Administrar o Cloud Manager

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

Administrar o Cloud Manager

Encontrando a ID do sistema do Cloud Manager

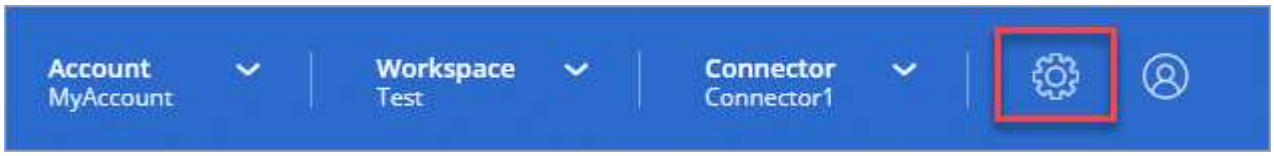
Para ajudá-lo a começar, seu representante da NetApp pode pedir a ID do sistema do Cloud Manager. O ID é normalmente utilizado para fins de licenciamento e resolução de problemas.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações.



2. Clique em **Painel de suporte**.

   A ID do sistema aparece no canto superior direito.

   Exemplo

Gerenciar conetores

Gerenciamento de conetores existentes

Depois de criar um ou mais conetores, você pode gerenciá-los alternando entre conetores, conetando-se à interface de usuário local em execução em um conetor e muito mais.

Comutação entre conetores

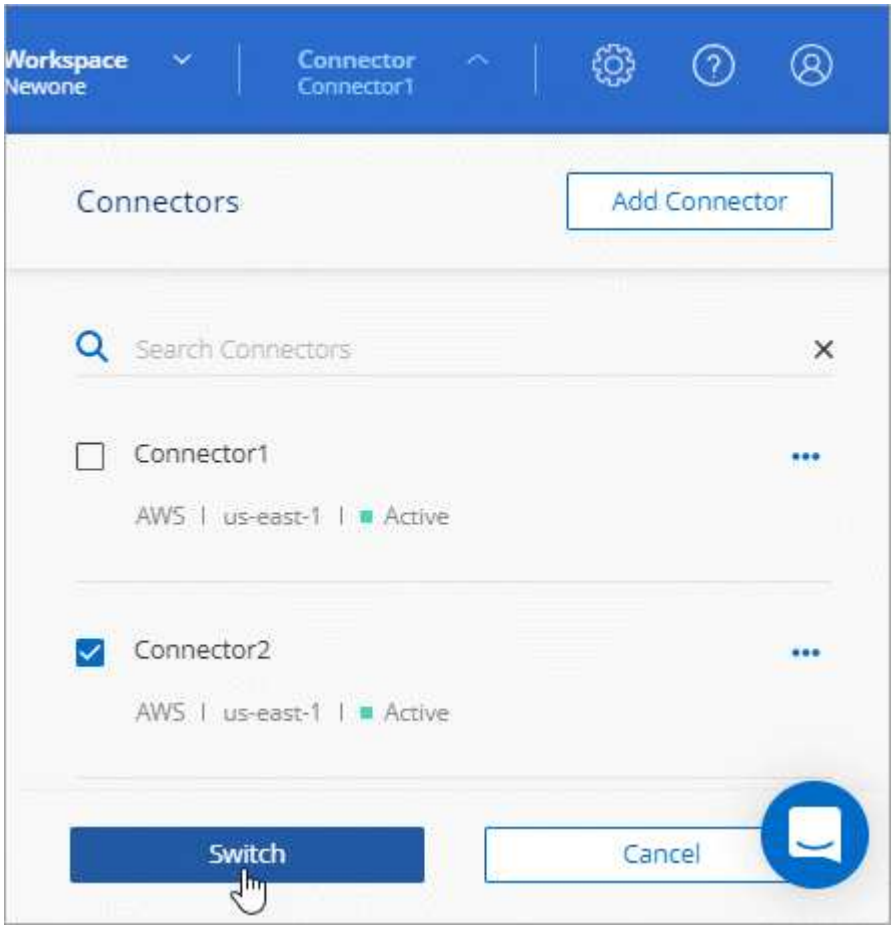
Se você tiver vários conetores, pode alternar entre eles para ver os ambientes de trabalho associados a um conetor específico.

Por exemplo, digamos que você está trabalhando em um ambiente multicloud. Você pode ter um conetor na

AWS e outro no Google Cloud. Você precisa alternar entre esses conetores para gerenciar os sistemas Cloud Volumes ONTAP executados nessas nuvens.

Passo

1. Clique no menu suspenso **Connector**, selecione outro conetor e clique em **Switch**.



O Cloud Manager atualiza e mostra os ambientes de trabalho associados ao conector selecionado.

Acessando a IU local

Embora você deva executar quase todas as tarefas a partir da interface de usuário SaaS, uma interface de usuário local ainda está disponível no conetor. Esta interface é necessária para algumas tarefas que precisam ser executadas a partir do próprio conetor:

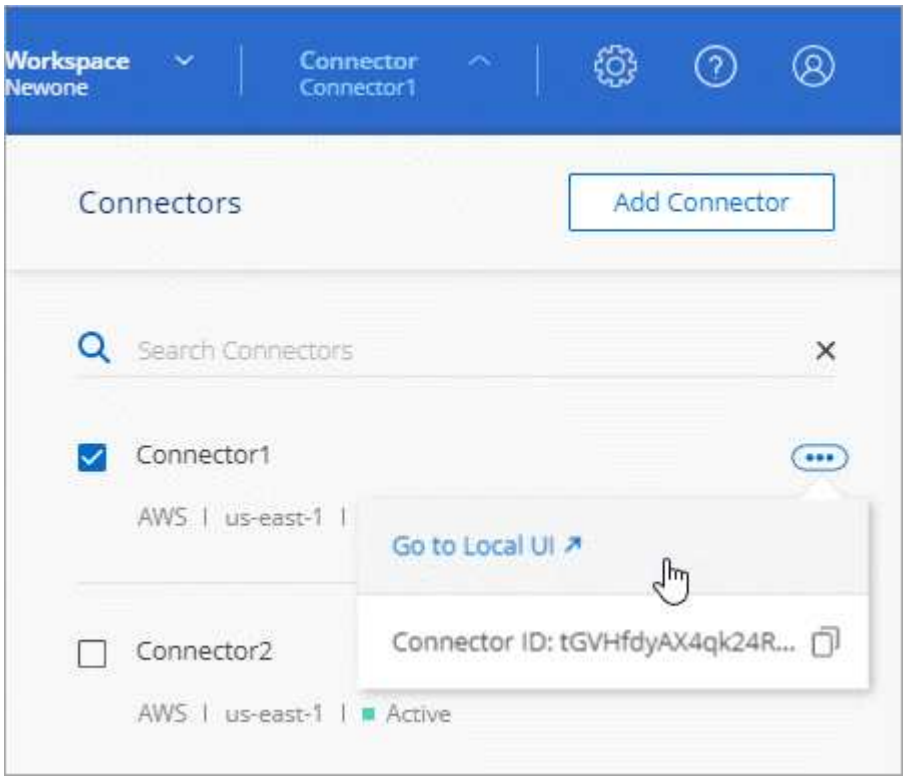
- "Configurando um servidor proxy"
- Instalando um patch (você normalmente trabalhará com o pessoal do NetApp para instalar um patch)
- Download de mensagens do AutoSupport (geralmente direcionadas pelo pessoal do NetApp quando você tiver problemas)

Passos

1. "Faça login na interface SaaS do Cloud Manager" De uma máquina que tenha uma conexão de rede com a instância do conetor.

   Se o conetor não tiver um endereço IP público, você precisará de uma conexão VPN ou precisará se conetar a partir de um host de salto que esteja na mesma rede que o conetor.

2. Clique no menu suspenso **Connector**, clique no menu de ação de um conetor e, em seguida, clique em **Go to local UI**.



A interface do Cloud Manager em execução no conetor é carregada em uma nova guia do navegador.

Removendo conetores do Cloud Manager

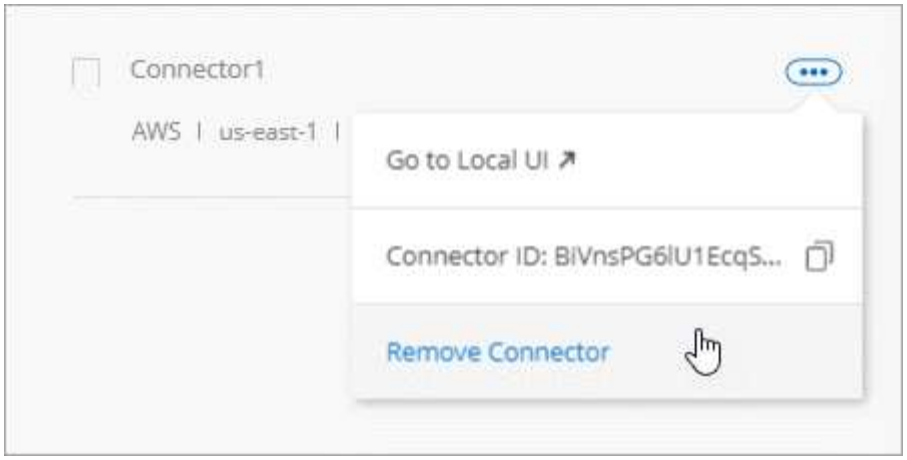
Se um conetor estiver inativo, você poderá removê-lo da lista de conetores no Cloud Manager. Pode fazê-lo se tiver eliminado a máquina virtual do conetor ou se tiver desinstalado o software do conetor.

Observe o seguinte sobre como remover um conetor:

- Esta ação não exclui a máquina virtual.
- Esta ação não pode ser revertida - uma vez que você remove um conetor do Cloud Manager, você não pode adicioná-lo de volta ao Cloud Manager.

Passos

1. Clique no menu suspenso conetor no cabeçalho do Cloud Manager.
2. Clique no menu de ação para um conetor inativo e clique em **Remove Connector**.



3. Introduza o nome do conetor para confirmar e, em seguida, clique em Remover.

Resultado

O Cloud Manager remove o conetor de seus Registros.

Desinstalar o software do conetor

O conetor inclui um script de desinstalação que você pode usar para desinstalar o software para solucionar problemas ou remover permanentemente o software do host.

Passo

1. A partir do host Linux, execute o script de desinstalação:

   /opt/application/NetApp/cloudmanager/bin/uninstall.sh [silent]

   silent executa o script sem solicitar confirmação.

E quanto às atualizações de software?

O conetor atualiza automaticamente o software para a versão mais recente, desde que seja "acesso de saída à internet" necessário obter a atualização de software.

Mais formas de criar conetores

Requisitos do host do conetor

O software do conetor deve ser executado em um host que atenda a requisitos específicos do sistema operacional, requisitos de RAM, requisitos de porta, etc.

Um host dedicado é necessário

O conetor não é suportado em um host que é compartilhado com outros aplicativos. O host deve ser um host dedicado.

CPU

4 núcleos ou 4 vCPUs

RAM

14 GB

Tipo de instância do AWS EC2

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o T3.xlarge e use esse tipo de instância quando você implantar o conetor diretamente do Cloud Manager.

Tamanho da VM do Azure

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o DS3 v2 e usar esse tamanho de VM quando você implantar o conetor diretamente do Cloud Manager.

Tipo de máquina GCP

Um tipo de instância que atende aos requisitos de CPU e RAM acima. Recomendamos o padrão n1-4 e usar esse tipo de máquina quando você implantar o conetor diretamente do Cloud Manager.

Sistemas operacionais suportados

- CentOS 7,6
- CentOS 7,7
- Red Hat Enterprise Linux 7,6
- Red Hat Enterprise Linux 7,7

  O sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registado, o sistema não poderá aceder aos repositórios para atualizar o software de 3rd partes necessário durante a instalação do conetor.

  O conetor é suportado em versões em inglês destes sistemas operativos.

Hipervisor

Um hypervisor bare metal ou hospedado certificado para executar o CentOS ou o Red Hat Enterprise Linux "Solução Red Hat: Quais hipervisores são certificados para executar o Red Hat Enterprise Linux?"

Espaço em disco em /opt

100 GB de espaço devem estar disponíveis

Acesso de saída à Internet

O acesso de saída à Internet é necessário para instalar o conetor e para que o conetor gerencie recursos e processos em seu ambiente de nuvem pública. Para obter uma lista de endpoints, "Requisitos de rede para o conetor"consulte .

Criando um conetor no AWS Marketplace

É melhor criar um conetor diretamente do Cloud Manager, mas você pode iniciar um conetor no AWS Marketplace, se preferir não especificar chaves de acesso da AWS. Depois de criar e configurar o conetor, o Cloud Manager o usará automaticamente quando você criar novos ambientes de trabalho.

Passos

1. Crie uma política e função do IAM para a instância do EC2:
   a. Faça o download da política do IAM do Cloud Manager a partir do seguinte local:

"Gerenciador de nuvem do NetApp: Políticas da AWS, Azure e GCP"

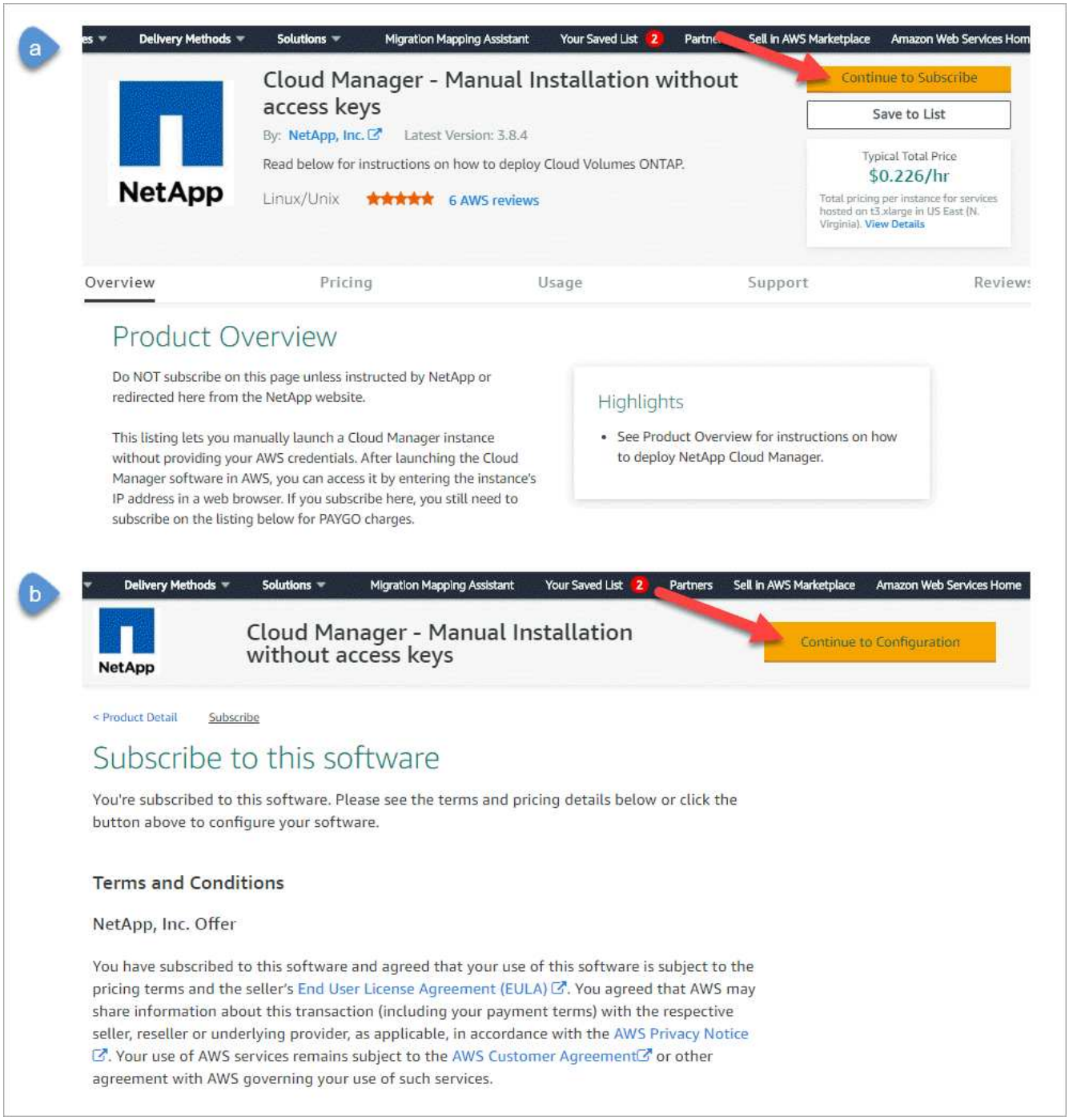
b. No console do IAM, crie sua própria política copiando e colando o texto da política do IAM do Cloud Manager.

c. Crie uma função do IAM com o tipo de função Amazon EC2 e anexe a política criada na etapa anterior à função.

2. Agora vá para o "Página do Cloud Manager no AWS Marketplace" para implantar o Cloud Manager a partir de uma AMI.

   O usuário do IAM deve ter permissões do AWS Marketplace para se inscrever e cancelar a assinatura.

3. Na página Marketplace, clique em **Continue to Subscribe** e clique em **Continue to Configuration**.



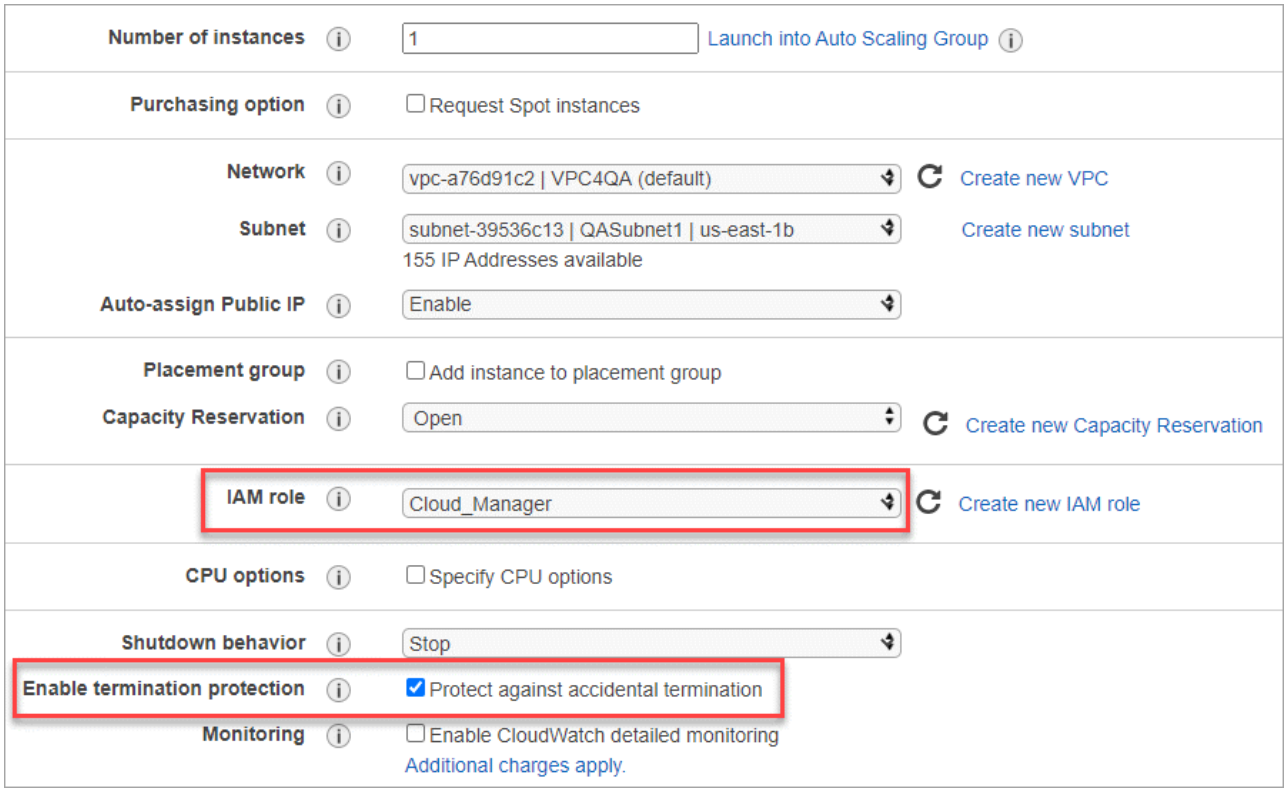
4. Altere qualquer uma das opções padrão e clique em **Continue to Launch**.
5. Em **escolha Ação**, selecione **Iniciar através de EC2** e, em seguida, clique em **Iniciar**.

   Estas etapas descrevem como iniciar a instância a partir do Console EC2 porque o console permite que você anexe uma função do IAM à instância do Cloud Manager. Isso não é possível usando a ação **Launch from Website**.

6. Siga as instruções para configurar e implantar a instância:
   - **Escolha tipo de instância**: Dependendo da disponibilidade da região, escolha um dos tipos de instância compatíveis (recomenda-se T3.xlarge).

     "Revise os requisitos da instância".

   - **Configurar instância**: Selecione uma VPC e uma sub-rede, escolha a função do IAM que você criou na etapa 1, ative a proteção de terminação (recomendada) e escolha qualquer outra opção de configuração que atenda aos seus requisitos.



   - **Adicionar armazenamento**: Mantenha as opções de armazenamento padrão.
   - **Add Tags**: Insira tags para a instância, se desejado.
   - **Configurar grupo de segurança**: Especifique os métodos de conexão necessários para a instância do conetor: SSH, HTTP e HTTPS.
   - **Revisão**: Revise suas seleções e clique em **Lançamento**.

     A AWS inicia o software com as configurações especificadas. A instância do conetor e o software devem estar sendo executados em aproximadamente cinco minutos.

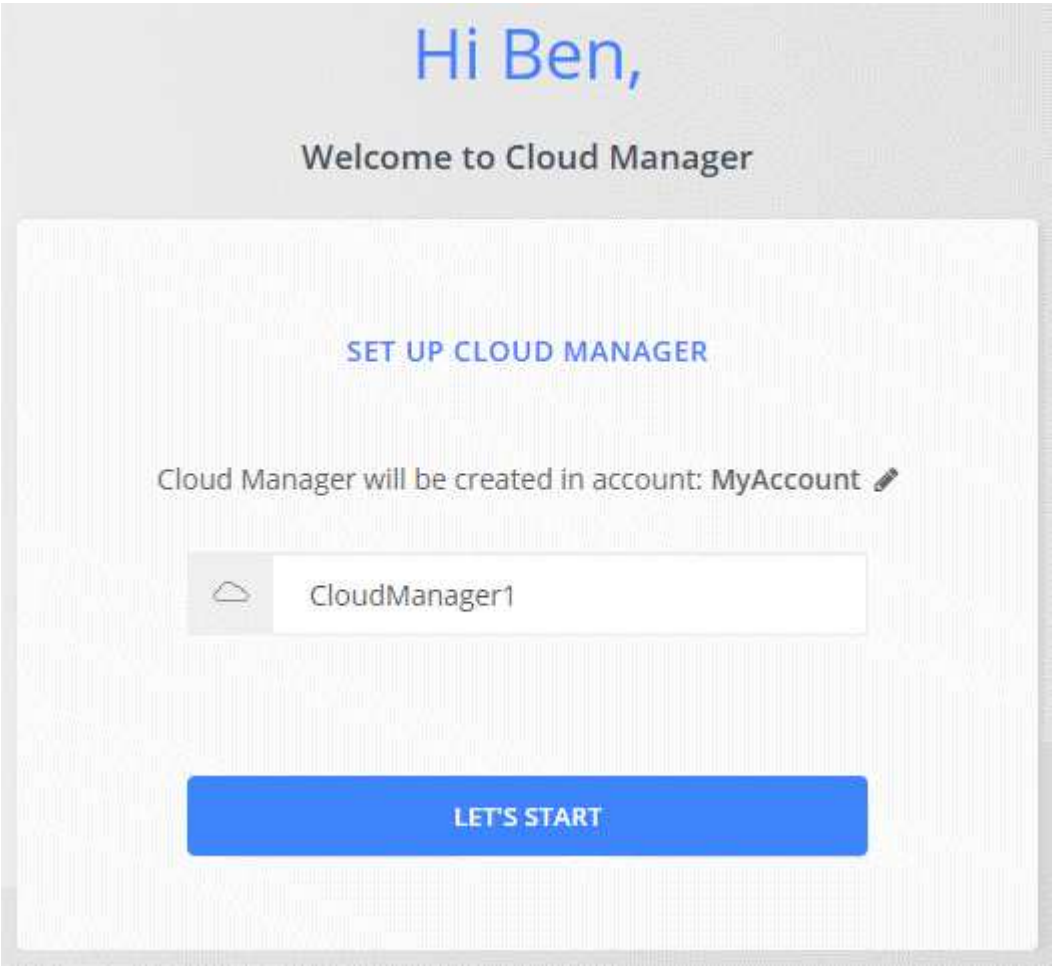
7. Abra um navegador da Web a partir de um host que tenha uma conexão com a instância do conetor e insira o seguinte URL:

http://ipaddress:80

8. Depois de iniciar sessão, configure o conetor:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor agora está instalado e configurado com sua conta do Cloud Central. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho. Mas se você tiver mais de um conetor, você precisará "alterne entre eles".

Criando um conetor a partir do Azure Marketplace

É melhor criar um conetor diretamente do Cloud Manager, mas você pode iniciar um conetor do Azure Marketplace, se preferir. Depois de criar e configurar o conetor, o Cloud Manager o usará automaticamente quando você criar novos ambientes de trabalho.

Criando um conetor no Azure

Implante o conetor no Azure usando a imagem no Azure Marketplace e faça login no conetor para especificar sua conta do Cloud Central.

Passos

1. "Vá para a página do Azure Marketplace para o Cloud Manager".
2. Clique em **Obtenha-o agora** e, em seguida, clique em **continuar**.
3. No portal do Azure, clique em **criar** e siga as etapas para configurar a máquina virtual.

   Observe o seguinte ao configurar a VM:

   - O Cloud Manager pode ter um desempenho ideal com discos HDD ou SSD.
   - Escolha um tamanho de VM que atenda aos requisitos de CPU e RAM. Recomendamos DS3 v2.

     "Revise os requisitos da VM".

   - Para o grupo de segurança de rede, o conetor requer conexões de entrada usando SSH, HTTP e HTTPS.

     "Saiba mais sobre as regras do grupo de segurança para o conetor".

   - Em **Gerenciamento**, ative **identidade gerenciada atribuída ao sistema** para o conetor selecionando **On**.

     Essa configuração é importante porque uma identidade gerenciada permite que a máquina virtual Connector se identifique no Azure ative Directory sem fornecer credenciais. "Saiba mais sobre identidades gerenciadas para recursos do Azure".

4. Na página **Revisão e criação**, revise suas seleções e clique em **criar** para iniciar a implantação.

   O Azure implanta a máquina virtual com as configurações especificadas. A máquina virtual e o software do conetor devem estar funcionando em aproximadamente cinco minutos.

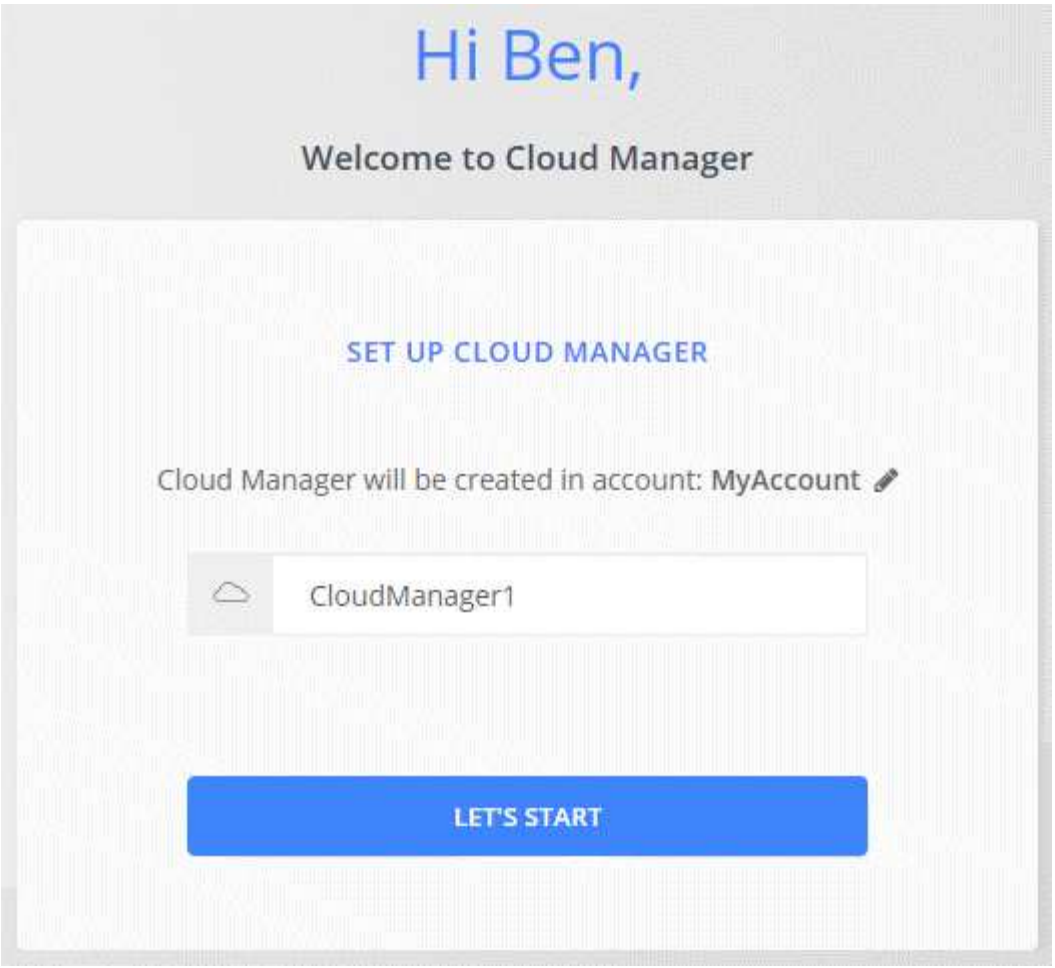
5. Abra um navegador da Web a partir de um host que tenha uma conexão com a máquina virtual do conetor e insira o seguinte URL:

   http://ipaddress:80

6. Depois de iniciar sessão, configure o conetor:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor está agora instalado e configurado. Você deve conceder permissões do Azure antes que os usuários possam implantar o Cloud Volumes ONTAP no Azure.

Concessão de permissões do Azure

Quando você implantou o conetor no Azure, você deve ter habilitado um "identidade gerenciada atribuída ao sistema". agora você deve conceder as permissões necessárias do Azure criando uma função personalizada e atribuindo a função à máquina virtual do conetor para uma ou mais assinaturas.

Passos

1. Crie uma função personalizada usando a política do Cloud Manager:

   a. Faça download do "Política do Azure do Cloud Manager".

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

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

      Exemplo

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

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

   O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Agora você deve ter uma função personalizada chamada Operador do Cloud Manager que você pode atribuir à máquina virtual do conetor.

2. Atribua a função à máquina virtual Connector para uma ou mais subscrições:
   a. Abra o serviço **assinaturas** e selecione a assinatura na qual deseja implantar sistemas Cloud Volumes ONTAP.
   b. Clique em **Access Control (IAM)**.
   c. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:
      - Selecione a função **Operador do Cloud Manager**.

        Operador do Cloud Manager é o nome padrão fornecido no "Política do Cloud Manager". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

      - Atribua acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual a máquina virtual do conetor foi criada.
      - Selecione a máquina virtual do conetor.
      - Clique em **Salvar**.
   d. Se você quiser implantar o Cloud Volumes ONTAP a partir de assinaturas adicionais, mude para essa assinatura e repita essas etapas.

Resultado

O conetor agora tem as permissões necessárias para gerenciar recursos e processos em seu ambiente de nuvem pública. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho. Mas se você tiver mais de um conetor, você precisará "alterne entre eles".

Instalar o software Connector em um host Linux existente

A maneira mais comum de criar um conetor é diretamente do Cloud Manager ou do mercado de um provedor de nuvem. Mas você tem a opção de baixar e instalar o software Connector em um host Linux existente em sua rede ou na nuvem.

Se você quiser criar um sistema Cloud Volumes ONTAP no Google Cloud, também precisa ter um conetor em execução no Google Cloud. Não é possível usar um conetor que esteja sendo executado em outro local.

Requisitos

- O host deve atender "Requisitos para o conetor"o .
- Um sistema Red Hat Enterprise Linux deve ser registrado no Red Hat Subscription Management. Se não estiver registado, o sistema não poderá aceder aos repositórios para atualizar o software de 3rd partes necessário durante a instalação.

- O instalador do conetor acessa vários URLs durante o processo de instalação. Você deve garantir que o acesso de saída à Internet é permitido a esses endpoints:
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

    O host pode tentar atualizar os pacotes do sistema operacional durante a instalação. O host pode entrar em Contato com diferentes sites de espelhamento para esses pacotes do sistema operacional.

Sobre esta tarefa

- Não são necessários Privileges raiz para instalar o conetor.
- A instalação instala as ferramentas de linha de comando da AWS (awscli) para habilitar procedimentos de recuperação do suporte ao NetApp.

  Se você receber uma mensagem informando que a instalação do awscli falhou, você pode ignorar a mensagem com segurança. O conetor pode funcionar com sucesso sem as ferramentas.

- O instalador disponível no site de suporte da NetApp pode ser uma versão anterior. Após a instalação, o conetor se atualiza automaticamente se uma nova versão estiver disponível.

Passos

1. Faça o download do software Cloud Manager no "Site de suporte da NetApp"e copie-o para o host Linux.

   Para obter ajuda para conetar e copiar o arquivo para uma instância do EC2 na AWS, "Documentação da AWS: Conexão com sua instância Linux usando SSH" consulte .

2. Atribua permissões para executar o script.

   Exemplo

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Execute o script de instalação:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent executa a instalação sem solicitar informações.

   proxy é necessário se o host estiver atrás de um servidor proxy.

   proxyport é a porta para o servidor proxy.

   proxyuser é o nome de usuário do servidor proxy, se a autenticação básica for necessária.

   proxypwd é a senha para o nome de usuário que você especificou.

3. A menos que você especificou o parâmetro silencioso, digite **Y** para continuar o script e insira as portas HTTP e HTTPS quando solicitado.

O Cloud Manager agora está instalado. No final da instalação, o serviço do Cloud Manager (occm) será reiniciado duas vezes se você tiver especificado um servidor proxy.

4. Abra um navegador da Web e insira o seguinte URL:

   https://ipaddress:port

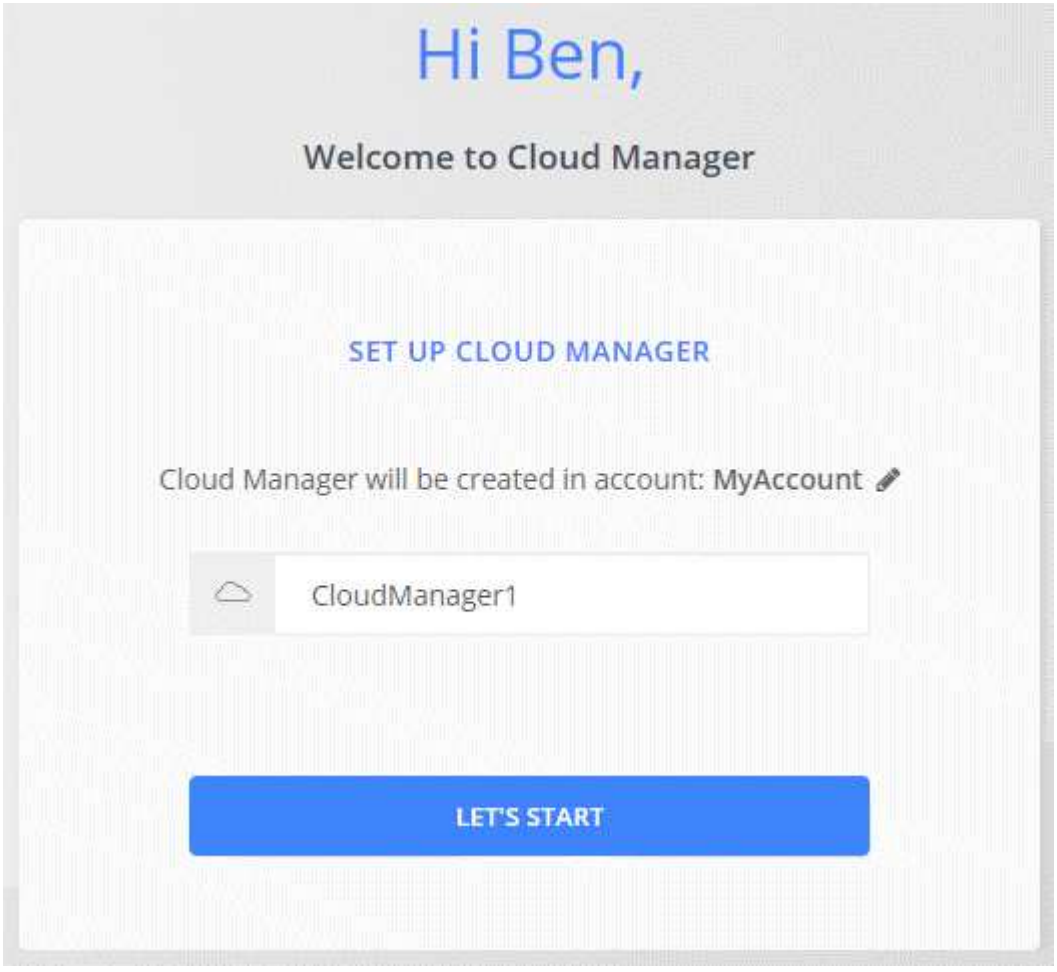
   Ipaddress pode ser localhost, um endereço IP privado ou um endereço IP público, dependendo da configuração do host. Por exemplo, se o conetor estiver na nuvem pública sem um endereço IP público, você deverá inserir um endereço IP privado de um host que tenha uma conexão com o host do conetor.

   Port é necessário se você alterou as portas HTTP (80) ou HTTPS (443) padrão. Por exemplo, se a porta HTTPS foi alterada para 8443, você digitaria https://ipaddress:8443

5. Inscreva-se no NetApp Cloud Central ou faça login.
6. Depois de fazer login, configure o Cloud Manager:
   a. Especifique a conta do Cloud Central a ser associada ao conetor.

      "Saiba mais sobre as contas do Cloud Central".

   b. Introduza um nome para o sistema.



Resultado

O conetor agora está instalado e configurado com sua conta do Cloud Central. O Cloud Manager usará automaticamente esse conetor quando você criar novos ambientes de trabalho.

Depois de terminar

Configure permissões para que o Cloud Manager possa gerenciar recursos e processos em seu ambiente de nuvem pública:

- AWS: "Configure uma conta da AWS e adicione-a ao Cloud Manager".
- Azure: "Configure uma conta do Azure e, em seguida, adicione-a ao Cloud Manager".
- GCP: Configure uma conta de serviço que tenha as permissões necessárias para criar e gerenciar sistemas Cloud Volumes ONTAP em projetos.
  a. "Crie uma função no GCP" isso inclui as permissões definidas no "Política do Cloud Manager para GCP".
  b. "Crie uma conta de serviço do GCP e aplique a função personalizada que você acabou de criar".
  c. "Associe esta conta de serviço à VM Connector".
  d. Se você quiser implantar o Cloud Volumes ONTAP em outros projetos "Conceda acesso adicionando a conta de serviço com a função Cloud Manager a esse projeto", . Você precisará repetir esta etapa para cada projeto.

Configuração padrão para o conetor

Se você precisar solucionar problemas do conetor, ele pode ajudar a entender como ele está configurado.

- Se você implantou o conetor do Cloud Manager (ou diretamente do mercado de um provedor de nuvem), observe o seguinte:
  - Na AWS, o nome de usuário da instância do EC2 Linux é EC2-user.
  - O sistema operativo da imagem é o seguinte:
    - AWS: Red Hat Enterprise Linux 7,5 (HVM)
    - Azure: Red Hat Enterprise Linux 7,6 (HVM)
    - GCP: CentOS 7,6

      O sistema operacional não inclui uma GUI. Tem de utilizar um terminal para aceder ao sistema.
- A pasta de instalação do conetor reside no seguinte local:

  /opt/application/NetApp/cloudmanager
- Os arquivos de log estão contidos na seguinte pasta:

  /opt/application/NetApp/cloudmanager/log
- O serviço Cloud Manager é chamado occm.
- O serviço occm depende do serviço MySQL.

  Se o serviço MySQL estiver inativo, o serviço occm também estará inativo.
- O Cloud Manager instala os seguintes pacotes no host Linux, se eles ainda não estiverem instalados:

- 7Zip
- AWSCLI
- Docker
- Java
- Kubectl
- MySQL
- Tridentctl
- Puxa
- Wget

- O conetor usa as seguintes portas no host Linux:
  - 80 para acesso HTTP
  - 443 para acesso HTTPS
  - 3306 para o banco de dados do Cloud Manager
  - 8080 para o proxy da API do Cloud Manager
  - 8666 para a API Service Manager
  - 8777 para a Health-Checker Container Service API

Gerenciar credenciais

AWS

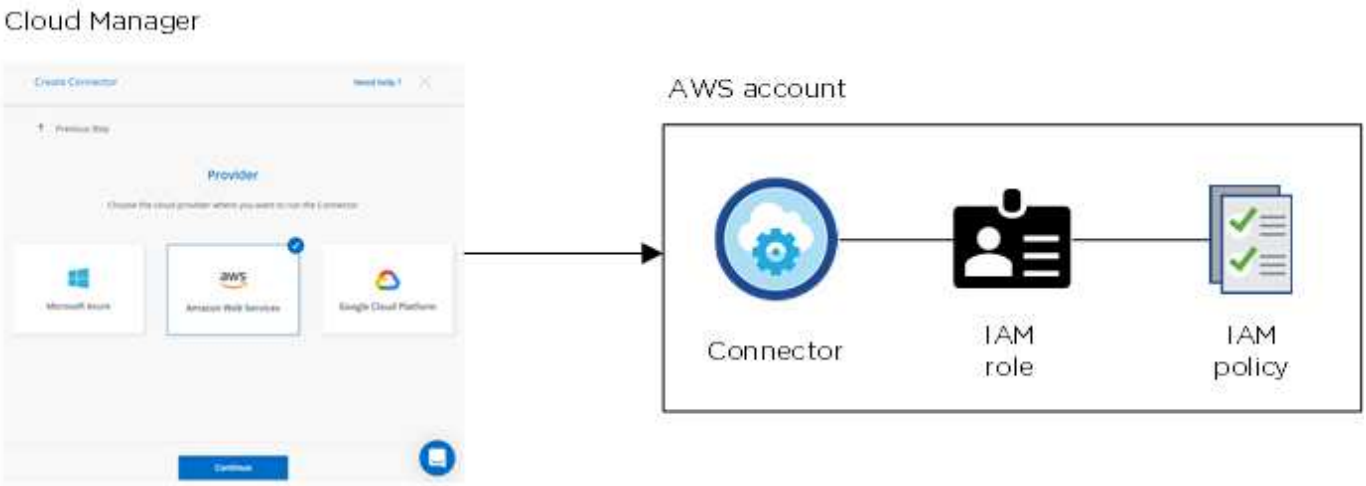
Credenciais e permissões da AWS

O Cloud Manager permite que você escolha as credenciais da AWS a serem usadas ao implantar o Cloud Volumes ONTAP. Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais da AWS ou adicionar credenciais adicionais.

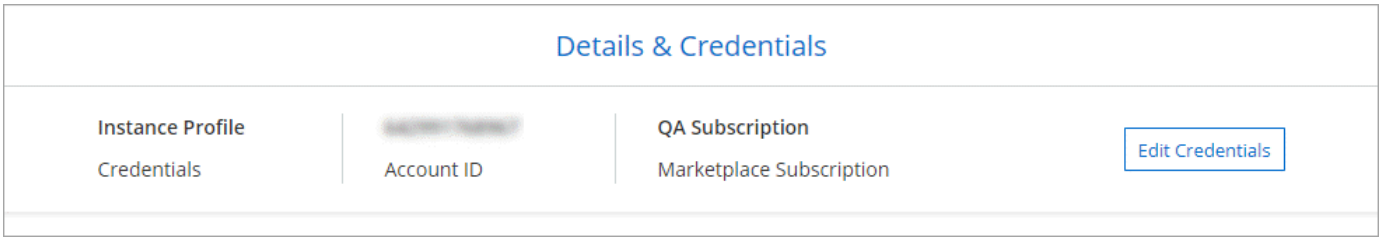
Credenciais iniciais da AWS

Ao implantar um conetor do Cloud Manager, você precisa usar uma conta da AWS que tenha permissões para iniciar a instância do Connector. As permissões necessárias estão listadas no "Política de implantação do Connector para AWS".

Quando o Cloud Manager inicia a instância do Connector na AWS, ele cria uma função do IAM e um perfil de instância para a instância. Ele também anexa uma política que fornece ao Cloud Manager permissões para gerenciar recursos e processos dentro dessa conta da AWS. "Veja como o Cloud Manager usa as permissões".

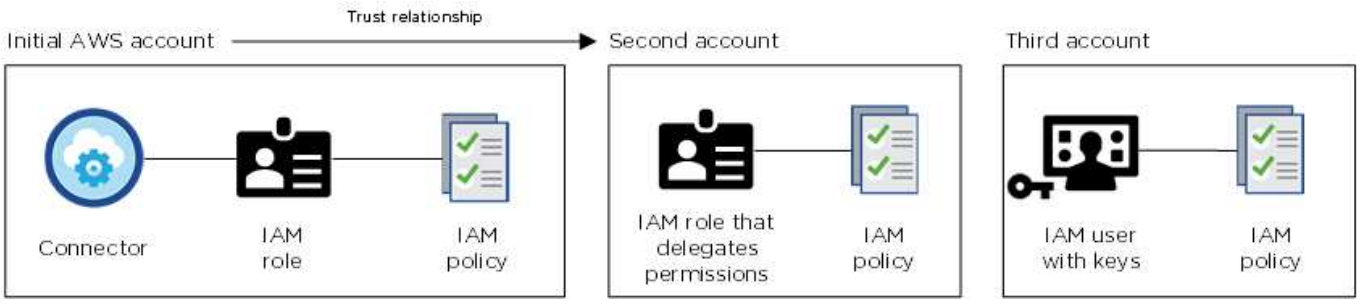


O Cloud Manager seleciona essas credenciais da AWS por padrão quando você cria um novo ambiente de trabalho para o Cloud Volumes ONTAP:



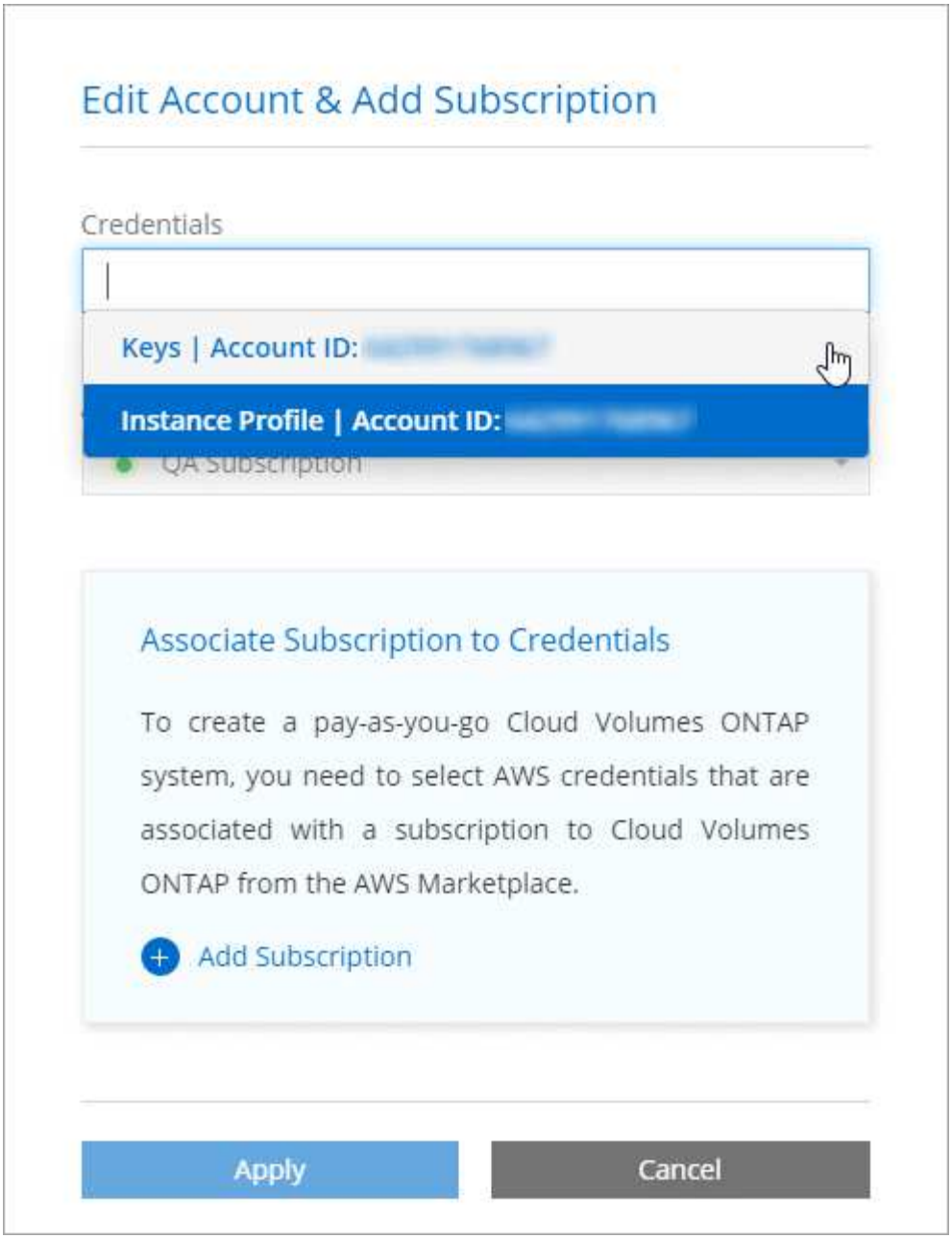
Credenciais adicionais da AWS

Se você quiser iniciar o Cloud Volumes ONTAP em diferentes contas da AWS, poderá usar "Forneça chaves da AWS para um usuário do IAM ou o ARN de uma função em uma conta confiável"o . A imagem a seguir mostra duas contas adicionais, uma fornecendo permissões por meio de uma função do IAM em uma conta confiável e outra por meio das chaves da AWS de um usuário do IAM:



Você deve "Adicione as credenciais da conta ao Cloud Manager"especificar o nome do recurso Amazon (ARN) da função do IAM ou as chaves da AWS para o usuário do IAM.

Depois de adicionar outro conjunto de credenciais, você pode alternar para elas ao criar um novo ambiente de trabalho:



E quanto às implantações do Marketplace e às implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é do Cloud Manager. Também é possível implantar um conetor na AWS a partir do "AWS Marketplace" e "Instale o conetor no local"do .

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a função do IAM e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, não é possível configurar uma função do IAM para o sistema do Cloud Manager, mas você pode fornecer permissões da mesma forma que faria para contas adicionais da AWS.

Como posso girar com segurança minhas credenciais da AWS?

Como descrito acima, o Cloud Manager permite que você forneça credenciais da AWS de algumas maneiras:

Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS.

Com as duas primeiras opções, o Cloud Manager usa o AWS Security Token Service para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática - é automático e seguro.

Se você fornecer ao Cloud Manager chaves de acesso da AWS, gire as chaves atualizando-as no Cloud Manager em um intervalo regular. Este é um processo completamente manual.

Gerenciamento de credenciais e assinaturas da AWS para o Cloud Manager

Ao criar um sistema Cloud Volumes ONTAP, você precisa selecionar as credenciais e a assinatura da AWS para usar com esse sistema. Se você gerenciar várias assinaturas da AWS, poderá atribuir cada uma delas a diferentes credenciais da AWS na página credenciais.

Antes de adicionar credenciais da AWS ao Cloud Manager, você precisa fornecer as permissões necessárias para essa conta. As permissões permitem que o Cloud Manager gerencie recursos e processos dentro dessa conta da AWS. A forma como você fornece as permissões depende se deseja fornecer ao Cloud Manager chaves AWS ou o ARN de uma função em uma conta confiável.

Quando você implantou um conetor do Cloud Manager, o Cloud Manager adicionou automaticamente credenciais da AWS para a conta na qual implantou o conetor. Esta conta inicial não é adicionada se você instalou manualmente o software Connector em um sistema existente. "Saiba mais sobre as credenciais e permissões da AWS".

Escolhas

- Concessão de permissões fornecendo chaves da AWS
- Concessão de permissões assumindo funções do IAM em outras contas

Como posso girar com segurança minhas credenciais da AWS?

O Cloud Manager permite que você forneça credenciais da AWS de algumas maneiras: Uma função do IAM associada à instância do Connector, assumindo uma função do IAM em uma conta confiável ou fornecendo chaves de acesso da AWS. "Saiba mais sobre as credenciais e permissões da AWS".

Com as duas primeiras opções, o Cloud Manager usa o AWS Security Token Service para obter credenciais temporárias que rodam constantemente. Este processo é a melhor prática, é automático e seguro.

Se você fornecer ao Cloud Manager chaves de acesso da AWS, gire as chaves atualizando-as no Cloud Manager em um intervalo regular. Este é um processo completamente manual.

Concessão de permissões fornecendo chaves da AWS

Se você quiser fornecer ao Cloud Manager chaves da AWS para um usuário do IAM, precisará conceder as permissões necessárias a esse usuário. A política do IAM do Cloud Manager define as ações e recursos da AWS que o Cloud Manager pode usar.

Passos

1. Faça download da política do IAM do Cloud Manager no "Página de políticas do Cloud Manager".
2. No console do IAM, crie sua própria política copiando e colando o texto da política do IAM do Cloud Manager.

   "Documentação da AWS: Criando políticas do IAM"

3. Anexe a política a uma função do IAM ou a um usuário do IAM.
   - "Documentação da AWS: Criando funções do IAM"
   - "Documentação da AWS: Adicionando e removendo políticas do IAM"

Resultado

A conta agora tem as permissões necessárias. Agora você pode adicioná-lo ao Cloud Manager.

Concessão de permissões assumindo funções do IAM em outras contas

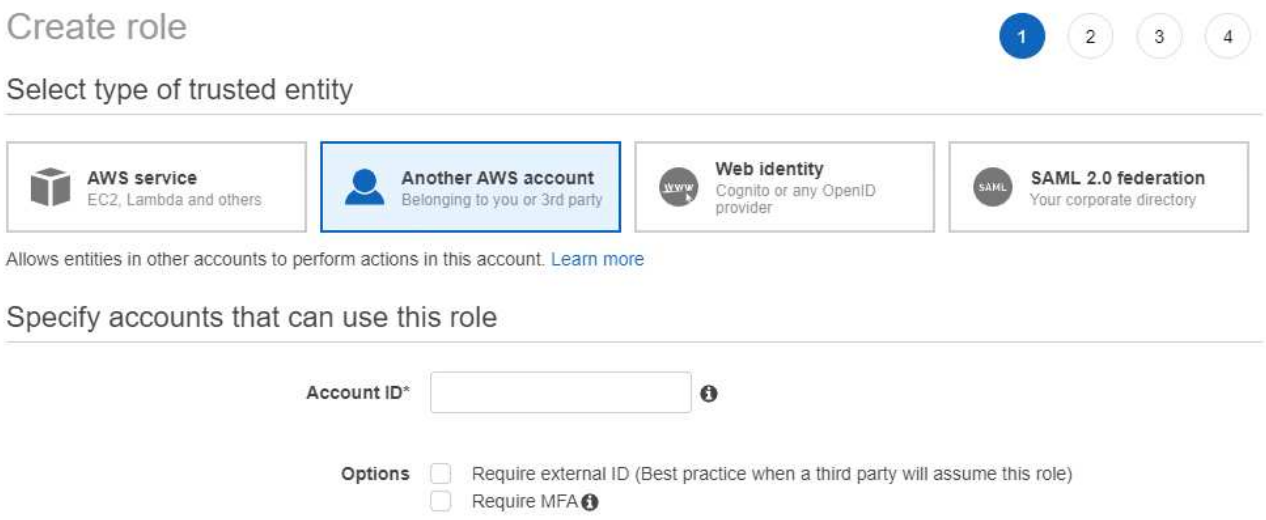
Você pode configurar uma relação de confiança entre a conta da AWS de origem na qual implantou a instância do Connector e outras contas da AWS usando funções do IAM. Em seguida, você fornecerá ao Cloud Manager o ARN das funções do IAM das contas confiáveis.

Passos

1. Vá para a conta de destino onde você deseja implantar o Cloud Volumes ONTAP e criar uma função do IAM selecionando **outra conta da AWS**.

   Certifique-se de fazer o seguinte:

   - Insira o ID da conta onde reside a instância do conetor.
   - Anexe a política do IAM do Cloud Manager, que está disponível no "Página de políticas do Cloud Manager".



2. Vá para a conta de origem onde reside a instância do conetor e selecione a função do IAM que está anexada à instância.

   a. Clique em **Anexar políticas** e, em seguida, clique em **criar política**.

   b. Crie uma política que inclua a ação "sts:AssumeRole" e o ARN da função que você criou na conta de destino.

Exemplo

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Resultado

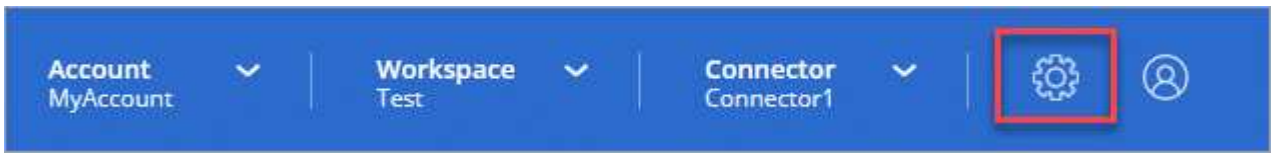
A conta agora tem as permissões necessárias. Agora você pode adicioná-lo ao Cloud Manager.

Adição de credenciais da AWS ao Cloud Manager

Depois de fornecer uma conta da AWS com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Cloud Manager. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



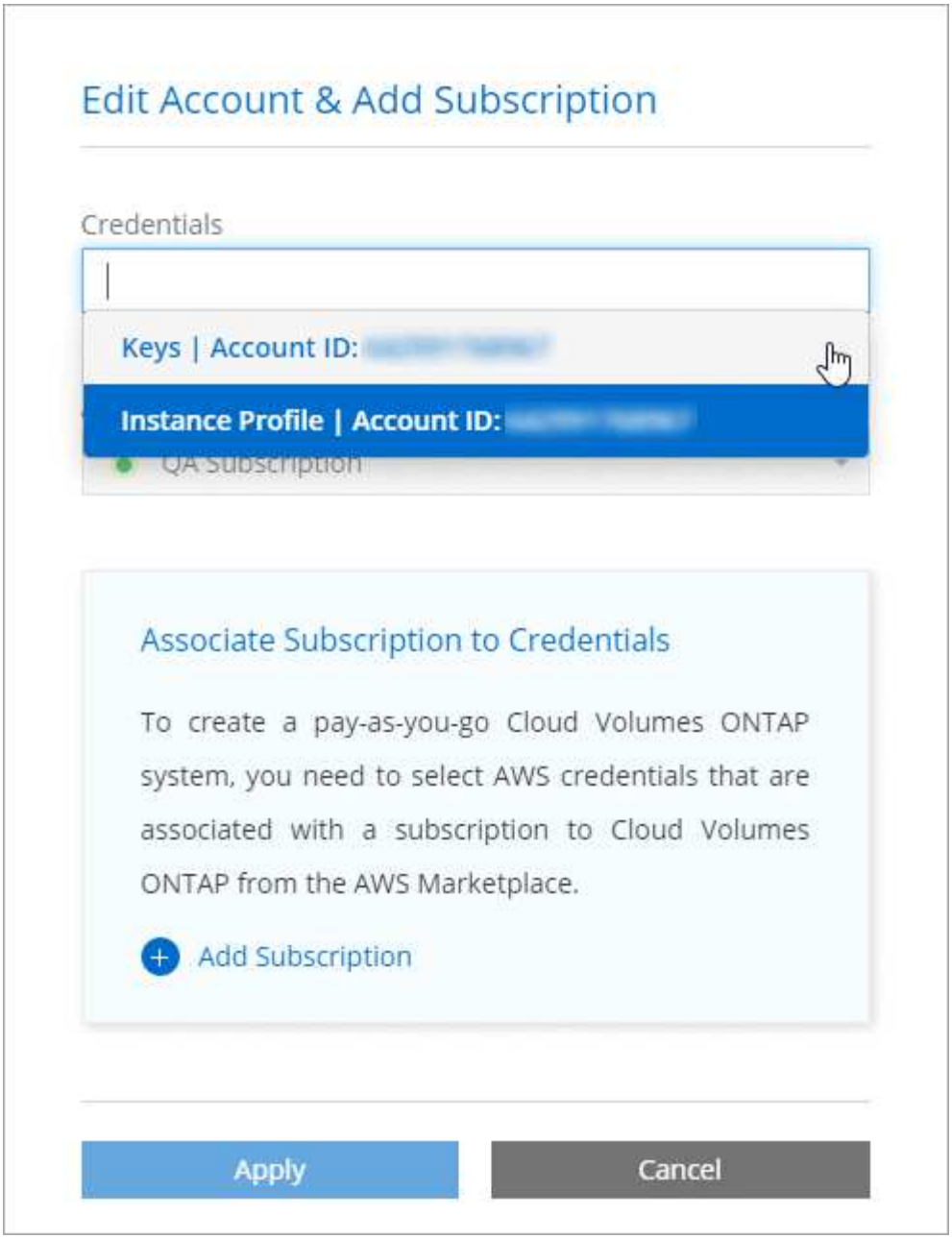
2. Clique em **Adicionar credenciais** e selecione **AWS**.
3. Forneça chaves da AWS ou o ARN de uma função IAM confiável.
4. Confirme se os requisitos da política foram atendidos e clique em **continuar**.
5. Escolha a assinatura paga conforme o uso que você deseja associar às credenciais ou clique em **Adicionar assinatura** se você ainda não tiver uma.

   Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, as credenciais da AWS devem estar associadas a uma assinatura do Cloud Volumes ONTAP no mercado AWS.

6. Clique em **Add**.

Resultado

Agora você pode alternar para um conjunto diferente de credenciais da página Detalhes e credenciais ao criar um novo ambiente de trabalho:



Associando uma assinatura da AWS às credenciais

Depois de adicionar suas credenciais da AWS ao Cloud Manager, você pode associar uma assinatura do AWS Marketplace a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Há dois cenários em que você pode associar uma assinatura do AWS Marketplace depois de adicionar as credenciais ao Cloud Manager:

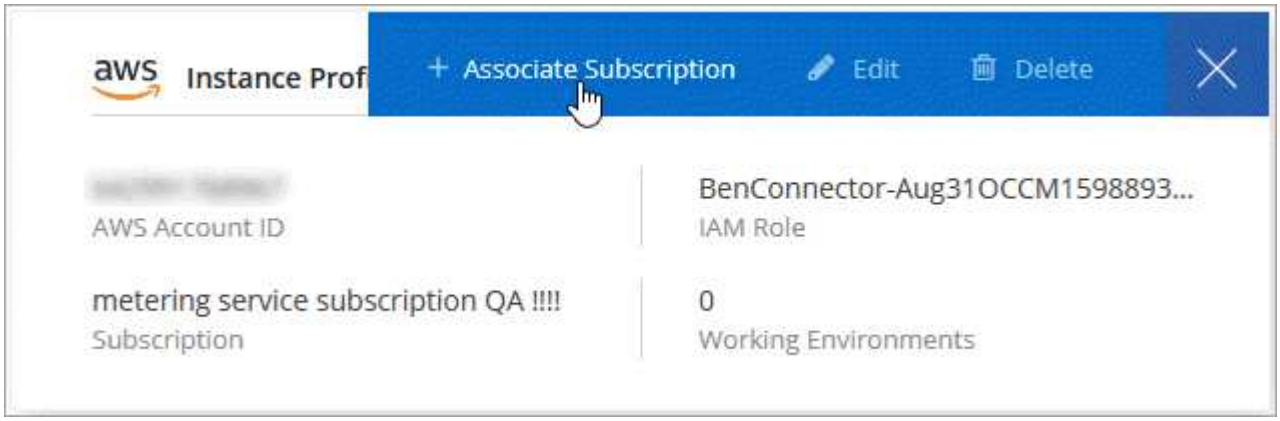
- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Cloud Manager.
- Você deseja substituir uma assinatura existente do AWS Marketplace por uma nova assinatura.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione uma assinatura na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.

   ► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

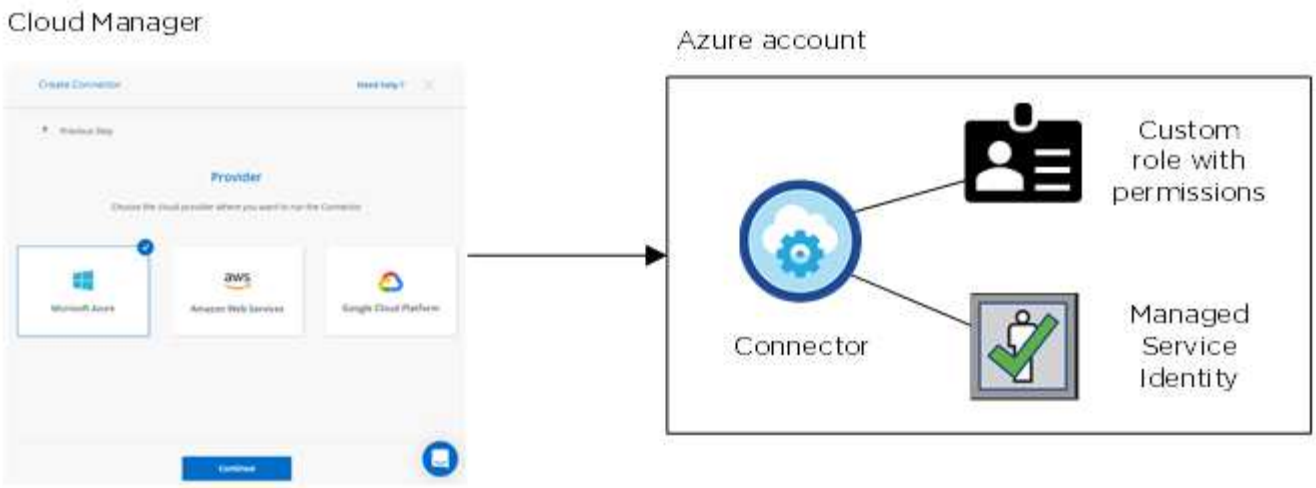
Credenciais e permissões do Azure

O Cloud Manager permite que você escolha as credenciais do Azure a serem usadas ao implantar o Cloud Volumes ONTAP. Você pode implantar todos os seus sistemas Cloud Volumes ONTAP usando as credenciais iniciais do Azure ou adicionar credenciais adicionais.

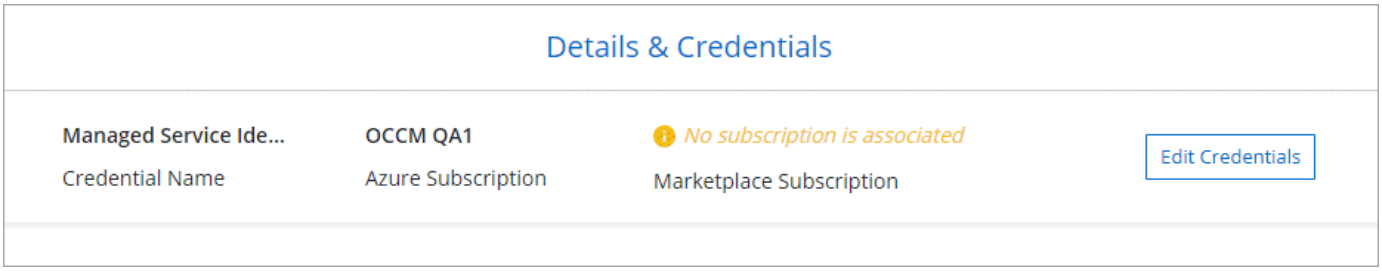
Credenciais iniciais do Azure

Ao implantar um conetor do Cloud Manager, você precisa usar uma conta do Azure que tenha permissões para implantar a máquina virtual do Connector. As permissões necessárias estão listadas no "Política de implantação do Connector para Azure".

Quando o Cloud Manager implanta a máquina virtual Connector no Azure, ele ativa uma "identidade gerenciada atribuída ao sistema" máquina virtual on, cria uma função personalizada e a atribui à máquina virtual. A função fornece ao Cloud Manager permissões para gerenciar recursos e processos dentro dessa assinatura do Azure. "Veja como o Cloud Manager usa as permissões".



O Cloud Manager seleciona essas credenciais do Azure por padrão quando você cria um novo ambiente de trabalho para o Cloud Volumes ONTAP:

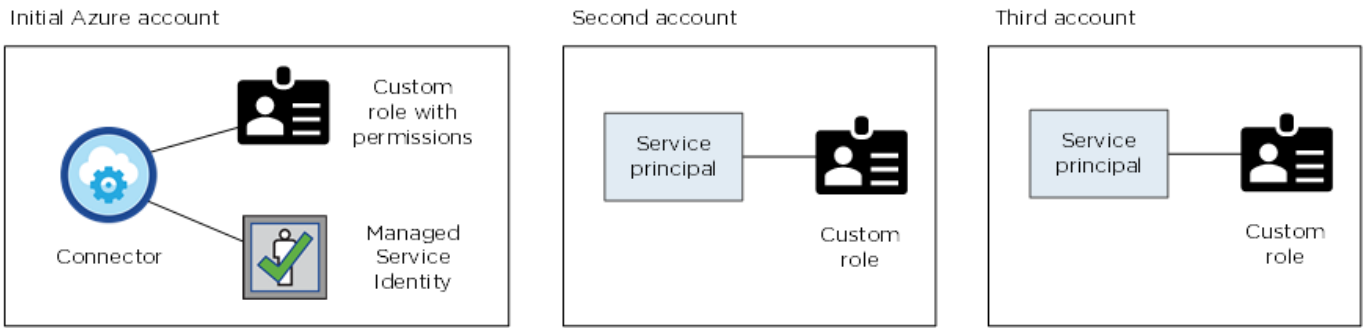


Subscrições adicionais do Azure para uma identidade gerida

A identidade gerenciada está associada à assinatura na qual você lançou o conetor. Se você quiser selecionar uma assinatura diferente do Azure, precisará "associe a identidade gerenciada a essas assinaturas"do .

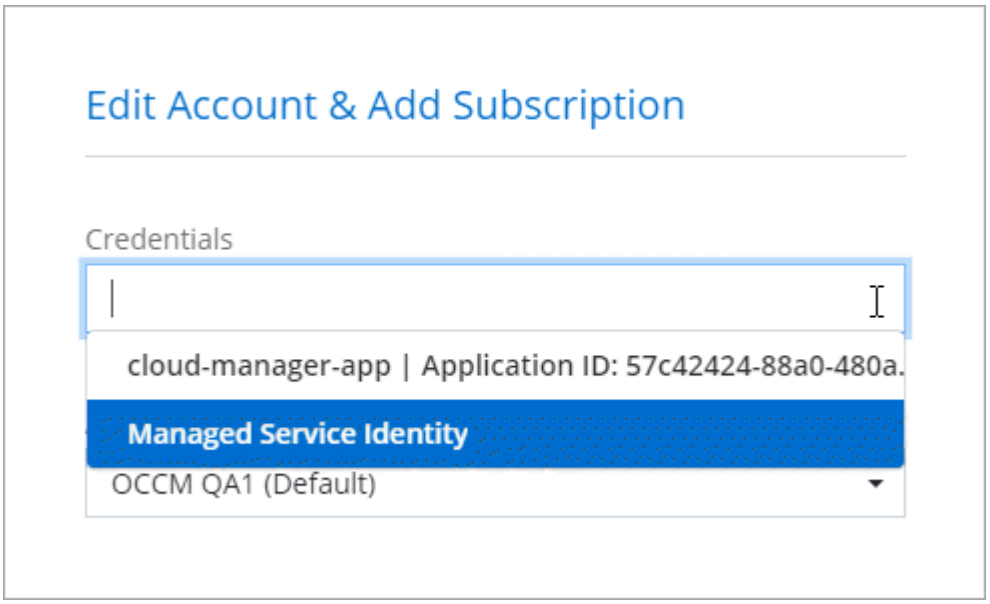
Credenciais adicionais do Azure

Se você quiser implantar o Cloud Volumes ONTAP usando diferentes credenciais do Azure, você deve conceder as permissões necessárias para "Criando e configurando um princípio de serviço no Azure ative Directory"cada conta do Azure. A imagem a seguir mostra duas contas adicionais, cada uma configurada com uma função principal de serviço e personalizada que fornece permissões:



Em seguida, você "Adicione as credenciais da conta ao Cloud Manager"forneceria detalhes sobre o diretor de serviço do AD.

Depois de adicionar outro conjunto de credenciais, você pode alternar para elas ao criar um novo ambiente de trabalho:



E quanto às implantações do Marketplace e às implantações locais?

As seções acima descrevem o método de implantação recomendado para o conetor, que é do NetApp Cloud Central. Você também pode implantar um conetor no Azure a partir do "Azure Marketplace", e pode "Instale o conetor no local".

Se você usar o Marketplace, as permissões serão fornecidas da mesma maneira. Você só precisa criar e configurar manualmente a identidade gerenciada para o conetor e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, não é possível configurar uma identidade gerenciada para o conetor, mas você pode fornecer permissões da mesma forma que faria para contas adicionais usando um princípio de serviço.

Gerenciamento de credenciais e assinaturas do Azure para o Cloud Manager

Ao criar um sistema Cloud Volumes ONTAP, você precisa selecionar as credenciais do Azure e a assinatura do Marketplace para usar com esse sistema. Se você gerenciar várias assinaturas do Azure Marketplace, poderá atribuir cada uma delas a diferentes credenciais do Azure na página credenciais.

Há duas maneiras de gerenciar credenciais do Azure no Cloud Manager. Primeiro, se você quiser implantar o Cloud Volumes ONTAP em diferentes contas do Azure, precisará fornecer as permissões necessárias e adicionar as credenciais ao Cloud Manager. A segunda maneira é associar assinaturas adicionais à identidade gerenciada do Azure.

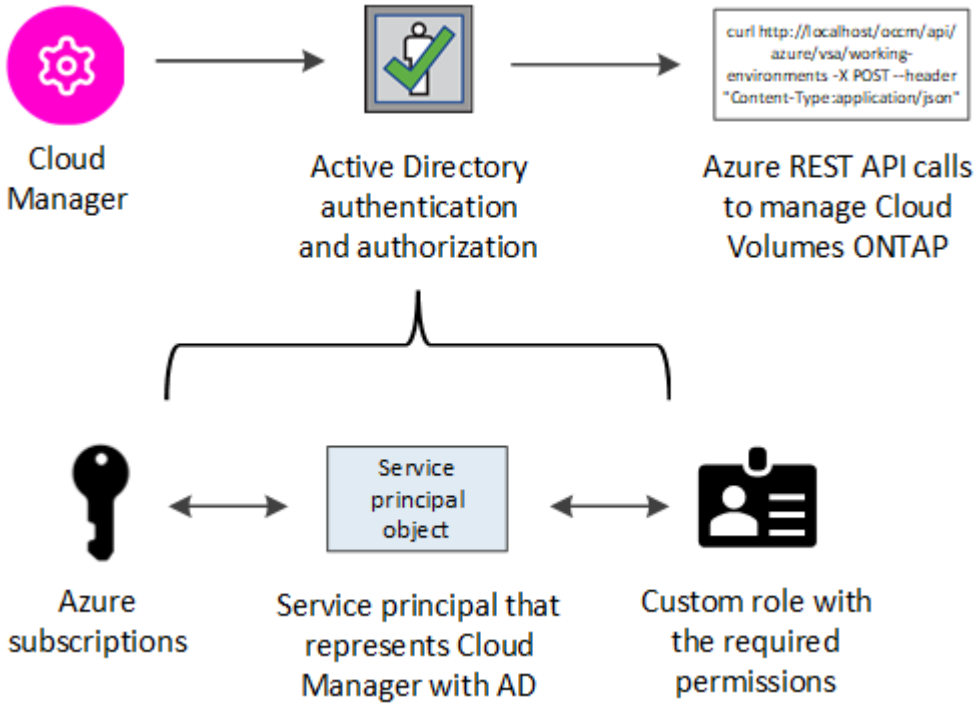
Ao implantar um conetor do Cloud Manager, o Cloud Manager adiciona automaticamente a conta do Azure na qual você implantou o conetor. Uma conta inicial não será adicionada se você tiver instalado manualmente o software Connector em um sistema existente. "Saiba mais sobre as contas e permissões do Azure".

Concessão de permissões do Azure usando um princípio de serviço

O Cloud Manager precisa de permissões para executar ações no Azure. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando um responsável de serviço no Azure ative Directory e obtendo as credenciais do Azure de que o Cloud Manager precisa.

Sobre esta tarefa

A imagem a seguir mostra como o Cloud Manager obtém permissões para executar operações no Azure. Um objeto principal de serviço, vinculado a uma ou mais assinaturas do Azure, representa o Cloud Manager no Azure ative Directory e é atribuído a uma função personalizada que permite as permissões necessárias.



Passos

1. Crie uma aplicação Azure ative Directory.
2. Atribua a aplicação a uma função.
3. Adicione permissões da API de Gerenciamento de Serviços do Windows Azure.
4. Obtenha o ID do aplicativo e o ID do diretório.
5. Crie um segredo de cliente.

Criando um aplicativo Azure ative Directory

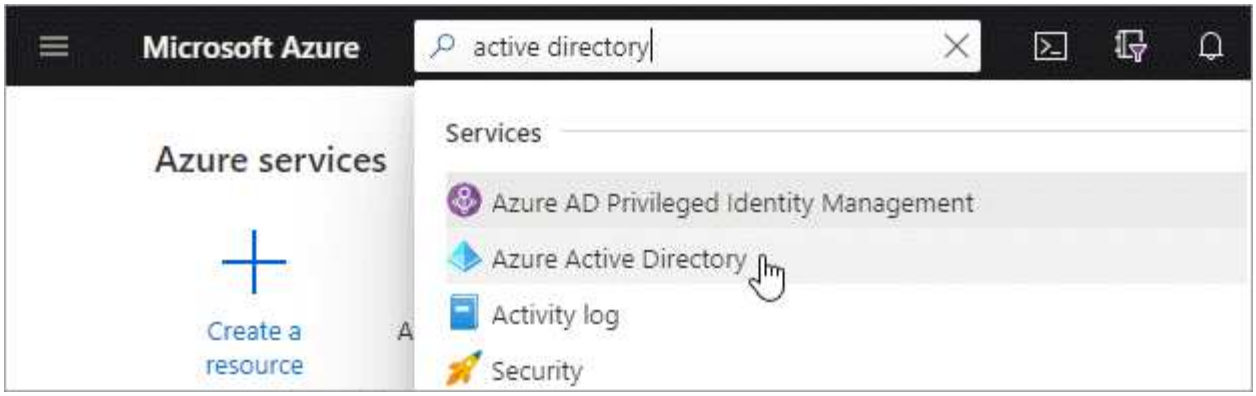
Crie um aplicativo e um diretor de serviço do Azure ative Directory (AD) que o Cloud Manager pode usar para controle de acesso baseado em funções.

Antes de começar

Você deve ter as permissões certas no Azure para criar um aplicativo do ative Directory e atribuir o aplicativo a uma função. Para obter detalhes, "Documentação do Microsoft Azure: Permissões necessárias" consulte .

Passos

1. No portal do Azure, abra o serviço **Azure ative Directory**.



2. No menu, clique em **inscrições de aplicativos**.
3. Clique em **novo registo**.
4. Especifique detalhes sobre o aplicativo:
   - **Nome**: Insira um nome para o aplicativo.
   - **Tipo de conta**: Selecione um tipo de conta (qualquer funcionará com o Cloud Manager).
   - * URI de redirecionamento*: Selecione **Web** e, em seguida, insira qualquer URL, por exemplo, https://url
5. Clique em **Register**.

Resultado

Você criou o aplicativo AD e o principal de serviço.

Atribuindo a aplicação a uma função

Você deve vincular o principal de serviço a uma ou mais assinaturas do Azure e atribuir-lhe a função personalizada "Operador do Gerenciador de nuvem do OnCommand" para que o Gerenciador de nuvem tenha permissões no Azure.

Passos

1. Crie uma função personalizada:

   a. Faça download do "Política do Azure do Cloud Manager".

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

   Você deve adicionar o ID para 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.

O exemplo a seguir mostra como criar uma função personalizada usando a CLI do Azure 2,0:

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Agora você deve ter uma função personalizada chamada *Cloud Manager Operator*.

2. Atribua o aplicativo à função:

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

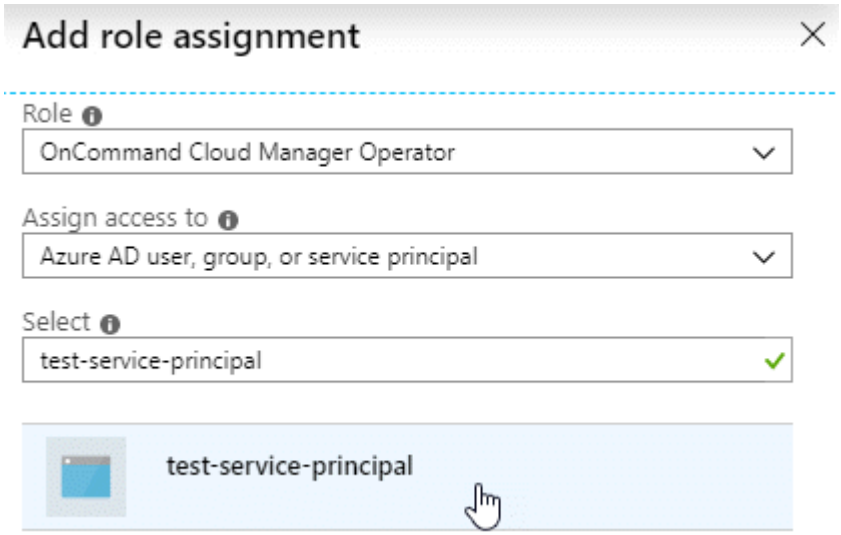
   b. Selecione a subscrição.

   c. Clique em **Access control (IAM) > Add > Add Role assignment** (Adicionar > Adicionar atribuição de função*).

   d. Selecione a função **Operador do Cloud Manager**.

   e. Mantenha **Usuário, grupo ou responsável de serviço do Azure AD** selecionado.

   f. Procure o nome do aplicativo (você não pode encontrá-lo na lista rolando).



   g. Selecione o aplicativo e clique em **Salvar**.

   O responsável de serviço do Cloud Manager agora tem as permissões necessárias do Azure para essa assinatura.

Se você quiser implantar o Cloud Volumes ONTAP a partir de várias assinaturas do Azure, então você deve vincular o principal de serviço a cada uma dessas assinaturas. O Cloud Manager permite que você selecione a assinatura que deseja usar ao implantar o Cloud Volumes ONTAP.

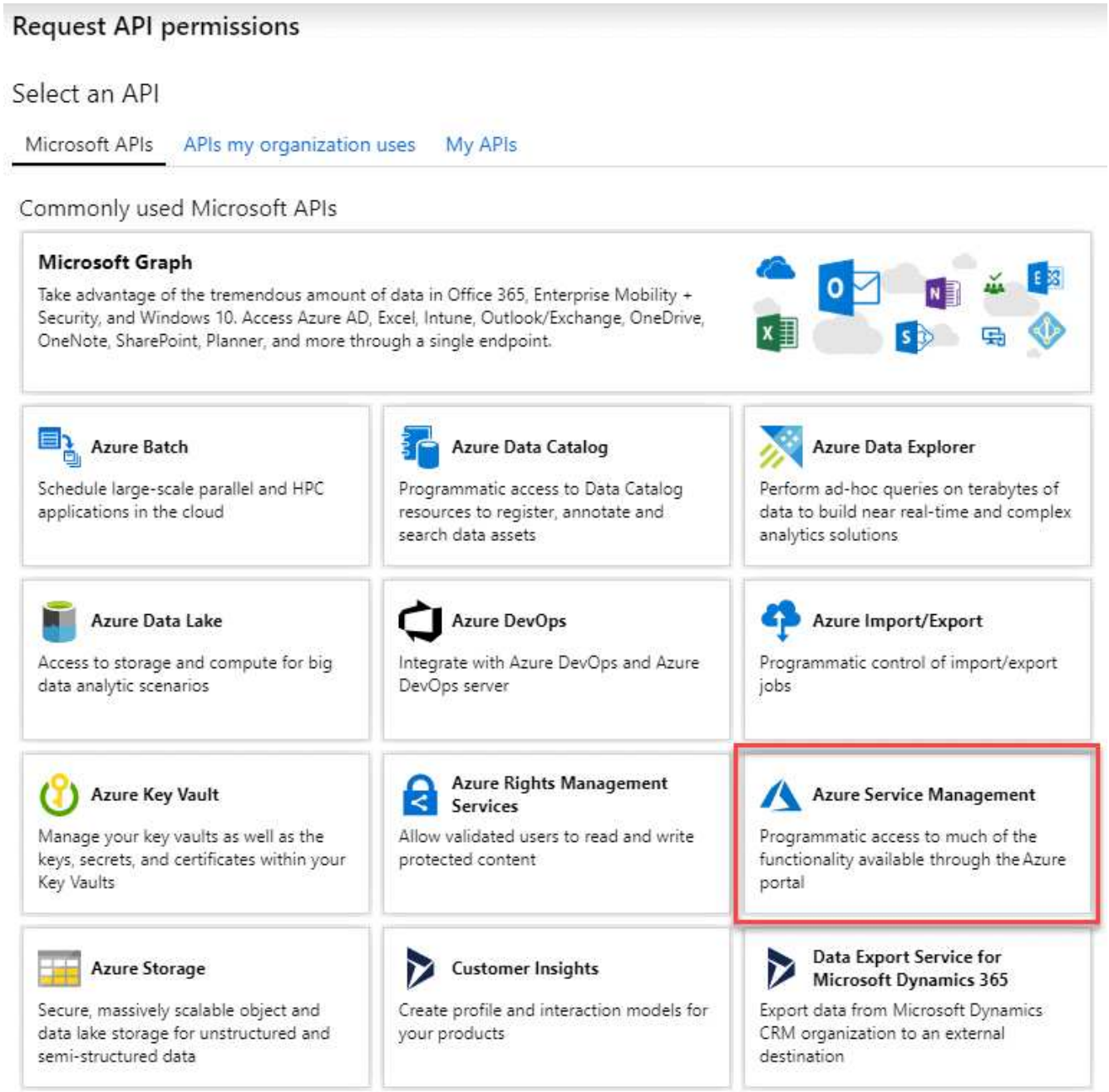
Adicionando permissões de API de Gerenciamento de Serviços do Windows Azure

O responsável do serviço deve ter permissões "Windows Azure Service Management API".

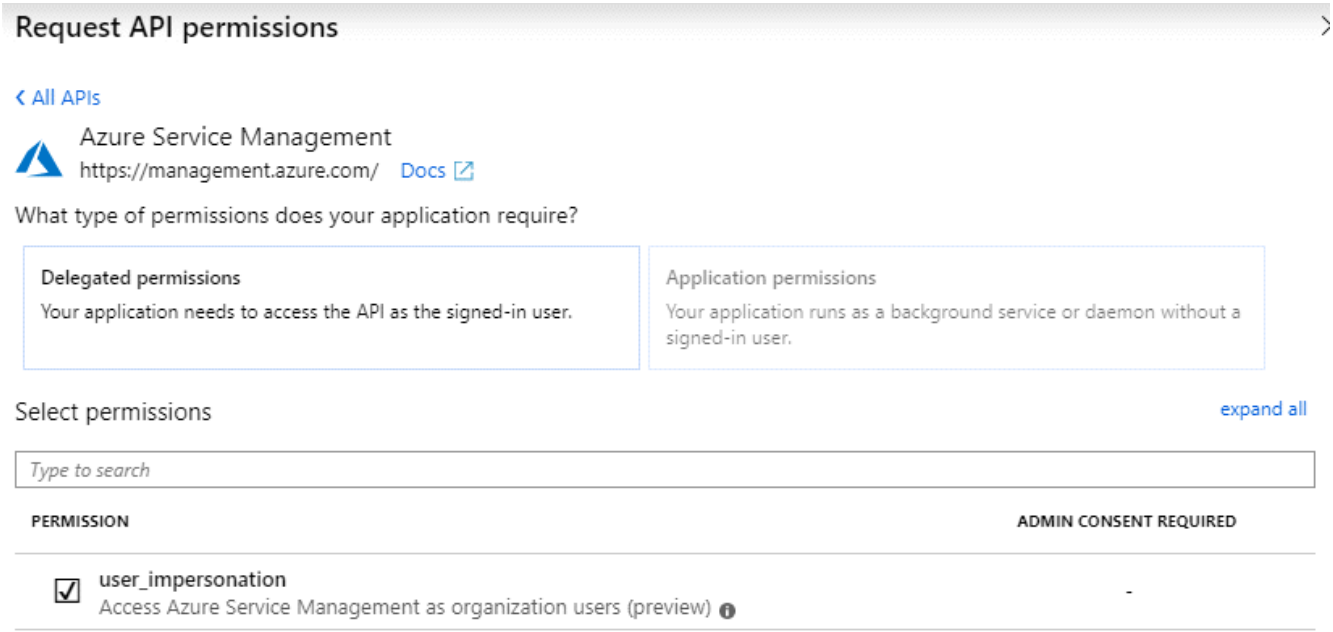
Passos

1. No serviço **Azure ative Directory**, clique em **inscrições de aplicativos** e selecione o aplicativo.
2. Clique em **permissões de API > Adicionar uma permissão**.

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



4. Clique em **Acesse o Gerenciamento de Serviços do Azure como usuários da organização** e clique em **Adicionar permissões**.

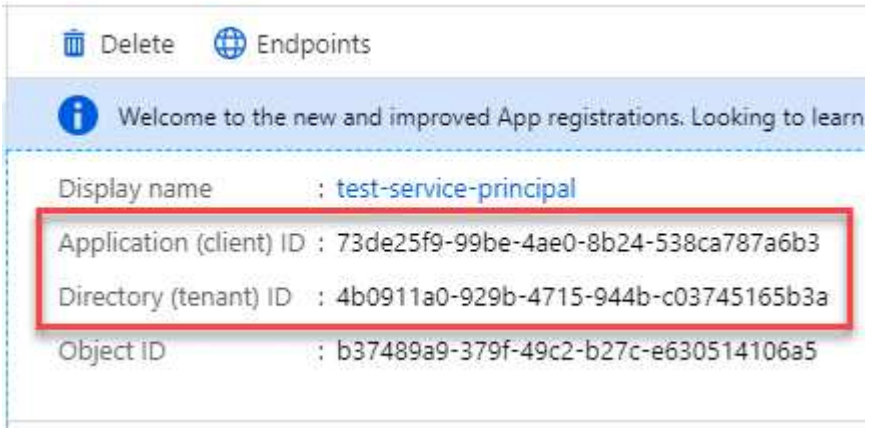


Obtendo o ID do aplicativo e o ID do diretório

Quando você adiciona a conta do Azure ao Cloud Manager, você precisa fornecer o ID do aplicativo (cliente) e o ID do diretório (locatário) para o aplicativo. O Cloud Manager usa as IDs para fazer login programaticamente.

Passos

1. No serviço **Azure ative Directory**, clique em **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Criando um segredo de cliente

Você precisa criar um segredo de cliente e, em seguida, fornecer ao Cloud Manager o valor do segredo para que o Cloud Manager possa usá-lo para autenticar com o Azure AD.

Quando você adiciona a conta ao Cloud Manager, o Cloud Manager se refere ao segredo do cliente como a chave do aplicativo.

Passos

1. Abra o serviço **Azure ative Directory**.
2. Clique em **inscrições de aplicativos** e selecione sua inscrição.
3. Clique em **certificados e segredos > segredo de novo cliente**.
4. Forneça uma descrição do segredo e uma duração.
5. Clique em **Add**.
6. Copie o valor do segredo do cliente.

Resultado

Seu responsável de serviço 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 Cloud Manager ao adicionar uma conta do Azure.

Adição de credenciais do Azure ao Cloud Manager

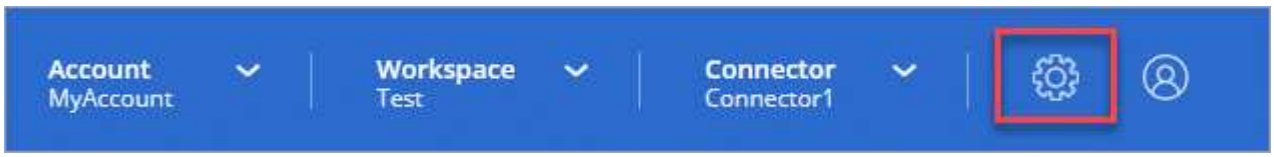
Depois de fornecer uma conta do Azure com as permissões necessárias, você pode adicionar as credenciais dessa conta ao Cloud Manager. Isso permite que você inicie sistemas Cloud Volumes ONTAP nessa conta.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



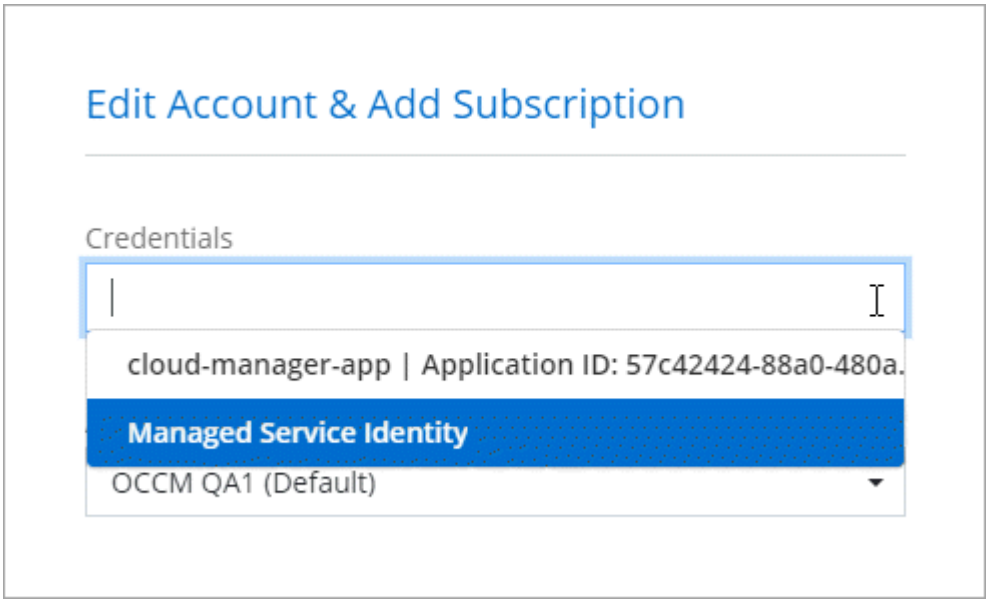
2. Clique em **Adicionar credenciais** e selecione **Microsoft Azure**.
3. Insira informações sobre o principal de serviço do Azure ative Directory que concede as permissões necessárias:
   - ID da aplicação (cliente): Obtendo o ID do aplicativo e o ID do diretórioConsulte .
   - ID do diretório (locatário): Obtendo o ID do aplicativo e o ID do diretórioConsulte .
   - Segredo do cliente: Criando um segredo de clienteConsulte .
4. Confirme se os requisitos da política foram atendidos e clique em **continuar**.
5. Escolha a assinatura paga conforme o uso que você deseja associar às credenciais ou clique em **Adicionar assinatura** se você ainda não tiver uma.

Para criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso, as credenciais do Azure devem estar associadas a uma assinatura do Cloud Volumes ONTAP no mercado Azure.

6. Clique em **Add**.

Resultado

Agora você pode alternar para diferentes conjuntos de credenciais na página Detalhes e credenciais "ao criar um novo ambiente de trabalho":



Associar uma subscrição do Azure Marketplace às credenciais

Depois de adicionar suas credenciais do Azure ao Cloud Manager, você pode associar uma assinatura do Azure Marketplace a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Há dois cenários em que você pode associar uma assinatura do Azure Marketplace depois de já ter adicionado as credenciais ao Cloud Manager:

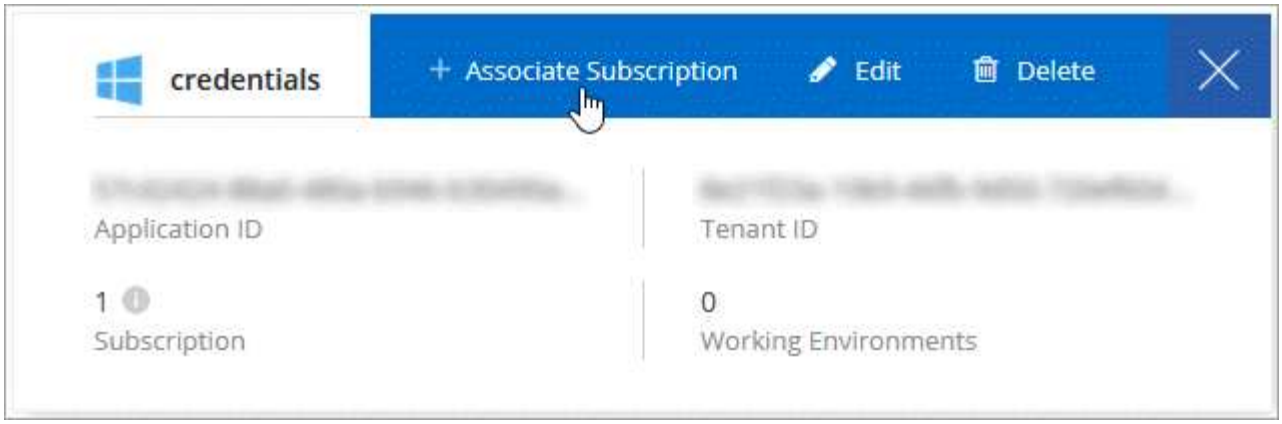
- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Cloud Manager.
- Você deseja substituir uma assinatura existente do Azure Marketplace por uma nova assinatura.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione uma assinatura na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.

   O vídeo a seguir começa no contexto do assistente de ambiente de trabalho, mas mostra o mesmo fluxo de trabalho depois de clicar em **Adicionar assinatura**:

   ► https://docs.netapp.com/pt-br/occm38//media/video_subscribing_azure.mp4 *(video)*

Associar subscrições adicionais do Azure a uma identidade gerida

O Cloud Manager permite que você escolha as credenciais do Azure e a assinatura do Azure na qual você deseja implantar o Cloud Volumes ONTAP. Não é possível selecionar uma assinatura diferente do Azure para o perfil de identidade gerenciado, a menos que você associe a "identidade gerenciada" essas assinaturas.

Sobre esta tarefa

Uma identidade gerenciada é "A conta inicial do Azure" quando você implementa um conetor do Cloud Manager. Quando você implantou o conetor, o Cloud Manager criou a função Operador do Cloud Manager e atribuiu-a à máquina virtual do conetor.

Passos

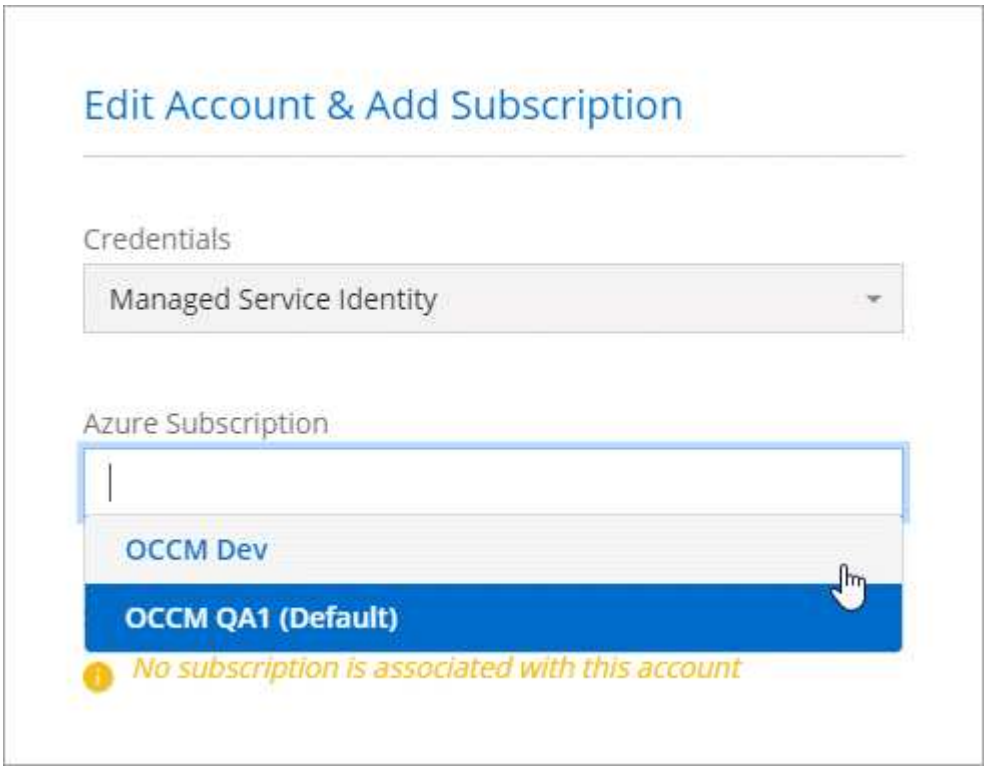
1. Faça login no portal do Azure.
2. Abra o serviço **assinaturas** e selecione a assinatura na qual deseja implantar o Cloud Volumes ONTAP.
3. Clique em **Access Control (IAM)**.
   a. Clique em **Adicionar** > **Adicionar atribuição de função** e, em seguida, adicione as permissões:
      - Selecione a função **Operador do Cloud Manager**.

        Operador do Cloud Manager é o nome padrão fornecido no "Política do Cloud Manager". Se você escolher um nome diferente para a função, selecione esse nome em vez disso.

      - Atribua acesso a uma **Máquina Virtual**.
      - Selecione a assinatura na qual a máquina virtual do conetor foi criada.
      - Selecione a máquina virtual do conetor.
      - Clique em **Salvar**.
4. Repita estes passos para subscrições adicionais.

Resultado

Ao criar um novo ambiente de trabalho, agora você deve ter a capacidade de selecionar entre várias assinaturas do Azure para o perfil de identidade gerenciado.



GCP

Projetos, permissões e contas do Google Cloud

Uma conta de serviço fornece ao Cloud Manager permissões para implantar e gerenciar sistemas Cloud Volumes ONTAP no mesmo projeto que o Cloud Manager ou em projetos diferentes.

Projeto e permissões para o Cloud Manager

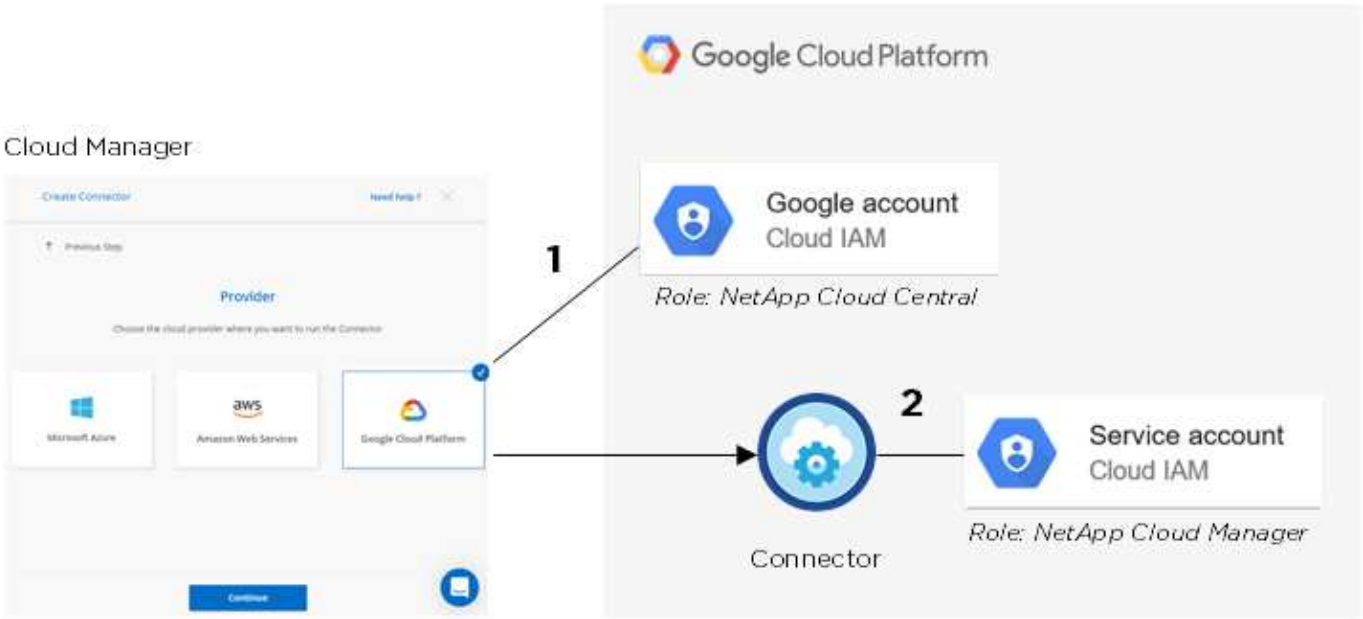
Antes de implantar o Cloud Volumes ONTAP no Google Cloud, você deve primeiro implantar um conetor em um projeto do Google Cloud. O conetor não pode ser executado em suas instalações ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de implantar um conetor diretamente do Cloud Manager:

1. Você precisa implantar um conetor usando uma conta do Google que tenha permissões para iniciar a instância de VM do Connector do Cloud Manager.
2. Ao implantar o conetor, você será solicitado a selecionar um "conta de serviço" para a instância de VM. O Cloud Manager obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP em seu nome. As permissões são fornecidas anexando uma função personalizada à conta de serviço.

Nós configuramos dois arquivos YAML que incluem as permissões necessárias para o usuário e a conta de serviço. "Saiba como usar os arquivos YAML para configurar permissões".

A imagem a seguir mostra os requisitos de permissão descritos nos números 1 e 2 acima:



Projeto para Cloud Volumes ONTAP

O Cloud Volumes ONTAP pode residir no mesmo projeto que o conetor, ou em um projeto diferente. Para implantar o Cloud Volumes ONTAP em um projeto diferente, você precisa primeiro adicionar a conta de serviço do Connector e a função a esse projeto.

- "Saiba como configurar a conta de serviço (consulte o passo 2)".
- "Saiba como implantar o Cloud Volumes ONTAP no GCP e selecione um projeto".

Conte com a categorização de dados

O Cloud Manager requer uma conta do GCP para o Cloud Volumes ONTAP 9,6, mas não para 9,7 e posterior. Para usar a disposição de dados em categorias com o Cloud Volumes ONTAP 9,7, siga a etapa 4 em "Introdução ao Cloud Volumes ONTAP no Google Cloud Platform".

É necessário adicionar uma conta do Google Cloud ao Cloud Manager para habilitar a disposição de dados em categorias em um sistema Cloud Volumes ONTAP 9,6. A categorização de dados categoriza automaticamente os dados inativos no storage de objetos de baixo custo, permitindo que você recupere espaço no storage primário e diminua o storage secundário.

Ao adicionar a conta, você precisa fornecer ao Cloud Manager uma chave de acesso ao storage para uma conta de serviço que tenha permissões de administrador do storage. O Cloud Manager usa as chaves de acesso para configurar e gerenciar um bucket do Cloud Storage para categorização de dados.

Depois de adicionar uma conta do Google Cloud, é possível habilitar a disposição em categorias de dados em volumes individuais ao criá-los, modificá-los ou replicá-los.

- "Saiba como configurar e adicionar contas do GCP ao Cloud Manager".
- "Saiba como categorizar dados inativos em armazenamento de objetos de baixo custo".

Gerenciamento de credenciais e assinaturas do GCP para o Cloud Manager

Você pode gerenciar dois tipos de credenciais do Google Cloud Platform a partir do Cloud Manager: As credenciais associadas à instância de VM Connector e às chaves de acesso ao storage usadas com um sistema Cloud Volumes ONTAP 9,6 para "categorização de dados".

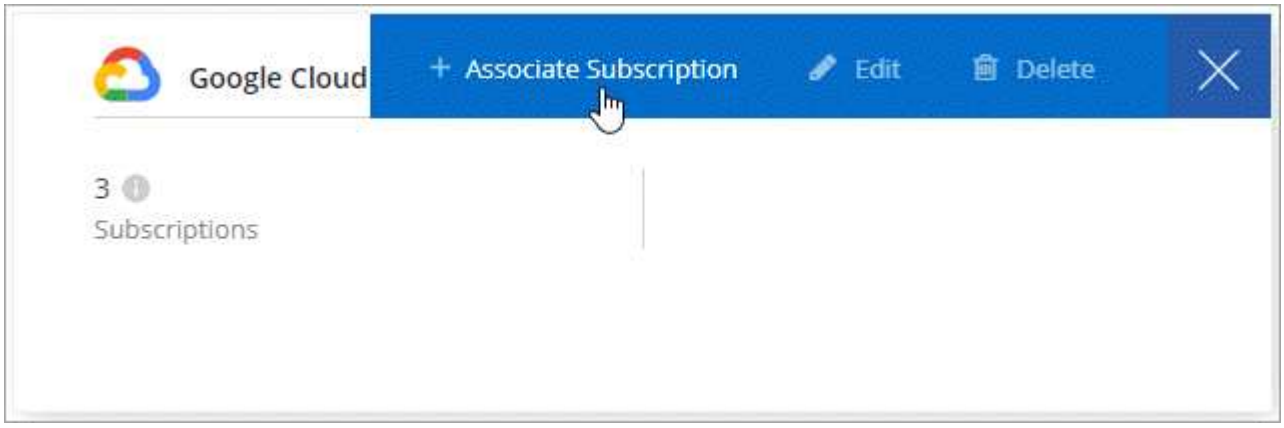
Associar uma assinatura do Marketplace às credenciais do GCP

Ao implantar um conetor no GCP, o Cloud Manager cria um conjunto padrão de credenciais associadas à instância de VM do Connector. Essas são as credenciais que o Cloud Manager usa para implantar o Cloud Volumes ONTAP.

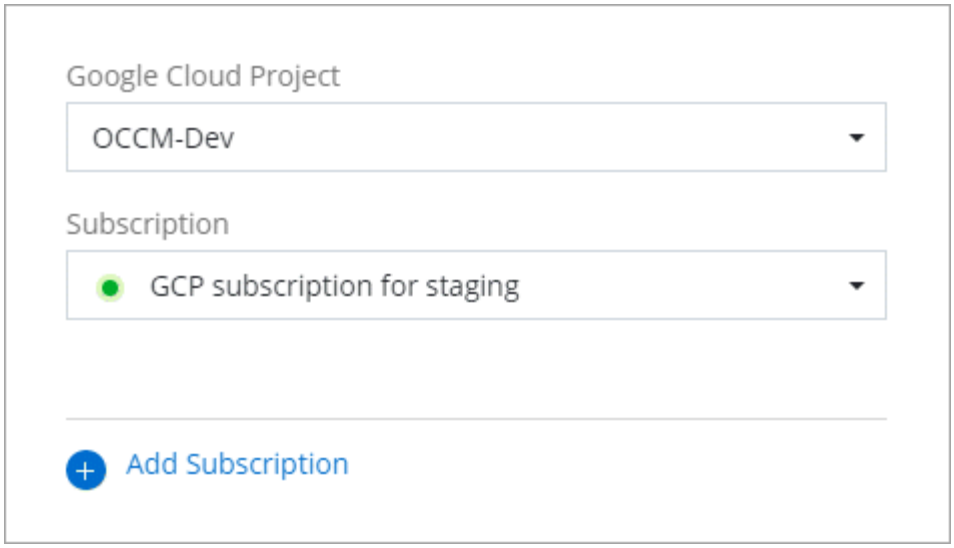
A qualquer momento, você pode alterar a assinatura do Marketplace associada a essas credenciais. A assinatura permite criar um sistema Cloud Volumes ONTAP com pagamento conforme o uso e usar outros serviços de nuvem da NetApp.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.
2. Passe o Mouse sobre um conjunto de credenciais e clique no menu de ação.
3. No menu, clique em **assinatura associada**.



4. Selecione um projeto e uma assinatura do Google Cloud na lista suspensa ou clique em **Adicionar assinatura** e siga as etapas para criar uma nova assinatura.



5. Clique em **Associate**.

Configuração e adição de contas do GCP para categorização de dados com o Cloud Volumes ONTAP 9,6

Se você quiser habilitar um sistema Cloud Volumes ONTAP 9,6 para "categorização de dados", você precisa fornecer ao Cloud Manager uma chave de acesso ao armazenamento para uma conta de serviço que tenha permissões de administrador de armazenamento. O Cloud Manager usa as chaves de acesso para configurar e gerenciar um bucket do Cloud Storage para categorização de dados.

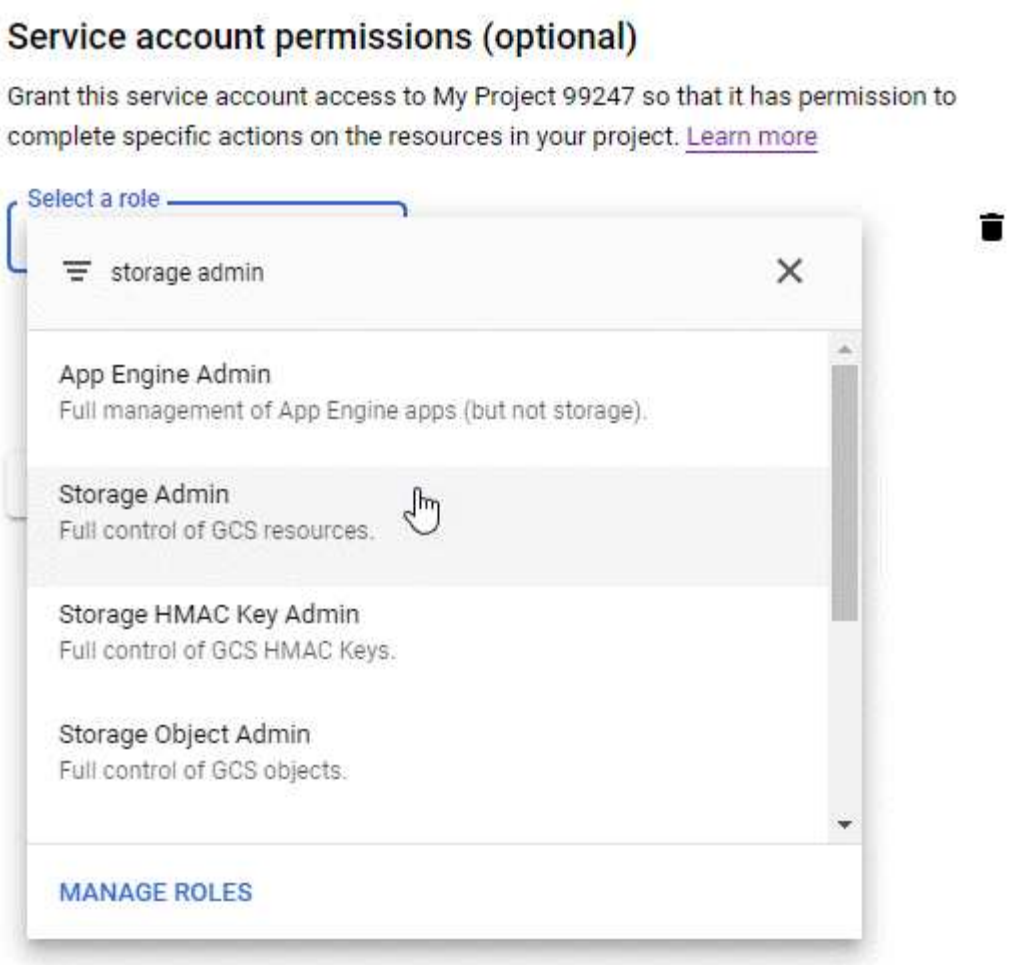
Para usar a disposição de dados em categorias com o Cloud Volumes ONTAP 9,7, siga a etapa 4 em "Introdução ao Cloud Volumes ONTAP no Google Cloud Platform".

Configurar uma conta de serviço e chaves de acesso para o Google Cloud Storage

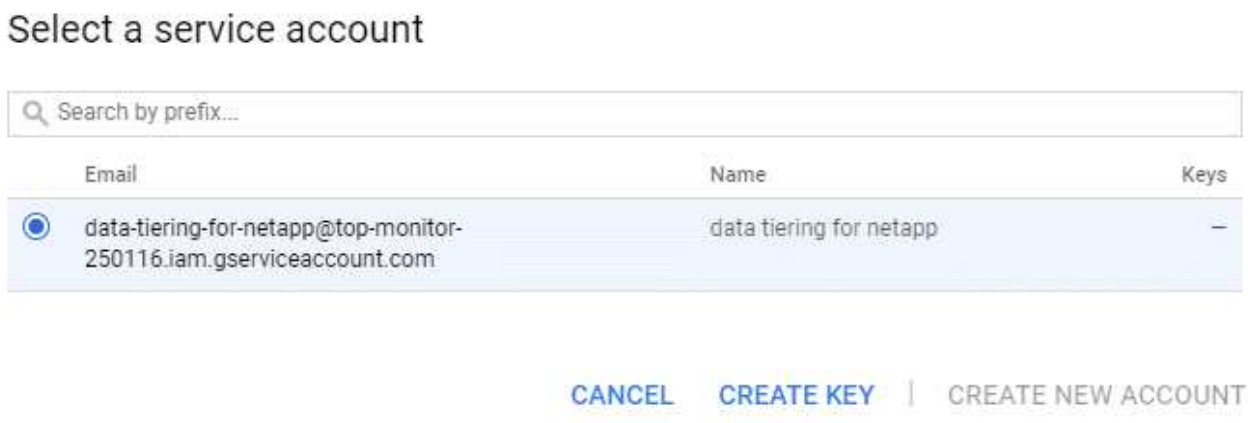
Uma conta de serviço permite que o Cloud Manager autentique e acesse buckets do Cloud Storage usados para categorização de dados. As chaves são necessárias para que o Google Cloud Storage saiba quem está fazendo a solicitação.

Passos

1. Abra o console do IAM do GCP e "Crie uma conta de serviço que tenha a função Administrador do storage"o .



2. Vá para "Configurações de armazenamento do GCP".
3. Se você for solicitado, selecione um projeto.
4. Clique no separador **interoperabilidade**.
5. Se ainda não o tiver feito, clique em **Ativar acesso à interoperabilidade**.
6. Em **chaves de acesso para contas de serviço**, clique em **criar uma chave para uma conta de serviço**.
7. Selecione a conta de serviço criada na etapa 1.



8. Clique em **criar chave**.

9. Copie a chave de acesso e o segredo.

   Você precisará inserir essas informações no Cloud Manager ao adicionar a conta do GCP para categorização de dados.

Adicionando uma conta do GCP ao Cloud Manager

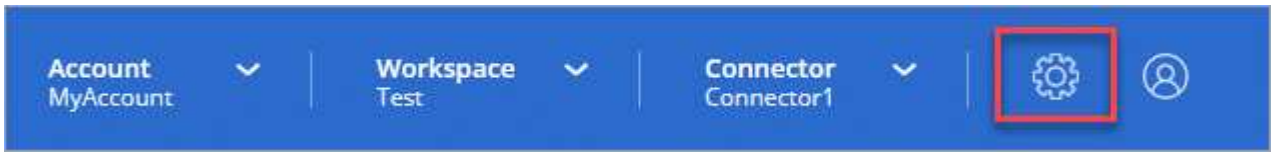
Agora que você tem uma chave de acesso para uma conta de serviço, pode adicioná-la ao Cloud Manager.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



2. Clique em **Adicionar credenciais** e selecione **Google Cloud**.
3. Introduza a chave de acesso e o segredo da conta de serviço.

   As chaves permitem que o Cloud Manager configure um bucket do Cloud Storage para categorização de dados.

4. Confirme se os requisitos da política foram atendidos e clique em **criar conta**.

O que se segue?

Agora é possível habilitar a disposição de dados em categorias em volumes individuais em um sistema Cloud Volumes ONTAP 9,6 ao criá-los, modificá-los ou replicá-los. Para obter detalhes, "Disposição em camadas dos dados inativos em storage de objetos de baixo custo"consulte .

Mas antes de fazer isso, certifique-se de que a sub-rede na qual o Cloud Volumes ONTAP reside esteja configurada para o acesso privado do Google. Para obter instruções, "Documentação do Google Cloud: Configurando o acesso privado do Google" consulte .

Adicionar contas do site de suporte da NetApp ao Cloud Manager

É necessário adicionar sua conta do site de suporte da NetApp ao Cloud Manager para implantar um sistema BYOL. Também é necessário Registrar sistemas pay-as-you-go e atualizar o software ONTAP.

Assista ao vídeo a seguir para saber como adicionar contas do site de suporte da NetApp ao Cloud Manager. Ou role para baixo para ler os passos.

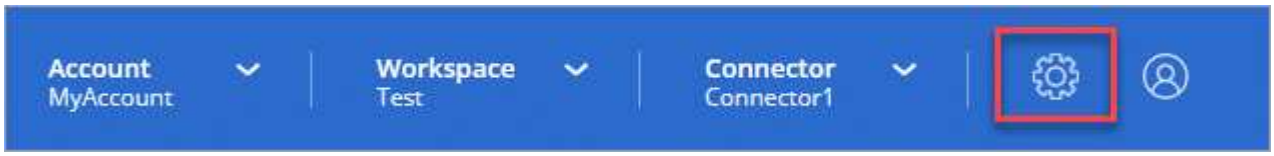
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. Se você ainda não tiver uma conta do site de suporte da NetApp, "registre-se para um".
2. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **credenciais**.



3. Clique em **Adicionar credenciais** e selecione **Site de suporte da NetApp**.
4. Especifique um nome para a conta e, em seguida, introduza o nome de utilizador e a palavra-passe.
   - A conta deve ser uma conta de cliente (não uma conta de convidado ou temporária).
   - Se você planeja implantar sistemas BYOL:
     - A conta deve estar autorizada a acessar os números de série dos sistemas BYOL.
     - Se você comprou uma assinatura BYOL segura, então uma conta NSS segura será necessária.
5. Clique em **criar conta.**

O que se segue?

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

- "Iniciando o Cloud Volumes ONTAP na AWS"
- "Iniciar o Cloud Volumes ONTAP no Azure"
- "Registar sistemas de pagamento conforme o uso"
- "Saiba como o Cloud Manager gerencia arquivos de licença"

Gerenciamento de usuários, workspaces, conetores e assinaturas

"Depois de executar a configuração inicial", Talvez seja necessário administrar as configurações da conta posteriormente gerenciando usuários, espaços de trabalho, conetores e assinaturas.

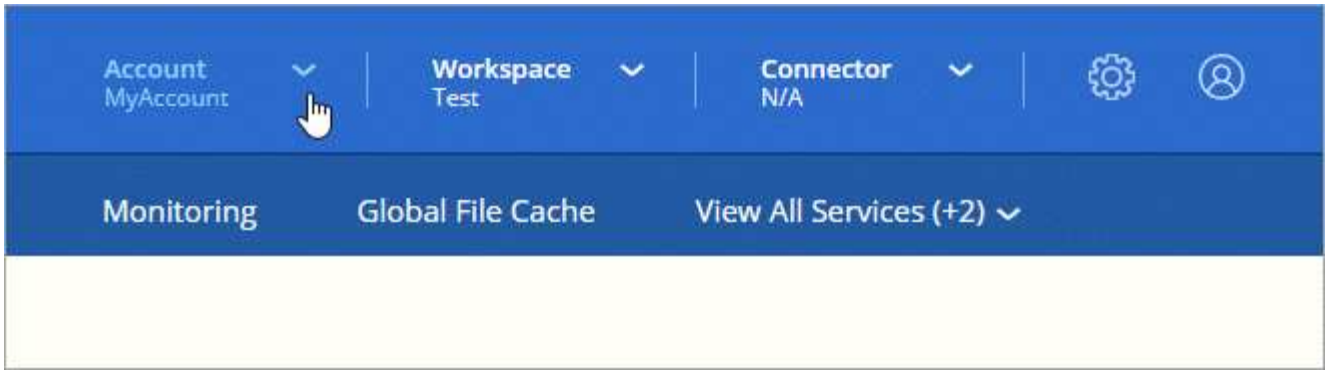
"Saiba mais sobre como as contas do Cloud Central funcionam".

Adicionando usuários

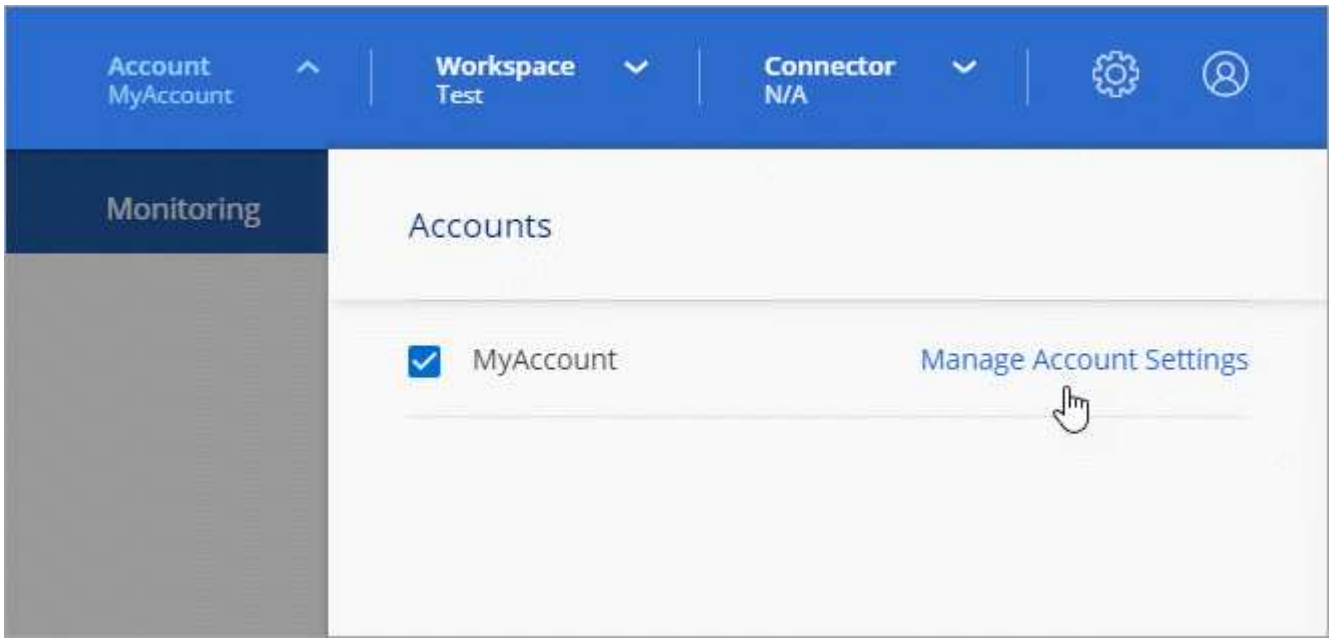
Associe usuários do Cloud Central à conta do Cloud Central para que esses usuários possam criar e gerenciar ambientes de trabalho no Cloud Manager.

Passos

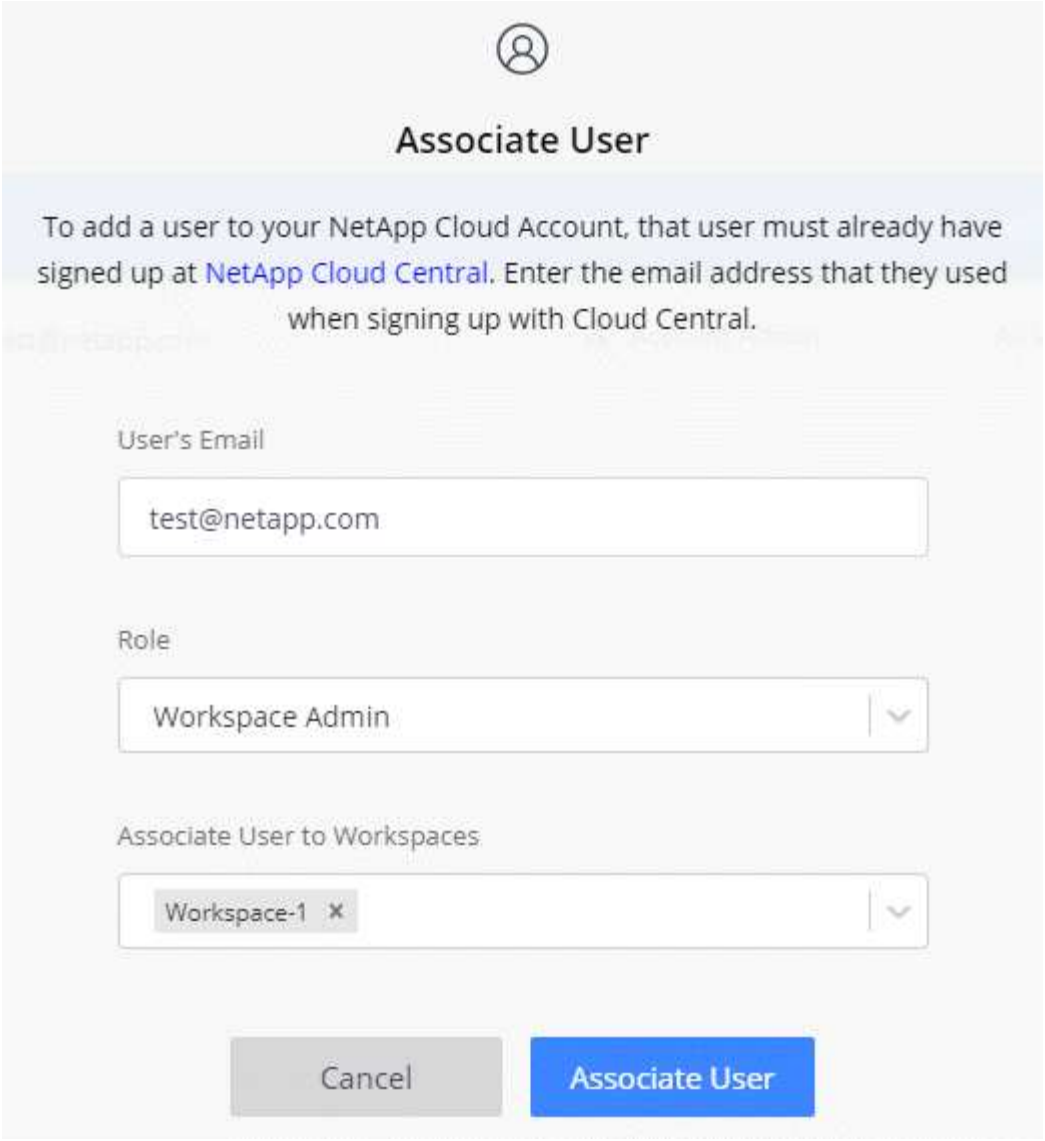
1. Se o usuário ainda não tiver feito isso, peça ao usuário para ir "Centro de nuvem da NetApp" e se inscrever.
2. Na parte superior do Cloud Manager, clique no menu suspenso **Account**.



3. Clique em **Gerenciar conta** ao lado da conta selecionada no momento.



4. Na guia usuários, clique em **Usuário associado**.
5. Insira o endereço de e-mail do usuário e selecione uma função para o usuário:
   - **Admin da conta**: Pode executar qualquer ação no Cloud Manager.
   - **Workspace Admin**: Pode criar e gerenciar recursos em workspaces atribuídos.
   - **Visualizador de conformidade**: Só pode visualizar informações de conformidade e gerar relatórios para espaços de trabalho que eles têm permissão para acessar.
6. Se você selecionou Workspace Admin ou Compliance Viewer, selecione um ou mais workspaces para associar a esse usuário.



7. Clique em **Usuário associado**.

Resultado

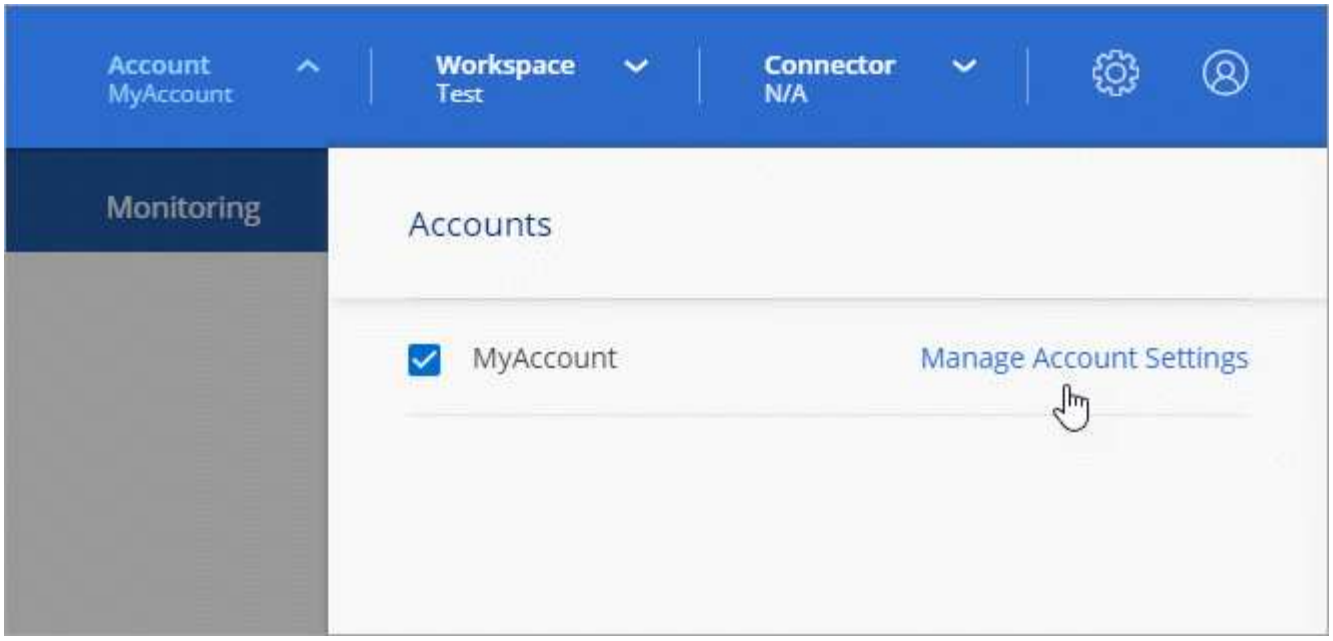
O usuário deve receber um e-mail do NetApp Cloud Central intitulado "Associação de Contas". O e-mail inclui as informações necessárias para acessar o Cloud Manager.

Removendo usuários

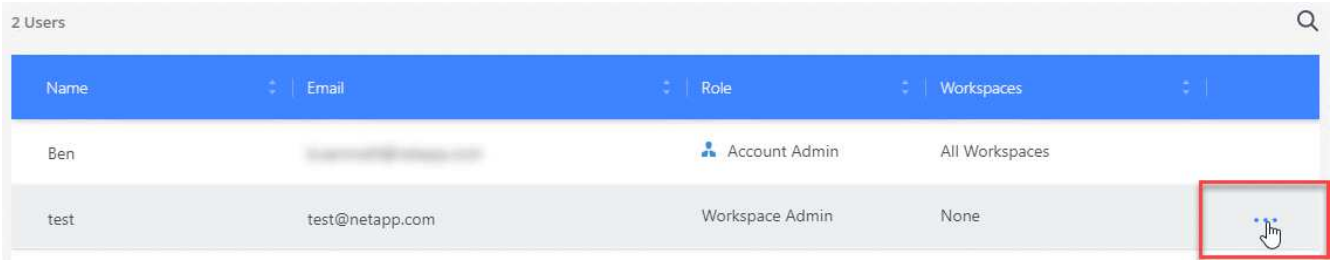
A desassociação de um usuário faz com que ele não possa mais acessar os recursos em uma conta do Cloud Central.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Disassocie User** e clique em **Disassocie** para confirmar.

Resultado

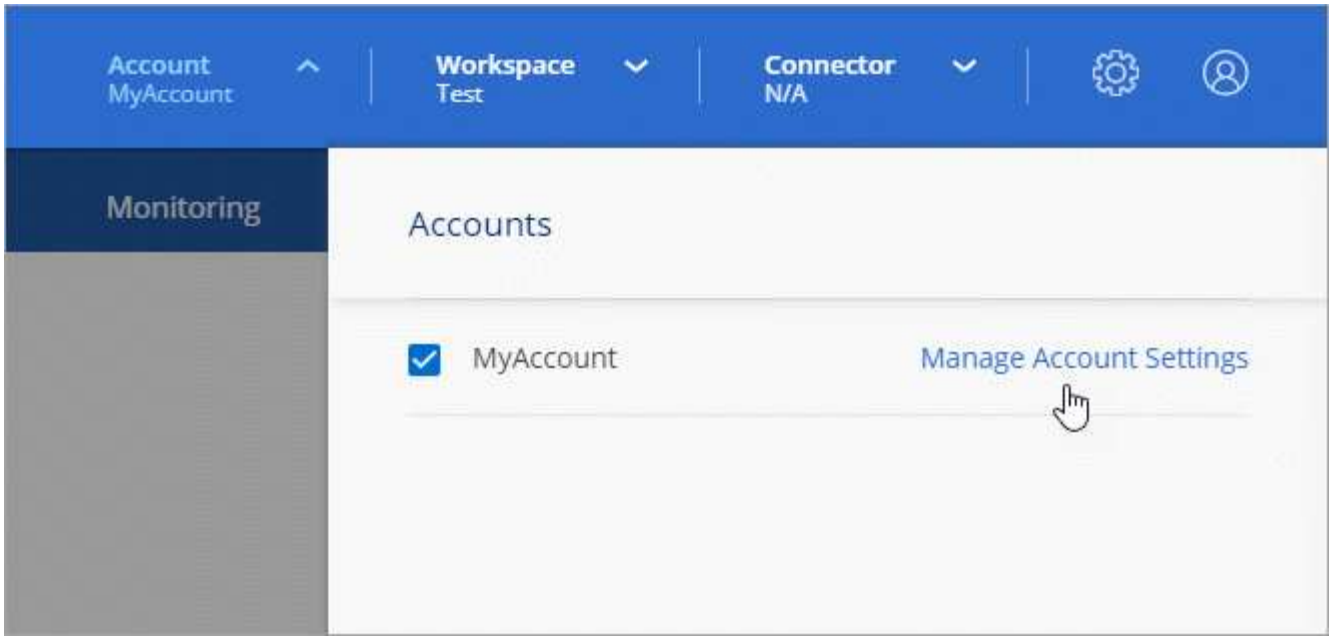
O usuário não pode mais acessar os recursos dessa conta do Cloud Central.

Gerenciando os workspaces de um administrador do espaço de trabalho

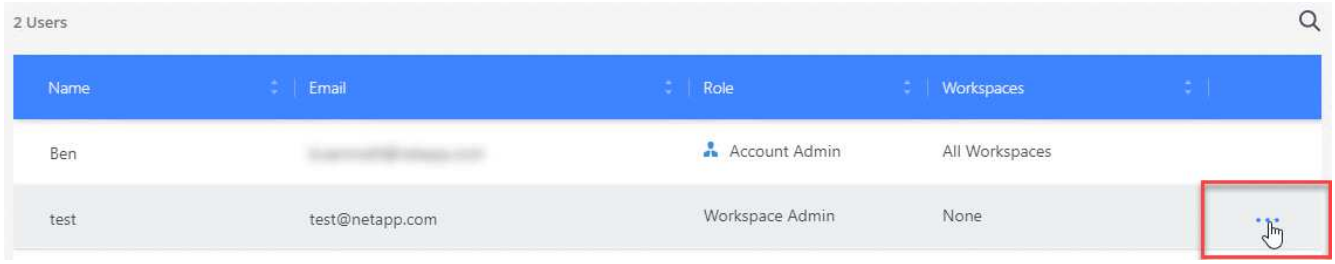
Você pode associar e desassociar administradores do Workspace a workspaces a qualquer momento. Associar o usuário permite que ele crie e visualize os ambientes de trabalho nesse espaço de trabalho.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.



2. Na guia usuários, clique no menu de ação na linha que corresponde ao usuário.



3. Clique em **Gerenciar espaços de trabalho**.
4. Selecione os espaços de trabalho a associar ao utilizador e clique em **aplicar**.

Resultado

O usuário agora pode acessar esses workspaces a partir do Cloud Manager, desde que o conetor também esteja associado aos workspaces.

Gerenciando espaços de trabalho

Gerencie seus workspaces criando, renomeando e excluindo-os. Observe que não é possível excluir um workspace se ele contiver recursos. Deve estar vazio.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Workspaces**.
3. Escolha uma das seguintes opções:
   - Clique em **Adicionar novo espaço de trabalho** para criar um novo espaço de trabalho.
   - Clique em **Renomear** para renomear a área de trabalho.
   - Clique em **Excluir** para excluir a área de trabalho.

Gerenciando espaços de trabalho de um conetor

Você precisa associar o conetor aos workspaces para que os administradores do Workspace possam acessar esses workspaces a partir do Cloud Manager.

Se você tiver apenas administradores de conta, associar o conetor com workspaces não será necessário. Administradores de conta têm a capacidade de acessar todos os espaços de trabalho no Cloud Manager por padrão.

"Saiba mais sobre usuários, workspaces e conetores".

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Connector**.
3. Clique em **Manage Workspaces** (gerir espaços de trabalho) para o conetor que pretende associar.
4. Selecione os espaços de trabalho a associar ao conetor e clique em **Apply**.

Gerenciamento de assinaturas

Depois de se inscrever no marketplace de um provedor de nuvem, cada assinatura estará disponível no widget Configurações de conta. Você tem a opção de renomear uma assinatura e desassociar a assinatura de uma ou mais contas.

Por exemplo, digamos que você tem duas contas e cada uma é cobrada através de assinaturas separadas. Você pode desassociar uma assinatura de uma das contas para que os usuários dessa conta não escolham acidentalmente a assinatura errada ao criar um ambiente de trabalho do Cloud volume ONTAP.

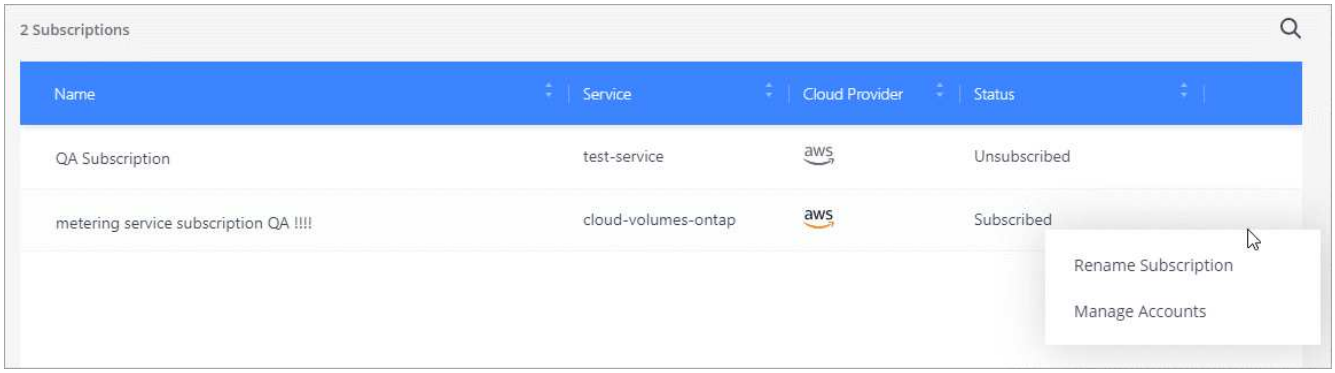
"Saiba mais sobre assinaturas".

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Clique em **Subscrições**.

   Você só verá as assinaturas associadas à conta que você está visualizando no momento.

3. Clique no menu de ação na linha que corresponde à assinatura que você deseja gerenciar.



4. Escolha para renomear a assinatura ou gerenciar as contas associadas à assinatura.

Alterar o nome da conta

Altere o nome da sua conta a qualquer momento para alterá-lo para algo significativo para você.

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Na guia **Visão geral**, clique no ícone de edição ao lado do nome da conta.
3. Digite um novo nome de conta e clique em **Salvar**.

Ativar ou desativar a plataforma SaaS

Não recomendamos desativar a plataforma SaaS a menos que você precise para cumprir com as políticas de segurança da sua empresa. Desativar a plataforma SaaS limita sua capacidade de usar os serviços de nuvem integrados da NetApp.

Os serviços a seguir não estarão disponíveis no Cloud Manager se você desativar a plataforma SaaS:

- Conformidade com a nuvem
- Kubernetes
- Disposição em camadas na nuvem
- Cache de arquivos global
- Monitoramento (Cloud Insights)

Passos

1. Na parte superior do Cloud Manager, clique no menu suspenso **Account** e clique em **Manage Account**.
2. Na guia **Visão geral**, alterne a opção para ativar o uso da plataforma SaaS.

Gerenciamento de um certificado HTTPS para acesso seguro

Por padrão, o Cloud Manager usa um certificado autoassinado para acesso HTTPS ao console da Web. Você pode instalar um certificado assinado por uma autoridade de certificação (CA), que fornece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

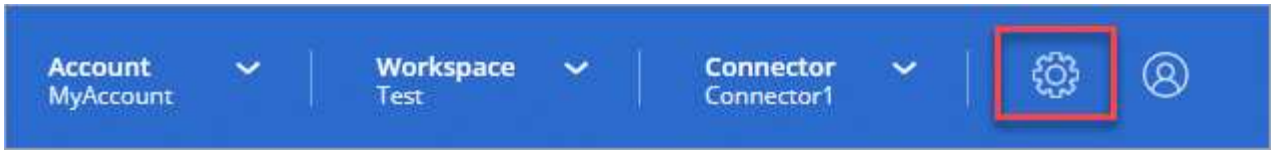
Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Instalar um certificado HTTPS

Instale um certificado assinado por uma CA para acesso seguro.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configuração HTTPS**.

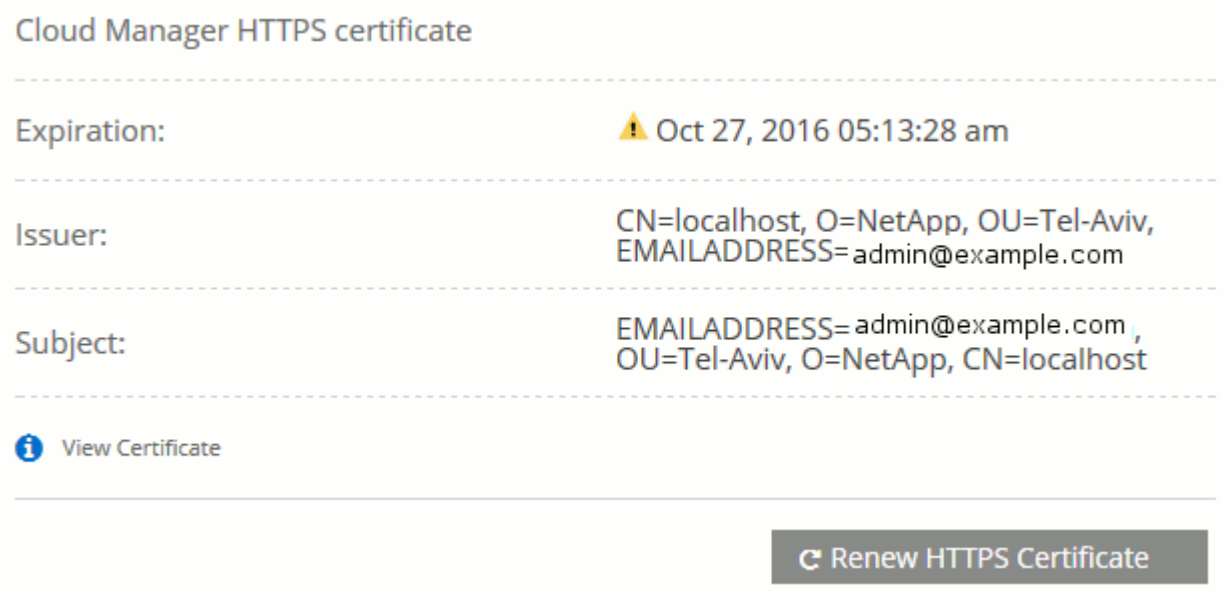


2. Na página Configuração HTTPS, instale um certificado gerando uma solicitação de assinatura de certificado (CSR) ou instalando seu próprio certificado assinado pela CA:

Opção	Descrição
Gerar um CSR	a. Insira o nome do host ou DNS do host do conetor (seu Nome Comum) e clique em **Generate CSR**. O Cloud Manager exibe uma solicitação de assinatura de certificado. b. Use o CSR para enviar uma solicitação de certificado SSL a uma CA. O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM). c. Copie o conteúdo do certificado assinado, cole-o no campo certificado e clique em **Instalar**.
Instale o seu próprio certificado assinado pela CA	a. Selecione **Instalar certificado assinado pela CA**. b. Carregue o arquivo de certificado e a chave privada e, em seguida, clique em **Install**. O certificado deve usar o formato X,509 codificado base-64 de Email Avançado de Privacidade (PEM).

Resultado

O Cloud Manager agora usa o certificado assinado pela CA para fornecer acesso HTTPS seguro. A imagem a seguir mostra um sistema do Cloud Manager configurado para acesso seguro:



Renovando o certificado HTTPS do Cloud Manager

Você deve renovar o certificado HTTPS do Cloud Manager antes de expirar para garantir acesso seguro ao console da Web do Cloud Manager. Se você não renovar o certificado antes que ele expire, um aviso será exibido quando os usuários acessarem o console da Web usando HTTPS.

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configuração HTTPS**.

   Detalhes sobre os relatórios do certificado do Cloud Manager, incluindo a data de expiração.

2. Clique em **renovar certificado HTTPS** e siga as etapas para gerar um CSR ou instalar seu próprio certificado assinado pela CA.

Resultado

O Cloud Manager usa o novo certificado assinado pela CA para fornecer acesso HTTPS seguro.

Remoção de ambientes de trabalho do Cloud Volumes ONTAP

O administrador da conta pode remover um ambiente de trabalho do Cloud Volumes ONTAP para movê-lo para outro sistema ou para solucionar problemas de descoberta.

Sobre esta tarefa

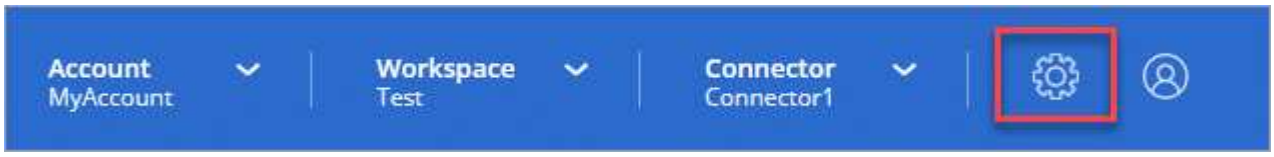
A remoção de um ambiente de trabalho do Cloud Volumes ONTAP remove-o do Cloud Manager. Ele não exclui o sistema Cloud Volumes ONTAP. Mais tarde, você pode redescobrir o ambiente de trabalho.

A remoção de um ambiente de trabalho do Cloud Manager permite que você faça o seguinte:

- Redescubra-o em outro espaço de trabalho
- Redescubra-o a partir de outro sistema Cloud Manager
- Redescubra se você teve problemas durante a descoberta inicial

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Ferramentas**.



2. Na página Ferramentas, clique em **Iniciar**.
3. Selecione o ambiente de trabalho do Cloud Volumes ONTAP que deseja remover.
4. Na página Revisão e aprovação, clique em **ir**.

Resultado

O Cloud Manager remove o ambiente de trabalho. Os usuários podem redescobrir esse ambiente de trabalho a partir da página ambientes de trabalho a qualquer momento.

Configurando um conetor para usar um servidor proxy

Se suas políticas corporativas determinarem que você usa um servidor proxy para toda a comunicação HTTP com a Internet, então você deve configurar seus conetores para usar esse servidor proxy. O servidor proxy pode estar na nuvem ou na rede.

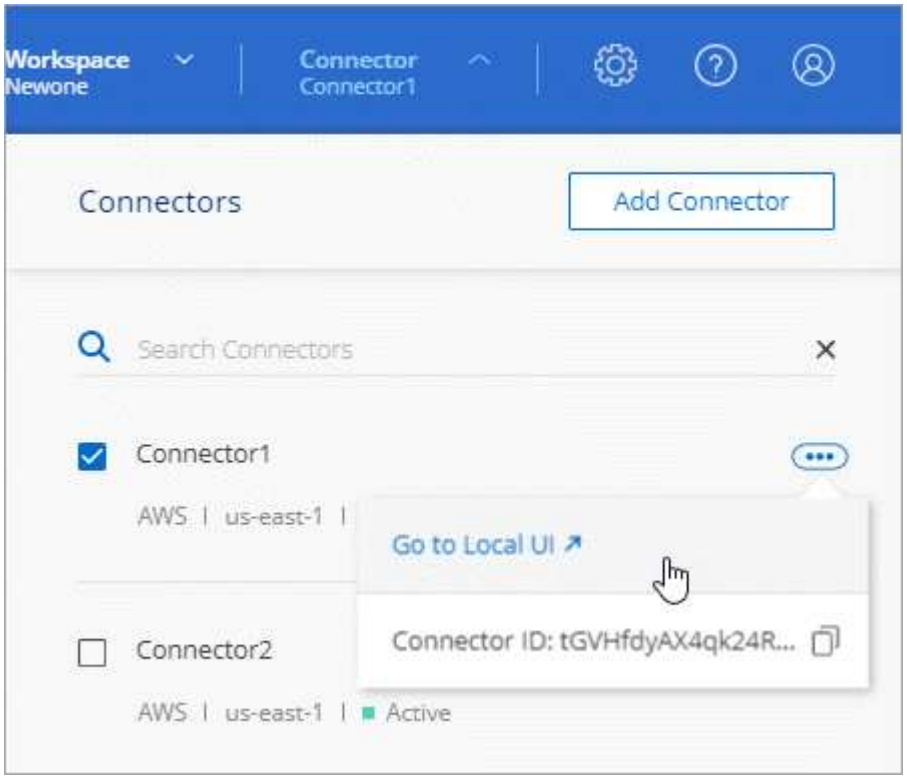
Quando você configura um conetor para usar um servidor proxy, esse conetor e os sistemas Cloud Volumes ONTAP que ele gerencia (incluindo quaisquer mediadores de HA), todos usam o servidor proxy.

Passos

1. "Faça login na interface SaaS do Cloud Manager" De uma máquina que tenha uma conexão de rede com a instância do conetor.

   Se o conetor não tiver um endereço IP público, você precisará de uma conexão VPN ou precisará se conetar a partir de um host de salto que esteja na mesma rede que o conetor.

2. Clique no menu suspenso **Connector** e clique em **Go to local UI** para obter um conetor específico.



   A interface do Cloud Manager em execução no conetor é carregada em uma nova guia do navegador.

3. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configurações do Cloud Manager**.

4. Em Proxy HTTP, digite o servidor usando a sintaxe http://address:port, especifique um nome de usuário e senha se a

autenticação básica for necessária para o servidor e clique em Salvar.

O Cloud Manager não suporta senhas que incluem o caractere A.

Resultado

Depois de especificar o servidor proxy, os novos sistemas Cloud Volumes ONTAP são configurados automaticamente para usar o servidor proxy ao enviar mensagens AutoSupport. Se você não especificou o servidor proxy antes que os usuários criem sistemas Cloud Volumes ONTAP, eles devem usar o Gerenciador do sistema para definir manualmente o servidor proxy nas opções do AutoSupport para cada sistema.

Substituindo bloqueios CIFS para o Cloud Volumes ONTAP HA no Azure

O administrador de conta pode habilitar uma configuração no Gerenciador de nuvem que impede problemas com failover de storage do Cloud Volumes ONTAP durante eventos de manutenção do Azure. Quando você ativa essa configuração, o Cloud Volumes ONTAP veta o CIFS bloqueia e redefine as sessões ativas do CIFS.

Sobre esta tarefa

O Microsoft Azure agenda eventos de manutenção periódica em suas máquinas virtuais. Quando ocorre um evento de manutenção em um nó em um par de HA do Cloud Volumes ONTAP, o par de HA inicia o takeover do storage. Se houver sessões CIFS ativas durante esse evento de manutenção, os bloqueios em arquivos CIFS podem impedir o failover de armazenamento.

Se ativar esta definição, o Cloud Volumes ONTAP vetará os bloqueios e redefinirá as sessões CIFS ativas. Como resultado, o par de HA pode concluir o failover de storage durante esses eventos de manutenção.

Esse processo pode ser disruptivo para clientes CIFS. Os dados que não forem comprometidos com clientes CIFS podem ser perdidos.

O que você vai precisar

Você precisa criar um conetor antes de alterar as configurações do Cloud Manager. "Saiba como".

Passos

1. No canto superior direito do console do Cloud Manager, clique no ícone Configurações e selecione **Configurações do Cloud Manager**.

2. Em **HA CIFS Locks**, marque a caixa de seleção e clique em **Save**.

Referência

Funções

As funções Admin da conta, Admin do espaço de trabalho e Visualizador de conformidade na nuvem fornecem permissões específicas aos usuários.

Tarefa	Administrador da conta	Admin da área de trabalho	Visualizador de conformidade na nuvem
Gerenciar ambientes de trabalho	Sim	Sim	Não
Ativar serviços em ambientes de trabalho	Sim	Sim	Não
Exibir status de replicação de dados	Sim	Sim	Não
Veja a linha do tempo	Sim	Sim	Não
Alterne entre espaços de trabalho	Sim	Sim	Sim
Ver os resultados da verificação de conformidade	Sim	Sim	Sim
Eliminar ambientes de trabalho	Sim	Não	Não
Conecte clusters do Kubernetes a ambientes de trabalho	Sim	Não	Não
Receba o relatório Cloud Volumes ONTAP	Sim	Não	Não
Crie conetores	Sim	Não	Não
Gerenciar contas do Cloud Central	Sim	Não	Não
Gerenciar credenciais	Sim	Não	Não
Modifique as configurações do Cloud Manager	Sim	Não	Não
Visualize e gerencie o Painel de suporte	Sim	Não	Não
Remova os ambientes de trabalho do Cloud Manager	Sim	Não	Não
Instale um certificado HTTPS	Sim	Não	Não

Links relacionados

- "Configurando espaços de trabalho e usuários na conta do Cloud Central"
- "Gerenciamento de espaços de trabalho e usuários na conta do Cloud Central"

Como o Cloud Manager usa permissões de provedor de nuvem

O Cloud Manager requer permissões para executar ações no seu provedor de nuvem. Essas permissões estão incluídas no "As políticas fornecidas pela NetApp". você pode

querer entender o que o Cloud Manager faz com essas permissões.

O que o Cloud Manager faz com as permissões da AWS

O Cloud Manager usa uma conta da AWS para fazer chamadas de API para vários serviços da AWS, incluindo EC2, S3, CloudFormation, IAM, o Security Token Service (STS) e o Key Management Service (KMS).

Ações	Finalidade
"EC2:StartInstances", "EC2:StopInstances", "EC2:DescribeInstances", "EC2:DescribeInstanceStatus", "EC2:RunInstances", "EC2:TerminateInstances", "EC2:ModifyInstanceAttribute",	Inicia uma instância do Cloud Volumes ONTAP e pára, inicia e monitora a instância.
"EC2:DescribeInstanceAttribute",	Verifica se a rede aprimorada está habilitada para tipos de instâncias compatíveis.
"EC2:DescribeRouteTables", "EC2:DescribeImages",	Inicia uma configuração Cloud Volumes ONTAP HA.
"EC2:CreateTags",	Marca todos os recursos que o Cloud Manager cria com as tags "WorkingEnvironment" e "WorkingEnvironmentId". O Cloud Manager usa essas tags para manutenção e alocação de custos.
"EC2:Createvolume", "EC2:DescribeVolumes", "EC2:ModifyVolumeAttribute", "EC2:Attachvolume", "EC2:Deletevolume", "EC2:Detachvolume",	Gerencia os volumes do EBS que o Cloud Volumes ONTAP usa como armazenamento back-end.
"EC2:CreateSecurityGroup", "EC2:DeleteSecurityGroup", "EC2:DescribeSecurityGroups", "EC2:RevokeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupEgress", "EC2:AuthorizeSecurityGroupIngress", "EC2:RevokeSecurityGroupIngress",	Cria grupos de segurança predefinidos para o Cloud Volumes ONTAP.
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	Cria e gerencia interfaces de rede para Cloud Volumes ONTAP na sub-rede de destino.
"EC2:DescribeSubnets", "EC2:DescribeVPCs",	Obtém a lista de sub-redes de destino e grupos de segurança, que é necessário ao criar um novo ambiente de trabalho para o Cloud Volumes ONTAP.
"EC2:DescribeDhcpOptions",	Determina os servidores DNS e o nome de domínio padrão ao iniciar instâncias do Cloud Volumes ONTAP.
"EC2:CreateSnapshot", "EC2:DeleteSnapshot", "EC2:DescribeSnapshots",	Tira instantâneos dos volumes do EBS durante a configuração inicial e sempre que uma instância do Cloud Volumes ONTAP é interrompida.
"EC2:GetConsoleOutput",	Captura o console do Cloud Volumes ONTAP, que está conetado às mensagens do AutoSupport.

Ações	Finalidade
"EC2:DescribeKeyPairs",	Obtém a lista de pares de chaves disponíveis ao iniciar instâncias.
"EC2:DescribeRegiões",	Obtém uma lista de regiões da AWS disponíveis.
"EC2:DeleteTags", "EC2:DescribeTags",	Gerencia tags para recursos associados às instâncias do Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Inicia instâncias do Cloud Volumes ONTAP.
"IAM:PassRole", "IAM:CreateRole", "IAM:DeleteRole", "IAM:PutRolePolicy", "IAM:CreateInstanceProfile", "IAM:DeleteRolePolicy", "iam:RoleAddToInstanceProfile", "iam:RemveRoleDeInstanceInstanceProfile", "iam:DeleteProfile", "iam:DeleteAddOutreAddOutreAddToInstanceProfile"	Inicia uma configuração Cloud Volumes ONTAP HA.
"iam:ListInstanceProfiles", "STS:DedeAuthorizationMessage", "EC2:AssociateIamInstanceProfile", "EC2:DescribeIamInstanceAssociations", "EC2:DisassociateIamInstanceProfile", "DescribeIamInstanceProfile",	Gerencia perfis de instâncias para instâncias do Cloud Volumes ONTAP.
"S3:GetBucketTagging", "S3:GetBucketLocation", "S3:ListAllMyBuckets", "S3:ListBucket"	Obtém informações sobre os buckets do AWS S3 para que o Cloud Manager possa se integrar ao serviço NetApp Data Fabric Cloud Sync.
"S3 S3:CreateBucket", "S3 S3 S3:DeleteBucket", "S3 S3:GetLifecycleConfiguration", "S3:PutLifecycleConfiguration", "S3:PutBucketTagging", "S3:ListBucketVersions", "S3:GetBucketPolicyStatus"	Gerencia o bucket do S3 usado pelo sistema Cloud Volumes ONTAP como uma camada de capacidade para categorização de dados.
"Kms:Lista*", "kms:Recriptografar*", "kms:descrever*", "kms:CreateGrant",	Permite a criptografia de dados do Cloud Volumes ONTAP usando o AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtém dados de custo da AWS para o Cloud Volumes ONTAP.
"EC2:CreatePlacementGroup", "EC2:DeletePlacementGroup"	Ao implantar uma configuração de HA em uma única zona de disponibilidade da AWS, o Cloud Manager inicia os dois nós de HA e o mediador em um grupo de posicionamento de spread da AWS.
"EC2:DescribeReservedInstancesOferings"	O Cloud Manager usa a permissão como parte da implantação do Cloud Compliance para escolher qual tipo de instância usar.

Ações	Finalidade
"S3 S3 S3:DeleteBucket", "S3 S3 S3 S3:GetLifecycleConfiguration", "S3 S3 S3 S3:PutLifecycleConfiguration", "S3:PutBucketTagging", "S3:ListBucketVersions", "S3:GetObject", "S3	O Cloud Manager usa essas permissões quando você ativa o serviço Backup to S3.

O que o Cloud Manager faz com as permissões do Azure

A política do Azure inclui as permissões que o Cloud Manager precisa para implantar e gerenciar o Cloud Volumes ONTAP no Azure.

Ações	Finalidade
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read","Microsoft.Compute/virtualMachines/write",	Cria Cloud Volumes ONTAP e pára, inicia, exclui e obtém o status do sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Permite a implantação do Cloud Volumes ONTAP a partir de um VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameavailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage	Gerencia contas e discos de armazenamento do Azure e anexa os discos ao Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Cria e gerencia interfaces de rede para Cloud Volumes ONTAP na sub-rede de destino.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Cria grupos de segurança de rede predefinidos para o Cloud Volumes ONTAP.

Ações	Finalidade
"Microsoft.resources/Subscrições/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Obtém informações de rede sobre regiões, a rede VNet de destino e a sub-rede e adiciona Cloud Volumes ONTAP aos VNets.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Habilita pontos de extremidade do serviço VNet para categorização de dados.
"Microsoft.resources/deployments/operations/read", "Microsoft.resources/deployments/deployments/write",	Implanta o Cloud Volumes ONTAP a partir de um modelo.
"Microsoft.resources/deploys/operations/read", "Microsoft.resources/deployments/deployments/write", "Microsoft.resources/resources/resources/lease", "Microsoft.resources	Cria e gerencia grupos de recursos para o Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Cria e gerencia snapshots gerenciados do Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Cria e gerencia conjuntos de disponibilidade para o Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offertypes/publishers/offertyes/offertyes/offertyes/offertyes/offerments/plans/agreements/write"	Habilita implantações programáticas no Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action","	Gerencia um balanceador de carga do Azure para pares de HA.
"Microsoft.Authorization/Locks/*"	Permite o gerenciamento de bloqueios em discos Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/Sites/*"	Gerencia o failover em pares de HA.

Ações	Finalidade
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",""	Permite o gerenciamento de endpoints privados. Os endpoints privados são usados quando a conetividade não é fornecida para fora da sub-rede. O Cloud Manager cria a conta de storage para HA com apenas conetividade interna na sub-rede.
"Microsoft.NetApp/netAppAccount/capacityPools/volumes/delete",	Permite que o Cloud Manager exclua volumes para Azure NetApp Files.
"Microsoft.resources/deployments/operationStatuses/read"	O Azure requer essa permissão para algumas implantações de máquinas virtuais (depende do hardware físico subjacente usado durante a implantação).
"Microsoft.resources/deployments/operationStatuses/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.resources/deployments/delete",	Permite que você use o Global File Cache.
"Microsoft.Compute/diskEncryptionSets/read"	Permite que o Cloud Manager criptografe discos gerenciados do Azure em sistemas Cloud Volumes ONTAP de nó único usando chaves externas de outra conta. Esse recurso é compatível com APIs.

O que o Cloud Manager faz com as permissões do GCP

A política do Cloud Manager do GCP inclui as permissões necessárias para implantar e gerenciar o Cloud Volumes ONTAP.

Ações	Finalidade
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use.	Para criar e gerenciar discos para Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Para criar regras de firewall para o Cloud Volumes ONTAP.

Ações	Finalidade
- Compute.globalOperations.get	Para obter o status das operações.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Para obter imagens para instâncias de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Para anexar e desanexar discos ao Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Para criar e excluir instâncias de VM do Cloud Volumes ONTAP.
- compute.instances.get	Para listar instâncias de VM.
- compute.instances.getSerialPortOutput	Para obter logs de console.
- compute.instances.list	Para recuperar a lista de instâncias em uma zona.
- compute.instances.setDeletionProtection	Para definir a proteção de exclusão na instância.
- compute.instances.setLabels	Para adicionar etiquetas.
- compute.instances.setMachineType	Para alterar o tipo de máquina para Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para adicionar metadados.
- compute.instances.setTags	Para adicionar etiquetas para regras de firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Para iniciar e parar o Cloud Volumes ONTAP.
- Compute.machineTypes.get	Para obter os números de núcleos para verificar qoutas.
- compute.projects.get	Para apoiar multi-projetos.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Para criar e gerenciar snapshots persistentes em disco.
- compute.networks.get - compute.networks.list - Compute.regions.get - Compute.regions.list - Compute.subnetworks.get - Compute.subnetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list	Para obter as informações de rede necessárias para criar uma nova instância de máquina virtual Cloud Volumes ONTAP.
- 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	Para implantar a instância de máquina virtual do Cloud Volumes ONTAP usando o Gerenciador de implantação do Google Cloud.
- LogEntries.list - logging.privateLogEntries.list	Para obter unidades de log de pilha.

Ações	Finalidade
- resourcemanager.projects.get	Para apoiar multi-projetos.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para criar e gerenciar um bucket do Google Cloud Storage para categorização de dados.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyrings.list	Para usar chaves de criptografia gerenciadas pelo cliente a partir do Serviço de gerenciamento de chaves na nuvem com o Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Para definir uma conta de serviço na instância do Cloud Volumes ONTAP. Essa conta de serviço fornece permissões para categorização de dados em um bucket do Google Cloud Storage.

Páginas do AWS Marketplace para o Cloud Manager e o Cloud Volumes ONTAP

Várias ofertas estão disponíveis no AWS Marketplace for Cloud Manager e no Cloud Volumes ONTAP. Se precisar de ajuda para entender o propósito de cada página, leia as descrições abaixo.

Em todos os casos, lembre-se de que você não pode iniciar o Cloud Volumes ONTAP no AWS a partir do AWS Marketplace. Você precisa iniciá-lo diretamente do Cloud Manager.

Meta	Página do AWS Marketplace para usar	Mais informações
Habilite o uso do Cloud Volumes ONTAP PAYGO, disposição em camadas na nuvem, conformidade com a nuvem e outros serviços complementares	"Gerenciador de nuvem - implantar Gerenciar Serviços de dados de nuvem da NetApp"	Esta subscrição permite o carregamento da versão PAYGO do Cloud Volumes ONTAP 9,6 e posterior. Ele também permite cobrança pelo Cloud Tiering, pelo Cloud Compliance e por outros serviços complementares. Você deve assinar essa oferta quando o Cloud Manager solicitar e redirecioná-lo para a página. O Cloud Manager solicita no assistente de ambiente de trabalho ou quando você adiciona novas credenciais nas Configurações. Esta página não permite que você inicie o Cloud Manager na AWS. Isso deve ser feito a partir de "Centro de nuvem da NetApp", ou, alternativamente, usando o AMI listado na linha 3 desta tabela.

Meta	Página do AWS Marketplace para usar	Mais informações
Habilite o uso do Cloud Volumes ONTAP PAYGO, disposição em camadas na nuvem, conformidade com a nuvem e outros serviços complementares *usando um contrato anual*	"Gerenciador de nuvem (contratos) - implantar Gerenciar serviços de dados de nuvem da NetApp"	Esta subscrição é uma alternativa à subscrição na primeira linha. Ele permite que você obtenha um pagamento antecipado anual para os anúncios. É principalmente para parceiros da NetApp.
Implante o Cloud Manager no AWS Marketplace usando uma AMI	"Cloud Manager - Instalação manual sem chaves de acesso"	Recomendamos que você inicie o Cloud Manager na AWS a partir "Centro de nuvem da NetApp"do , mas você pode iniciá-lo a partir desta página do AWS Marketplace, se preferir.
Ativar a implantação do Cloud Volumes ONTAP PAYGO (9,5 ou anterior)	• "Cloud Volumes ONTAP para AWS" • "Cloud Volumes ONTAP para AWS: Alta disponibilidade"	Essas páginas do AWS Marketplace permitem que você assine as versões de nó único ou HA do Cloud Volumes ONTAP PAYGO para as versões 9,5 e anteriores. A partir da versão 9,6, você precisa se inscrever na página do AWS Marketplace listada na linha 1 desta tabela para implantações PAYGO.

Informações sobre direitos autorais

Informações sobre marcas comerciais