# Configurazione di Cloud Manager

## Cloud Manager 3.6

NetApp
March 25, 2024

# Sommario

Configurazione di Cloud Manager . . . . . 1
Aggiunta di account cloud provider a Cloud Manager . . . . . 1
Aggiunta di account NetApp Support Site a Cloud Manager . . . . . 10
Installazione di un certificato HTTPS per un accesso sicuro . . . . . 11
Configurazione di utenti e tenant . . . . . 12
Configurazione di AWS KMS . . . . . 13

# Configurazione di Cloud Manager

## Aggiunta di account cloud provider a Cloud Manager

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

Quando si implementa Cloud Manager da Cloud Central, Cloud Manager aggiunge automaticamente un "account cloud provider" Per l'account in cui hai implementato Cloud Manager. Se il software Cloud Manager è stato installato manualmente su un sistema esistente, non viene aggiunto un account di provider cloud iniziale.

### 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 a tali account 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.

- Concessione delle autorizzazioni quando si forniscono le chiavi AWS
- Concessione delle autorizzazioni assumendo ruoli IAM in altri account

#### Concessione delle autorizzazioni quando si forniscono 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.

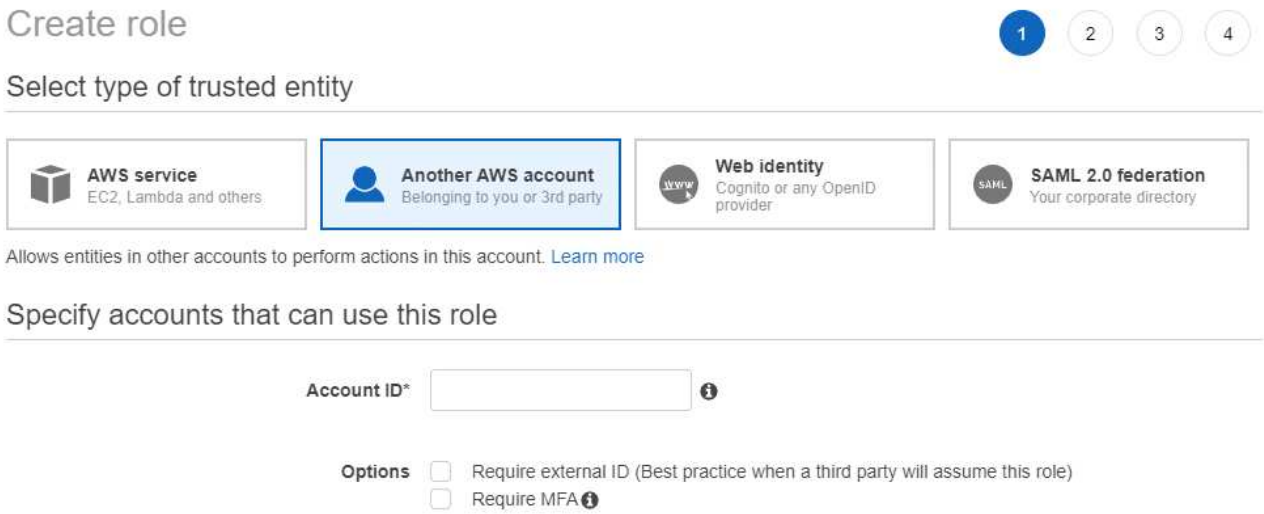
**Fasi**

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".




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

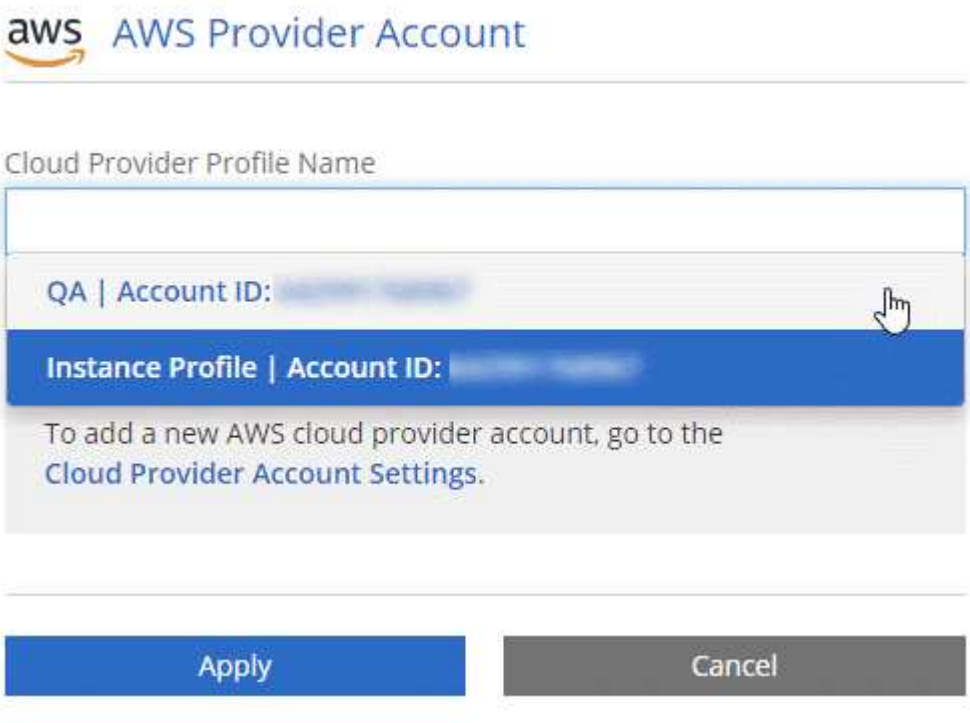
Dopo aver fornito un account AWS con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

**Fasi**

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Impostazioni account**.
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.

- Concessione delle autorizzazioni di Azure mediante un'entità del servizio
- Aggiunta di account Azure a Cloud Manager

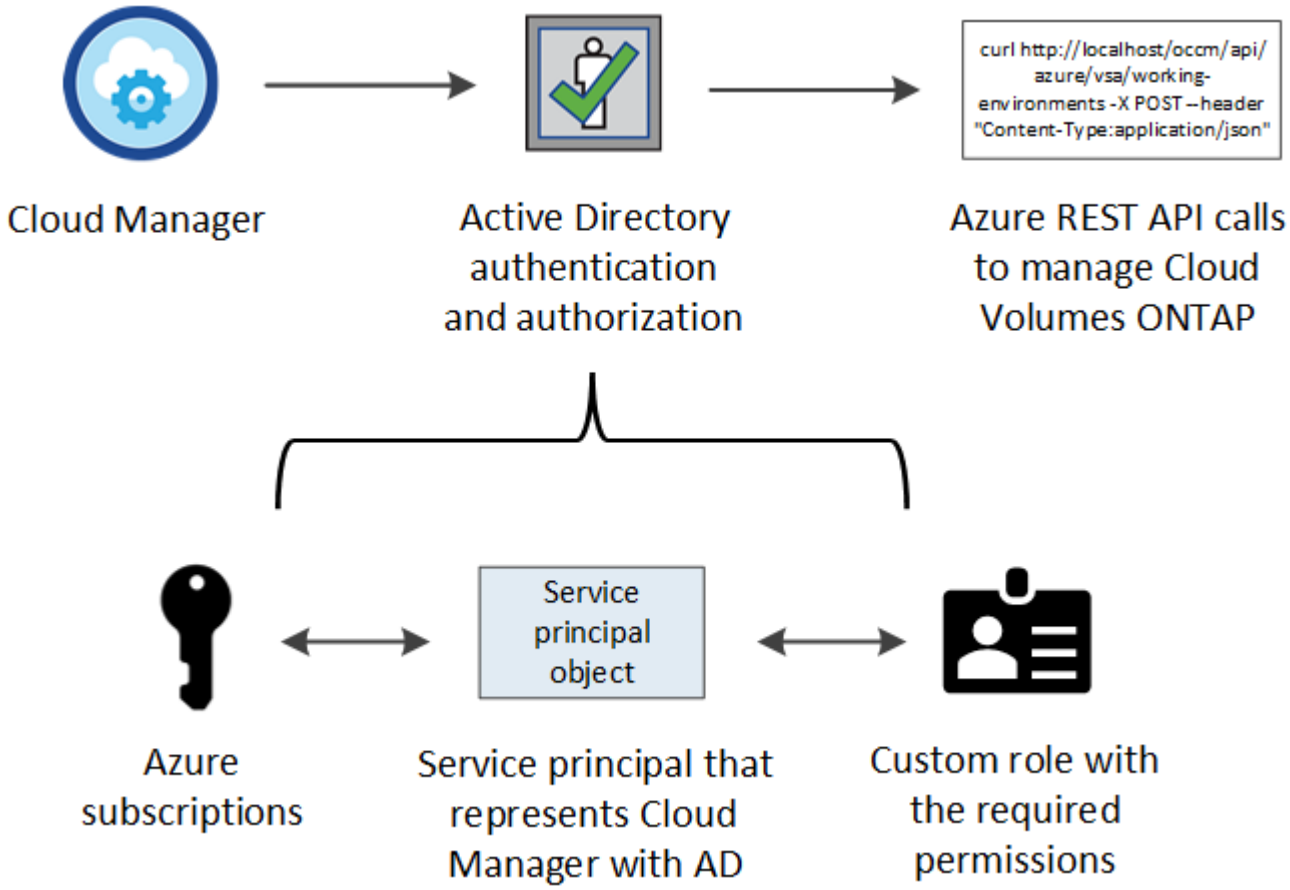
### Concessione delle autorizzazioni di Azure mediante un'entità del servizio

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.




La procedura seguente utilizza il nuovo portale Azure. In caso di problemi, utilizzare il portale Azure classic.

**Fasi**

1. Creare un ruolo personalizzato con le autorizzazioni di Cloud Manager richieste.
2. Creare un'entità del servizio Active Directory.
3. Assegnare il ruolo personalizzato di Cloud Manager Operator all'entità del servizio.

#### Creazione di un ruolo personalizzato con le autorizzazioni di Cloud Manager richieste

È necessario un ruolo personalizzato per fornire a Cloud Manager le autorizzazioni necessarie per avviare e gestire Cloud Volumes ONTAP in Azure.

**Fasi**

1. Scaricare il "Policy di Cloud Manager Azure".
2. 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"
```

3. 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_3.6.1.json**

**Risultato**

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

#### Creazione di un'entità del servizio Active Directory

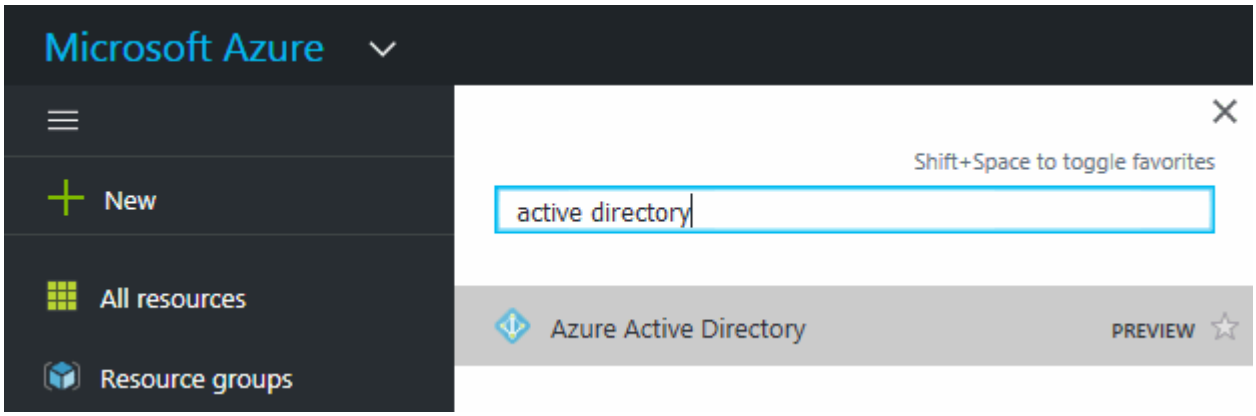
È necessario creare un'entità del servizio Active Directory in modo che Cloud Manager possa autenticarsi con Azure Active Directory.

**Prima di iniziare**

È necessario disporre delle autorizzazioni appropriate in Azure per creare un'applicazione Active Directory e assegnarla a un ruolo. Per ulteriori informazioni, fare riferimento a. "Documentazione di Microsoft Azure: Utilizza il portale per creare un'applicazione Active Directory e un service principal in grado di accedere alle risorse".

**Fasi**

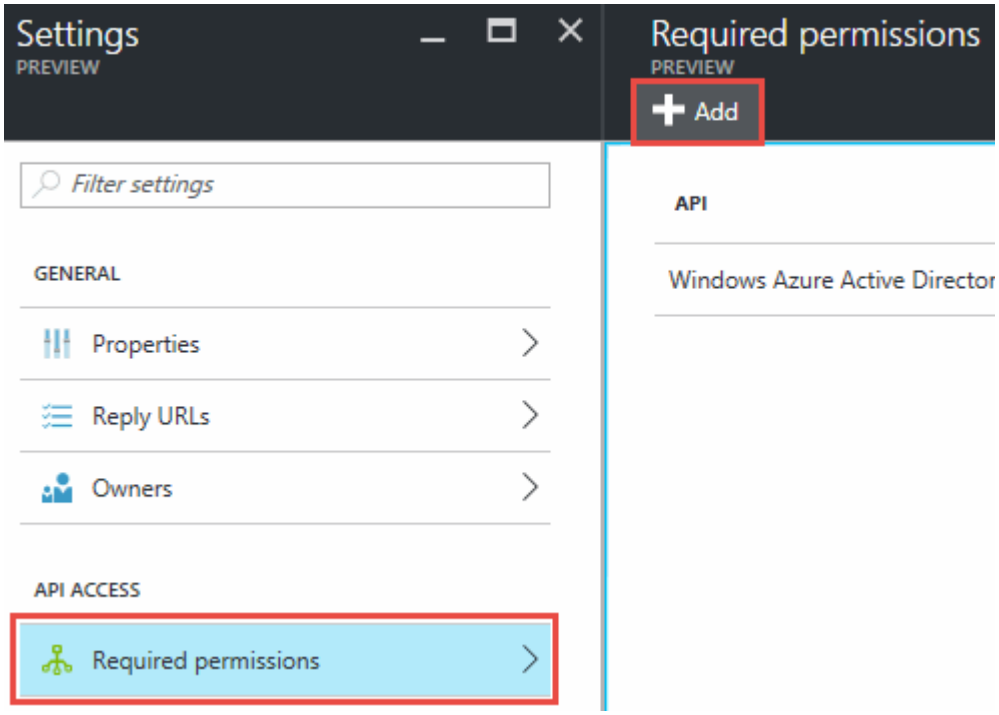
1. Dal portale Azure, aprire il servizio **Azure Active Directory**.



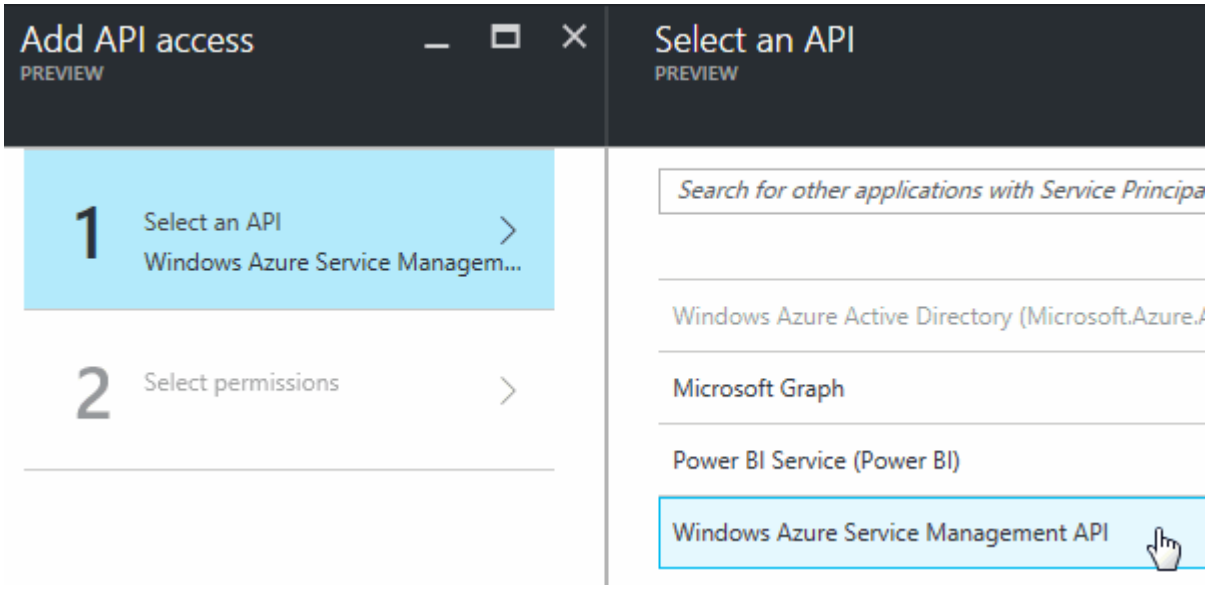

2. Nel menu, fare clic su **App Registrations (Legacy)**.
3. Creare l'entità del servizio:
   a. Fare clic su **Nuova registrazione applicazione**.
   b. Immettere un nome per l'applicazione, mantenere selezionata l'opzione **Web app/API**, quindi immettere un URL, ad esempio http://url
   c. Fare clic su **Create** (Crea).
4. Modificare l'applicazione per aggiungere le autorizzazioni richieste:

a. Selezionare l'applicazione creata.

b. In Impostazioni, fare clic su **autorizzazioni richieste**, quindi fare clic su **Aggiungi**.




c. Fare clic su **Select an API** (Seleziona un'API), selezionare **Windows Azure Service Management API**, quindi fare clic su **Select** (Seleziona).




d. Fare clic su **Access Azure Service Management as organization users** (Accedi a Azure Service Management come utenti dell'organizzazione), fare clic su **Select** (Seleziona), quindi su **Done** (fine)

5. Creare una chiave per l'entità del servizio:

a. In Impostazioni, fare clic su **chiavi**.

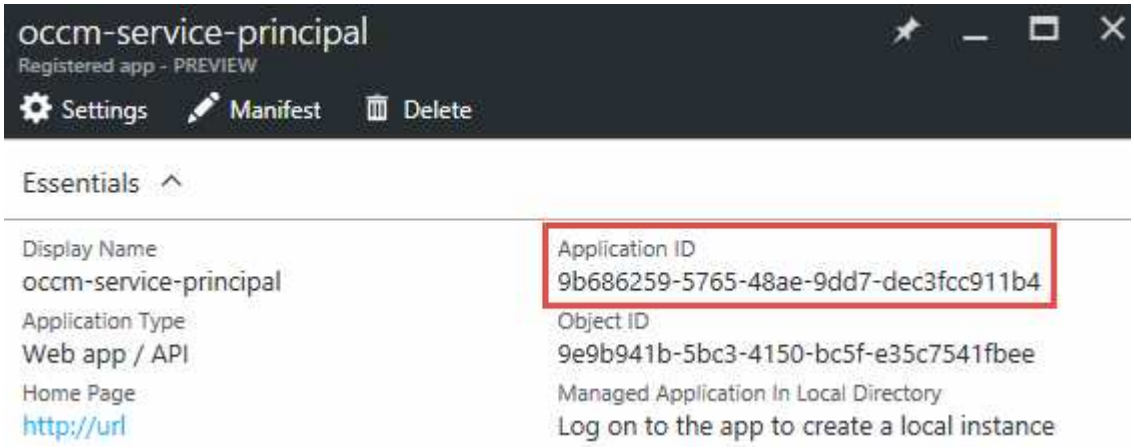
b. Inserire una descrizione, selezionare una durata, quindi fare clic su **Salva**.

c. Copiare il valore della chiave.

Quando Aggiungi un account cloud provider a Cloud Manager, devi inserire il valore della chiave.

d. Fare clic su **Proprietà**, quindi copiare l'ID dell'applicazione per l'entità del servizio.

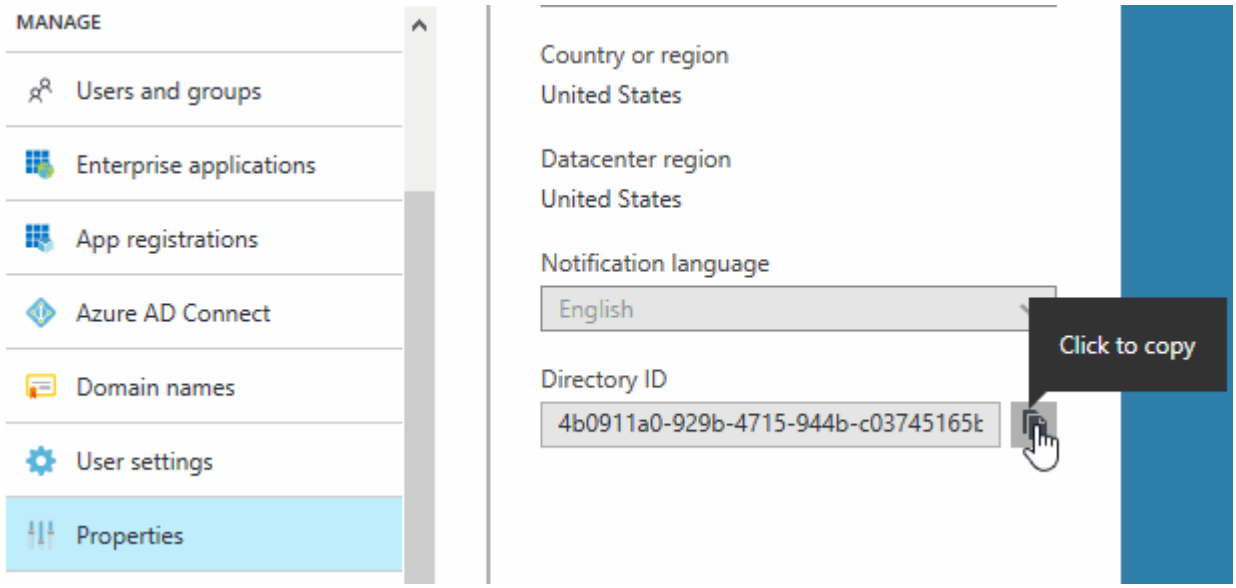
Analogamente al valore della chiave, è necessario inserire l'ID dell'applicazione in Cloud Manager quando si aggiunge un account del provider cloud a Cloud Manager.




6. Ottenere l'ID del tenant Active Directory per la propria organizzazione:

a. Nel menu Active Directory, fare clic su **Proprietà**.

b. Copiare l'ID della directory.




Proprio come l'ID dell'applicazione e la chiave dell'applicazione, è necessario inserire l'ID tenant di Active Directory quando si aggiunge un account del provider cloud a Cloud Manager.

**Risultato**

A questo punto, si dovrebbe disporre di un'entità del servizio Active Directory e copiare l'ID dell'applicazione, la chiave dell'applicazione e l'ID del tenant Active Directory. Devi inserire queste informazioni in Cloud Manager quando Aggiungi un account cloud provider.

#### Assegnazione del ruolo Cloud Manager Operator all'entità del servizio

È necessario associare l'entità del servizio a una o più sottoscrizioni Azure e assegnarle il ruolo Cloud Manager Operator in modo che Cloud Manager disponga delle autorizzazioni in Azure.

**A proposito di questa attività**

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.

**Fasi**

1. Dal portale Azure, selezionare **Subscriptions** (Abbonamenti) nel riquadro di sinistra.
2. Selezionare l'abbonamento.
3. Fare clic su **Access Control (IAM)**, quindi su **Add**.
4. Selezionare il ruolo **operatore cloud OnCommand**.
5. Cercare il nome dell'applicazione (non è possibile trovarla nell'elenco scorrendo).
6. Selezionare l'applicazione, fare clic su **Select**, quindi fare clic su **OK**.

**Risultato**

L'entità del servizio per Cloud Manager dispone ora delle autorizzazioni Azure richieste.

### Aggiunta di account Azure a Cloud Manager

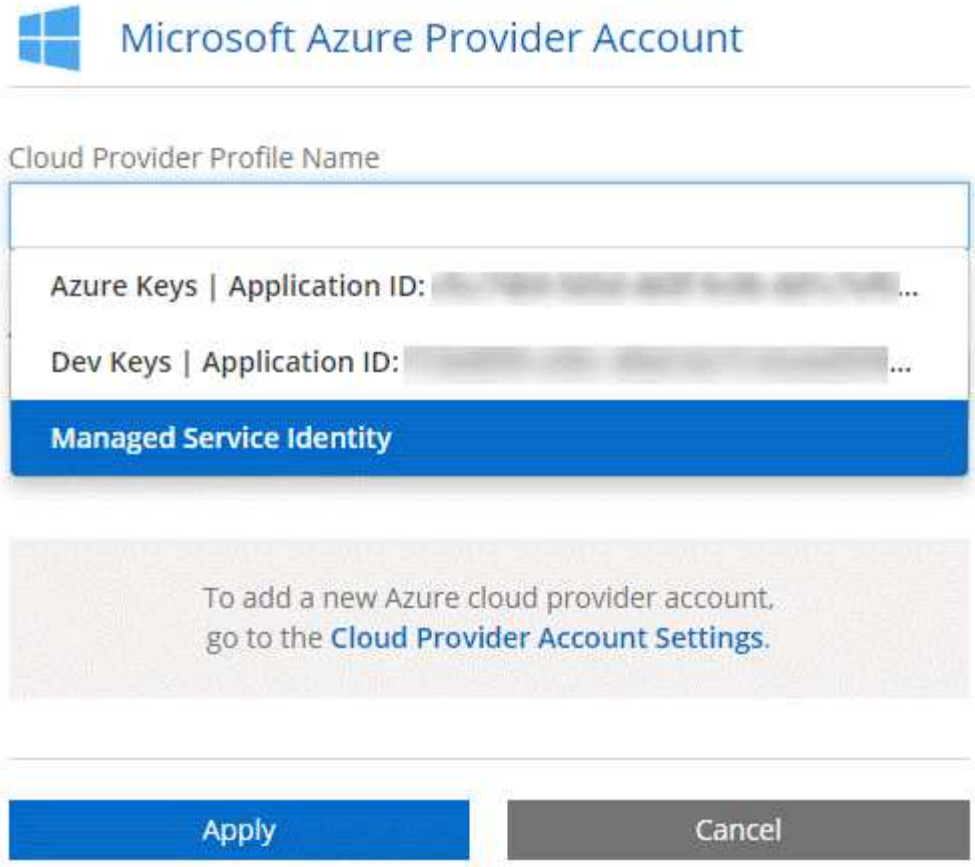
Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

**Fasi**

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Impostazioni account**.
2. Fare clic su **Aggiungi nuovo account** e selezionare **Microsoft Azure**.
3. Immettere le informazioni sull'entità del servizio Azure Active Directory che concede le autorizzazioni richieste.
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:




## 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'iniziale "account cloud provider" 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**.

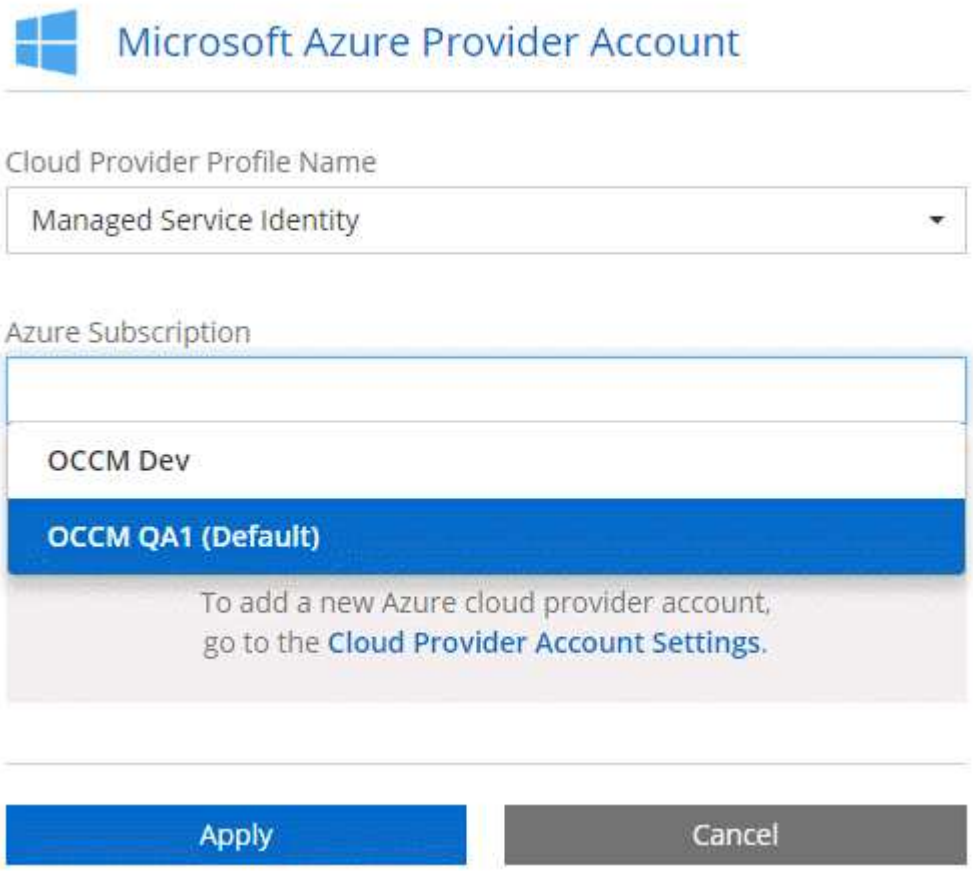
> L'operatore di gestione cloud di OnCommand è il nome predefinito fornito in "Policy di Cloud Manager". Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

- 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.




# 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'elenco a discesa delle attività, quindi selezionare **Impostazioni account**.
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**

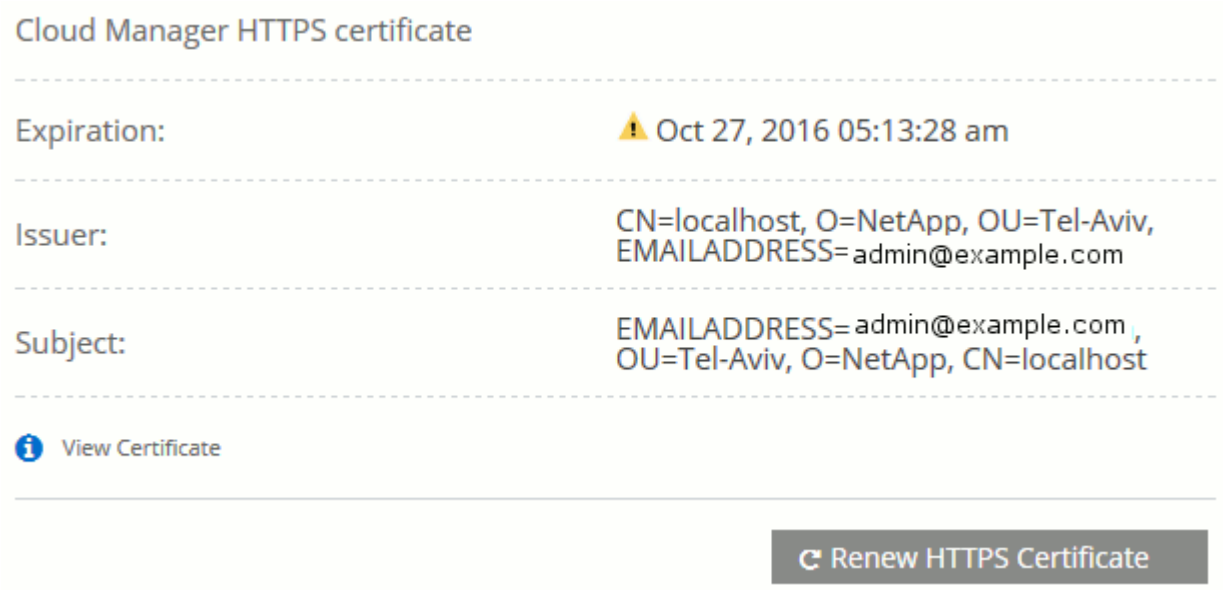
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **HTTPS Setup**.
2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio certificato firmato dalla CA:

| Opzione | Descrizione |
|---|---|
| Generare una CSR | a. Inserire il nome host o il DNS dell'host Cloud Manager (nome comune), quindi fare clic su **generate CSR** (genera CSR).<br><br>Cloud Manager visualizza una richiesta di firma del certificato.<br><br>b. Utilizzare la CSR per inviare una richiesta di certificato SSL a una CA.<br><br>Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.<br><br>c. Copiare il contenuto del certificato firmato, incollarlo nel campo certificato, quindi fare clic su **Installa**. |

| Opzione | Descrizione |
| --- | --- |
| Installare il proprio certificato firmato dalla CA | a. Selezionare **Installa certificato firmato dalla CA**.<br>b. Caricare il file del certificato e la chiave privata, quindi fare clic su **Installa**.<br>Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64. |

**Risultato**

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




# Configurazione di utenti e tenant

Cloud Manager consente di aggiungere altri utenti Cloud Central a Cloud Manager e di isolare gli ambienti di lavoro utilizzando i tenant.

## Aggiunta di utenti a Cloud Manager

Se altri utenti devono utilizzare il sistema Cloud Manager, devono iscriversi a un account in NetApp Cloud Central. È quindi possibile aggiungere gli utenti a Cloud Manager.

**Fasi**

1. Se l'utente non dispone ancora di un account in NetApp Cloud Central, invia un link al tuo sistema Cloud Manager e fai in modo che si iscriva.

   Attendere che l'utente confermi di aver effettuato la registrazione a un account.

2. In Cloud Manager, fare clic sull'icona dell'utente, quindi fare clic su **View Users** (Visualizza utenti).
3. Fare clic su **New User** (nuovo utente).
4. Inserire l'indirizzo e-mail associato all'account utente, selezionare un ruolo e fare clic su **Aggiungi**.

**Quali sono le prossime novità?**

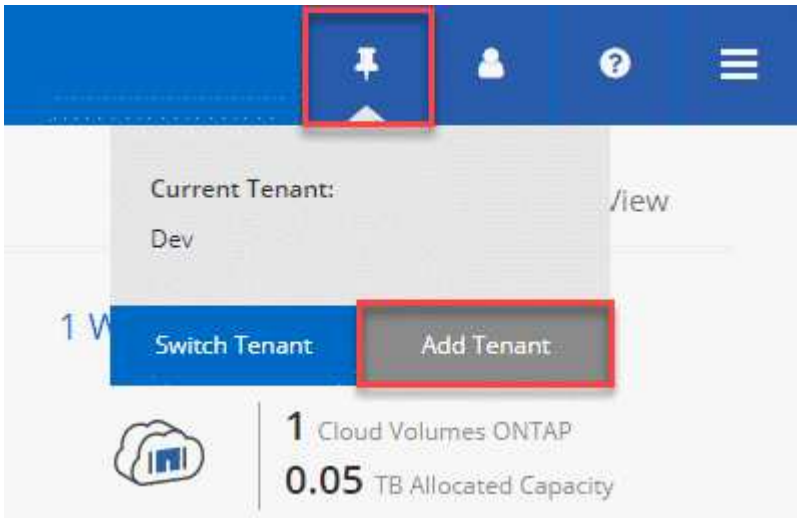
Informare l'utente che ora può accedere al sistema Cloud Manager.

## Creazione di tenant

I tenant consentono di isolare gli ambienti di lavoro in gruppi separati. Si creano uno o più ambienti di lavoro all'interno di un tenant. "Scopri di più sui tenant".

**Fasi**

1. Fare clic sull'icona dei tenant, quindi su **Aggiungi tenant**.




2. Immettere un nome, una descrizione e un centro di costo, se necessario.
3. Fare clic su **Save** (Salva).

**Quali sono le prossime novità?**

Ora puoi passare a questo nuovo tenant e aggiungere gli amministratori tenant e gli amministratori dell'ambiente di lavoro a questo tenant.

# 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.

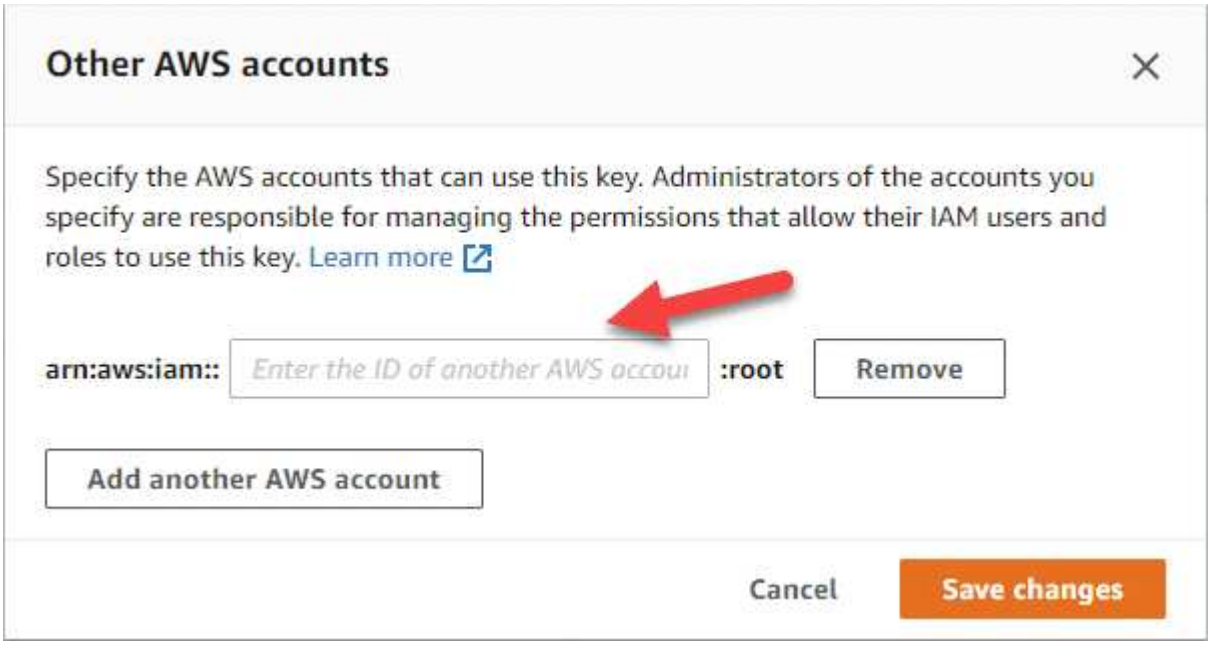
   b. Selezionare la chiave.

   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".