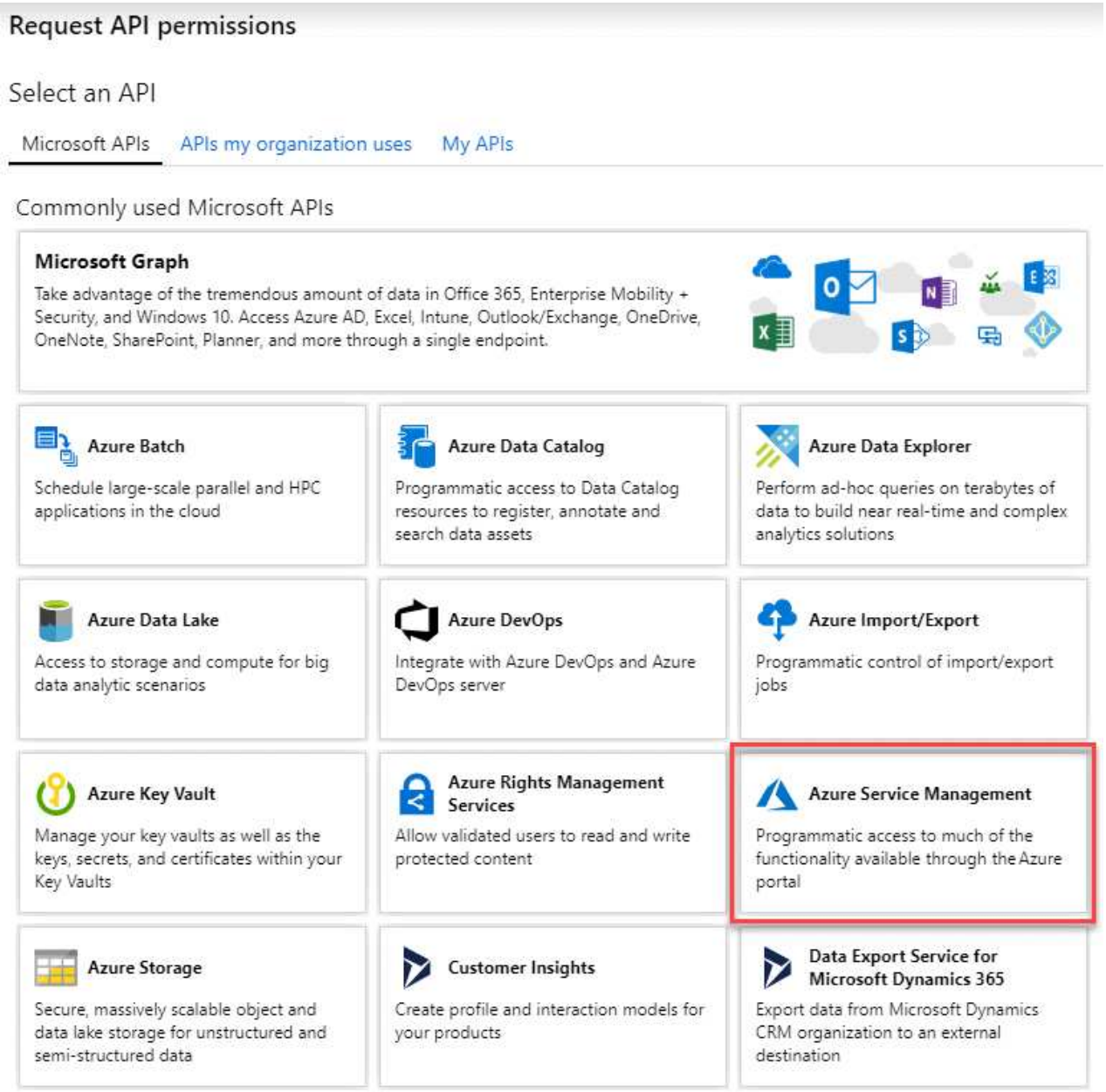
6. Clique em **Revisar + atribuir**.

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

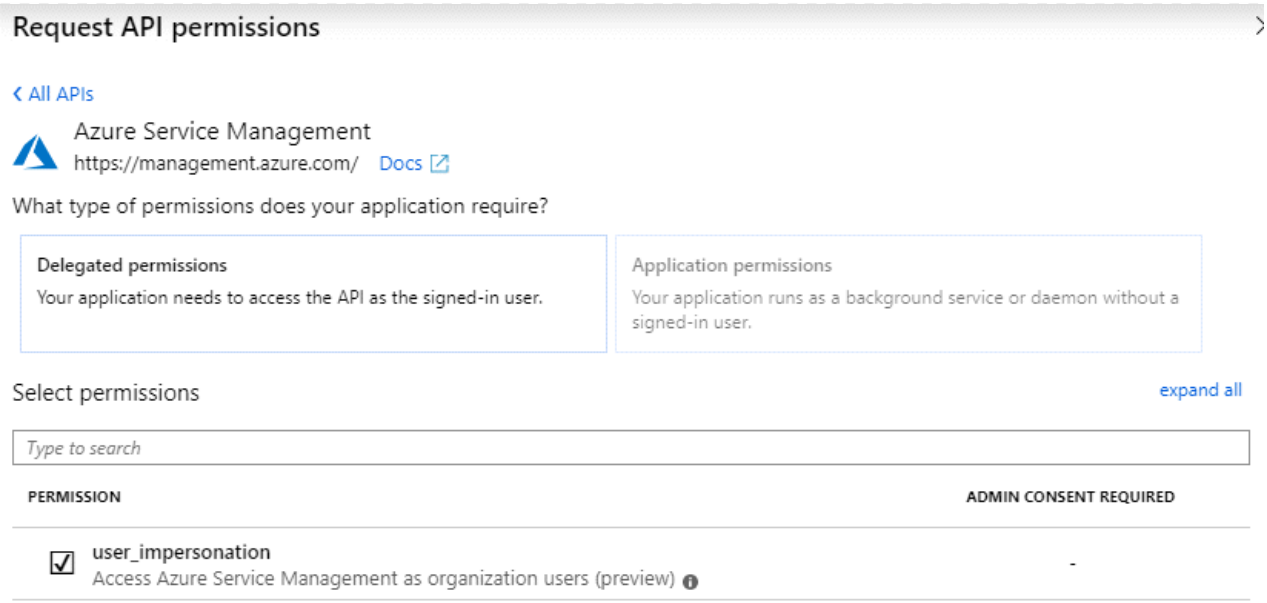
   Se você quiser gerenciar recursos em várias assinaturas do Azure, deverá vincular a entidade de serviço a cada uma dessas assinaturas. Por exemplo, o Console permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

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**.

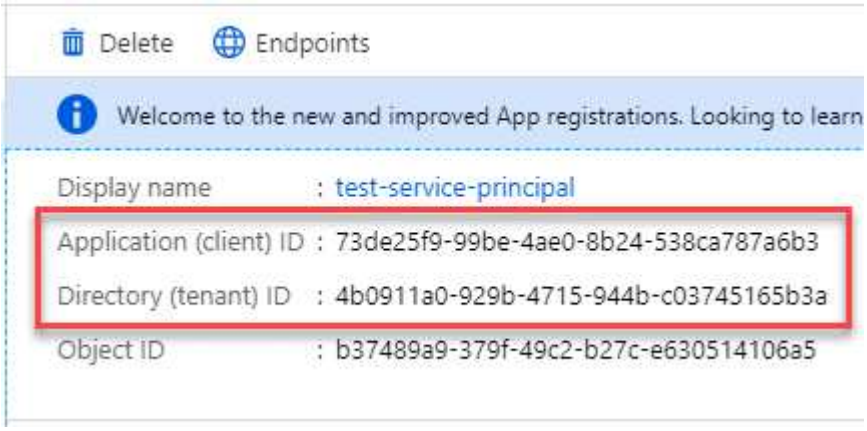


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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.

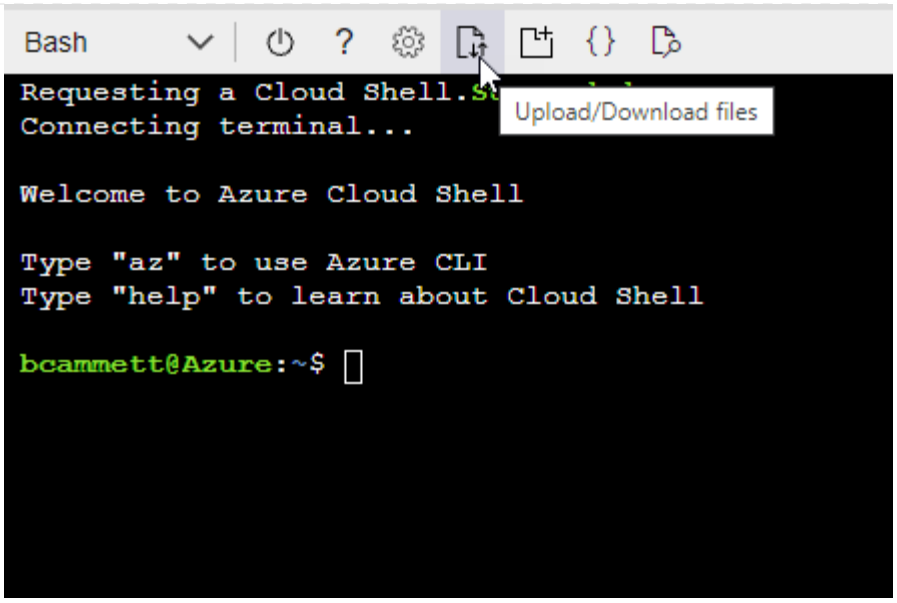
   Exemplo

   ```
   "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

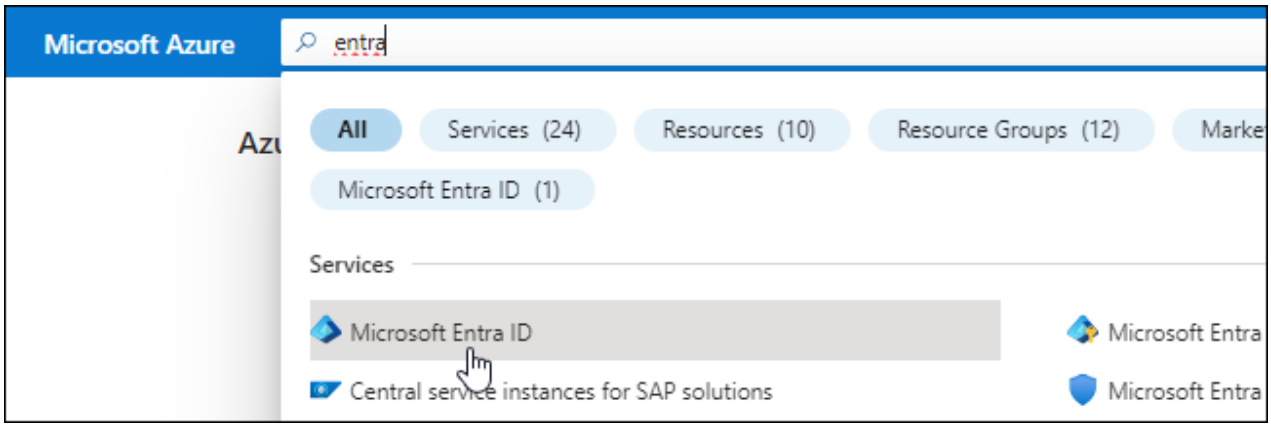
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o Console.

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 .

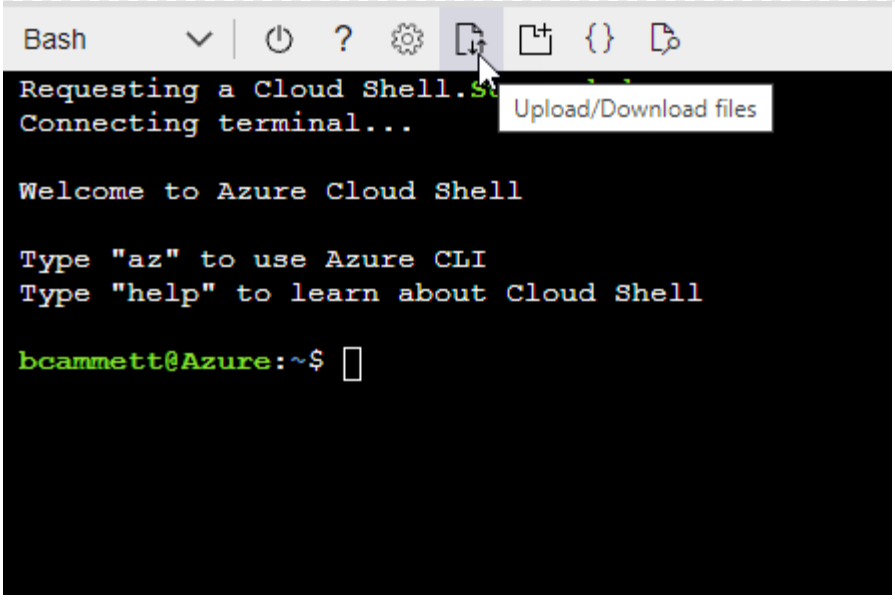
Exemplo

```
"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**.

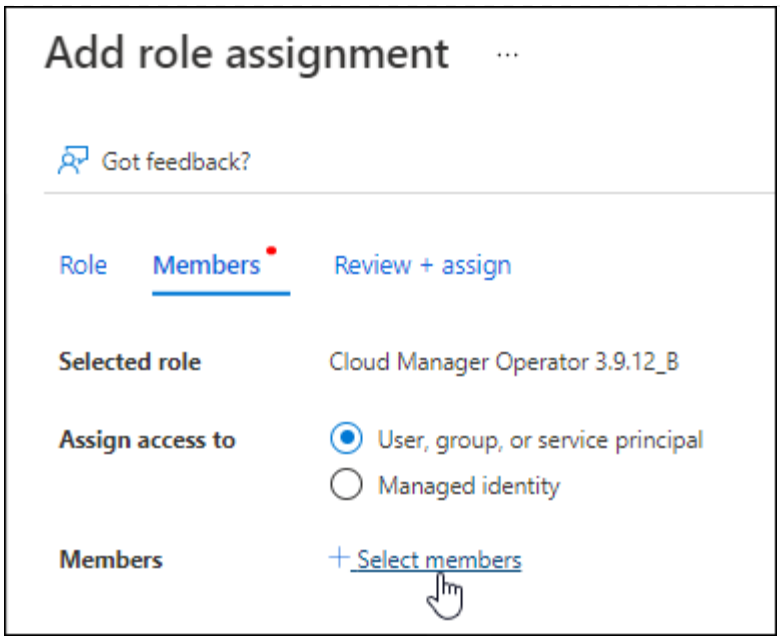
   b. Selecione a assinatura.

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

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

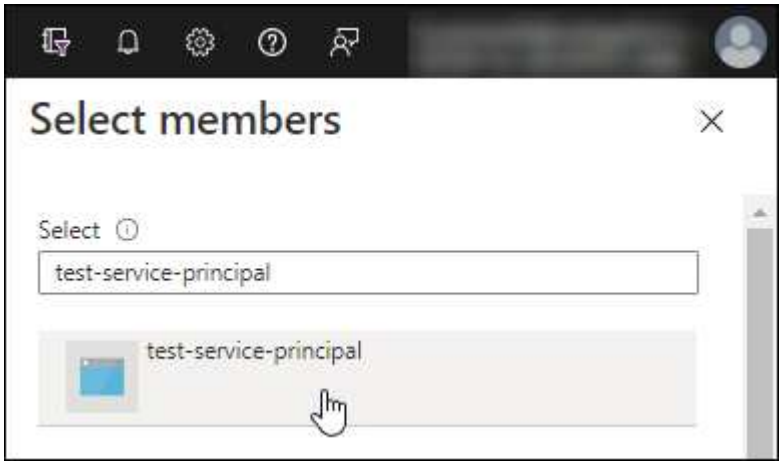
   e. Na aba **Membros**, complete os seguintes passos:

      - 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**.

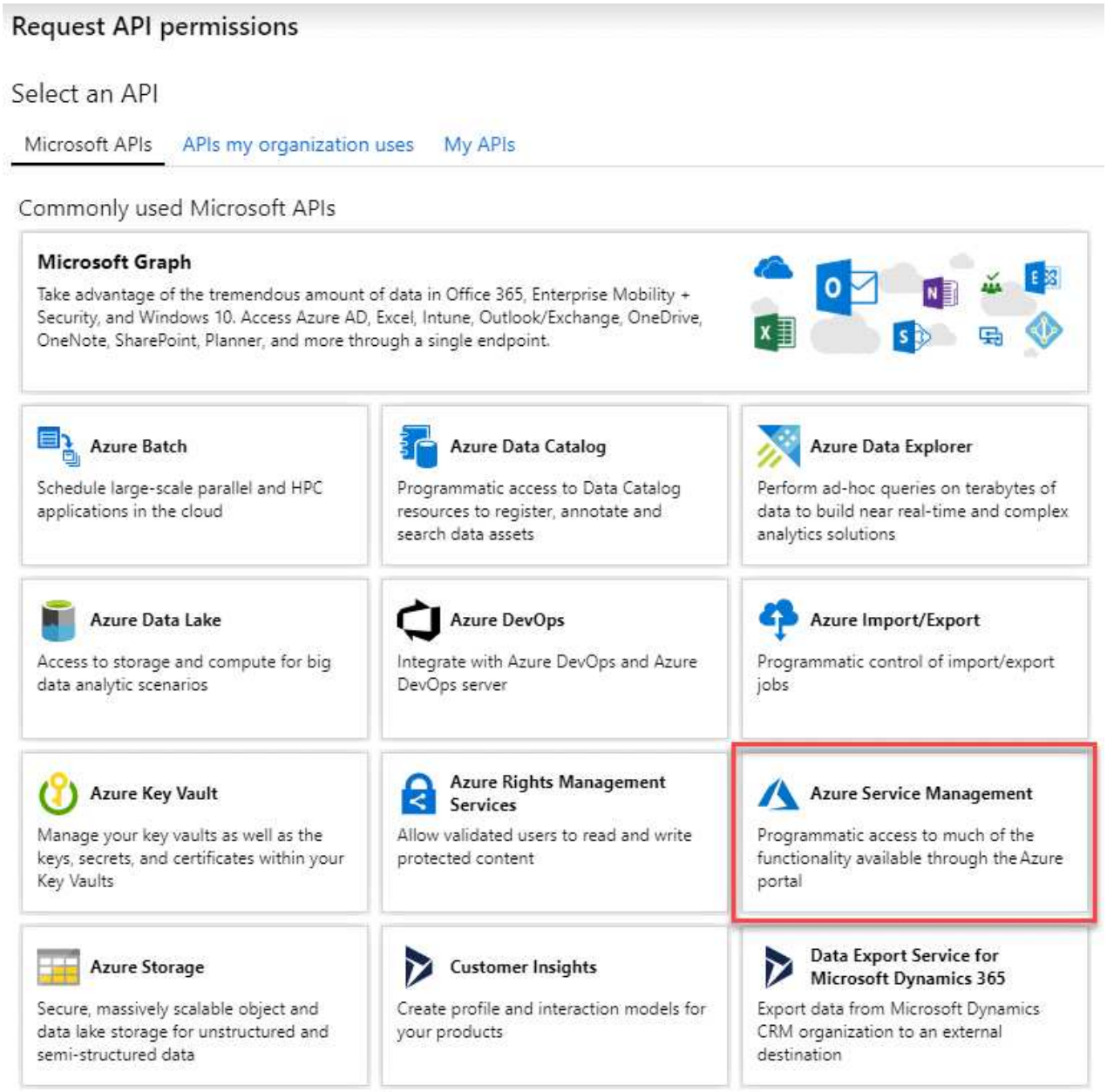
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

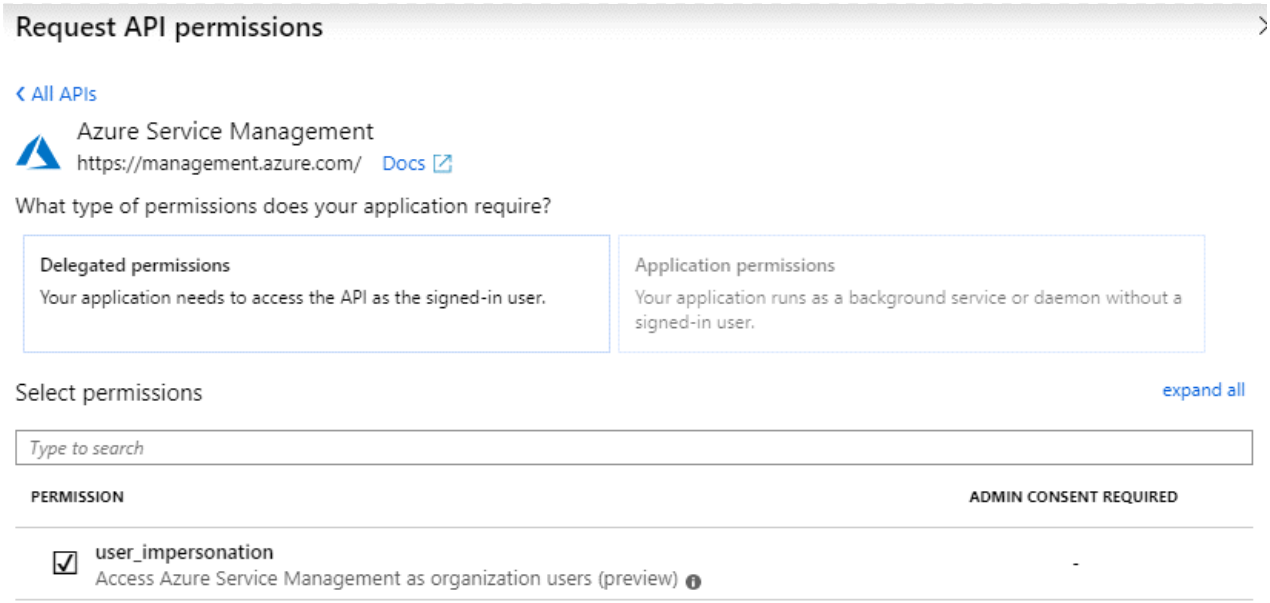
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

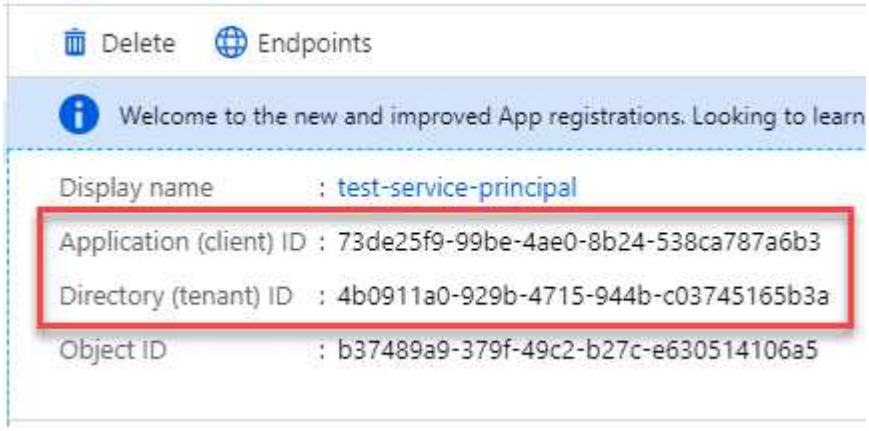


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

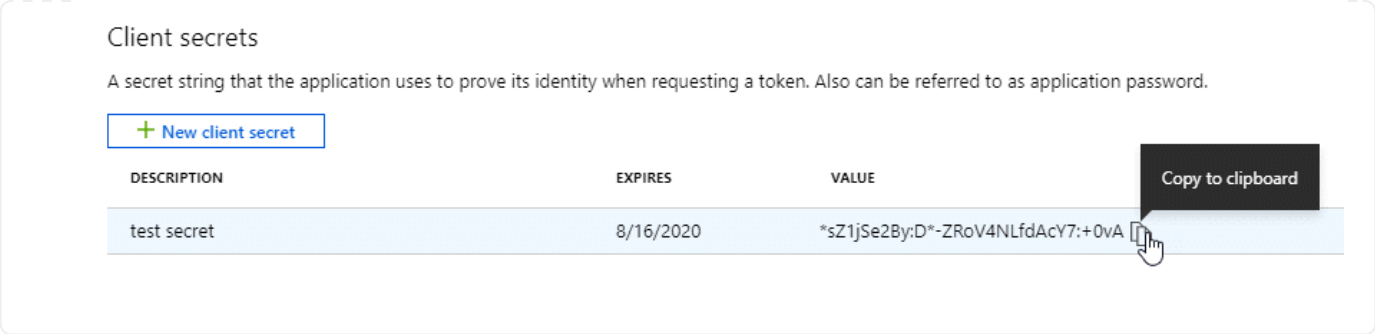
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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.

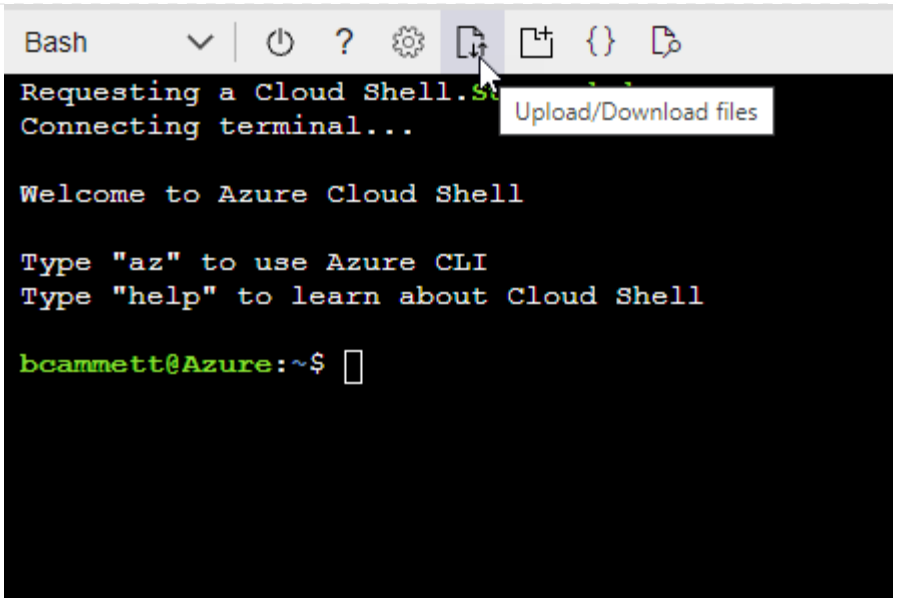
   Exemplo

   ```
   "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

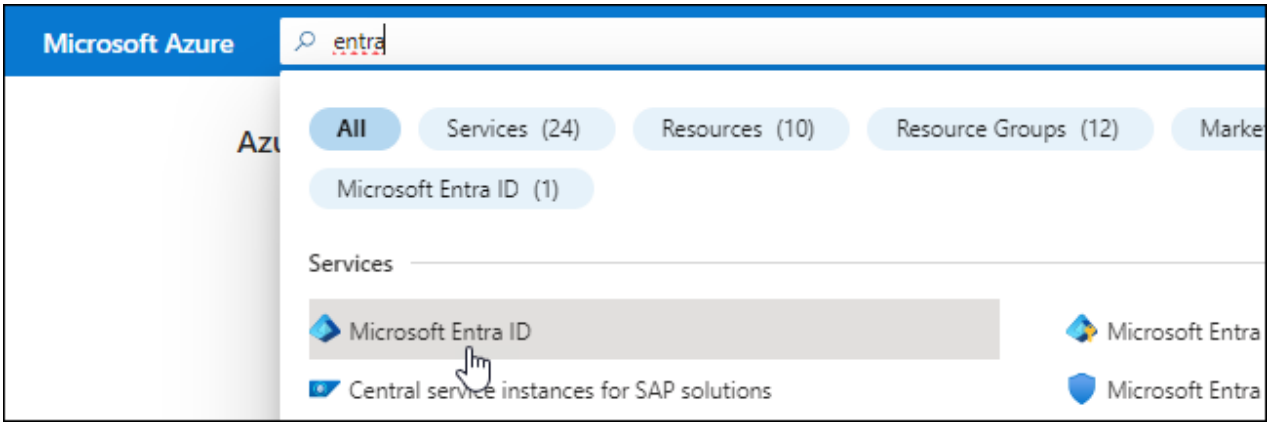
Crie e configure uma entidade de serviço no Microsoft Entra ID e obtenha as credenciais do Azure necessárias para o agente do Console.

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 .

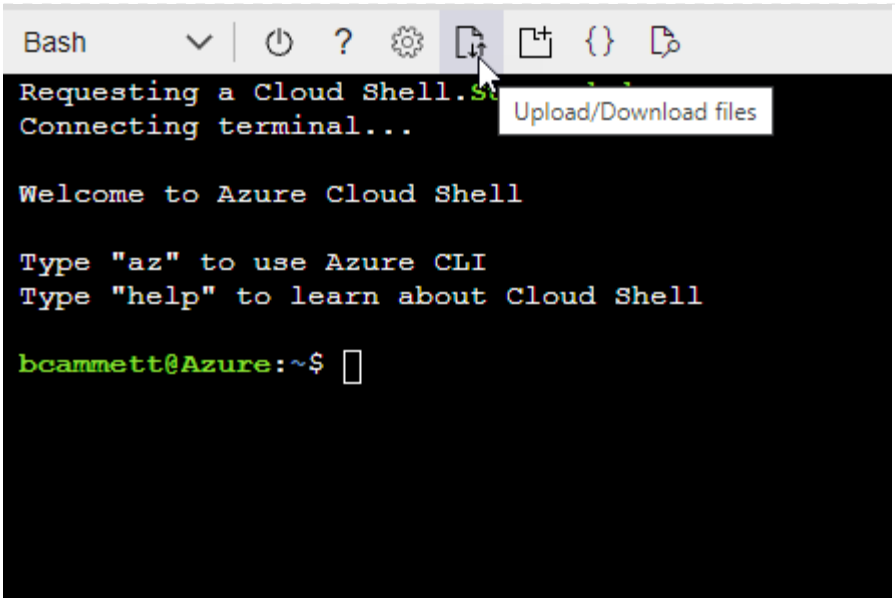
Exemplo

```
"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**.

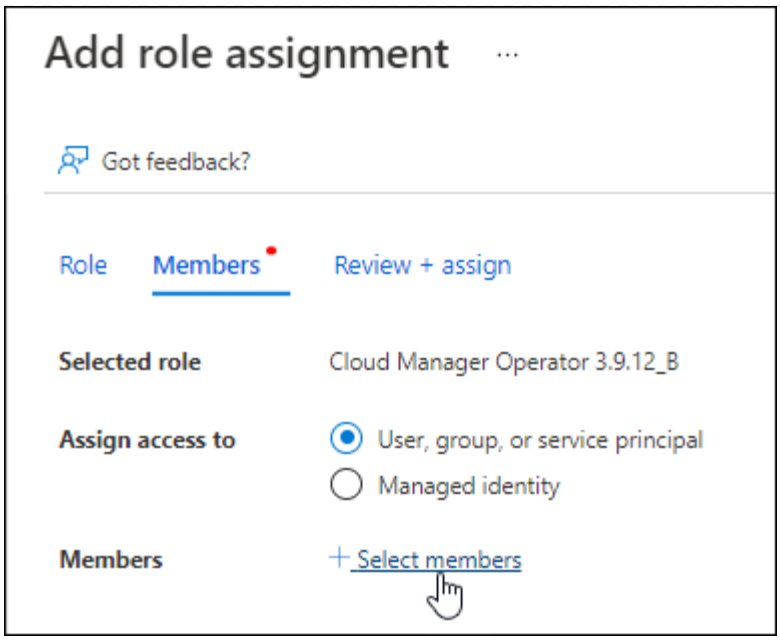
   b. Selecione a assinatura.

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

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

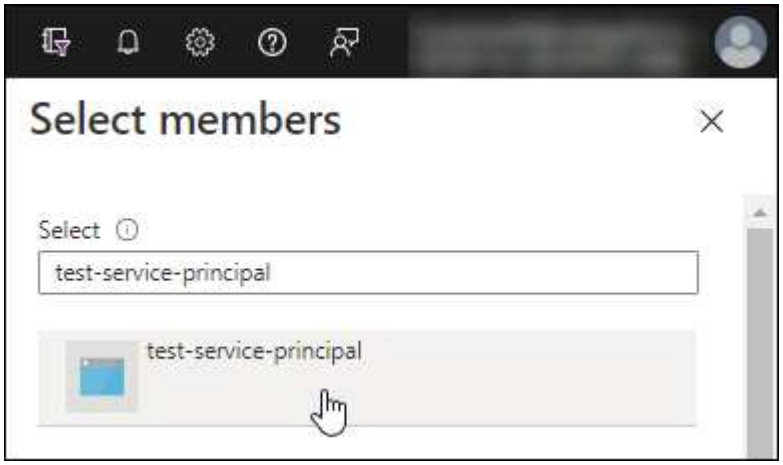
   e. Na aba **Membros**, complete os seguintes passos:

      - 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**.

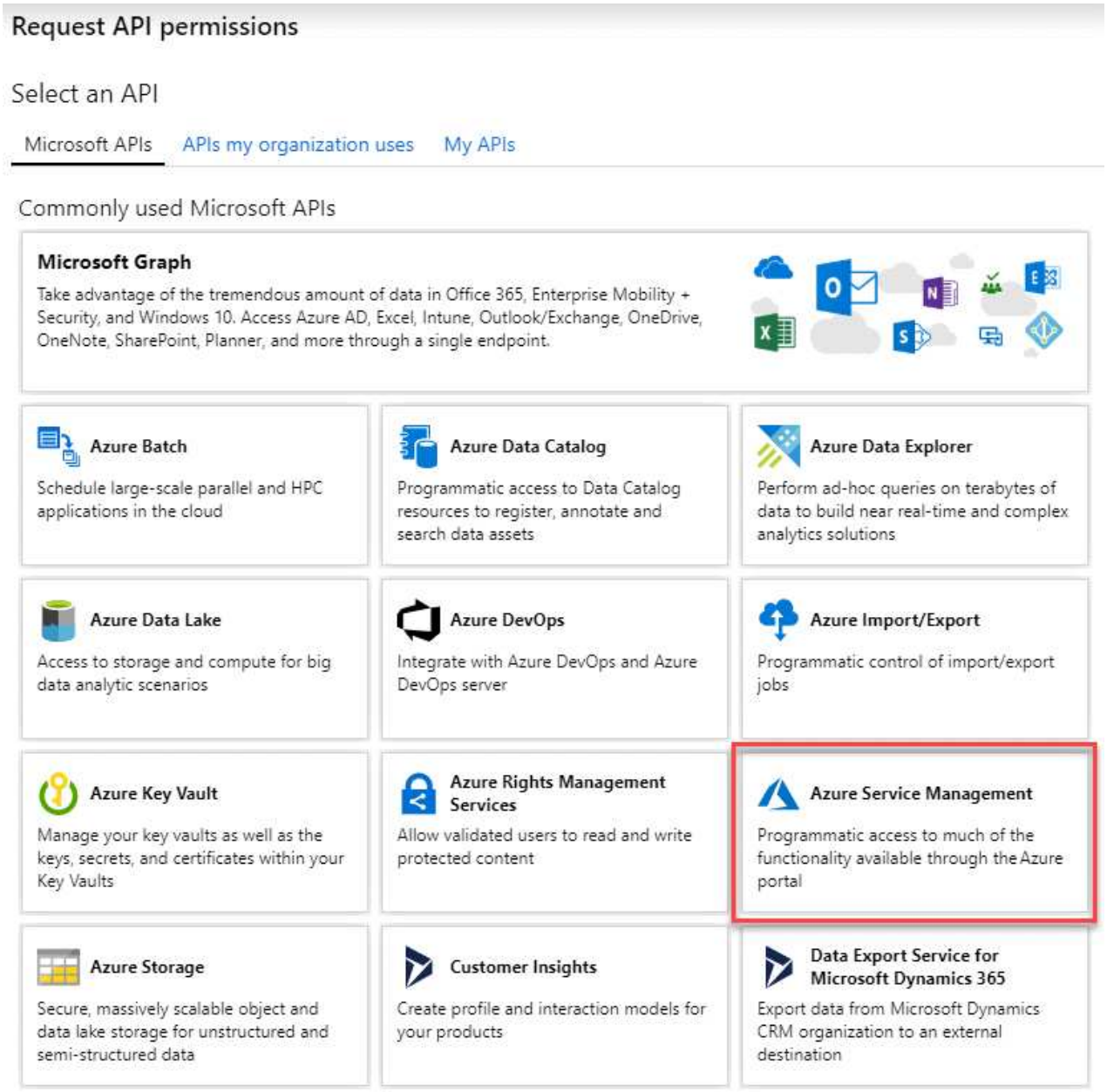
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

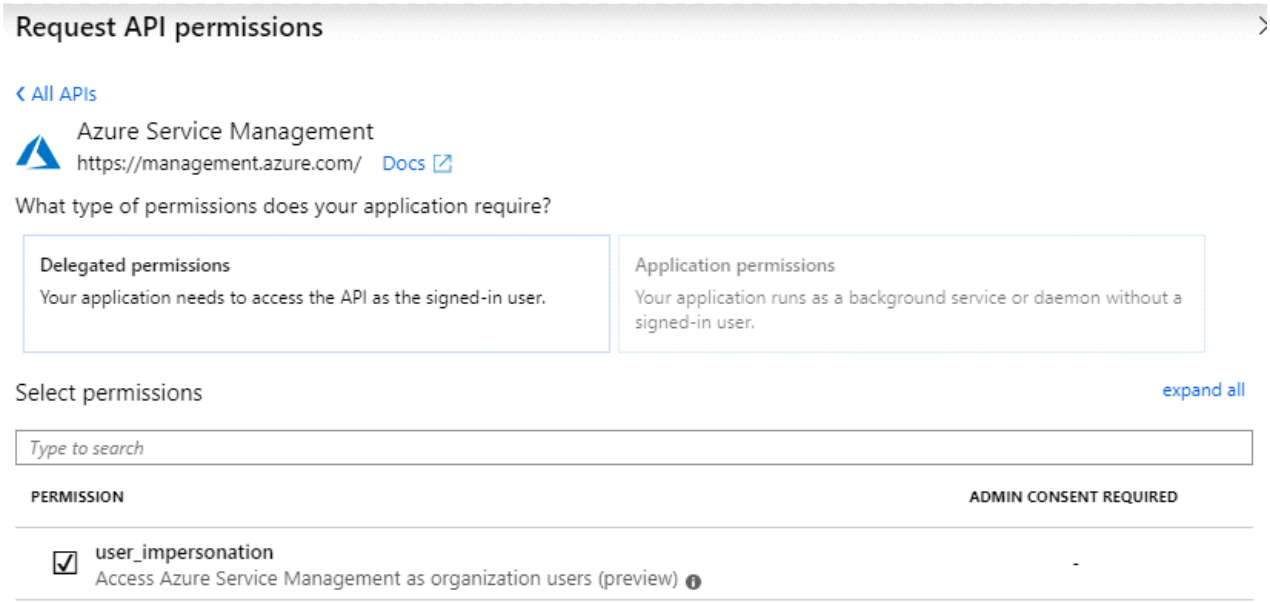
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

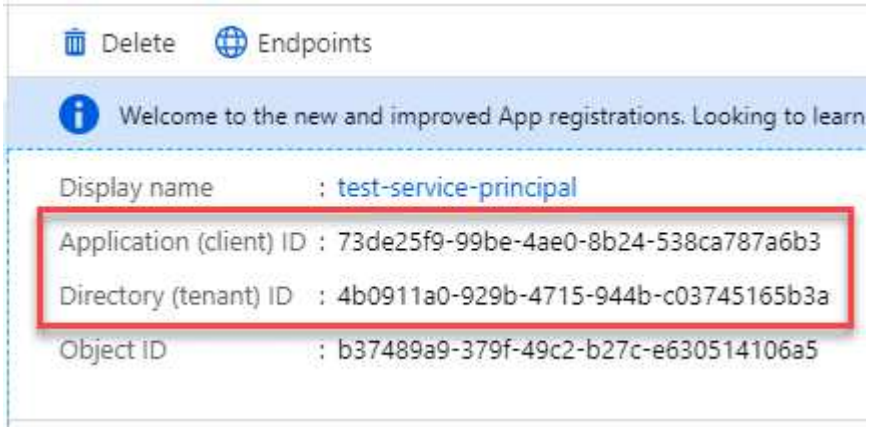


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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 Gerenciador de Implantação em Nuvem V2
   - API do Cloud Infrastructure Manager
   - 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)
   - Cloud Key Management Service (KMS) API (Necessário apenas se você planeja usar NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))
   - API de Cotas na Nuvem (necessária para implantações do Cloud Volumes ONTAP usando o Infrastructure Manager)

"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 Gerenciador de Implantação em Nuvem V2
   - API do Cloud Infrastructure Manager
   - 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)
   - Cloud Key Management Service (KMS) API (Necessário apenas se você planeja usar NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))
   - API de Cotas na Nuvem (necessária para implantações do Cloud Volumes ONTAP usando o Infrastructure Manager)

"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 Gerenciador de Implantação em Nuvem V2
   - API do Cloud Infrastructure Manager
   - 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)
   - Cloud Key Management Service (KMS) API (Necessário apenas se você planeja usar NetApp Backup and Recovery com chaves de criptografia gerenciadas pelo cliente (CMEK))
   - API de Cotas na Nuvem (necessária para implantações do Cloud Volumes ONTAP usando o Infrastructure Manager)

"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

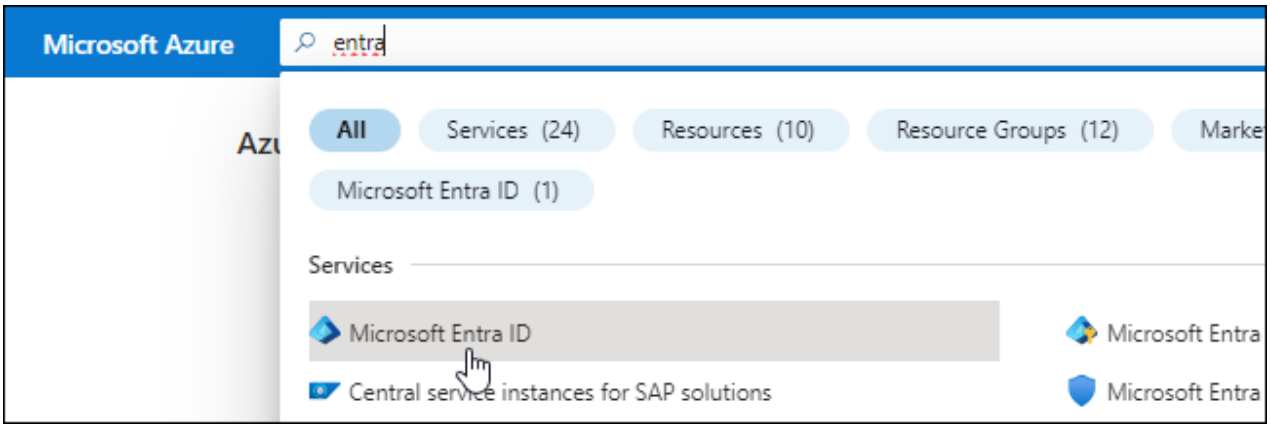
Quando o agente do Console é instalado no local, você precisa fornecer ao agente do Console permissões do Azure configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

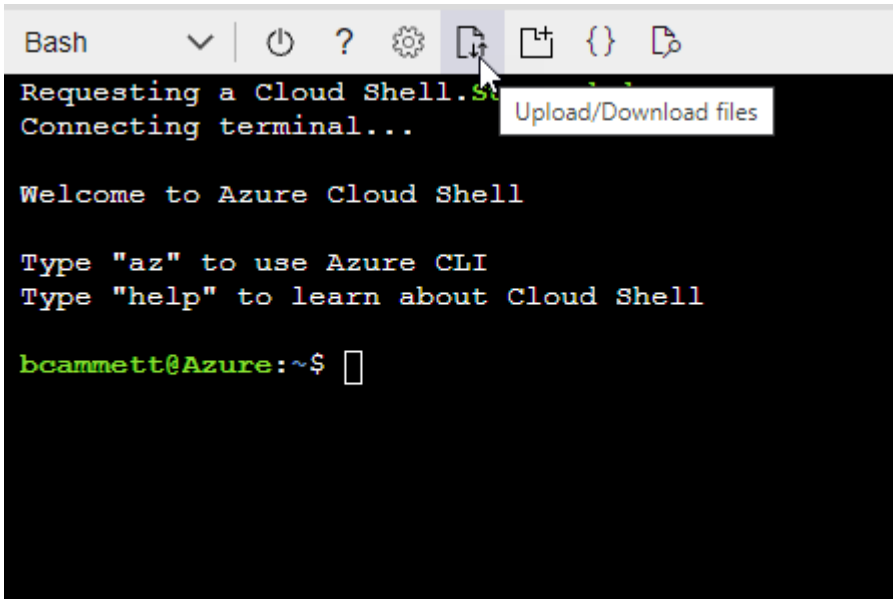
      Exemplo

```
"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**.

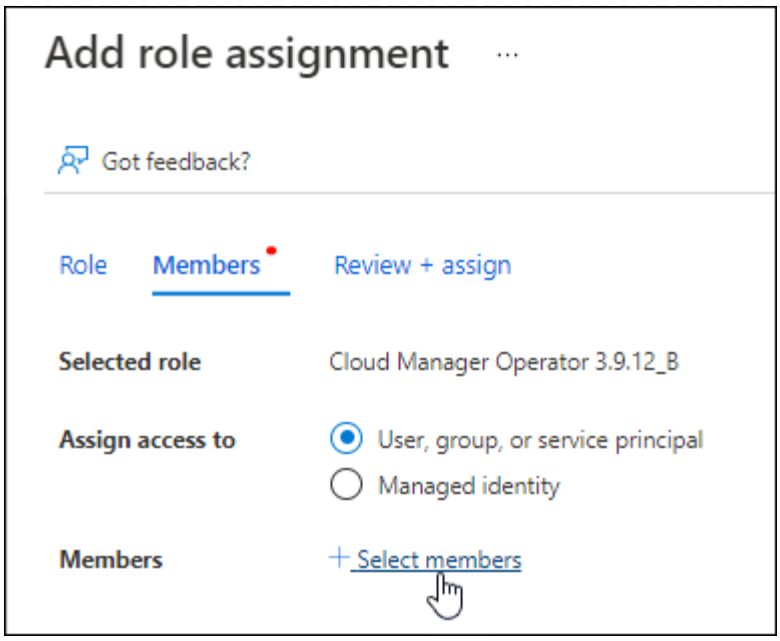
   b. Selecione a assinatura.

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

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

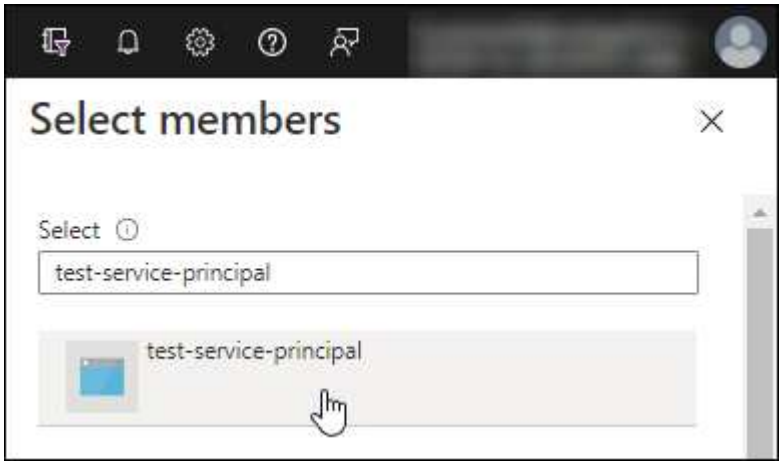
   e. Na aba **Membros**, complete os seguintes passos:

   - 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**.

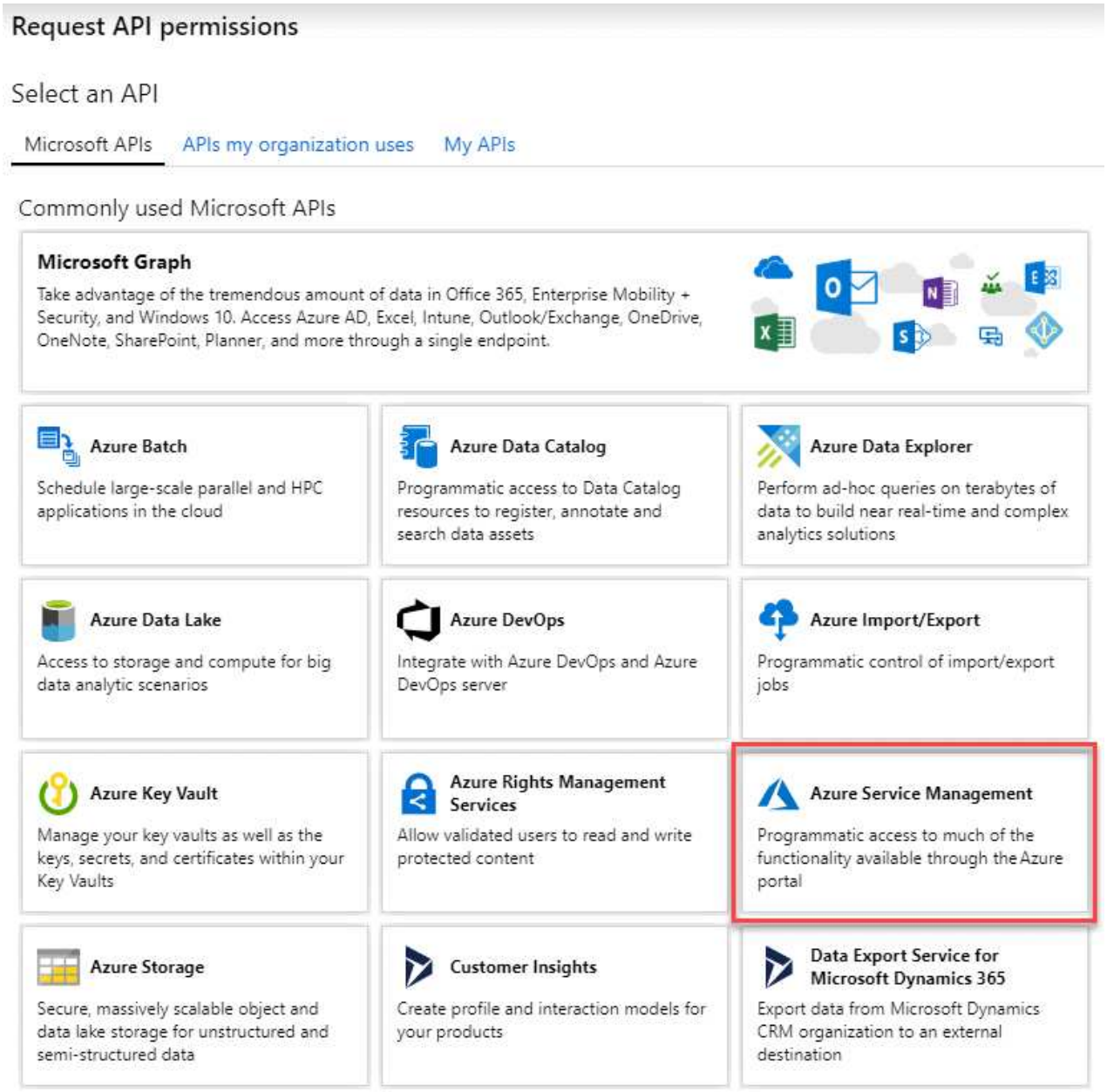
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

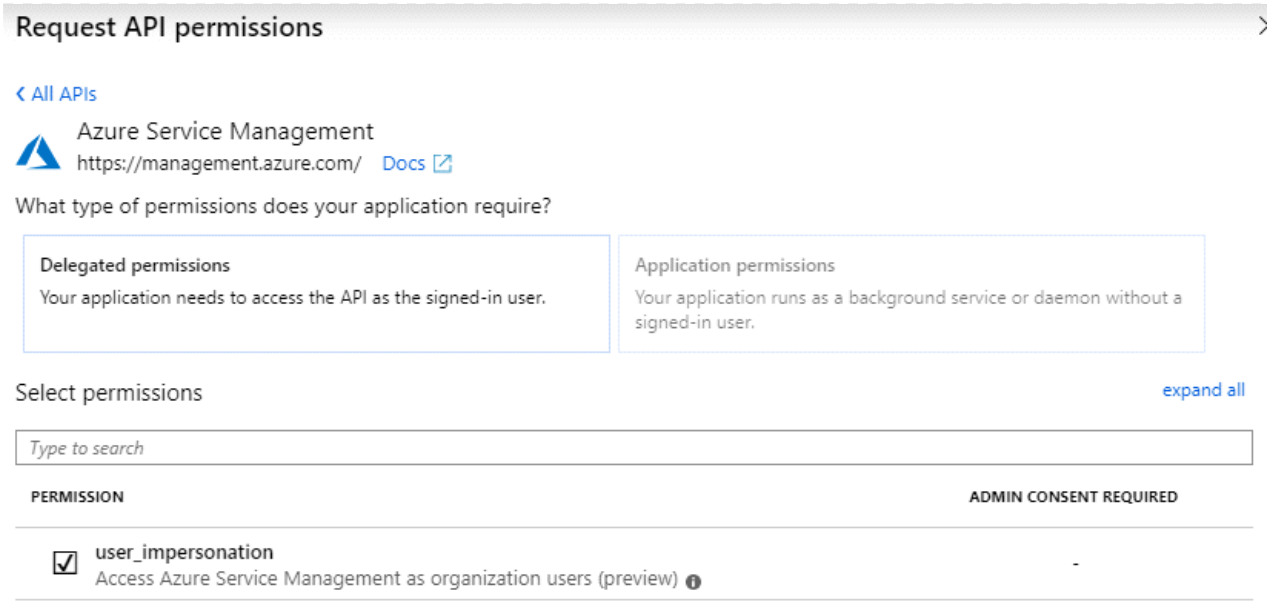
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

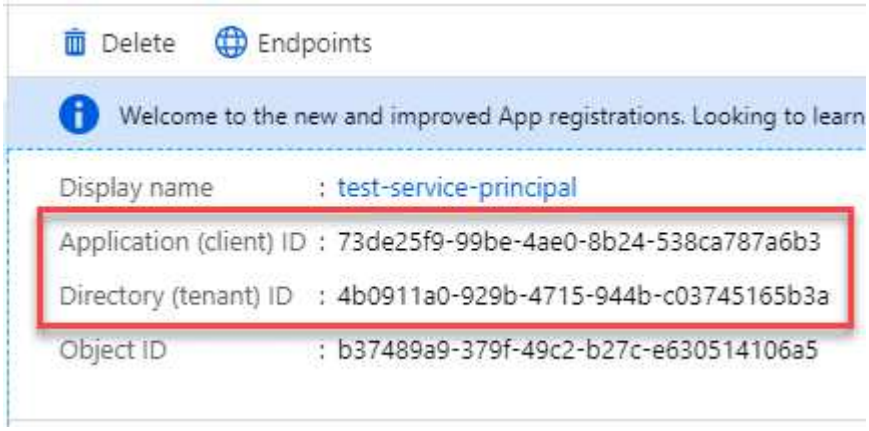


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

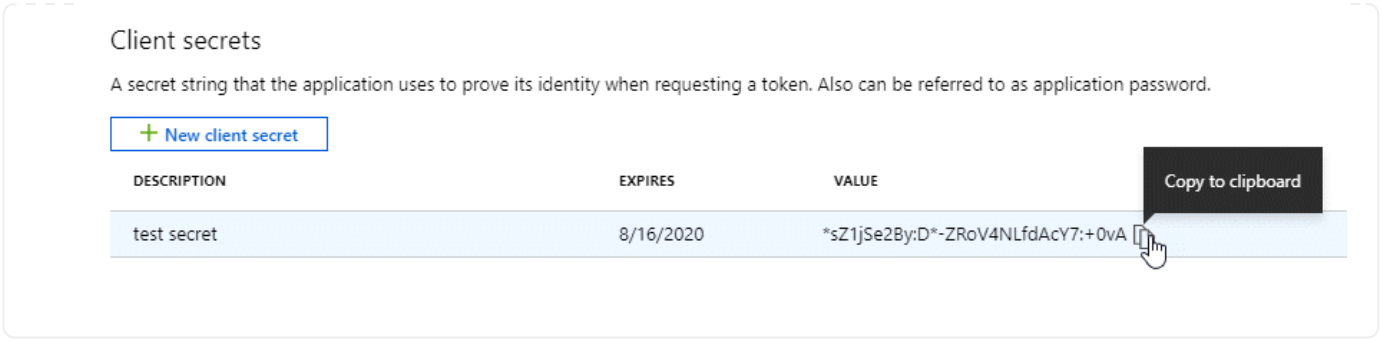
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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

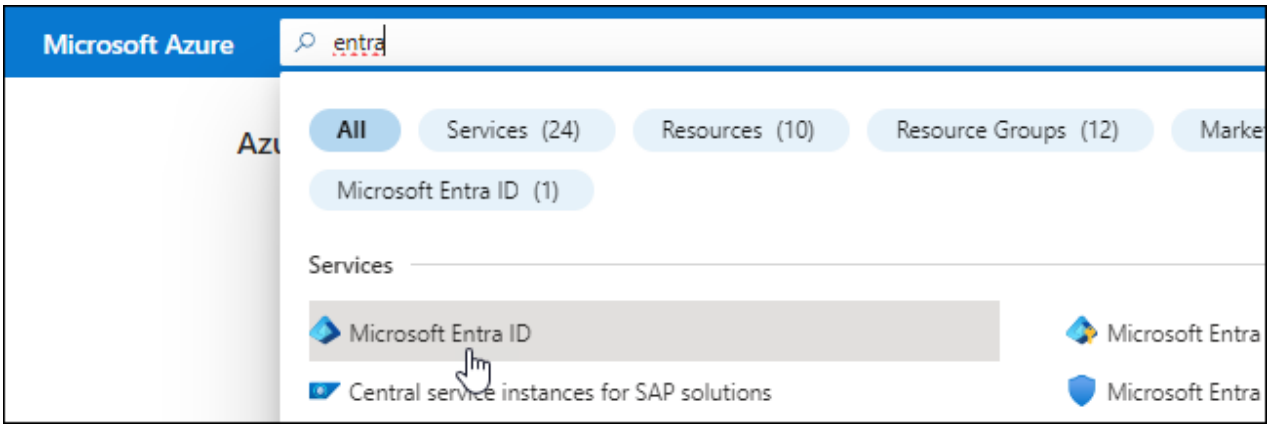
Quando o agente do Console estiver instalado no local, você precisará conceder permissões do Azure ao agente do Console configurando uma entidade de serviço no Microsoft Entra ID e obtendo as credenciais do Azure necessárias para o agente do Console.

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 .

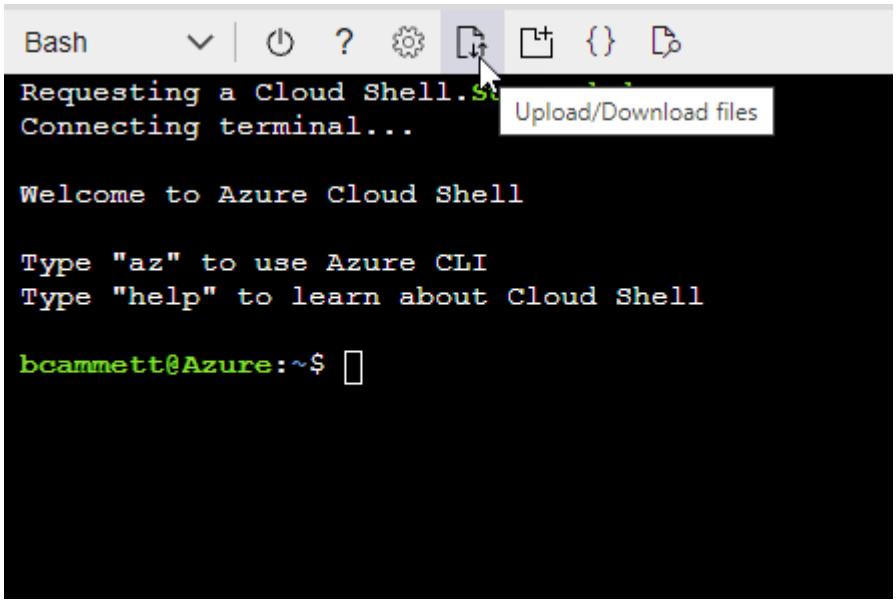
      Exemplo

```
"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:

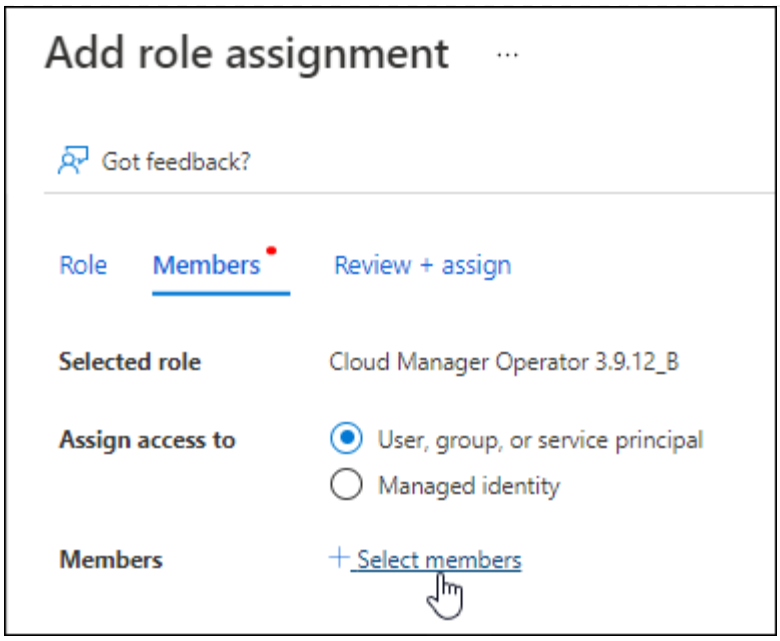
```
az role definition create --role-definition agent_Policy.json
```

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:

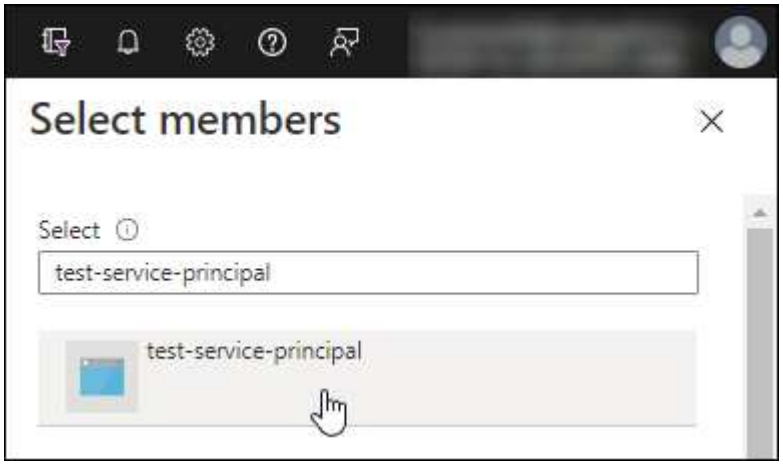
   a. No portal do Azure, abra o serviço **Assinaturas**.
   b. Selecione a assinatura.
   c. Selecione **Controle de acesso (IAM) > Adicionar > Adicionar atribuição de função**.
   d. Na guia **Função**, selecione a função **Operador de console** e selecione **Avançar**.
   e. Na aba **Membros**, complete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

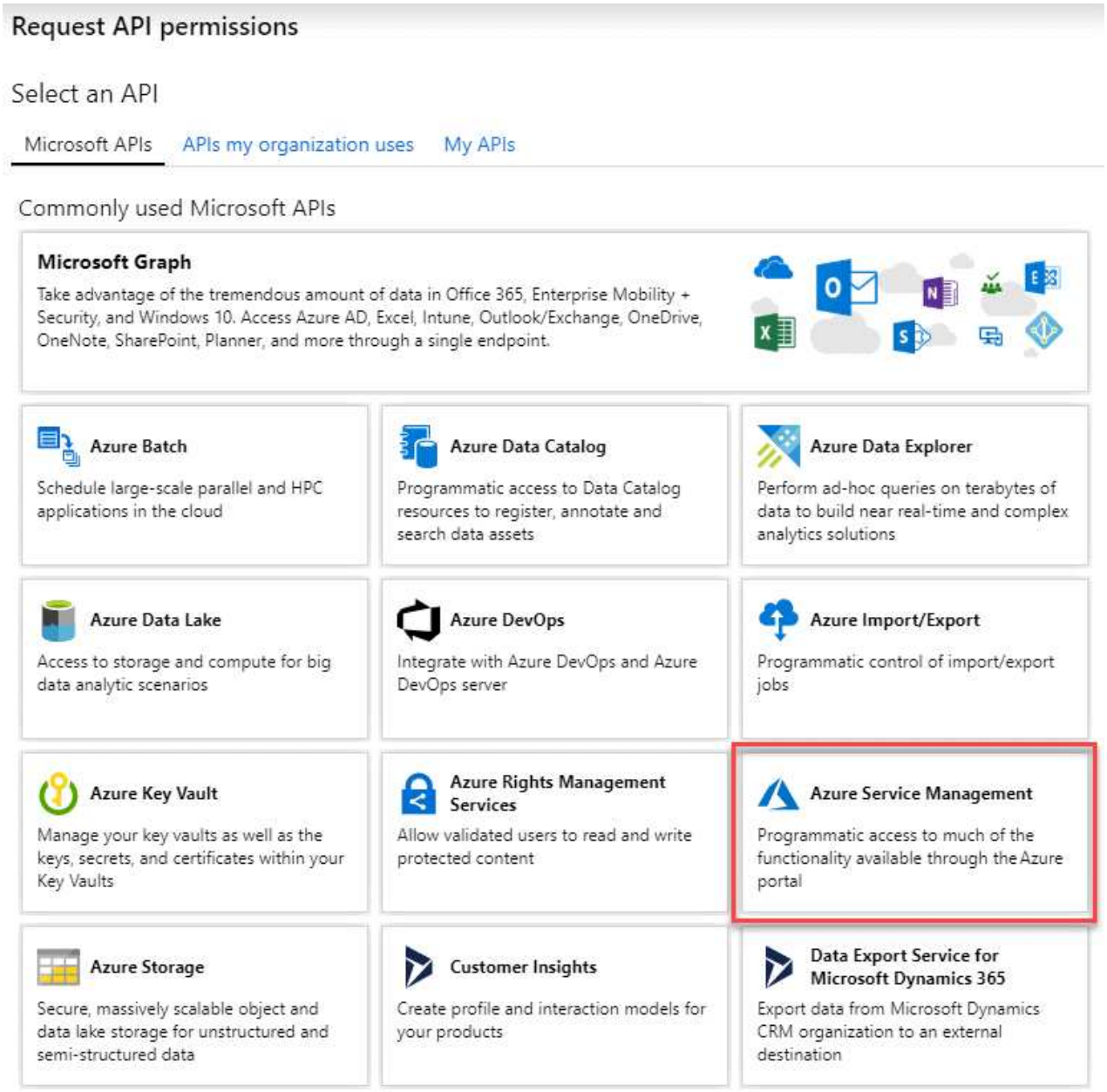
O principal de serviço agora tem as permissões necessárias do Azure para implantar o agente do Console.

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.

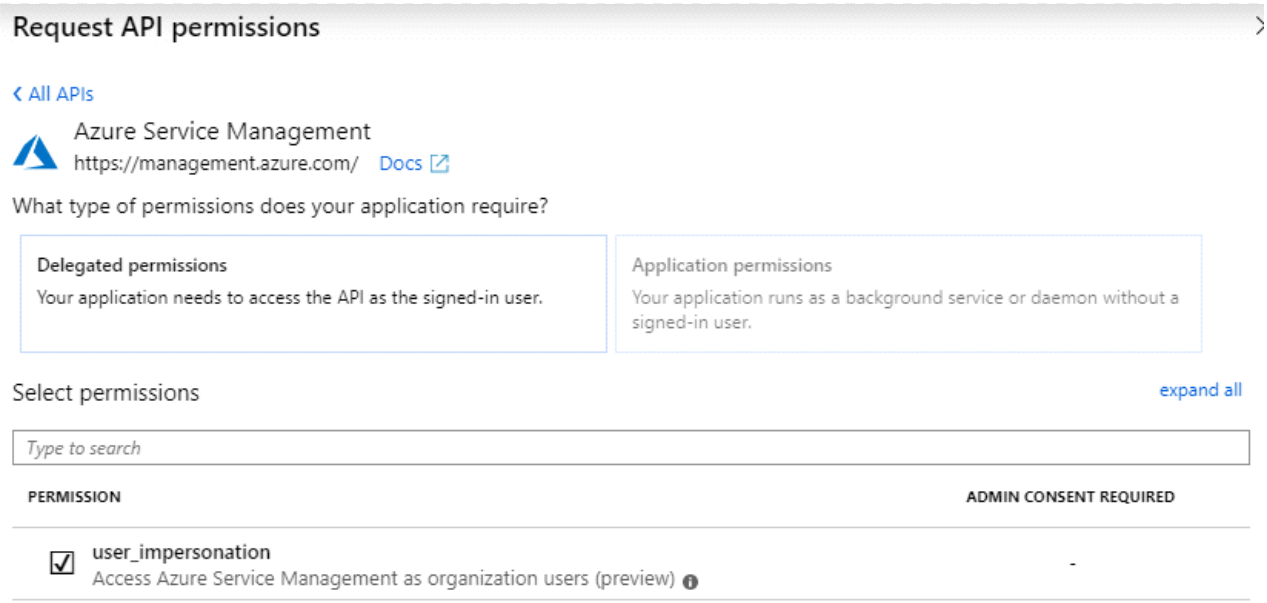
Adicionar permissões da API de Gerenciamento de Serviços do Windows Azure

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**.

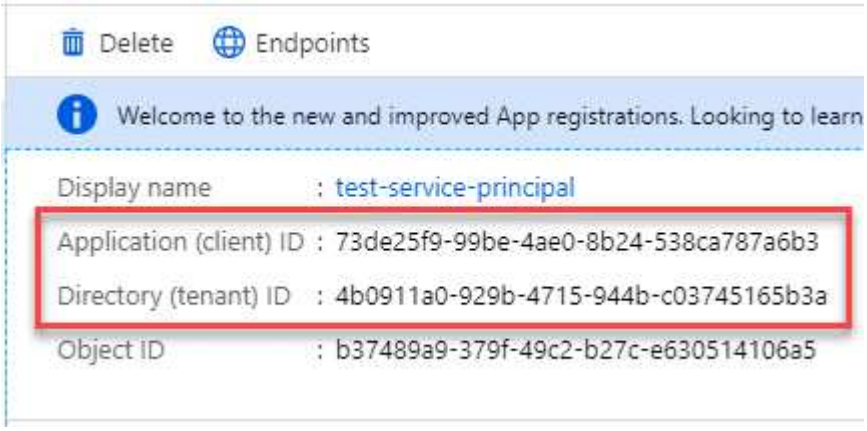


4. Selecione **Acessar o Gerenciamento de Serviços do Azure como usuários da organização** e, em seguida, selecione **Adicionar permissões**.



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

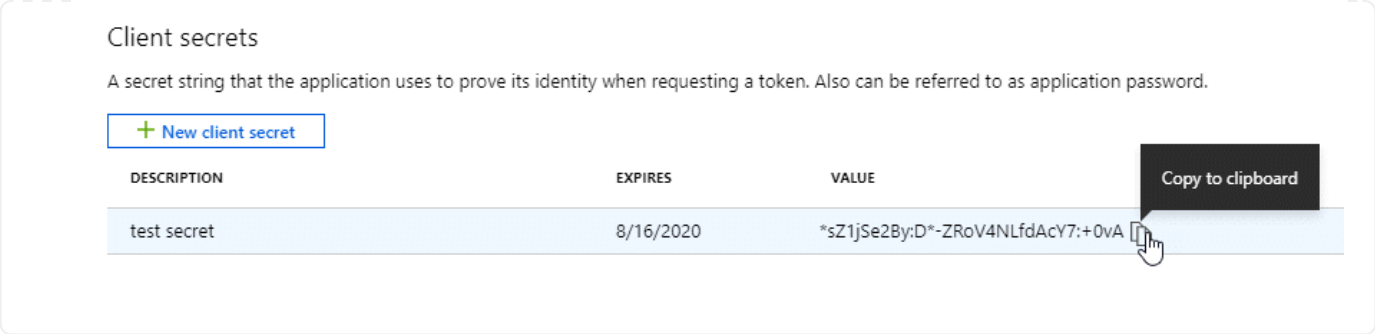
1. No serviço **Microsoft Entra ID**, selecione **Registros de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



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

Informações sobre direitos autorais

Informações sobre marcas comerciais