



Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

- Azure 1
 - Credenziali e permessi di Azure 1
 - Gestione delle credenziali e delle sottoscrizioni di Azure per Cloud Manager 3

Azure

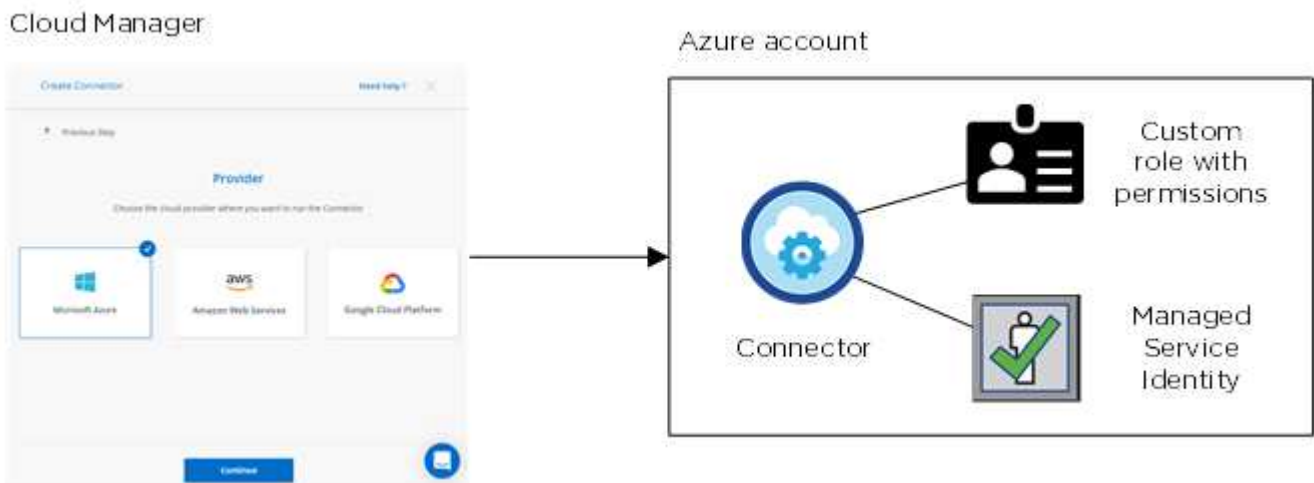
Credenziali e permessi di Azure

Cloud Manager consente di scegliere le credenziali Azure da utilizzare durante l'implementazione di Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali iniziali di Azure oppure aggiungere ulteriori credenziali.

Credenziali iniziali di Azure

Quando si implementa un connettore da Cloud Manager, è necessario utilizzare un account Azure che disponga delle autorizzazioni necessarie per implementare la macchina virtuale del connettore. Le autorizzazioni richieste sono elencate nella ["Policy di implementazione del connettore per Azure"](#).

Quando Cloud Manager implementa la macchina virtuale del connettore in Azure, abilita una ["identità gestita assegnata dal sistema"](#) sulla macchina virtuale, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce a Cloud Manager le autorizzazioni per gestire risorse e processi all'interno dell'abbonamento Azure. ["Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager"](#).



Cloud Manager seleziona queste credenziali Azure per impostazione predefinita quando crei un nuovo ambiente di lavoro per Cloud Volumes ONTAP:

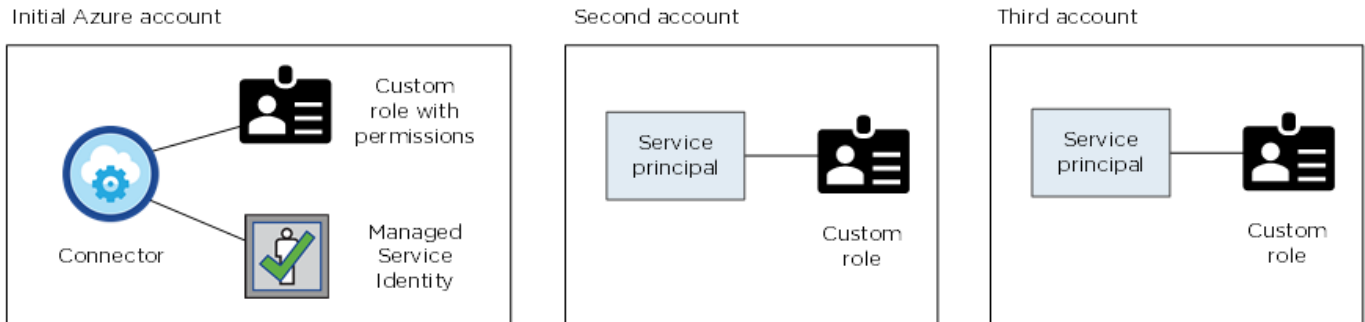
Details & Credentials			
Managed Service Ide...	OCCM QA1	<i>No subscription is associated</i>	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

Abbonamenti Azure aggiuntivi per un'identità gestita

L'identità gestita è associata all'abbonamento con cui è stato avviato il connettore. Se si desidera selezionare un abbonamento Azure diverso, è necessario ["associare l'identità gestita a tali sottoscrizioni"](#).

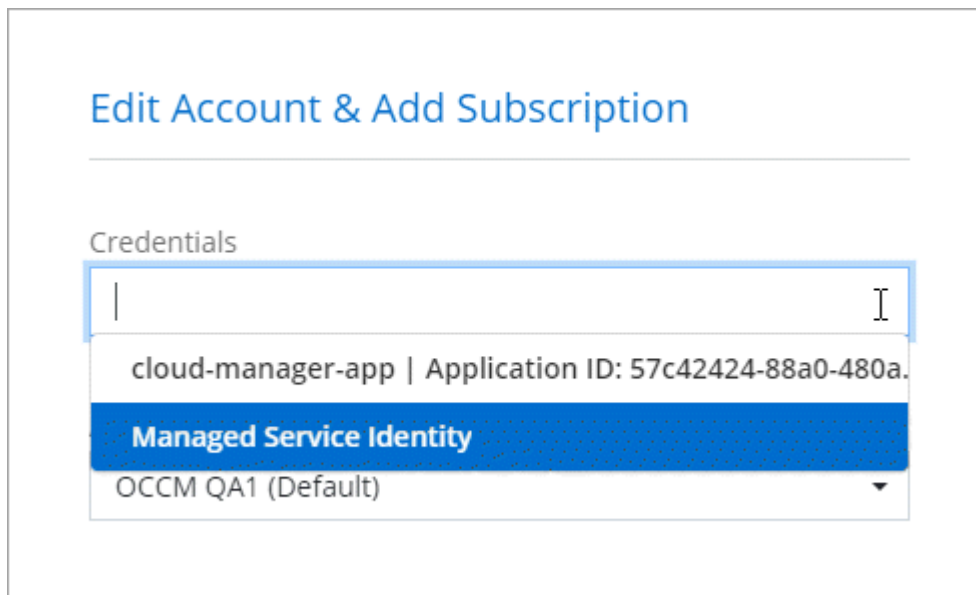
Credenziali Azure aggiuntive

Se si desidera implementare Cloud Volumes ONTAP utilizzando credenziali Azure diverse, è necessario concedere le autorizzazioni richieste da ["Creazione e configurazione di un'entità di servizio in Azure Active Directory"](#) Per ciascun account Azure. L'immagine seguente mostra due account aggiuntivi, ciascuno configurato con un'entità del servizio e un ruolo personalizzato che fornisce le autorizzazioni:



Allora ["Aggiungere le credenziali dell'account a Cloud Manager"](#) Fornendo dettagli sull'identità del servizio ad.

Dopo aver aggiunto un altro set di credenziali, è possibile passare a queste quando si crea un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, che proviene da NetApp Cloud Central. È inoltre possibile implementare un connettore in Azure da ["Azure Marketplace"](#) e puoi farlo ["Installare il connettore on-premise"](#).

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente l'identità gestita per il connettore, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un'identità gestita per il connettore, ma è possibile fornire autorizzazioni esattamente come per gli account aggiuntivi utilizzando un'entità del servizio.

Gestione delle credenziali e delle sottoscrizioni di Azure per Cloud Manager

Quando si crea un sistema Cloud Volumes ONTAP, è necessario selezionare le credenziali Azure e l'abbonamento Marketplace da utilizzare con tale sistema. Se si gestiscono più sottoscrizioni Azure Marketplace, è possibile assegnarle a diverse credenziali Azure dalla pagina credenziali.

Esistono due modi per gestire le credenziali Azure in Cloud Manager. Innanzitutto, se si desidera implementare Cloud Volumes ONTAP in diversi account Azure, è necessario fornire le autorizzazioni necessarie e aggiungere le credenziali a Cloud Manager. Il secondo metodo consiste nell'associare sottoscrizioni aggiuntive all'identità gestita da Azure.



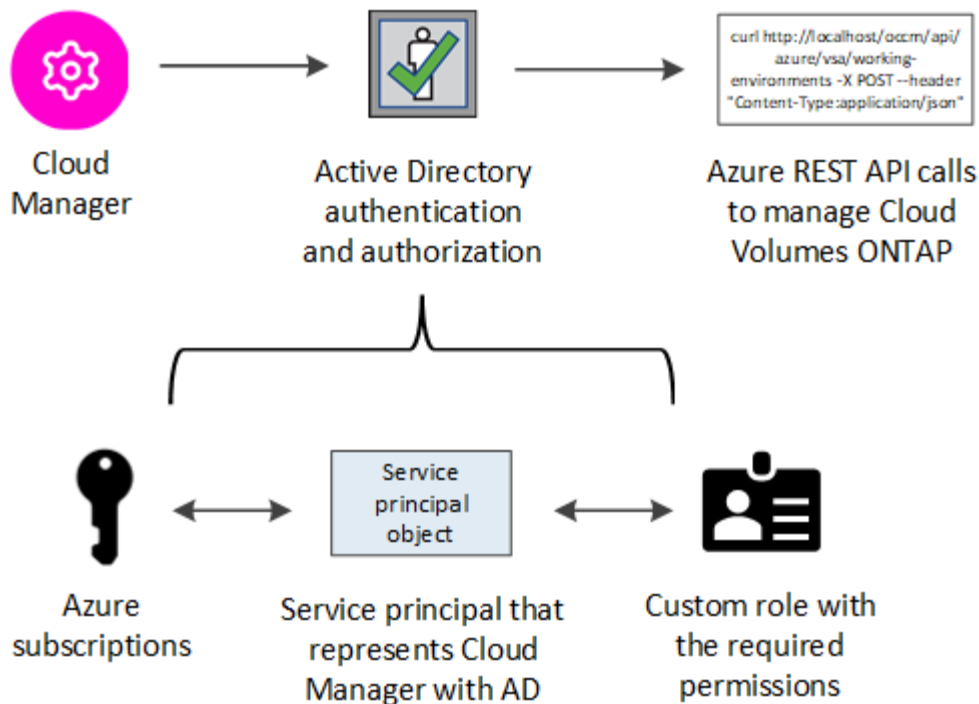
Quando si implementa un connettore da Cloud Manager, Cloud Manager aggiunge automaticamente l'account Azure in cui è stato implementato il connettore. Se il software Connector è stato installato manualmente su un sistema esistente, non viene aggiunto un account iniziale. ["Scopri gli account e le autorizzazioni di Azure"](#).

Concessione delle autorizzazioni di Azure mediante un'entità del servizio

Cloud Manager ha bisogno delle autorizzazioni per eseguire azioni in Azure. È possibile concedere le autorizzazioni richieste a un account Azure creando e impostando un'entità di servizio in Azure Active Directory e ottenendo le credenziali Azure di cui Cloud Manager ha bisogno.

A proposito di questa attività

La seguente immagine mostra come Cloud Manager ottiene le autorizzazioni per eseguire operazioni in Azure. Un oggetto principale del servizio, legato a una o più sottoscrizioni Azure, rappresenta Cloud Manager in Azure Active Directory e viene assegnato a un ruolo personalizzato che consente le autorizzazioni richieste.



Fasi

1. Creare un'applicazione Azure Active Directory.
2. Assegnare l'applicazione a un ruolo.
3. Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure.
4. Ottenere l'ID dell'applicazione e l'ID della directory.
5. Creare un client segreto.

Creazione di un'applicazione Azure Active Directory

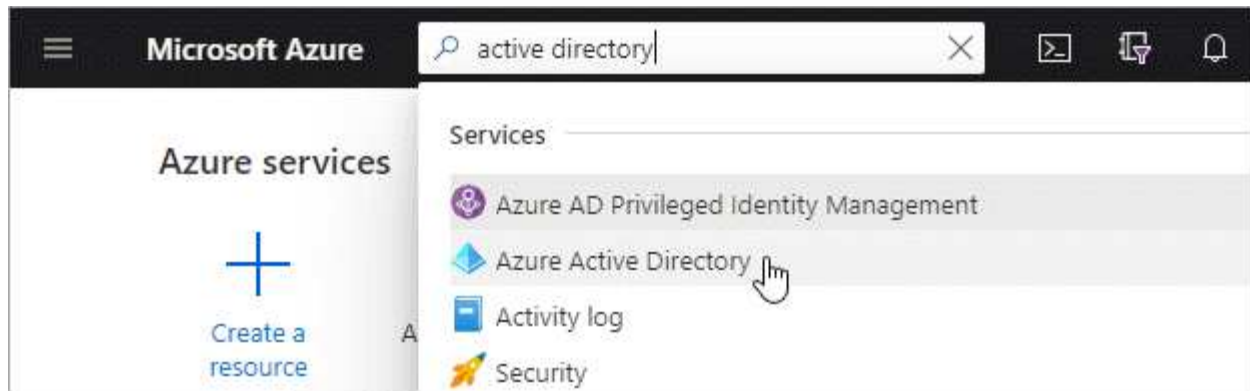
Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per il controllo degli accessi in base al ruolo.

Prima di iniziare

Per creare un'applicazione Active Directory e assegnarla a un ruolo, è necessario disporre delle autorizzazioni appropriate in Azure. Per ulteriori informazioni, fare riferimento a ["Documentazione di Microsoft Azure: Autorizzazioni richieste"](#).

Fasi

1. Dal portale Azure, aprire il servizio **Azure Active Directory**.



2. Nel menu, fare clic su **App Registrations**.
3. Fare clic su **Nuova registrazione**.
4. Specificare i dettagli dell'applicazione:
 - **Nome**: Immettere un nome per l'applicazione.
 - **Tipo di account**: Selezionare un tipo di account (qualsiasi verrà utilizzato con Cloud Manager).
 - **Redirect URI** (reindirizzamento URI): Selezionare **Web** e inserire un URL qualsiasi, ad esempio <https://url>
5. Fare clic su **Registra**.

Risultato

Hai creato l'applicazione ad e il service principal.

Assegnazione dell'applicazione a un ruolo

È necessario associare l'entità del servizio a una o più sottoscrizioni Azure e assegnarle il ruolo personalizzato di "operatore cloud manager OnCommand" in modo che quest'ultimo disponga delle autorizzazioni.

Fasi

1. Creare un ruolo personalizzato:
 - a. Scaricare il "[Policy di Cloud Manager Azure](#)".
 - b. Modificare il file JSON aggiungendo gli ID di abbonamento Azure all'ambito assegnabile.

È necessario aggiungere l'ID per ogni abbonamento Azure da cui gli utenti creeranno i sistemi Cloud Volumes ONTAP.

Esempio

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

- c. Utilizzare il file JSON per creare un ruolo personalizzato in Azure.

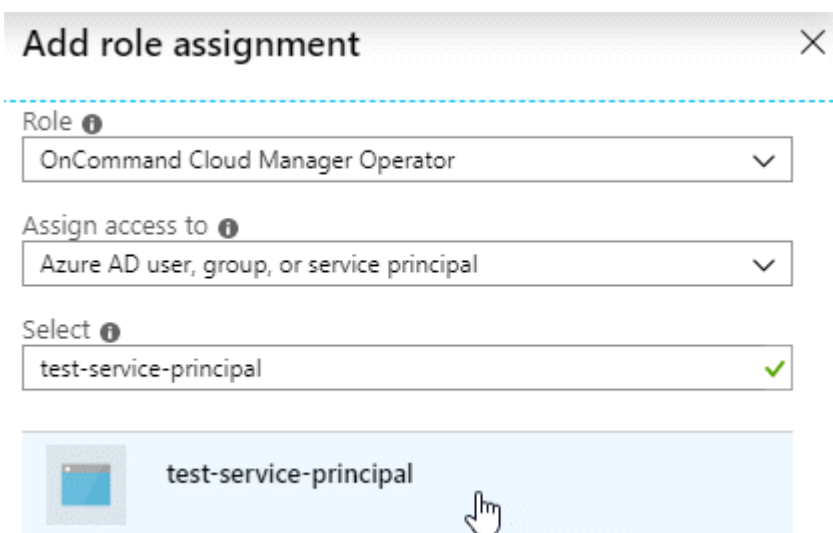
Nell'esempio seguente viene illustrato come creare un ruolo personalizzato utilizzando Azure CLI 2.0:

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

Ora dovresti avere un ruolo personalizzato chiamato *Cloud Manager Operator*.

2. Assegnare l'applicazione al ruolo:

- a. Dal portale Azure, aprire il servizio **Subscriptions**.
- b. Selezionare l'abbonamento.
- c. Fare clic su **Access control (IAM) > Add > Add role assignment** (controllo accesso (IAM) > Add > Add role assign
- d. Selezionare il ruolo **Cloud Manager Operator**.
- e. Mantieni selezionata l'opzione **Azure ad user, group o service principal**.
- f. Cercare il nome dell'applicazione (non è possibile trovarla nell'elenco scorrendo).



- g. Selezionare l'applicazione e fare clic su **Save** (Salva).

Il service principal per Cloud Manager dispone ora delle autorizzazioni Azure necessarie per tale abbonamento.

Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Cloud Manager consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

Aggiunta delle autorizzazioni API per la gestione dei servizi di Windows Azure

L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

Fasi


1. Nel servizio **Azure Active Directory**, fare clic su **App Registrations** e selezionare l'applicazione.
2. Fare clic su **API permissions > Add a permission** (autorizzazioni API > Aggiungi autorizzazione)
3. In **Microsoft API**, selezionare **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. Fare clic su **Access Azure Service Management as organization users** (Accedi a Azure Service Management come utenti dell'organizzazione), quindi fare clic su **Add permissions** (

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](#)

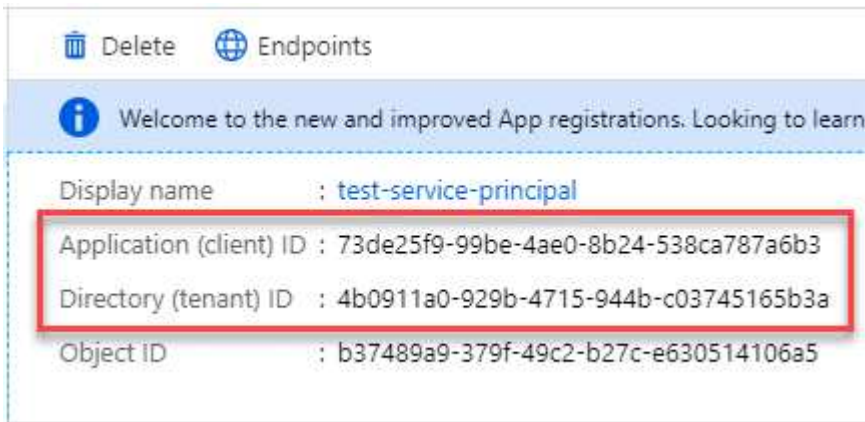
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) 	-

Ottenere l'ID dell'applicazione e l'ID della directory

Quando si aggiunge l'account Azure a Cloud Manager, è necessario fornire l'ID dell'applicazione (client) e l'ID della directory (tenant) per l'applicazione. Cloud Manager utilizza gli ID per effettuare l'accesso a livello di programmazione.

Fasi

1. Nel servizio **Azure Active Directory**, fare clic su **App Registrations** e selezionare l'applicazione.
2. Copiare **Application (client) ID** e **Directory (tenant) ID**.



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

Creazione di un client segreto

È necessario creare un client secret e quindi fornire a Cloud Manager il valore del segreto in modo che Cloud Manager possa utilizzarlo per l'autenticazione con Azure ad.



Quando si aggiunge l'account a Cloud Manager, Cloud Manager fa riferimento al segreto del client come Application Key.

Fasi

1. Aprire il servizio **Azure Active Directory**.
2. Fare clic su **App Registrations** e selezionare l'applicazione.
3. Fare clic su **certificati e segreti > nuovo segreto client**.
4. Fornire una descrizione del segreto e una durata.
5. Fare clic su **Aggiungi**.
6. Copiare il valore del client secret.

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

Risultato

L'entità del servizio è ora impostata e l'ID dell'applicazione (client), l'ID della directory (tenant) e il valore del client secret dovrebbero essere stati copiati. Devi inserire queste informazioni in Cloud Manager quando Aggiungi un account Azure.

Aggiunta di credenziali Azure a Cloud Manager

Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "[Scopri come](#)".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



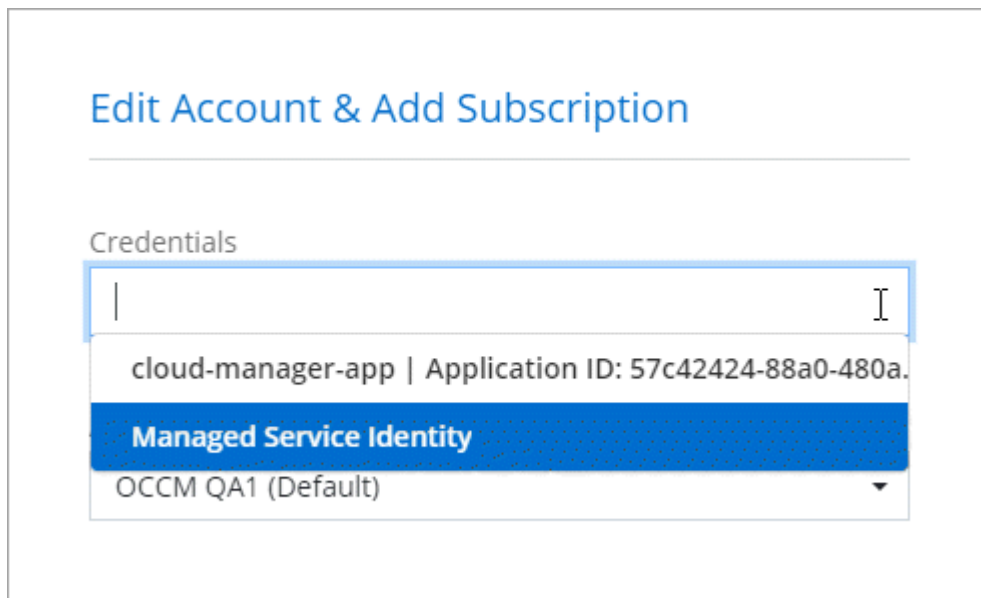
2. Fare clic su **Aggiungi credenziali** e selezionare **Microsoft Azure**.
3. Immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
 - ID applicazione (client): Vedere [Ottenerne l'ID dell'applicazione e l'ID della directory](#).
 - ID directory (tenant): Vedere [Ottenerne l'ID dell'applicazione e l'ID della directory](#).
 - Segreto del client: Vedere [Creazione di un client segreto](#).
4. Confermare che i requisiti della policy sono stati soddisfatti, quindi fare clic su **continua**.
5. Scegli l'abbonamento pay-as-you-go che desideri associare alle credenziali o fai clic su **Aggiungi abbonamento** se non ne hai ancora uno.

Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, le credenziali Azure devono essere associate a un abbonamento a Cloud Volumes ONTAP da Azure Marketplace.

6. Fare clic su **Aggiungi**.

Risultato

È ora possibile passare a un set di credenziali diverso dalla pagina Dettagli e credenziali "[quando si crea un nuovo ambiente di lavoro](#)":



Associazione di un abbonamento a Azure Marketplace alle credenziali

Dopo aver aggiunto le tue credenziali Azure a Cloud Manager, puoi associare un abbonamento a Azure Marketplace a tali credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

Esistono due scenari in cui è possibile associare un abbonamento a Azure Marketplace dopo aver aggiunto le credenziali a Cloud Manager:

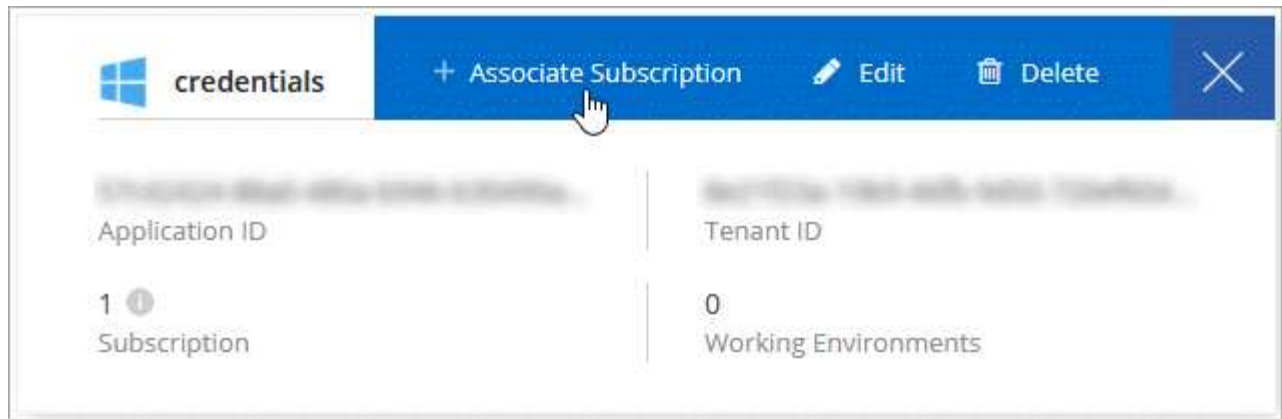
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento a Azure Marketplace esistente con un nuovo abbonamento.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "[Scopri come](#)".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Passare il mouse su un set di credenziali e fare clic sul menu delle azioni.
3. Dal menu, fare clic su **Associa abbonamento**.



4. Selezionare un abbonamento dall'elenco a discesa oppure fare clic su **Aggiungi abbonamento** e seguire la procedura per creare un nuovo abbonamento.

Il seguente video inizia dal contesto della procedura guidata dell'ambiente di lavoro, ma mostra lo stesso flusso di lavoro dopo aver fatto clic su **Add Subscription** (Aggiungi abbonamento):

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

Associazione di sottoscrizioni Azure aggiuntive a un'identità gestita

Cloud Manager consente di scegliere le credenziali Azure e l'abbonamento Azure in cui si desidera implementare Cloud Volumes ONTAP. Non è possibile selezionare un'altra sottoscrizione Azure per il profilo di identità gestita, a meno che non venga associato a. "identità gestita" con questi abbonamenti.

A proposito di questa attività

Un'identità gestita è "L'account Azure iniziale" Quando si implementa un connettore da Cloud Manager. Quando hai implementato il connettore, Cloud Manager ha creato il ruolo Cloud Manager Operator e lo ha assegnato alla macchina virtuale del connettore.

Fasi

1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare Cloud Volumes ONTAP.
3. Fare clic su **controllo di accesso (IAM)**.
 - a. Fare clic su **Aggiungi > Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
 - Selezionare il ruolo **Cloud Manager Operator**.



Cloud Manager Operator è il nome predefinito fornito in "Policy di Cloud Manager". Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

- Assegnare l'accesso a una **macchina virtuale**.
 - Selezionare l'abbonamento in cui è stata creata la macchina virtuale Connector.
 - Selezionare la macchina virtuale Connector.
 - Fare clic su **Save** (Salva).
4. Ripetere questa procedura per gli abbonamenti aggiuntivi.

Risultato

Quando crei un nuovo ambiente di lavoro, dovresti ora avere la possibilità di scegliere tra più sottoscrizioni Azure per il profilo di identità gestito.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.