Per iniziare

Cloud Manager 3.6

NetApp
October 23, 2024

Sommario

Per iniziare

Panoramica dell'implementazione

Prima di iniziare, potresti voler comprendere meglio le opzioni per l'implementazione di OnCommand 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
- Cloud IBM
- Nella tua rete

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

Posizione	Come implementare Cloud Manager
AWS	"Implementazione di Cloud Manager da NetApp Cloud Central"
AWS C2S	"Implementa Cloud Manager da AWS Intelligence Community Marketplace"
Area di Azure generalmente disponibile	"Implementazione di Cloud Manager da NetApp Cloud Central"
Governo di Azure	"Implementa Cloud Manager da Azure US Government Marketplace"
Azure Germania	"Scaricare e installare il software su un host Linux"
Cloud IBM	"Scaricare e installare il software su un host Linux"
Rete on-premise	"Scaricare e installare il software su un host Linux"

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.

- "Aggiunta di account Cloud Provider a Cloud Manager"
- "Installazione di un certificato HTTPS"
- "Configurazione di utenti e tenant"
- "Configurazione di AWS KMS"

Implementazione di Cloud Volumes ONTAP

Dopo aver attivato e attivato Cloud Manager, puoi iniziare a implementare Cloud Volumes ONTAP in AWS e in Microsoft Azure.

"Introduzione ad AWS" e. "Introduzione ad Azure" 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 9.5"
- "Pianificazione della configurazione"
- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"

Introduzione a Cloud Volumes ONTAP in AWS

Puoi iniziare a utilizzare Cloud Volumes ONTAP in AWS da NetApp Cloud Central.

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 Iscriviti a Cloud Volumes ONTAP dal marketplace AWS

Iscrizione da "AWS Marketplace" è necessario accettare i termini del software. Devi solo iscriverti al Marketplace. L'avvio di Cloud Volumes ONTAP da qualsiasi luogo, ma non è supportato.

3 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.

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.

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 Cloud Provider 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

Puoi iniziare a utilizzare Cloud Volumes ONTAP in Azure da NetApp Cloud Central. Sono disponibili istruzioni separate per implementare Cloud Manager in "Aree pubbliche degli Stati Uniti Azure" e in "Regioni Azure Germania".

1 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".

2 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".

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 Cloud Provider 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"

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

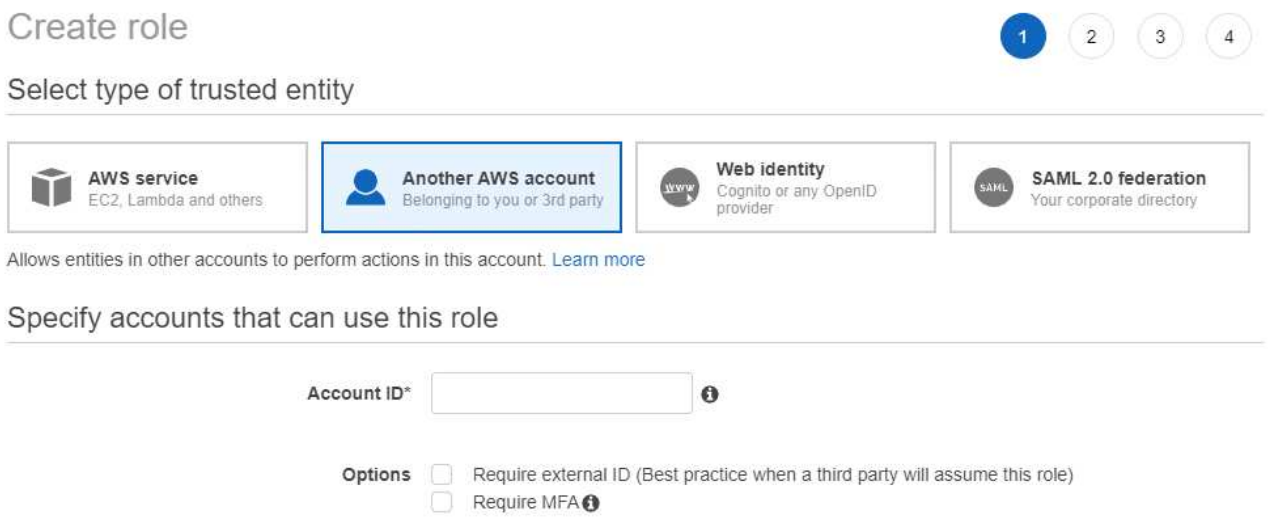
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Cloud Manager e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

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

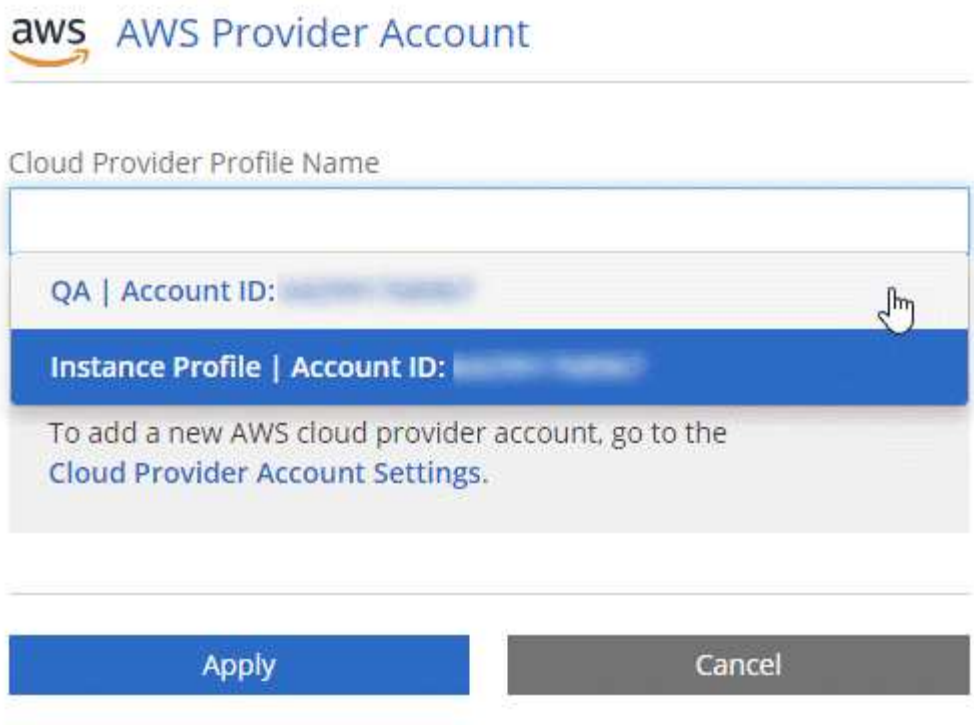
Dopo aver fornito un account AWS con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

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.

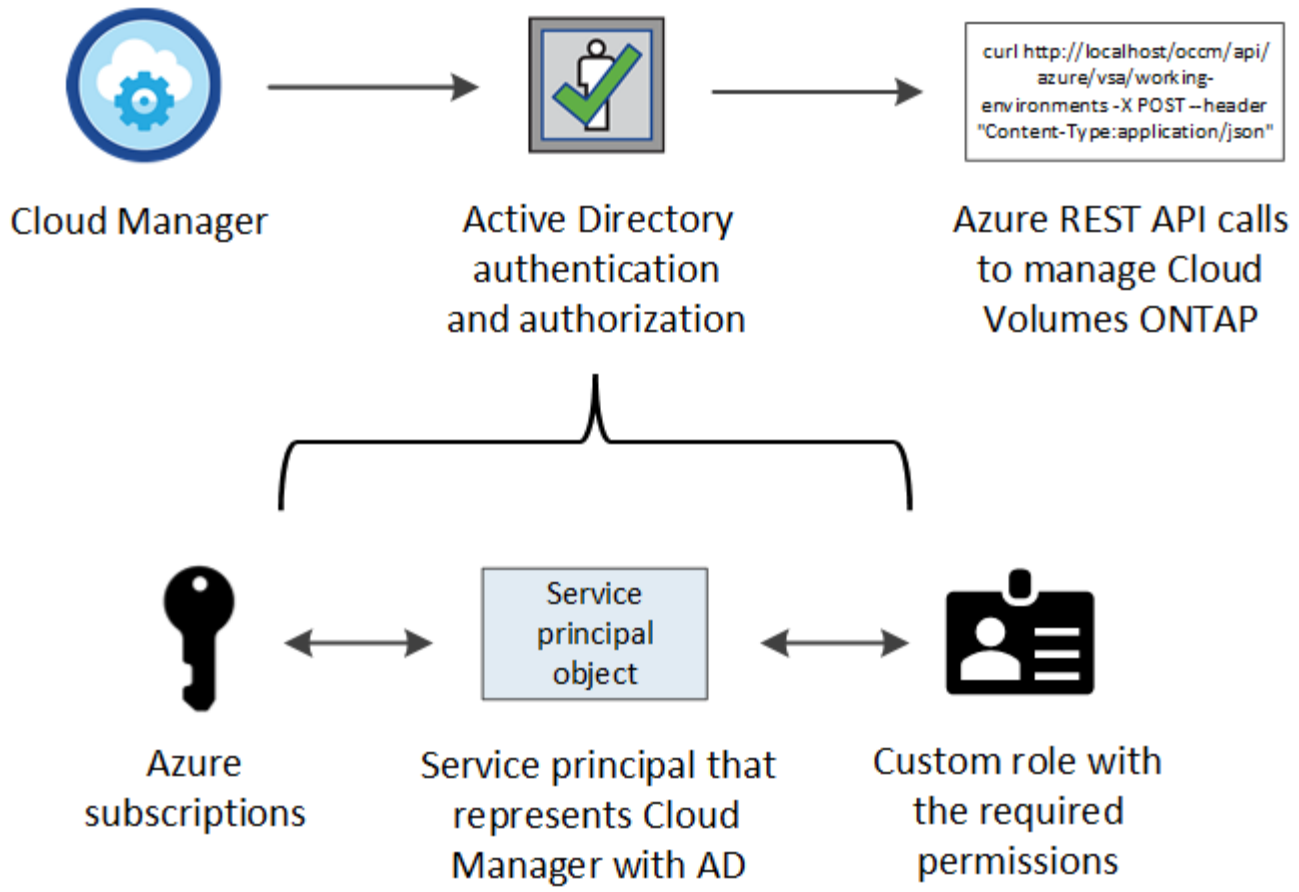
- Concessione delle autorizzazioni di Azure mediante un'entità del servizio
- Aggiunta di account Azure a Cloud Manager

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

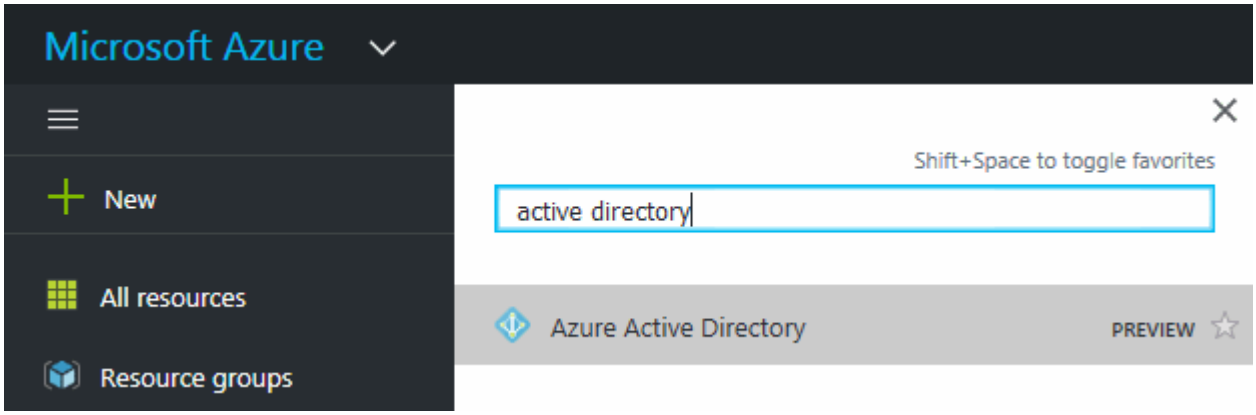
È necessario creare un'entità del servizio Active Directory in modo che Cloud Manager possa autenticarsi con Azure Active Directory.

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

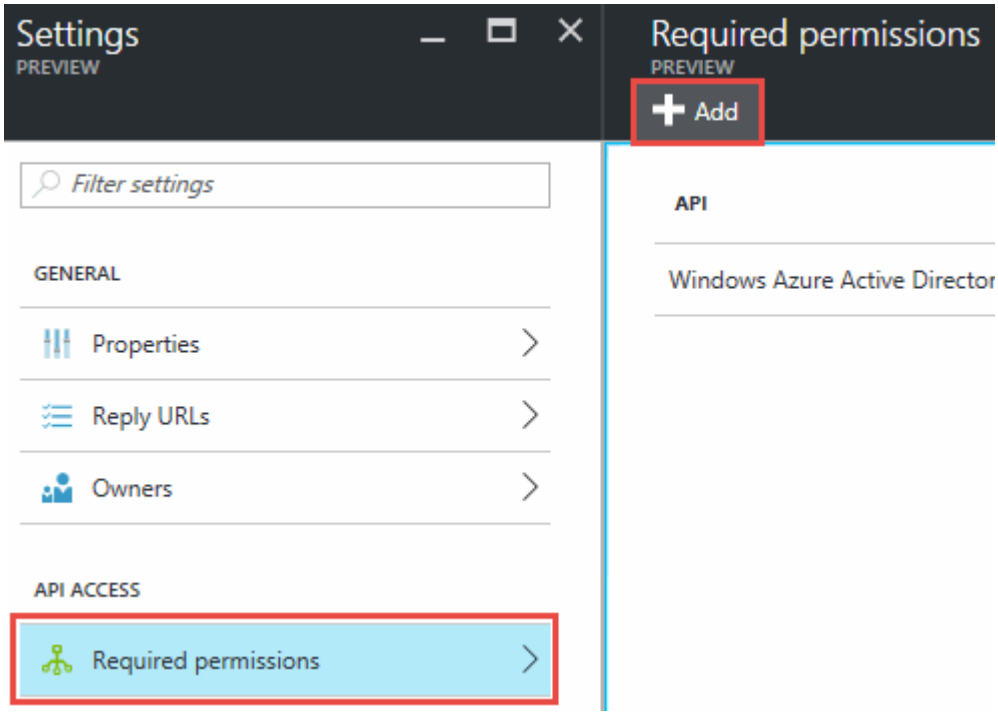
1. Dal portale Azure, aprire il servizio **Azure Active Directory**.



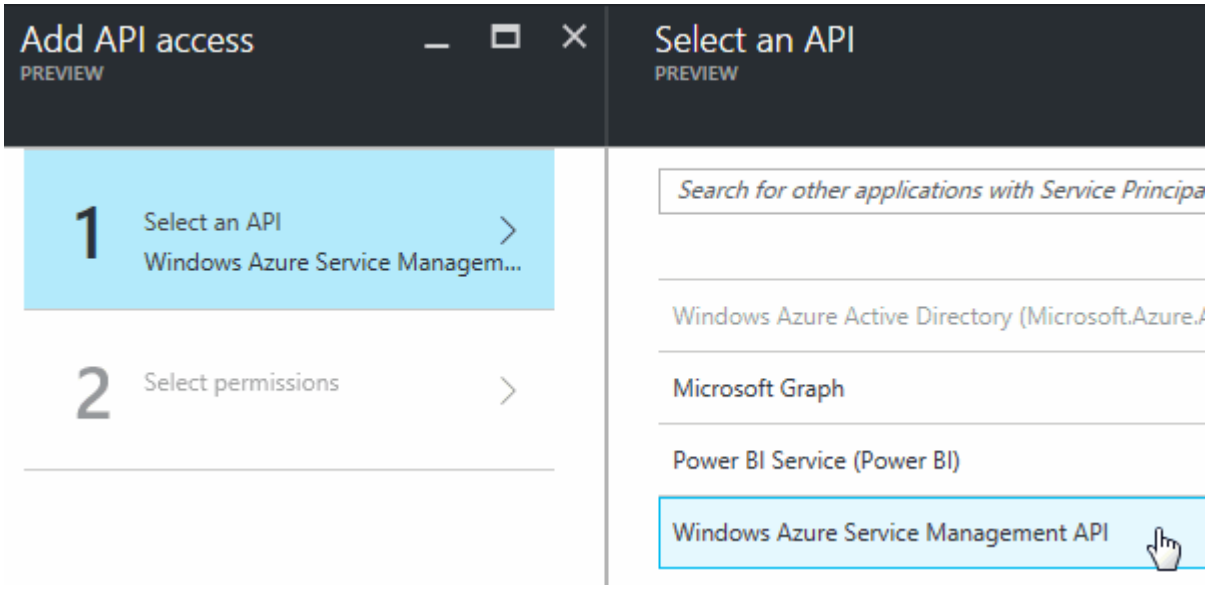
2. Nel menu, fare clic su **App Registrations (Legacy)**.
3. Creare l'entità del servizio:
   a. Fare clic su **Nuova registrazione applicazione**.
   b. Immettere un nome per l'applicazione, mantenere selezionata l'opzione **Web app/API**, quindi immettere un URL, ad esempio http://url
   c. Fare clic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

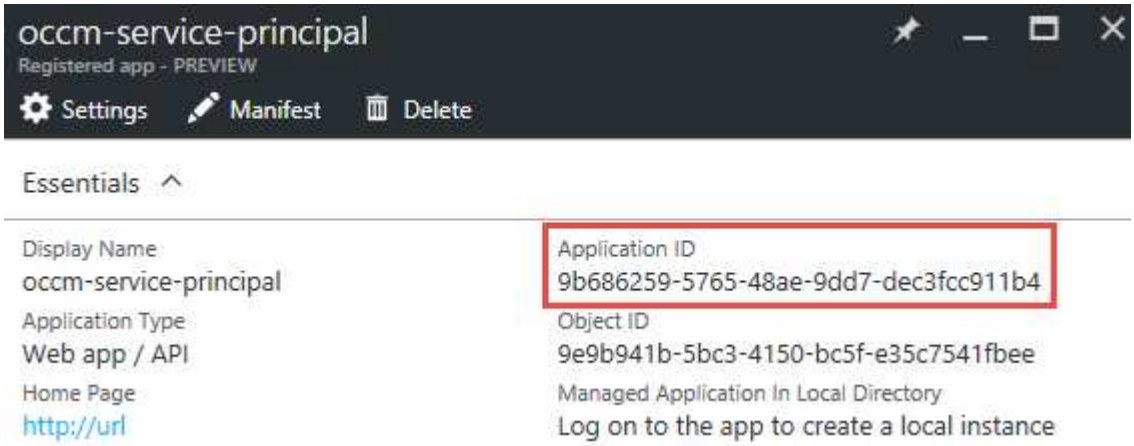
b. Inserire una descrizione, selezionare una durata, quindi fare clic su **Salva**.

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.

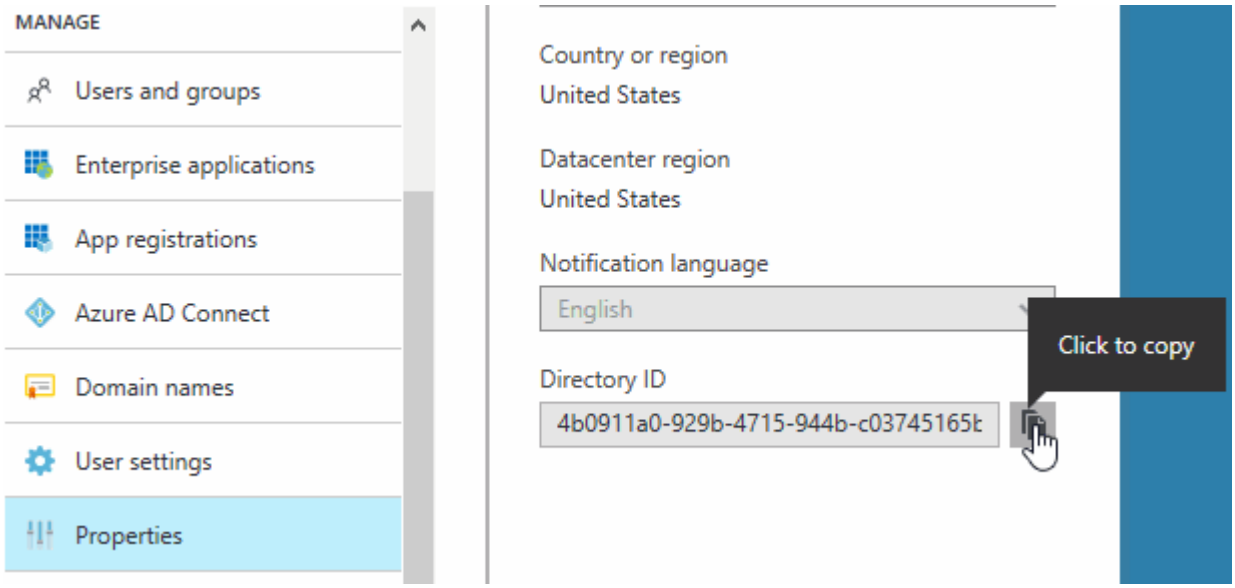
Analogamente al valore della chiave, è necessario inserire l'ID dell'applicazione in Cloud Manager quando si aggiunge un account del provider cloud a Cloud Manager.



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

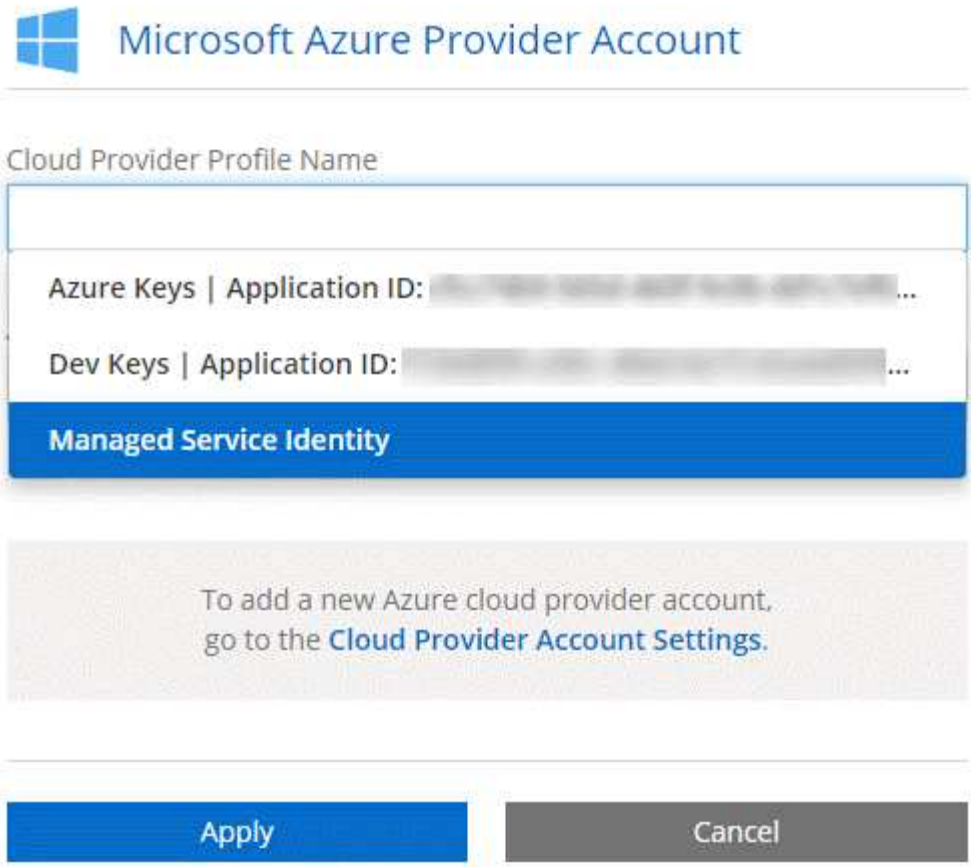
Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

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.

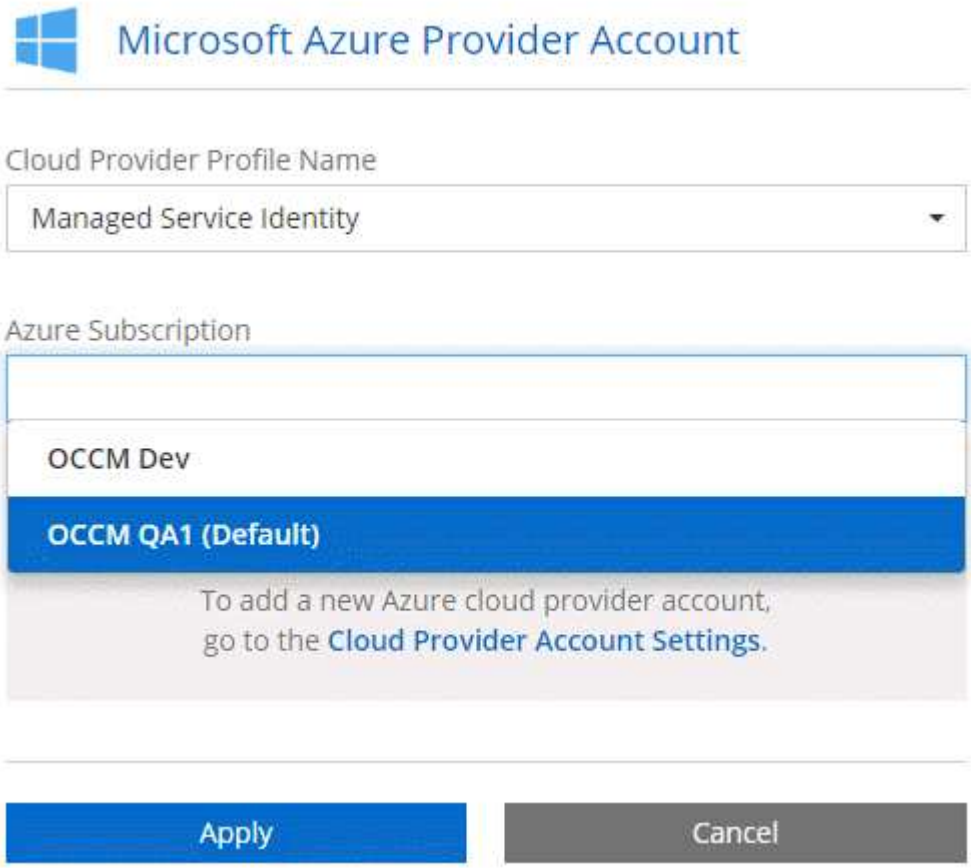
      - Assegnare l'accesso a una **macchina virtuale**.

- 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

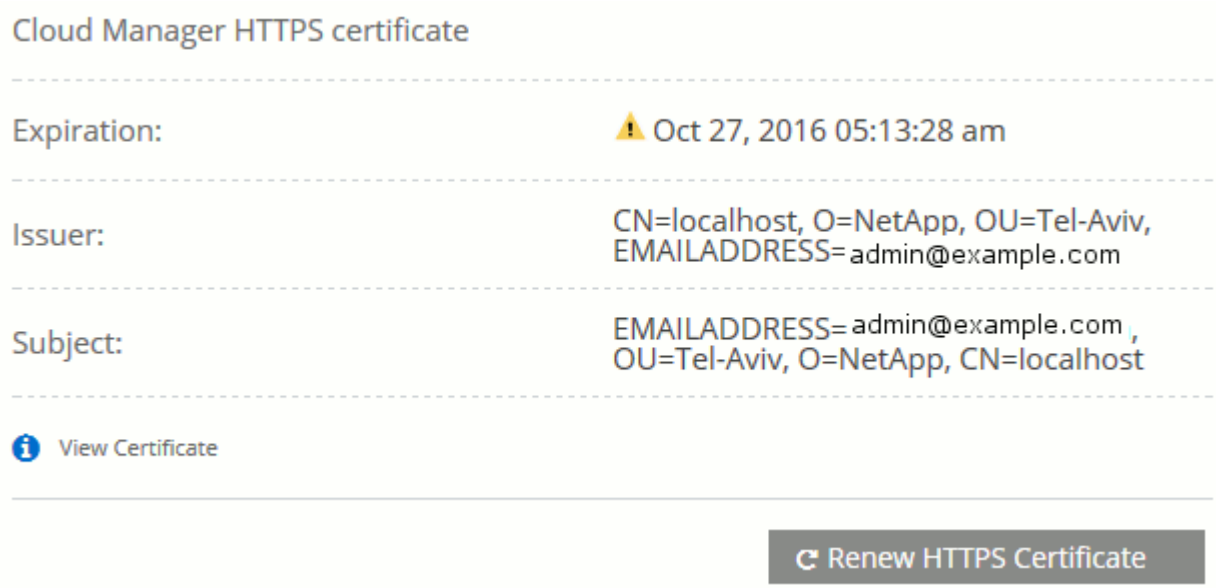
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **HTTPS Setup**.
2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio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

Opzione	Descrizione
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 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.

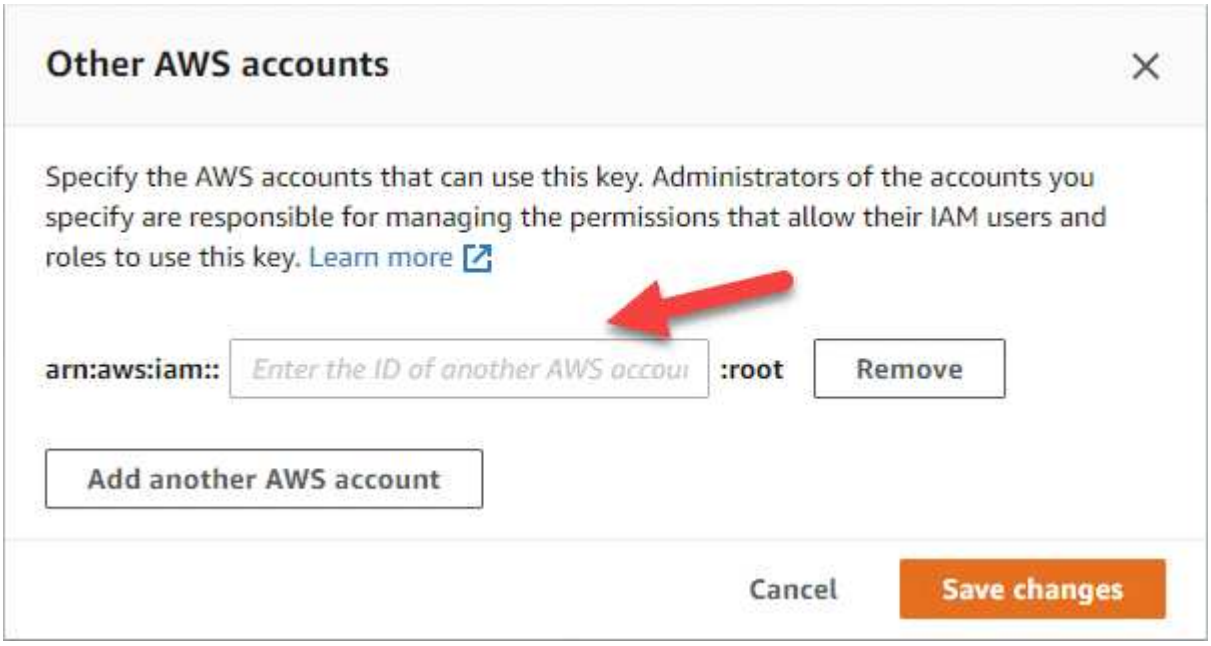
   b. Selezionare la chiave.

   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".

Requisiti di rete

Requisiti di rete per Cloud Manager

È necessario configurare la rete in modo che Cloud Manager possa implementare i sistemi Cloud Volumes ONTAP in AWS o in Microsoft Azure. 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 AWS e ai VNet Azure in cui si desidera implementare Cloud Volumes ONTAP.

Ad esempio, se si installa Cloud Manager nella rete aziendale, è necessario impostare una connessione VPN a AWS VPC o Azure 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.

Accesso a Internet in uscita 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): • CloudFormation • Elastic Compute Cloud (EC2) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • S3 (Simple Storage Service) L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. "Per ulteriori informazioni, fare riferimento alla documentazione AWS."	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.

Endpoint	Scopo
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione di licenze e supporto.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Accesso a Internet in uscita 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
https://management.azure.com https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.

Endpoint	Scopo
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione di licenze e supporto.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Accesso a Internet in uscita 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	Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web. A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host: • Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale • Un IP pubblico funziona in qualsiasi scenario di rete 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.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central.
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Accesso a Internet in uscita 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"
- 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.

Stai cercando l'elenco degli endpoint a cui Cloud Manager richiede l'accesso? Ora vengono gestiti in un'unica sede. "Fare clic qui per ulteriori informazioni".

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)".

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: Implementazione di Active Directory Domain Services su AWS Cloud Quick Start Reference".

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".

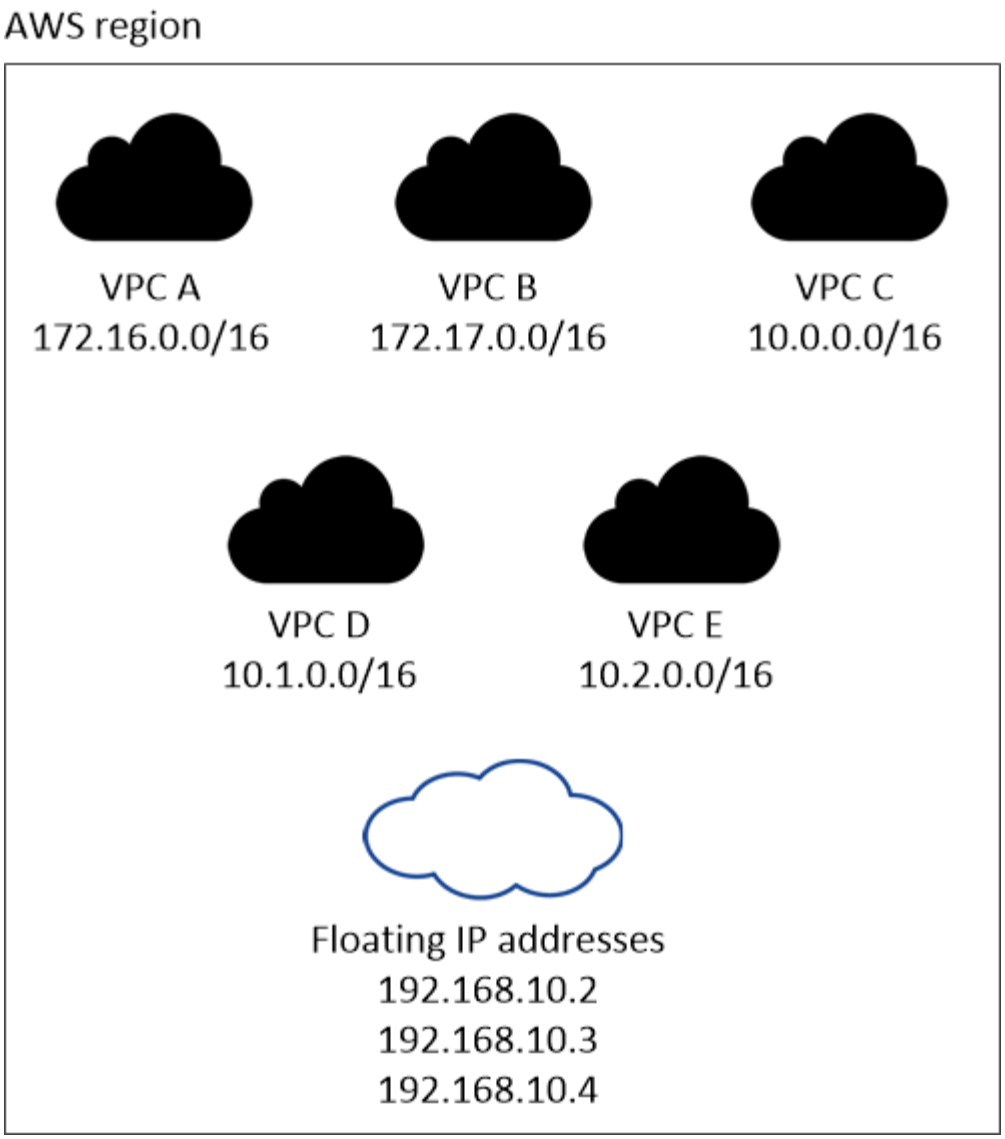
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

> 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.



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".

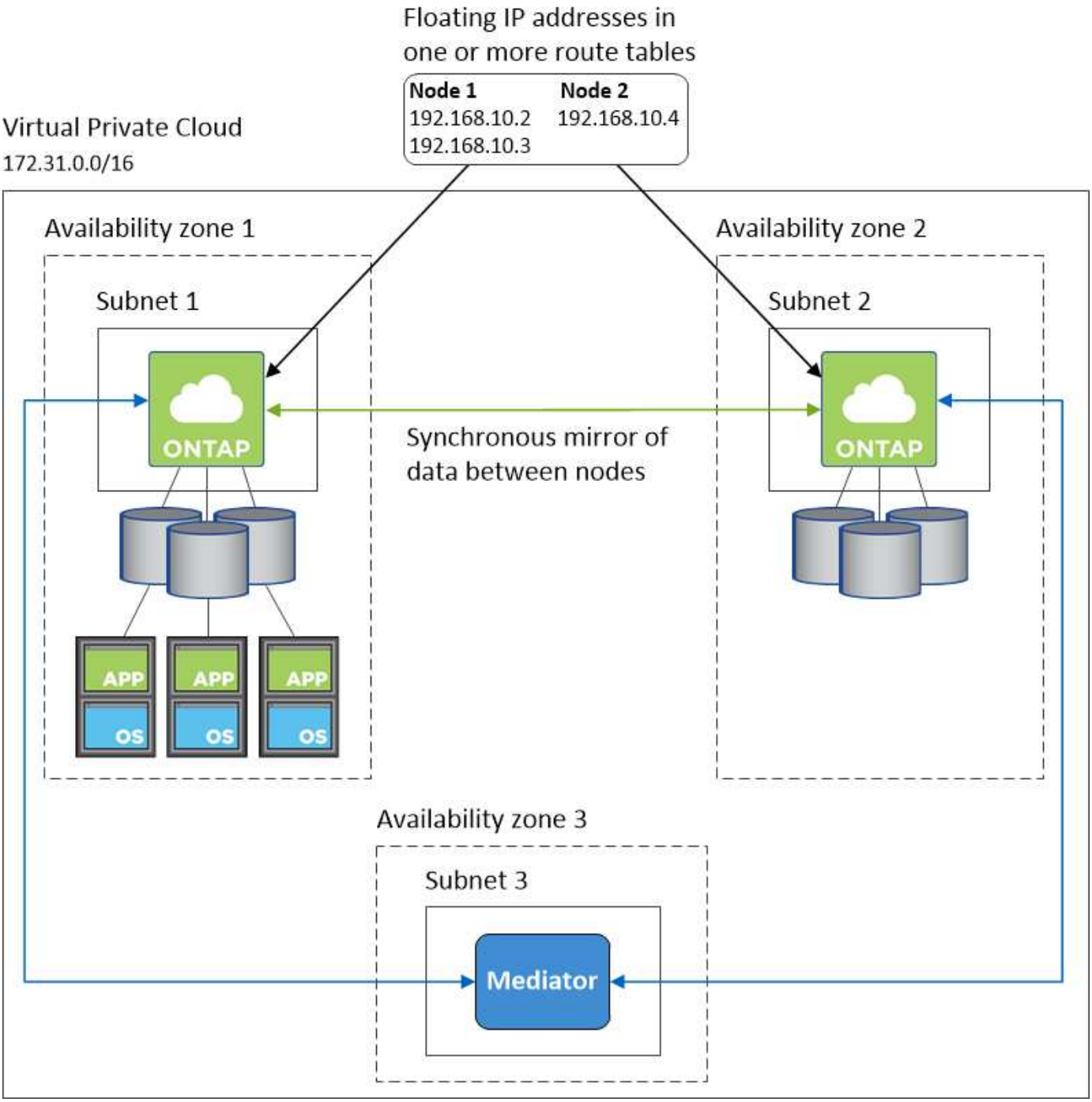
Connessione ai tool di gestione NetApp

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

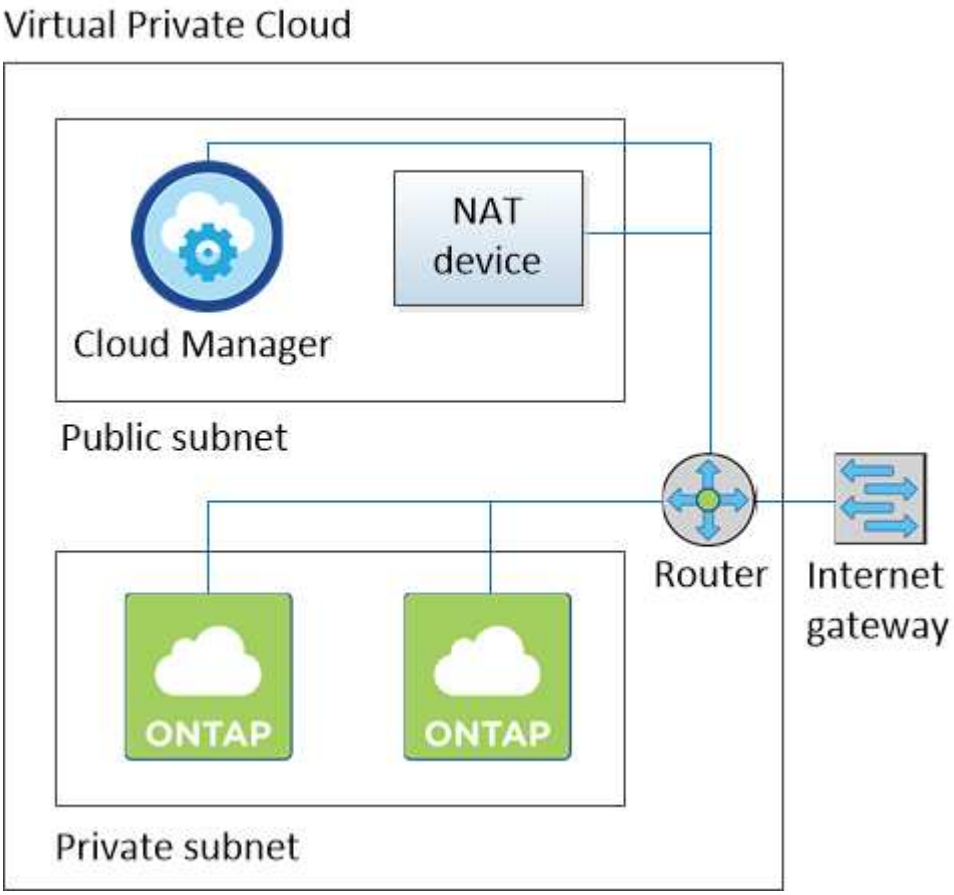
Questa configurazione VPC include subnet pubbliche e private, un gateway Internet che connette il VPC a Internet e un gateway NAT o istanza NAT nella subnet pubblica che abilita il traffico Internet in uscita dalla

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:



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

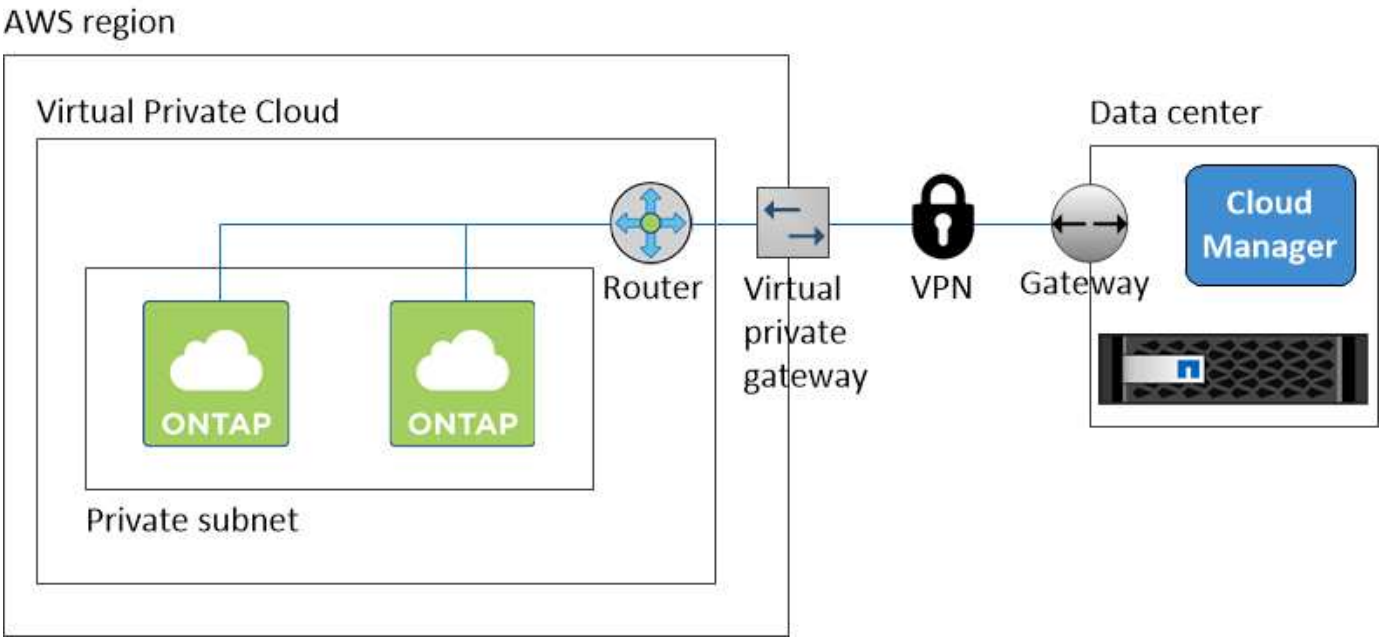
Questa configurazione VPC è una configurazione di cloud ibrido in cui Cloud Volumes ONTAP diventa un'estensione del tuo ambiente privato. La configurazione include una subnet privata e un gateway privato virtuale con una connessione VPN alla rete. Il routing attraverso il tunnel VPN consente alle istanze 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:



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

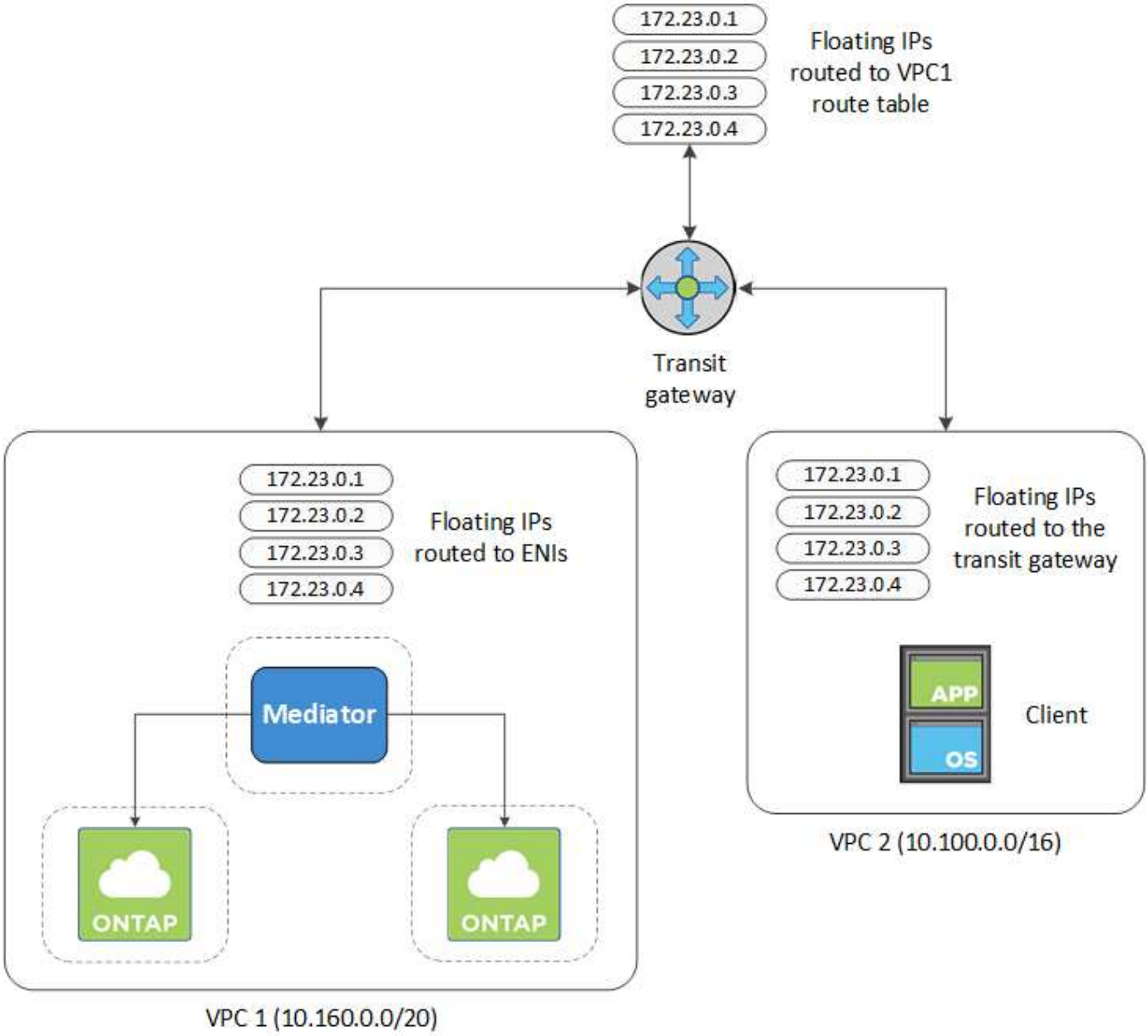
Impostare un gateway di transito AWS per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

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

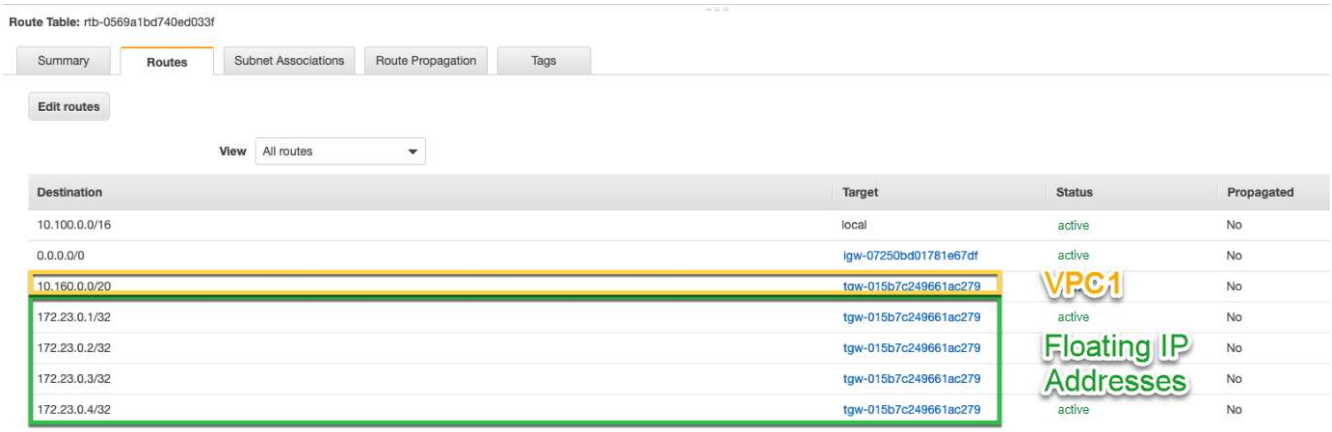
CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 | vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	Floating IP Addresses	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603		static	active

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

   a. Aggiungere voci di routing agli indirizzi IP mobili.

   b. Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

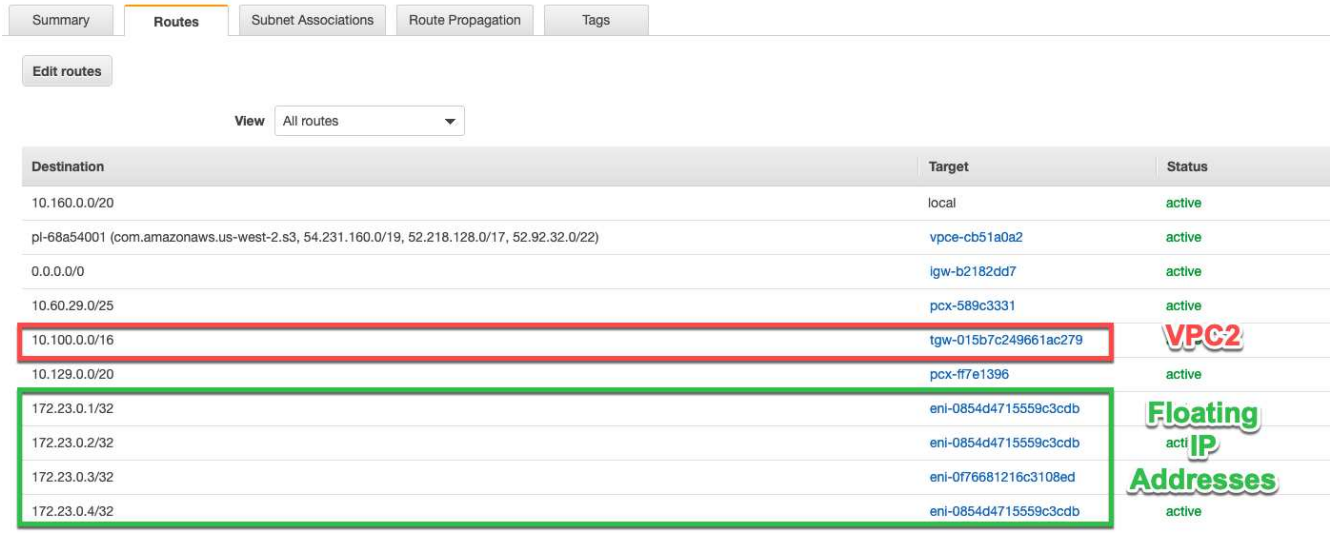
   L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.

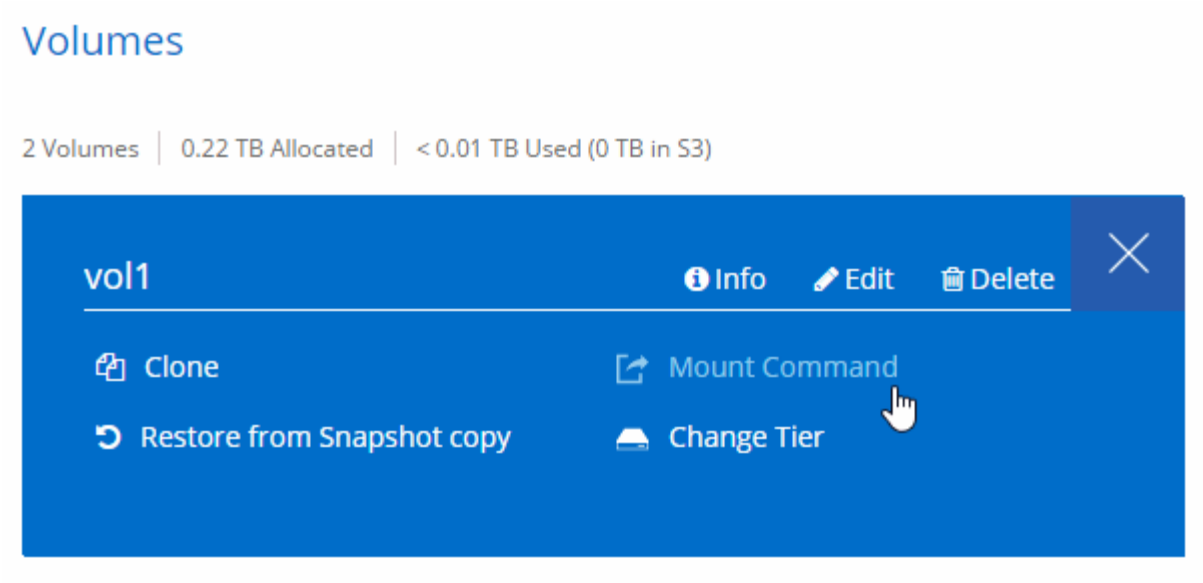
   Questo passaggio è importante perché completa il routing tra i VPC.

   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.



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**.



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

È necessario configurare la rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

> Stai cercando l'elenco degli endpoint a cui Cloud Manager richiede l'accesso? Ora vengono gestiti in un'unica sede. "Fare clic qui per ulteriori informazioni".

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 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

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 a Azure BLOB storage per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold nello storage Azure Blob, non è necessario configurare un endpoint del servizio VNET, purché Cloud Manager disponga delle autorizzazioni necessarie:

```
"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".

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.

Tipi di istanze AWS EC2 supportati

t3.medium (consigliato), t2.medium e m4.large

Dimensioni delle macchine virtuali Azure supportate

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

Sistemi operativi supportati

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

  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 Linuxhttps://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.

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 per AWS"
   - "Requisiti di rete per Cloud Volumes ONTAP for Azure"
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-V3.6.3.sh
   . Eseguire lo script di installazione:
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.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:

   https://ipaddress:port

   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 https://ipaddress:8443

7. Iscriviti a un account NetApp Cloud Central o effettua l'accesso se ne hai già uno.
8. Al momento dell'iscrizione o dell'accesso, Cloud Manager aggiunge automaticamente l'account utente come amministratore del sistema.
9. Dopo aver effettuato l'accesso, immettere un nome per il sistema Cloud Manager.

Al termine

Imposta le autorizzazioni per i tuoi account AWS e Azure in modo che Cloud Manager possa implementare Cloud Volumes ONTAP:

- Se si desidera implementare Cloud Volumes ONTAP in AWS, "Configurare un account AWS e aggiungerlo a Cloud Manager".
- Se si desidera implementare Cloud Volumes ONTAP in Azure, "Configura un account Azure e aggiungilo a Cloud Manager".

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'opzione 1-click.

Fasi

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

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

   "Cloud manager di NetApp OnCommand: Policy AWS e Azure"

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. Accedere alla "Pagina Cloud Manager su AWS Marketplace".
3. Fare clic su **continua**.
4. Nella scheda Custom Launch (Avvio personalizzato), fare clic su **Launch with EC2 Console** (Avvia con console EC2) per la propria area geografica, quindi effettuare le seguenti selezioni:

   a. A seconda della disponibilità della regione, scegliere il tipo di istanza t3.medium (consigliato), t2.medium o m4.Large.

   b. Selezionare un VPC, una subnet, un ruolo IAM e altre opzioni di configurazione che soddisfino i propri requisiti.

   c. Mantenere le opzioni di storage predefinite.

   d. Se necessario, inserire i tag per l'istanza.

   e. Specificare i metodi di connessione richiesti per l'istanza di Cloud Manager: SSH, HTTP e HTTPS.

   f. Fare clic su **Avvia**.

Risultato

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

Al termine

Accedere a Cloud Manager immettendo l'indirizzo IP pubblico o privato in un browser Web, quindi completare l'installazione guidata.

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:

   http://ipaddress:80

   Al momento dell'accesso, Cloud Manager aggiunge automaticamente l'account utente come amministratore del sistema.

6. Dopo aver effettuato l'accesso, immettere un nome per il sistema Cloud Manager.

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-3b42-4ae7-9bzzbce5bzzbce5bce5bzzbce5bce5bce5b5b

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

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

   az role Definition create --role-Definition C:/Policy_for_cloud_Manager_Azure_3.6.1.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. Cerca OnCommand Cloud Manager nel portale per il governo degli Stati Uniti.
2. 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.

3. 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.

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

   http://ipaddress:80

   Al momento dell'accesso, Cloud Manager aggiunge automaticamente l'account utente come amministratore del sistema.

5. Dopo aver effettuato l'accesso, immettere un nome per il sistema Cloud Manager.

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-3b42-4ae7-9bzzbce5bzzbce5bce5bzzbce5bce5bce5b5b

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

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

az role Definition create --role-Definition C:/Policy_for_cloud_Manager_Azure_3.6.1.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.