



Azure

Cloud Manager 3.8

NetApp
October 22, 2024

Índice

- Azure 1
 - Credenciais e permissões do Azure 1
 - Gerenciamento de credenciais e assinaturas do Azure para o Cloud Manager 3

Azure

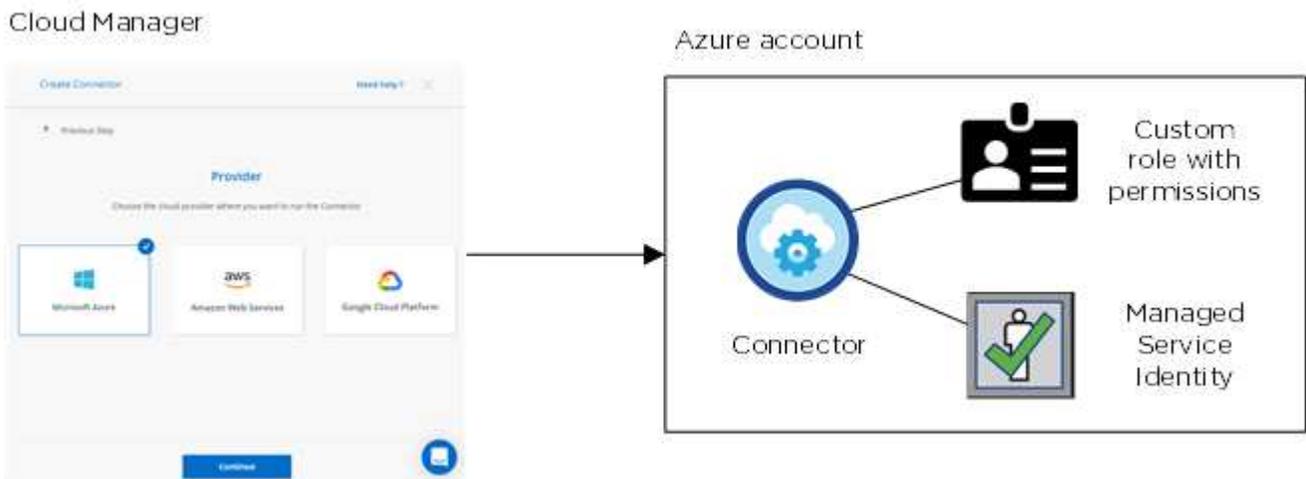
Credenciais e permissões do Azure

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 conector 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:

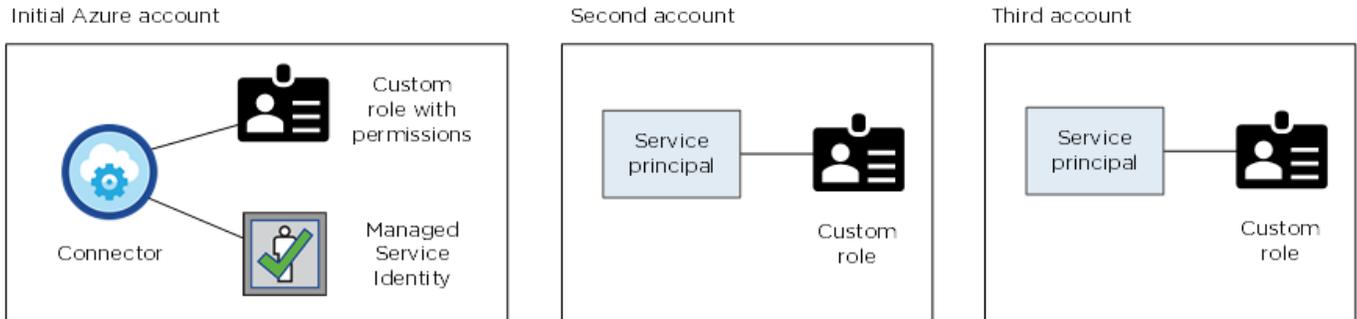
Details & Credentials			
Managed Service Ide...	OCCM QA1	! No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

Subscrições adicionais do Azure para uma identidade gerida

A identidade gerenciada está associada à assinatura na qual você lançou o conector. Se você quiser selecionar uma assinatura diferente do Azure, precisará ["associe a identidade gerenciada a essas assinaturas"](#)do .

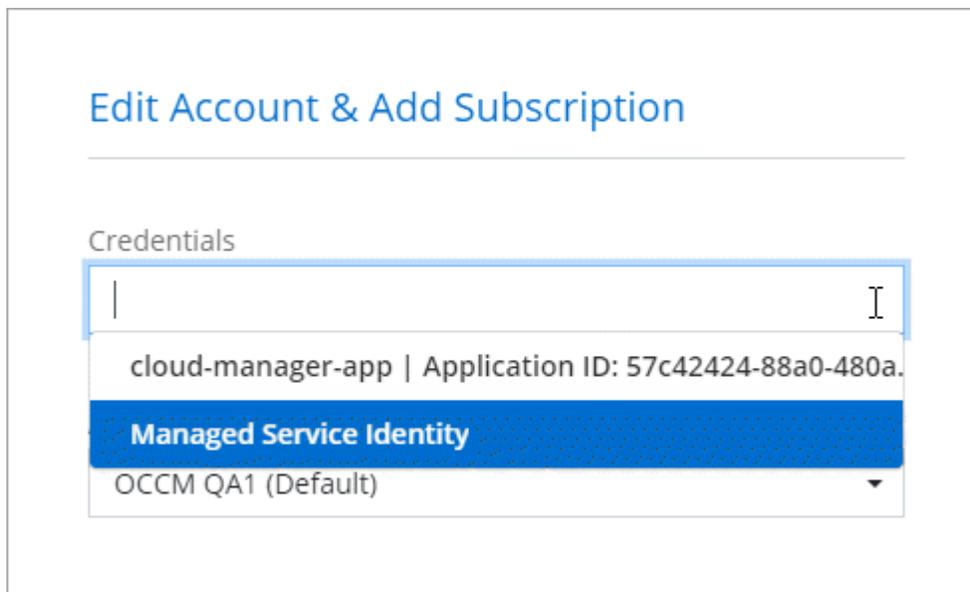
Credenciais adicionais do Azure

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 ativo 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 conector, que é do NetApp Cloud Central. Você também pode implantar um conector no Azure a partir do "[Azure Marketplace](#)", e pode "[Instale o conector 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 conector e, em seguida, fornecer permissões para quaisquer contas adicionais.

Para implantações locais, não é possível configurar uma identidade gerenciada para o conector, 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.



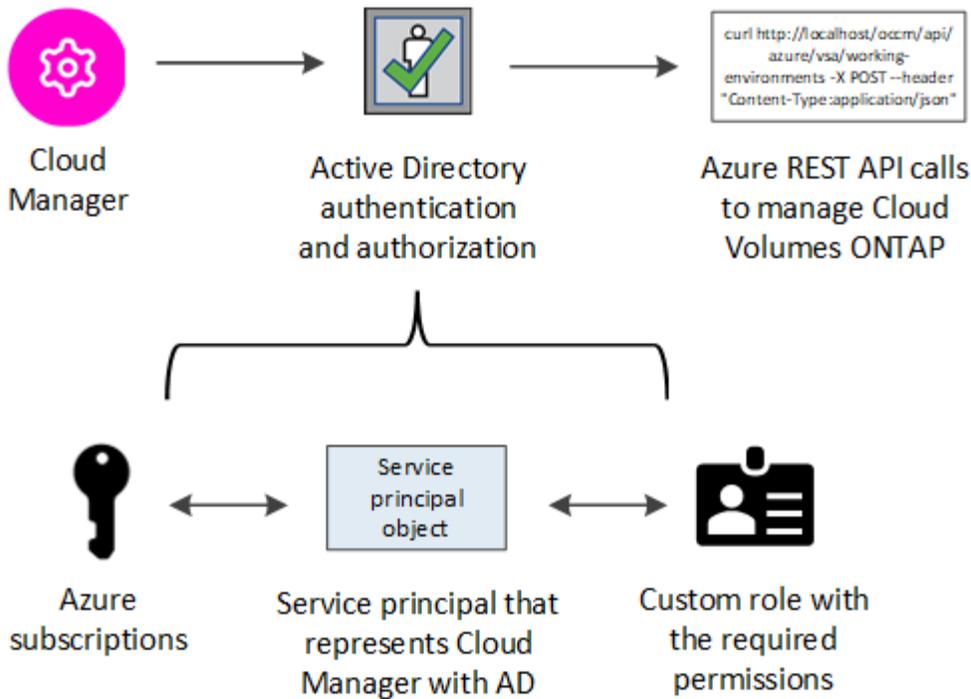
Ao implantar um conector do Cloud Manager, o Cloud Manager adiciona automaticamente a conta do Azure na qual você implantou o conector. Uma conta inicial não será adicionada se você tiver instalado manualmente o software Connector em um sistema existente. "[Saiba mais sobre as contas e permissões do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

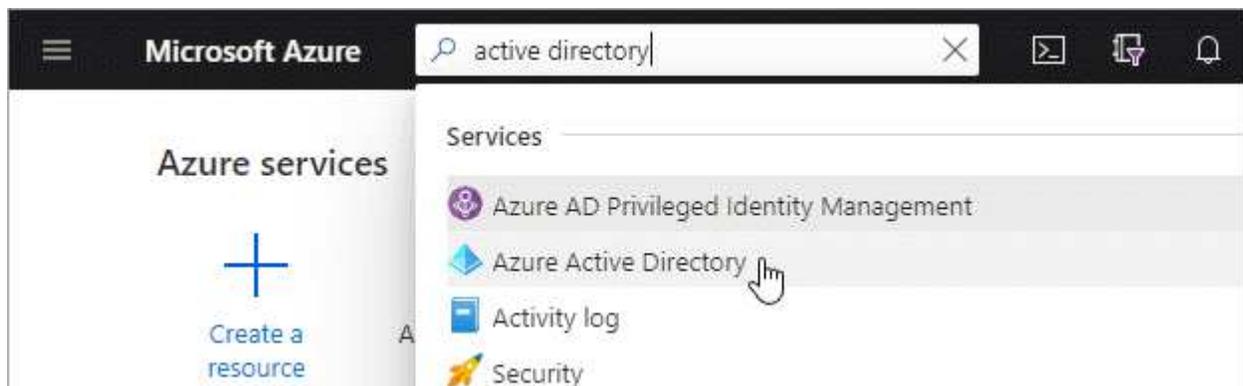
Crie um aplicativo e um diretor de serviço do Azure ativo Directory (AD) que o Cloud Manager pode usar para controle de acesso baseado em funções.

Antes de começar

Você deve ter as permissões certas no Azure para criar um aplicativo do ativo 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 ativo Directory**.



2. No menu, clique em **inscrições de aplicativos**.
3. Clique em **novos registros**.
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 **Registrar**.

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).

Add role assignment [X]

Role ⓘ
OnCommand Cloud Manager Operator [v]

Assign access to ⓘ
Azure AD user, group, or service principal [v]

Select ⓘ
test-service-principal [v]

test-service-principal

- 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 ativo 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**.

Request API permissions

Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint. 		
Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
Azure Data Lake Access to storage and compute for big data analytic scenarios	Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Import/Export Programmatic control of import/export jobs
Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	Azure Rights Management Services Allow validated users to read and write protected content	Azure Service Management Programmatic access to much of the functionality available through the Azure portal
Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	Customer Insights Create profile and interaction models for your products	Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)

 Azure Service Management
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

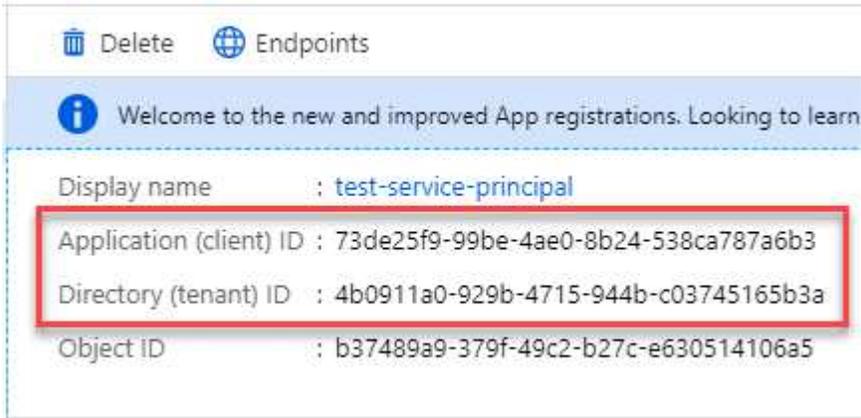
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) 	-

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 ativo Directory**, clique em **inscrições de aplicativos** e selecione o aplicativo.
2. Copie o **ID do aplicativo (cliente)** e o **ID do diretório (locatário)**.



Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 active 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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	Copy to clipboard

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 conector 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**.



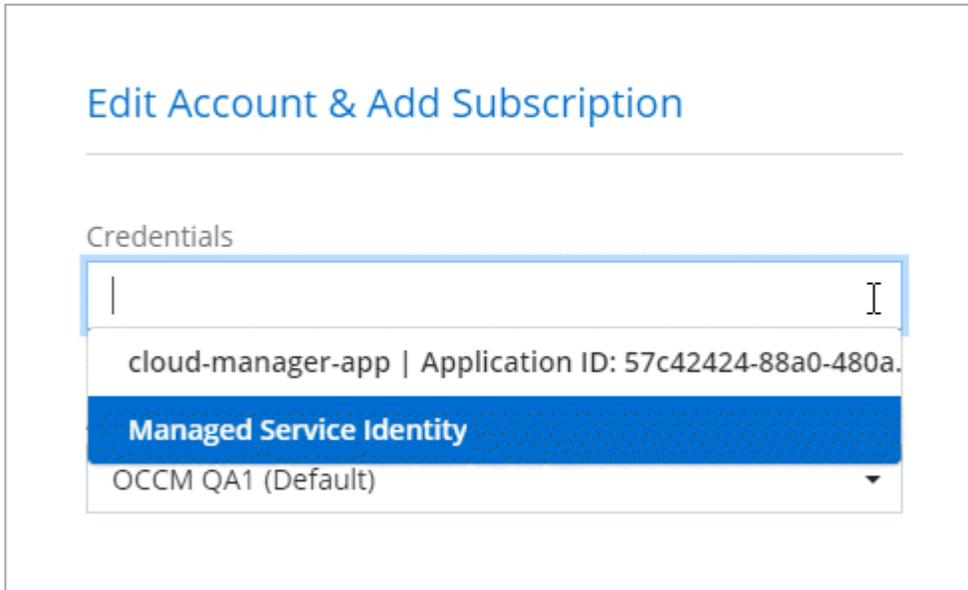
2. Clique em **Adicionar credenciais** e selecione **Microsoft Azure**.
3. Insira informações sobre o principal de serviço do Azure active Directory que concede as permissões necessárias:
 - ID da aplicação (cliente): [Obtendo o ID do aplicativo e o ID do diretório](#)Consulte .
 - ID do diretório (locatário): [Obtendo o ID do aplicativo e o ID do diretório](#)Consulte .
 - Segredo do cliente: [Criando um segredo de cliente](#)Consulte .
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:

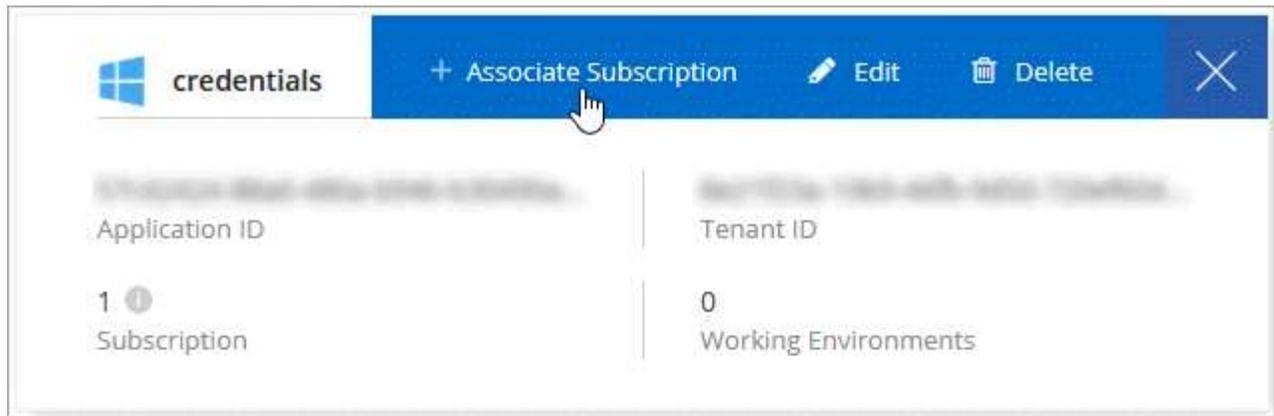
- Você não associou uma assinatura quando adicionou inicialmente as credenciais ao Cloud Manager.
- Você deseja substituir uma assinatura existente do Azure Marketplace por uma nova assinatura.

O que você vai precisar

Você precisa criar um conector 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 conector do Cloud Manager. Quando você implantou o conector, o Cloud Manager criou a função Operador do Cloud Manager e atribuiu-a à máquina virtual do conector.

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 conector foi criada.
 - Selecione a máquina virtual do conector.
 - 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.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.