Amministrare Cloud Manager

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

Amministrare Cloud Manager

Individuazione dell'ID di sistema di Cloud Manager

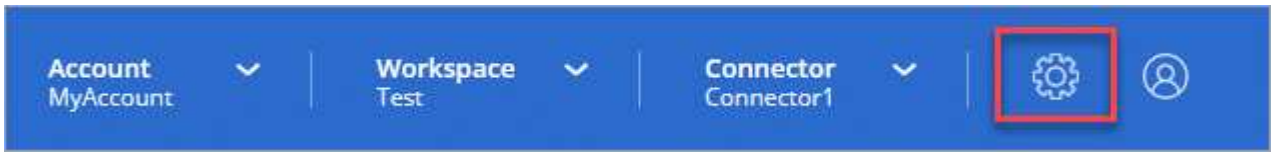
Per aiutarti a iniziare, il tuo rappresentante NetApp potrebbe richiedere l'ID di sistema Cloud Manager. L'ID viene generalmente utilizzato a scopo di licensing e troubleshooting.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

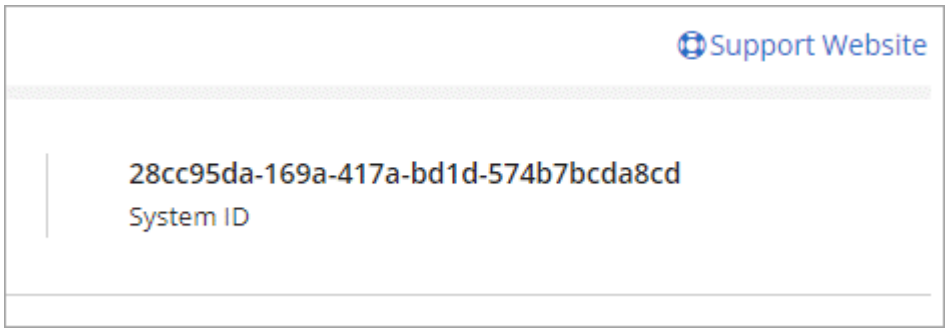
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni.



2. Fare clic su **Support Dashboard**.

   L'ID di sistema viene visualizzato in alto a destra.

   Esempio



Gestire i connettori

Gestione dei connettori esistenti

Dopo aver creato uno o più connettori, è possibile gestirli passando da connettori a interfacce utente locali in esecuzione su un connettore e altro ancora.

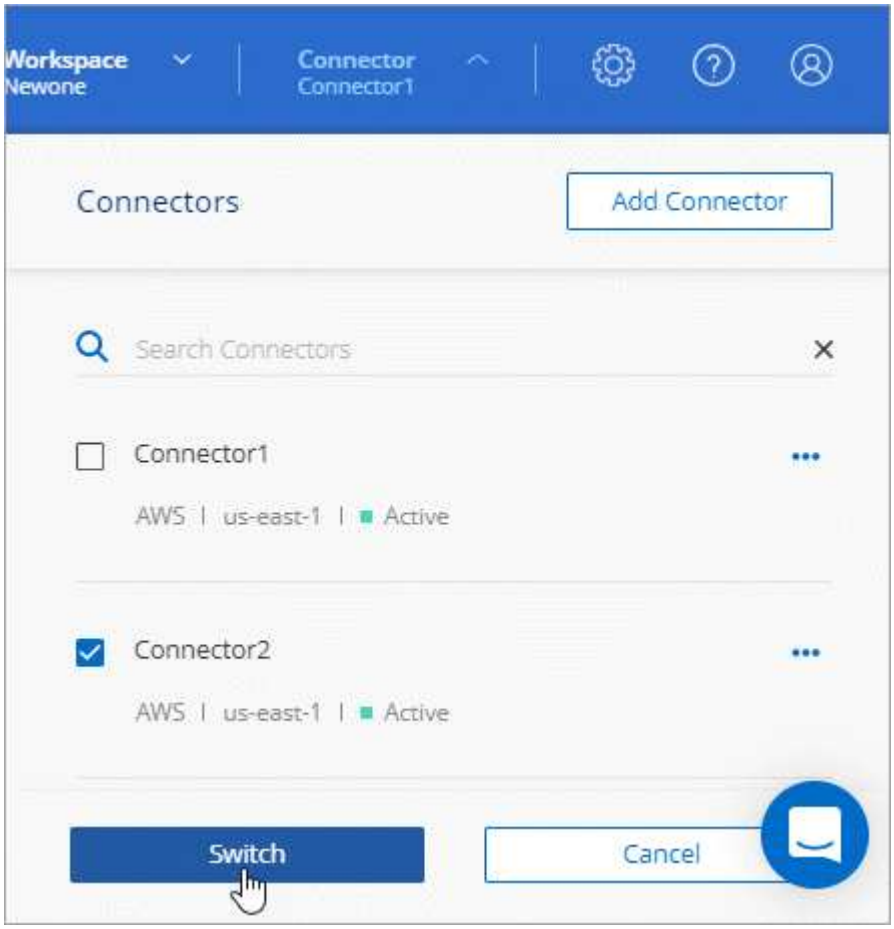
Passaggio da un connettore all'altro

Se si dispone di più connettori, è possibile passare da un connettore all'altro per visualizzare gli ambienti di lavoro associati a uno specifico connettore.

Ad esempio, supponiamo di lavorare in un ambiente multi-cloud. In AWS potrebbe essere presente un connettore e in Google Cloud un altro connettore. Per gestire i sistemi Cloud Volumes ONTAP in esecuzione in tali cloud, è necessario passare da un connettore all'altro.

Fase

1. Fare clic sull'elenco a discesa **Connector**, selezionare un altro connettore, quindi fare clic su **Switch**.



Cloud Manager aggiorna e mostra gli ambienti di lavoro associati al connettore selezionato.

Accesso all'interfaccia utente locale

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Questa interfaccia è necessaria per alcune attività che devono essere eseguite dal connettore stesso:

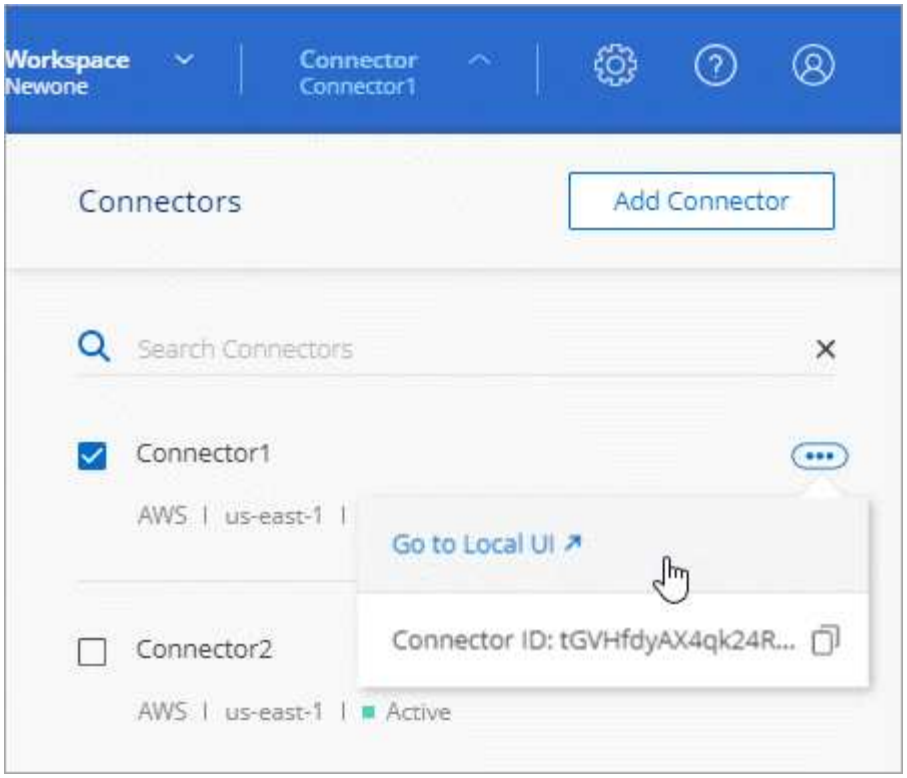
- "Impostazione di un server proxy"
- Installazione di una patch (in genere collaborerete con il personale NetApp per installare una patch)
- Download dei messaggi AutoSupport (solitamente indirizzati dal personale NetApp in caso di problemi)

Fasi

1. "Accedere all'interfaccia SaaS di Cloud Manager" Da un computer che dispone di una connessione di rete all'istanza del connettore.

   Se il connettore non dispone di un indirizzo IP pubblico, è necessaria una connessione VPN oppure è necessario connettersi da un host di collegamento che si trova nella stessa rete del connettore.

2. Fare clic sull'elenco a discesa **Connector**, selezionare il menu delle azioni di un connettore, quindi fare clic su **Go to Local UI** (Vai all'interfaccia utente locale).



L'interfaccia di Cloud Manager in esecuzione sul connettore viene caricata in una nuova scheda del browser.

Rimozione dei connettori da Cloud Manager

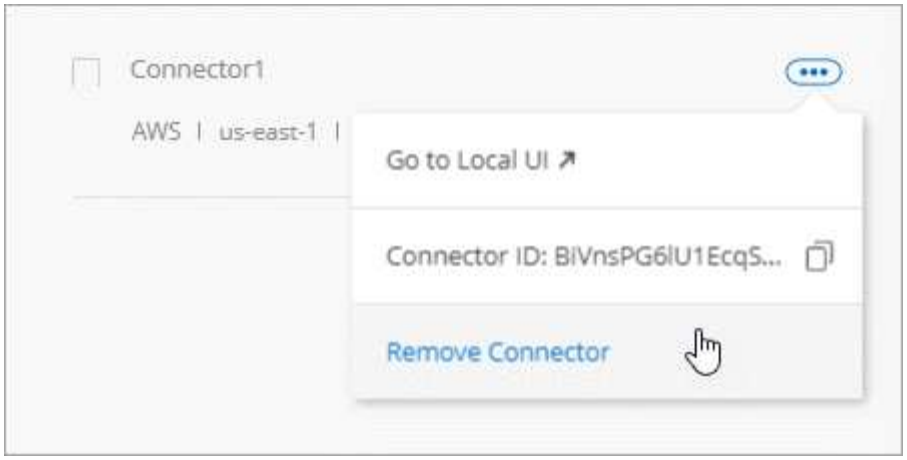
Se un connettore non è attivo, è possibile rimuoverlo dall'elenco dei connettori in Cloud Manager. Questa operazione può essere eseguita se la macchina virtuale Connector è stata eliminata o se il software Connector è stato disinstallato.

Tenere presente quanto segue per la rimozione di un connettore:

- Questa azione non elimina la macchina virtuale.
- Questa azione non può essere ripristinata - una volta rimosso un connettore da Cloud Manager, non puoi aggiungerlo di nuovo a Cloud Manager.

Fasi

1. Fare clic sull'elenco a discesa Connector dall'intestazione Cloud Manager.
2. Fare clic sul menu delle azioni per un connettore inattivo e fare clic su **Remove Connector** (Rimuovi connettore).



3. Inserire il nome del connettore da confermare, quindi fare clic su Remove (Rimuovi).

Risultato

Cloud Manager rimuove il connettore dai record.

Disinstallazione del software Connector

Il connettore include uno script di disinstallazione che è possibile utilizzare per disinstallare il software per risolvere i problemi o per rimuovere in modo permanente il software dall'host.

Fase

1. Eseguire lo script di disinstallazione dall'host Linux:

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

   silent esegue lo script senza richiedere conferma.

E gli aggiornamenti software?

Il connettore aggiorna automaticamente il software alla versione più recente, a patto che sia disponibile "accesso a internet in uscita" per ottenere l'aggiornamento software.

Altri modi per creare connettori

Requisiti host del connettore

Il software del connettore deve essere eseguito su un host che soddisfi i requisiti specifici del sistema operativo, della RAM, dei requisiti delle porte e così via.

È richiesto un host dedicato

Il connettore non è supportato su un host condiviso con altre applicazioni. L'host deve essere un host dedicato.

CPU

4 core o 4 vCPU

RAM

14 GB

Tipo di istanza AWS EC2

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare t3.xlarge e quel tipo di istanza quando si implementa il connettore direttamente da Cloud Manager.

Dimensione delle macchine virtuali Azure

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare DS3 v2 e le dimensioni delle macchine virtuali quando si implementa il connettore direttamente da Cloud Manager.

Tipo di macchina GCP

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare n1-standard-4 e questo tipo di macchina quando si implementa il connettore direttamente da Cloud Manager.

Sistemi operativi supportati

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  Il sistema Red Hat Enterprise Linux deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione del connettore.

  Il connettore è supportato dalle versioni in lingua inglese di questi sistemi operativi.

Hypervisor

Un hypervisor bare metal o in hosting certificato per l'esecuzione di CentOS o Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Soluzione Red Hat: Quali hypervisor sono certificati per eseguire Red Hat Enterprise Linux?"^]

Spazio su disco in /opz

Devono essere disponibili 100 GB di spazio

Accesso a Internet in uscita

L'accesso a Internet in uscita è necessario per installare il connettore e per gestire le risorse e i processi all'interno dell'ambiente di cloud pubblico. Per un elenco degli endpoint, vedere "Requisiti di rete per il connettore".

Creazione di un connettore da AWS Marketplace

Si consiglia di creare un connettore direttamente da Cloud Manager, ma è possibile avviare un connettore da AWS Marketplace, se non si desidera specificare le chiavi di accesso AWS. Dopo aver creato e configurato il connettore, Cloud Manager lo utilizzerà automaticamente quando si creano nuovi ambienti di lavoro.

Fasi

1. Creare un criterio e un ruolo IAM per l'istanza EC2:

a. Scarica la policy IAM di Cloud Manager dal seguente percorso:

   "NetApp Cloud Manager: Policy AWS, Azure e GCP"

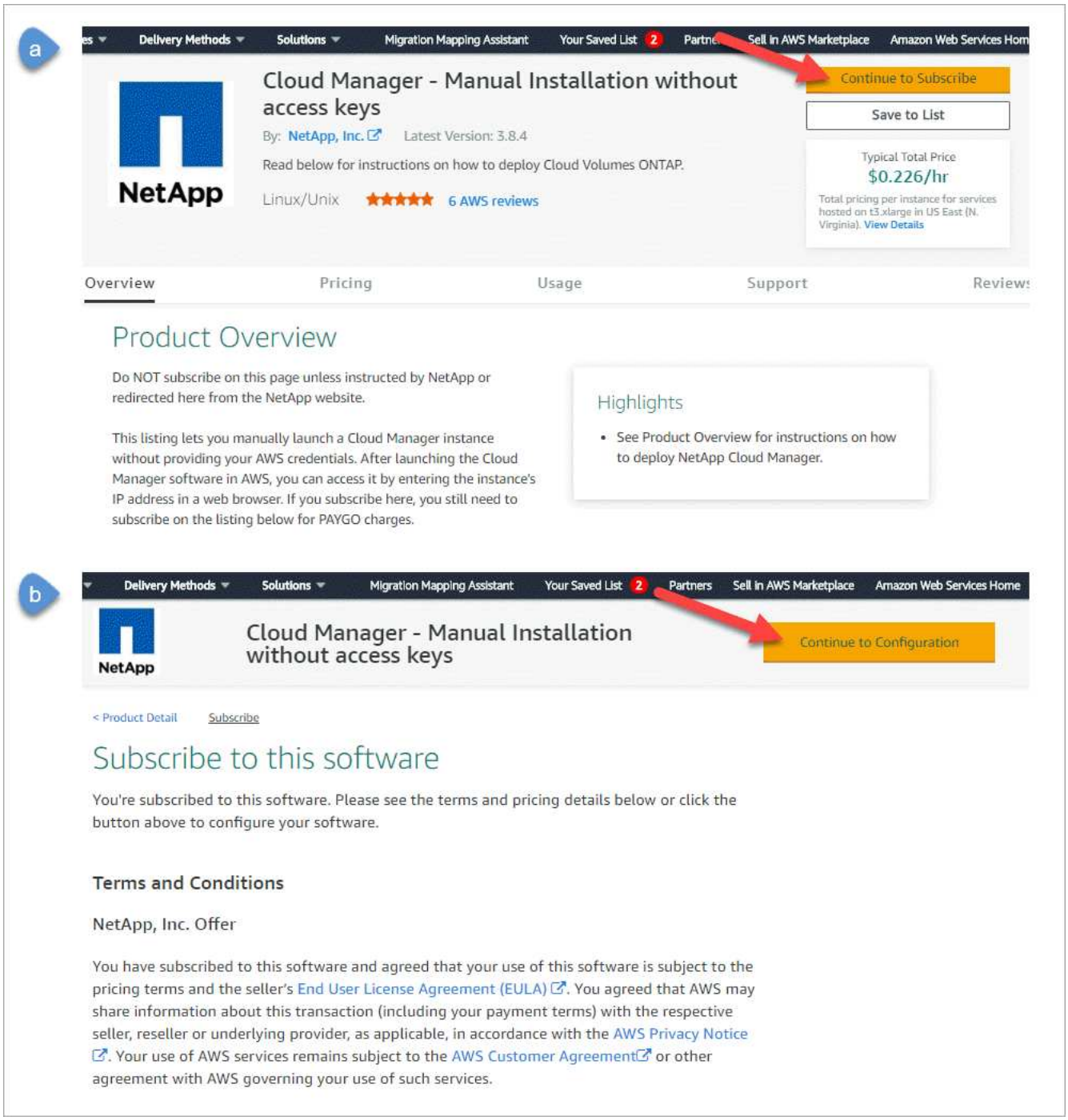
b. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.

c. Creare un ruolo IAM con il tipo di ruolo Amazon EC2 e allegare al ruolo il criterio creato nel passaggio precedente.

2. Passare alla "Pagina Cloud Manager su AWS Marketplace" Per implementare Cloud Manager da un AMI.

   L'utente IAM deve disporre delle autorizzazioni AWS Marketplace per iscriversi e annullare l'iscrizione.

3. Nella pagina Marketplace, fare clic su **Continue to Subscribe**, quindi fare clic su **Continue to Configuration**.



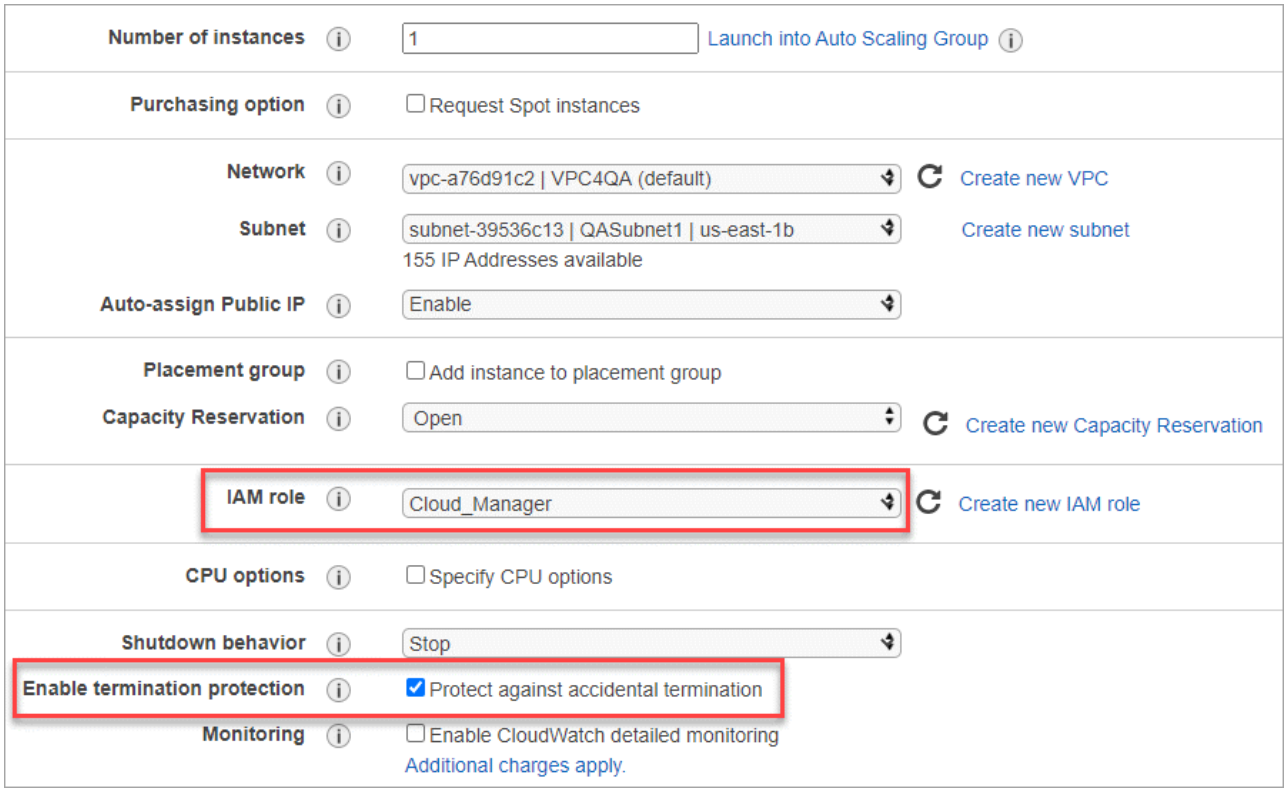
4. Modificare una delle opzioni predefinite e fare clic su **Continue to Launch** (continua fino all'avvio).
5. In **Choose Action** (Scegli azione), selezionare **Launch through EC2** (Avvia tramite EC2*), quindi fare clic su **Launch** (Avvia).

   Questi passaggi descrivono come avviare l'istanza dalla console EC2 perché la console consente di associare un ruolo IAM all'istanza di Cloud Manager. Ciò non è possibile utilizzando l'azione **Launch from Website** (Avvia dal sito Web).

6. Seguire le istruzioni per configurare e implementare l'istanza:
   - **Choose Instance Type** (Scegli tipo di istanza): A seconda della disponibilità della regione, scegliere uno dei tipi di istanza supportati (si consiglia t3.xlarge).

"Esaminare i requisiti dell'istanza".

- **Configure Instance** (Configura istanza): Selezionare un VPC e una subnet, scegliere il ruolo IAM creato al punto 1, abilitare la protezione di terminazione (scelta consigliata) e scegliere qualsiasi altra opzione di configurazione che soddisfi i requisiti.



- **Add Storage** (Aggiungi storage): Mantenere le opzioni di storage predefinite.
- **Add Tags** (Aggiungi tag): Se si desidera, inserire i tag per l'istanza.
- **Configure Security Group** (Configura gruppo di protezione): Specificare i metodi di connessione richiesti per l'istanza del connettore: SSH, HTTP e HTTPS.
- **Revisione**: Rivedere le selezioni e fare clic su **Avvia**.

  AWS avvia il software con le impostazioni specificate. L'istanza di Connector e il software dovrebbero essere in esecuzione in circa cinque minuti.

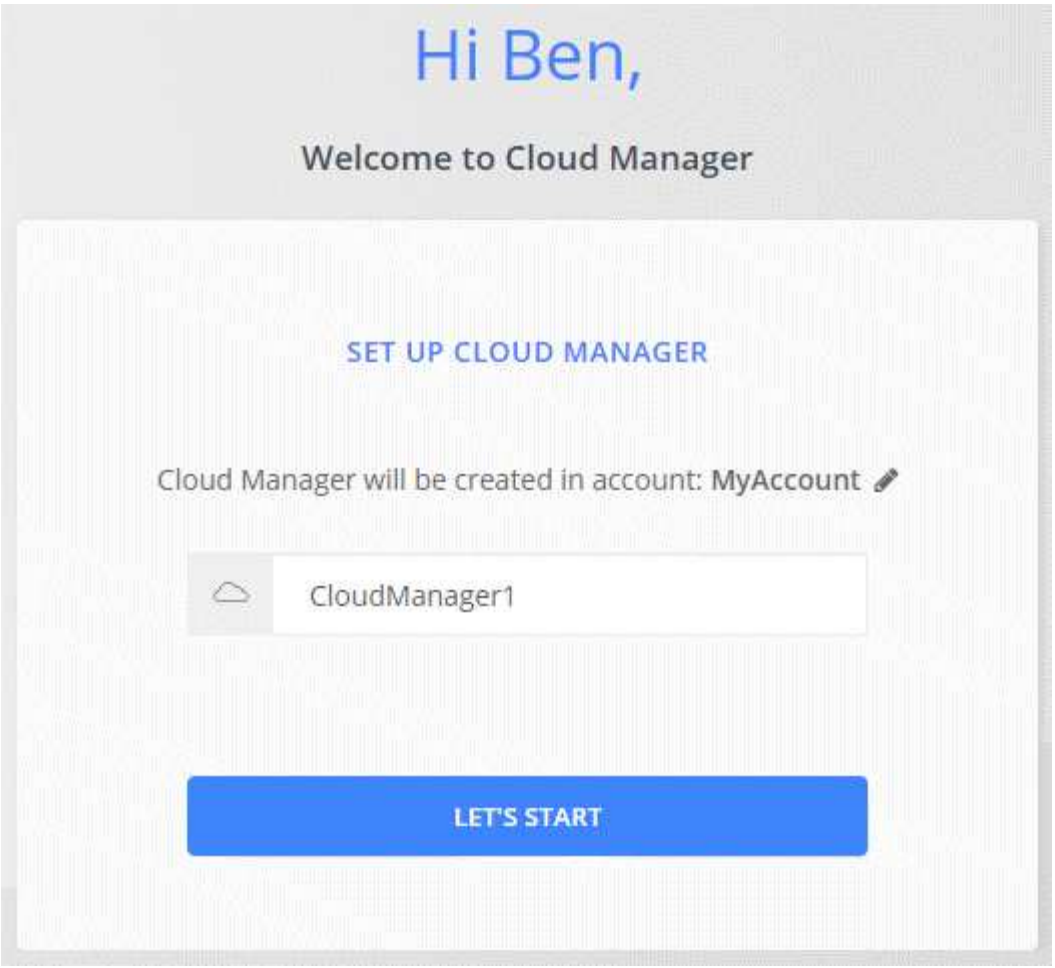
7. Aprire un browser Web da un host connesso all'istanza del connettore e immettere il seguente URL:

   http://ipaddress:80

8. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account Cloud Central da associare al connettore.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Il connettore è ora installato e configurato con il tuo account Cloud Central. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro. Tuttavia, se si dispone di più connettori, è necessario "passare da un'opzione all'altra".

Creazione di un connettore da Azure Marketplace

Si consiglia di creare un connettore direttamente da Cloud Manager, ma è possibile avviare un connettore da Azure Marketplace, se si preferisce. Dopo aver creato e configurato il connettore, Cloud Manager lo utilizzerà automaticamente quando si creano nuovi ambienti di lavoro.

Creazione di un connettore in Azure

Implementare il connettore in Azure utilizzando l'immagine in Azure Marketplace, quindi accedere al connettore per specificare l'account Cloud Central.

Fasi

1. "Vai alla pagina di Azure Marketplace per Cloud Manager".
2. Fare clic su **Get it now** (scarica ora), quindi su **Continue** (continua).
3. Dal portale Azure, fare clic su **Create** (Crea) e seguire la procedura per configurare la macchina virtuale.

   Durante la configurazione della macchina virtuale, tenere presente quanto segue:

- Cloud Manager può funzionare in modo ottimale con dischi HDD o SSD.
- Scegli una macchina virtuale che soddisfi i requisiti di CPU e RAM. Si consiglia DS3 v2.

  "Esaminare i requisiti delle macchine virtuali".

- Per il gruppo di protezione della rete, il connettore richiede connessioni in entrata utilizzando SSH, HTTP e HTTPS.

  "Scopri di più sulle regole dei gruppi di sicurezza per il connettore".

- In **Management**, abilitare **System Assigned Managed Identity** per il connettore selezionando **ON**.

  Questa impostazione è importante perché un'identità gestita consente alla macchina virtuale del connettore di identificarsi in Azure Active Directory senza fornire credenziali. "Scopri di più sulle identità gestite per le risorse Azure".

4. Nella pagina **Review + create**, esaminare le selezioni e fare clic su **Create** per avviare l'implementazione.

   Azure implementa la macchina virtuale con le impostazioni specificate. La macchina virtuale e il software del connettore dovrebbero essere in esecuzione in circa cinque minuti.

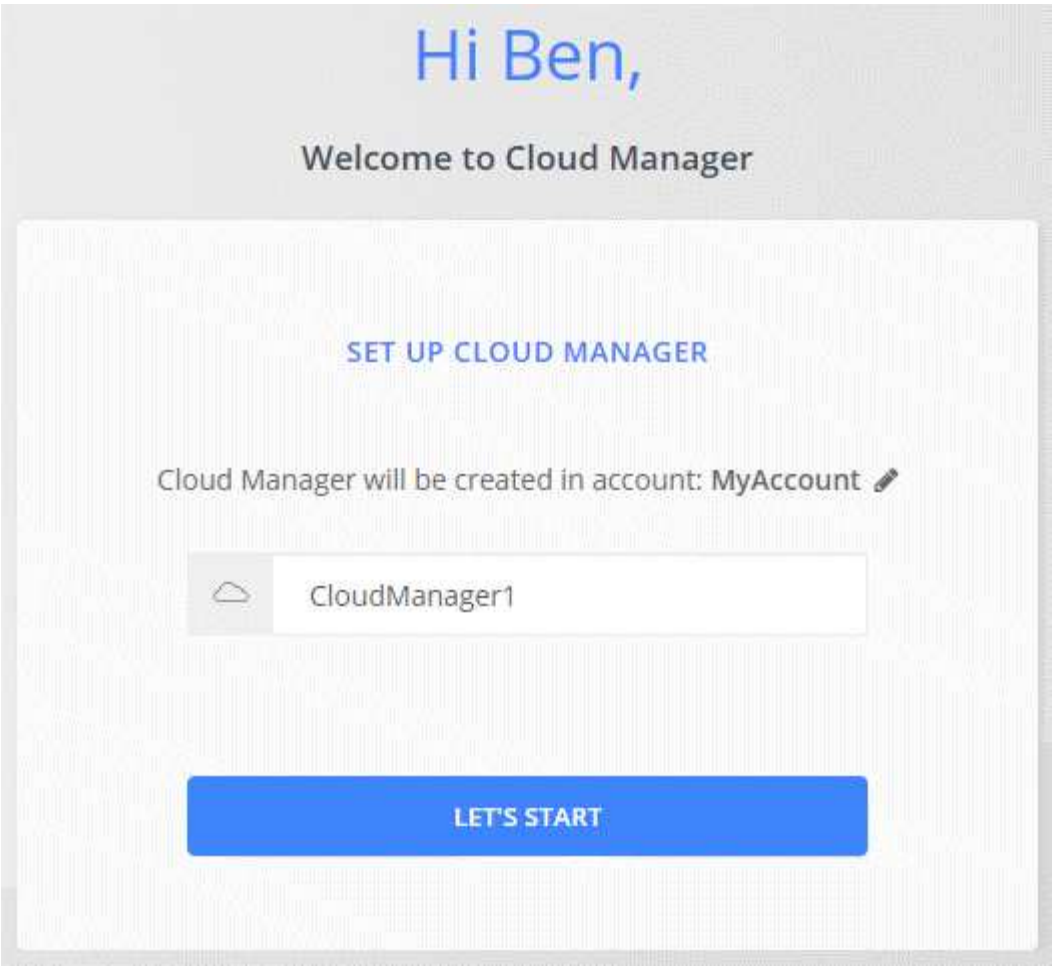
5. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   http://ipaddress:80

6. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account Cloud Central da associare al connettore.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Il connettore è stato installato e configurato. È necessario concedere le autorizzazioni Azure prima che gli utenti possano implementare Cloud Volumes ONTAP in Azure.

Concessione delle autorizzazioni Azure

Quando si implementa il connettore in Azure, è necessario aver attivato un "identità gestita assegnata dal sistema". È ora necessario concedere le autorizzazioni necessarie per Azure creando un ruolo personalizzato e assegnando il ruolo alla macchina virtuale del connettore per una o più sottoscrizioni.

Fasi

1. Creare un ruolo personalizzato utilizzando la policy di Cloud Manager:

   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-c25fbzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscriptions/398e471c-3b42-4ae7-9bzzbce5bzzbce5bce5bzzbce5bce5bce5b5b

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 che puoi assegnare alla macchina virtuale del connettore.

2. Assegnare il ruolo alla macchina virtuale Connector per una o più sottoscrizioni:
   a. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare i sistemi Cloud Volumes ONTAP.
   b. Fare clic su **controllo di accesso (IAM)**.
   c. 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).
   d. Se si desidera implementare Cloud Volumes ONTAP da abbonamenti aggiuntivi, passare a tale abbonamento e ripetere la procedura.

Risultato

Il connettore dispone ora delle autorizzazioni necessarie all'IT per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro. Tuttavia, se si dispone di più connettori, è necessario "passare da un'opzione all'altra".

Installazione del software del connettore su un host Linux esistente

Il modo più comune per creare un connettore è direttamente da Cloud Manager o dal mercato di un cloud provider. Tuttavia, è possibile scaricare e installare il software del connettore su un host Linux esistente nella rete o nel cloud.

Se si desidera creare un sistema Cloud Volumes ONTAP in Google Cloud, è necessario disporre di un connettore in esecuzione anche in Google Cloud. Non è possibile utilizzare un connettore in esecuzione in un'altra posizione.

Requisiti

- L'host deve soddisfare "Requisiti per il connettore".
- Un sistema Red Hat Enterprise Linux deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.

- Il programma di installazione di Connector accede a diversi URL durante il processo di installazione. È necessario assicurarsi che l'accesso a Internet in uscita sia consentito a questi endpoint:
  - 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

    L'host potrebbe tentare di aggiornare i pacchetti del sistema operativo durante l'installazione. L'host può contattare diversi siti di mirroring per questi pacchetti di sistemi operativi.

A proposito di questa attività

- Per installare il connettore non sono necessari i privilegi di root.
- L'installazione installa gli strumenti della riga di comando AWS (awscli) per abilitare le procedure di ripristino dal supporto NetApp.

  Se viene visualizzato un messaggio che indica che l'installazione di awscli non è riuscita, ignorare il messaggio. Il connettore può funzionare correttamente senza gli strumenti.

- Il programma di installazione disponibile sul NetApp Support Site potrebbe essere una versione precedente. Dopo l'installazione, il connettore si aggiorna automaticamente se è disponibile una nuova versione.

Fasi

1. Scaricare il software Cloud Manager da "Sito di supporto NetApp", Quindi copiarlo sull'host Linux.

   Per informazioni sulla connessione e la copia del file in un'istanza EC2 in AWS, vedere "Documentazione AWS: Connessione all'istanza Linux tramite SSH".

2. Assegnare le autorizzazioni per eseguire lo script.

   Esempio

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Eseguire lo script di installazione:
   ```

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

   silent esegue l'installazione senza richiedere informazioni.

   proxy è richiesto se l'host si trova dietro un server proxy.

   proxyport è la porta del server proxy.

   proxyuser è il nome utente del server proxy, se è richiesta l'autenticazione di base.

   proxypwd è la password per il nome utente specificato.

3. A meno che non sia stato specificato il parametro silent, digitare **Y** per continuare lo script, quindi immettere le porte HTTP e HTTPS quando richiesto.

Cloud Manager è ora installato. Al termine dell'installazione, il servizio Cloud Manager (occm) viene riavviato due volte se è stato specificato un server proxy.

4. Aprire un browser Web e immettere il seguente URL:

   https://ipaddress:port

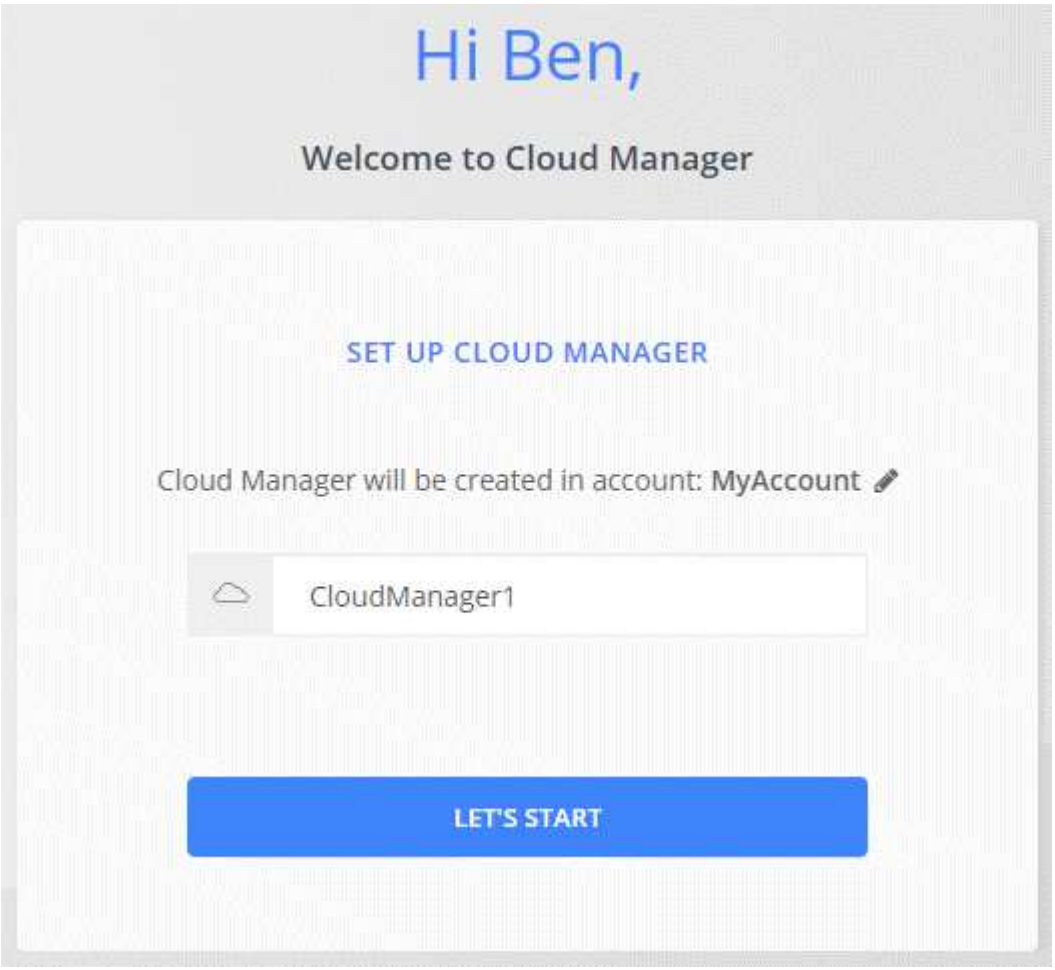
   Ipaddress può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host. Ad esempio, se il connettore si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario inserire un indirizzo IP privato da un host che ha una connessione all'host del connettore.

   Port è obbligatorio se sono state modificate le porte HTTP (80) o HTTPS (443) predefinite. Ad esempio, se la porta HTTPS è stata modificata in 8443, immettere https://ipaddress:8443

5. Iscriviti a NetApp Cloud Central o effettua l'accesso.
6. Dopo aver effettuato l'accesso, configurare Cloud Manager:
   a. Specificare l'account Cloud Central da associare al connettore.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Il connettore è ora installato e configurato con il tuo account Cloud Central. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro.

Al termine

Imposta le autorizzazioni in modo che Cloud Manager possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico:

- AWS: "Configurare un account AWS e aggiungerlo a Cloud Manager".
- Azure: "Configura un account Azure e aggiungilo a Cloud Manager".
- GCP: Impostare un account di servizio che disponga delle autorizzazioni necessarie a Cloud Manager per creare e gestire i sistemi Cloud Volumes ONTAP nei progetti.
  a. "Creare un ruolo in GCP" che include le autorizzazioni definite in "Policy di Cloud Manager per GCP".
  b. "Creare un account di servizio GCP e applicare il ruolo personalizzato appena creato".
  c. "Associare questo account di servizio alla macchina virtuale del connettore".
  d. Se si desidera implementare Cloud Volumes ONTAP in altri progetti, "Concedere l'accesso aggiungendo l'account di servizio con il ruolo Cloud Manager a quel progetto". Dovrai ripetere questo passaggio per ogni progetto.

Configurazione predefinita per il connettore

Se è necessario risolvere i problemi del connettore, potrebbe essere utile comprendere come è configurato.

- Se hai implementato il connettore da Cloud Manager (o direttamente dal mercato di un cloud provider), prendi nota di quanto segue:
  - In AWS, il nome utente per l'istanza EC2 Linux è ec2-user.
  - Il sistema operativo per l'immagine è il seguente:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.
- La cartella di installazione del connettore si trova nella seguente posizione:

  /opt/application/netapp/cloudmanager
- I file di log sono contenuti nella seguente cartella:

  /opt/application/netapp/cloudmanager/log
- Il servizio Cloud Manager è denominato occm.
- Il servizio occm dipende dal servizio MySQL.

  Se il servizio MySQL non è attivo, anche il servizio occm è inattivo.

- Cloud Manager installa i seguenti pacchetti sull'host Linux, se non sono già installati:
  - 7zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Tirare
  - Wget
- Il connettore utilizza le seguenti porte sull'host Linux:
  - 80 per l'accesso HTTP
  - 443 per l'accesso HTTPS
  - 3306 per il database Cloud Manager
  - 8080 per il proxy API Cloud Manager
  - 8666 per l'API di Service Manager
  - 8777 per l'API del servizio container Health-Checker

Gestire le credenziali

AWS

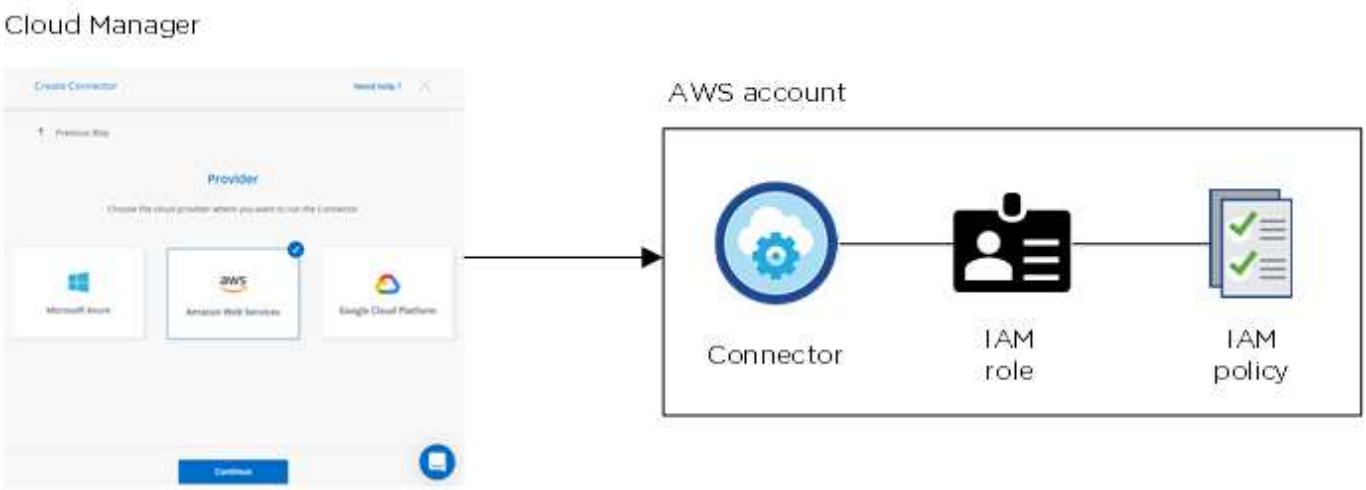
Credenziali e autorizzazioni AWS

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

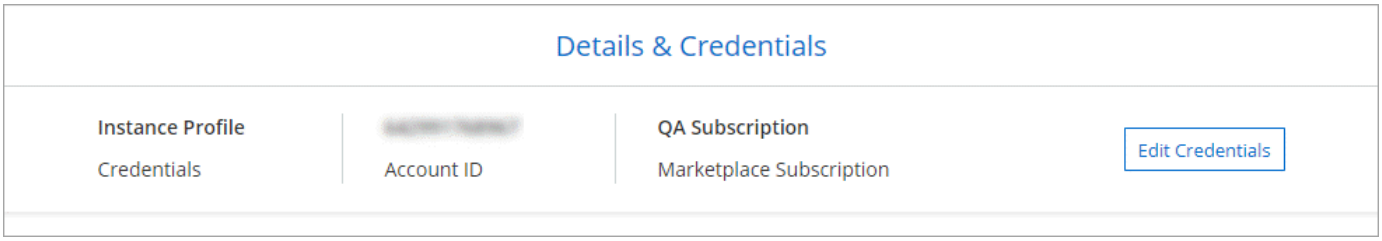
Credenziali AWS iniziali

Quando si implementa un connettore da Cloud Manager, è necessario utilizzare un account AWS che disponga delle autorizzazioni per avviare l'istanza di Connector. Le autorizzazioni richieste sono elencate nella "Policy di implementazione del connettore per AWS".

Quando Cloud Manager avvia l'istanza del connettore in AWS, crea un ruolo IAM e un profilo di istanza per l'istanza. Allega inoltre una policy che fornisce a Cloud Manager le autorizzazioni per gestire risorse e processi all'interno di tale account AWS. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".

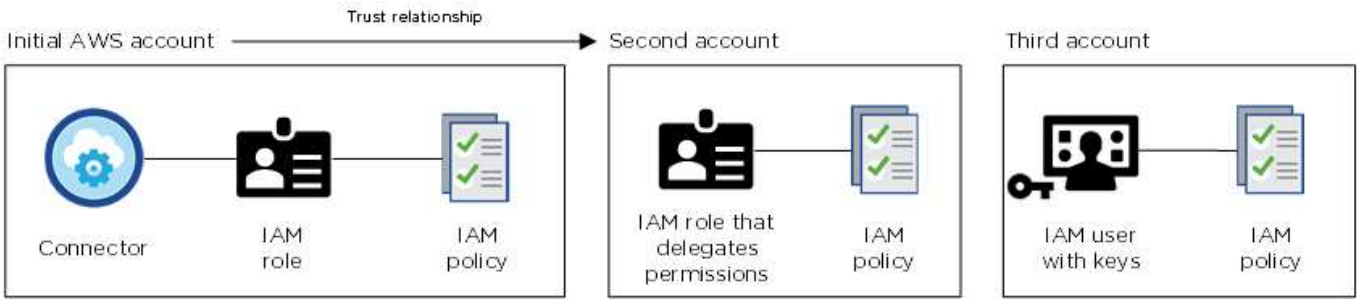


Cloud Manager seleziona queste credenziali AWS per impostazione predefinita quando crei un nuovo ambiente di lavoro per Cloud Volumes ONTAP:



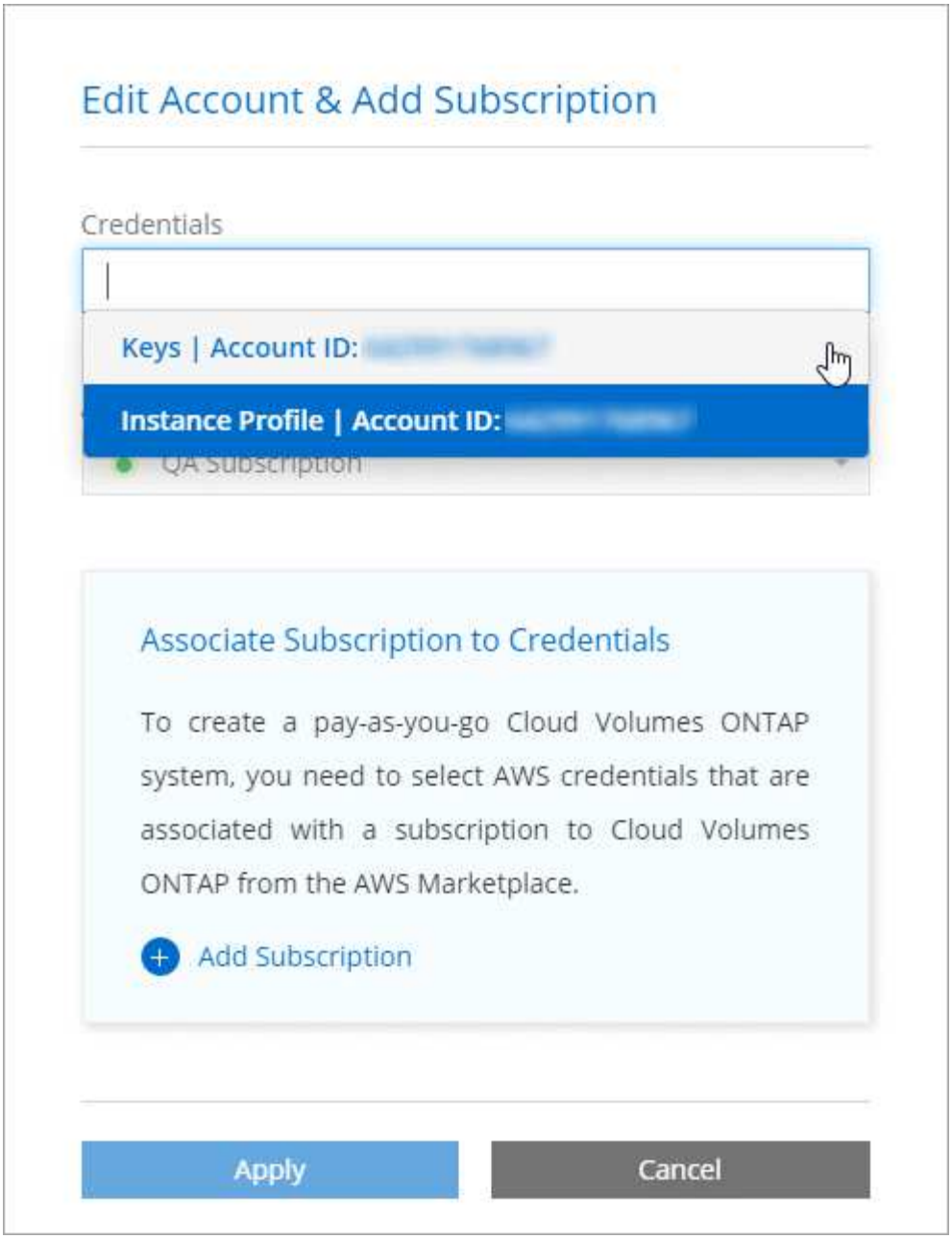
Credenziali AWS aggiuntive

Se si desidera avviare Cloud Volumes ONTAP in diversi account AWS, è possibile farlo "Fornire le chiavi AWS per un utente IAM o l'ARN di un ruolo in un account attendibile". L'immagine seguente mostra due account aggiuntivi, uno che fornisce le autorizzazioni tramite un ruolo IAM in un account attendibile e l'altro tramite le chiavi AWS di un utente IAM:



Allora "Aggiungere le credenziali dell'account a Cloud Manager" Specificando il nome risorsa Amazon (ARN) del ruolo IAM o le chiavi AWS per l'utente IAM.

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 Cloud Manager. È inoltre possibile implementare un connettore in AWS da "Mercato AWS" 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 il ruolo IAM, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un ruolo IAM per il sistema Cloud Manager, ma è possibile fornire le autorizzazioni esattamente come si farebbe per altri account AWS.

Come si possono ruotare in modo sicuro le credenziali AWS?

Come descritto in precedenza, Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le

chiavi di accesso AWS.

Con le prime due opzioni, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice: È automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Gestione delle credenziali AWS e delle sottoscrizioni per Cloud Manager

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

Prima di aggiungere le credenziali AWS a Cloud Manager, è necessario fornire le autorizzazioni necessarie per tale account. Le autorizzazioni consentono a Cloud Manager di gestire risorse e processi all'interno di tale account AWS. La modalità di fornitura delle autorizzazioni dipende dal fatto che si desideri fornire a Cloud Manager le chiavi AWS o l'ARN di un ruolo in un account attendibile.

Quando hai implementato un connettore da Cloud Manager, Cloud Manager ha aggiunto automaticamente le credenziali AWS per l'account in cui hai implementato il connettore. Questo account iniziale non viene aggiunto se il software Connector è stato installato manualmente su un sistema esistente. "Scopri le credenziali e le autorizzazioni AWS".

Scelte

- Concessione delle autorizzazioni fornendo le chiavi AWS
- Concessione delle autorizzazioni assumendo ruoli IAM in altri account

Come si possono ruotare in modo sicuro le credenziali AWS?

Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le chiavi di accesso AWS. "Scopri di più sulle credenziali e le autorizzazioni AWS".

Con le prime due opzioni, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice, è automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Concessione delle autorizzazioni fornendo le chiavi AWS

Se si desidera fornire a Cloud Manager le chiavi AWS per un utente IAM, è necessario concedere le autorizzazioni necessarie a tale utente. La policy IAM di Cloud Manager definisce le azioni e le risorse AWS che Cloud Manager può utilizzare.

Fasi

1. Scarica la policy IAM di Cloud Manager da "Pagina delle policy di Cloud Manager".
2. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud

Manager.

"Documentazione AWS: Creazione di policy IAM"

3. Allegare il criterio a un ruolo IAM o a un utente IAM.
   - "Documentazione AWS: Creazione dei ruoli IAM"
   - "Documentazione di AWS: Aggiunta e rimozione dei criteri IAM"

Risultato

L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Concessione delle autorizzazioni assumendo ruoli IAM in altri account

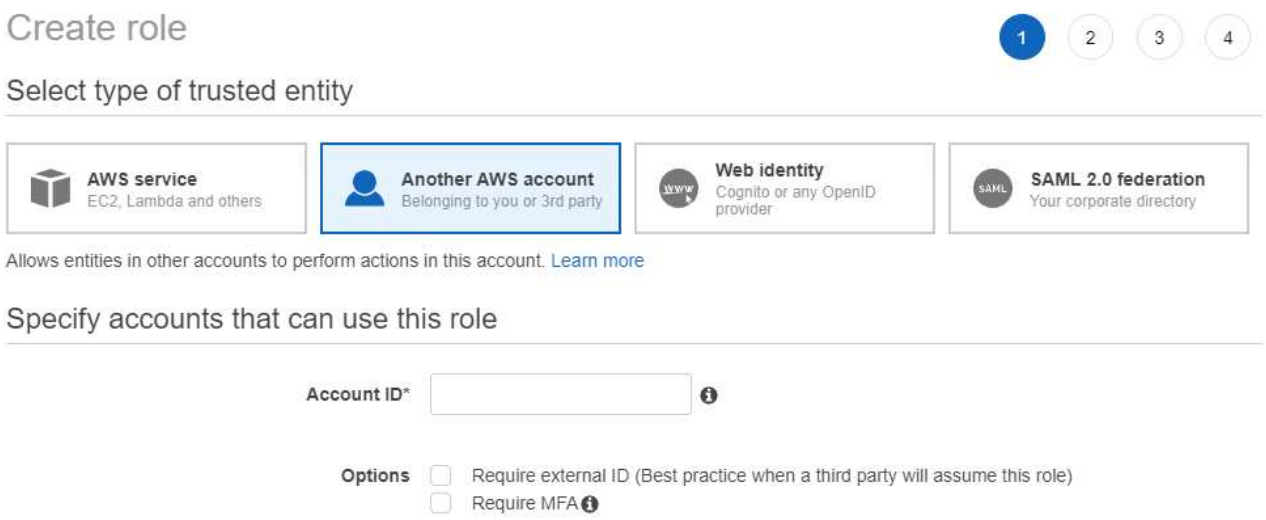
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Connector e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

Fasi

1. Accedere all'account di destinazione in cui si desidera implementare Cloud Volumes ONTAP e creare un ruolo IAM selezionando **un altro account AWS**.

   Assicurarsi di effettuare le seguenti operazioni:

   - Inserire l'ID dell'account in cui risiede l'istanza di Connector.
   - Allegare la policy IAM di Cloud Manager, disponibile in "Pagina delle policy di Cloud Manager".



2. Accedere all'account di origine in cui risiede l'istanza di Connector e selezionare il ruolo IAM associato all'istanza.

   a. Fare clic su **Allega policy**, quindi su **Crea policy**.

   b. Creare una policy che includa l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

      Esempio

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

Risultato

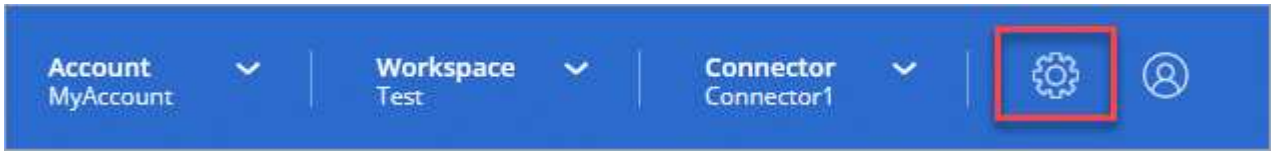
L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Aggiunta di credenziali AWS a Cloud Manager

Dopo aver fornito un account AWS 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.

Fasi

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



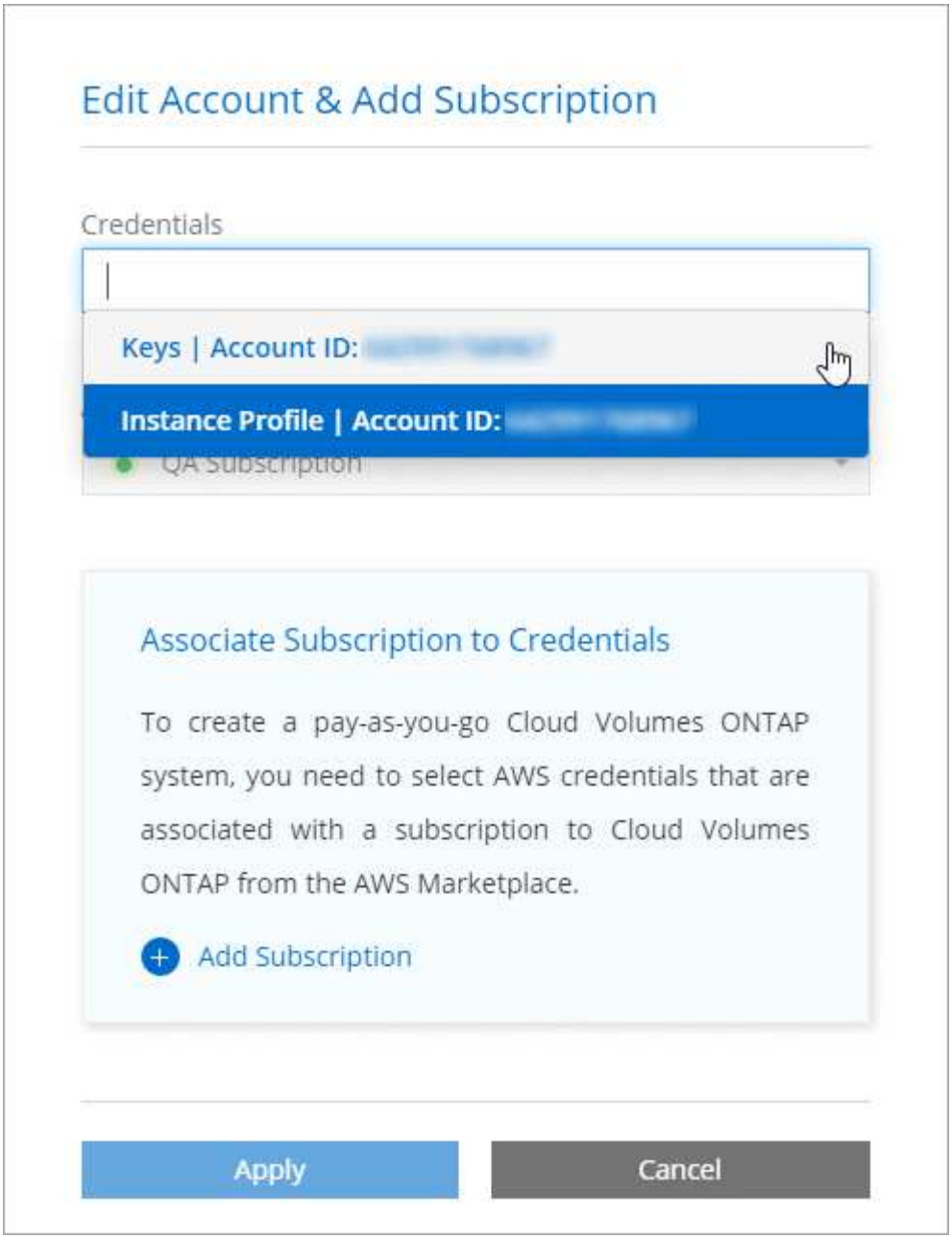
2. Fare clic su **Add Credentials** (Aggiungi credenziali) e selezionare **AWS**.
3. Fornire le chiavi AWS o l'ARN di un ruolo IAM attendibile.
4. Confermare che i requisiti della policy sono stati soddisfatti e fare clic su **continua**.
5. Scegli l'abbonamento pay-as-you-go che desideri associare alle 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 AWS devono essere associate a un abbonamento a Cloud Volumes ONTAP da AWS 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 AWS alle credenziali

Dopo aver aggiunto le credenziali AWS a Cloud Manager, è possibile associare un abbonamento AWS 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 AWS Marketplace dopo aver aggiunto le credenziali a Cloud Manager:

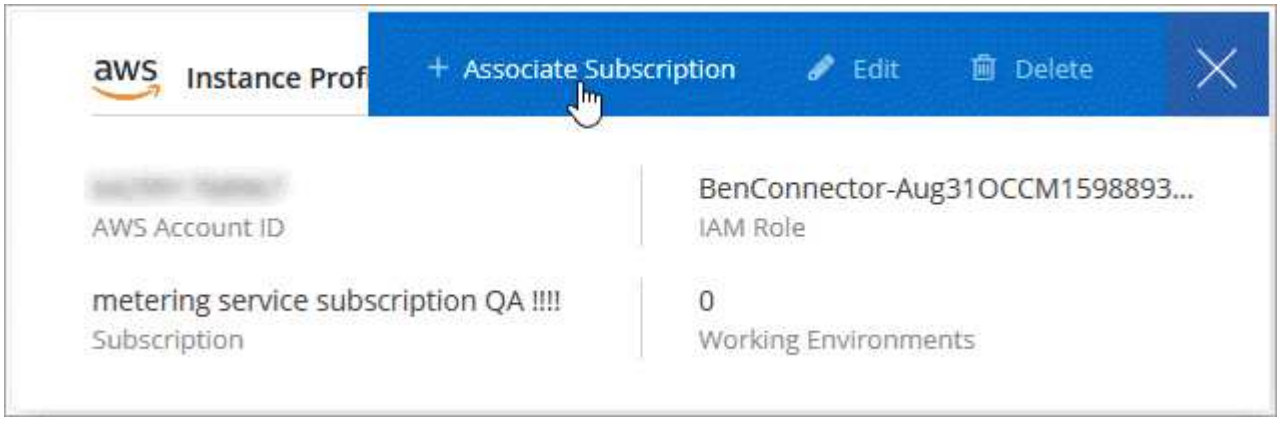
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento AWS Marketplace esistente con un nuovo abbonamento.

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.

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

Azure

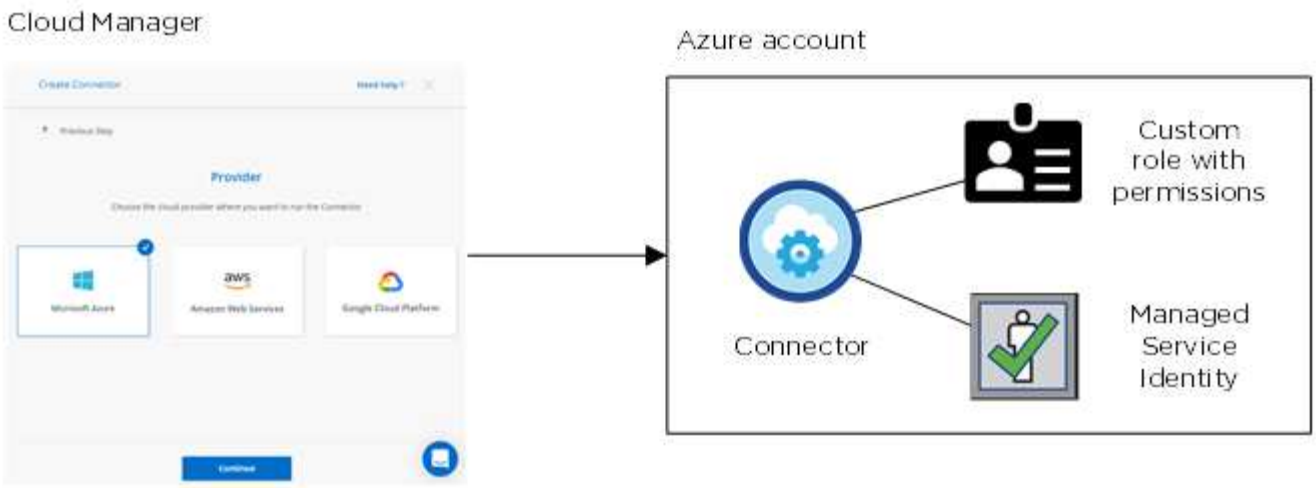
Credenziali e permessi di Azure

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.

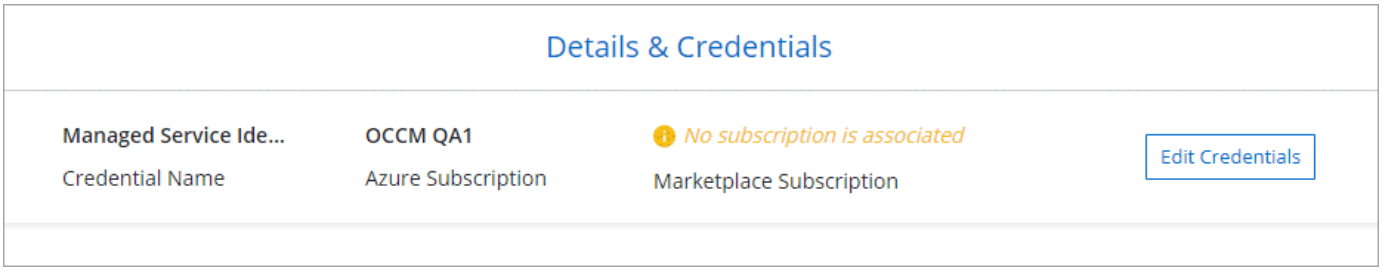
Credenziali iniziali di Azure

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:

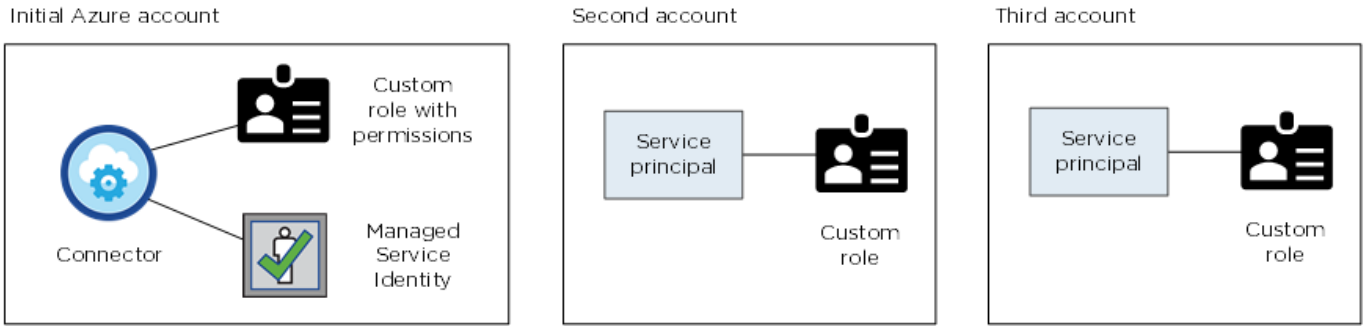


Abbonamenti Azure aggiuntivi per un'identità gestita

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".

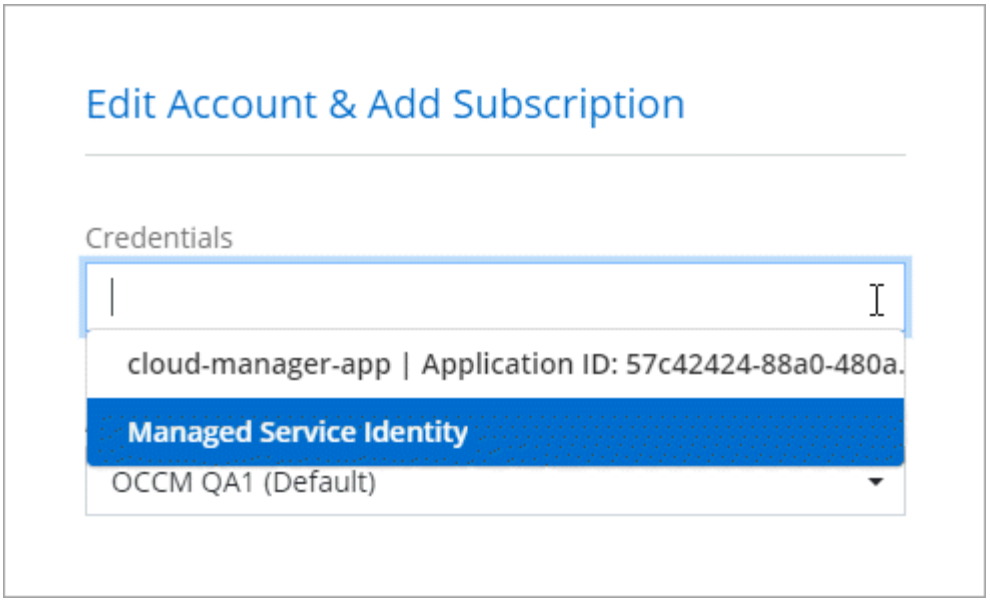
Credenziali Azure aggiuntive

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.

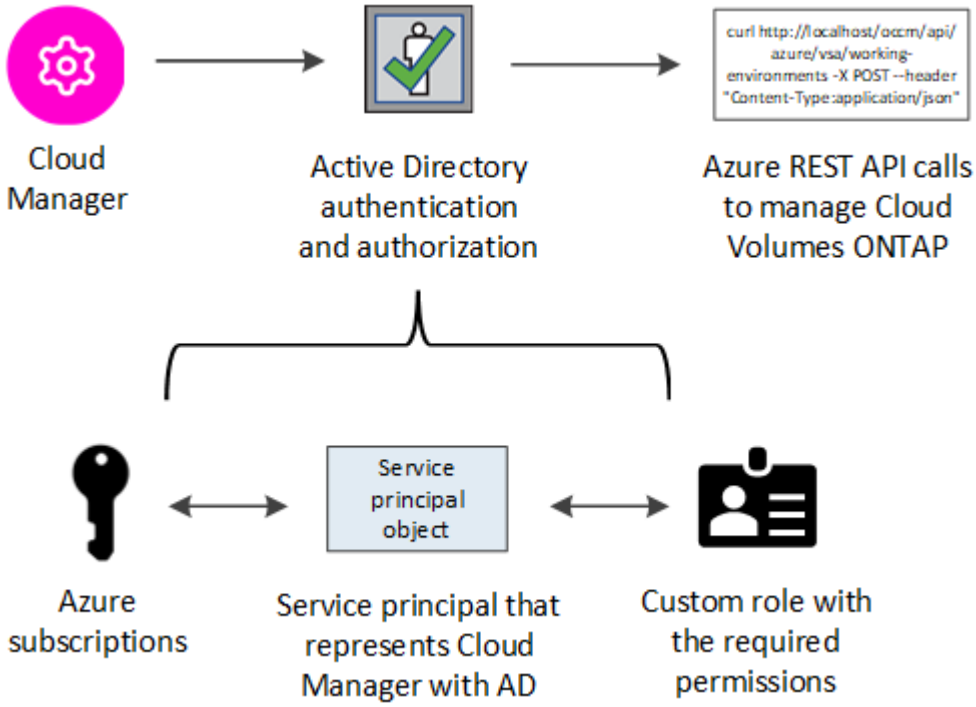
Quando si implementa un connettore da Cloud Manager, Cloud Manager aggiunge automaticamente l'account Azure in cui è stato implementato il connettore. Se il software Connector è stato installato manualmente su un sistema esistente, non viene aggiunto un account iniziale. "Scopri gli account e le autorizzazioni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

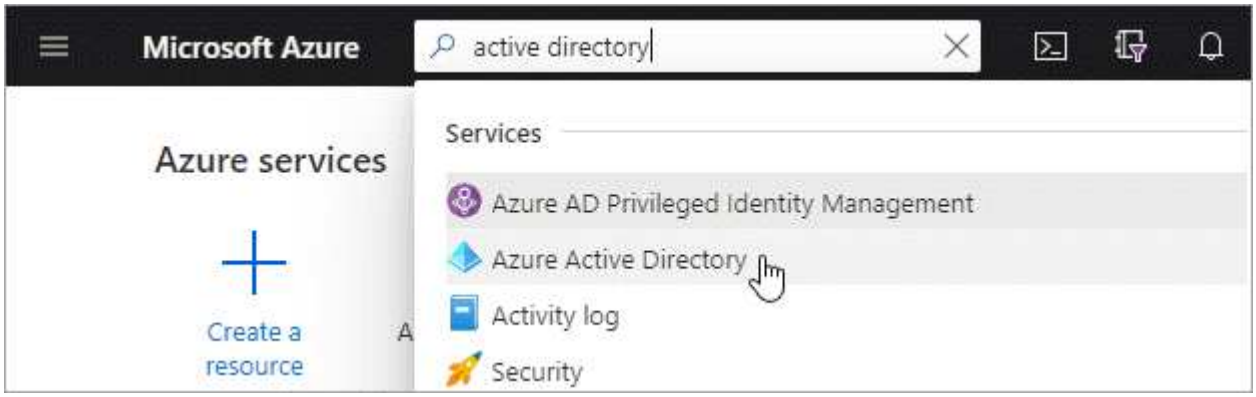
Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per il controllo degli accessi in base al ruolo.

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**.

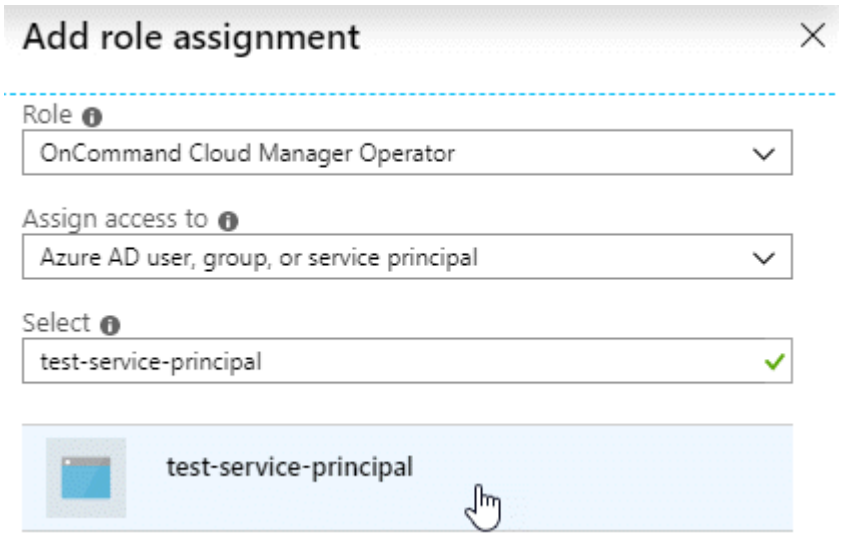
   b. Selezionare l'abbonamento.

   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.

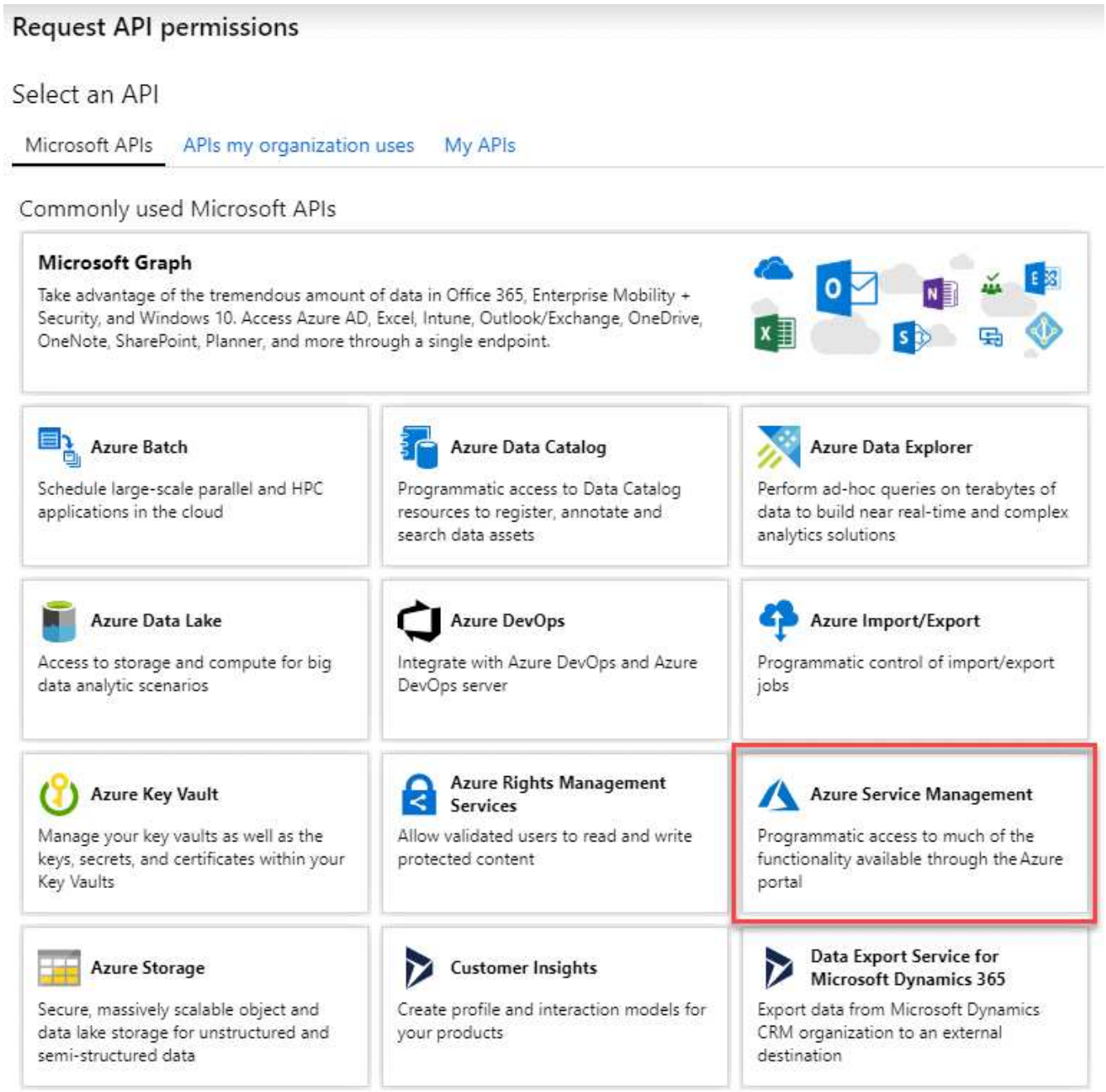
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Cloud Manager consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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

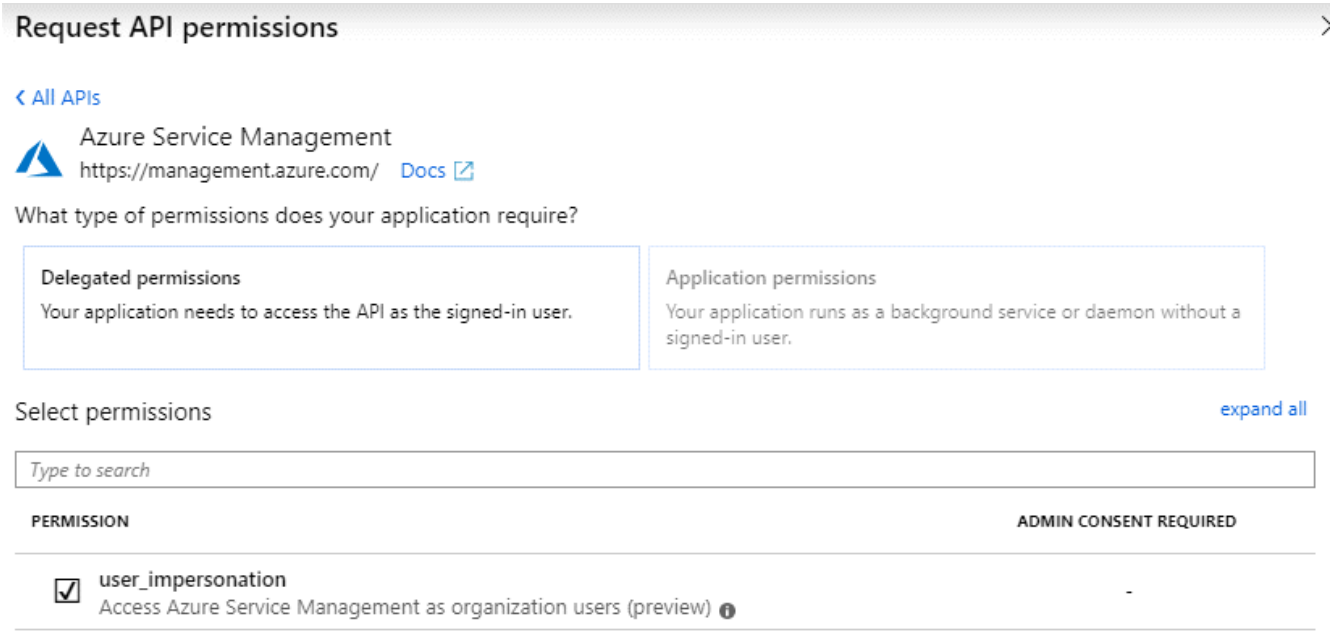
L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

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**.



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** (

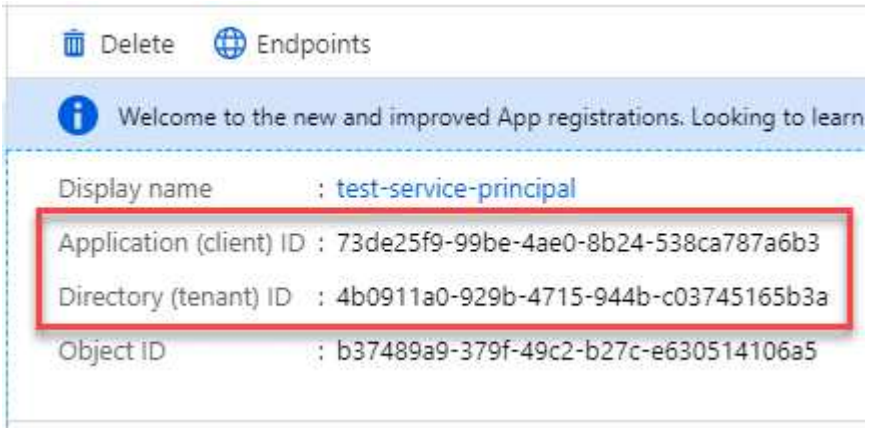


Ottenere l'ID dell'applicazione e l'ID della directory

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**.



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.

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

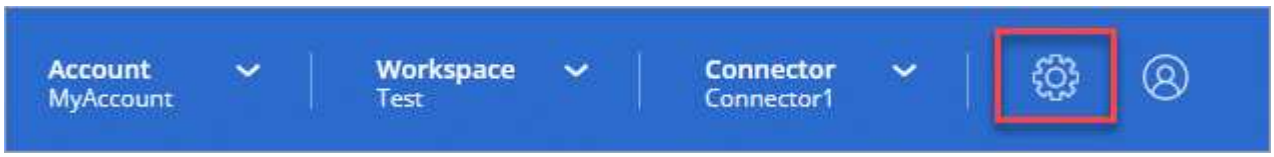
Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

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**.



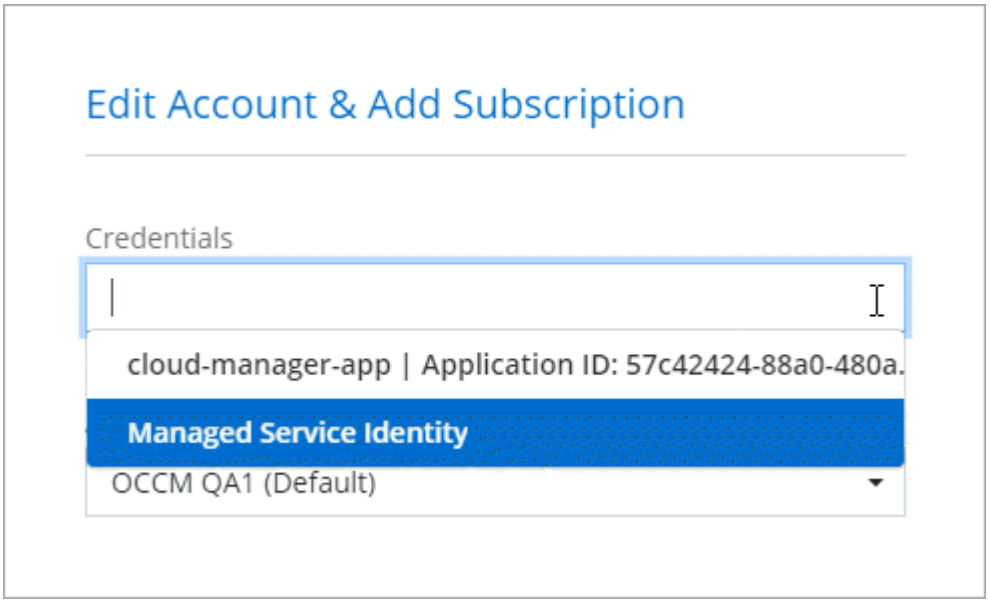
2. Fare clic su **Aggiungi credenziali** e selezionare **Microsoft Azure**.
3. Immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
   - ID applicazione (client): Vedere Ottenere l'ID dell'applicazione e l'ID della directory.
   - ID directory (tenant): Vedere Ottenere 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:

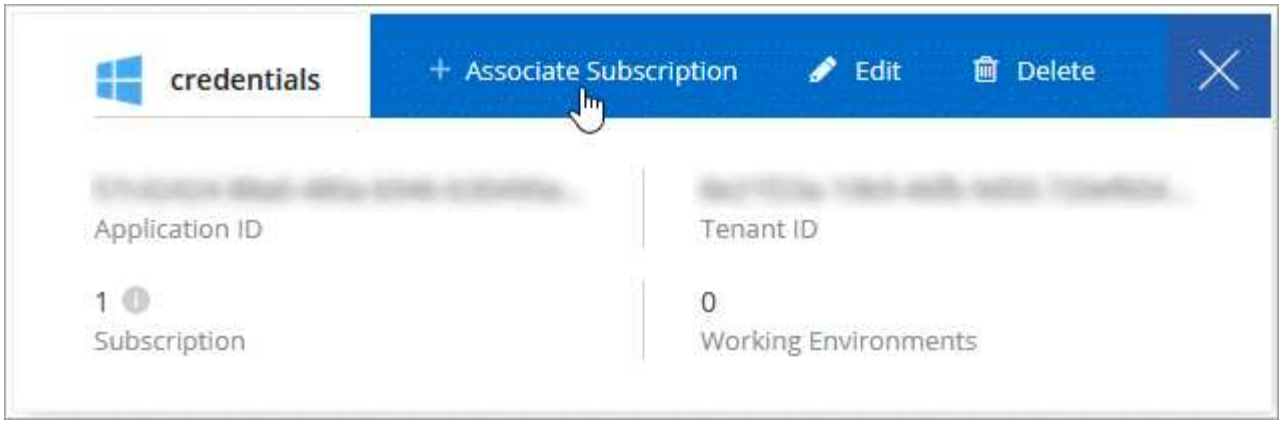
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento a Azure Marketplace esistente con un nuovo abbonamento.

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

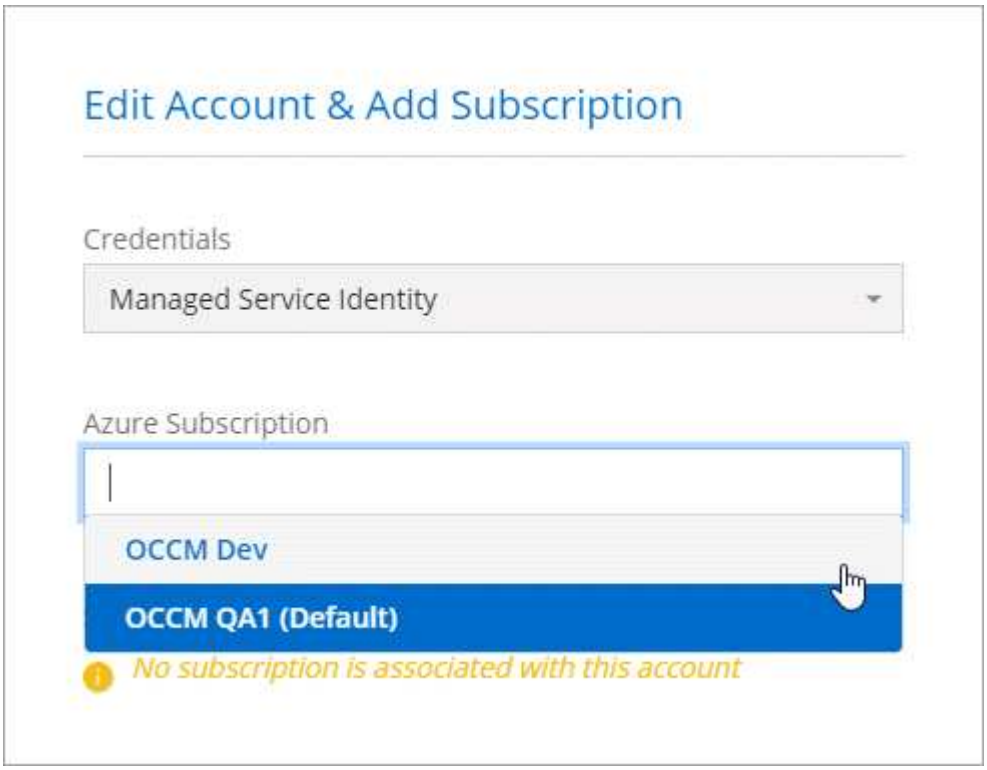
1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare Cloud Volumes ONTAP.
3. Fare clic su **controllo di accesso (IAM)**.
   a. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
     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



GCP

Progetti, autorizzazioni e account Google Cloud

Un account di servizio fornisce a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP nello stesso progetto di Cloud Manager o in progetti diversi.

Progetto e permessi per Cloud Manager

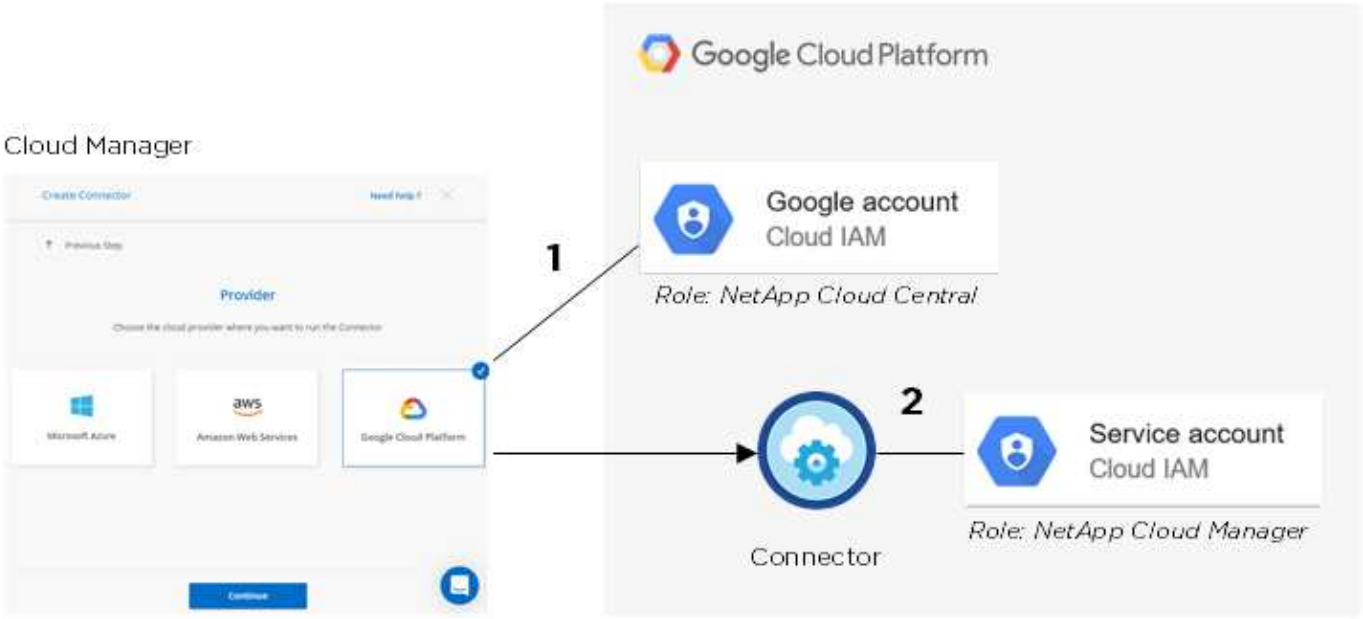
Prima di poter implementare Cloud Volumes ONTAP in Google Cloud, devi prima implementare un connettore in un progetto Google Cloud. Il connettore non può essere in esecuzione in sede o in un altro cloud provider.

Prima di implementare un connettore direttamente da Cloud Manager, è necessario disporre di due set di autorizzazioni:

1. È necessario implementare un connettore utilizzando un account Google che disponga delle autorizzazioni per avviare l'istanza di Connector VM da Cloud Manager.
2. Quando si implementa il connettore, viene richiesto di selezionare un "account di servizio" Per l'istanza della macchina virtuale. Cloud Manager ottiene le autorizzazioni dall'account del servizio per creare e gestire i sistemi Cloud Volumes ONTAP per conto dell'utente. Le autorizzazioni vengono fornite allegando un ruolo personalizzato all'account del servizio.

Abbiamo impostato due file YAML che includono le autorizzazioni richieste per l'utente e l'account del servizio. "Scopri come utilizzare i file YAML per impostare le autorizzazioni".

La seguente immagine mostra i requisiti di autorizzazione descritti nei numeri 1 e 2 precedenti:



Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto del connettore o in un progetto diverso. Per implementare Cloud Volumes ONTAP in un progetto diverso, è necessario prima aggiungere l'account e il ruolo del servizio Connector a tale progetto.

- "Informazioni su come configurare l'account di servizio (vedere il passaggio 2)".
- "Scopri come implementare Cloud Volumes ONTAP in GCP e selezionare un progetto".

Account per il tiering dei dati

Cloud Manager richiede un account GCP per Cloud Volumes ONTAP 9.6, ma non per la versione 9.7 e successive. Se si desidera utilizzare il tiering dei dati con Cloud Volumes ONTAP 9.7, seguire il passaggio 4 in "Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google".

Per abilitare il tiering dei dati su un sistema Cloud Volumes ONTAP 9.6, è necessario aggiungere un account Google Cloud a Cloud Manager. Il tiering dei dati esegue automaticamente il tiering dei dati cold in uno storage a oggetti a basso costo, consentendoti di recuperare spazio sullo storage primario e ridurre lo storage secondario.

Quando si aggiunge l'account, è necessario fornire a Cloud Manager una chiave di accesso allo storage per un account di servizio che dispone delle autorizzazioni Storage Admin. Cloud Manager utilizza le chiavi di accesso per configurare e gestire un bucket di cloud storage per il tiering dei dati.

Dopo aver aggiunto un account Google Cloud, è possibile attivare il tiering dei dati sui singoli volumi quando vengono creati, modificati o replicati.

- "Scopri come configurare e aggiungere account GCP a Cloud Manager".
- "Scopri come eseguire il tiering dei dati inattivi verso uno storage a oggetti a basso costo".

Gestione delle credenziali GCP e delle sottoscrizioni per Cloud Manager

È possibile gestire due tipi di credenziali di Google Cloud Platform da Cloud Manager: Le

credenziali associate all'istanza di Connector VM e le chiavi di accesso allo storage utilizzate con un sistema Cloud Volumes ONTAP 9.6 per "tiering dei dati".

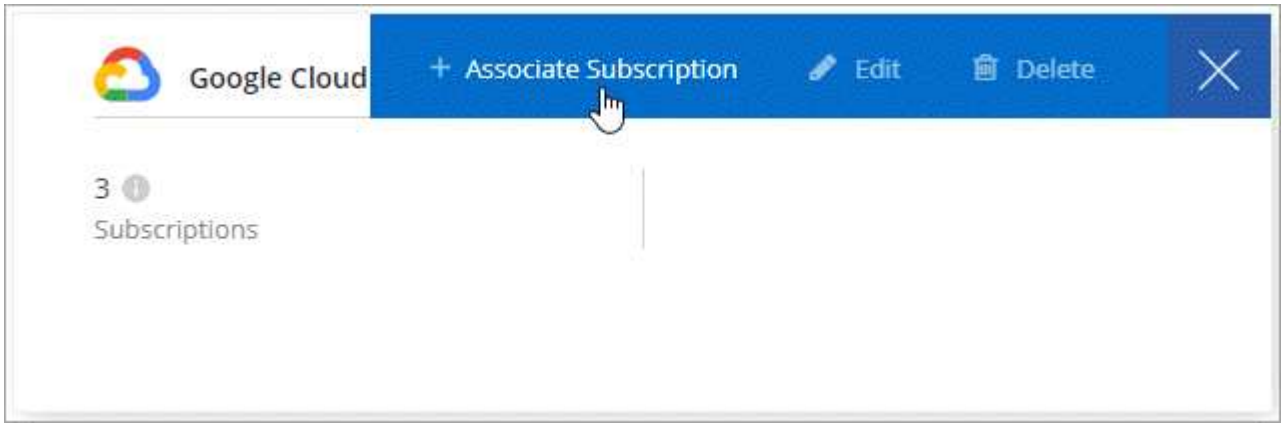
Associazione di un abbonamento a Marketplace con le credenziali GCP

Quando si implementa un connettore in GCP, Cloud Manager crea un set predefinito di credenziali associate all'istanza della macchina virtuale del connettore. Queste sono le credenziali utilizzate da Cloud Manager per implementare Cloud Volumes ONTAP.

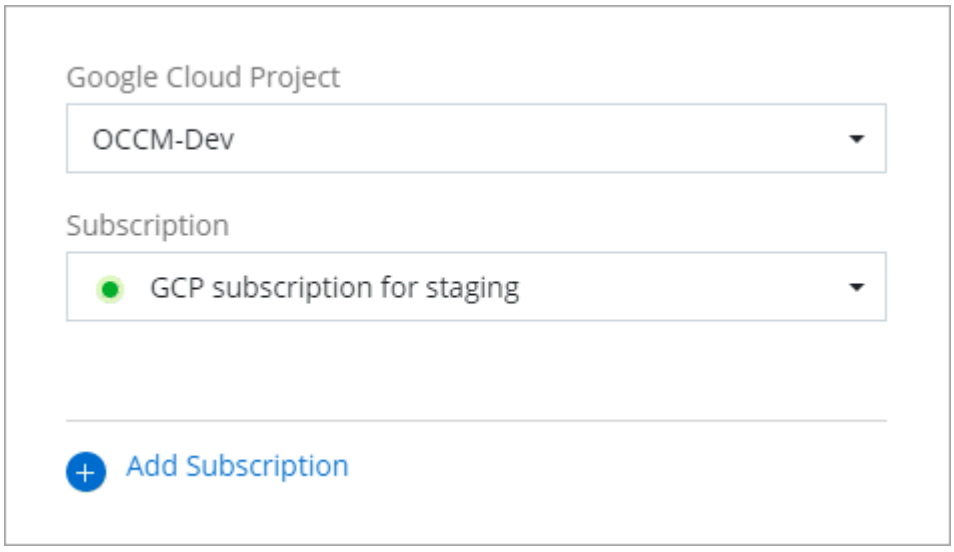
In qualsiasi momento, è possibile modificare l'abbonamento Marketplace associato a queste credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

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. Seleziona un progetto Google Cloud e un abbonamento dall'elenco a discesa oppure fai clic su **Aggiungi abbonamento** e segui la procedura per creare un nuovo abbonamento.



5. Fare clic su **Associa**.

Impostazione e aggiunta di account GCP per il tiering dei dati con Cloud Volumes ONTAP 9.6

Se si desidera attivare un sistema Cloud Volumes ONTAP 9.6 per "tiering dei dati", È necessario fornire a Cloud Manager una chiave di accesso allo storage per un account di servizio che dispone delle autorizzazioni Storage Admin. Cloud Manager utilizza le chiavi di accesso per configurare e gestire un bucket di cloud storage per il tiering dei dati.

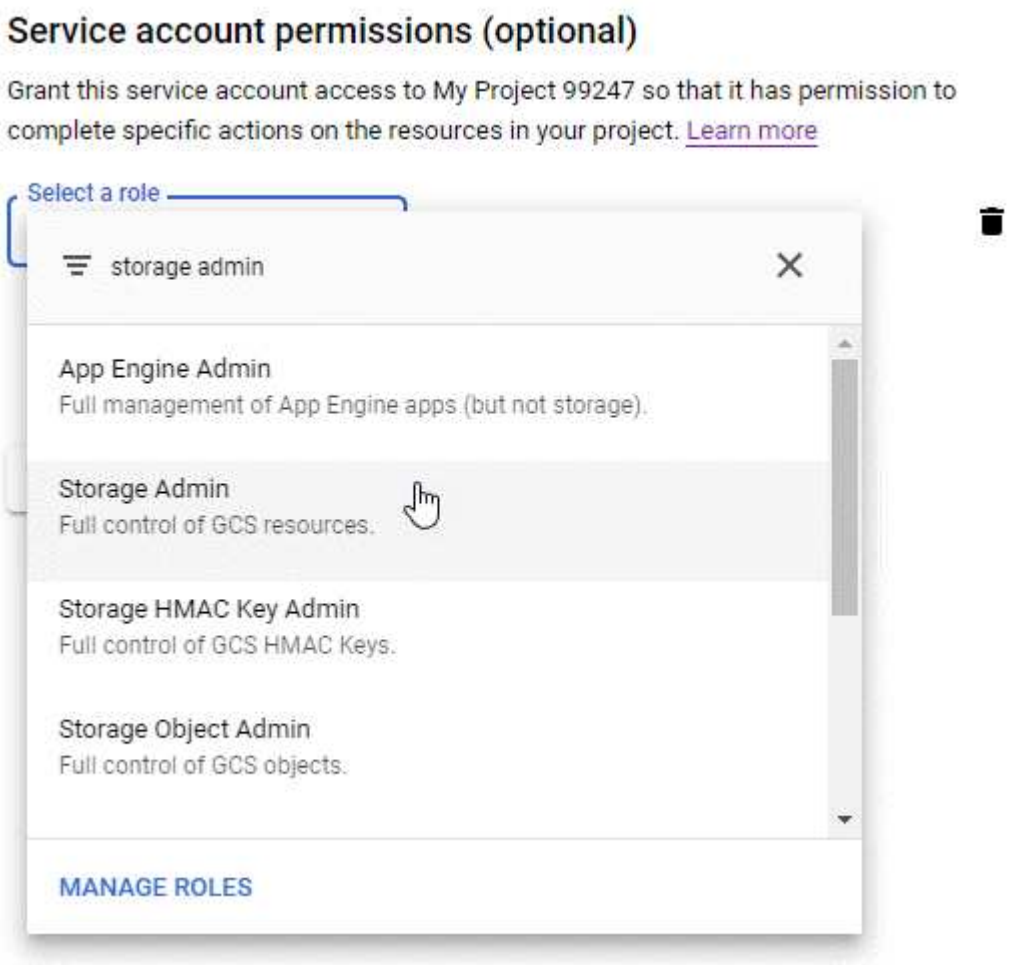
Se si desidera utilizzare il tiering dei dati con Cloud Volumes ONTAP 9.7, seguire il passaggio 4 in "Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google".

Impostazione di un account di servizio e di chiavi di accesso per Google Cloud Storage

Un account di servizio consente a Cloud Manager di autenticare e accedere ai bucket Cloud Storage utilizzati per il tiering dei dati. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

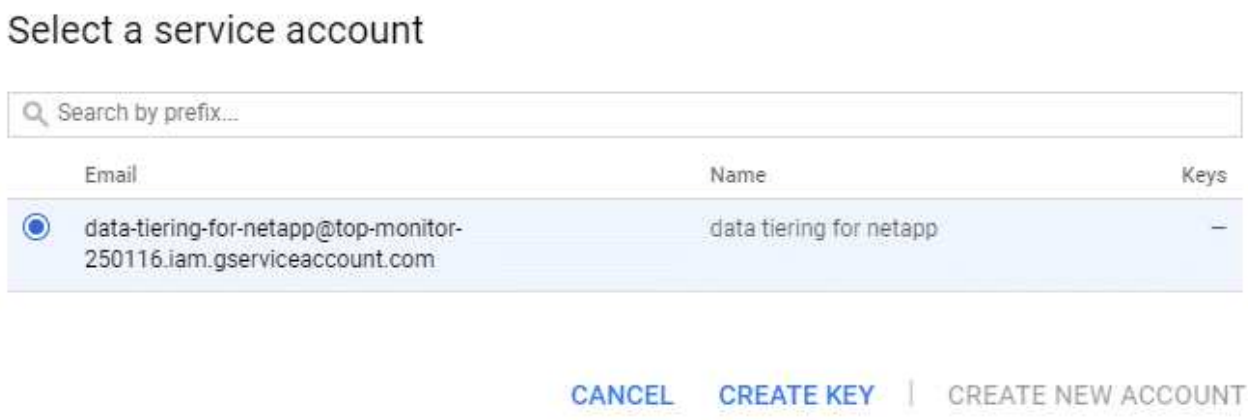
Fasi

1. Aprire la console IAM GCP e. "Creare un account di servizio con il ruolo di amministratore dello storage".



2. Passare a. "Impostazioni storage GCP".
3. Se richiesto, selezionare un progetto.
4. Fare clic sulla scheda **interoperabilità**.
5. Se non è già stato fatto, fare clic su **Enable Interoperability access** (attiva accesso all'interoperabilità).

6. In **chiavi di accesso per gli account di servizio**, fare clic su **Crea una chiave per un account di servizio**.
7. Selezionare l'account di servizio creato al punto 1.



8. Fare clic su **Create Key** (Crea chiave).
9. Copiare la chiave di accesso e il segreto.

   Devi inserire queste informazioni in Cloud Manager quando Aggiungi l'account GCP per il tiering dei dati.

Aggiunta di un account GCP a Cloud Manager

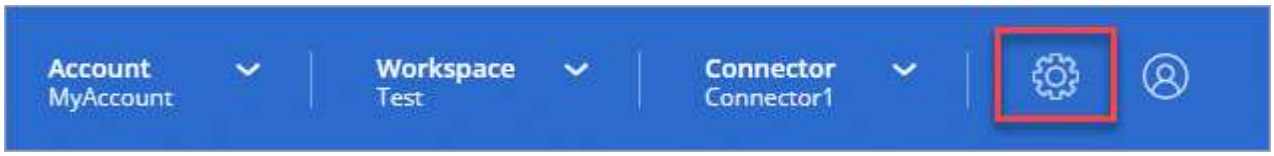
Ora che si dispone di una chiave di accesso per un account di servizio, è possibile aggiungerla a Cloud Manager.

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 **Google Cloud**.
3. Inserire la chiave di accesso e il segreto per l'account del servizio.

   Le chiavi consentono a Cloud Manager di configurare un bucket di cloud storage per il tiering dei dati.

4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

Quali sono le prossime novità?

È ora possibile attivare il tiering dei dati su singoli volumi su un sistema Cloud Volumes ONTAP 9.6 quando vengono creati, modificati o replicati. Per ulteriori informazioni, vedere "Tiering dei dati inattivi su storage a

oggetti a basso costo".

Prima di procedere, assicurarsi che la subnet in cui risiede Cloud Volumes ONTAP sia configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access".

Aggiunta di account NetApp Support Site a Cloud Manager

Per implementare un sistema BYOL, è necessario aggiungere il tuo account NetApp Support Site a Cloud Manager. È inoltre necessario registrare i sistemi pay-as-you-go e aggiornare il software ONTAP.

Guarda il video seguente per scoprire come aggiungere gli account NetApp Support Site a Cloud Manager. In alternativa, scorrere verso il basso per leggere i passaggi.

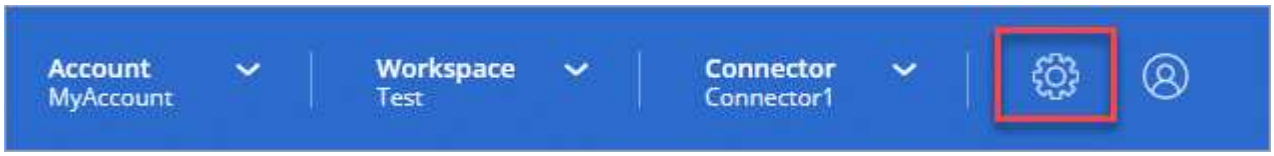
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

1. Se non disponi ancora di un account NetApp Support Site, "registratevi per uno".
2. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



3. Fare clic su **Aggiungi credenziali** e selezionare **NetApp Support Site**.
4. Specificare un nome per l'account, quindi immettere il nome utente e la password.
   - L'account deve essere un account a livello di cliente (non un account guest o temporaneo).
   - Se si prevede di implementare sistemi BYOL:
     - L'account deve essere autorizzato ad accedere ai numeri di serie dei sistemi BYOL.
     - Se hai acquistato un abbonamento BYOL sicuro, è necessario un account NSS sicuro.
5. Fare clic su **Crea account.**

Quali sono le prossime novità?

Gli utenti possono ora selezionare l'account durante la creazione di nuovi sistemi Cloud Volumes ONTAP e la registrazione di sistemi esistenti.

- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"
- "Registrazione di sistemi pay-as-you-go"
- "Scopri come Cloud Manager gestisce i file di licenza"

Gestione di utenti, aree di lavoro, connettori e sottoscrizioni

"Dopo aver eseguito la configurazione iniziale", Potrebbe essere necessario amministrare le impostazioni dell'account in un secondo momento gestendo utenti, aree di lavoro, connettori e sottoscrizioni.

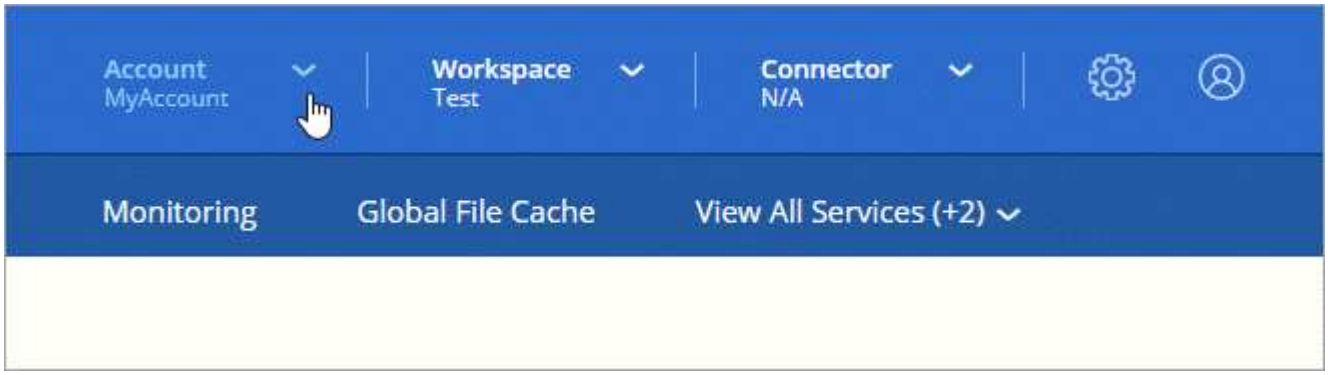
"Scopri di più sul funzionamento degli account Cloud Central".

Aggiunta di utenti

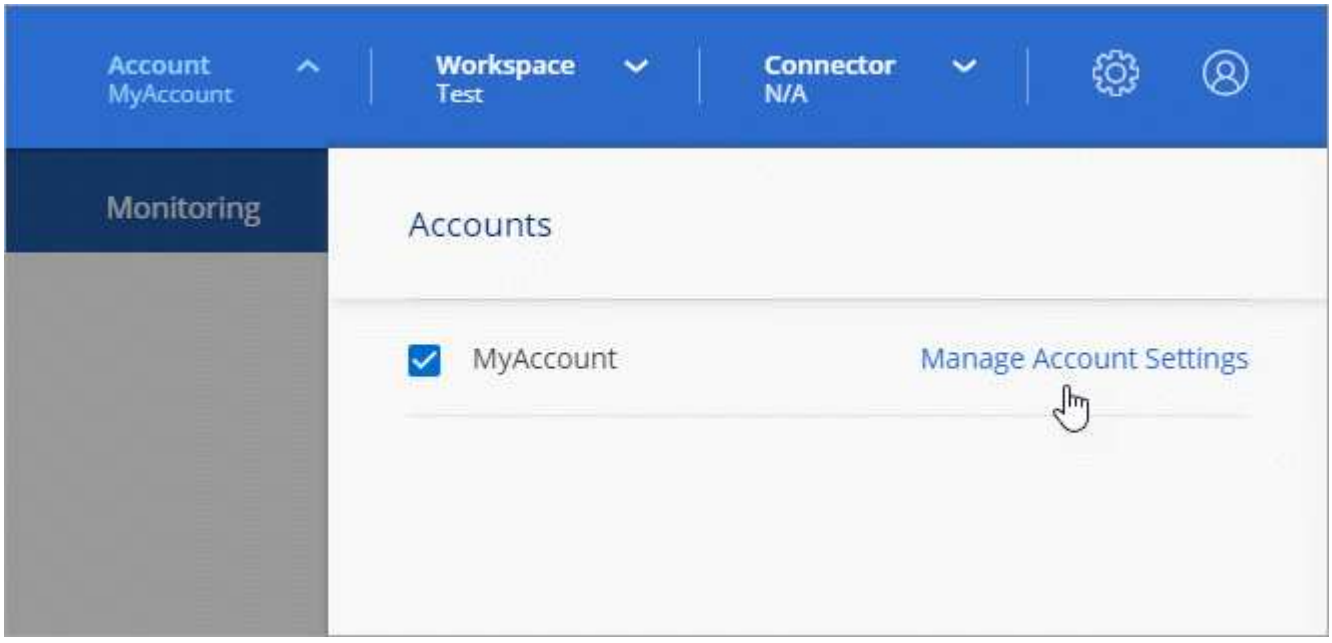
Associa gli utenti di Cloud Central all'account Cloud Central in modo che questi utenti possano creare e gestire ambienti di lavoro in Cloud Manager.

Fasi

1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "NetApp Cloud Central" e iscriverti.
2. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account**.



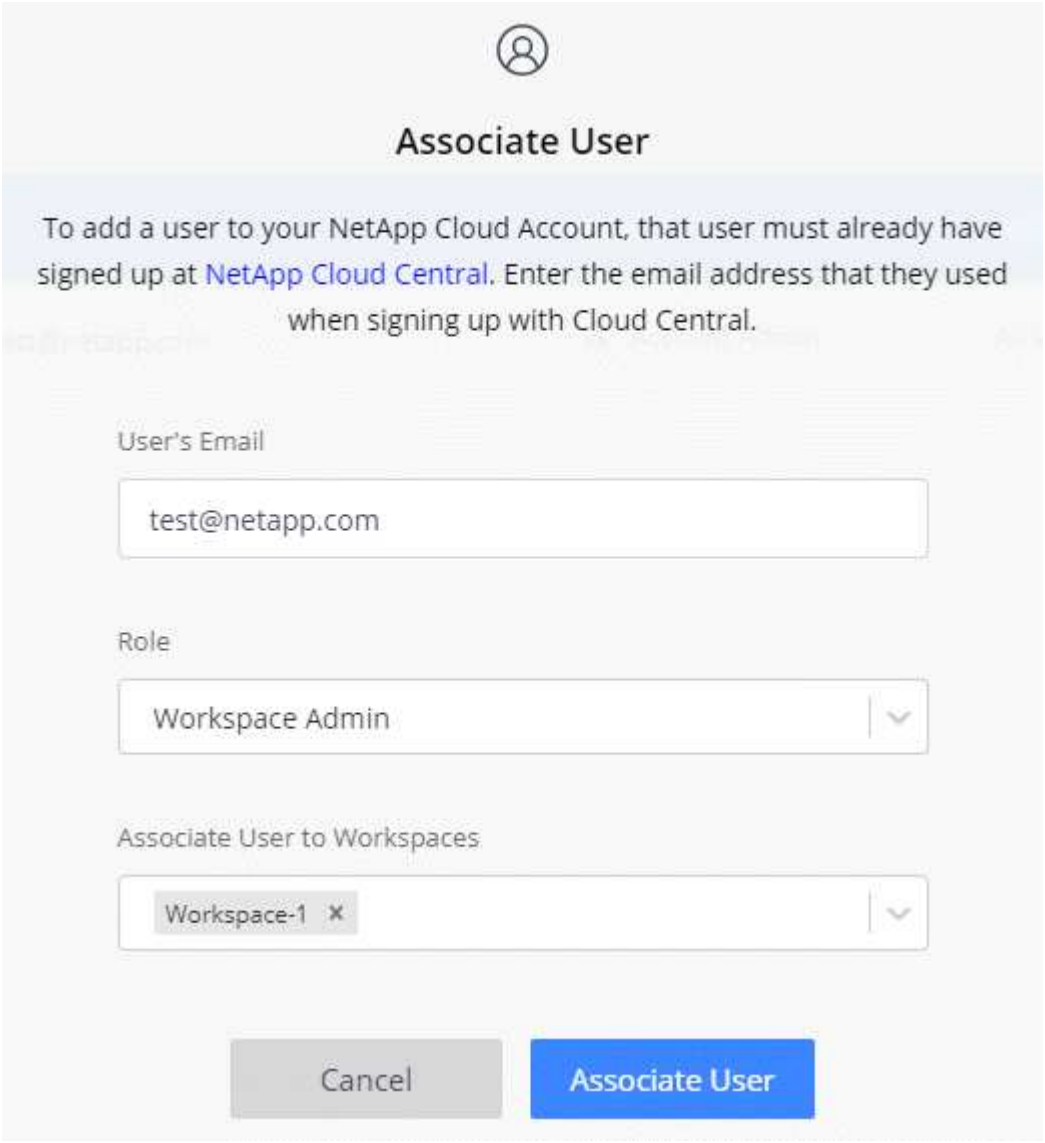
3. Fare clic su **Manage account** (Gestisci account) accanto all'account attualmente selezionato.



4. Dalla scheda Users (utenti), fare clic su **associate User** (Associa utente).
5. Inserire l'indirizzo e-mail dell'utente e selezionare un ruolo per l'utente:

- **Account Admin**: Può eseguire qualsiasi azione in Cloud Manager.
- **Workspace Admin**: Consente di creare e gestire le risorse nelle aree di lavoro assegnate.
- **Compliance Viewer**: È in grado di visualizzare solo le informazioni di conformità e generare report per le aree di lavoro a cui sono autorizzati ad accedere.

6. Se si seleziona Workspace Admin (Amministratore area di lavoro) o Compliance Viewer (Visualizzatore conformità), selezionare una o più aree di lavoro da associare all'utente.



7. Fare clic su **Associa utente**.

Risultato

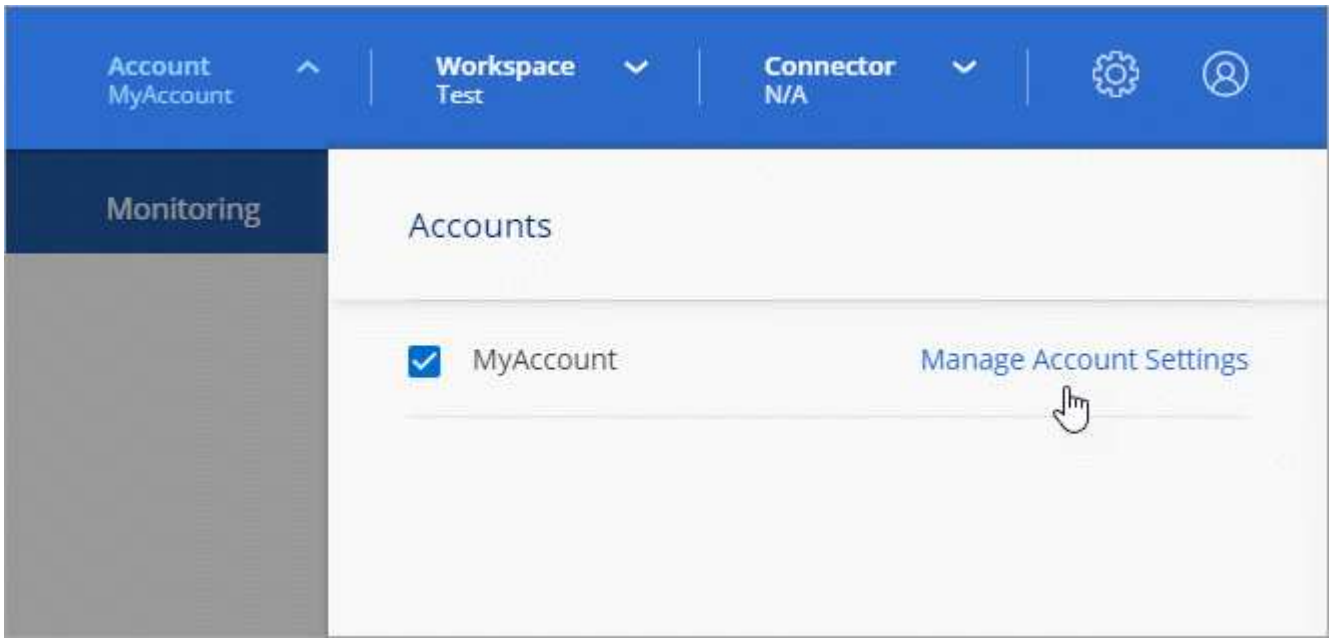
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

Rimozione degli utenti

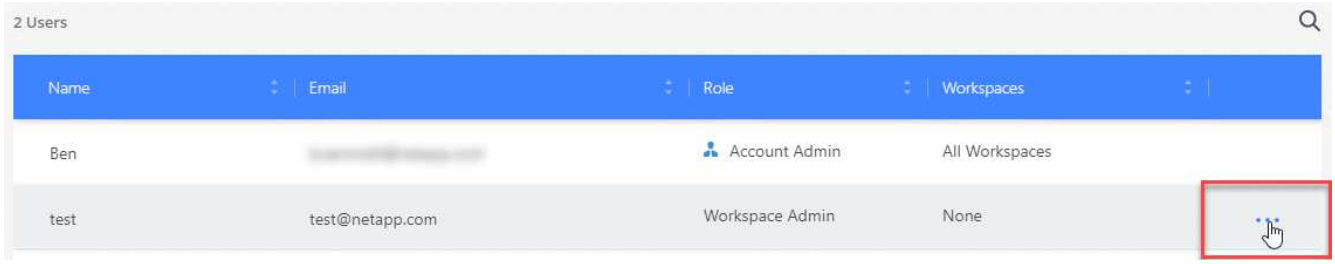
La disassociazione di un utente lo rende in modo che non possa più accedere alle risorse in un account Cloud Central.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Dalla scheda Users (utenti), fare clic sul menu delle azioni nella riga corrispondente all'utente.



3. Fare clic su **dissocia utente** e fare clic su **dissocia** per confermare.

Risultato

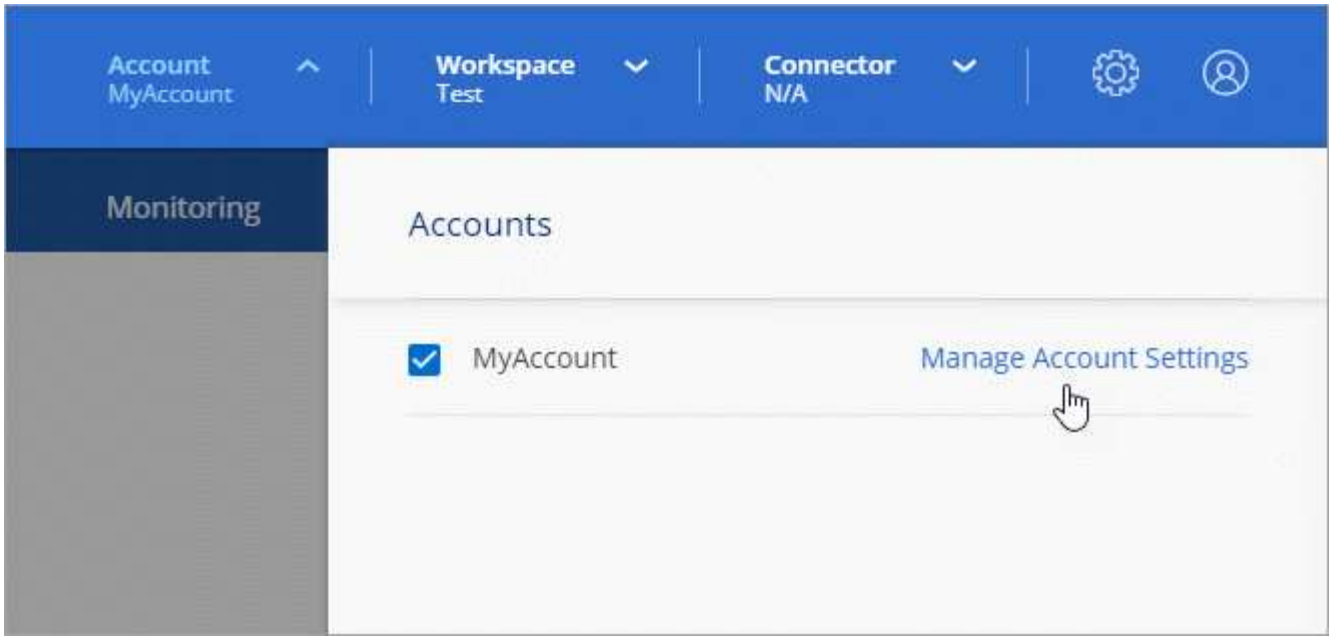
L'utente non può più accedere alle risorse di questo account Cloud Central.

Gestione delle aree di lavoro di un amministratore dell'area di lavoro

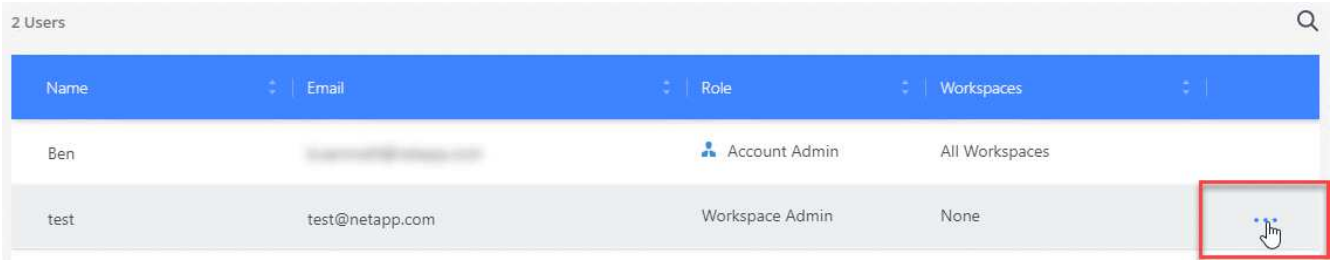
È possibile associare e disassociare gli amministratori Workspace alle aree di lavoro in qualsiasi momento. L'associazione dell'utente consente di creare e visualizzare gli ambienti di lavoro in tale area di lavoro.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Dalla scheda Users (utenti), fare clic sul menu delle azioni nella riga corrispondente all'utente.



3. Fare clic su **Gestisci aree di lavoro**.
4. Selezionare le aree di lavoro da associare all'utente e fare clic su **Apply** (Applica).

Risultato

L'utente può ora accedere a tali aree di lavoro da Cloud Manager, purché il connettore sia stato associato anche alle aree di lavoro.

Gestione delle aree di lavoro

Gestisci le tue aree di lavoro creando, rinominando ed eliminando le aree di lavoro. Nota: Non è possibile eliminare un'area di lavoro se contiene risorse. Deve essere vuoto.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Workspaces**.
3. Scegliere una delle seguenti opzioni:
   - Fare clic su **Add New Workspace** (Aggiungi nuova area di lavoro) per creare una nuova area di lavoro.
   - Fare clic su **Rename** (Rinomina) per rinominare l'area di lavoro.
   - Fare clic su **Delete** (Elimina) per eliminare l'area di lavoro.

Gestione delle aree di lavoro di un connettore

È necessario associare il connettore alle aree di lavoro in modo che gli amministratori di Workspace possano accedere a tali aree di lavoro da Cloud Manager.

Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita.

"Scopri di più su utenti, aree di lavoro e connettori".

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Connector** (connettore).
3. Fare clic su **Manage Workspaces** (Gestisci aree di lavoro) per il connettore che si desidera associare.
4. Selezionare le aree di lavoro da associare al connettore e fare clic su **Apply** (Applica).

Gestione delle sottoscrizioni

Dopo aver effettuato l'iscrizione dal marketplace di un provider cloud, ogni abbonamento è disponibile dal widget Impostazioni account. È possibile rinominare un abbonamento e disassociarlo da uno o più account.

Ad esempio, supponiamo di avere due account e di fatturarvi ciascuno tramite abbonamenti separati. Potresti disassociare un abbonamento da uno degli account, in modo che gli utenti di quell'account non scelgano accidentalmente l'abbonamento sbagliato quando crei un ambiente di lavoro Cloud Volume ONTAP.

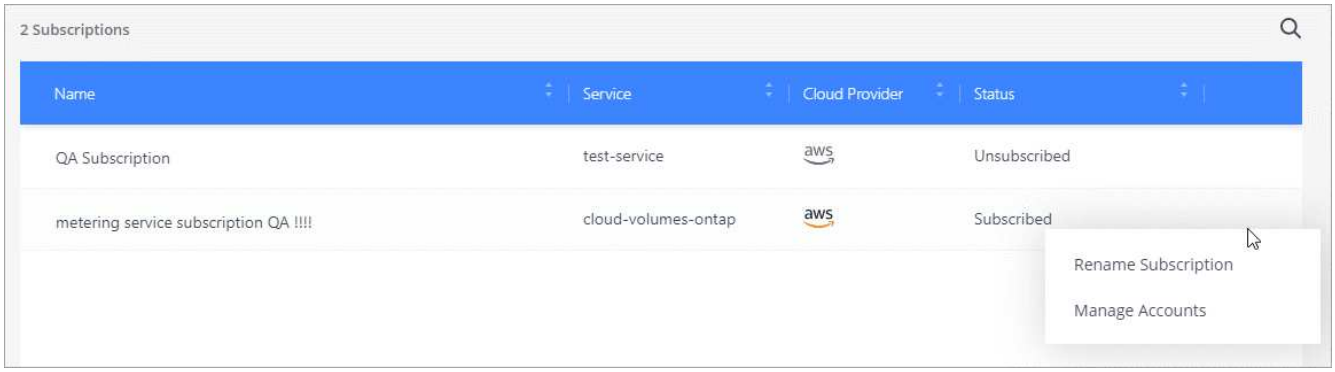
"Scopri di più sugli abbonamenti".

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Abbonamenti**.

   Verranno visualizzati solo gli abbonamenti associati all'account attualmente visualizzato.

3. Fare clic sul menu delle azioni nella riga corrispondente all'abbonamento che si desidera gestire.



4. Scegliere di rinominare l'abbonamento o di gestire gli account associati all'abbonamento.

Modifica del nome dell'account

Modificare il nome dell'account in qualsiasi momento per modificarlo in un elemento significativo per l'utente.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Nella scheda **Panoramica**, fare clic sull'icona di modifica accanto al nome dell'account.
3. Digitare un nuovo nome account e fare clic su **Salva**.

Attivazione o disattivazione della piattaforma SaaS

Si consiglia di non disattivare la piattaforma SaaS a meno che non sia necessario per rispettare le policy di sicurezza della propria azienda. La disattivazione della piattaforma SaaS limita la tua capacità di utilizzare i servizi cloud integrati di NetApp.

I seguenti servizi non sono disponibili da Cloud Manager se si disattiva la piattaforma SaaS:

- Conformità al cloud
- Kubernetes
- Tiering nel cloud
- Global file cache
- Monitoraggio (Cloud Insights)

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Nella scheda **Panoramica**, attivare l'opzione Usa la piattaforma SaaS.

Gestione di un certificato HTTPS per un accesso sicuro

Per impostazione predefinita, Cloud Manager utilizza un certificato autofirmato per l'accesso HTTPS alla console Web. È possibile installare un certificato firmato da un'autorità di certificazione (CA), che offre una protezione migliore rispetto a un certificato autofirmato.

Prima di iniziare

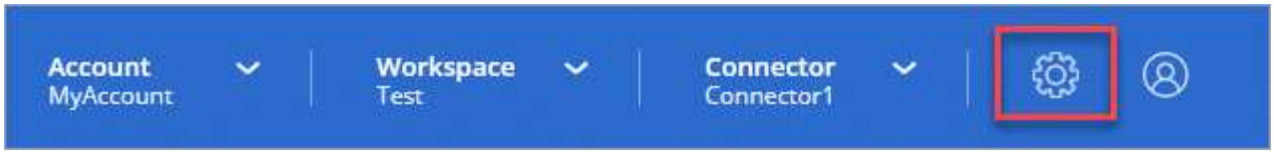
È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Installazione di un certificato HTTPS

Installare un certificato firmato da una CA per un accesso sicuro.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Settings (Impostazioni) e selezionare **HTTPS Setup** (Configurazione HTTPS).

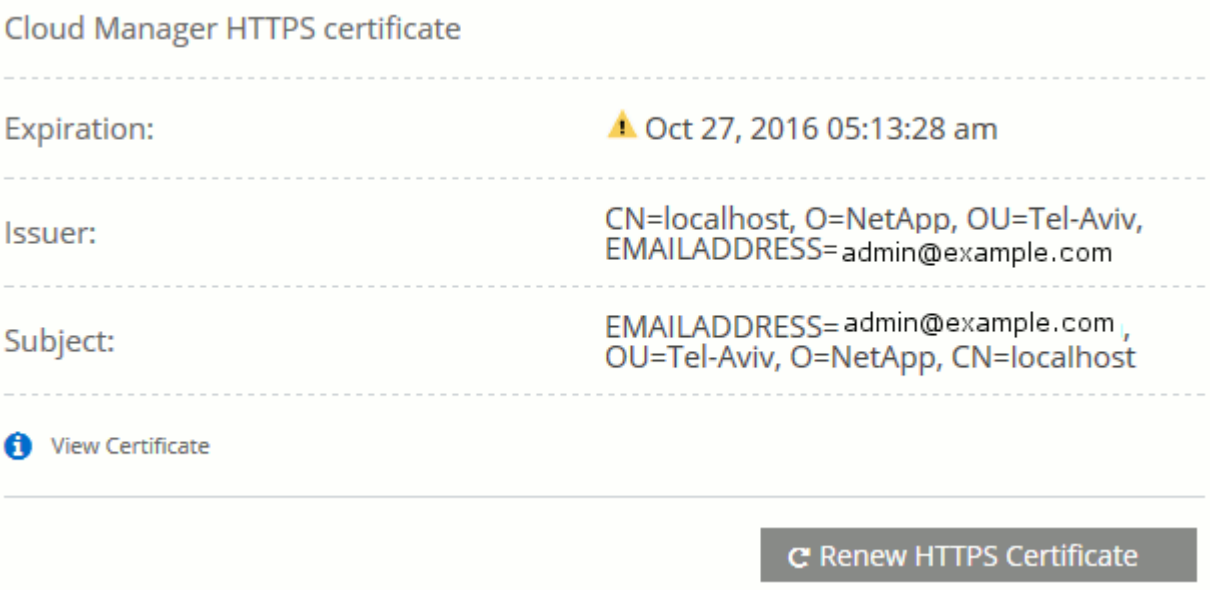


2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio certificato firmato dalla CA:

Opzione	Descrizione
Generare una CSR	a. Immettere il nome host o il DNS dell'host del connettore (il nome comune), quindi fare clic su **generate CSR** (genera CSR). Cloud Manager visualizza una richiesta di firma del certificato. b. Utilizzare la CSR per inviare una richiesta di certificato SSL a una CA. Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64. c. Copiare il contenuto del certificato firmato, incollarlo nel campo certificato, quindi fare clic su **Installa**.
Installare il proprio certificato firmato dalla CA	a. Selezionare **Installa certificato firmato dalla CA**. b. Caricare il file del certificato e la chiave privata, quindi fare clic su **Installa**. Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.

Risultato

Cloud Manager utilizza ora il certificato firmato dalla CA per fornire un accesso HTTPS sicuro. L'immagine seguente mostra un sistema Cloud Manager configurato per l'accesso sicuro:



Rinnovo del certificato HTTPS di Cloud Manager

È necessario rinnovare il certificato HTTPS di Cloud Manager prima della scadenza per garantire un accesso sicuro alla console Web di Cloud Manager. Se il certificato non viene rinnovato prima della scadenza, viene visualizzato un avviso quando gli utenti accedono alla console Web utilizzando HTTPS.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Settings (Impostazioni) e selezionare **HTTPS Setup** (Configurazione HTTPS).

   Vengono visualizzati i dettagli del certificato Cloud Manager, inclusa la data di scadenza.

2. Fare clic su **Renew HTTPS Certificate** (Rinnova certificato HTTPS) e seguire la procedura per generare una CSR o installare un certificato CA personalizzato.

Risultato

Cloud Manager utilizza il nuovo certificato firmato dalla CA per fornire un accesso HTTPS sicuro.

Rimozione degli ambienti di lavoro Cloud Volumes ONTAP

L'amministratore dell'account può rimuovere un ambiente di lavoro Cloud Volumes ONTAP per spostarlo in un altro sistema o per risolvere i problemi di rilevamento.

A proposito di questa attività

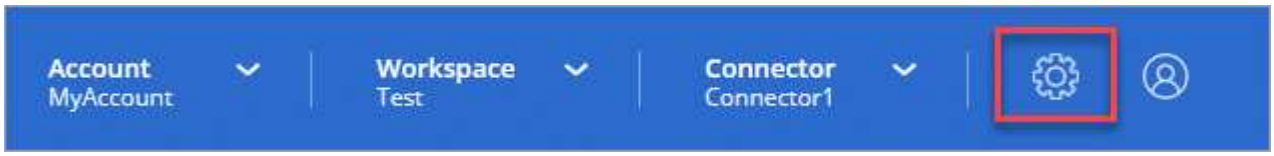
La rimozione di un ambiente di lavoro Cloud Volumes ONTAP lo rimuove da Cloud Manager. Non elimina il sistema Cloud Volumes ONTAP. In seguito, sarà possibile riscoprire l'ambiente di lavoro.

La rimozione di un ambiente di lavoro da Cloud Manager consente di effettuare le seguenti operazioni:

- Riscoprirla in un altro spazio di lavoro
- Riscoprilo da un altro sistema Cloud Manager
- Riscoprirla se si sono verificati problemi durante il rilevamento iniziale

Fasi

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



2. Dalla pagina Tools (Strumenti), fare clic su **Launch** (Avvia).
3. Selezionare l'ambiente di lavoro Cloud Volumes ONTAP che si desidera rimuovere.
4. Nella pagina Review and Approve (esamina e approva), fare clic su **Go** (Vai).

Risultato

Cloud Manager rimuove l'ambiente di lavoro. Gli utenti possono riscoprire questo ambiente di lavoro dalla pagina ambienti di lavoro in qualsiasi momento.

Configurazione di un connettore per l'utilizzo di un server proxy

Se le policy aziendali stabiliscono che si utilizza un server proxy per tutte le comunicazioni HTTP a Internet, è necessario configurare i connettori in modo che utilizzino tale server proxy. Il server proxy può trovarsi nel cloud o nella rete.

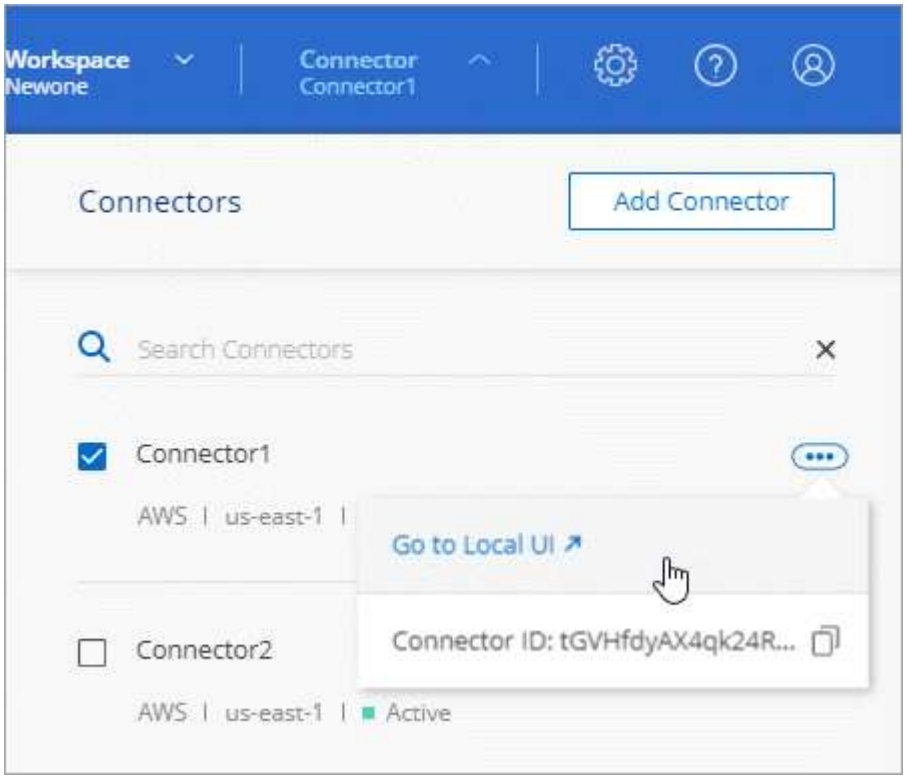
Quando si configura un connettore per l'utilizzo di un server proxy, il connettore e i sistemi Cloud Volumes ONTAP gestiti (inclusi i mediatori ha) utilizzano tutti il server proxy.

Fasi

1. "Accedere all'interfaccia SaaS di Cloud Manager" Da un computer che dispone di una connessione di rete all'istanza del connettore.

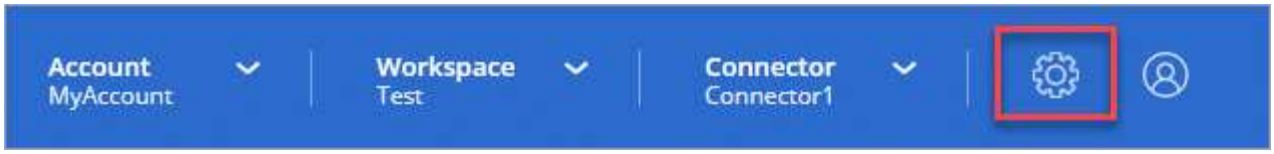
   Se il connettore non dispone di un indirizzo IP pubblico, è necessaria una connessione VPN oppure è necessario connettersi da un host di collegamento che si trova nella stessa rete del connettore.

2. Fare clic sull'elenco a discesa **Connector** (connettore), quindi fare clic su **Go to local UI** (Vai all'interfaccia utente locale) per un connettore specifico.



   L'interfaccia di Cloud Manager in esecuzione sul connettore viene caricata in una nuova scheda del browser.

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



4. In HTTP Proxy (Proxy HTTP), immettere il server utilizzando la sintassi http://address:port, Specificare un nome utente e una password se è richiesta l’autenticazione di base per il server, quindi fare clic su Salva.

Cloud Manager non supporta password che includono il carattere @.

Risultato

Dopo aver specificato il server proxy, i nuovi sistemi Cloud Volumes ONTAP vengono configurati automaticamente per l'utilizzo del server proxy durante l'invio di messaggi AutoSupport. Se non è stato specificato il server proxy prima che gli utenti creino sistemi Cloud Volumes ONTAP, devono utilizzare Gestione sistema per impostare manualmente il server proxy nelle opzioni AutoSupport per ciascun sistema.

Esclusione dei blocchi CIFS per Cloud Volumes ONTAP ha in Azure

L'amministratore dell'account può attivare un'impostazione in Cloud Manager che impedisce i problemi di failover dello storage Cloud Volumes ONTAP durante gli eventi di manutenzione di Azure. Quando si attiva questa impostazione, Cloud Volumes ONTAP esegue il veto di CIFS e ripristina le sessioni CIFS attive.

A proposito di questa attività

Microsoft Azure pianifica gli eventi di manutenzione periodica sulle macchine virtuali. Quando si verifica un evento di manutenzione su un nodo di una coppia Cloud Volumes ONTAP ha, la coppia ha avvia il Takeover dello storage. Se durante questo evento di manutenzione sono presenti sessioni CIFS attive, i blocchi sui file CIFS possono impedire il failover dello storage.

Se si attiva questa impostazione, Cloud Volumes ONTAP veto i blocchi e ripristina le sessioni CIFS attive. Di conseguenza, la coppia ha può completare il failover dello storage durante questi eventi di manutenzione.

Questo processo potrebbe interrompere i client CIFS. I dati non impegnati dai client CIFS potrebbero andare persi.

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 **Impostazioni Cloud Manager**.

2. In **ha CIFS Locks**, selezionare la casella di controllo e fare clic su **Save** (Salva).

Riferimento

Ruoli

I ruoli account Admin (Amministratore account), Workspace Admin (Amministratore area di lavoro) e Cloud Compliance Viewer (Visualizzatore conformità cloud) forniscono autorizzazioni specifiche agli utenti.

Attività	Amministratore account	Amministratore dello spazio di lavoro	Cloud Compliance Viewer
Gestire gli ambienti di lavoro	Sì	Sì	No
Abilitare i servizi negli ambienti di lavoro	Sì	Sì	No
Visualizzare lo stato della replica dei dati	Sì	Sì	No
Visualizza la timeline	Sì	Sì	No
Passare da un'area di lavoro all'altra	Sì	Sì	Sì
Visualizzare i risultati della scansione Compliance	Sì	Sì	Sì
Eliminare gli ambienti di lavoro	Sì	No	No
Connettere i cluster Kubernetes agli ambienti di lavoro	Sì	No	No
Ricevere il report Cloud Volumes ONTAP	Sì	No	No
Creare connettori	Sì	No	No
Gestire gli account Cloud Central	Sì	No	No
Gestire le credenziali	Sì	No	No
Modificare le impostazioni di Cloud Manager	Sì	No	No
Visualizza e gestisci la dashboard di supporto	Sì	No	No
Rimuovere gli ambienti di lavoro da Cloud Manager	Sì	No	No
Installare un certificato HTTPS	Sì	No	No

Link correlati

- "Impostazione di aree di lavoro e utenti nell'account Cloud Central"
- "Gestione degli spazi di lavoro e degli utenti nell'account Cloud Central"

In che modo Cloud Manager utilizza le autorizzazioni del cloud provider

Cloud Manager richiede autorizzazioni per eseguire azioni nel tuo cloud provider. Queste autorizzazioni sono incluse in "Le policy fornite da NetApp". Potresti voler capire cosa fa Cloud Manager con queste autorizzazioni.

Cosa fa Cloud Manager con le autorizzazioni AWS

Cloud Manager utilizza un account AWS per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Il servizio token di protezione (STS) e il servizio di gestione delle chiavi (KMS).

Azioni	Scopo
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescripbeInstances", "ec2:DescripbeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Avvia un'istanza di Cloud Volumes ONTAP e interrompe, avvia e monitora l'istanza.
"ec2:DescripbeInstanceAttribute",	Verifica che la rete avanzata sia abilitata per i tipi di istanze supportati.
"ec2:DescripbeRouteTable", "ec2:DescripbeImages",	Avvia una configurazione Cloud Volumes ONTAP ha.
"ec2:CreateTags",	Contrassegna ogni risorsa creata da Cloud Manager con i tag "WorkingEnvironment" e "WorkingEnvironmentId". Cloud Manager utilizza questi tag per la manutenzione e l'allocazione dei costi.
"ec2:CreateVolume", "ec2:DescripbeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestisce i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end.
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescripbeSecurityGroups", "ec2:RevokeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea gruppi di protezione predefiniti per Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescripbeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"ec2:DescripbeSubnet", "ec2:DescripbeVpcs",	Ottiene l'elenco delle subnet di destinazione e dei gruppi di protezione necessari per la creazione di un nuovo ambiente di lavoro per Cloud Volumes ONTAP.
"ec2:DescripbeDhcpOptions",	Determina i server DNS e il nome di dominio predefinito quando si avviano le istanze di Cloud Volumes ONTAP.

Azioni	Scopo
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescripbeSnapshot",	Esegue snapshot dei volumi EBS durante la configurazione iniziale e ogni volta che un'istanza di Cloud Volumes ONTAP viene arrestata.
"ec2:GetConsoleOutput",	Acquisisce la console Cloud Volumes ONTAP, che è collegata ai messaggi AutoSupport.
"ec2:DescripbeKeyPairs",	Ottiene l'elenco delle coppie di chiavi disponibili quando si avviano le istanze.
"ec2:DescripbeRegions",	Ottiene un elenco delle regioni AWS disponibili.
"ec2:DeleteTags", "ec2:DescripteTags",	Gestisce i tag per le risorse associate alle istanze di Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "Cloudformation:DeleteStack", "Cloudformation:DescripbeStack", "Cloudformation:DescripbeStackEvents", "Cloudformation:ValidateTemplate",	Avvia le istanze di Cloud Volumes ONTAP.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Avvia una configurazione Cloud Volumes ONTAP ha.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescripbeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Gestisce i profili di istanza per le istanze di Cloud Volumes ONTAP.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBucket", "s3:ListBucket"	Ottiene informazioni sui bucket AWS S3 in modo che Cloud Manager possa integrarsi con il servizio NetApp Data Fabric Cloud Sync.
"s3:Createbucket", "s3:Deletebucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Gestisce il bucket S3 utilizzato da un sistema Cloud Volumes ONTAP come Tier di capacità per il tiering dei dati.
"Kms:List*", "kms:ReEncrypt*", "kms:descrive*", "kms:CreateGrant",	Attiva la crittografia dei dati di Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi AWS (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Ottiene i dati dei costi AWS per Cloud Volumes ONTAP.

Azioni	Scopo
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	Quando si implementa una configurazione ha in una singola AWS Availability zone, Cloud Manager lancia i due nodi ha e il mediatore in un gruppo di posizionamento AWS Spread.
"ec2:DescripteReservedInstancesOfferings" (ec2:DescripteReservedInstancesOff	Cloud Manager utilizza l'autorizzazione come parte dell'implementazione di Cloud Compliance per scegliere il tipo di istanza da utilizzare.
"s3:Deletebucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetObject", "s3:ListBucket", "s3:ListAllMyBucket", "s3:GetBucketTagging", "s3:GetBucketLocation" "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicicAccessBlock"	Cloud Manager utilizza queste autorizzazioni quando si attiva il servizio Backup in S3.

Cosa fa Cloud Manager con le autorizzazioni Azure

La policy di Cloud Manager Azure include le autorizzazioni necessarie per implementare e gestire Cloud Volumes ONTAP in Azure.

Azioni	Scopo
"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",	Crea Cloud Volumes ONTAP e arresta, avvia, elimina e ottiene lo stato del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Consente l'implementazione di Cloud Volumes ONTAP da un 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/storageAccounts/rigeneratekey/action", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/uses/Read",	Gestisce gli account e i dischi dello storage Azure e li collega a Cloud Volumes ONTAP.

Azioni	Scopo
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action", 	Crea gruppi di sicurezza di rete predefiniti per Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/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", 	Ottiene informazioni di rete relative alle regioni, alla rete virtuale di destinazione e alla subnet e aggiunge Cloud Volumes ONTAP ai reti virtuali.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Attiva gli endpoint del servizio VNET per il tiering dei dati.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Deployments/write",	Implementa Cloud Volumes ONTAP da un modello.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Read", "Microsoft.Resources/subscriptions/operationresults/Read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/Read", "Microsoft.Resources/subscriptions/resourceGroups/write",	Crea e gestisce gruppi di risorse per Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Crea e gestisce snapshot gestite da Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Crea e gestisce i set di disponibilità per Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offers/publisher/offers/plans/agreements/Read", "Microsoft.MarketplaceOrdering/offers/plans/agreements/write"	Consente implementazioni programmatiche da Azure Marketplace.

Azioni	Scopo
"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",	Gestisce un bilanciamento del carico Azure per le coppie ha.
"Microsoft.Authorization/Blocks/*"	Consente la gestione dei blocchi sui dischi Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestisce il failover per le coppie ha.
"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",	Consente la gestione di endpoint privati. Gli endpoint privati vengono utilizzati quando la connettività non viene fornita all'esterno della subnet. Cloud Manager crea l'account storage per ha con solo connettività interna all'interno della subnet.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Consente a Cloud Manager di eliminare i volumi per Azure NetApp Files.
"Microsoft.Resources/Deployments/OperationStatuses/Read"	Azure richiede questa autorizzazione per alcune implementazioni di macchine virtuali (dipende dall'hardware fisico sottostante utilizzato durante l'implementazione).
"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",	Consente di utilizzare Global file cache.

Azioni	Scopo
"Microsoft.Compute/diskEncryptionSets/read"	Consente a Cloud Manager di crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. Questa funzionalità è supportata tramite API.

Cosa fa Cloud Manager con le autorizzazioni GCP

La policy di Cloud Manager per GCP include le autorizzazioni necessarie a Cloud Manager per implementare e gestire Cloud Volumes ONTAP.

Azioni	Scopo
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Per creare e gestire dischi per Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Per creare regole firewall per Cloud Volumes ONTAP.
- Compute.globalOperations.get	Per ottenere lo stato delle operazioni.
- Compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Per ottenere immagini per istanze di macchine virtuali.
- compute.instances.attachDisk - compute.instances.detachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Per creare ed eliminare istanze di Cloud Volumes ONTAP VM.
- compute.instances.get	Per elencare le istanze di macchine virtuali.
- compute.instances.getSerialPortOutput	Per ottenere i log della console.
- compute.instances.list	Per recuperare l’elenco di istanze in una zona.
- compute.instances.setDeletionProtection	Per impostare la protezione di eliminazione sull’istanza.
- compute.instances.setLabels	Per aggiungere etichette.
- compute.instances.setMachineType	Per modificare il tipo di macchina per Cloud Volumes ONTAP.
- compute.instances.setMetadata	Per aggiungere metadati.
- compute.instances.setTags	Per aggiungere tag per le regole del firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Per avviare e arrestare Cloud Volumes ONTAP.
- Compute.machineTypes.get	Per ottenere il numero di core per controllare le qoutas.
- compute.projects.get	Per supportare progetti multipli.

Azioni	Scopo
- Compute.Snapshot.create - compute.snapshots.delete - compute.Snapshot.get - compute.Snapshot.list - compute.snapshots.setLabels	Per creare e gestire snapshot di dischi persistenti.
- 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.zone.list	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale 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 - deploymentmanager.resources.get - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.typeopers.get.get.get - deploymentmanager.get.list	Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Per ottenere unità di log stack.
- resourcemanager.projects.get	Per supportare progetti multipli.
- storage.bucket.create - storage.buckets.delete - storage.bucket.get - storage.bucket.list - storage.bucket.update	Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptKeys.get - cloudkms.cryptKeys.list - cloudkms.keyrings.list	Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Per impostare un account di servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud.

Pagine del marketplace AWS per Cloud Manager e Cloud Volumes ONTAP

Nel marketplace AWS sono disponibili diverse offerte per Cloud Manager e Cloud Volumes ONTAP. Se hai bisogno di aiuto per comprendere lo scopo di ciascuna pagina, leggi le descrizioni riportate di seguito.

In tutti i casi, non è possibile avviare Cloud Volumes ONTAP in AWS dal marketplace AWS. È necessario avviarlo direttamente da Cloud Manager.

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Abilita l'utilizzo di PAYGO Cloud Volumes ONTAP, Tier cloud, conformità cloud e altri servizi aggiuntivi	"Cloud Manager - implementazione di gestione dei servizi dati cloud NetApp"	Questo abbonamento consente di addebitare il costo per LA versione PAYGO di Cloud Volumes ONTAP 9.6 e versioni successive. Consente inoltre di addebitare costi per il Cloud Tiering, la Cloud Compliance e altri servizi aggiuntivi. Devi iscriverti a questa offerta quando Cloud Manager ti richiede e ti reindirizza alla pagina. Cloud Manager visualizza un messaggio nella procedura guidata ambiente di lavoro o quando si aggiungono nuove credenziali in Impostazioni. Questa pagina non consente di avviare Cloud Manager in AWS. Questo dovrebbe essere fatto da "NetApp Cloud Central", O in alternativa utilizzando l'AMI elencato nella riga 3 di questa tabella.
Abilita l'utilizzo di PAYGO Cloud Volumes ONTAP, Tier cloud, conformità cloud e altri servizi aggiuntivi *utilizzando un contratto annuale*	"Cloud Manager (contratti) - implementa Gestisci NetApp Cloud Data Services"	Questo abbonamento è un'alternativa all'abbonamento della prima riga. Consente di ottenere un pagamento anticipato annuale per gli elenchi. È principalmente per i partner NetApp.
Implementare Cloud Manager da AWS Marketplace utilizzando un AMI	"Cloud Manager - Installazione manuale senza chiavi di accesso"	Si consiglia di avviare Cloud Manager in AWS da "NetApp Cloud Central", Ma è possibile avviarlo da questa pagina di AWS Marketplace, se si preferisce.
Implementazione di Cloud Volumes ONTAP PAYGO (9.5 o precedente)	• "Cloud Volumes ONTAP per AWS" • "Cloud Volumes ONTAP per AWS - alta disponibilità"	Queste pagine di AWS Marketplace consentono di sottoscrivere le versioni a nodo singolo o ha di Cloud Volumes ONTAP PAYGO per le versioni 9.5 e precedenti. A partire dalla versione 9.6, è necessario iscriversi alla pagina AWS Marketplace elencata nella riga 1 di questa tabella per le implementazioni PAYGO.

Informazioni sul copyright

Informazioni sul marchio commerciale