Configurare Cloud Manager

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

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.

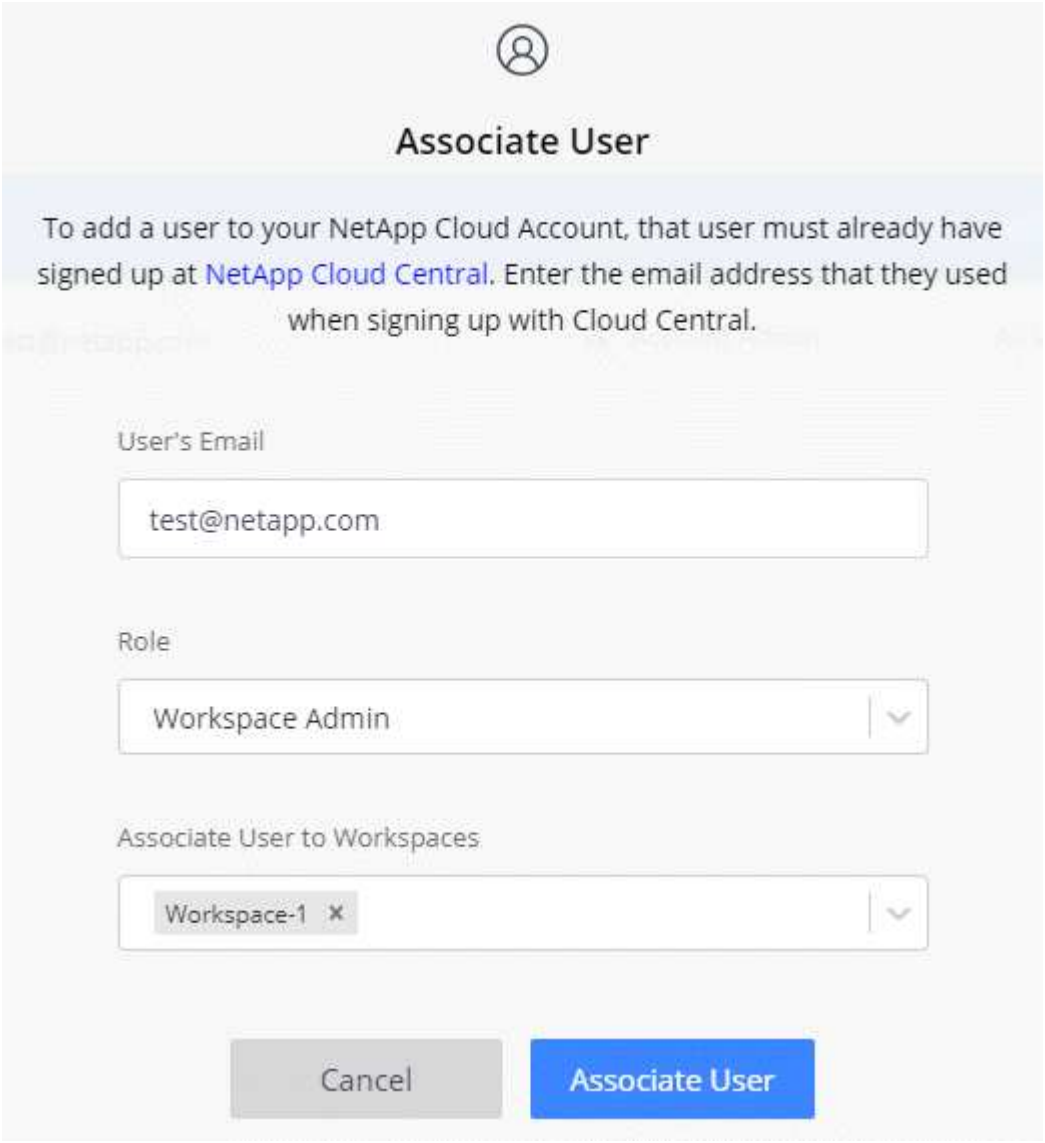
Aggiunta di utenti

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.



6. Fare clic su **Associa utente**.

Risultato

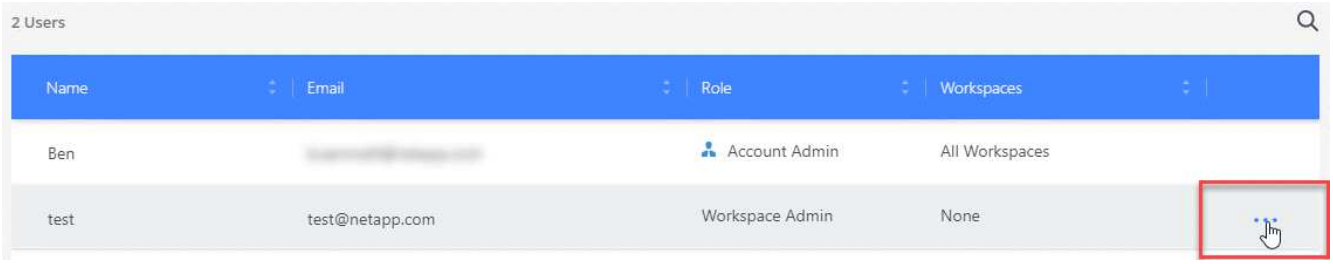
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

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.



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

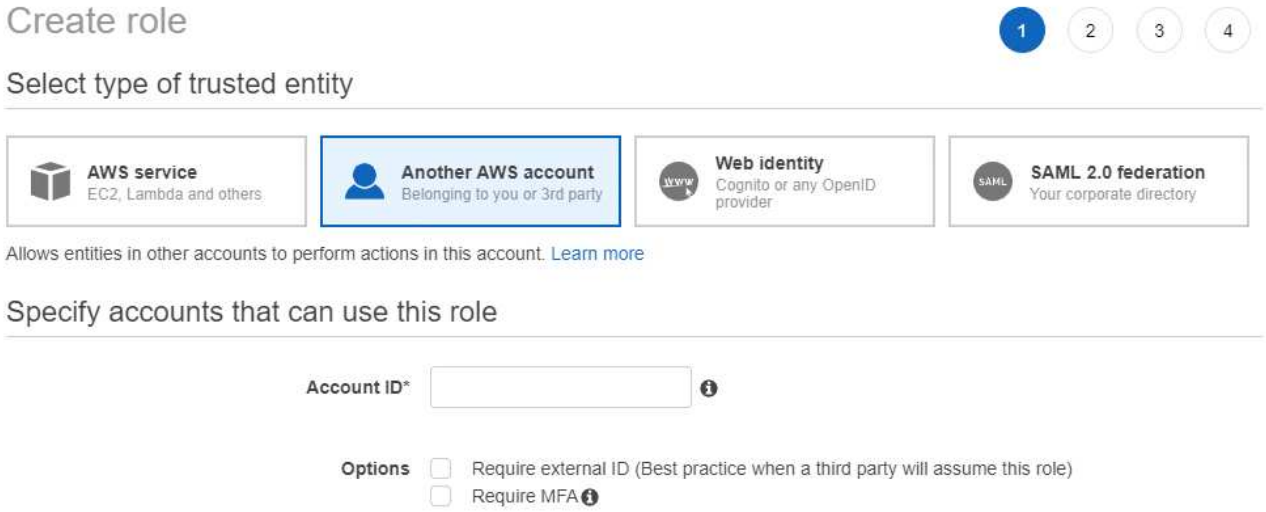
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Cloud Manager e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

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".



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.

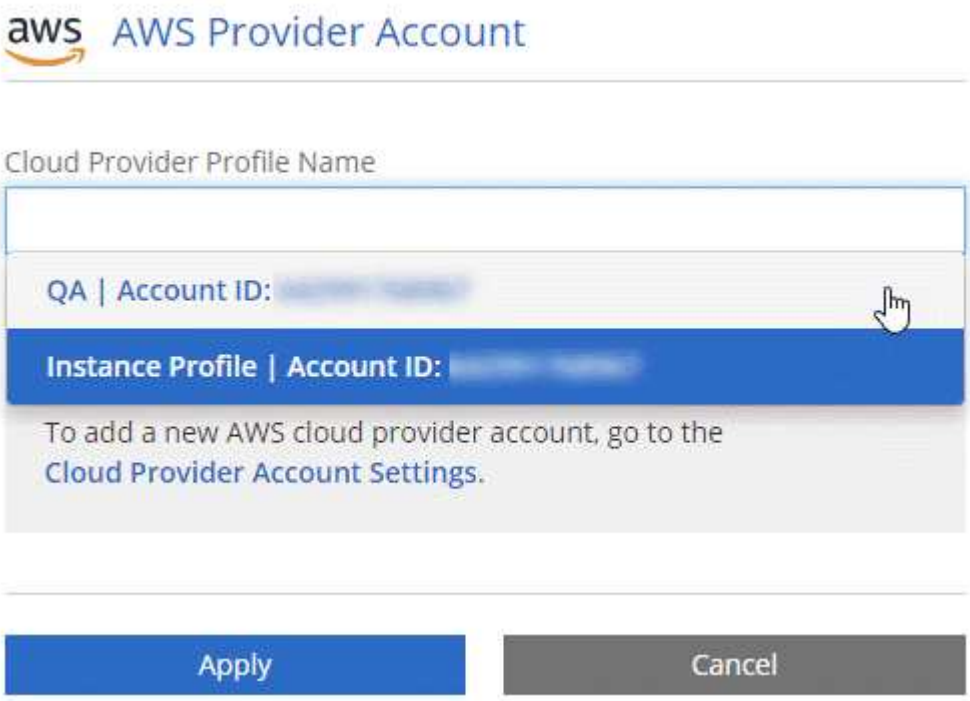
Fasi

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

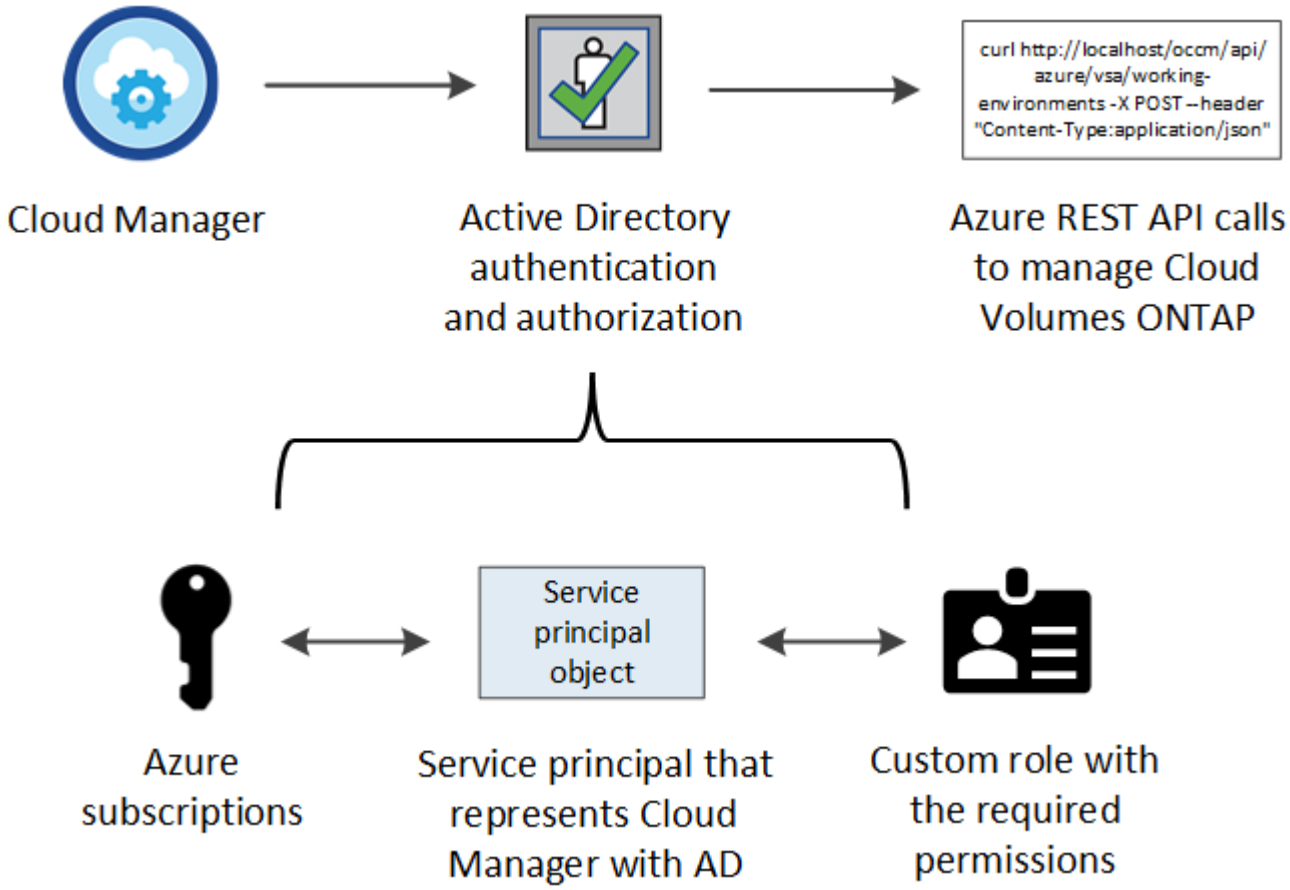
Quando distribuisci Cloud Manager da Cloud Central, Cloud Manager aggiunge automaticamente l'account Azure in cui hai implementato Cloud Manager. Se il software Cloud Manager è stato installato manualmente su un sistema esistente, non viene aggiunto un account iniziale. "Scopri gli account e le autorizzazioni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

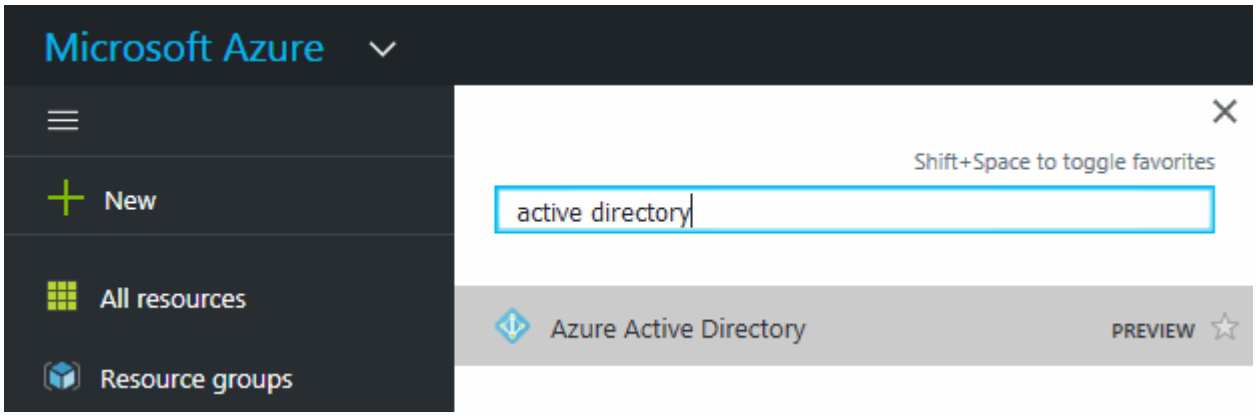
Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per il controllo degli accessi in base al ruolo.

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**.

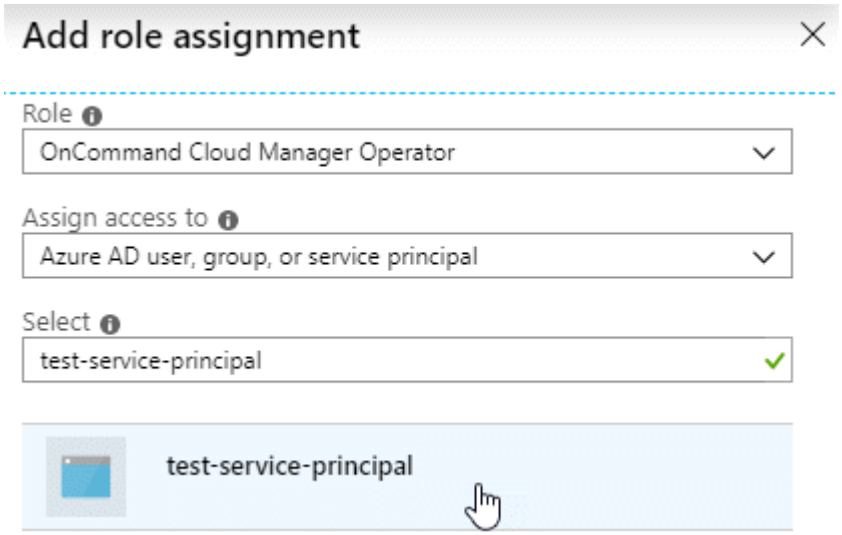
   b. Selezionare l'abbonamento.

   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.

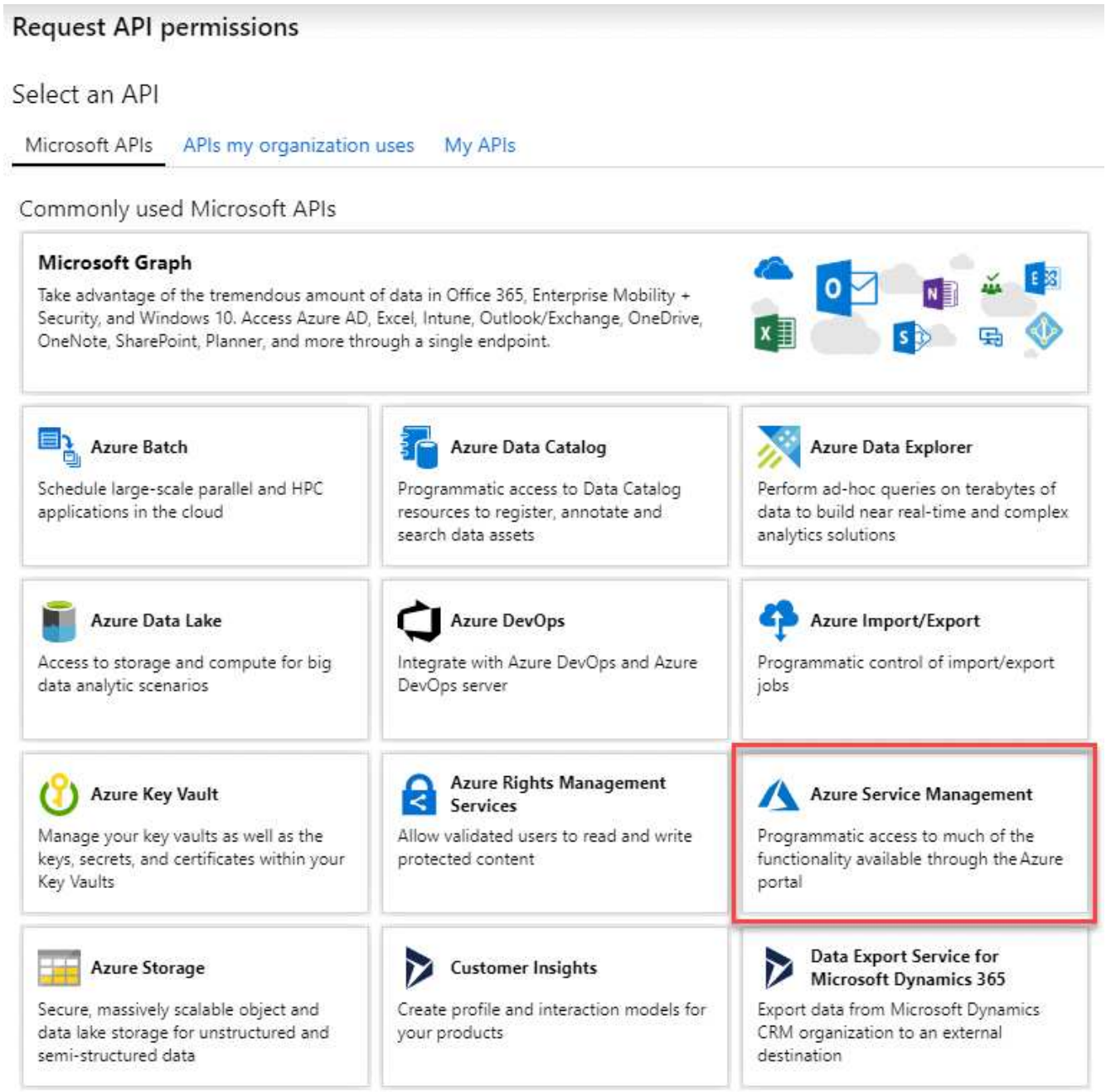
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Cloud Manager consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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

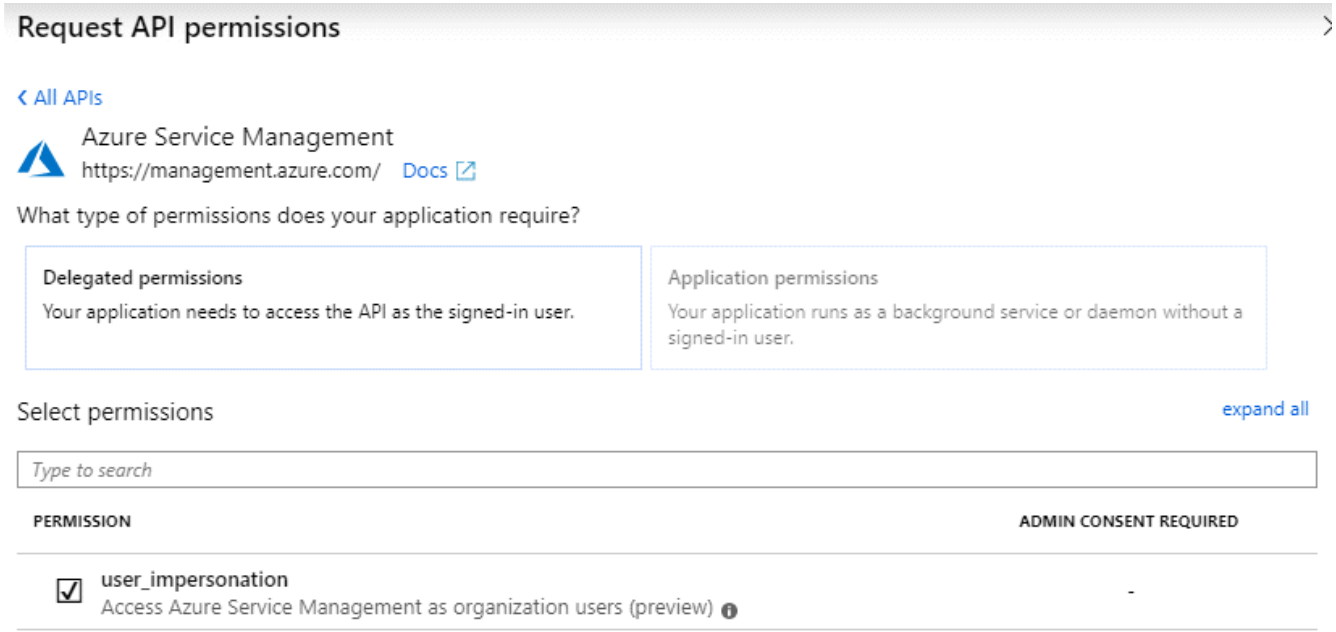
L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

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**.



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

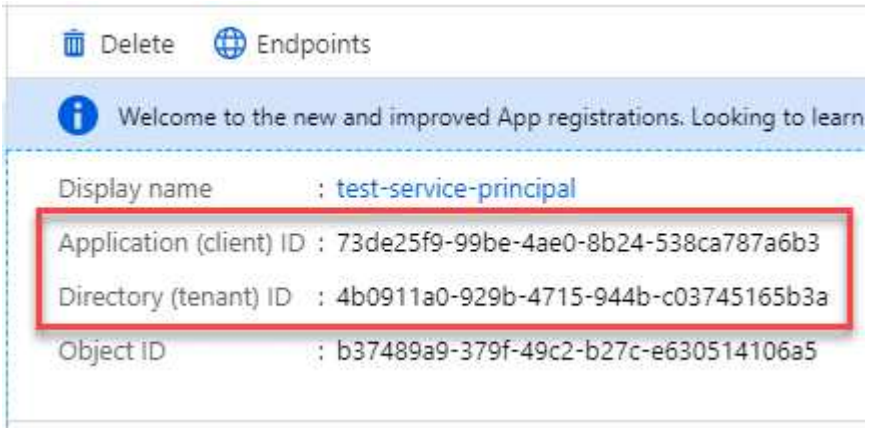


Ottenere l'ID dell'applicazione e l'ID della directory

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

Fasi

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



Creazione di un client segreto

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

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

Fasi

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

Risultato

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

Aggiunta di 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.

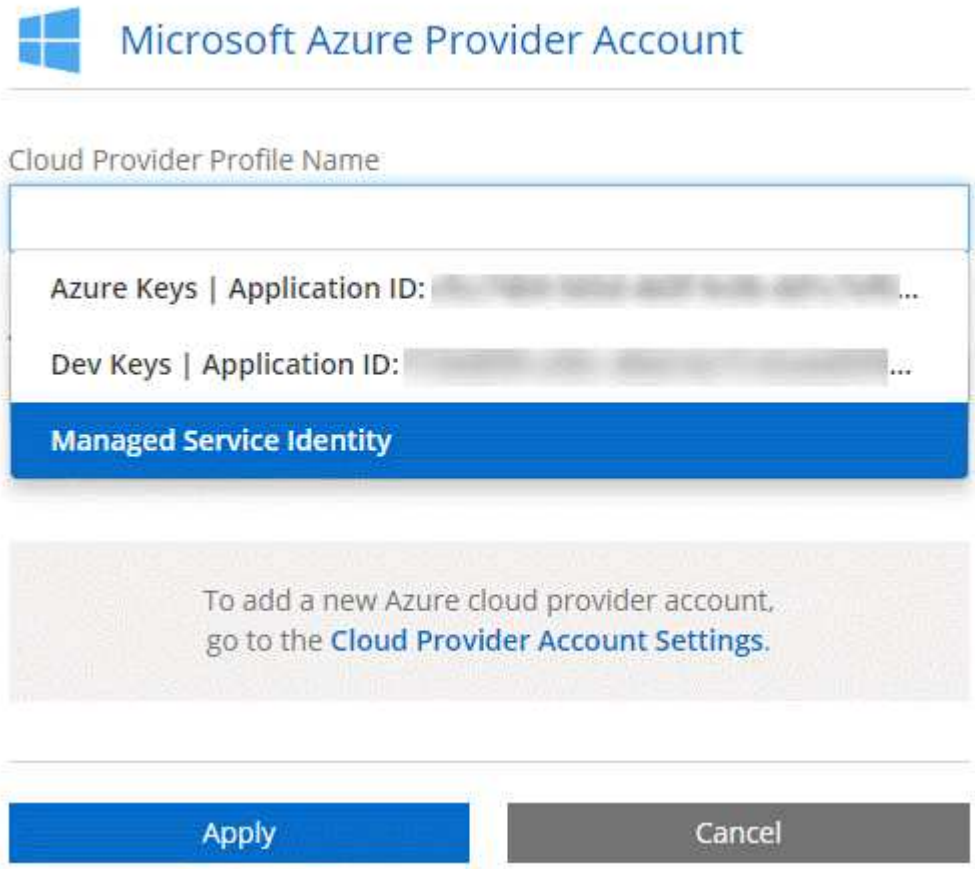
Fasi

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 Ottenere l'ID dell'applicazione e l'ID della directory.
   - ID tenant (o ID directory): Vedere Ottenere 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:



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**.

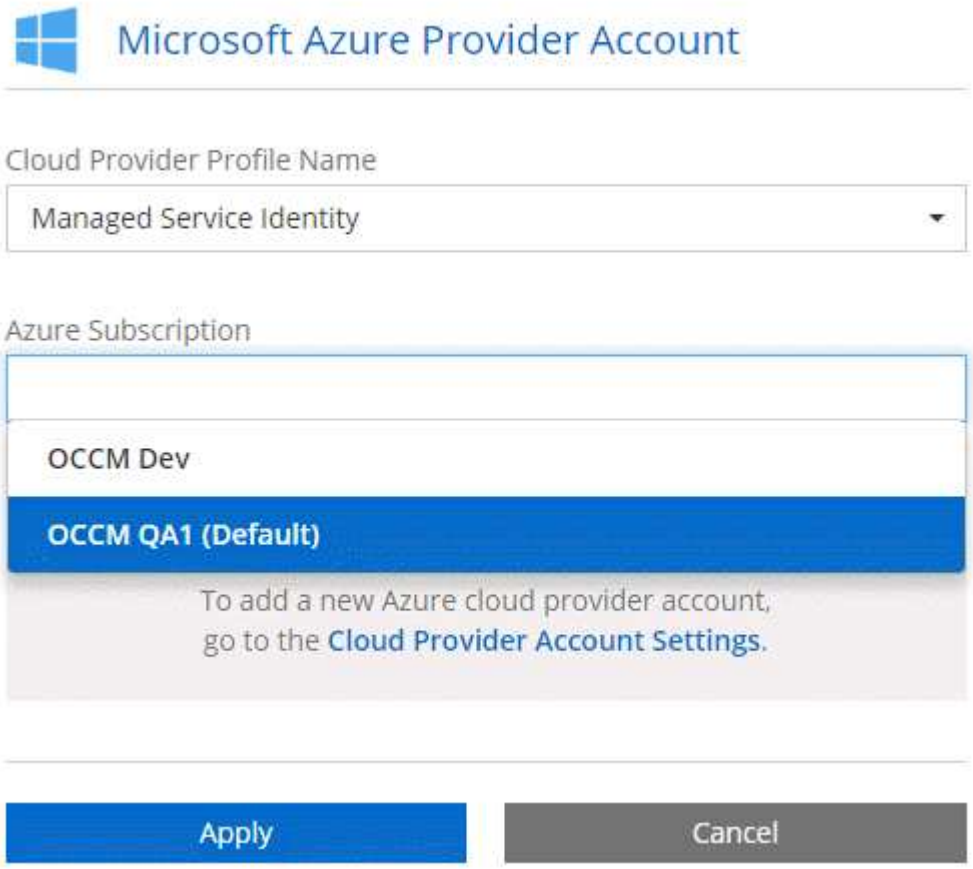
> L'operatore di gestione cloud di OnCommand è il nome predefinito fornito in "Policy di Cloud Manager". Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

- 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.



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.

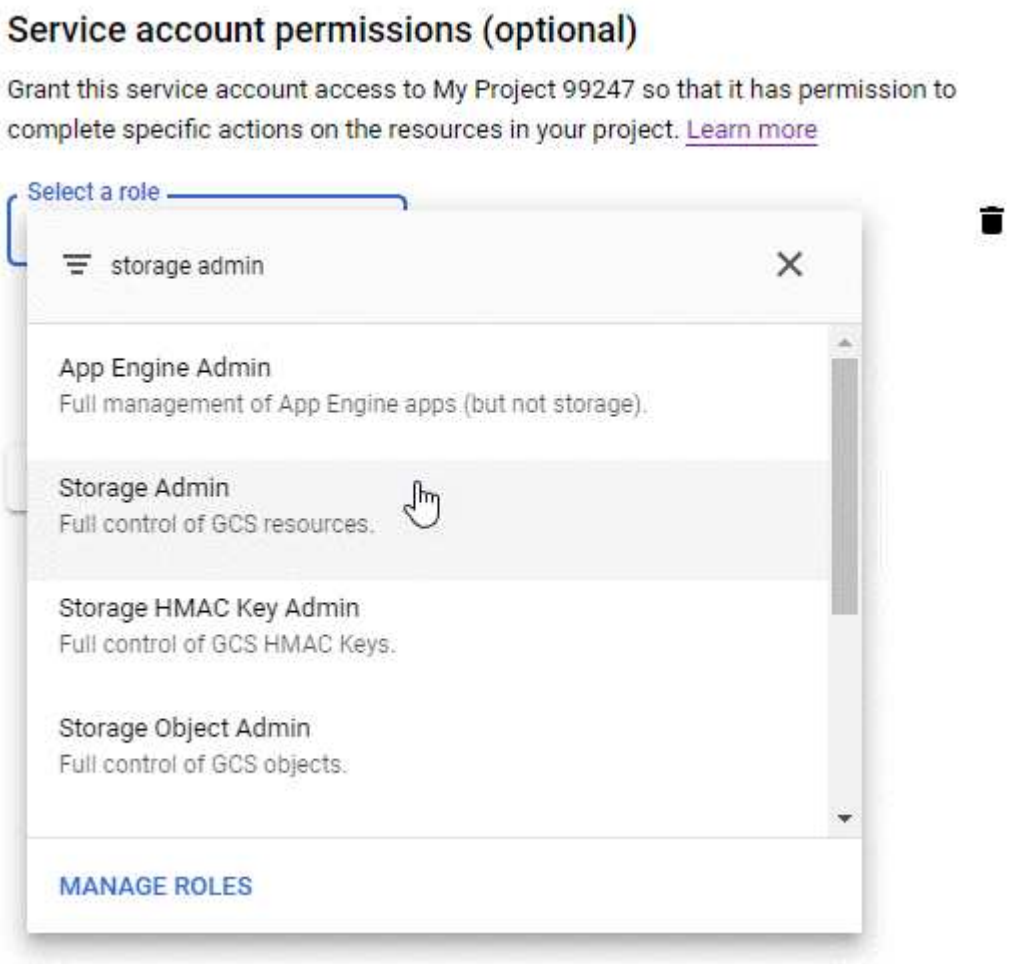
Impostazione di un account di servizio e di chiavi di accesso per Google Cloud Storage

Un account di servizio consente a Cloud Manager di autenticare e accedere ai bucket Cloud Storage utilizzati

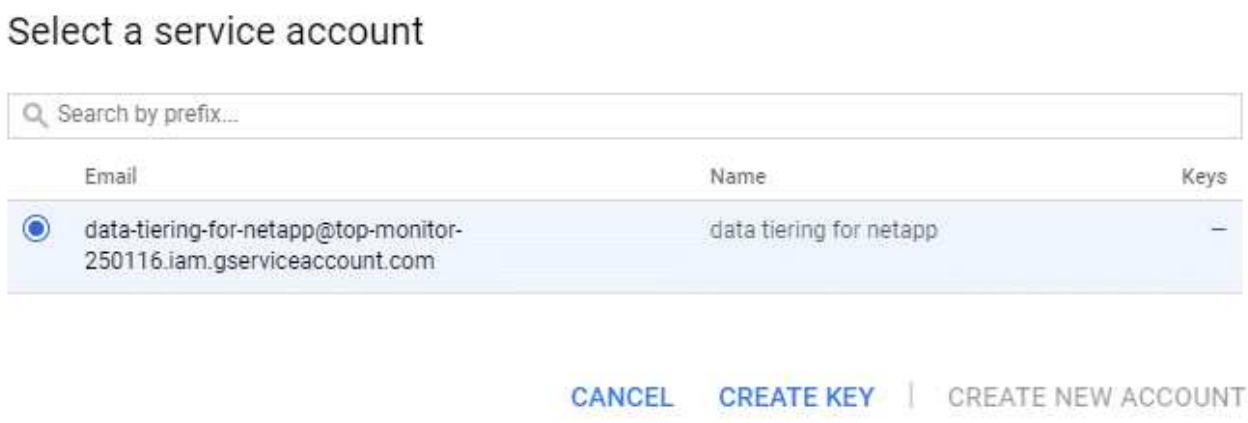
per il tiering dei dati. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

Fasi

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



2. Passare a. "Impostazioni storage GCP".
3. Se richiesto, selezionare un progetto.
4. Fare clic sulla scheda **interoperabilità**.
5. Se non è già stato fatto, fare clic su **Enable Interoperability access** (attiva accesso all'interoperabilità).
6. In **chiavi di accesso per gli account di servizio**, fare clic su **Crea una chiave per un account di servizio**.
7. Selezionare l'account di servizio creato al punto 1.



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

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

Aggiunta di un account GCP a Cloud Manager

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

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

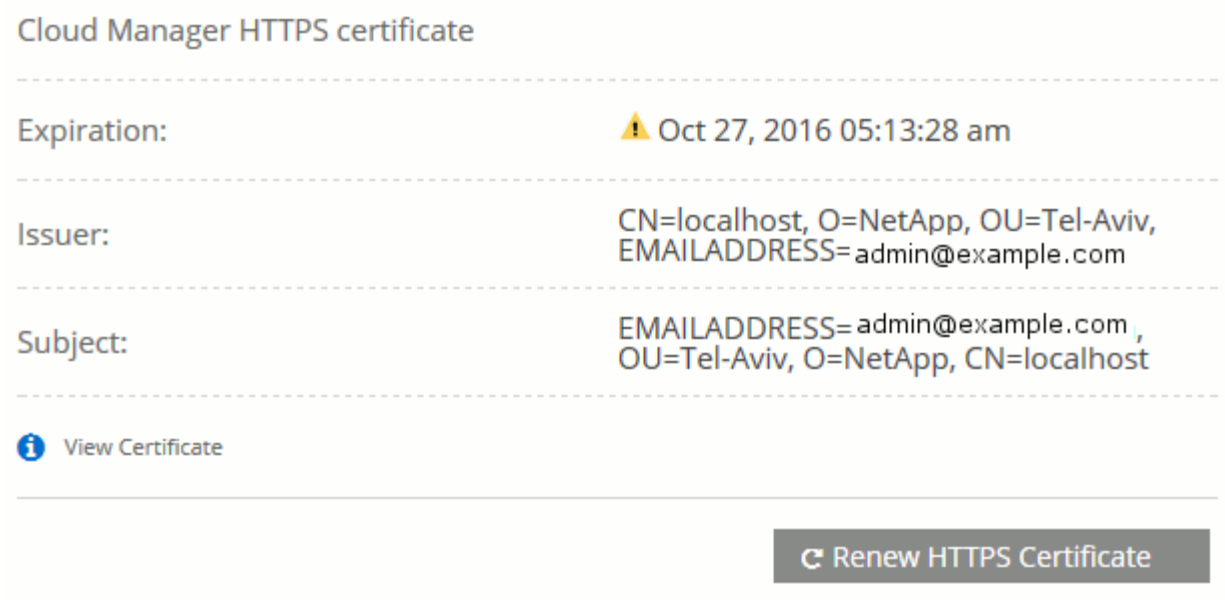
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Settings (Impostazioni) e selezionare **HTTPS Setup** (Configurazione HTTPS).

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

Risultato

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



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:

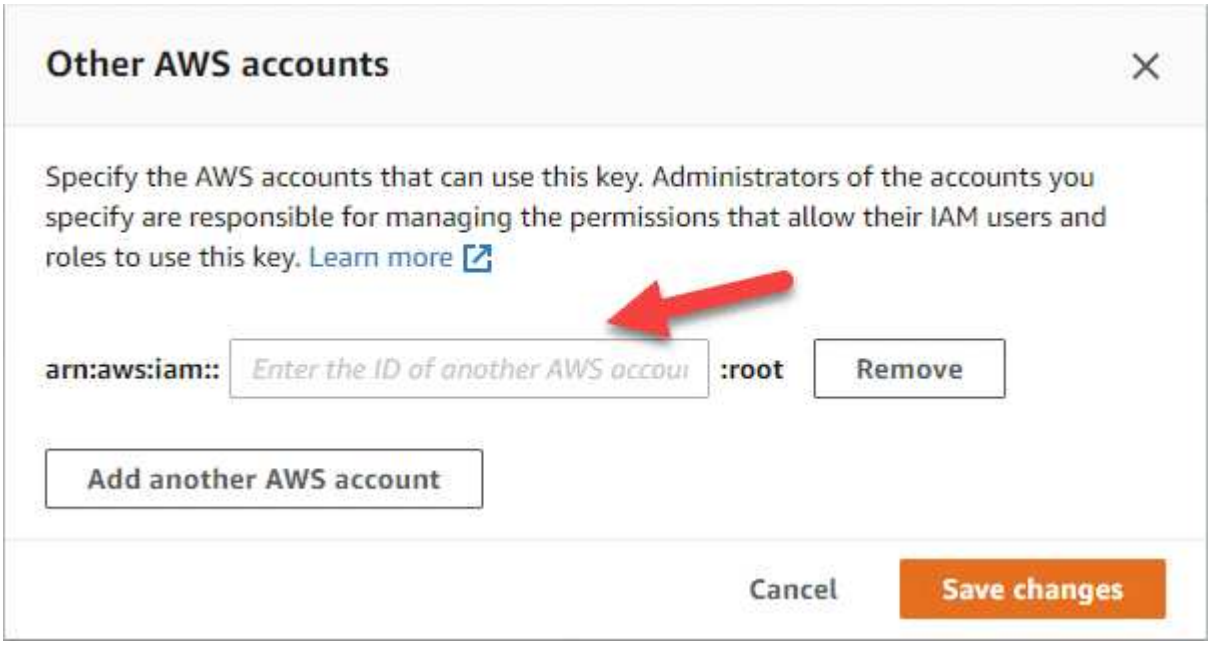
   a. Accedere alla console KMS dall'account in cui risiede il CMK.
   b. Selezionare la chiave.
   c. Nel riquadro **General Configuration** (Configurazione generale), copiare l'ARN della chiave.

      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".

Informazioni sul copyright

Informazioni sul marchio commerciale