



# Inizia subito

## Cloud Manager 3.7

NetApp  
March 25, 2024

# Sommario

- Inizia subito ..... 1
- Panoramica dell'implementazione ..... 1
- Introduzione a Cloud Volumes ONTAP in AWS ..... 2
- Introduzione a Cloud Volumes ONTAP in Azure ..... 4
- Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google ..... 5
- Configurare Cloud Manager ..... 7
- Requisiti di rete ..... 29
- Opzioni di implementazione aggiuntive ..... 46
- Mantenere operativo Cloud Manager ..... 60

# Inizia subito

## Panoramica dell'implementazione

Prima di iniziare, potresti voler comprendere meglio le opzioni per l'implementazione di Cloud Manager e Cloud Volumes ONTAP.

### Installazione di Cloud Manager

Il software Cloud Manager è necessario per implementare e gestire Cloud Volumes ONTAP. È possibile implementare Cloud Manager in una delle seguenti posizioni:

- Amazon Web Services (AWS)
- Microsoft Azure
- Piattaforma Google Cloud

Cloud Manager deve essere nella piattaforma cloud Google quando si implementa Cloud Volumes ONTAP in GCP.

- Cloud IBM
- Nella tua rete

La modalità di implementazione di Cloud Manager dipende dalla posizione scelta:

Posizione per Cloud Manager	Come implementare Cloud Manager
AWS	<ol style="list-style-type: none"><li>1. <a href="#">"Implementazione di Cloud Manager da NetApp Cloud Central"</a> (consigliato)</li><li>2. <a href="#">"Implementazione da AWS Marketplace"</a></li><li>3. <a href="#">"Scaricare e installare il software su un host Linux"</a></li></ol>
AWS C2S	<a href="#">"Implementa Cloud Manager da AWS Intelligence Community Marketplace"</a>
Area di Azure generalmente disponibile	<ol style="list-style-type: none"><li>1. <a href="#">"Implementazione di Cloud Manager da NetApp Cloud Central"</a> (consigliato)</li><li>2. <a href="#">"Implementazione da Azure Marketplace"</a></li><li>3. <a href="#">"Scaricare e installare il software su un host Linux"</a></li></ol>
Governo di Azure	<a href="#">"Implementa Cloud Manager da Azure US Government Marketplace"</a>
Azure Germania	<a href="#">"Scaricare e installare il software su un host Linux"</a>

Posizione per Cloud Manager	Come implementare Cloud Manager
Piattaforma Google Cloud	<ol style="list-style-type: none"> <li>1. <a href="#">"Implementazione di Cloud Manager da NetApp Cloud Central"</a> (consigliato)</li> <li>2. <a href="#">"Scaricare e installare il software su un host Linux"</a></li> </ol> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Non puoi implementare Cloud Manager in Google Cloud da GCP Marketplace</p> </div>
Cloud IBM	<a href="#">"Scaricare e installare il software su un host Linux"</a>
Rete on-premise	<a href="#">"Scaricare e installare il software su un host Linux"</a>

## Configurazione di Cloud Manager

Dopo aver installato Cloud Manager, potrebbe essere necessario eseguire ulteriori operazioni di configurazione, ad esempio l'aggiunta di account di provider cloud aggiuntivi, l'installazione di un certificato HTTPS e altro ancora.

- ["Configurazione dell'account Cloud Central"](#)
- ["Aggiunta di account AWS a Cloud Manager"](#)
- ["Aggiunta di account Azure a Cloud Manager"](#)
- ["Installazione di un certificato HTTPS"](#)
- ["Configurazione di AWS KMS"](#)

## Implementazione di Cloud Volumes ONTAP

Una volta attivato Cloud Manager, puoi iniziare a implementare Cloud Volumes ONTAP nel tuo cloud provider.

["Introduzione ad AWS"](#), ["Introduzione ad Azure"](#), e ["Introduzione a GCP"](#) Fornire istruzioni per l'installazione e l'esecuzione rapida di Cloud Volumes ONTAP. Per ulteriore assistenza, fare riferimento a quanto segue:

- ["Configurazioni supportate per Cloud Volumes ONTAP 9.7 in AWS"](#)
- ["Configurazioni supportate per Cloud Volumes ONTAP 9.7 in Azure"](#)
- ["Configurazioni supportate per Cloud Volumes ONTAP 9.7 in GCP"](#)
- ["Pianificazione della configurazione"](#)
- ["Avvio di Cloud Volumes ONTAP in AWS"](#)
- ["Lancio di Cloud Volumes ONTAP in Azure"](#)
- ["Avvio di Cloud Volumes ONTAP in GCP"](#)

## Introduzione a Cloud Volumes ONTAP in AWS

Inizia a utilizzare Cloud Volumes ONTAP configurando AWS e lanciando il software Cloud Manager da NetApp Cloud Central. È disponibile una versione di prova gratuita di 30 giorni per il primo sistema Cloud Volumes ONTAP lanciato in AWS.

## 1

### Configurare la rete

1. Abilitare l'accesso a Internet in uscita dal VPC di destinazione in modo che Cloud Manager e Cloud Volumes ONTAP possano contattare diversi endpoint.

Questo passaggio è importante perché Cloud Manager non può implementare Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "[Cloud Manager](#)" e "[Cloud Volumes ONTAP](#)".

2. Impostare un endpoint VPC sul servizio S3.

È necessario un endpoint VPC se si desidera eseguire il tiering dei dati cold da Cloud Volumes ONTAP a uno storage a oggetti a basso costo.

## 2

### Fornire le autorizzazioni AWS richieste

Quando si implementa Cloud Manager da NetApp Cloud Central, è necessario utilizzare un account AWS che disponga delle autorizzazioni necessarie per implementare l'istanza.

1. Accedere alla console AWS IAM e creare un criterio copiando e incollando il contenuto di "[Policy NetApp Cloud Central per AWS](#)".
2. Allegare il criterio all'utente IAM.

## 3

### Iscriviti a AWS Marketplace

"[Iscriviti a Cloud Manager da AWS Marketplace](#)" Per garantire che non si verificano interruzioni del servizio al termine della prova gratuita di Cloud Volumes ONTAP. Da questo abbonamento ti verranno addebitati i costi per ogni sistema PAYGO Cloud Volumes ONTAP creato e per ogni funzionalità add-on che abiliti.

Se stai lanciando Cloud Volumes ONTAP con la tua licenza, "[Quindi, dovrai iscriverti a questa offerta in AWS Marketplace](#)".

## 4

### Lanciate Cloud Manager da NetApp Cloud Central

Il software Cloud Manager è necessario per implementare e gestire Cloud Volumes ONTAP. L'avvio di un'istanza di Cloud Manager richiede pochi minuti "[Cloud Central](#)".

## 5

### Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Una volta pronto Cloud Manager, fai clic su Create (Crea), seleziona il tipo di sistema che desideri avviare e completa i passaggi della procedura guidata. Dopo 25 minuti, il primo sistema Cloud Volumes ONTAP dovrebbe essere attivo e funzionante.

Guarda il seguente video per una presentazione di questi passaggi:

► [https://docs.netapp.com/it-it/occm37//media/video\\_getting\\_started\\_aws.mp4](https://docs.netapp.com/it-it/occm37//media/video_getting_started_aws.mp4) (video)

## Link correlati

- ["Valutazione"](#)
- ["Requisiti di rete per Cloud Manager"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in AWS"](#)
- ["Regole del gruppo di sicurezza per AWS"](#)
- ["Aggiunta di account AWS a Cloud Manager"](#)
- ["Cosa fa Cloud Manager con le autorizzazioni AWS"](#)
- ["Avvio di Cloud Volumes ONTAP in AWS"](#)
- ["Avvio di Cloud Manager da AWS Marketplace"](#)

# Introduzione a Cloud Volumes ONTAP in Azure

Inizia a utilizzare Cloud Volumes ONTAP configurando Azure e implementando il software Cloud Manager da NetApp Cloud Central. Sono disponibili istruzioni separate per implementare Cloud Manager in ["Aree pubbliche degli Stati Uniti Azure"](#) e in ["Regioni Azure Germania"](#).



## Configurare la rete

Abilitare l'accesso a Internet in uscita dal VNET di destinazione in modo che Cloud Manager e Cloud Volumes ONTAP possano contattare diversi endpoint.

Questo passaggio è importante perché Cloud Manager non può implementare Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per ["Cloud Manager"](#) e ["Cloud Volumes ONTAP"](#).



## Fornire le autorizzazioni Azure richieste

Quando si implementa Cloud Manager da NetApp Cloud Central, è necessario utilizzare un account Azure che disponga delle autorizzazioni necessarie per implementare la macchina virtuale Cloud Manager.

1. Scaricare il ["Policy di NetApp Cloud Central per Azure"](#).
2. Modificare il file JSON aggiungendo il proprio ID di abbonamento Azure al campo "AssignableScopes".
3. Utilizzare il file JSON per creare un ruolo personalizzato in Azure denominato *Azure SetupAsService*.

Esempio: **az role Definition create --role-Definition C:/Policy\_for\_Setup\_as\_Service\_Azure.json**

4. Dal portale Azure, assegnare il ruolo personalizzato all'utente che implementerà Cloud Manager da Cloud Central.



## Lanciate Cloud Manager da NetApp Cloud Central

Il software Cloud Manager è necessario per implementare e gestire Cloud Volumes ONTAP. L'avvio di un'istanza di Cloud Manager richiede pochi minuti ["Cloud Central"](#).

## 4

### Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Una volta pronto Cloud Manager, fai clic su Create (Crea), seleziona il tipo di sistema che desideri implementare e completa le fasi della procedura guidata. Dopo 25 minuti, il primo sistema Cloud Volumes ONTAP dovrebbe essere attivo e funzionante.

#### Link correlati

- ["Valutazione"](#)
- ["Requisiti di rete per Cloud Manager"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in Azure"](#)
- ["Regole del gruppo di sicurezza per Azure"](#)
- ["Aggiunta di account Azure a Cloud Manager"](#)
- ["Cosa fa Cloud Manager con le autorizzazioni Azure"](#)
- ["Lancio di Cloud Volumes ONTAP in Azure"](#)
- ["Lancio di Cloud Manager da Azure Marketplace"](#)

## Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google

Inizia a utilizzare Cloud Volumes ONTAP configurando il GCP e implementando il software Cloud Manager da NetApp Cloud Central.

Cloud Manager deve essere installato nella piattaforma cloud di Google per implementare Cloud Volumes ONTAP in GCP.

## 1

### Configurare la rete

Abilitare l'accesso a Internet in uscita dal VPC di destinazione in modo che Cloud Manager e Cloud Volumes ONTAP possano contattare diversi endpoint.

Questo passaggio è importante perché Cloud Manager non può implementare Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per ["Cloud Manager"](#) e ["Cloud Volumes ONTAP"](#).

## 2

### Impostare i permessi e i progetti GCP

Assicurarsi che siano presenti due set di autorizzazioni:

1. Assicurarsi che l'utente GCP che implementa Cloud Manager da NetApp Cloud Central disponga delle autorizzazioni in ["Policy Cloud Central per GCP"](#).

["È possibile creare un ruolo personalizzato utilizzando il file YAML"](#) quindi allegarlo all'utente. Per creare il ruolo, dovrai utilizzare la riga di comando di gcloud.

2. Impostare un account di servizio che disponga delle autorizzazioni necessarie per creare e gestire i sistemi

Cloud Volumes ONTAP nei progetti.

Questo account di servizio verrà associato alla macchina virtuale Cloud Manager nel passaggio 6.

- ["Creare un ruolo in GCP"](#) che include le autorizzazioni definite in ["Policy di Cloud Manager per GCP"](#). Anche in questo caso, è necessario utilizzare la riga di comando di gcloud.

Le autorizzazioni contenute in questo file YAML sono diverse da quelle del passaggio 2a.

- ["Creare un account di servizio GCP e applicare il ruolo personalizzato appena creato"](#).
- 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.

### 3

#### Configurare GCP per il tiering dei dati

È necessario soddisfare due requisiti per il Tier dei dati cold da Cloud Volumes ONTAP 9.7 a uno storage a oggetti a basso costo (un bucket di storage cloud di Google):

1. ["Creare un account di servizio"](#) Che ha il ruolo di amministratore dello storage predefinito e l'account del servizio Cloud Manager come utente.

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, sarà necessario selezionare questo account di servizio in un secondo momento. Questo account di servizio è diverso dall'account di servizio creato al punto 2.

2. ["Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google"](#).

Se si desidera utilizzare il tiering dei dati con Cloud Volumes ONTAP 9.6, ["quindi, procedere come segue"](#).

### 4

#### Abilitare le API di Google Cloud

["Abilita le seguenti API di Google Cloud nel tuo progetto"](#). Queste API sono necessarie per implementare Cloud Manager e Cloud Volumes ONTAP.

- API di Cloud Deployment Manager V2
- API Cloud Resource Manager
- API di Compute Engine
- API di registrazione Stackdriver

### 5

#### Iscriviti al GCP Marketplace

["Iscriviti a Cloud Volumes ONTAP dal mercato GCP"](#) per garantire che il servizio non si disservi al termine della prova gratuita. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP creato.



## 6

### Lanciate Cloud Manager da NetApp Cloud Central

Il software Cloud Manager è necessario per implementare e gestire Cloud Volumes ONTAP. Bastano pochi minuti per avviare un'istanza di Cloud Manager in GCP da ["Cloud Central"](#).

Quando scegli GCP come provider cloud, Google ti chiede di accedere al tuo account e di concedere le autorizzazioni. Facendo clic su "Allow" (Consenti) viene consentito l'accesso alle API di calcolo necessarie per implementare Cloud Manager.

## 7

### Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Una volta pronto Cloud Manager, fai clic su Create (Crea), seleziona il tipo di sistema che desideri implementare e completa le fasi della procedura guidata. Dopo 25 minuti, il primo sistema Cloud Volumes ONTAP dovrebbe essere attivo e funzionante.

#### Link correlati

- ["Valutazione"](#)
- ["Requisiti di rete per Cloud Manager"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in GCP"](#)
- ["Regole firewall per GCP"](#)
- ["Cosa fa Cloud Manager con le autorizzazioni GCP"](#)
- ["Avvio di Cloud Volumes ONTAP in GCP"](#)
- ["Download e installazione del software Cloud Manager su un host Linux"](#)

## Configurare Cloud Manager

### Impostazione di aree di lavoro e utenti nell'account Cloud Central

Ogni sistema Cloud Manager è associato a un *account NetApp Cloud Central*. Configura l'account Cloud Central associato al tuo sistema Cloud Manager in modo che un utente possa accedere a Cloud Manager e implementare i sistemi Cloud Volumes ONTAP nelle aree di lavoro. Basta aggiungere un utente o più utenti e aree di lavoro.

L'account viene mantenuto in Cloud Central, pertanto qualsiasi modifica apportata sarà disponibile per altri sistemi Cloud Manager e per altri servizi dati cloud NetApp. ["Scopri di più sul funzionamento degli account Cloud Central"](#).

#### Aggiunta di aree di lavoro

In Cloud Manager, le aree di lavoro consentono di isolare un set di ambienti di lavoro da altri ambienti di lavoro e da altri utenti. Ad esempio, è possibile creare due aree di lavoro e associare utenti separati alle aree di lavoro.

#### Fasi

1. Fare clic su **Impostazioni account**.



2. Fare clic su **Workspaces**.
3. Fare clic su **Aggiungi nuova area di lavoro**.
4. Immettere un nome per l'area di lavoro e fare clic su **Aggiungi**.

#### Al termine


È ora possibile associare utenti e connettori di servizio allo spazio di lavoro.

#### 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 creare un account.
2. In Cloud Manager, fare clic su **Impostazioni account**.
3. Nella scheda Users (utenti), fare clic su **associate User** (Associa utente).
4. 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.
5. Se si seleziona Workspace Admin (Amministrazione area di lavoro), selezionare una o più aree di lavoro da associare all'utente.



## Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

Role

Associate User to Workspaces

6. 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.

### Associazione di Workspace Admins alle aree di lavoro

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

### Fasi

1. Fare clic su **Impostazioni account**.
2. Fare clic sul menu delle azioni nella riga corrispondente all'utente.

2 Users

Name	Email	Role	Workspaces
Ben		Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

3. Fare clic su **Gestisci aree di lavoro**.
4. Selezionare una o più aree di lavoro e fare clic su **Applica**.

### Risultato

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

### Associazione dei connettori di servizio alle aree di lavoro

Un Service Connector fa parte del sistema Cloud Manager. Viene eseguito sull'istanza della macchina virtuale implementata nel provider di cloud o su un host on-premise configurato. È necessario associare questo connettore di servizio 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 di servizio 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 di servizio"](#).

### Fasi

1. Fare clic su **Impostazioni account**.
2. Fare clic su **Service Connector**.
3. Fare clic su **Manage Workspaces** (Gestisci aree di lavoro) per il Service Connector che si desidera associare.
4. Selezionare una o più aree di lavoro e fare clic su **Applica**.

### Risultato

Gli amministratori dell'area di lavoro possono ora accedere alle aree di lavoro associate, purché l'utente sia stato associato anche all'area di lavoro.

## Impostazione e aggiunta di account AWS a Cloud Manager

Se si desidera implementare Cloud Volumes ONTAP in diversi account AWS, è necessario fornire le autorizzazioni necessarie e aggiungere i dettagli a Cloud Manager. 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 implementa Cloud Manager da Cloud Central, Cloud Manager aggiunge automaticamente l'account AWS in cui hai implementato Cloud Manager. Se il software Cloud Manager è stato installato manualmente su un sistema esistente, non viene aggiunto un account iniziale. ["Informazioni sugli account e sulle autorizzazioni AWS"](#).

## Scelte

- [Concessione delle autorizzazioni fornendo le chiavi AWS](#)
- [Concessione delle autorizzazioni assumendo ruoli IAM in altri account](#)

### 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 Cloud Manager 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 Cloud Manager.
- Allegare la policy IAM di Cloud Manager, disponibile in ["Pagina delle policy di Cloud Manager"](#).

## Create role



### Select type of trusted entity

Four options for trusted entity type are shown in a row:

- AWS service**: EC2, Lambda and others.
- Another AWS account**: Belonging to you or 3rd party. This option is highlighted with a blue border.
- Web identity**: Cognito or any OpenID provider.
- SAML 2.0 federation**: Your corporate directory.

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*  ⓘ

- Options
- Require external ID (Best practice when a third party will assume this role)
  - Require MFA ⓘ

- Accedere all'account di origine in cui risiede l'istanza di Cloud Manager e selezionare il ruolo IAM associato all'istanza.
  - Fare clic su **Trust Relationship > Edit trust relationship**.
  - Aggiungi 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 account AWS a Cloud Manager

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

### Fasi

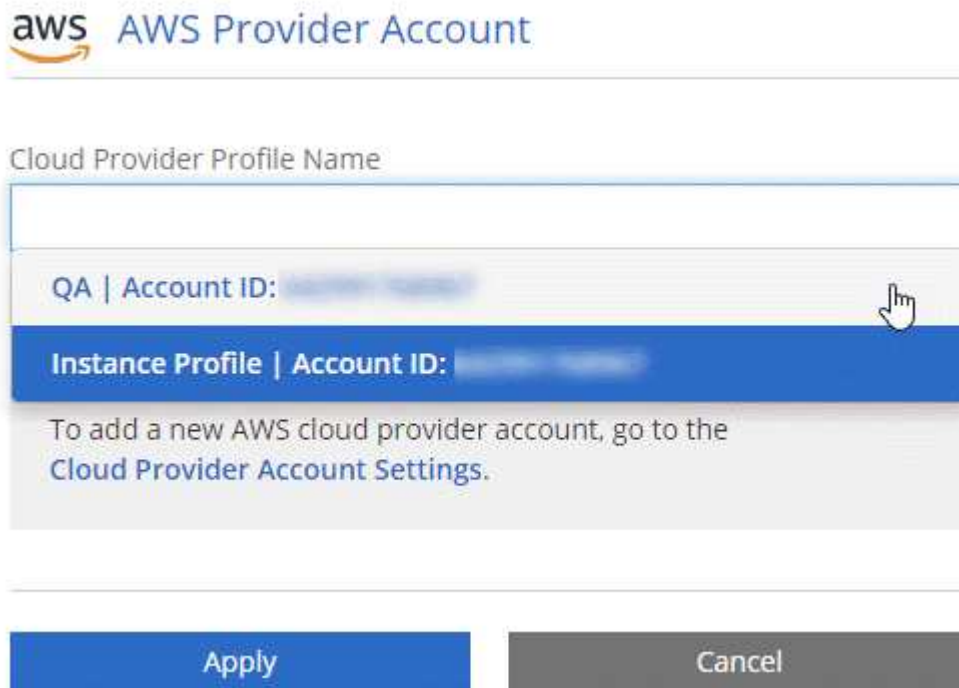
- Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **Cloud Provider & Support Accounts**.



2. Fare clic su **Add New account** (Aggiungi nuovo account) e selezionare **AWS**.
3. Scegliere se si desidera fornire le chiavi AWS o l'ARN di un ruolo IAM attendibile.
4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

### Risultato

È ora possibile passare a un altro account dalla pagina Dettagli e credenziali quando si crea un nuovo ambiente di lavoro:



## Configurazione e aggiunta di account Azure a Cloud Manager

Se si desidera implementare Cloud Volumes ONTAP in diversi account Azure, è necessario fornire le autorizzazioni necessarie a tali account e aggiungere dettagli sugli account a Cloud Manager.



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

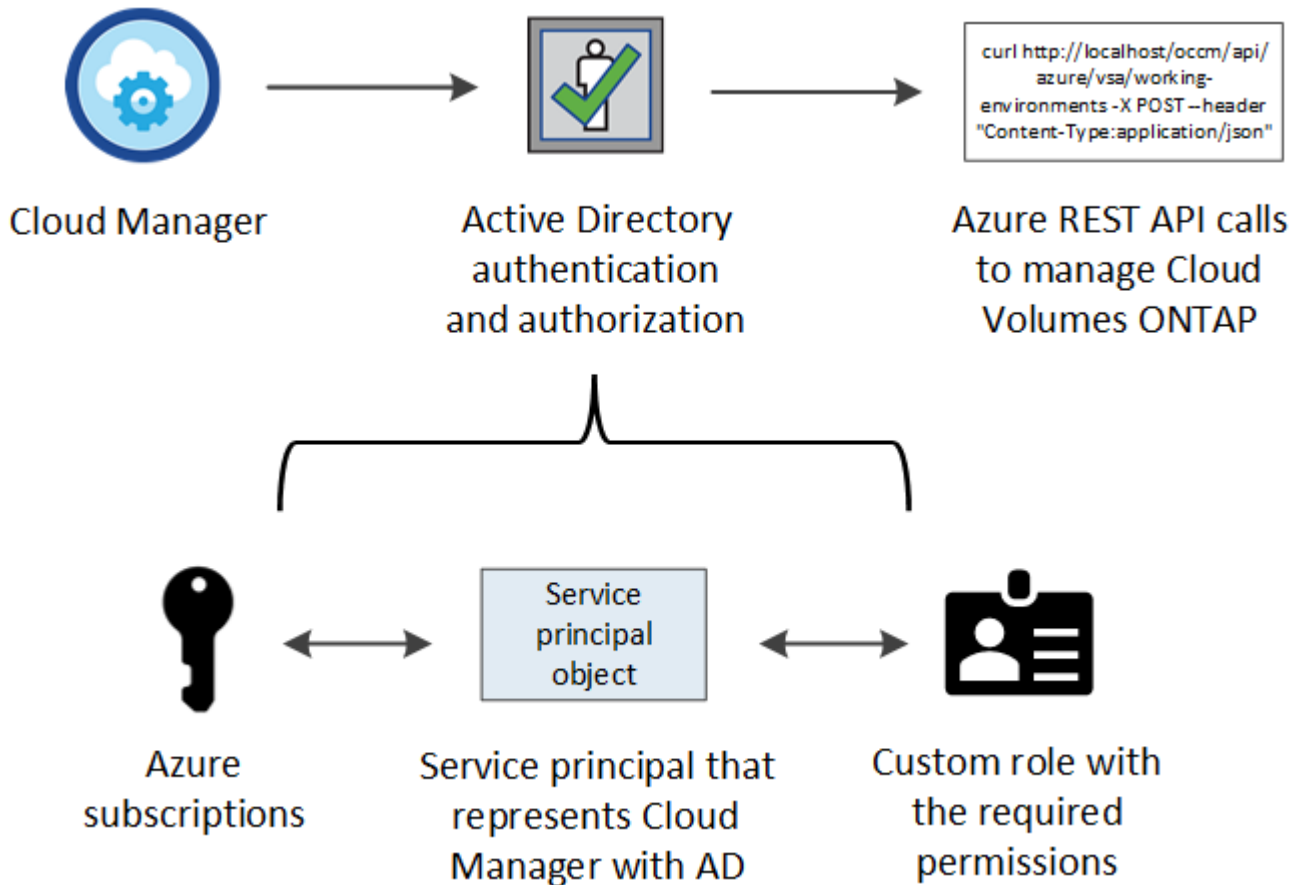
### Concessione delle autorizzazioni di Azure mediante un'entità del servizio

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.

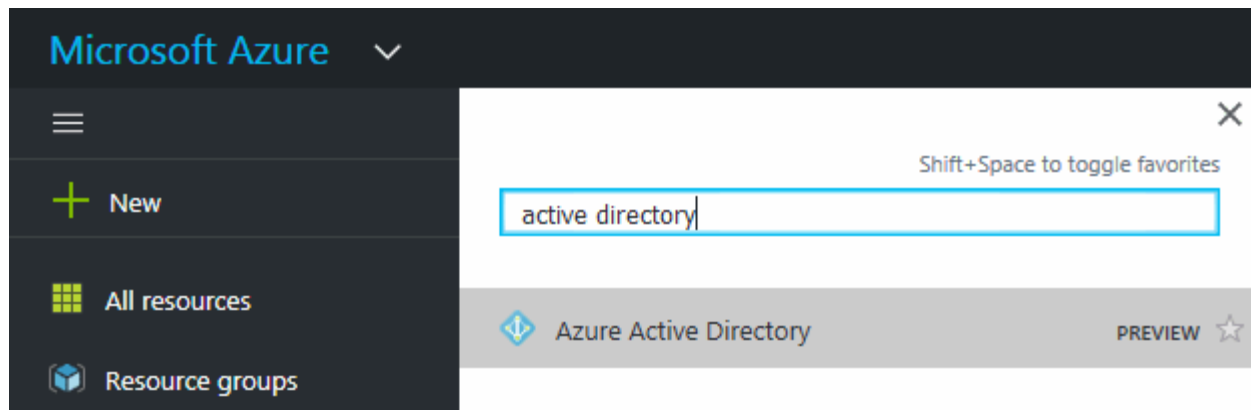
#### Prima di iniziare

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"
```

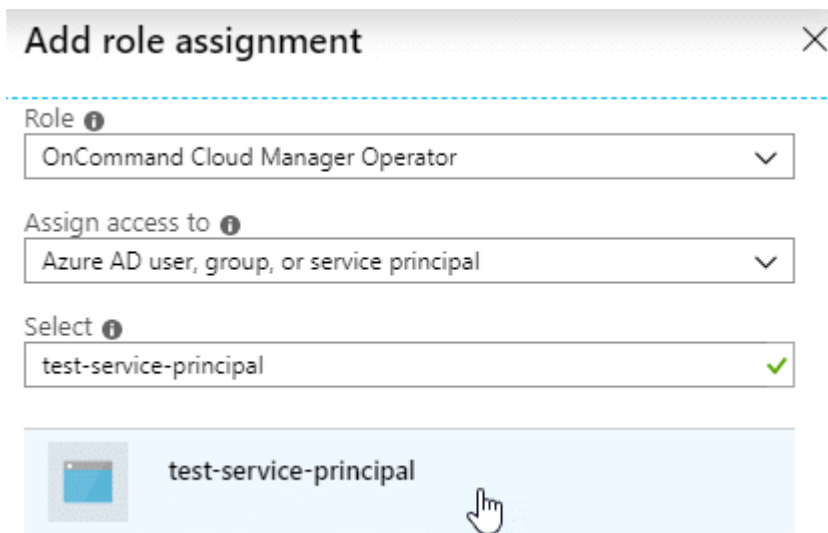
- c. Utilizzare il file JSON per creare un ruolo personalizzato in Azure.

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\_3.7.4.json**

Ora dovresti avere un ruolo personalizzato chiamato *operatore cloud manager OnCommand*.

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 **operatore cloud OnCommand**.
  - e. Mantieni selezionata l'opzione **Azure ad user, group o service principal**.
  - f. Cercare il nome dell'applicazione (non è possibile trovarla nell'elenco scorrendo).



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

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

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

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

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

#### **Fasi**


1. Nel servizio **Azure Active Directory**, fare clic su **App Registrations** e selezionare l'applicazione.
2. Fare clic su **API permissions > Add a permission** (autorizzazioni API > Aggiungi autorizzazione)
3. In **Microsoft API**, selezionare **Azure Service Management**.

## Request API permissions

Select an API

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


Commonly used Microsoft APIs

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

4. Fare clic su **Access Azure Service Management as organization users** (Accedi a Azure Service Management come utenti dell'organizzazione), quindi fare clic su **Add permissions** (

## Request API permissions

[< All APIs](#)

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

What type of permissions does your application require?

### Delegated permissions

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

### Application permissions

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

Select permissions

[expand all](#)

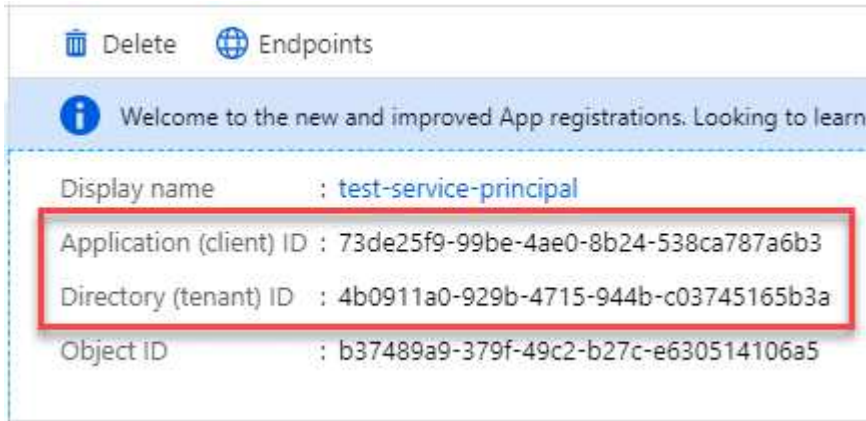
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) 	-

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

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

### Fasi

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



Delete Endpoints

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

Display name : test-service-principal

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

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

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

### Creazione di un client segreto

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



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

### Fasi

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

### Client secrets

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

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0v4NLfdAcY7:+0vA	

### 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 account Azure a Cloud Manager

Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungerlo 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 **Cloud Provider & Support Accounts**.



2. Fare clic su **Aggiungi nuovo account** e selezionare **Microsoft Azure**.
3. Immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
  - ID applicazione: Vedere [Ottenerne l'ID dell'applicazione e l'ID della directory](#).
  - ID tenant (o ID directory): Vedere [Ottenerne l'ID dell'applicazione e l'ID della directory](#).
  - Application Key (chiave applicativa) (il segreto del client): Vedere [Creazione di un client segreto](#).
4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

### Risultato

È ora possibile passare a un altro account dalla pagina Dettagli e credenziali quando si crea un nuovo ambiente di lavoro:



Cloud Provider Profile Name

Azure Keys   Application ID: [REDACTED] ...
Dev Keys   Application ID: [REDACTED] ...
<b>Managed Service Identity</b>

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

## Associazione di sottoscrizioni Azure aggiuntive a un'identità gestita

Cloud Manager consente di scegliere l'account 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 Cloud Manager da NetApp Cloud Central. Quando hai implementato Cloud Manager, Cloud Central ha creato il ruolo di operatore di Cloud Manager di OnCommand e lo ha assegnato alla macchina virtuale di Cloud Manager.

### Fasi

1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare i sistemi 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 **operatore cloud OnCommand**.



L'operatore di gestione cloud di OnCommand 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 Cloud Manager.
- Selezionare la macchina virtuale Cloud Manager.
- 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.

**Microsoft Azure Provider Account**

Cloud Provider Profile Name  
Managed Service Identity

Azure Subscription

OCCM Dev
<b>OCCM QA1 (Default)</b>

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply Cancel

## Configurazione e aggiunta di account GCP a Cloud Manager

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

### 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.

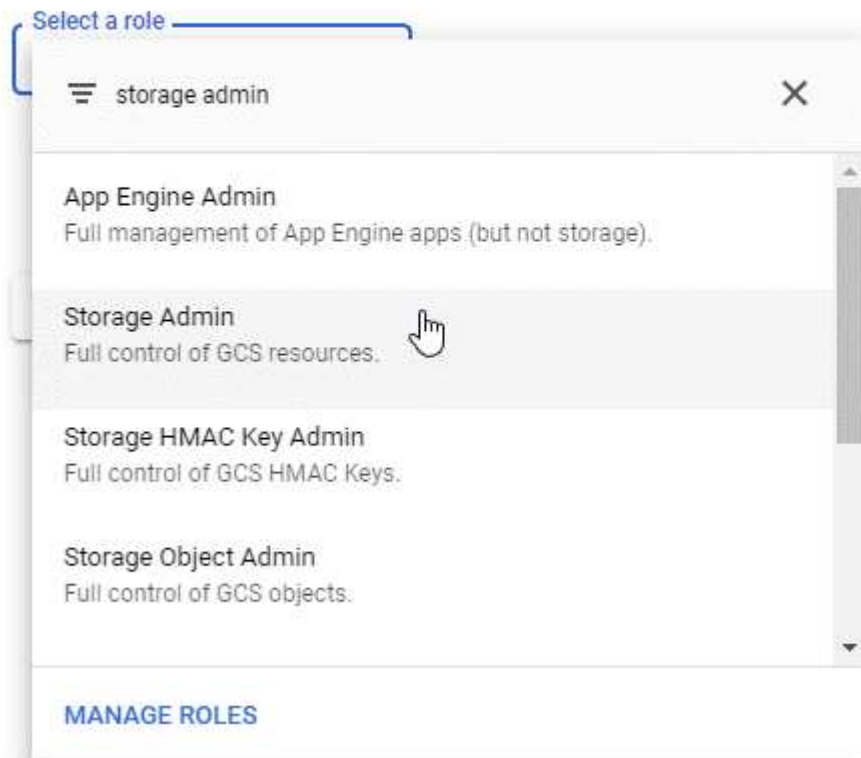
### Fasi



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

## Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



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.



## Select a service account

Email	Name	Keys
<input checked="" type="radio"/> data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	—

[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

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.

#### Fasi

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



2. Fare clic su **Aggiungi nuovo account** e selezionare **GCP**.
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 sui singoli volumi 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>

### 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 **Cloud Provider & Support Accounts**.



3. Fare clic su **Add New account** (Aggiungi nuovo account) e selezionare **NetApp Support Site** (Sito di supporto NetApp).
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](#)"

## Installazione 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.

### 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	<ol style="list-style-type: none"><li>a. Inserire il nome host o il DNS dell'host Cloud Manager (nome comune), quindi fare clic su <b>generate CSR</b> (genera CSR).  Cloud Manager visualizza una richiesta di firma del certificato.</li><li>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.</li><li>c. Copiare il contenuto del certificato firmato, incollarlo nel campo certificato, quindi fare clic su <b>Installa</b>.</li></ol>
Installare il proprio certificato firmato dalla CA	<ol style="list-style-type: none"><li>a. Selezionare <b>Installa certificato firmato dalla CA</b>.</li><li>b. Caricare il file del certificato e la chiave privata, quindi fare clic su <b>Installa</b>.  Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.</li></ol>

### 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:

## Cloud Manager HTTPS certificate

Expiration:

⚠ Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv,  
EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com,  
OU=Tel-Aviv, O=NetApp, CN=localhost

 [View Certificate](#)

 [Renew HTTPS Certificate](#)

## Configurazione di AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario configurare il servizio di gestione delle chiavi AWS.

### Fasi

1. Assicurarsi che esista una chiave master cliente (CMK) attiva.

Il CMK può essere un CMK gestito da AWS o un CMK gestito dal cliente. Può trovarsi nello stesso account AWS di Cloud Manager e Cloud Volumes ONTAP o in un altro account AWS.

["Documentazione AWS: Customer Master Keys \(CMK\)"](#)

2. Modificare il criterio chiave per ogni CMK aggiungendo il ruolo IAM che fornisce le autorizzazioni a Cloud Manager come *utente chiave*.

L'aggiunta del ruolo IAM come utente chiave consente a Cloud Manager di utilizzare la CMK con Cloud Volumes ONTAP.

["Documentazione AWS: Modifica delle chiavi"](#)

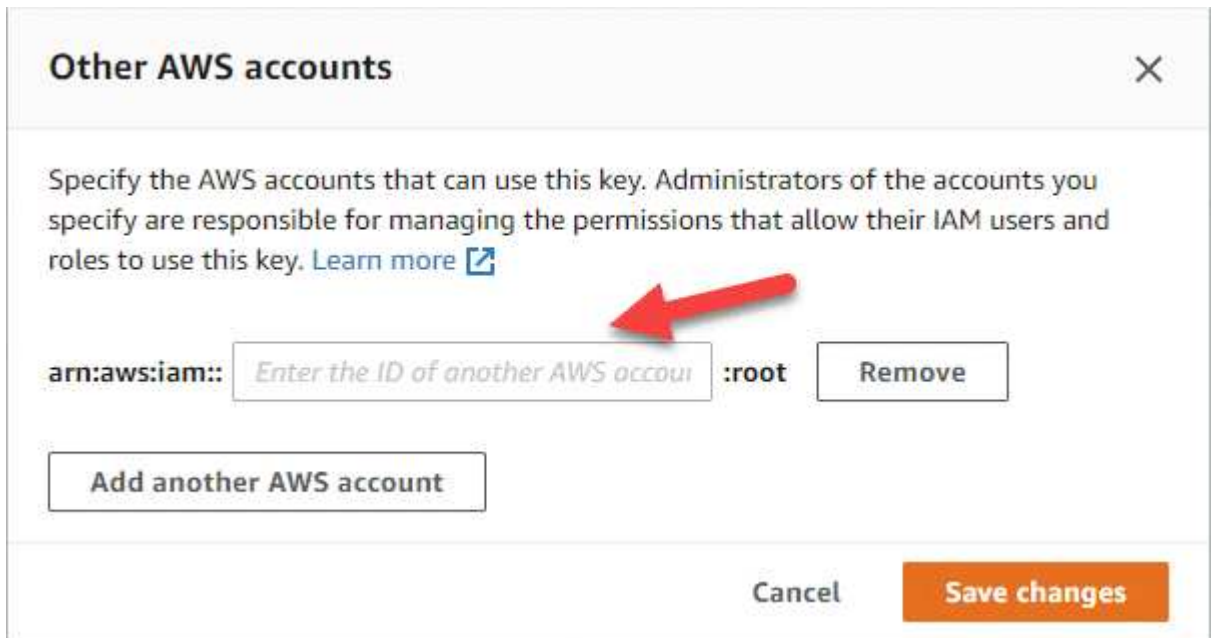
3. Se il CMK si trova in un account AWS diverso, completare la seguente procedura:

- a. Accedere alla console KMS dall'account in cui risiede il CMK.
- b. Selezionare la chiave.
- c. Nel riquadro **General Configuration** (Configurazione generale), copiare l'ARN della chiave.

Quando crei il sistema Cloud Volumes ONTAP, dovrai fornire l'ARN a Cloud Manager.

- d. Nel riquadro **altri account AWS**, aggiungere l'account AWS che fornisce le autorizzazioni a Cloud Manager.

Nella maggior parte dei casi, si tratta dell'account in cui risiede Cloud Manager. Se Cloud Manager non fosse installato in AWS, sarebbe l'account per cui hai fornito le chiavi di accesso AWS a Cloud Manager.



- e. Passare ora all'account AWS che fornisce le autorizzazioni a Cloud Manager e aprire la console IAM.
- f. Creare un criterio IAM che includa le autorizzazioni elencate di seguito.
- g. Allegare il criterio al ruolo IAM o all'utente IAM che fornisce le autorizzazioni a Cloud Manager.

Il seguente criterio fornisce le autorizzazioni necessarie a Cloud Manager per utilizzare il CMK dall'account AWS esterno. Assicurarsi di modificare la regione e l'ID account nelle sezioni "risorsa".

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

Per ulteriori informazioni su questo processo, vedere ["Documentazione AWS: Consentire agli account AWS esterni di accedere a un CMK"](#).

# Requisiti di rete

## Requisiti di rete per Cloud Manager

Configura la tua rete in modo che Cloud Manager possa implementare i sistemi Cloud Volumes ONTAP in AWS, Microsoft Azure o Google Cloud Platform. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.



Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, Cloud Manager richiede di specificare il proxy durante la configurazione. È inoltre possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a ["Configurazione di Cloud Manager per l'utilizzo di un server proxy"](#).

### Connessione alle reti di destinazione

Cloud Manager richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud Volumes ONTAP.

Ad esempio, se si installa Cloud Manager nella rete aziendale, è necessario impostare una connessione VPN al VPC o a VNET in cui si avvia Cloud Volumes ONTAP.

### Accesso a Internet in uscita

Cloud Manager richiede l'accesso a Internet in uscita per implementare e gestire Cloud Volumes ONTAP. L'accesso a Internet in uscita è necessario anche quando si accede a Cloud Manager dal browser Web e si esegue il programma di installazione di Cloud Manager su un host Linux.

Le sezioni seguenti identificano gli endpoint specifici.

### Endpoint per gestire Cloud Volumes ONTAP in AWS

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in AWS:

Endpoint	Scopo
Servizi AWS (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Servizio di gestione delle chiavi (KMS)</li><li>• Servizio token di sicurezza (STS)</li><li>• S3 (Simple Storage Service)</li></ul> L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. <a href="#">"Per ulteriori informazioni, fare riferimento alla documentazione AWS."</a>	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP in AWS.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Richieste API a NetApp Cloud Central.

Endpoint	Scopo
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Fornisce l'accesso a immagini, manifesti e modelli software.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
<a href="https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist">https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist</a>	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	Comunicazione con NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

#### Endpoint per gestire Cloud Volumes ONTAP in Azure

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in Microsoft Azure:

Endpoint	Scopo
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure.



Endpoint	Scopo
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Richieste API a NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Fornisce l'accesso a immagini, manifesti e modelli software.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Comunicazione con NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

### Endpoint per gestire Cloud Volumes ONTAP in GCP

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in GCP:

Endpoint	Scopo
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Consente a Cloud Manager di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Richieste API a NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Fornisce l'accesso a immagini, manifesti e modelli software.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Comunicazione con NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

#### Endpoint a cui si accede dal browser Web

Gli utenti devono accedere a Cloud Manager da un browser Web. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host Cloud Manager	<p>Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.</p> <p>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:</p> <ul style="list-style-type: none"> <li>• Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale</li> <li>• Un IP pubblico funziona in qualsiasi scenario di rete</li> </ul> <p>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

#### Endpoint per installare Cloud Manager su un host Linux

Il programma di installazione di Cloud Manager deve accedere ai seguenti URL durante il processo di installazione:

- <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>

#### Porte e gruppi di sicurezza

- Se si implementa Cloud Manager da Cloud Central o dalle immagini del marketplace, fare riferimento a quanto segue:
  - ["Regole del gruppo di sicurezza per Cloud Manager in AWS"](#)
  - ["Regole del gruppo di sicurezza per Cloud Manager in Azure"](#)
  - ["Regole firewall per Cloud Manager in GCP"](#)
- Se si installa Cloud Manager su un host Linux esistente, vedere ["Requisiti degli host di Cloud Manager"](#).

#### Requisiti di rete per Cloud Volumes ONTAP in AWS

Configurare la rete AWS in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

#### Requisiti generali di rete AWS per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

## Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in modo proattivo lo stato di salute dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS di AWS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

Se si dispone di un'istanza NAT, è necessario definire una regola del gruppo di sicurezza in entrata che consenta il traffico HTTPS dalla subnet privata a Internet.

## Accesso a Internet in uscita per il mediatore ha

L'istanza di ha mediator deve disporre di una connessione in uscita al servizio AWS EC2 in modo che possa fornire assistenza per il failover dello storage. Per fornire la connessione, è possibile aggiungere un indirizzo IP pubblico, specificare un server proxy o utilizzare un'opzione manuale.

L'opzione manuale può essere un gateway NAT o un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2. Per ulteriori informazioni sugli endpoint VPC, fare riferimento a "[Documentazione AWS: Endpoint VPC di interfaccia \(AWS PrivateLink\)](#)".

## Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in AWS:

- Nodo singolo: 6 indirizzi IP
- Coppie HA in un singolo AZS: 15 indirizzi
- Coppie HA in più AZS: 15 o 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM su sistemi a nodo singolo, ma non su coppie ha in un singolo AZ. È possibile scegliere se creare una LIF di gestione SVM su coppie ha in più AZS.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

## Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a "[Regole del gruppo di sicurezza](#)".

## Connessione da Cloud Volumes ONTAP ad AWS S3 per il tiering dei dati

Se si desidera utilizzare EBS come Tier di performance e AWS S3 come Tier di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione consiste nella creazione di un endpoint VPC per il servizio S3. Per istruzioni, vedere "[Documentazione AWS: Creazione di un endpoint gateway](#)".

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di Cloud Volumes ONTAP. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, Cloud Volumes ONTAP non può connettersi al servizio S3.

In caso di problemi, vedere "[AWS Support Knowledge Center: Perché non è possibile connettersi a un](#)

[bucket S3 utilizzando un endpoint VPC gateway?"](#)

## Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra AWS VPC e l'altra rete, ad esempio Azure VNET o la rete aziendale. Per istruzioni, vedere ["Documentazione AWS: Configurazione di una connessione VPN AWS"](#).

## DNS e Active Directory per CIFS

Se si desidera eseguire il provisioning dello storage CIFS, è necessario configurare DNS e Active Directory in AWS o estendere la configurazione on-premise ad AWS.

Il server DNS deve fornire servizi di risoluzione dei nomi per l'ambiente Active Directory. È possibile configurare i set di opzioni DHCP in modo che utilizzino il server DNS EC2 predefinito, che non deve essere il server DNS utilizzato dall'ambiente Active Directory.

Per istruzioni, fare riferimento a ["Documentazione AWS: Active Directory Domain Services su AWS Cloud: Implementazione di riferimento rapido"](#).

## Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP ha che utilizzano zone di disponibilità multiple (AZS). Prima di avviare una coppia ha, è necessario esaminare questi requisiti perché è necessario inserire i dettagli di rete in Cloud Manager.

Per informazioni sul funzionamento delle coppie ha, vedere ["Coppie ad alta disponibilità"](#).

## Zone di disponibilità

Questo modello di implementazione ha utilizza più AZS per garantire un'elevata disponibilità dei dati. È necessario utilizzare un AZ dedicato per ogni istanza di Cloud Volumes ONTAP e per l'istanza del mediatore, che fornisce un canale di comunicazione tra la coppia ha.

## Indirizzi IP mobili per dati NAS e gestione cluster/SVM

Le configurazioni HA in più AZS utilizzano indirizzi IP mobili che migrano tra nodi in caso di guasti. Non sono accessibili in modo nativo dall'esterno del VPC, a meno che non si ["Configurare un gateway di transito AWS"](#).

Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.



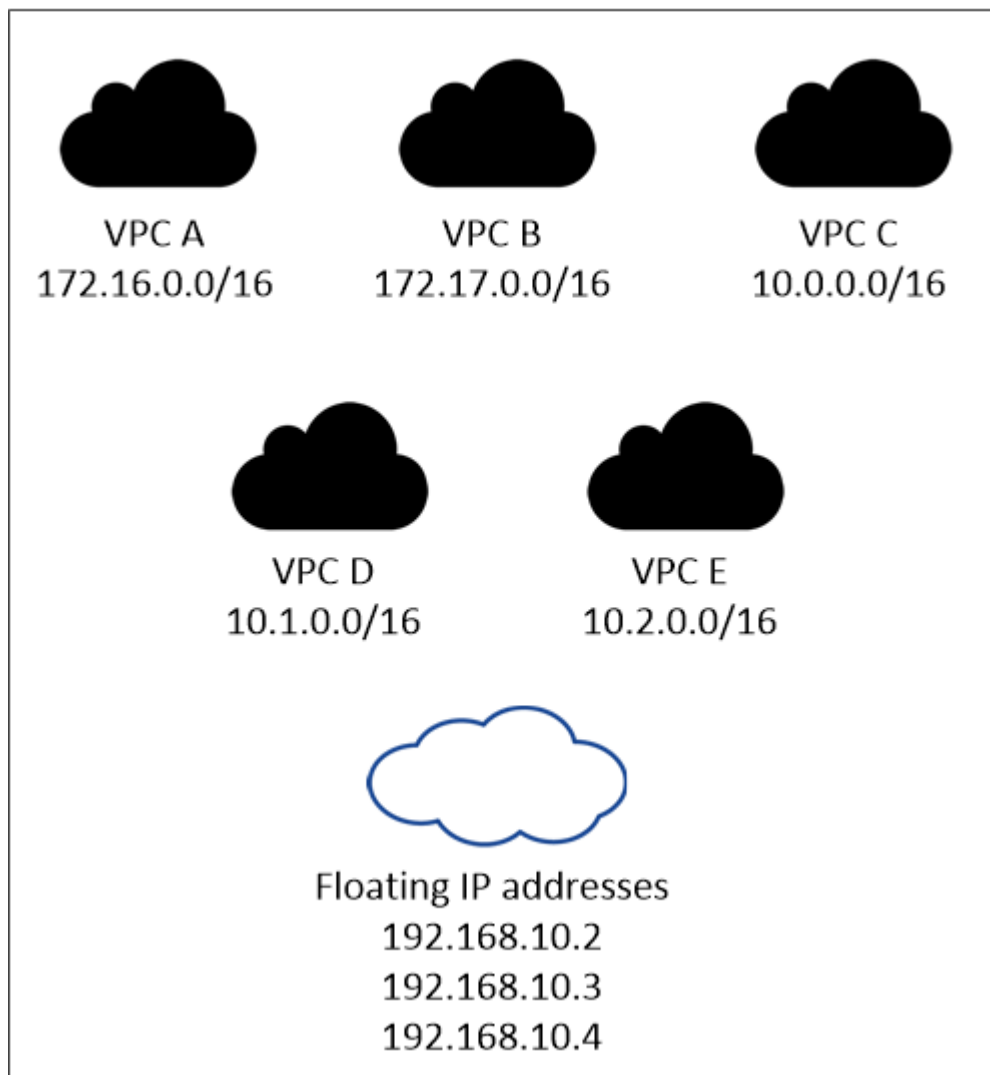
Se si utilizza SnapDrive per Windows o SnapCenter con la coppia ha, è necessario un indirizzo IP mobile per la LIF di gestione SVM. Se non si specifica l'indirizzo IP durante l'implementazione del sistema, è possibile creare la LIF in un secondo momento. Per ulteriori informazioni, vedere ["Configurazione di Cloud Volumes ONTAP"](#).

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP ha, è necessario inserire gli indirizzi IP mobili in Cloud Manager. Cloud Manager assegna gli indirizzi IP alla coppia ha quando avvia il sistema.

Gli indirizzi IP mobili devono essere al di fuori dei blocchi CIDR per tutti i VPC nella regione AWS in cui si implementa la configurazione ha. Gli indirizzi IP mobili sono una subnet logica esterna ai VPC della propria regione.

Nell'esempio seguente viene illustrata la relazione tra gli indirizzi IP mobili e i VPC in una regione AWS. Mentre gli indirizzi IP mobili si trovano al di fuori dei blocchi CIDR per tutti i VPC, sono instradabili alle subnet attraverso le tabelle di routing.

## AWS region



Cloud Manager crea automaticamente indirizzi IP statici per l'accesso iSCSI e NAS da client esterni al VPC. Non è necessario soddisfare alcun requisito per questi tipi di indirizzi IP.

### Gateway di transito per abilitare l'accesso IP mobile dall'esterno del VPC

"[Configurare un gateway di transito AWS](#)" Per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

### Tabelle di percorso

Dopo aver specificato gli indirizzi IP mobili in Cloud Manager, è necessario selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili. In questo modo si abilita l'accesso del client alla coppia ha.

Se si dispone di una sola tabella di routing per le subnet nel VPC (la tabella di routing principale), Cloud Manager aggiunge automaticamente gli indirizzi IP mobili alla tabella di routing. Se si dispone di più tabelle di routing, è molto importante selezionare le tabelle di routing corrette quando si avvia la coppia ha. In caso contrario, alcuni client potrebbero non avere accesso a Cloud Volumes ONTAP.

Ad esempio, potrebbero essere presenti due subnet associate a diverse tabelle di routing. Se si seleziona la tabella di route A, ma non la tabella di route B, i client nella subnet associata alla tabella di route A

possono accedere alla coppia ha, ma i client nella subnet associata alla tabella di route B.

Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a. "[Documentazione AWS: Tabelle di percorso](#)".

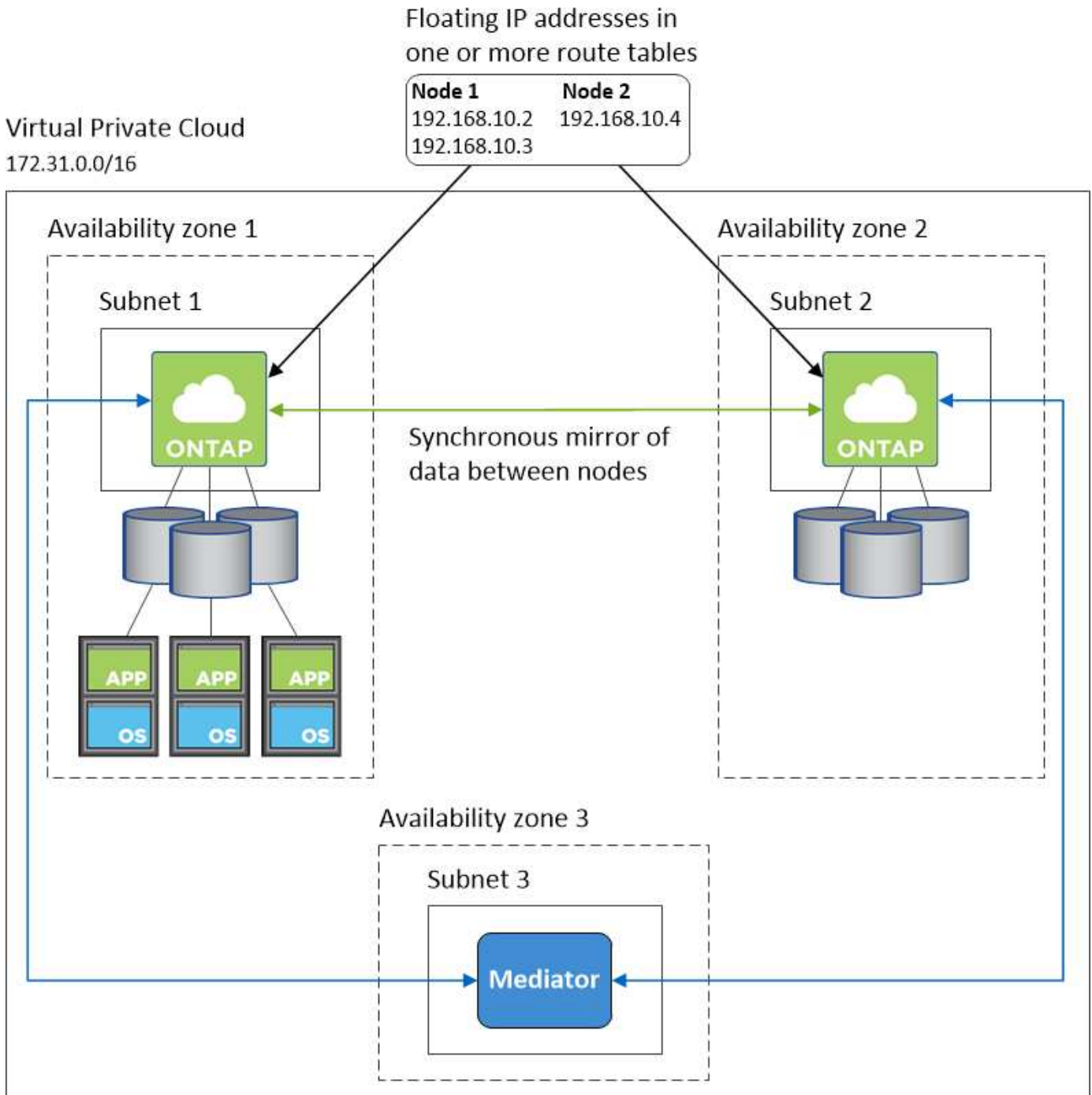
### **Connessione ai tool di gestione NetApp**

Per utilizzare gli strumenti di gestione NetApp con configurazioni ha che si trovano in più AZS, sono disponibili due opzioni di connessione:

1. Implementare gli strumenti di gestione NetApp in un VPC diverso e. "[Configurare un gateway di transito AWS](#)". Il gateway consente l'accesso all'indirizzo IP mobile per l'interfaccia di gestione del cluster dall'esterno del VPC.
2. Implementare gli strumenti di gestione NetApp nello stesso VPC con una configurazione di routing simile a quella dei client NAS.

### **Configurazione di esempio**

La seguente immagine mostra una configurazione ha ottimale in AWS che opera come configurazione Active-passive:



### Configurazioni VPC di esempio

Per comprendere meglio come implementare Cloud Manager e Cloud Volumes ONTAP in AWS, è necessario esaminare le configurazioni VPC più comuni.

- Un VPC con subnet pubbliche e private e un dispositivo NAT
- Un VPC con una subnet privata e una connessione VPN alla rete

#### Un VPC con subnet pubbliche e private e un dispositivo NAT

Questa configurazione VPC include subnet pubbliche e private, un gateway Internet che connette il VPC a Internet e un gateway NAT o istanza NAT nella subnet pubblica che abilita il traffico Internet in uscita dalla



subnet privata. In questa configurazione, è possibile eseguire Cloud Manager in una subnet pubblica o in una subnet privata, ma la subnet pubblica è consigliata perché consente l'accesso da host esterni al VPC. È quindi possibile avviare le istanze di Cloud Volumes ONTAP nella subnet privata.

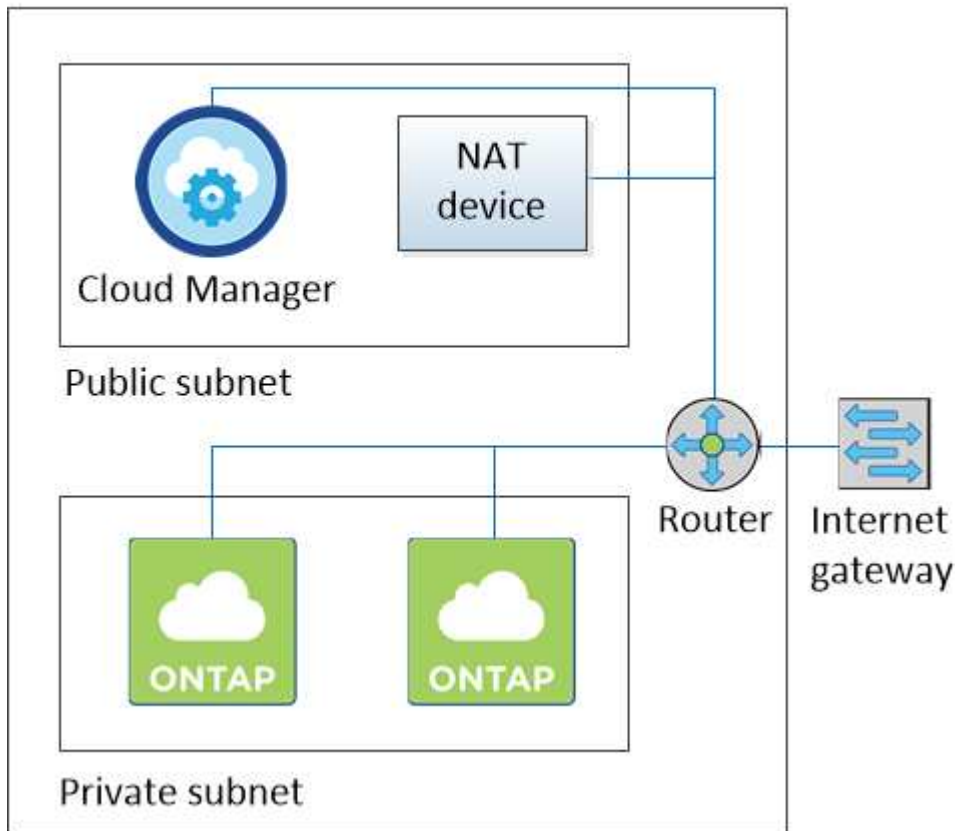


Invece di un dispositivo NAT, è possibile utilizzare un proxy HTTP per fornire la connettività Internet.

Per ulteriori informazioni su questo scenario, fare riferimento a "[Documentazione AWS: Scenario 2: VPC con subnet pubbliche e private \(NAT\)](#)".

La seguente figura mostra Cloud Manager in esecuzione in una subnet pubblica e in sistemi a nodo singolo in esecuzione in una subnet privata:

## Virtual Private Cloud



### Un VPC con una subnet privata e una connessione VPN alla rete

Questa configurazione VPC è una configurazione di cloud ibrido in cui Cloud Volumes ONTAP diventa un'estensione del tuo ambiente privato. La configurazione include una subnet privata e un gateway privato virtuale con una connessione VPN alla rete. Il routing attraverso il tunnel VPN consente alle istanze EC2 di accedere a Internet attraverso la rete e i firewall. È possibile eseguire Cloud Manager nella subnet privata o nel data center. Quindi, avviare Cloud Volumes ONTAP nella subnet privata.



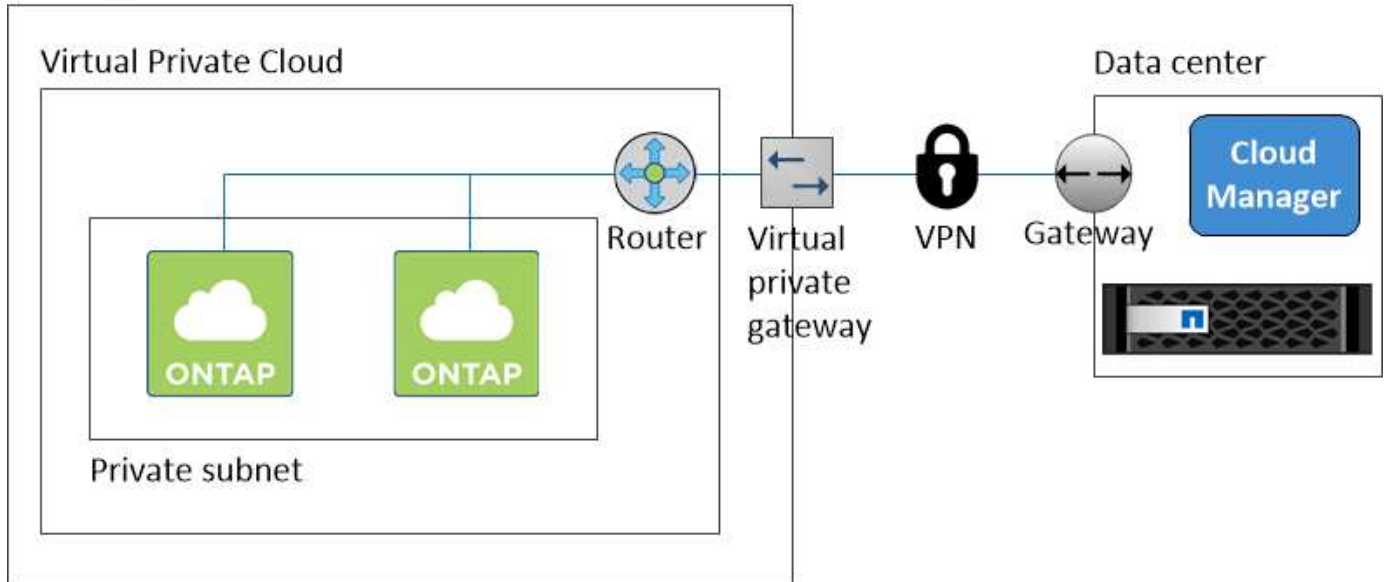
In questa configurazione è anche possibile utilizzare un server proxy per consentire l'accesso a Internet. Il server proxy può trovarsi nel data center o in AWS.

Se si desidera replicare i dati tra i sistemi FAS nel data center e i sistemi Cloud Volumes ONTAP in AWS, è necessario utilizzare una connessione VPN in modo che il collegamento sia sicuro.

Per ulteriori informazioni su questo scenario, fare riferimento a. "[Documentazione AWS: Scenario 4: Solo VPC con subnet privata e accesso VPN gestito da AWS](#)".

La seguente figura mostra Cloud Manager in esecuzione nel data center e nei sistemi a nodo singolo in esecuzione in una subnet privata:

AWS region



## Configurazione di un gateway di transito AWS per coppie ha in più AZS

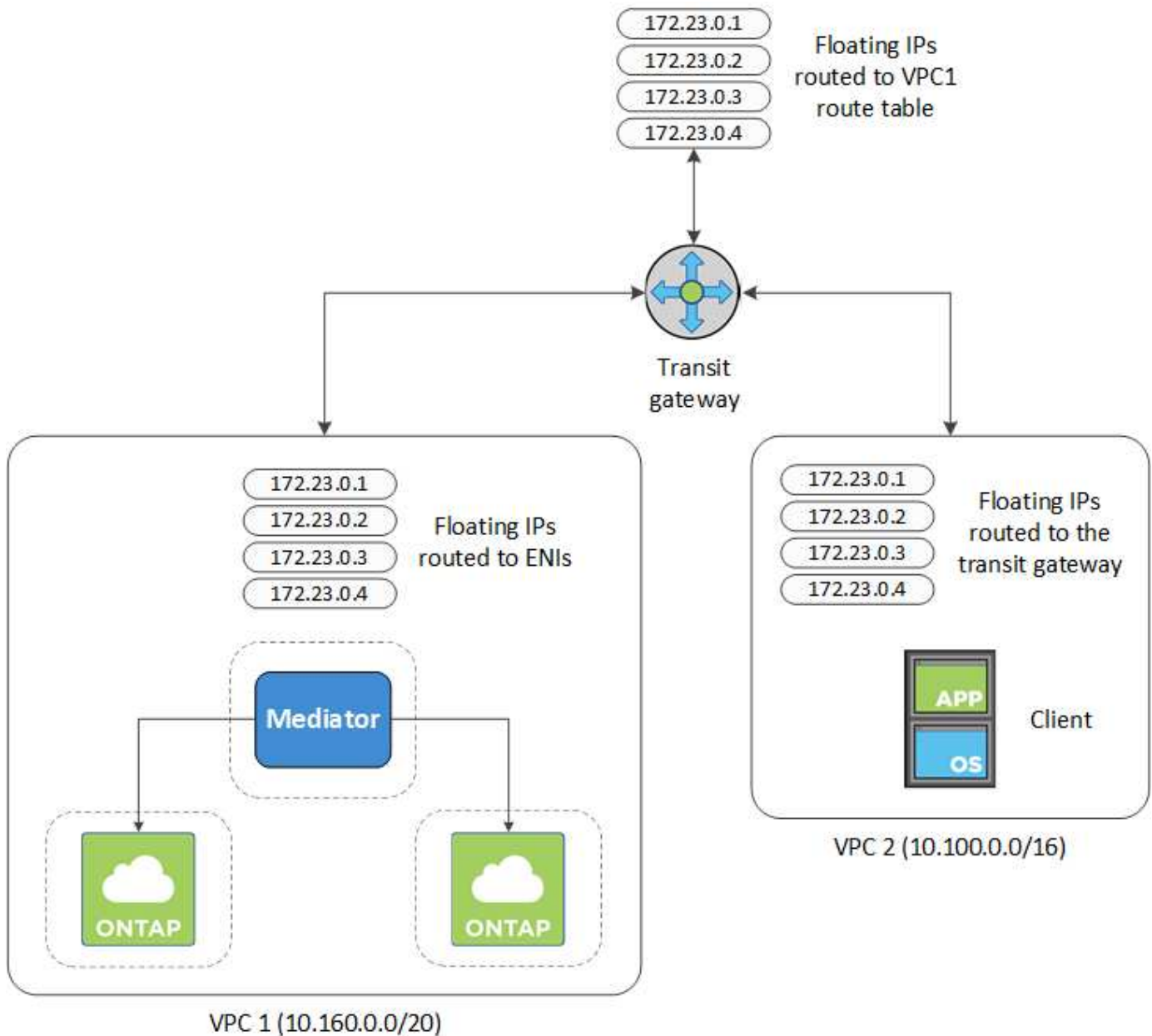
Impostare un gateway di transito AWS per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

Quando una configurazione Cloud Volumes ONTAP ha viene distribuita in più zone di disponibilità AWS, sono richiesti indirizzi IP mobili per l'accesso ai dati NAS dall'interno del VPC. Questi indirizzi IP mobili possono migrare tra i nodi in caso di guasti, ma non sono accessibili in modo nativo dall'esterno del VPC. Gli indirizzi IP privati separati forniscono l'accesso ai dati dall'esterno del VPC, ma non forniscono il failover automatico.

Gli indirizzi IP mobili sono richiesti anche per l'interfaccia di gestione del cluster e per la LIF di gestione SVM opzionale.

Se si imposta un gateway di transito AWS, si abilita l'accesso agli indirizzi IP mobili dall'esterno del VPC in cui risiede la coppia ha. Ciò significa che i client NAS e gli strumenti di gestione NetApp esterni al VPC possono accedere agli IP mobili.

Ecco un esempio che mostra due VPC connessi da un gateway di transito. Un sistema ha risiede in un VPC, mentre un client risiede nell'altro. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP mobile.



La seguente procedura illustra come configurare una configurazione simile.

### Fasi

1. "Creare un gateway di transito e collegare i VPC al gateway".
2. Creare le route nella tabella delle route del gateway di transito specificando gli indirizzi IP mobili della coppia ha.

Gli indirizzi IP mobili sono disponibili nella pagina Working Environment Information (informazioni sull'ambiente di lavoro) di Cloud Manager. Ecco un esempio:

## NFS & CIFS access from within the VPC using Floating IP

### Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

- Aggiungere voci di routing agli indirizzi IP mobili.
- Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

4. Modificare la tabella di routing per il VPC della coppia ha aggiungendo un percorso al VPC che richiede l'accesso agli indirizzi IP mobili.

Questo passaggio è importante perché completa il routing tra i VPC.

L'immagine di esempio seguente mostra la tabella di percorso per VPC 1. Include un routing agli indirizzi IP mobili e a VPC 2, che è dove risiede un client. Cloud Manager ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha implementato la coppia ha.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

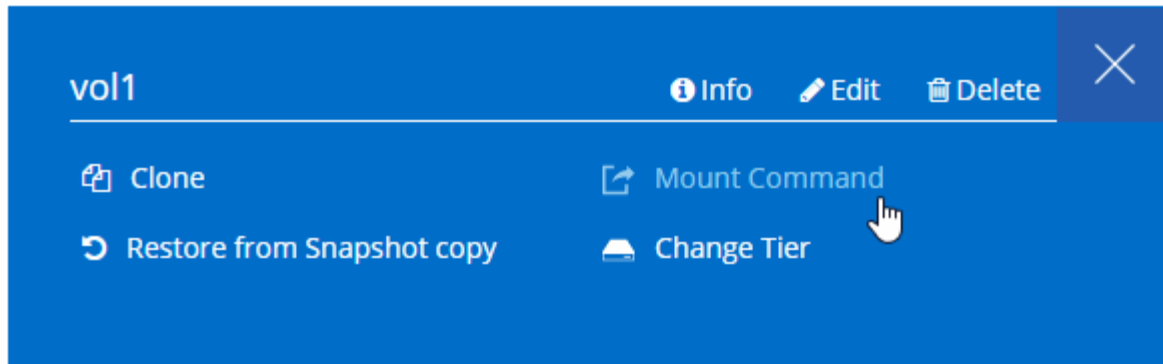
VPC2  
Floating act IP Addresses

5. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

È possibile trovare l'indirizzo IP corretto in Cloud Manager selezionando un volume e facendo clic su **Mount Command**.

# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



## Link correlati

- ["Coppie ad alta disponibilità in AWS"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in AWS"](#)

## Requisiti di rete per Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

### Accesso a Internet in uscita per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in maniera proattiva lo stato dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

### Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a. "[Regole del gruppo di sicurezza](#)".

### Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in Azure:

- Nodo singolo: 5 indirizzi IP
- Coppia HA: 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM sulle coppie ha, ma non sui sistemi a nodo singolo in Azure.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

### Connessione da Cloud Volumes ONTAP a Azure BLOB storage per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold allo storage Azure Blob, non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

Queste autorizzazioni sono incluse nella versione più recente ["Policy di Cloud Manager"](#).

Per ulteriori informazioni sull'impostazione del tiering dei dati, vedere ["Tiering dei dati cold su storage a oggetti a basso costo"](#).

### Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in Azure e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra Azure VNET e l'altra rete, ad esempio un VPC AWS o la rete aziendale.

Per istruzioni, fare riferimento a ["Documentazione di Microsoft Azure: Crea una connessione Site-to-Site nel portale Azure"](#).

## Requisiti di rete per Cloud Volumes ONTAP in GCP

Configura la tua rete della piattaforma cloud Google in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

### VPC condiviso

Cloud Manager e Cloud Volumes ONTAP sono supportati in un VPC condiviso con la piattaforma cloud Google.

Un VPC condiviso consente di configurare e gestire centralmente le reti virtuali in più progetti. È possibile configurare reti VPC condivise nel *progetto host* e implementare le istanze di Cloud Manager e macchina virtuale Cloud Volumes ONTAP in un *progetto di servizio*. ["Documentazione di Google Cloud: Panoramica VPC condivisa"](#).

L'unico requisito è fornire le seguenti autorizzazioni all'account di servizio Cloud Manager nel progetto host VPC condiviso:

```
compute.firewalls.* compute.networks.* compute.subnetworks.*
```

Cloud Manager necessita di queste autorizzazioni per eseguire query su firewall, VPC e subnet nel progetto host.

### Accesso a Internet in uscita per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in maniera proattiva lo stato dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

## Numero di indirizzi IP

Cloud Manager assegna 5 indirizzi IP a Cloud Volumes ONTAP in GCP.

Si noti che Cloud Manager non crea una LIF di gestione SVM per Cloud Volumes ONTAP in GCP.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

## Regole del firewall

Non è necessario creare regole firewall perché Cloud Manager fa tutto questo per te. Se è necessario utilizzare il proprio, fare riferimento a ["Regole del firewall GCP"](#).

## Connessione da Cloud Volumes ONTAP allo storage cloud Google per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold in un bucket di storage cloud Google, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a ["Documentazione di Google Cloud: Configurazione di Private Google Access"](#).

Per ulteriori passaggi necessari per impostare il tiering dei dati in Cloud Manager, consulta ["Tiering dei dati cold su storage a oggetti a basso costo"](#).

## Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in GCP e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra il VPC e l'altra rete, ad esempio la rete aziendale.

Per istruzioni, fare riferimento a ["Documentazione di Google Cloud: Panoramica di Cloud VPN"](#).

# Opzioni di implementazione aggiuntive

## Requisiti degli host di Cloud Manager

Se si installa Cloud Manager sul proprio host, è necessario verificare il supporto per la configurazione, che include i requisiti del sistema operativo, i requisiti delle porte e così via.



È possibile installare Cloud Manager sul proprio host in GCP, ma non nella rete on-premise. Cloud Manager deve essere installato in GCP per implementare Cloud Volumes ONTAP in GCP.

## È richiesto un host dedicato

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

## Tipi di istanze AWS EC2 supportati

- t2.medio
- t3.medium (consigliato)



- m4.large
- m5.xlarge
- m5.2xgrande
- m5.4xgrande
- m5.8xlarge

### **Dimensioni delle macchine virtuali Azure supportate**

A2, D2 v2 o D2 v3 (in base alla disponibilità)

### **Tipi di macchine GCP supportati**

Un tipo di macchina con almeno 2 vCPU e 4 GB di memoria.

### **Sistemi operativi supportati**

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

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 di Cloud Manager.

Cloud Manager 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 Linux <https://access.redhat.com/certified-hypervisors>["Soluzione Red Hat: Quali hypervisor sono certificati per eseguire Red Hat Enterprise Linux?"^]

### **CPU**

2.27 GHz o superiore con due core

### **RAM**

4 GB

### **Spazio libero su disco**

50 GB

### **Accesso a Internet in uscita**

L'accesso a Internet in uscita è necessario quando si installa Cloud Manager e quando si utilizza Cloud Manager per implementare Cloud Volumes ONTAP. Per un elenco degli endpoint, vedere "[Requisiti di rete per Cloud Manager](#)".

## Porte

Devono essere disponibili le seguenti porte:

- 80 per l'accesso HTTP
- 443 per l'accesso HTTPS
- 3306 per il database Cloud Manager
- 8080 per il proxy API Cloud Manager

Se altri servizi utilizzano queste porte, l'installazione di Cloud Manager non riesce.



Si è verificato un potenziale conflitto con la porta 3306. Se un'altra istanza di MySQL è in esecuzione sull'host, utilizza la porta 3306 per impostazione predefinita. È necessario modificare la porta utilizzata dall'istanza MySQL esistente.

Quando si installa Cloud Manager, è possibile modificare le porte HTTP e HTTPS predefinite. Non è possibile modificare la porta predefinita per il database MySQL. Se si modificano le porte HTTP e HTTPS, assicurarsi che gli utenti possano accedere alla console Web di Cloud Manager da un host remoto:

- Modificare il gruppo di sicurezza per consentire le connessioni in entrata attraverso le porte.
- Specificare la porta quando si immette l'URL nella console Web di Cloud Manager.

## Installazione di Cloud Manager su un host Linux esistente

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



È possibile installare Cloud Manager sul proprio host in GCP, ma non nella rete on-premise. Cloud Manager deve essere installato in GCP per implementare Cloud Volumes ONTAP in GCP.

### Prima di iniziare

- 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 di Cloud Manager.
- Il programma di installazione di Cloud Manager accede a diversi URL durante il processo di installazione. È necessario assicurarsi che l'accesso a Internet in uscita sia consentito a tali endpoint. Fare riferimento a ["Requisiti di rete per Cloud Manager"](#).

### A proposito di questa attività

- Per installare Cloud Manager non sono necessari i privilegi di root.
- Cloud Manager installa gli strumenti della riga di comando AWS (awscli) per abilitare le procedure di recovery dal supporto NetApp.

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

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

versione.

## Fasi

1. Verifica dei requisiti di rete:
  - ["Requisiti di rete per Cloud Manager"](#)
  - ["Requisiti di rete per Cloud Volumes ONTAP in AWS"](#)
  - ["Requisiti di rete per Cloud Volumes ONTAP in Azure"](#)
  - ["Requisiti di rete per Cloud Volumes ONTAP in GCP"](#)
2. Revisione ["Requisiti degli host di Cloud Manager"](#).
3. Scaricare il software dal ["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"](#).

4. Assegnare le autorizzazioni per eseguire lo script.

## Esempio

```
chmod +x OnCommandCloudManager-V3.7.0.sh
. Eseguire lo script di installazione:
```

```
./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

*silent* esegue l'installazione senza richiedere informazioni.

*Proxy* è richiesto se l'host Cloud Manager 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.

5. 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.

Se si modificano le porte HTTP e HTTPS, assicurarsi che gli utenti possano accedere alla console Web di Cloud Manager da un host remoto:

- Modificare il gruppo di sicurezza per consentire le connessioni in entrata attraverso le porte.
- Specificare la porta quando si immette l'URL nella console Web di Cloud Manager.

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.

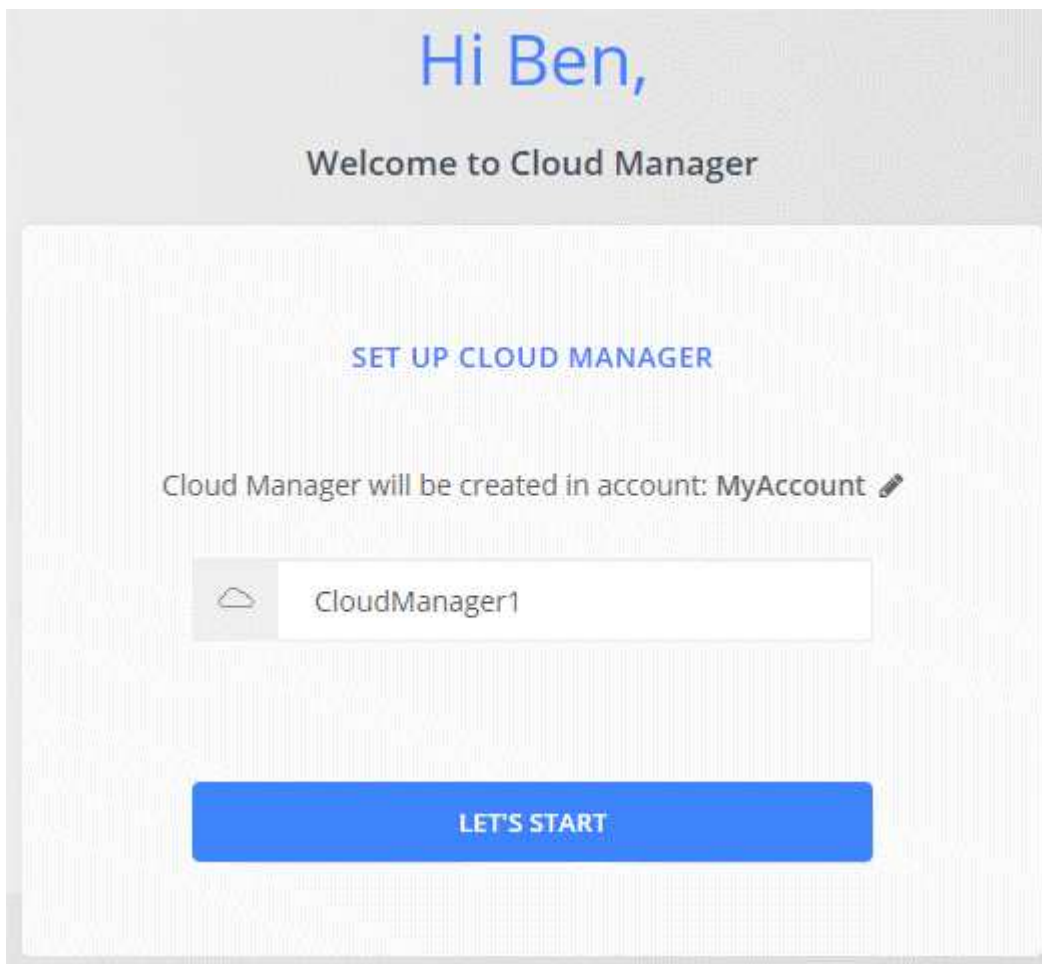
6. Aprire un browser Web e immettere il seguente URL:

`<a href="https://<em>ipaddress</em>:<em>port</em>" class="bare">https://<em>ipaddress</em>:<em>port</em></a>`

*Ipaddress* può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host Cloud Manager. Ad esempio, se Cloud Manager 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 Cloud Manager.

*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 `<a href="https://<em>ipaddress</em>:8443" class="bare">https://<em>ipaddress</em>:8443</a>`

7. Iscriviti a NetApp Cloud Central o effettua l'accesso.
8. Dopo aver effettuato l'accesso, configurare Cloud Manager:
  - a. Specificare l'account Cloud Central da associare al sistema Cloud Manager.  
["Scopri di più sugli account Cloud Central"](#).
  - b. Immettere un nome per il sistema.



#### **Al termine**

Imposta le autorizzazioni in modo che Cloud Manager possa implementare Cloud Volumes ONTAP nel tuo cloud provider:

- 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 Cloud Manager"](#).
  - 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.

## Avvio di Cloud Manager da AWS Marketplace

Si consiglia di avviare Cloud Manager in AWS utilizzando ["NetApp Cloud Central"](#), Ma è possibile avviarlo da AWS Marketplace, se necessario.



Se lanciate Cloud Manager da AWS Marketplace, Cloud Manager è ancora integrato con NetApp Cloud Central. ["Scopri di più sull'integrazione"](#).

### A proposito di questa attività

La seguente procedura descrive 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).

### 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. ["Iscriviti a AWS Marketplace"](#) Per garantire che non si verificano interruzioni del servizio al termine della prova gratuita di Cloud Volumes ONTAP. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata.
3. Passare alla ["Pagina Cloud Manager su AWS Marketplace"](#) Per implementare Cloud Manager da un AMI.
4. Nella pagina Marketplace, fare clic su **Continue to Subscribe**, quindi fare clic su **Continue to Configuration**.
5. Modificare una delle opzioni predefinite e fare clic su **Continue to Launch** (continua fino all'avvio).
6. In **Choose Action** (Scegli azione), selezionare **Launch through EC2** (Avvia tramite EC2\*), quindi fare clic su **Launch** (Avvia).
7. 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.medium).

["Esaminare l'elenco dei tipi di istanze supportati"](#).

- **Configure Instance** (Configura istanza): Selezionare un VPC e una subnet, il ruolo IAM creato al punto 1 e altre opzioni di configurazione che soddisfano i requisiti.

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option  Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)  
251 IP Addresses available

Auto-assign Public IP

Placement group  Add instance to placement group

Capacity Reservation  [Create new Capacity Reservation](#)

**IAM role**  [Create new IAM role](#)

- **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**: Specificare i metodi di connessione richiesti per l'istanza di Cloud Manager: SSH, HTTP e HTTPS.
- **Revisione**: Rivedere le selezioni e fare clic su **Avvia**.

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

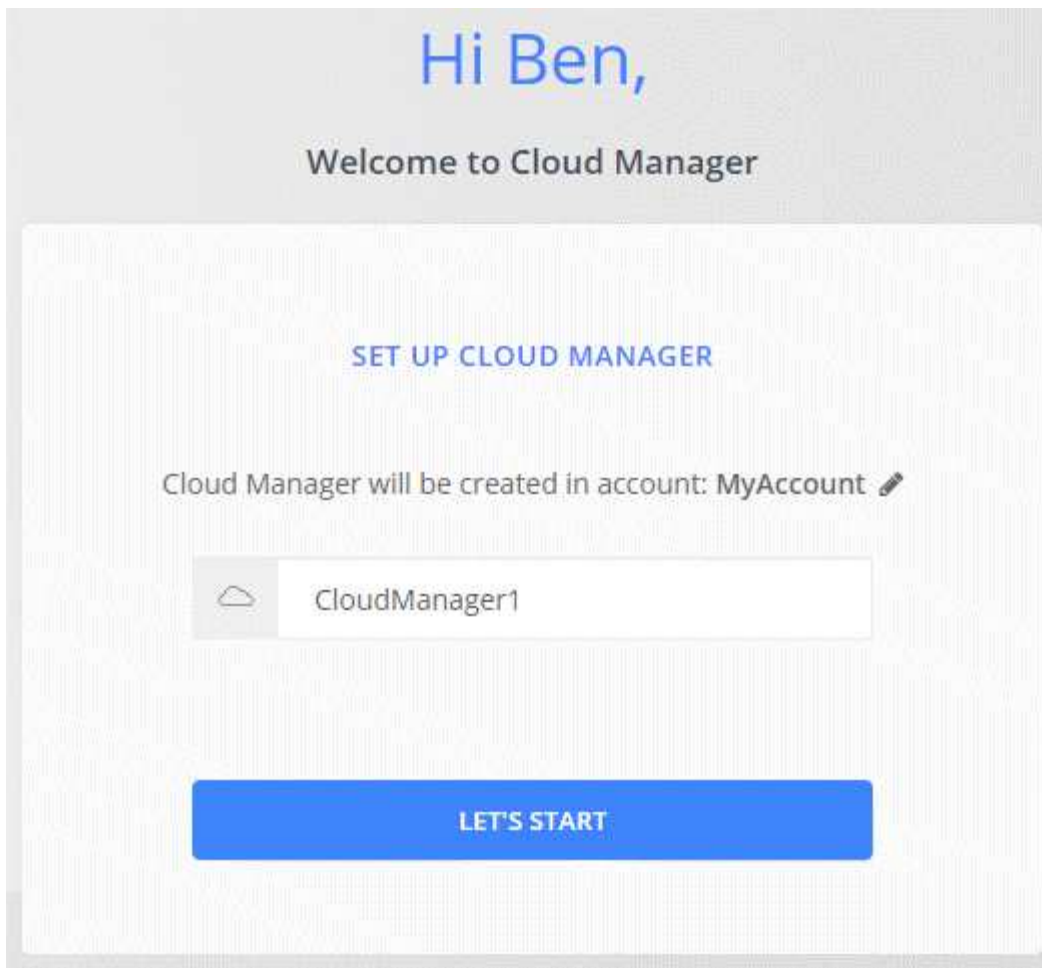
8. Aprire un browser Web da un host connesso alla macchina virtuale Cloud Manager e immettere il seguente URL:

`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

9. Dopo aver effettuato l'accesso, configurare Cloud Manager:
  - a. Specificare l'account Cloud Central da associare al sistema Cloud Manager.

["Scopri di più sugli account Cloud Central"](#).

- b. Immettere un nome per il sistema.



### Risultato

Cloud Manager è ora installato e configurato.

### Implementazione di Cloud Manager da Azure Marketplace

Si consiglia di implementare Cloud Manager in Azure utilizzando ["NetApp Cloud Central"](#), Ma è possibile implementarlo da Azure Marketplace, se necessario.

Sono disponibili istruzioni separate per implementare Cloud Manager in ["Aree pubbliche degli Stati Uniti Azure"](#) e in ["Regioni Azure Germania"](#).



Se si implementa Cloud Manager da Azure Marketplace, Cloud Manager è ancora integrato con NetApp Cloud Central. ["Scopri di più sull'integrazione"](#).

### Implementazione di Cloud Manager in Azure

Devi installare e configurare Cloud Manager per poterlo utilizzare per avviare Cloud Volumes ONTAP in Azure.

#### 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.
- Scegliere una delle dimensioni consigliate per le macchine virtuali: A2, D2 v2 o D2 v3 (in base alla disponibilità).
- Per il gruppo di sicurezza della rete, Cloud Manager richiede connessioni in entrata utilizzando SSH, HTTP e HTTPS.

["Scopri di più sulle regole dei gruppi di sicurezza per Cloud Manager"](#).

- In **Management**, abilitare **System Assigned Managed Identity** per Cloud Manager selezionando **on**.

Questa impostazione è importante perché un'identità gestita consente alla macchina virtuale Cloud Manager 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 Cloud Manager dovrebbero essere in esecuzione in circa cinque minuti.

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

`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

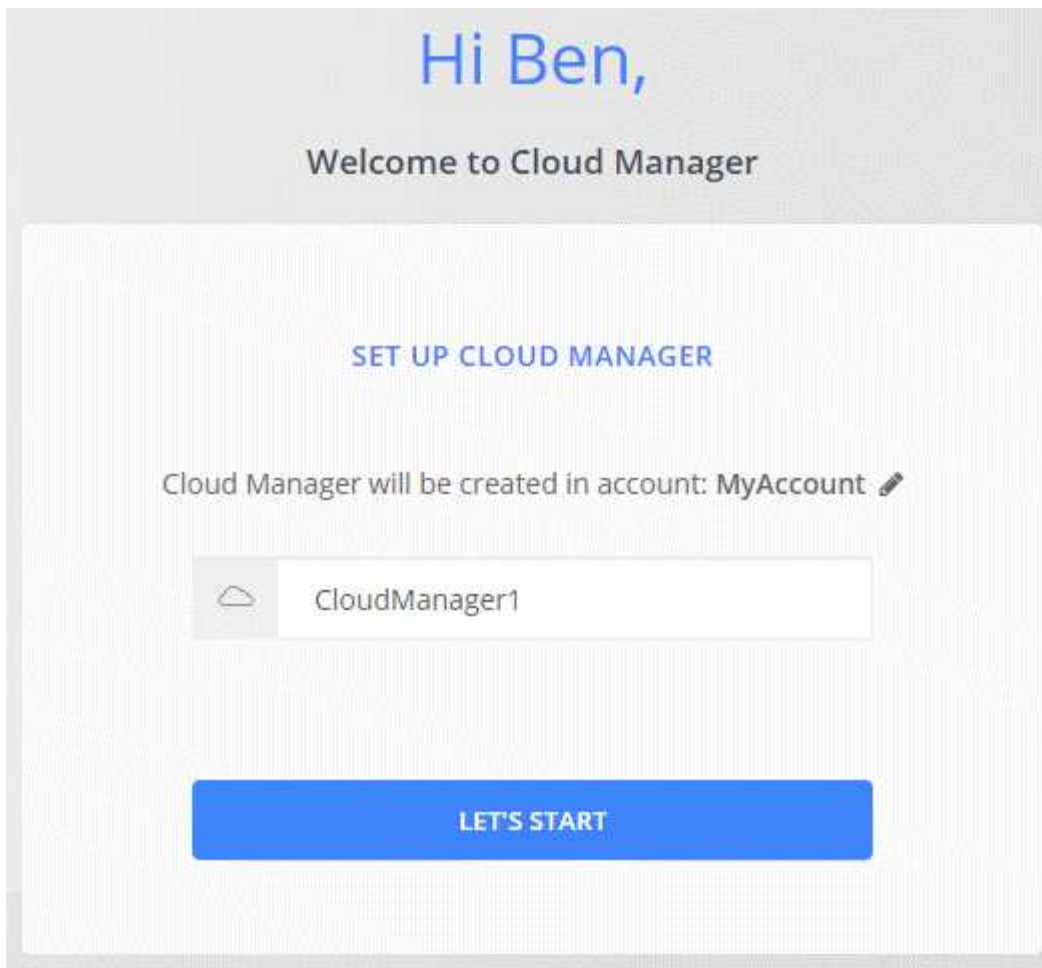
6. Dopo aver effettuato l'accesso, configurare Cloud Manager:

- a. Specificare l'account Cloud Central da associare al sistema Cloud Manager.

["Scopri di più sugli account Cloud Central"](#).

- b. Immettere un nome per il sistema.





### Risultato

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

### Concessione delle autorizzazioni Azure a Cloud Manager

Quando hai implementato Cloud Manager in Azure, dovresti aver attivato una ["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 Cloud Manager 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-  
9bzzbce5bzzbce5bce5bzzbce5bce5b5b
```

- 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_3.7.4.json
```

Ora dovresti avere un ruolo personalizzato chiamato operatore cloud manager di OnCommand che puoi assegnare alla macchina virtuale di Cloud Manager.

2. Assegnare il ruolo alla macchina virtuale Cloud Manager 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 **operatore cloud OnCommand**.



L'operatore di gestione cloud di OnCommand 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 Cloud Manager.
  - Selezionare la macchina virtuale Cloud Manager.
  - 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

Cloud Manager dispone ora delle autorizzazioni necessarie per implementare e gestire Cloud Volumes ONTAP in Azure.

## Implementazione di Cloud Manager in un'area governativa statunitense di Azure

Per attivare Cloud Manager in un'area governativa degli Stati Uniti, è necessario innanzitutto implementare Cloud Manager da Azure Government Marketplace. Fornire quindi le autorizzazioni necessarie a Cloud Manager per implementare e gestire i sistemi Cloud Volumes ONTAP.

Per un elenco delle regioni governative statunitensi Azure supportate, vedere "[Cloud Volumes Global Regions](#)".

## Implementazione di Cloud Manager da Azure US Government Marketplace

Cloud Manager è disponibile come immagine in Azure US Government Marketplace.

## Fasi

1. Assicurati che Azure Government Marketplace sia attivato nel tuo abbonamento:
  - a. Accedere al portale come amministratore aziendale.

- b. Selezionare **Manage** (Gestisci).
- c. In **Dettagli registrazione**, fare clic sull'icona a forma di matita accanto a **Azure Marketplace**.
- d. Selezionare **Enabled**.
- e. Fare clic su **Save** (Salva).

["Documentazione di Microsoft Azure: Azure Government Marketplace"](#)

2. Cerca OnCommand Cloud Manager nel portale per il governo degli Stati Uniti.
3. 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.
- Scegliere una delle dimensioni consigliate per le macchine virtuali: A2, D2 v2 o D2 v3 (in base alla disponibilità).
- Per il gruppo di sicurezza di rete, è consigliabile scegliere **Avanzate**.

L'opzione **Advanced** crea un nuovo gruppo di sicurezza che include le regole in entrata richieste per Cloud Manager. Se si sceglie Basic (base), fare riferimento a ["Regole del gruppo di sicurezza"](#) per l'elenco delle regole richieste.

4. Nella pagina di riepilogo, esaminare le selezioni e fare clic su **Create** (Crea) per avviare l'implementazione.

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

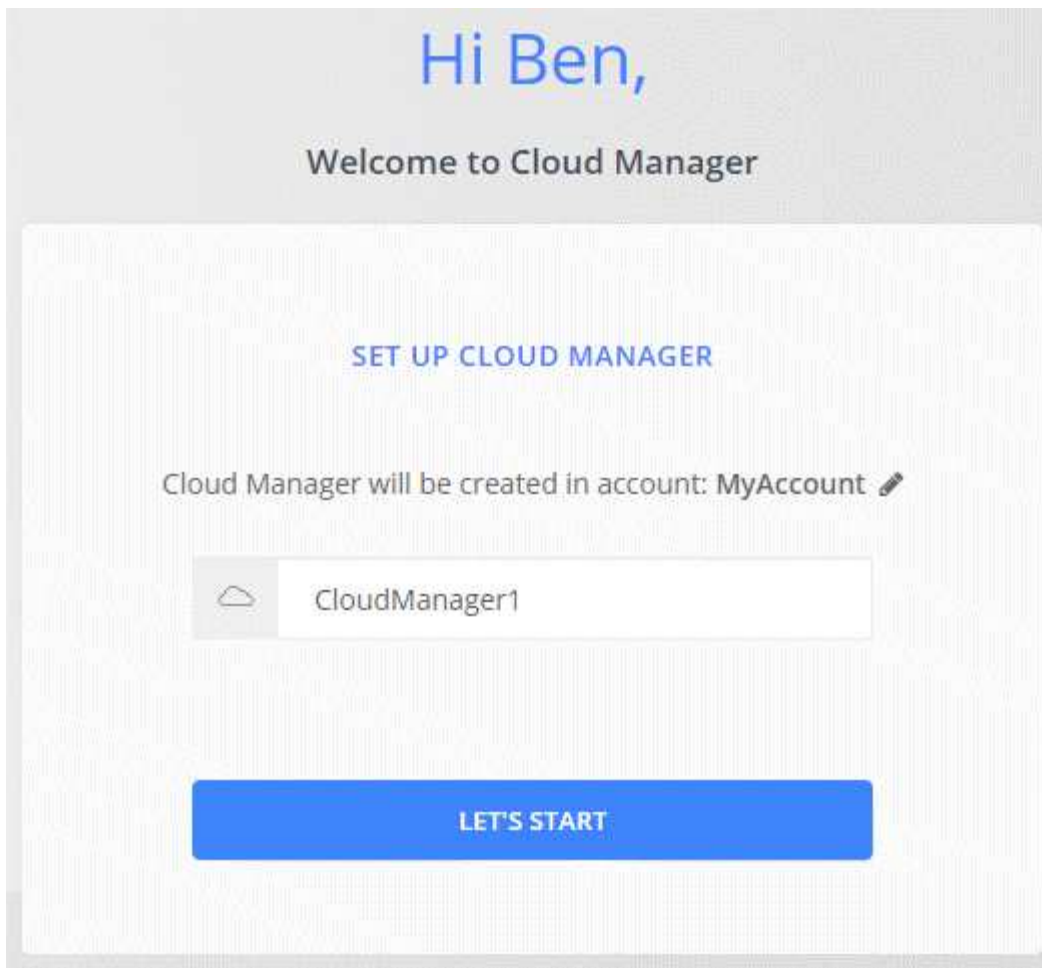
5. Aprire un browser Web da un host connesso alla macchina virtuale Cloud Manager e immettere il seguente URL:

`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

6. Dopo aver effettuato l'accesso, configurare Cloud Manager:
  - a. Specificare l'account Cloud Central da associare al sistema Cloud Manager.

["Scopri di più sugli account Cloud Central"](#).

- b. Immettere un nome per il sistema.



## Risultato

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

## Concessione delle autorizzazioni Azure a Cloud Manager utilizzando un'identità gestita

Il modo più semplice per fornire le autorizzazioni consiste nell'attivare un "identità gestita" Sulla macchina virtuale Cloud Manager, quindi assegnando le autorizzazioni necessarie alla macchina virtuale. Se si preferisce, un metodo alternativo è quello di ["Concedere le autorizzazioni ad Azure utilizzando un'entità del servizio"](#).

## Fasi

1. Abilitare un'identità gestita sulla macchina virtuale Cloud Manager:
  - a. Accedere alla macchina virtuale Cloud Manager e selezionare **Identity**.
  - b. In **System Assigned** (sistema assegnato), fare clic su **on**, quindi su **Save** (Salva).
2. 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-  
9bzzbce5bzzbce5bce5bzzbce5bce5b5b
```

- 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_3.7.4.json
```

Ora dovresti avere un ruolo personalizzato chiamato operatore cloud manager di OnCommand che puoi assegnare alla macchina virtuale di Cloud Manager.

3. Assegnare il ruolo alla macchina virtuale Cloud Manager 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**, fare clic su **Aggiungi assegnazione ruolo**, quindi aggiungere le autorizzazioni:
    - Selezionare il ruolo **operatore cloud OnCommand**.



L'operatore di gestione cloud di OnCommand 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 Cloud Manager.
  - Digitare il nome della macchina virtuale e selezionarlo.
  - 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

Cloud Manager dispone ora delle autorizzazioni necessarie per implementare e gestire Cloud Volumes ONTAP in Azure.

## Installazione di Cloud Manager in una regione di Azure Germania

Azure Marketplace non è disponibile nelle regioni di Azure Germany, pertanto è necessario scaricare il programma di installazione di Cloud Manager dal sito di supporto NetApp e installarlo su un host Linux esistente nella regione.

## Fasi

1. ["Esaminare i requisiti di rete per Azure"](#).
2. ["Esaminare i requisiti degli host di Cloud Manager"](#).
3. ["Scarica e installa Cloud Manager"](#).
4. ["Concedere le autorizzazioni Azure a Cloud Manager utilizzando un'entità del servizio"](#).

**Al termine**

Cloud Manager è ora pronto per implementare Cloud Volumes ONTAP nella regione di Azure Germania, proprio come in qualsiasi altra regione. Tuttavia, potrebbe essere necessario eseguire prima un'ulteriore configurazione.

## **Mantenere operativo Cloud Manager**

Cloud Manager deve rimanere sempre in esecuzione.

Cloud Manager è un componente chiave per lo stato di salute e la fatturazione di Cloud Volumes ONTAP. Se Cloud Manager viene spento, i sistemi Cloud Volumes ONTAP si spegneranno dopo aver perso la comunicazione con Cloud Manager per più di 4 giorni.

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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