Cloud Manager e documentazione Cloud Volumes ONTAP

Cloud Manager 3.7

NetApp
October 23, 2024

Sommario

Cloud Manager e documentazione Cloud Volumes ONTAP

Cloud Manager consente di implementare e gestire NetApp Cloud Volumes ONTAP, una soluzione per la gestione dei dati che offre protezione, visibilità e controllo per i carichi di lavoro basati sul cloud.

BlueXP

NetApp BlueXP estende e migliora le funzionalità fornite tramite Cloud Manager.

"Consulta la documentazione BlueXP"

Scopri le novità

- "Novità di Cloud Manager"
- "Novità di Cloud Volumes ONTAP"

Inizia subito

- "Inizia ad utilizzare AWS"
- "Inizia ad utilizzare Azure"
- "Inizia a utilizzare Google Cloud Platform"
- "Trova le configurazioni supportate per Cloud Volumes ONTAP"
- "Esaminate i requisiti di rete per Cloud Manager"
- "Esaminare i requisiti di rete per Cloud Volumes ONTAP per AWS"
- "Esaminate i requisiti di rete per Cloud Volumes ONTAP for Azure"
- "Esaminare i requisiti di rete per Cloud Volumes ONTAP per GCP"
- "Pianificare la configurazione di Cloud Volumes ONTAP"

Automatizza con le API

- "Guida per sviluppatori API"
- "Esempi di automazione"

Connettiti con i colleghi, ottieni assistenza e trova ulteriori informazioni

- "Community NetApp: Servizi dati cloud"
- "Supporto NetApp Cloud Volumes ONTAP"
- "Dove trovare assistenza e ulteriori informazioni"

Note di rilascio

Cloud Manager

Novità di Cloud Manager 3.7

In genere, Cloud Manager introduce una nuova release ogni mese per offrire nuove funzionalità, miglioramenti e correzioni di bug.

Cerchi una release precedente?"Novità del 3.6"
"Novità del 3.5"
"Novità del 3.4"

Aggiornamento di Cloud Manager 3.7.5 (16 dicembre 2019)

Questo aggiornamento include i seguenti miglioramenti:

- Cloud Volumes ONTAP 9.7
- Conformità del cloud per Cloud Volumes ONTAP

Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 è ora disponibile in AWS, Azure e Google Cloud Platform.

"Scopri le novità di Cloud Volumes ONTAP 9.7".

Conformità del cloud per Cloud Volumes ONTAP

La conformità al cloud è un servizio di privacy e conformità dei dati per Cloud Volumes ONTAP in AWS e Azure. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili nei sistemi Cloud Volumes ONTAP.

Cloud Compliance è attualmente disponibile come release a disponibilità controllata.

"Scopri di più sulla conformità al cloud".

Cloud Manager 3.7.5 (3 dicembre 2019)

Cloud Manager 3.7.5 include i seguenti miglioramenti.

- Elevata velocità di scrittura per Cloud Volumes ONTAP in GCP
- Cluster ONTAP on-premise come storage persistente per Kubernetes
- Ultima versione di Trident per Kubernetes
- Supporto per gli account storage Azure General-purpose v2
- Prefissi nei nomi degli account di storage Azure utilizzando le API

Elevata velocità di scrittura per Cloud Volumes ONTAP in GCP

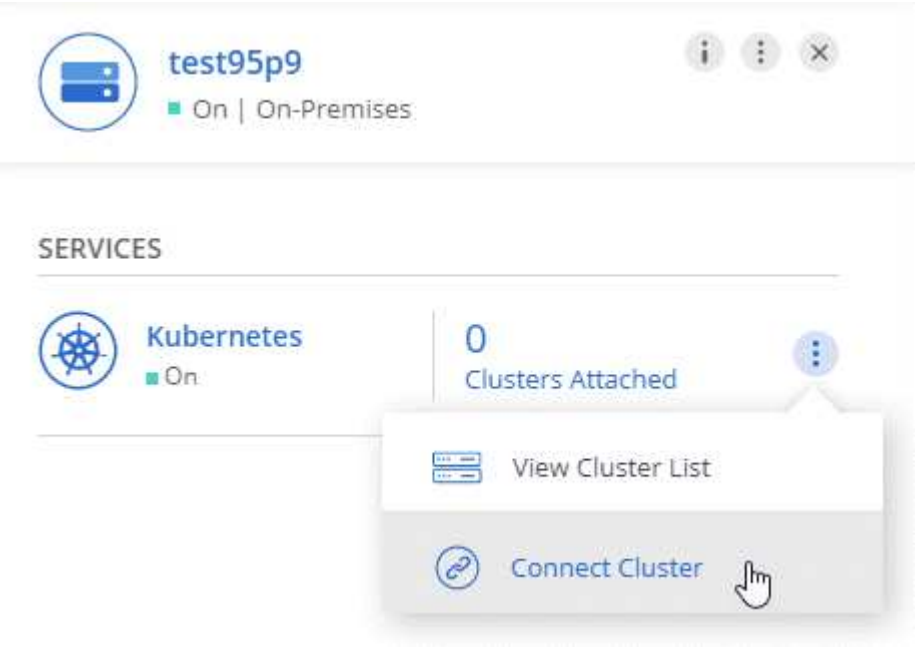
Ora puoi abilitare un'elevata velocità di scrittura su sistemi Cloud Volumes ONTAP nuovi ed esistenti nella piattaforma cloud Google. L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide.

- "Scopri come scegliere una velocità di scrittura"
- "Scopri come modificare la velocità di scrittura sui sistemi esistenti"

Cluster ONTAP on-premise come storage persistente per Kubernetes

Cloud Manager consente ora di utilizzare cluster ONTAP on-premise come storage persistente per i container. Analogamente a Cloud Volumes ONTAP, Cloud Manager automatizza l'implementazione di NetApp Trident e connette ONTAP ai cluster Kubernetes.

Dopo aver aggiunto un cluster Kubernetes a Cloud Manager, puoi connetterlo ai cluster ONTAP on-premise dalla pagina Working Environments (ambienti di lavoro):



"Scopri come iniziare".

Ultima versione di Trident per Kubernetes

Cloud Manager installa ora una versione più recente di Trident (versione 19.07.1) quando colleghi un ambiente di lavoro a un cluster Kubernetes.

Supporto per gli account storage Azure General-purpose v2

Quando si implementano nuovi sistemi Cloud Volumes ONTAP in Azure, gli account storage creati da Cloud Manager per la diagnostica e il tiering dei dati sono ora account storage v2 generici.

Prefissi nei nomi degli account di storage Azure utilizzando le API

Ora puoi aggiungere un prefisso ai nomi degli account di storage Azure creati da Cloud Manager per Cloud Volumes ONTAP. È sufficiente utilizzare il parametro *storageAccountPrefix* quando si implementa un nuovo sistema Cloud Volumes ONTAP in Azure.

"Per ulteriori informazioni sull'utilizzo delle API, consulta la API Developer Guide".

Cloud Manager 3.7.4 (6 ottobre 2019)

Cloud Manager 3.7.4 include i seguenti miglioramenti.

- Supporto per Azure NetApp Files
- Miglioramenti di Cloud Volumes ONTAP per GCP
- Miglioramento del backup su S3
- Crittografia dei dischi di boot e root in AWS
- Supporto per la regione AWS Bahrain
- Supporto per la regione nord degli Emirati Arabi Uniti di Azure

Supporto per Azure NetApp Files

Ora puoi visualizzare e creare volumi NFS per Azure NetApp Files direttamente da Cloud Manager. Questo miglioramento continua il nostro obiettivo di aiutarti a gestire il tuo cloud storage da una singola interfaccia.

"Scopri come iniziare".

Questa funzione richiede nuove autorizzazioni, come mostrato nella più recente "Policy di Cloud Manager per Azure".

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

Miglioramenti di Cloud Volumes ONTAP per GCP

Cloud Manager 3.7.4 offre i seguenti miglioramenti a Cloud Volumes ONTAP per la piattaforma cloud Google:

Abbonamenti pay-as-you-go nel GCP Marketplace

Ora puoi pagare per Cloud Volumes ONTAP mentre vai iscrivendoti a Cloud Volumes ONTAP nel marketplace della piattaforma cloud di Google.

"Mercato della piattaforma cloud di Google: Cloud manager per Cloud Volumes ONTAP"

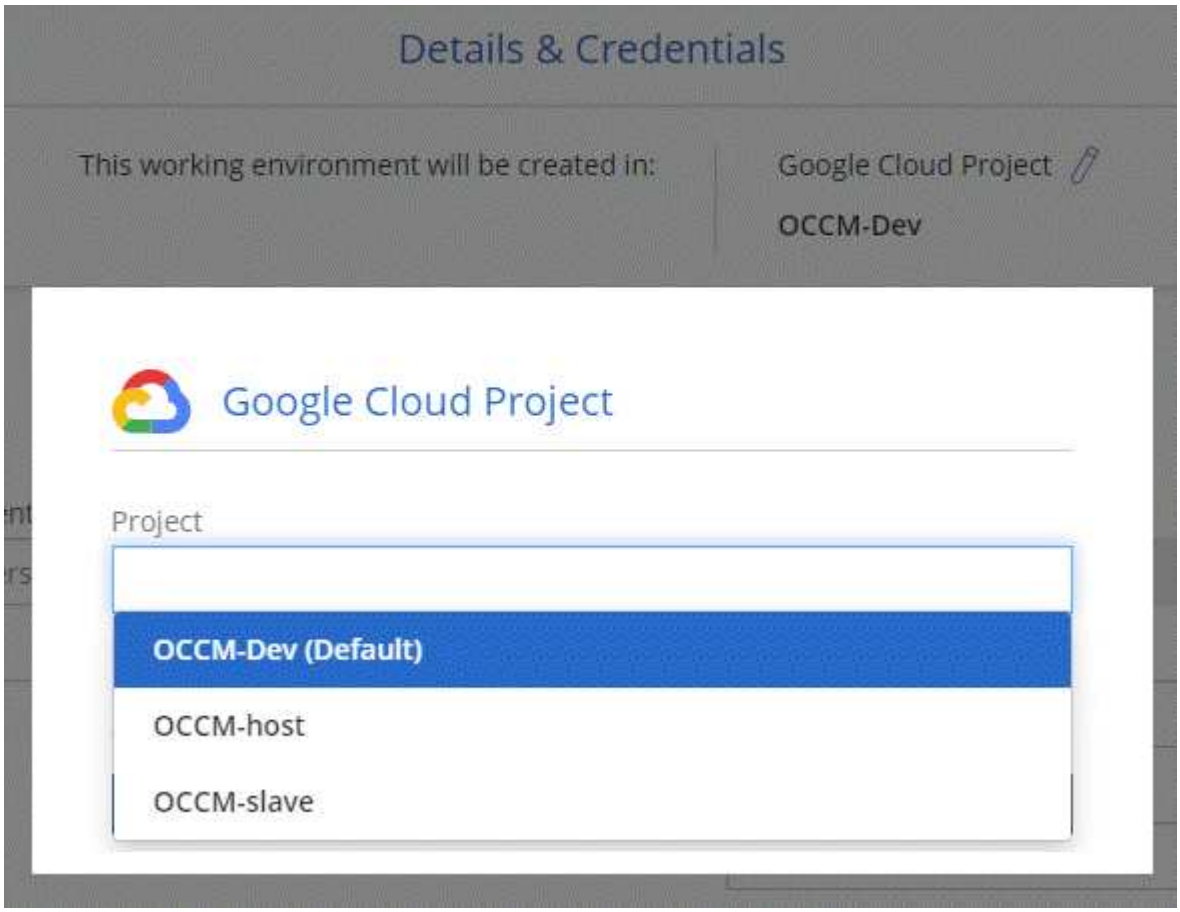
VPC condiviso

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

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

Più progetti Google Cloud

Cloud Volumes ONTAP non deve più essere nello stesso progetto di Cloud Manager. Aggiungi l'account e il ruolo del servizio Cloud Manager a progetti aggiuntivi e potrai scegliere tra i progetti che distribuisci Cloud Volumes ONTAP.



Per ulteriori informazioni sulla configurazione dell'account del servizio Cloud Manager, "vedere la fase 4b di questa pagina".

Chiavi di crittografia gestite dal cliente quando si utilizzano API Cloud Manager

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare le API di Cloud Manager per creare un nuovo sistema Cloud Volumes ONTAP che utilizza *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che vengono generate e gestite in GCP utilizzando il Cloud Key Management Service.

Fare riferimento a. "Guida per sviluppatori API" Per ulteriori informazioni sull'utilizzo dei parametri "GcpEncryption".

Questa funzione richiede nuove autorizzazioni, come mostrato nella più recente "Policy di Cloud Manager per GCP":

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Miglioramento del backup su S3

È ora possibile eliminare i backup dei volumi esistenti. In precedenza, era possibile eliminare solo i backup dei volumi che erano stati eliminati.

"Scopri di più su Backup in S3".

Crittografia dei dischi di boot e root in AWS

Quando si attiva la crittografia dei dati utilizzando il servizio di gestione delle chiavi AWS, vengono crittografati anche i dischi di avvio e i dischi root per Cloud Volumes ONTAP. Questo include il disco di boot per l'istanza del mediatore in una coppia ha. I dischi vengono crittografati utilizzando la CMK selezionata quando si crea l'ambiente di lavoro.

> I dischi di boot e root sono sempre crittografati in Azure e Google Cloud Platform perché la crittografia è attivata per impostazione predefinita in tali provider cloud.

Supporto per la regione AWS Bahrain

Cloud Manager e Cloud Volumes ONTAP sono ora supportati nell'area AWS Medio Oriente (Bahrein).

Supporto per la regione nord degli Emirati Arabi Uniti di Azure

Cloud Manager e Cloud Volumes ONTAP sono ora supportati nella regione nord degli Emirati Arabi Uniti.

"Visualizza tutte le regioni supportate".

Aggiornamento di Cloud Manager 3.7.3 (15 settembre 2019)

Cloud Manager consente ora di eseguire il backup dei dati da Cloud Volumes ONTAP ad Amazon S3.

Backup su S3

Backup su S3 è un servizio add-on per Cloud Volumes ONTAP che offre funzionalità di backup e ripristino completamente gestite per la protezione e l'archiviazione a lungo termine dei dati cloud. I backup vengono memorizzati nello storage a oggetti S3, indipendentemente dalle copie Snapshot del volume utilizzate per il ripristino o il cloning a breve termine.

"Scopri come iniziare".

Questa funzione richiede un aggiornamento di "Policy di Cloud Manager". Sono ora necessarie le seguenti autorizzazioni endpoint VPC:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Cloud Manager 3.7.3 (11 settembre 2019)

Cloud Manager 3.7.3 include i seguenti miglioramenti.

- Rilevamento e gestione di Cloud Volumes Service per AWS
- È richiesto un nuovo abbonamento in AWS Marketplace
- Supporto per AWS GovCloud (USA-Est)

Rilevamento e gestione di Cloud Volumes Service per AWS

Cloud Manager ti consente ora di scoprire i volumi cloud nel tuo "Cloud Volumes Service per AWS" iscrizione. Dopo il rilevamento, puoi aggiungere altri volumi cloud direttamente da Cloud Manager. Questo miglioramento offre un singolo pannello di controllo da cui è possibile gestire il cloud storage NetApp.

"Scopri come iniziare".

È richiesto un nuovo abbonamento in AWS Marketplace

"Un nuovo abbonamento è disponibile in AWS Marketplace". Questo abbonamento una tantum è necessario per implementare Cloud Volumes ONTAP 9.6 PAYGO (ad eccezione del sistema in prova gratuita per 30 giorni). L'abbonamento ci consente inoltre di offrire funzionalità aggiuntive per Cloud Volumes ONTAP PAYGO e BYOL. Da questo abbonamento ti verranno addebitati i costi per ogni sistema PAYGO Cloud Volumes ONTAP creato e per ogni funzionalità add-on che abiliti.

A partire dalla versione 9.6, questo nuovo metodo di abbonamento sostituisce le due sottoscrizioni AWS Marketplace esistenti per Cloud Volumes ONTAP PAYGO a cui si è precedentemente abbonati. È comunque necessario effettuare gli abbonamenti tramite "Pagine esistenti di AWS Marketplace durante l'implementazione di Cloud Volumes ONTAP BYOL".

"Scopri di più su ogni pagina di AWS Marketplace".

Supporto per AWS GovCloud (USA-Est)

Cloud Manager e Cloud Volumes ONTAP sono ora supportati nell'area AWS GovCloud (USA-Est).

Disponibilità generale di Cloud Volumes ONTAP in GCP (3 settembre 2019)

Cloud Volumes ONTAP è ora generalmente disponibile nella piattaforma cloud Google (GCP) quando si porta la propria licenza (BYOL). È disponibile anche una promozione pay-as-you-go. La promozione offre licenze gratuite per un numero illimitato di sistemi e scadrà alla fine di settembre 2019.

- "Scopri come iniziare a utilizzare GCP"
- "Visualizzare le configurazioni supportate"

Cloud Manager 3.7.2 (5 agosto 2019)

- Licenze FlexCache
- Kubernetes classi di storage per iSCSI
- Gestione degli inode
- Supporto per la regione di Hong Kong in AWS
- Supporto per le regioni centrali australiane in Azure

Licenze FlexCache

Cloud Manager genera ora una licenza FlexCache per tutti i nuovi sistemi Cloud Volumes ONTAP. La licenza include un limite di utilizzo di 500 GB.

Per generare la licenza, Cloud Manager deve accedere a https://ipa-signer.cloudmanager.netapp.com. Assicurarsi che questo URL sia accessibile dal firewall.

Kubernetes classi di storage per iSCSI

Quando si connette Cloud Volumes ONTAP a un cluster Kubernetes, Cloud Manager crea ora due classi di storage Kubernetes aggiuntive che è possibile utilizzare con i volumi persistenti iSCSI:

- **netapp-file-san**: Per il binding di volumi persistenti iSCSI a sistemi Cloud Volumes ONTAP a nodo singolo
- **netapp-file-ridondanti-san**: Per il binding di volumi persistenti iSCSI a coppie Cloud Volumes ONTAP ha

Gestione degli inode

Cloud Manager ora monitora l'utilizzo dell'inode su un volume. Quando viene utilizzato il 85% degli inode, Cloud Manager aumenta le dimensioni del volume per aumentare il numero di inode disponibili. Il numero di file che un volume può contenere è determinato dal numero di inode.

> Cloud Manager monitora l'utilizzo dell'inode solo quando Capacity Management Mode (modalità di gestione della capacità) è impostato su Automatic (automatica) (impostazione predefinita).

Supporto per la regione di Hong Kong in AWS

Cloud Manager e Cloud Volumes ONTAP sono ora supportati nell'area Asia-Pacifico (Hong Kong) in AWS.

Supporto per le regioni centrali australiane in Azure

Cloud Manager e Cloud Volumes ONTAP sono ora supportati nelle seguenti aree di Azure:

- Australia Centrale
- Australia Centrale 2

"Consulta l'elenco completo delle regioni supportate".

Aggiornamento su backup e ripristino (15 luglio 2019)

A partire dalla versione 3.7.1, Cloud Manager non supporta più il download e l'utilizzo di un backup per ripristinare la configurazione di Cloud Manager. "Per ripristinare Cloud Manager, devi seguire questa procedura".

Cloud Manager 3.7.1 (1 luglio 2019)

- Questa versione include principalmente correzioni di bug.
- Include un miglioramento: Ora Cloud Manager installa una licenza NetApp per la crittografia dei volumi (NVE) su ogni sistema Cloud Volumes ONTAP registrato con il supporto NetApp (sia sistemi nuovi che esistenti).
  - "Aggiunta di account NetApp Support Site a Cloud Manager"
  - "Registrazione di sistemi pay-as-you-go"
  - "Configurazione di NetApp Volume Encryption"

> Cloud Manager non installa la licenza NVE sui sistemi che risiedono nell'area geografica Cina.

Aggiornamento di Cloud Manager 3.7 (16 giugno 2019)

Cloud Volumes ONTAP 9.6 è ora disponibile in AWS, Azure e in Google Cloud Platform come anteprima privata. Per partecipare all'anteprima privata, invia una richiesta all'indirizzo ng-Cloud-Volume-ONTAP-preview@netapp.com.

"Scopri le novità di Cloud Volumes ONTAP 9.6"

Cloud Manager 3.7 (5 giugno 2019)

- Supporto per la prossima release di Cloud Volumes ONTAP 9.6
- Account NetApp Cloud Central
- Backup e ripristino con Cloud Backup Service

Supporto per la prossima release di Cloud Volumes ONTAP 9.6

Cloud Manager 3.7 include il supporto per la prossima release di Cloud Volumes ONTAP 9.6. La versione 9.6 include un'anteprima privata di Cloud Volumes ONTAP nella piattaforma cloud di Google. Aggiorneremo le note di rilascio non appena sarà disponibile 9.6.

Account NetApp Cloud Central

Abbiamo migliorato il modo in cui gestisci le tue risorse cloud. Ciascun sistema Cloud Manager verrà associato a un *account NetApp Cloud Central*. L'account consente la multi-tenancy ed è pianificato per altri servizi dati cloud NetApp in futuro.

In Cloud Manager, un account Cloud Central è un container per i tuoi sistemi Cloud Manager e le *aree di lavoro* in cui gli utenti implementano Cloud Volumes ONTAP.

"Scopri come gli account Cloud Central consentono la multi-tenancy".

> Cloud Manager deve accedere a _ https://cloudmanager.cloud.netapp.com_ per connettersi al servizio account Cloud Central. Aprire questo URL sul firewall per assicurarsi che Cloud Manager possa contattare il servizio.

Integrazione del sistema con gli account Cloud Central

Qualche tempo dopo l'aggiornamento a Cloud Manager 3.7, NetApp sceglierà sistemi Cloud Manager specifici da integrare con gli account Cloud Central. Durante questo processo, NetApp crea un account, assegna nuovi ruoli a ciascun utente, crea aree di lavoro e colloca gli ambienti di lavoro esistenti in tali aree di lavoro. Non c'è alcuna interruzione dei sistemi Cloud Volumes ONTAP.

"In caso di domande, consulta le domande frequenti".

Backup e ripristino con Cloud Backup Service

NetApp Cloud Backup Service per Cloud Volumes ONTAP offre funzionalità di backup e ripristino completamente gestite per la protezione e l'archiviazione a lungo termine dei dati del cloud. È possibile integrare Cloud Backup Service con Cloud Volumes ONTAP per AWS. I backup creati dal servizio vengono memorizzati nello storage a oggetti AWS S3.

"Scopri di più su Cloud Backup Service".

Per iniziare, installare e configurare l'agente di backup, quindi avviare le operazioni di backup e ripristino. Se

hai bisogno di aiuto, ti consigliamo di contattarci utilizzando l'icona della chat in Cloud Manager.

Questo processo manuale non è più supportato. La funzionalità Backup in S3 è stata integrata in Cloud Manager nella release 3.7.3.

Problemi noti

I problemi noti identificano i problemi che potrebbero impedire l'utilizzo corretto di questa versione del prodotto.

Non ci sono problemi noti in questa versione di Cloud Manager.

I problemi noti relativi a Cloud Volumes ONTAP sono disponibili in "Note di rilascio di Cloud Volumes ONTAP" E per il software ONTAP in generale in "Note di rilascio di ONTAP".

Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

Cloud Manager deve rimanere sempre in esecuzione

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

Gli host Linux condivisi non sono supportati

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

Cloud Manager non supporta i volumi FlexGroup

Anche se Cloud Volumes ONTAP supporta FlexGroup Volumes, non lo fa. Se si crea un volume FlexGroup da Gestore di sistema o dall'interfaccia CLI, impostare la modalità di gestione della capacità di Cloud Manager su Manuale. La modalità automatica potrebbe non funzionare correttamente con i volumi FlexGroup.

Active Directory non è supportato per impostazione predefinita con le nuove installazioni di Cloud Manager

A partire dalla versione 3.4, le nuove installazioni di Cloud Manager non supportano l'utilizzo dell'autenticazione Active Directory dell'organizzazione per la gestione degli utenti. Se necessario, NetApp può aiutarti a configurare Active Directory con Cloud Manager. Fare clic sull'icona della chat in basso a destra in Cloud Manager per ottenere assistenza.

Limitazioni dell'area geografica AWS GovCloud (USA)

- Cloud Manager deve essere implementato nell'area geografica AWS GovCloud (USA) se si desidera avviare istanze di Cloud Volumes ONTAP nell'area geografica AWS GovCloud (USA).
- Se implementato nell'area geografica AWS GovCloud (USA), Cloud Manager non è in grado di rilevare i cluster ONTAP in una configurazione NetApp Private Storage per Microsoft Azure o NetApp Private

Storage per SoftLayer.

Cloud Manager non imposta i volumi iSCSI

Quando si crea un volume in Cloud Manager utilizzando Storage System View, è possibile scegliere il protocollo NFS o CIFS. Per creare un volume per iSCSI, è necessario utilizzare Gestore di sistema di OnCommand.

Limitazione di Storage Virtual Machine (SVM)

Cloud Volumes ONTAP supporta una SVM per la gestione dei dati e una o più SVM utilizzate per il disaster recovery. L'unica SVM che serve dati copre l'intero sistema Cloud Volumes ONTAP (coppia ha o nodo singolo).

Cloud Manager non fornisce alcun supporto di configurazione o orchestrazione per il disaster recovery SVM. Inoltre, non supporta attività correlate allo storage su SVM aggiuntive. Per il disaster recovery di SVM, è necessario utilizzare System Manager o CLI.

Concetti

Panoramica di Cloud Manager e Cloud Volumes ONTAP

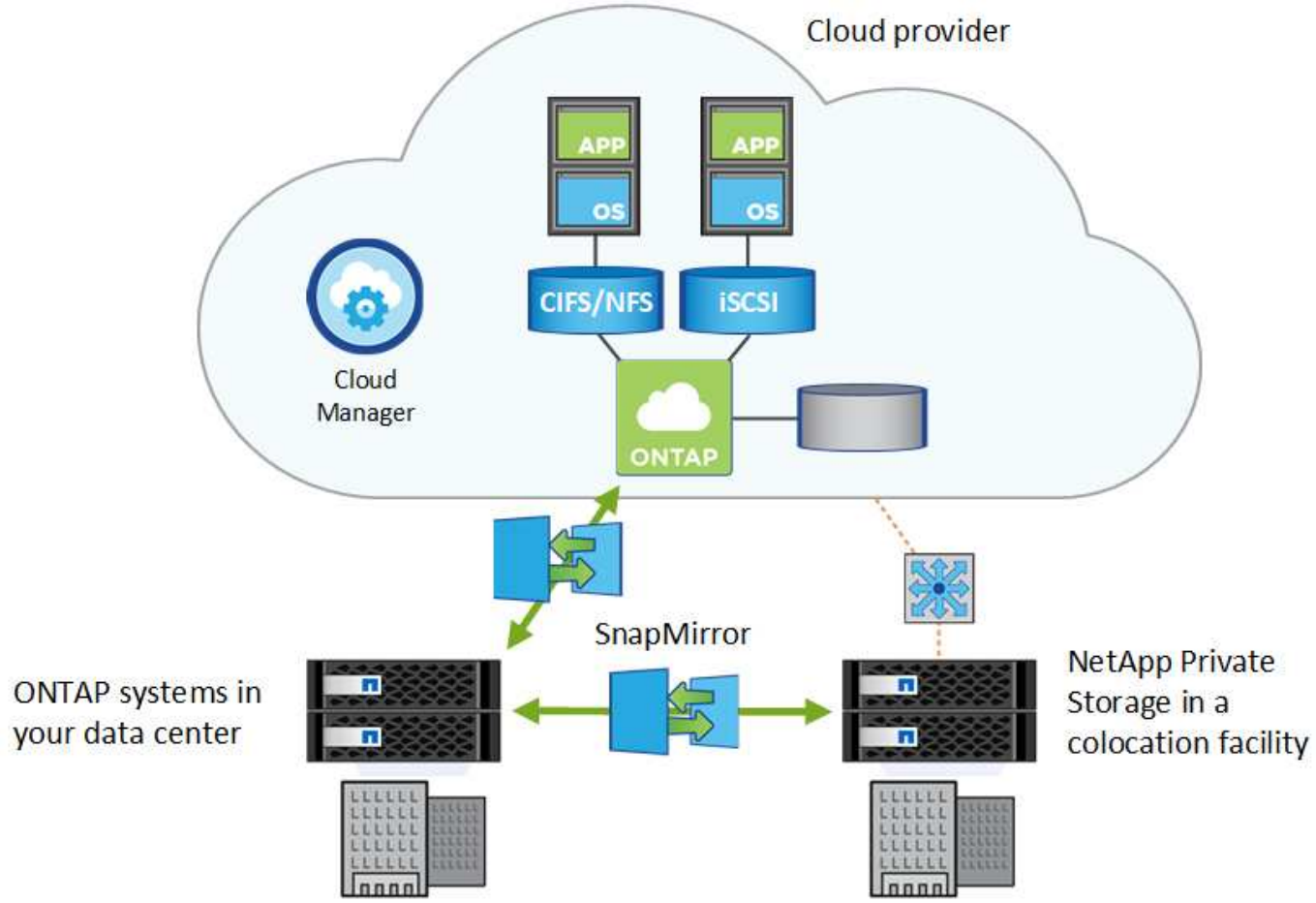
Cloud Manager ti consente di implementare Cloud Volumes ONTAP, che offre funzionalità di livello Enterprise per il tuo cloud storage, e di replicare facilmente i dati tra cloud ibridi basati su NetApp.

Cloud Manager

Cloud Manager è stato costruito pensando alla semplicità. Ti guida nella configurazione di Cloud Volumes ONTAP in pochi passaggi, semplifica la gestione dei dati offrendo provisioning dello storage semplificato e gestione automatica della capacità, consente la replica dei dati drag-and-drop in un cloud ibrido e molto altro ancora.

Cloud Manager è necessario per implementare e gestire Cloud Volumes ONTAP, ma può anche rilevare ed eseguire il provisioning dello storage per cluster ONTAP on-premise. Questo offre un punto di controllo centrale per la tua infrastruttura di cloud e storage on-premise.

Puoi eseguire Cloud Manager nel cloud o nella tua rete: Serve solo una connessione alle reti in cui desideri implementare Cloud Volumes ONTAP. La seguente immagine mostra Cloud Manager e Cloud Volumes ONTAP in esecuzione in un cloud provider. Mostra inoltre la replica dei dati in un cloud ibrido.



"Scopri di più su Cloud Manager"

Cloud Volumes ONTAP

Cloud Volumes ONTAP è un'appliance di storage solo software che esegue il software di gestione dei dati ONTAP nel cloud. Puoi utilizzare Cloud Volumes ONTAP per carichi di lavoro di produzione, disaster recovery, DevOps, condivisioni di file e gestione del database.

Cloud Volumes ONTAP estende lo storage aziendale al cloud con le seguenti funzionalità chiave:

- Le efficienze dello storage sfruttano la deduplica integrata dei dati, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi dello storage.
- L'alta disponibilità garantisce affidabilità aziendale e operazioni continue in caso di guasti nel tuo ambiente cloud.
- Replica dei dati Cloud Volumes ONTAP sfrutta SnapMirror, la tecnologia di replica leader del settore di NetApp, per replicare i dati on-premise nel cloud, in modo da poter disporre di copie secondarie per diversi casi di utilizzo.
- Tiering dei dati passa tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.
- La coerenza delle applicazioni garantisce la coerenza delle copie Snapshot di NetApp utilizzando NetApp SnapCenter.

Le licenze per le funzioni ONTAP sono incluse in Cloud Volumes ONTAP.

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

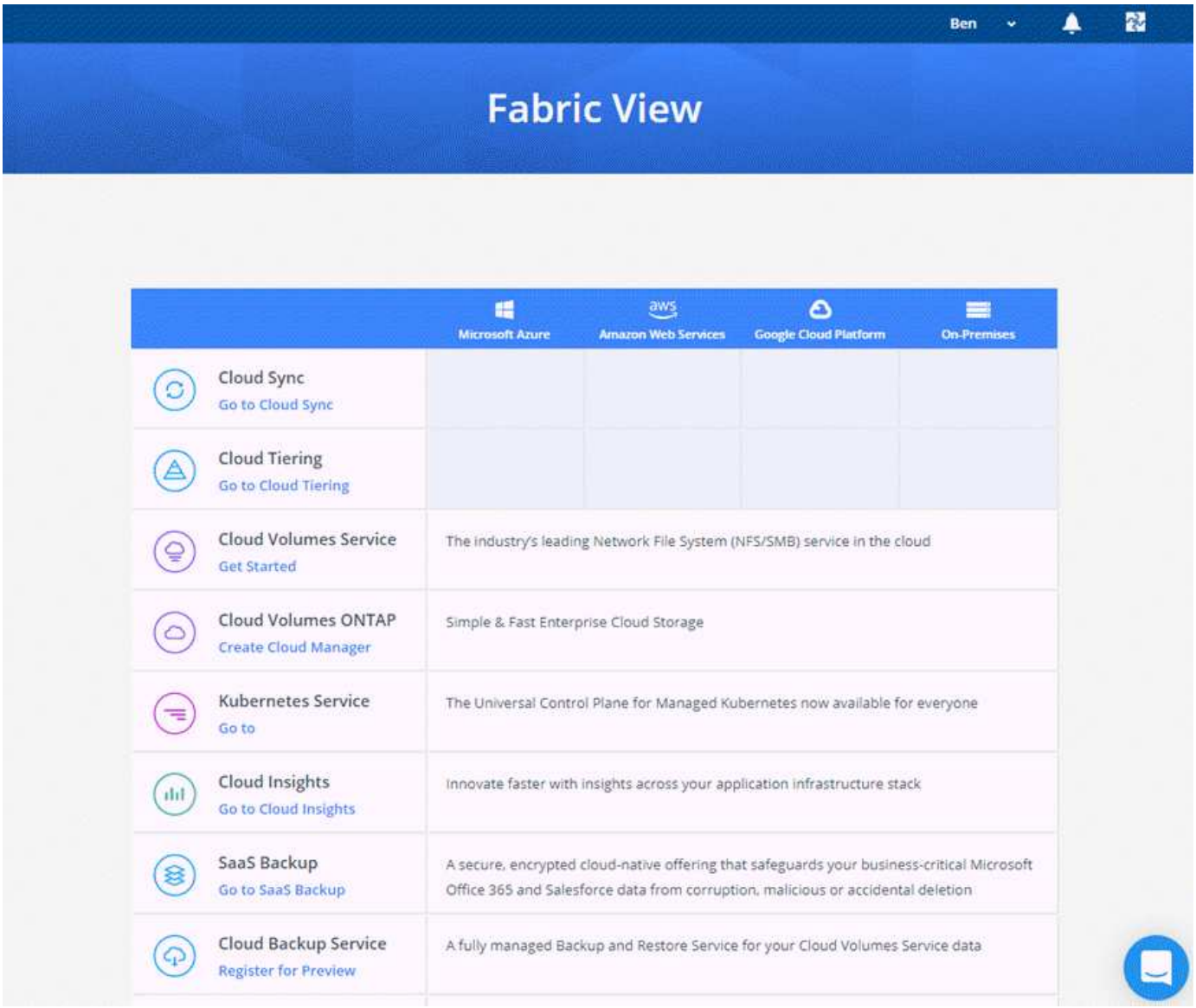
"Scopri di più su Cloud Volumes ONTAP"

NetApp Cloud Central

"NetApp Cloud Central" Fornisce una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi ti consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il backup dei dati SaaS e migrare e controllare in modo efficace i dati su più cloud.

L'integrazione di Cloud Manager con NetApp Cloud Central offre diversi vantaggi, tra cui un'esperienza di implementazione semplificata, un'unica posizione per visualizzare e gestire più sistemi Cloud Manager e autenticazione utente centralizzata.

Con l'autenticazione utente centralizzata, è possibile utilizzare lo stesso set di credenziali nei sistemi Cloud Manager e tra Cloud Manager e altri servizi dati, come Cloud Sync. È anche facile reimpostare la password se la si dimentica.



Account Cloud Central

Ogni sistema Cloud Manager è associato a un *account NetApp Cloud Central*. Un account Cloud Central offre multi-tenancy e consente di organizzare utenti e risorse in aree di lavoro isolate.

Un account Cloud Central consente la multi-tenancy:

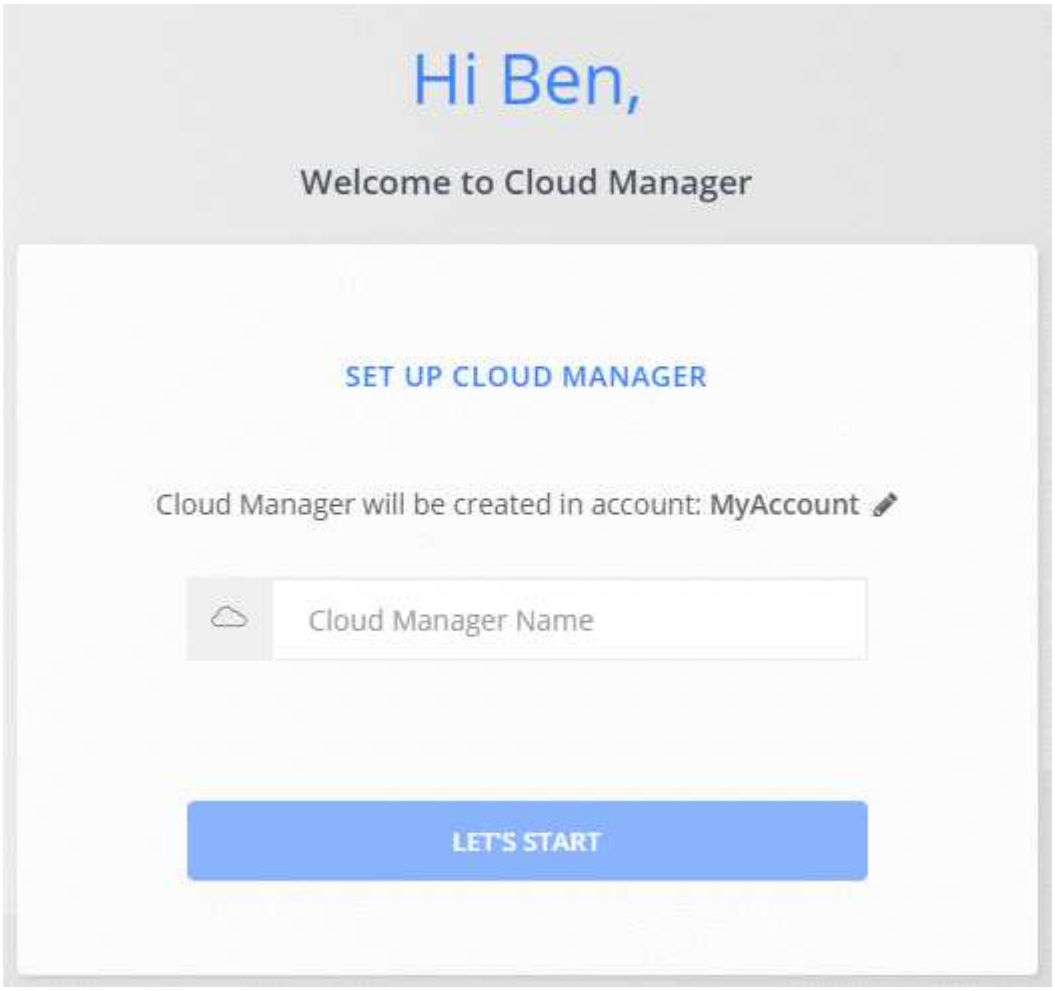
- Un singolo account Cloud Central può includere più sistemi Cloud Manager che soddisfano diverse esigenze di business.

  Poiché gli utenti sono associati all'account Cloud Central, non è necessario configurare gli utenti per ogni singolo sistema Cloud Manager.

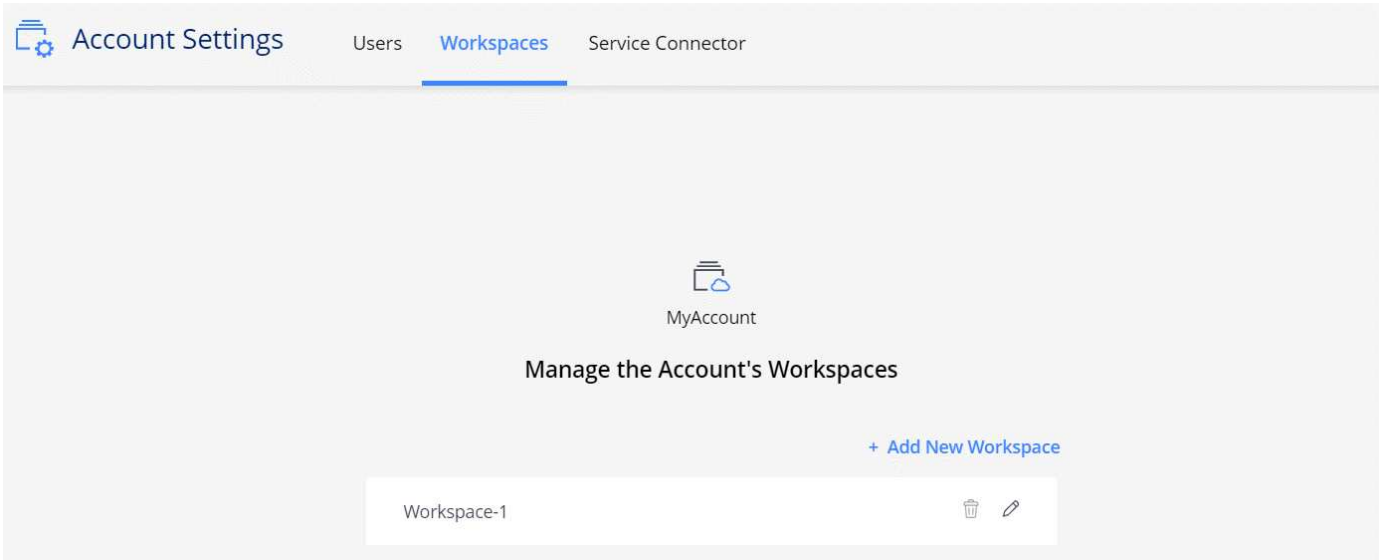
- All'interno di ogni sistema Cloud Manager, più utenti possono implementare e gestire i sistemi Cloud Volumes ONTAP in ambienti isolati, chiamati spazi di lavoro.

  Queste aree di lavoro sono invisibili agli altri utenti, a meno che non siano condivise.

Quando si implementa Cloud Manager, si seleziona l'account Cloud Central da associare al sistema:



Gli amministratori degli account possono quindi modificare le impostazioni di questo account gestendo utenti, aree di lavoro e connettori di servizio:



Per istruzioni dettagliate, vedere "Configurazione dell'account Cloud Central".

Cloud Manager deve accedere a _ https://cloudmanager.cloud.netapp.com_ per connettersi al servizio account Cloud Central. Aprire questo URL sul firewall per assicurarsi che Cloud Manager possa contattare il servizio.

Utenti, aree di lavoro e connettori di servizio

Il widget Impostazioni account in Cloud Manager consente agli amministratori account di gestire un account Cloud Central. Se hai appena creato il tuo account, partirai da zero. Tuttavia, se hai già configurato un account, vedrai *tutti* gli utenti, le aree di lavoro e i connettori di servizio associati all'account.

Utenti

Si tratta di utenti di NetApp Cloud Central che si associano al proprio account Cloud Central. L'associazione di un utente a un account e a una o più aree di lavoro in tale account consente a tali utenti di creare e gestire ambienti di lavoro in Cloud Manager.

Quando si associa un utente, viene assegnato un ruolo:

- *Account Admin*: Può eseguire qualsiasi azione in Cloud Manager.
- *Workspace Admin*: Consente di creare e gestire le risorse nell'area di lavoro assegnata.

Aree di lavoro

In Cloud Manager, uno spazio di lavoro isola qualsiasi numero di *ambienti di lavoro* da altri ambienti di lavoro. Gli amministratori dell'area di lavoro non possono accedere agli ambienti di lavoro in un'area di lavoro a meno che l'amministratore dell'account non colleghi l'amministratore a tale area di lavoro.

Un ambiente di lavoro rappresenta un sistema storage:

- Un sistema Cloud Volumes ONTAP a nodo singolo o una coppia ha
- Un cluster ONTAP on-premise nella rete
- Un cluster ONTAP in una configurazione di storage privato NetApp

Connettori di servizio

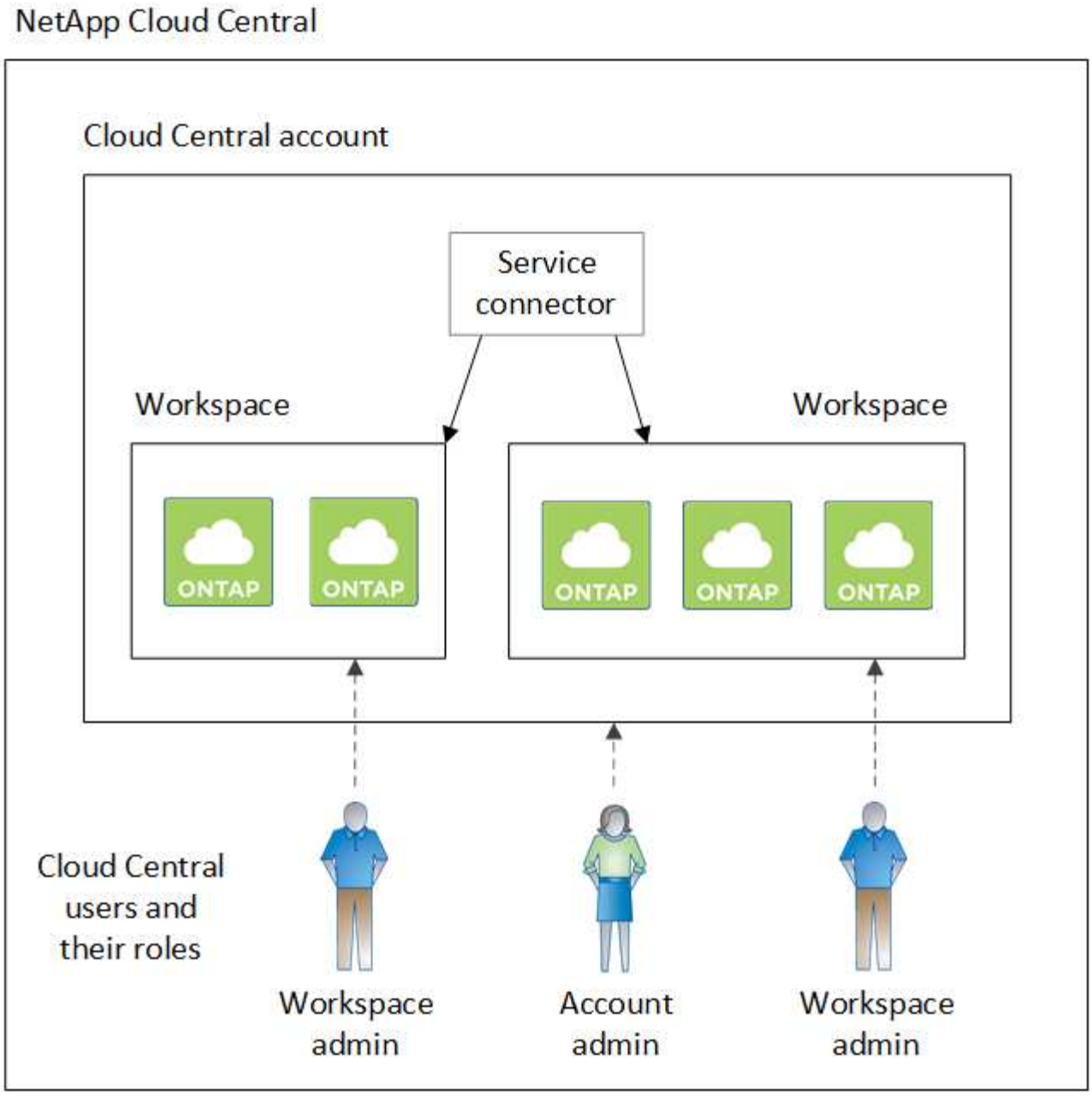
Un Service Connector fa parte di Cloud Manager. Esegue gran parte del software Cloud Manager (come l'interfaccia utente), ad eccezione di alcuni servizi Cloud Central a cui si connette (account auth0 e Cloud Central). Il Service Connector viene eseguito sull'istanza della macchina virtuale implementata nel provider di servizi cloud o su un host on-premise configurato.

È possibile utilizzare un connettore di servizio con più di un servizio dati cloud NetApp. Ad esempio, se si dispone già di un Service Connector per Cloud Manager, è possibile selezionarlo quando si imposta il servizio Cloud Tiering.

Esempi

Nell'esempio seguente viene illustrato un account che utilizza due aree di lavoro per creare ambienti isolati per i sistemi Cloud Volumes ONTAP. Ad esempio, un'area di lavoro potrebbe essere per un ambiente di staging, mentre l'altra per un ambiente di produzione.

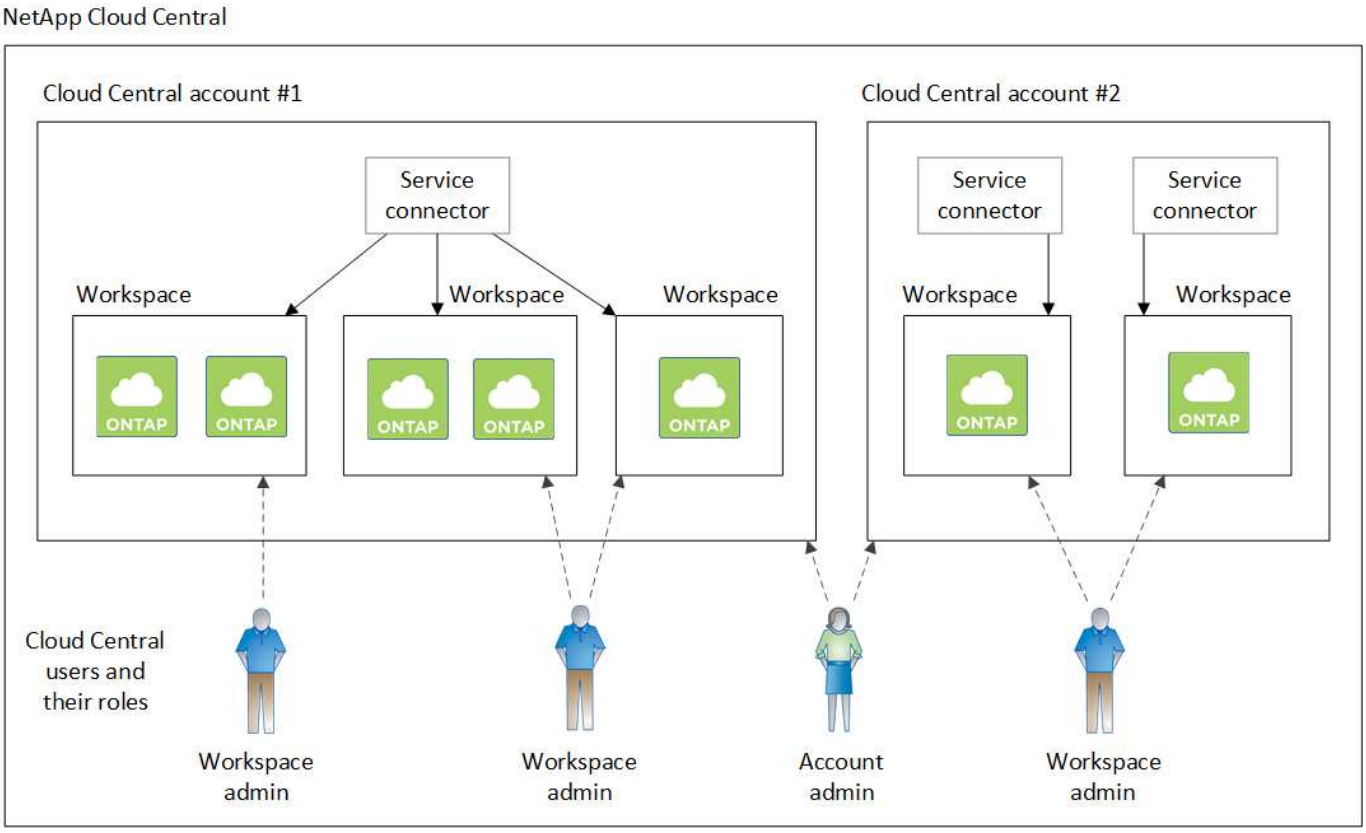
Cloud Manager e i sistemi Cloud Volumes ONTAP non risiedono nell'account NetApp Cloud Central, ma vengono eseguiti in un cloud provider. Si tratta di una rappresentazione concettuale della relazione tra ciascun componente.



Ecco un altro esempio che mostra il più alto livello di multi-tenancy utilizzando due account Cloud Central separati. Ad esempio, un service provider potrebbe utilizzare Cloud Manager in un account Cloud Central per fornire servizi ai propri clienti, mentre utilizza un altro account per fornire il disaster recovery per una delle proprie business unit.

L'account 2 include due connettori di servizio separati. Questo potrebbe verificarsi se i sistemi sono in regioni separate o in provider cloud separati.

Anche in questo caso, i sistemi Cloud Manager e Cloud Volumes ONTAP non risiedono nell'account NetApp Cloud Central, ma sono in esecuzione in un cloud provider. Si tratta di una rappresentazione concettuale della relazione tra ciascun componente.



FAQ per l'integrazione con gli account Cloud Central

Qualche tempo dopo l'aggiornamento a Cloud Manager 3.7, NetApp sceglierà sistemi Cloud Manager specifici da integrare con gli account Cloud Central. Queste FAQ possono rispondere alle domande che potresti avere sul processo.

Quanto tempo richiede il processo?

In pochi minuti.

Cloud Manager non sarà disponibile?

No, puoi comunque accedere al tuo sistema Cloud Manager.

E Cloud Volumes ONTAP?

Non c'è alcuna interruzione dei sistemi Cloud Volumes ONTAP.

Cosa succede durante questo processo?

Durante il processo di integrazione, NetApp esegue le seguenti operazioni:

1. Crea un nuovo account Cloud Central e lo associa al tuo sistema Cloud Manager.
2. Assegna nuovi ruoli a ciascun utente esistente:
   - Gli amministratori di Cloud Manager diventano account Admins
   - Gli amministratori dei tenant e gli amministratori dell'ambiente di lavoro diventano amministratori dell'area di lavoro

3. Crea aree di lavoro che sostituiscono i tenant esistenti.
4. Posiziona i tuoi ambienti di lavoro in quelle aree di lavoro.
5. Associa il connettore di servizio a tutte le aree di lavoro.

È importante dove ho installato il sistema Cloud Manager?

No NetApp integrerà i sistemi con gli account Cloud Central indipendentemente da dove risiedono, sia in AWS, Azure o on-premise.

Account di cloud provider

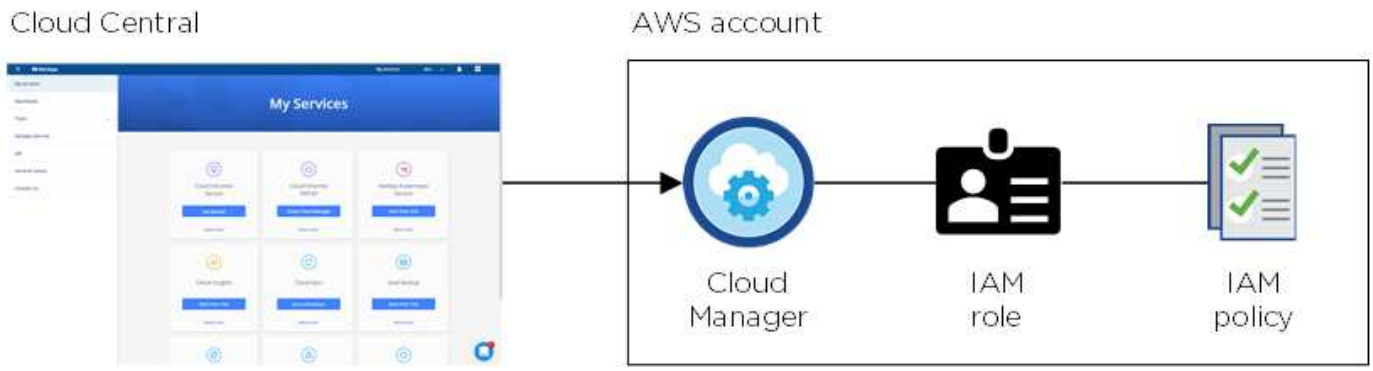
Account e autorizzazioni AWS

Cloud Manager consente di scegliere l'account AWS in cui si desidera implementare un sistema Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP nell'account AWS iniziale oppure impostare account aggiuntivi.

L'account AWS iniziale

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

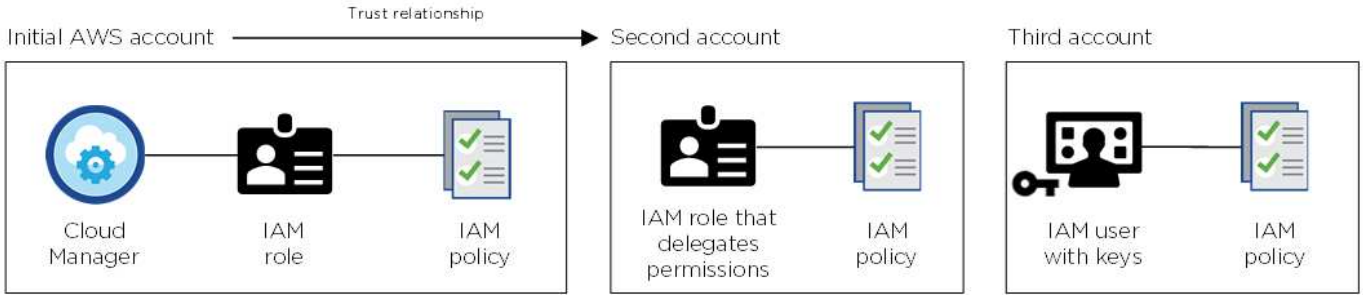
Quando Cloud Central avvia l'istanza di Cloud Manager in AWS, crea un ruolo IAM e un profilo di istanza per l'istanza. Allega inoltre una policy che fornisce a Cloud Manager le autorizzazioni per implementare e gestire Cloud Volumes ONTAP in quell'account AWS. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".



Cloud Manager seleziona questo account cloud provider per impostazione predefinita quando crei un nuovo ambiente di lavoro:

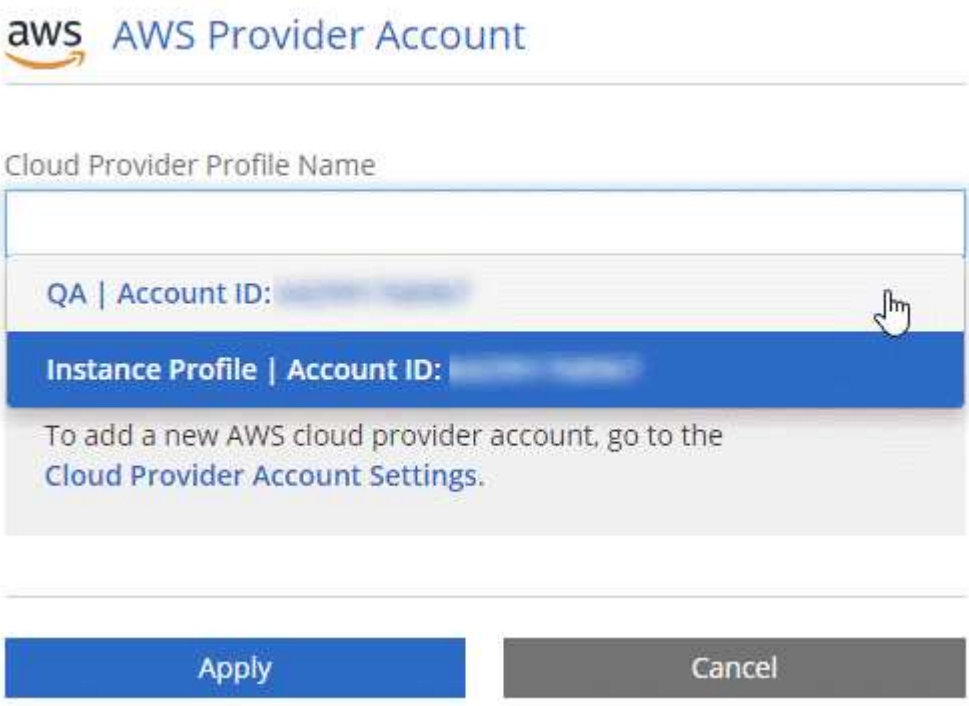
Account AWS aggiuntivi

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



Allora "Aggiungi gli account del provider cloud a Cloud Manager" Specificando il nome risorsa Amazon (ARN) del ruolo IAM o le chiavi AWS per l'utente IAM.

Dopo aver aggiunto un altro account, è possibile passare a tale account durante la creazione di un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato da NetApp Cloud Central. È inoltre possibile implementare Cloud Manager in AWS da "Mercato AWS" e puoi farlo "Installazione di Cloud Manager on-premise".

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente il ruolo IAM, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

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

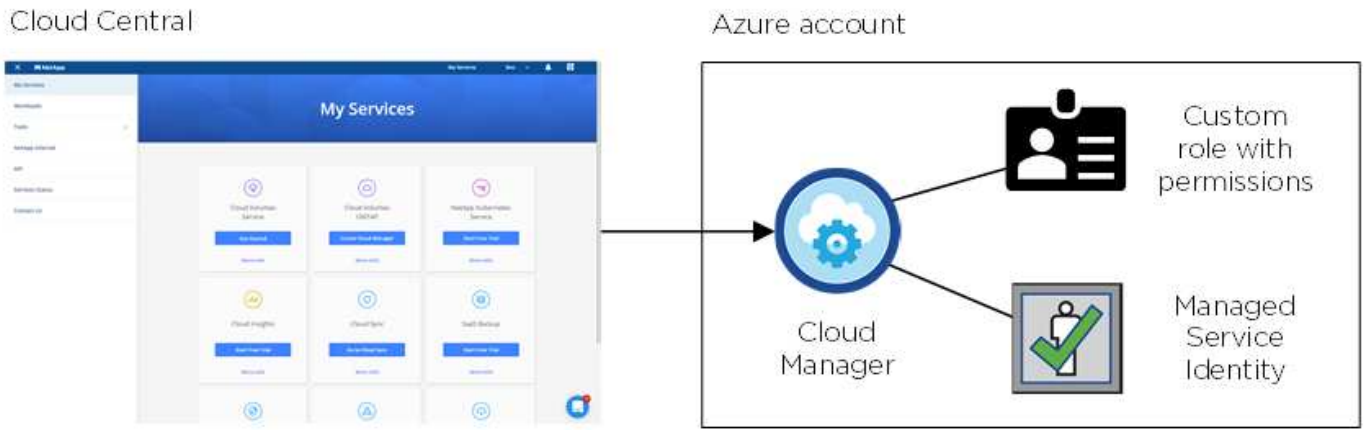
Account e autorizzazioni Azure

Cloud Manager consente di scegliere l'account Azure in cui si desidera implementare un sistema Cloud Volumes ONTAP. Puoi implementare tutti i tuoi sistemi Cloud Volumes ONTAP nell'account Azure iniziale oppure puoi impostare altri account.

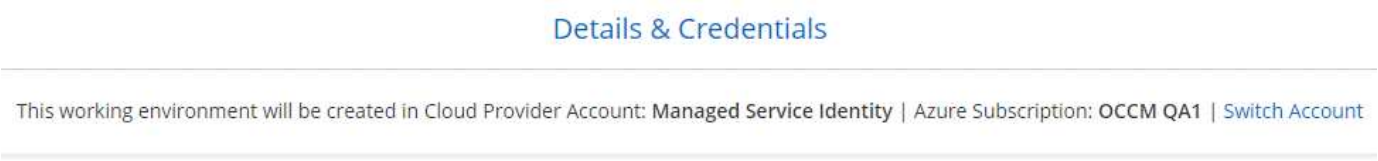
L'account Azure iniziale

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. Le autorizzazioni richieste sono elencate nella "Policy di NetApp Cloud Central per Azure".

Quando Cloud Central implementa la macchina virtuale Cloud Manager in Azure, abilita una "identità gestita assegnata dal sistema" Sulla macchina virtuale Cloud Manager, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce a Cloud Manager le autorizzazioni per implementare e gestire Cloud Volumes ONTAP in quell'abbonamento Azure. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".



Cloud Manager seleziona questo account cloud provider per impostazione predefinita quando crei un nuovo ambiente di lavoro:

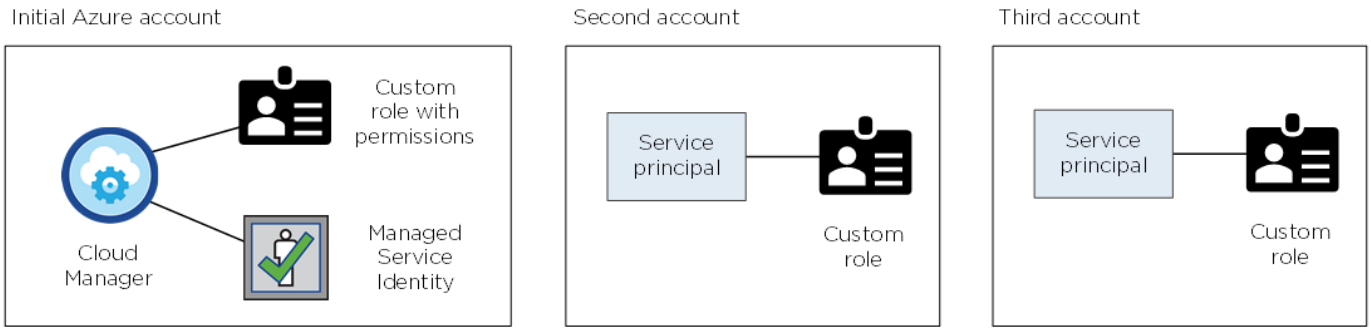


Abbonamenti Azure aggiuntivi per l'account iniziale

L'identità gestita è associata all'abbonamento con cui hai lanciato Cloud Manager. Se si desidera selezionare un abbonamento Azure diverso, è necessario "associare l'identità gestita a tali sottoscrizioni".

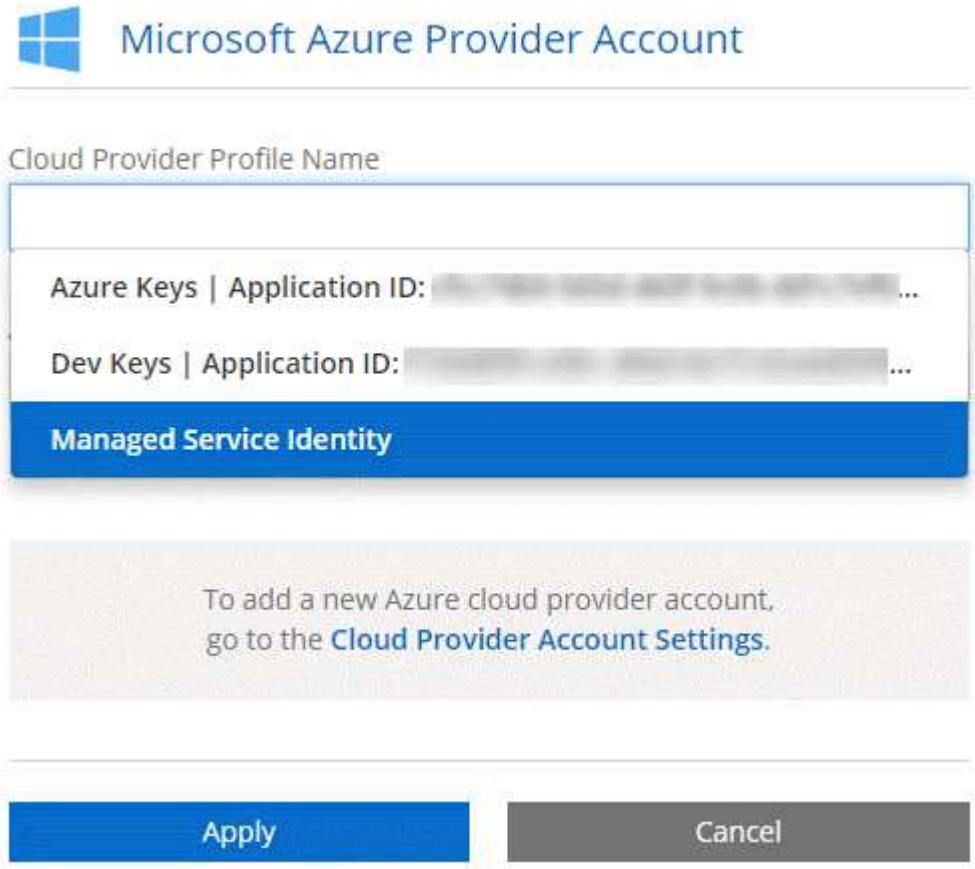
Altri account Azure

Se si desidera implementare Cloud Volumes ONTAP in diversi account Azure, è necessario concedere le autorizzazioni richieste da "Creazione e configurazione di un'entità di servizio in Azure Active Directory" Per ciascun account Azure. L'immagine seguente mostra due account aggiuntivi, ciascuno configurato con un'entità del servizio e un ruolo personalizzato che fornisce le autorizzazioni:



Allora "Aggiungi gli account del provider cloud a Cloud Manager" Fornendo dettagli sull'identità del servizio ad.

Dopo aver aggiunto un altro account, è possibile passare a tale account durante la creazione di un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato da NetApp Cloud Central. È inoltre possibile implementare Cloud Manager in Azure da "Azure Marketplace"e puoi farlo "Installazione di Cloud Manager on-premise".

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. Devi solo creare e configurare manualmente l'identità gestita per Cloud Manager, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un'identità gestita per il sistema Cloud Manager, ma è possibile fornire autorizzazioni come fareste per altri account.

Progetti, autorizzazioni e account Google Cloud

Un account di servizio fornisce a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP nello stesso progetto di Cloud Manager o in progetti diversi. Gli account Google Cloud aggiunti a Cloud Manager vengono utilizzati per abilitare il tiering dei dati.

Progetto e permessi per Cloud Manager

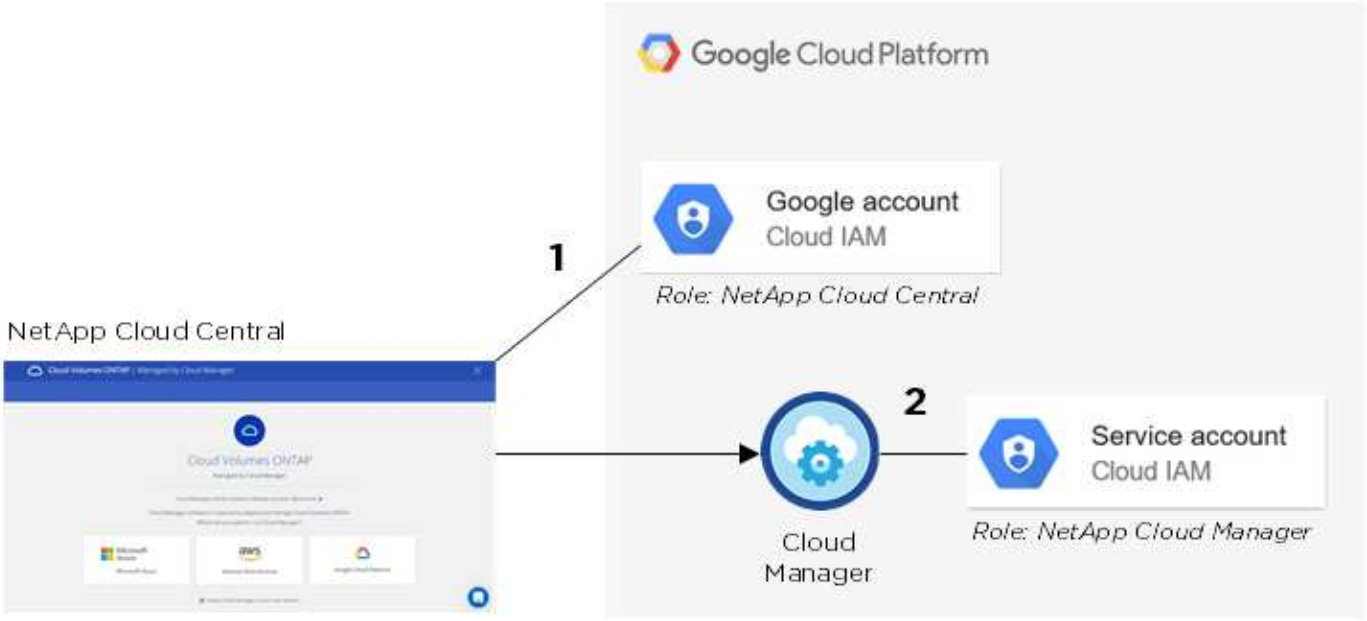
Prima di poter implementare Cloud Volumes ONTAP in Google Cloud, devi prima implementare Cloud Manager in un progetto Google Cloud. Cloud Manager non può essere eseguito in sede o in un altro cloud provider.

Prima di implementare Cloud Manager da, è necessario disporre di due set di autorizzazioni "NetApp Cloud Central":

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

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

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



Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto di Cloud Manager o in un progetto diverso. Per implementare Cloud Volumes ONTAP in un progetto diverso, devi prima aggiungere l'account del servizio e il ruolo di Cloud Manager a quel progetto.

- "Scopri come configurare l'account di servizio Cloud Manager (vedi punto 4)".
- "Scopri come implementare Cloud Volumes ONTAP in GCP e selezionare un progetto".

Account per il tiering dei dati

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

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

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

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

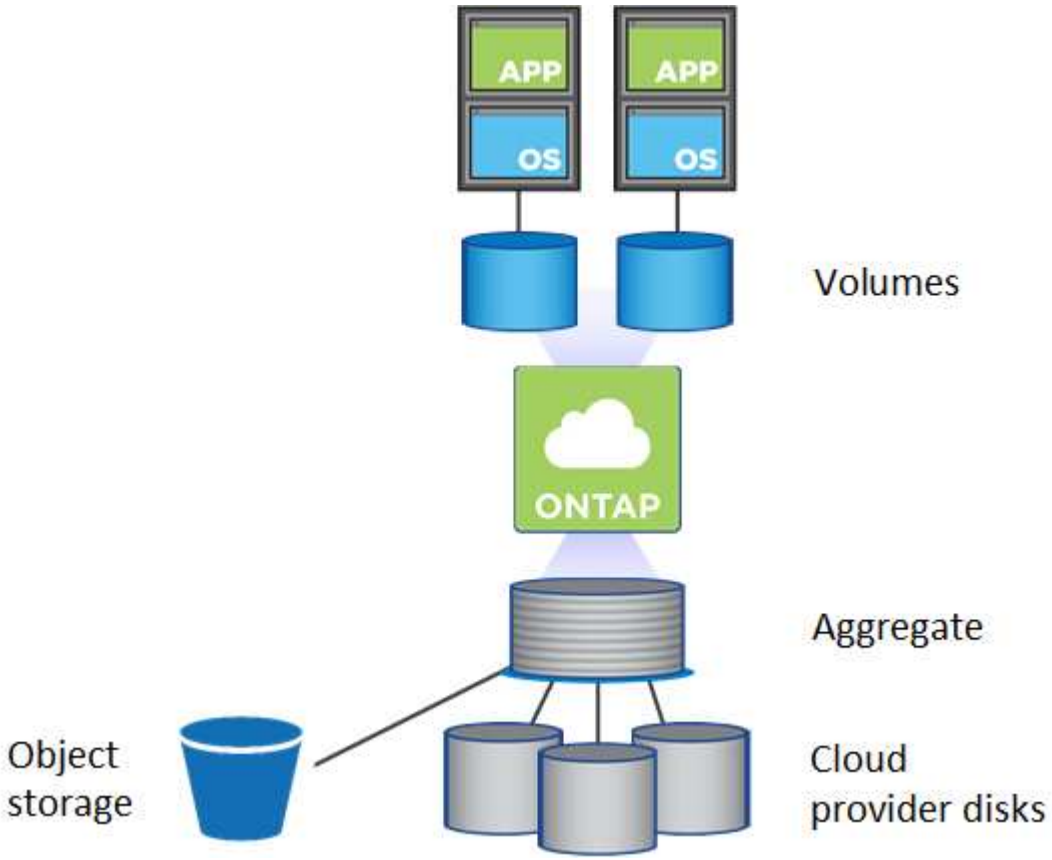
Storage

Dischi e aggregati

Comprendere come Cloud Volumes ONTAP utilizza il cloud storage può aiutarti a comprendere i costi dello storage.

Panoramica

Cloud Volumes ONTAP utilizza lo storage del cloud provider come dischi e li raggruppa in uno o più aggregati. Gli aggregati forniscono storage a uno o più volumi.



Sono supportati diversi tipi di dischi cloud. Quando si crea un volume e si sceglie il tipo di disco e la dimensione predefinita del disco quando si implementa Cloud Volumes ONTAP.

La quantità totale di storage acquistata da un cloud provider è la *capacità raw*. La *capacità utilizzabile* è inferiore perché circa il 12-14% è un overhead riservato all'utilizzo di Cloud Volumes ONTAP. Ad esempio, se Cloud Manager crea un aggregato da 500 GB, la capacità utilizzabile è di 442.94 GB.

Storage AWS

In AWS, Cloud Volumes ONTAP utilizza lo storage EBS per i dati dell'utente e lo storage NVMe locale come cache flash su alcuni tipi di istanze EC2.

Storage EBS

In AWS, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. La dimensione massima del disco è di 16 TB.

Il tipo di disco EBS sottostante può essere SSD General Purpose, SSD IOPS con provisioning, HDD ottimizzato per il throughput o HDD freddo. È possibile associare un disco EBS con Amazon S3 a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

Ad un livello elevato, le differenze tra i tipi di dischi EBS sono le seguenti:

- I dischi SSD per uso generico bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS.
- I dischi SSD IOPS con provisioning sono destinati ad applicazioni critiche che richiedono le massime performance a un costo più elevato.
- I dischi HDD_ ottimizzati per il throughput sono per carichi di lavoro con accesso frequente che richiedono un throughput rapido e coerente a un prezzo inferiore.
- I dischi *Cold HDD* sono destinati ai backup o ai dati a cui si accede raramente, perché le performance sono molto basse. Come i dischi HDD ottimizzati per il throughput, le performance sono definite in termini di throughput.

  I dischi rigidi Cold non sono supportati con configurazioni ha e con tiering dei dati.

Storage NVMe locale

Alcuni tipi di istanze EC2 includono lo storage NVMe locale, utilizzato da Cloud Volumes ONTAP "Flash cache".

Link correlati

- "Documentazione AWS: Tipi di volume EBS"
- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in AWS"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in AWS"
- "Analisi delle configurazioni supportate per Cloud Volumes ONTAP in AWS"

Storage Azure

In Azure, un aggregato può contenere fino a 12 dischi delle stesse dimensioni. Il tipo di disco e le dimensioni massime dipendono dall'utilizzo di un sistema a nodo singolo o di una coppia ha:

Sistemi a nodo singolo

I sistemi a nodo singolo possono utilizzare tre tipi di dischi gestiti Azure:

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.
- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

  Ogni tipo di disco gestito ha una dimensione massima di 32 TB.

  È possibile associare un disco gestito con lo storage Azure Blob a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

Coppie HA

Le coppie HA utilizzano i blob di pagina Premium, che hanno una dimensione massima del disco di 8 TB.

Link correlati

- "Documentazione di Microsoft Azure: Introduzione allo storage Microsoft Azure"

- "Scopri come scegliere i tipi di dischi e le dimensioni dei dischi per i tuoi sistemi in Azure"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in Azure"

Storage GCP

In GCP, un aggregato può contenere fino a 6 dischi delle stesse dimensioni. La dimensione massima del disco è di 16 TB.

Il tipo di disco può essere *dischi persistenti SSD Zonal* o *dischi persistenti standard Zonal*. È possibile associare dischi persistenti con un bucket di storage Google a. "eseguire il tier dei dati inattivi per lo storage a oggetti a basso costo".

Link correlati

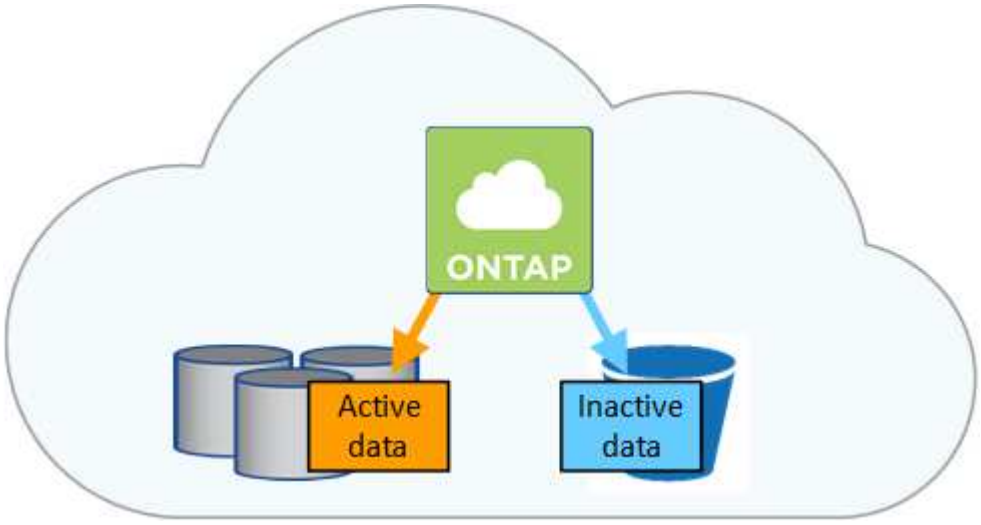
- "Documentazione di Google Cloud Platform: Opzioni di storage"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in GCP"

Tipo RAID

Il tipo di RAID per ciascun aggregato Cloud Volumes ONTAP è RAID0 (striping). Non sono supportati altri tipi di RAID. Cloud Volumes ONTAP si affida al cloud provider per la disponibilità e la durata dei dischi.

Panoramica sul tiering dei dati

Riduci i costi di storage abilitando il tiering automatizzato dei dati inattivi su storage a oggetti a basso costo. I dati attivi rimangono in SSD o HDD ad alte prestazioni, mentre i dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo. In questo modo è possibile recuperare spazio sullo storage primario e ridurre lo storage secondario.



Cloud Volumes ONTAP supporta il tiering dei dati in AWS, Azure e Google Cloud Platform. Il tiering dei dati è basato sulla tecnologia FabricPool.

Non è necessario installare una licenza per le funzionalità per attivare il tiering dei dati (FabricPool).

Tiering dei dati in AWS

Quando si abilita il tiering dei dati in AWS, Cloud Volumes ONTAP utilizza EBS come Tier di performance per i dati hot e AWS S3 come Tier di capacità per i dati inattivi. La modifica del livello di tiering di un sistema consente di scegliere una classe di storage S3 diversa.

Tier di performance

Il livello di performance può essere SSD General Purpose, SSD IOPS con provisioning o HDD ottimizzati per il throughput.

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi su un singolo bucket S3 utilizzando la classe di storage *Standard*. Standard è ideale per i dati ad accesso frequente memorizzati in più zone di disponibilità.

Cloud Manager crea un singolo bucket S3 per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket S3 diverso per ciascun volume.

Livelli di tiering

Se non intendi accedere ai dati inattivi, puoi ridurre i costi di storage modificando il livello di tiering di un sistema in uno dei seguenti: *Intelligent Tiering*, *One-zone infrequent Access* o *Standard-infrequent Access*. Quando si modifica il livello di tiering, i dati inattivi iniziano nella classe di storage Standard e vengono spostati nella classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi è necessario prendere in considerazione questo aspetto prima di modificare il livello di tiering. "Scopri di più sulle classi di storage Amazon S3".

È possibile modificare il livello di tiering dopo aver creato il sistema. Per ulteriori informazioni, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

Il livello di tiering è esteso a livello di sistema, non per volume.

Tiering dei dati in Azure

Quando abiliti il tiering dei dati in Azure, Cloud Volumes ONTAP utilizza i dischi gestiti da Azure come Tier di performance per i dati hot e lo storage Blob Azure come Tier di capacità per i dati inattivi. La modifica del livello di tiering di un sistema consente di scegliere un diverso livello di storage Azure.

Tier di performance

Il Tier di performance può essere SSD o HDD.

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo container blob utilizzando il Tier di storage Azure *hot*. Il Tier hot è ideale per i dati ad accesso frequente.

Cloud Manager crea un nuovo account storage con un singolo container per ogni ambiente di lavoro Cloud Volumes ONTAP. Il nome dell'account di storage è casuale. Non viene creato un container diverso per ogni volume.

Livelli di tiering

Se non intendi accedere ai dati inattivi, puoi ridurre i costi di storage modificando il livello di tiering di un sistema nel Tier di storage Azure *COOL*. Quando si modifica il livello di tiering, i dati inattivi vengono avviati nel livello di hot storage e spostati nel livello di cool storage, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi è necessario prendere in considerazione questo aspetto prima di modificare il livello di tiering. "Scopri di più sui Tier di accesso allo storage Azure Blob".

È possibile modificare il livello di tiering dopo aver creato il sistema. Per ulteriori informazioni, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

Il livello di tiering è esteso a livello di sistema, non per volume.

Tiering dei dati in GCP

Quando abiliti il tiering dei dati in GCP, Cloud Volumes ONTAP utilizza i dischi persistenti come Tier di performance per i dati hot e un bucket di storage cloud di Google come Tier di capacità per i dati inattivi.

Tier di performance

Il Tier di performance può essere SSD o HDD (dischi standard).

Tier di capacità

Un sistema Cloud Volumes ONTAP esegue il Tier dei dati inattivi in un singolo bucket di storage cloud di Google utilizzando la classe di storage *regionale*.

Cloud Manager crea un singolo bucket per ogni ambiente di lavoro e lo nomina fabric-pool-*cluster unique identifier*. Non viene creato un bucket diverso per ogni volume.

Livelli di tiering

Al momento non sono supportate altre classi di storage GCP.

Tiering dei dati e limiti di capacità

Se si abilita il tiering dei dati, il limite di capacità di un sistema rimane invariato. Il limite viene distribuito tra il Tier di performance e il Tier di capacità.

Policy di tiering dei volumi

Per attivare il tiering dei dati, è necessario selezionare una policy di tiering dei volumi quando si crea, modifica o replica un volume. È possibile selezionare un criterio diverso per ciascun volume.

Alcuni criteri di tiering hanno un periodo di raffreddamento minimo associato, che imposta il tempo in cui i dati dell'utente in un volume devono rimanere inattivi per essere considerati "freddi" e spostati al livello di capacità.

Cloud Manager consente di scegliere tra le seguenti policy di tiering dei volumi quando si crea o modifica un volume:

Solo Snapshot

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei dati cold user delle copie Snapshot non associate al file system attivo al Tier di capacità. Il periodo di raffreddamento è di circa 2 giorni.

In lettura, i blocchi di dati cold sul Tier di capacità diventano hot e vengono spostati sul Tier di performance.

Automatico

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei blocchi di dati cold in un volume fino a raggiungere un livello di capacità. I dati cold non includono solo le copie

Snapshot, ma anche i dati cold user dal file system attivo. Il periodo di raffreddamento è di circa 31 giorni.

Questo criterio è supportato a partire da Cloud Volumes ONTAP 9.4.

Se letti in modo casuale, i blocchi di dati cold nel Tier di capacità diventano hot e passano al Tier di performance. Se letti in base a letture sequenziali, come quelle associate a scansioni di indice e antivirus, i blocchi di dati cold rimangono freddi e non passano al livello di performance.

Nessuno

Mantiene i dati di un volume nel Tier di performance, evitando che vengano spostati nel Tier di capacità.

Quando si replica un volume, è possibile scegliere se eseguire il Tier dei dati sullo storage a oggetti. In questo caso, Cloud Manager applica il criterio **Backup** al volume di protezione dei dati. A partire da Cloud Volumes ONTAP 9.6, la policy di tiering **all** sostituisce la policy di backup.

La disattivazione di Cloud Volumes ONTAP influisce sul periodo di raffreddamento

I blocchi di dati vengono raffreddati mediante scansioni di raffreddamento. Durante questo processo, i blocchi che non sono stati utilizzati hanno spostato la temperatura del blocco (raffreddato) al valore successivo più basso. Il tempo di raffreddamento predefinito dipende dalla policy di tiering del volume:

- Auto: 31 giorni
- Solo snapshot: 2 giorni

Affinché la scansione di raffreddamento funzioni, è necessario che Cloud Volumes ONTAP sia in esecuzione. Se Cloud Volumes ONTAP è disattivato, anche il raffreddamento si interrompe. Di conseguenza, potrebbero verificarsi tempi di raffreddamento più lunghi.

Impostazione del tiering dei dati

Per istruzioni e un elenco delle configurazioni supportate, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

Gestione dello storage

Cloud Manager offre una gestione semplificata e avanzata dello storage Cloud Volumes ONTAP.

> Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da Cloud Manager. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti per i provider di cloud.

Provisioning dello storage

Cloud Manager semplifica il provisioning dello storage per Cloud Volumes ONTAP acquistando dischi e gestendo aggregati per te. È sufficiente creare volumi. Se lo si desidera, è possibile utilizzare un'opzione di allocazione avanzata per eseguire il provisioning degli aggregati.

Provisioning semplificato

Gli aggregati forniscono lo storage cloud ai volumi. Cloud Manager crea aggregati per te quando avvii un'istanza e quando esegui il provisioning di volumi aggiuntivi.

Quando crei un volume, Cloud Manager esegue una delle tre operazioni seguenti:

- Posiziona il volume su un aggregato esistente con spazio libero sufficiente.
- Il volume viene inserito in un aggregato esistente acquistando più dischi per tale aggregato.
- L'IT acquista dischi per un nuovo aggregato e colloca il volume su tale aggregato.

Cloud Manager determina dove posizionare un nuovo volume prendendo in considerazione diversi fattori: La dimensione massima di un aggregato, l'attivazione del thin provisioning e le soglie di spazio libero per gli aggregati.

L'amministratore dell'account può modificare le soglie di spazio libero dalla pagina **Impostazioni**.

Selezione delle dimensioni dei dischi per gli aggregati in AWS

Quando Cloud Manager crea nuovi aggregati per Cloud Volumes ONTAP in AWS, aumenta gradualmente la dimensione del disco in un aggregato, con l'aumentare del numero di aggregati nel sistema. Cloud Manager consente di utilizzare la capacità massima del sistema prima che raggiunga il numero massimo di dischi dati consentito da AWS.

Ad esempio, Cloud Manager può scegliere le seguenti dimensioni dei dischi per gli aggregati in un sistema Cloud Volumes ONTAP Premium o BYOL:

Numero aggregato	Dimensioni del disco	Capacità aggregata massima
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

È possibile scegliere autonomamente le dimensioni del disco utilizzando l'opzione Advanced allocation (allocazione avanzata).

Allocazione avanzata

Invece di consentire a Cloud Manager di gestire gli aggregati per te, puoi farlo da solo. "Dalla pagina **allocazione avanzata**", è possibile creare nuovi aggregati che includono un numero specifico di dischi, aggiungere dischi a un aggregato esistente e creare volumi in aggregati specifici.

Gestione della capacità

L'account Admin può scegliere se Cloud Manager notifica le decisioni relative alla capacità dello storage o se Cloud Manager gestisce automaticamente i requisiti di capacità per te. Potrebbe essere utile comprendere il funzionamento di queste modalità.

Gestione automatica della capacità

Per impostazione predefinita, Capacity Management Mode (modalità di gestione della capacità) è impostata su Automatic (automatica). In questa modalità, Cloud Manager acquista automaticamente nuovi dischi per le istanze di Cloud Volumes ONTAP quando è necessaria una maggiore capacità, elimina raccolte di dischi inutilizzate (aggregati), sposta i volumi tra aggregati quando necessario e tenta di eliminare i dischi guasti.

I seguenti esempi illustrano il funzionamento di questa modalità:

- Se un aggregato con 5 o meno dischi EBS raggiunge la soglia di capacità, Cloud Manager acquista automaticamente nuovi dischi per quell'aggregato in modo che i volumi possano continuare a crescere.
- Se un aggregato con 12 dischi Azure raggiunge la soglia di capacità, Cloud Manager sposta automaticamente un volume da tale aggregato a un aggregato con capacità disponibile o a un nuovo aggregato.

  Se Cloud Manager crea un nuovo aggregato per il volume, sceglie una dimensione del disco che si adatta alle dimensioni del volume.

  Si noti che lo spazio libero è ora disponibile sull'aggregato originale. I volumi esistenti o nuovi volumi possono utilizzare tale spazio. In questo scenario, non è possibile restituire lo spazio ad AWS o Azure.

- Se un aggregato non contiene volumi per più di 12 ore, Cloud Manager lo elimina.

Gestione degli inode con gestione automatica della capacità

Cloud Manager monitora l'utilizzo dell'inode su un volume. Quando viene utilizzato il 85% degli inode, Cloud Manager aumenta le dimensioni del volume per aumentare il numero di inode disponibili. Il numero di file che un volume può contenere è determinato dal numero di inode.

Gestione manuale della capacità

Se l'account Admin imposta la modalità di gestione della capacità su manuale, Cloud Manager visualizza i messaggi azione richiesta quando è necessario prendere decisioni in merito alla capacità. Gli stessi esempi descritti nella modalità automatica si applicano alla modalità manuale, ma spetta all'utente accettare le azioni.

Storage WORM

È possibile attivare lo storage WORM (Write Once, Read Many) su un sistema Cloud Volumes ONTAP per conservare i file in forma non modificata per un periodo di conservazione specificato. Lo storage WORM è basato sulla tecnologia SnapLock in modalità Enterprise, il che significa che i file WORM sono protetti a livello di file.

Una volta che un file è stato salvato nello storage WORM, non può essere modificato, anche dopo la scadenza del periodo di conservazione. Un clock a prova di manomissione determina quando è trascorso il periodo di conservazione di un file WORM.

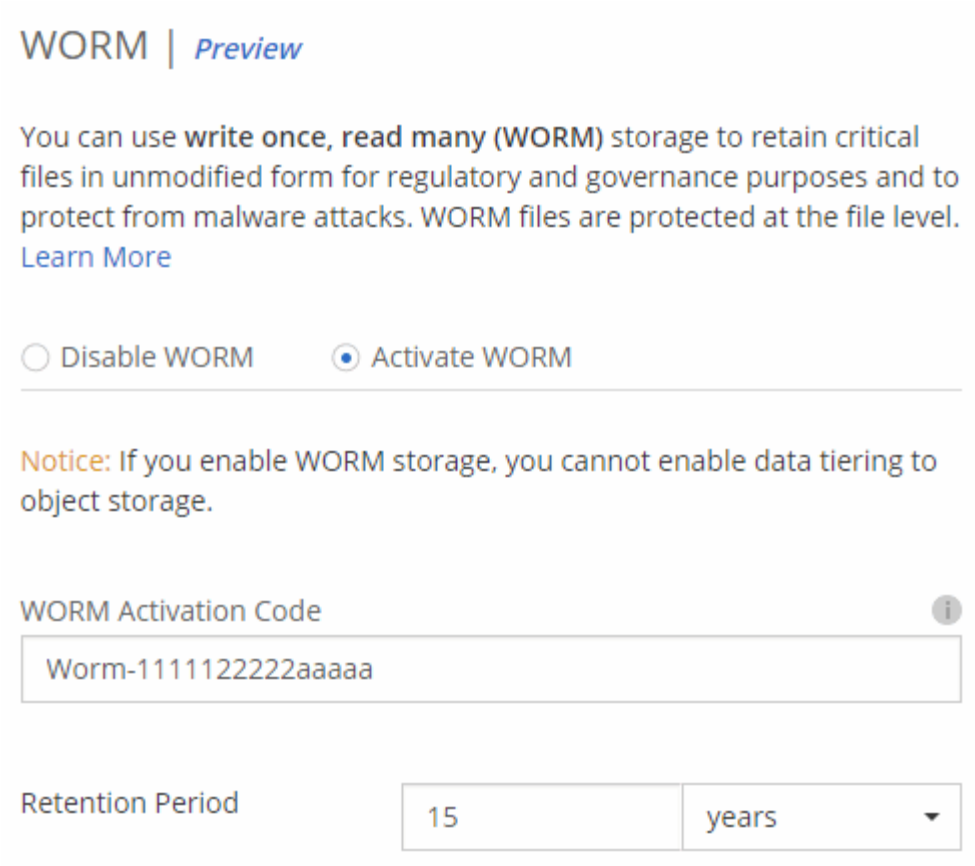
Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari.

Attivazione dello storage WORM

È possibile attivare lo storage WORM su un sistema Cloud Volumes ONTAP quando si crea un nuovo ambiente di lavoro. Ciò include la specifica di un codice di attivazione e l'impostazione del periodo di conservazione predefinito per i file. È possibile ottenere un codice di attivazione utilizzando l'icona della chat in basso a destra dell'interfaccia di Cloud Manager.

Non è possibile attivare lo storage WORM su singoli volumi. WORM deve essere attivato a livello di sistema.

L'immagine seguente mostra come attivare lo storage WORM durante la creazione di un ambiente di lavoro:



Commit dei file in WORM

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare l'interfaccia utente di ONTAP per il commit automatico dei file in WORM. È inoltre possibile utilizzare un file .WORM appendibile per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log.

Dopo aver attivato lo storage WORM su un sistema Cloud Volumes ONTAP, è necessario utilizzare l'interfaccia utente di ONTAP per la gestione dello storage WORM. Per istruzioni, fare riferimento a. "Documentazione ONTAP".

Il supporto Cloud Volumes ONTAP per lo storage WORM equivale alla modalità aziendale SnapLock.

Limitazioni

- Se si elimina o si sposta un disco direttamente da AWS o Azure, è possibile eliminare un volume prima della data di scadenza.
- Quando lo storage WORM è attivato, non è possibile abilitare il tiering dei dati sullo storage a oggetti.

Coppie ad alta disponibilità

Coppie ad alta disponibilità in AWS

Una configurazione Cloud Volumes ONTAP ad alta disponibilità (ha) offre operazioni senza interruzioni e tolleranza agli errori. In AWS, i dati vengono sottoposti a mirroring sincrono tra i due nodi.

Panoramica

In AWS, le configurazioni Cloud Volumes ONTAP ha includono i seguenti componenti:

- Due nodi Cloud Volumes ONTAP i cui dati vengono sottoposti a mirroring sincrono l'uno con l'altro.
- Istanza di mediatore che fornisce un canale di comunicazione tra i nodi per assistere nei processi di acquisizione e giveback dello storage.

> L'istanza del mediatore esegue il sistema operativo Linux su un'istanza t2.micro e utilizza un disco magnetico EBS di circa 8 GB.

Takeover e giveback dello storage

Se un nodo non funziona, l'altro nodo può servire i dati per il proprio partner per fornire un servizio dati continuo. I client possono accedere agli stessi dati dal nodo partner perché i dati sono stati sottoposti a mirroring sincrono con il partner.

Dopo il riavvio del nodo, il partner deve risincronizzare i dati prima di poter restituire lo storage. Il tempo necessario per la risincronizzazione dei dati dipende dalla quantità di dati modificati mentre il nodo era inattivo.

RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 60 secondi. In caso di interruzione, i dati devono essere disponibili in 60 secondi o meno.

Modelli di implementazione HA

È possibile garantire l'elevata disponibilità dei dati implementando una configurazione ha in più zone di disponibilità (AZS) o in un singolo AZ. Per scegliere la configurazione più adatta alle proprie esigenze, è necessario esaminare ulteriori dettagli su ciascuna configurazione.

Cloud Volumes ONTAP ha in più zone di disponibilità

L'implementazione di una configurazione ha in zone di disponibilità multiple (AZS) garantisce un'elevata disponibilità dei dati in caso di guasto con un'istanza AZ o che esegue un nodo Cloud Volumes ONTAP. È necessario comprendere in che modo gli indirizzi IP NAS influiscono sull'accesso ai dati e sul failover dello storage.

Accesso ai dati NFS e CIFS

Quando una configurazione ha viene distribuita in più zone di disponibilità, *indirizzi IP mobili* abilitano l'accesso al client NAS. Gli indirizzi IP mobili, che devono essere al di fuori dei blocchi CIDR per tutti i VPC della regione, possono migrare tra i nodi in caso di guasti. Non sono accessibili in modo nativo ai client che si trovano al di fuori del VPC, a meno che non si "Configurare un gateway di transito AWS".

Se non è possibile configurare un gateway di transito, gli indirizzi IP privati sono disponibili per i client NAS esterni al VPC. Tuttavia, questi indirizzi IP sono statici e non possono eseguire il failover tra i nodi.

Prima di implementare una configurazione ha in più zone di disponibilità, è necessario esaminare i requisiti per gli indirizzi IP mobili e le tabelle di routing. È necessario specificare gli indirizzi IP mobili quando si implementa

la configurazione. Gli indirizzi IP privati vengono creati automaticamente da Cloud Manager.

Per ulteriori informazioni, vedere "Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS".

Accesso ai dati iSCSI

La comunicazione dati tra più VPC non è un problema, poiché iSCSI non utilizza indirizzi IP mobili.

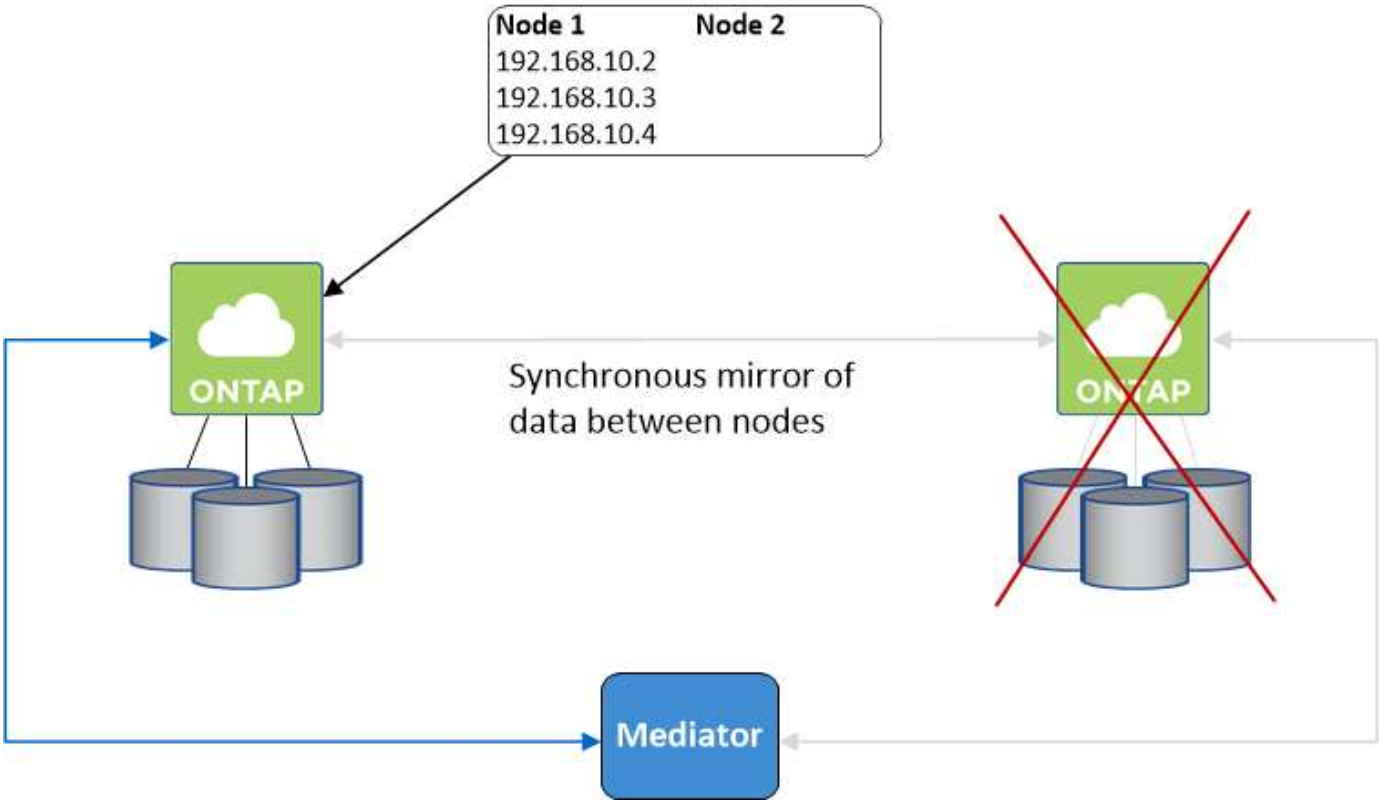
Takeover e giveback dello storage per iSCSI

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

Takeover e giveback dello storage per NAS

Quando l'acquisizione avviene in una configurazione NAS utilizzando IP mobili, l'indirizzo IP mobile del nodo utilizzato dai client per accedere ai dati viene spostato nell'altro nodo. L'immagine seguente mostra l'acquisizione dello storage in una configurazione NAS utilizzando IP mobili. Se il nodo 2 non funziona, l'indirizzo IP mobile per il nodo 2 passa al nodo 1.



Gli IP dei dati NAS utilizzati per l'accesso VPC esterno non possono migrare tra i nodi in caso di guasti. Se un nodo non è in linea, è necessario rimontarlo manualmente sui client esterni al VPC utilizzando l'indirizzo IP sull'altro nodo.

Una volta che il nodo guasto torna in linea, rimontare i client sui volumi utilizzando l'indirizzo IP originale. Questo passaggio è necessario per evitare il trasferimento di dati non necessari tra due nodi ha, che può

causare un impatto significativo sulle performance e sulla stabilità.

È possibile identificare facilmente l'indirizzo IP corretto da Cloud Manager selezionando il volume e facendo clic su **Mount Command**.

Cloud Volumes ONTAP ha in una singola zona di disponibilità

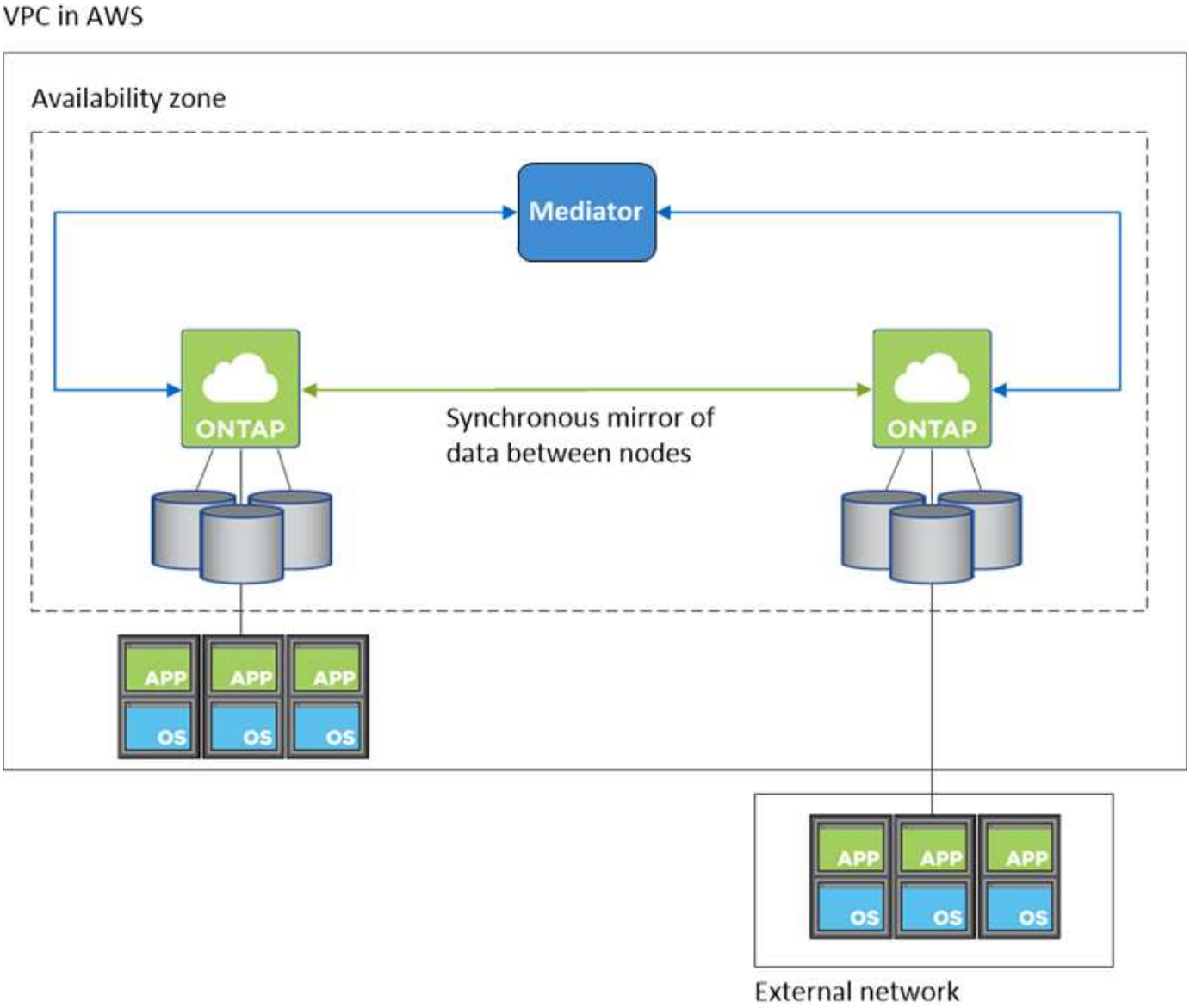
L'implementazione di una configurazione ha in una singola zona di disponibilità (AZ) può garantire un'elevata disponibilità dei dati in caso di guasto di un'istanza che esegue un nodo Cloud Volumes ONTAP. Tutti i dati sono accessibili in modo nativo dall'esterno del VPC.

> Cloud Manager crea un "Gruppo di posizionamento AWS Spread" E lancia i due nodi ha in quel gruppo di posizionamento. Il gruppo di posizionamento riduce il rischio di guasti simultanei distribuendo le istanze su hardware sottostante distinto. Questa funzionalità migliora la ridondanza dal punto di vista del calcolo e non dal punto di vista del guasto del disco.

Accesso ai dati

Poiché questa configurazione si trova in un singolo AZ, non richiede indirizzi IP mobili. È possibile utilizzare lo stesso indirizzo IP per l'accesso ai dati dall'interno del VPC e dall'esterno del VPC.

La seguente immagine mostra una configurazione ha in un singolo AZ. I dati sono accessibili dall'interno del VPC e dall'esterno del VPC.



Takeover e giveback dello storage

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

> Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

Per le configurazioni NAS, gli indirizzi IP dei dati possono migrare tra i nodi ha in caso di guasti. In questo modo si garantisce l'accesso del client allo storage.

Come funziona lo storage in una coppia ha

A differenza di un cluster ONTAP, lo storage in una coppia Cloud Volumes ONTAP ha non viene condiviso tra i nodi. I dati vengono invece sottoposti a mirroring sincrono tra i nodi in modo che siano disponibili in caso di guasto.

Allocazione dello storage

Quando si crea un nuovo volume e sono necessari dischi aggiuntivi, Cloud Manager assegna lo stesso numero di dischi a entrambi i nodi, crea un aggregato mirrorato e crea il nuovo volume. Ad esempio, se sono necessari due dischi per il volume, Cloud Manager assegna due dischi per nodo per un totale di quattro dischi.

Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

È possibile impostare una configurazione Active-Active solo quando si utilizza Cloud Manager nella vista del sistema di storage.

Aspettative di performance per una configurazione ha

Una configurazione Cloud Volumes ONTAP ha replica in modo sincrono i dati tra i nodi, consumando la larghezza di banda della rete. Di conseguenza, rispetto a una configurazione Cloud Volumes ONTAP a nodo singolo, è possibile aspettarsi le seguenti performance:

- Per le configurazioni ha che servono dati da un solo nodo, le prestazioni di lettura sono paragonabili alle prestazioni di lettura di una configurazione a nodo singolo, mentre le prestazioni di scrittura sono inferiori.
- Per le configurazioni ha che servono dati da entrambi i nodi, le performance di lettura sono superiori rispetto alle performance di lettura di una configurazione a nodo singolo e le performance di scrittura sono uguali o superiori.

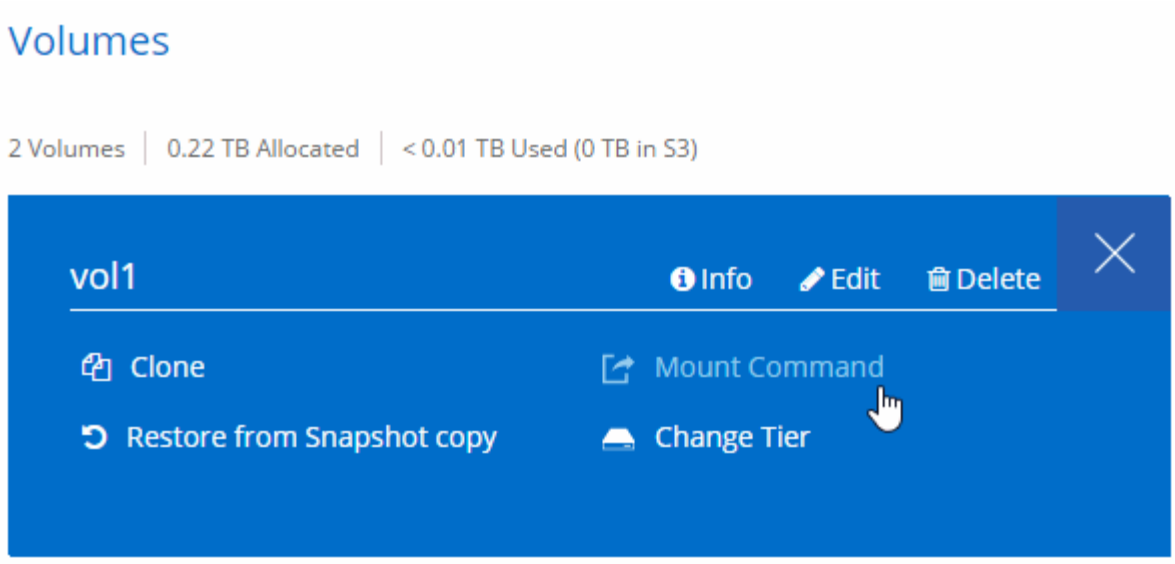
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, vedere "Performance".

Accesso client allo storage

I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico passa tra entrambi i nodi, riducendo le performance.

Se si sposta un volume tra nodi in una coppia ha, è necessario rimontarlo utilizzando l'indirizzo IP dell'altro nodo. In caso contrario, si possono ottenere prestazioni ridotte. Se i client supportano i riferimenti NFSv4 o il reindirizzamento delle cartelle per CIFS, è possibile attivare tali funzionalità sui sistemi Cloud Volumes ONTAP per evitare di rimontare il volume. Per ulteriori informazioni, consultare la documentazione di ONTAP.

È possibile identificare facilmente l'indirizzo IP corretto da Cloud Manager:

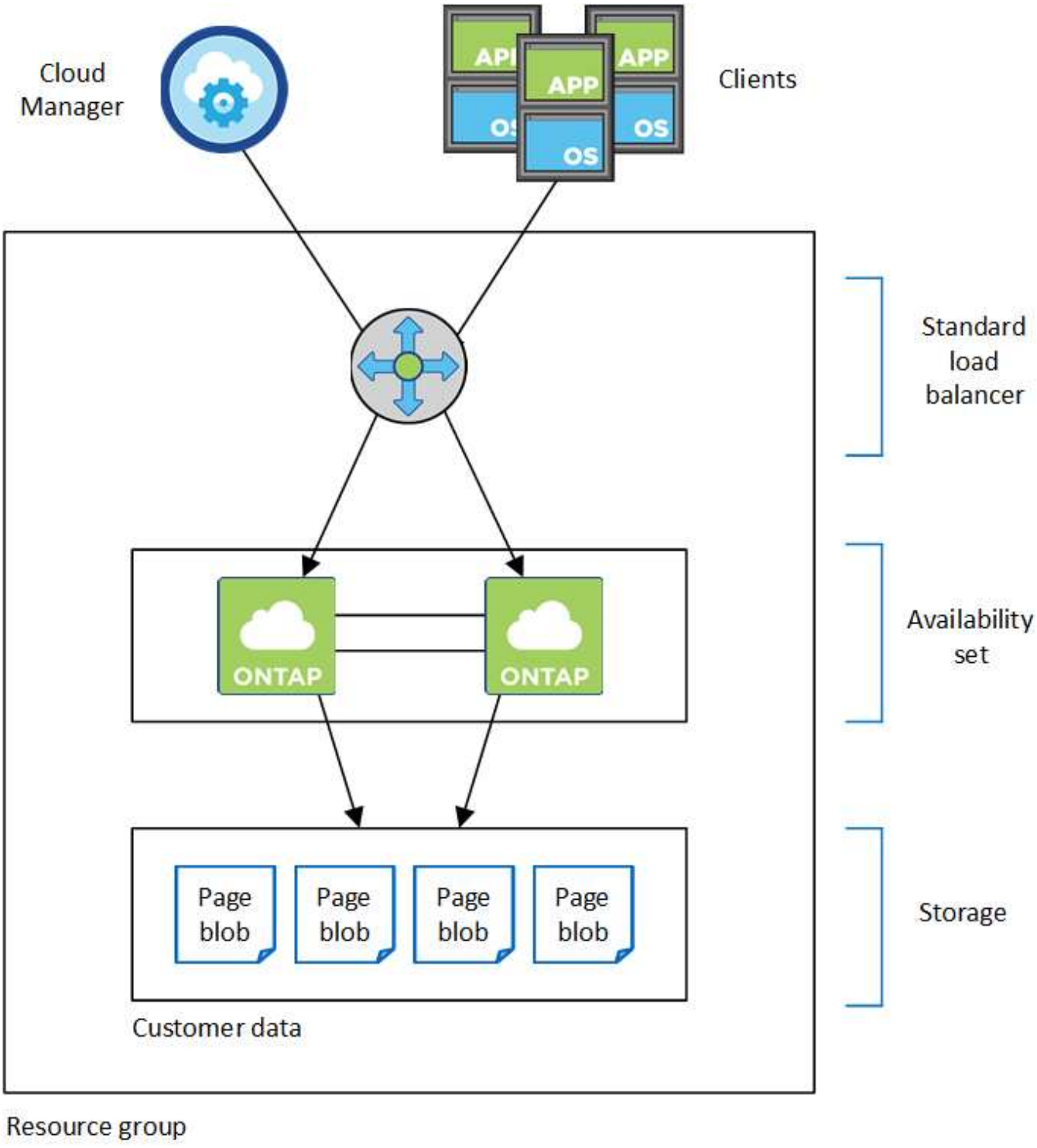


Coppie ad alta disponibilità in Azure

Una coppia Cloud Volumes ONTAP ad alta disponibilità (ha) offre affidabilità aziendale e operazioni continue in caso di guasti nel tuo ambiente cloud. In Azure, lo storage viene condiviso tra i due nodi.

Componenti HA

Una configurazione Cloud Volumes ONTAP ha in Azure include i seguenti componenti:



Tenere presente quanto segue sui componenti di Azure implementati da Cloud Manager:

Bilanciamento del carico standard Azure

Il bilanciamento del carico gestisce il traffico in entrata verso la coppia Cloud Volumes ONTAP ha.

Set di disponibilità

Il set di disponibilità garantisce che i nodi si trovino in diversi domini di errore e aggiornamento.

Dischi

I dati dei clienti si trovano nelle pagine di Premium Storage. Ogni nodo ha accesso allo storage dell'altro nodo. È inoltre necessario uno storage aggiuntivo per i dati di boot, root e core:

- Due dischi SSD Premium da 90 GB per il volume di boot (uno per nodo)
- Due blob di pagina Premium Storage da 140 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 128 GB per il risparmio di core (uno per nodo)

Account storage

- Per i dischi gestiti è necessario un account di storage.
- Per le pagine blob dello storage Premium sono necessari uno o più account di storage, in quanto viene raggiunto il limite di capacità del disco per account di storage.

  "Documentazione di Azure: Obiettivi di scalabilità e performance dello storage Azure per gli account storage".

- Per il tiering dei dati sullo storage Azure Blob è necessario un account storage.

RPO e RTO

Una configurazione ad alta disponibilità dei dati viene mantenuta come segue:

- L'obiettivo del punto di ripristino (RPO) è di 0 secondi. I tuoi dati sono coerenti con le transazioni senza alcuna perdita di dati.
- L'obiettivo del tempo di ripristino (RTO) è di 60 secondi. In caso di interruzione, i dati devono essere disponibili in 60 secondi o meno.

Takeover e giveback dello storage

Analogamente a un cluster ONTAP fisico, lo storage in una coppia Azure ha viene condiviso tra i nodi. Le connessioni allo storage del partner consentono a ciascun nodo di accedere allo storage dell'altro in caso di *takeover*. I meccanismi di failover del percorso di rete garantiscono che client e host continuino a comunicare con il nodo esistente. Il partner _restituisce lo storage quando il nodo viene riportato in linea.

Per le configurazioni NAS, gli indirizzi IP dei dati migrano automaticamente tra i nodi ha in caso di guasti.

Per iSCSI, Cloud Volumes ONTAP utilizza MPIO (Multipath i/o) e ALUA (Asymmetric Logical Unit Access) per gestire il failover del percorso tra i percorsi ottimizzati per attività e non ottimizzati.

Per informazioni su quali configurazioni host specifiche supportano ALUA, consultare "Tool di matrice di interoperabilità NetApp" E la guida all'installazione e all'installazione delle utility host per il sistema operativo host.

Configurazioni dello storage

È possibile utilizzare una coppia ha come configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, o come configurazione Active-passive, in cui il nodo passivo risponde alle richieste di dati solo se ha assunto lo storage per il nodo attivo.

Limitazioni DI HA

Le seguenti limitazioni influiscono sulle coppie Cloud Volumes ONTAP ha in Azure:

- Le coppie HA sono supportate con Cloud Volumes ONTAP standard, Premium e BYOL. Esplora non è supportato.
- NFSv4 non è supportato. NFSv3 è supportato.
- Le coppie HA non sono supportate in alcune regioni.

  "Consulta l'elenco delle aree Azure supportate".

"Scopri come implementare un sistema ha in Azure".

Valutazione

È possibile valutare Cloud Volumes ONTAP prima di pagare il software.

Una versione di prova gratuita di 30 giorni di un sistema Cloud Volumes ONTAP a nodo singolo è disponibile all'indirizzo "NetApp Cloud Central". Non sono previsti costi software orarie, ma i costi dell'infrastruttura sono ancora applicati. Una versione di prova gratuita viene convertita automaticamente in un abbonamento oraria a pagamento alla scadenza.

Se hai bisogno di assistenza per la prova di concetto, contatta "Il team di vendita" oppure contattatelo tramite l'opzione di chat disponibile all'interno del sito "NetApp Cloud Central" E da Cloud Manager.

Licensing

Ogni sistema Cloud Volumes ONTAP BYOL deve avere una licenza installata con un abbonamento attivo. Se non viene installata una licenza attiva, il sistema Cloud Volumes ONTAP si spegne dopo 30 giorni. Cloud Manager semplifica il processo gestendo le licenze e avvisandovi prima della scadenza.

Gestione delle licenze per un nuovo sistema

Quando si crea un sistema BYOL, Cloud Manager richiede un account NetApp Support Site. Cloud Manager utilizza l'account per scaricare il file di licenza da NetApp e installarlo sul sistema Cloud Volumes ONTAP.

"Scopri come aggiungere account NetApp Support Site a Cloud Manager".

Se Cloud Manager non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile ottenere il file da solo e caricarlo manualmente in Cloud Manager. Per istruzioni, vedere "Installazione dei file di licenza sui sistemi Cloud Volumes ONTAP BYOL".

Scadenza della licenza

Cloud Manager ti avvisa 30 giorni prima della scadenza della licenza e di nuovo alla scadenza della stessa. La seguente immagine mostra un avviso di scadenza di 30 giorni:

È possibile selezionare l'ambiente di lavoro per rivedere il messaggio.

Se la licenza non viene rinnovata in tempo, il sistema Cloud Volumes ONTAP si spegne automaticamente. Se viene riavviato, si spegne di nuovo.

Cloud Volumes ONTAP può anche inviare notifiche tramite e-mail, un host trapSNMP o un server syslog utilizzando le notifiche degli eventi EMS (sistema di gestione degli eventi). Per istruzioni, consultare "Guida rapida alla configurazione EMS di ONTAP 9".

Rinnovo della licenza

Quando rinnovi un abbonamento BYOL contattando un rappresentante NetApp, Cloud Manager ottiene automaticamente la nuova licenza da NetApp e la installa sul sistema Cloud Volumes ONTAP.

Se Cloud Manager non riesce ad accedere al file di licenza tramite la connessione Internet sicura, è possibile ottenere il file da solo e caricarlo manualmente in Cloud Manager. Per istruzioni, vedere "Installazione dei file di licenza sui sistemi Cloud Volumes ONTAP BYOL".

Sicurezza

Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.

Crittografia dei dati inattivi

Cloud Volumes ONTAP supporta le seguenti tecnologie di crittografia:

- Crittografia dei volumi NetApp (a partire da Cloud Volumes ONTAP 9.5)
- Servizio di gestione delle chiavi AWS
- Azure Storage Service Encryption
- Crittografia predefinita di Google Cloud Platform

È possibile utilizzare NetApp Volume Encryption con crittografia AWS, Azure o GCP nativa, che crittografa i dati a livello di hypervisor.

Crittografia dei volumi NetApp

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. I dati, le copie Snapshot e i metadati sono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume.

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp con un server di gestione delle chiavi esterno. Onboard Key Manager non è supportato. I Key Manager supportati sono disponibili in "Tool di matrice

di interoperabilità NetApp" Nella soluzione **Key Manager**.

È possibile attivare NetApp Volume Encryption su un volume nuovo o esistente utilizzando CLI o System Manager. Cloud Manager non supporta NetApp Volume Encryption. Per istruzioni, vedere "Crittografia dei volumi con NetApp Volume Encryption".

Servizio di gestione delle chiavi AWS

Quando si avvia un sistema Cloud Volumes ONTAP in AWS, è possibile attivare la crittografia dei dati utilizzando "AWS Key Management Service (KMS)". Cloud Manager richiede le chiavi dati utilizzando una chiave master del cliente (CMK).

Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

Se si desidera utilizzare questa opzione di crittografia, assicurarsi che AWS KMS sia configurato correttamente. Per ulteriori informazioni, vedere "Configurazione di AWS KMS".

Azure Storage Service Encryption

"Azure Storage Service Encryption" Per i dati inattivi è attivato per impostazione predefinita per i dati Cloud Volumes ONTAP in Azure. Non è richiesta alcuna configurazione.

Le chiavi gestite dal cliente non sono supportate con Cloud Volumes ONTAP.

Crittografia predefinita di Google Cloud Platform

"Crittografia dei dati inattivi di Google Cloud Platform" È attivato per impostazione predefinita per Cloud Volumes ONTAP. Non è richiesta alcuna configurazione.

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare le API di Cloud Manager per creare un sistema Cloud Volumes ONTAP che utilizza *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che vengono generate e gestite in GCP utilizzando il Cloud Key Management Service.

Fare riferimento a. "Guida per sviluppatori API" Per ulteriori informazioni sull'utilizzo dei parametri "GcpEncryption".

Scansione virus ONTAP

È possibile utilizzare la funzionalità antivirus integrata nei sistemi ONTAP per proteggere i dati da virus o altri codici dannosi.

La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

Per informazioni su vendor, software e versioni supportate da Vscan, consultare "Matrice di interoperabilità NetApp".

Per informazioni su come configurare e gestire la funzionalità antivirus sui sistemi ONTAP, consultare "Guida alla configurazione antivirus di ONTAP 9".

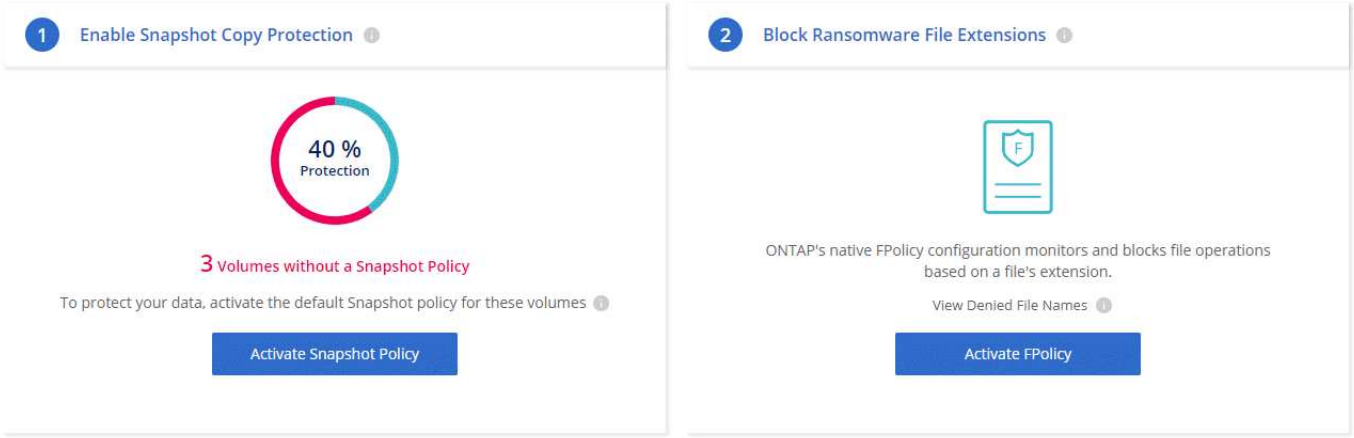
Protezione ransomware

Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. Cloud Manager consente di implementare la soluzione NetApp per ransomware, che fornisce strumenti efficaci per visibilità, rilevamento e risoluzione dei problemi.

- Cloud Manager identifica i volumi che non sono protetti da una policy Snapshot e consente di attivare la policy Snapshot predefinita su tali volumi.

  Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

- Cloud Manager consente inoltre di bloccare le estensioni di file ransomware comuni attivando la soluzione FPolicy di ONTAP.



"Scopri come implementare la soluzione NetApp per ransomware".

Performance

Puoi esaminare i risultati delle performance per aiutarti a decidere quali carichi di lavoro sono appropriati per Cloud Volumes ONTAP.

Per Cloud Volumes ONTAP per AWS, fare riferimento a. "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni".

Per Cloud Volumes ONTAP per Microsoft Azure, fare riferimento a. "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi".

Inizia subito

Panoramica dell'implementazione

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

Installazione di Cloud Manager

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

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

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

- Cloud IBM
- Nella tua rete

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

Posizione per Cloud Manager	Come implementare Cloud Manager
AWS	1. "Implementazione di Cloud Manager da NetApp Cloud Central" (consigliato) 2. "Implementazione da AWS Marketplace" 3. "Scaricare e installare il software su un host Linux"
AWS C2S	"Implementa Cloud Manager da AWS Intelligence Community Marketplace"
Area di Azure generalmente disponibile	1. "Implementazione di Cloud Manager da NetApp Cloud Central" (consigliato) 2. "Implementazione da Azure Marketplace" 3. "Scaricare e installare il software su un host Linux"
Governo di Azure	"Implementa Cloud Manager da Azure US Government Marketplace"
Azure Germania	"Scaricare e installare il software su un host Linux"

Posizione per Cloud Manager	Come implementare Cloud Manager
Piattaforma Google Cloud	1. "Implementazione di Cloud Manager da NetApp Cloud Central" (consigliato) 2. "Scaricare e installare il software su un host Linux" Non puoi implementare Cloud Manager in Google Cloud da GCP Marketplace
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.

- "Configurazione dell'account Cloud Central"
- "Aggiunta di account AWS a Cloud Manager"
- "Aggiunta di account Azure a Cloud Manager"
- "Installazione di un certificato HTTPS"
- "Configurazione di AWS KMS"

Implementazione di Cloud Volumes ONTAP

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

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

- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in AWS"
- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in Azure"
- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in GCP"
- "Pianificazione della configurazione"
- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"
- "Avvio di Cloud Volumes ONTAP in GCP"

Introduzione a Cloud Volumes ONTAP in AWS

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

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.

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.

Iscriviti a AWS Marketplace

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

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

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 avviare e completa i passaggi della procedura guidata. Dopo 25 minuti, il primo sistema Cloud Volumes ONTAP dovrebbe essere attivo e funzionante.

Guarda il seguente video per una presentazione di questi passaggi:

► https://docs.netapp.com/it-it/occm37//media/video_getting_started_aws.mp4 *(video)*

Link correlati

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

Introduzione a Cloud Volumes ONTAP in Azure

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

Configurare la rete

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

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

Fornire le autorizzazioni Azure richieste

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

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

   Esempio: **az role Definition create --role-Definition C:/Policy_for_Setup_as_Service_Azure.json**

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

Lanciate Cloud Manager da NetApp Cloud Central

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

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

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

Link correlati

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

Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google

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

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

Configurare la rete

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

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

Impostare i permessi e i progetti GCP

Assicurarsi che siano presenti due set di autorizzazioni:

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

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

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

Cloud Volumes ONTAP nei progetti.

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

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

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

- "Creare un account di servizio GCP e applicare il ruolo personalizzato appena creato".
- Se si desidera implementare Cloud Volumes ONTAP in altri progetti, "Concedere l'accesso aggiungendo l'account di servizio con il ruolo Cloud Manager a quel progetto". Dovrai ripetere questo passaggio per ogni progetto.

Configurare GCP per il tiering dei dati

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

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

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

2. "Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google".

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

Abilitare le API di Google Cloud

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

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

Iscriviti al GCP Marketplace

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

Lanciate Cloud Manager da NetApp Cloud Central

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

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

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

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

Link correlati

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

Configurare Cloud Manager

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

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

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

Aggiunta di aree di lavoro

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

Fasi

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

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

Al termine

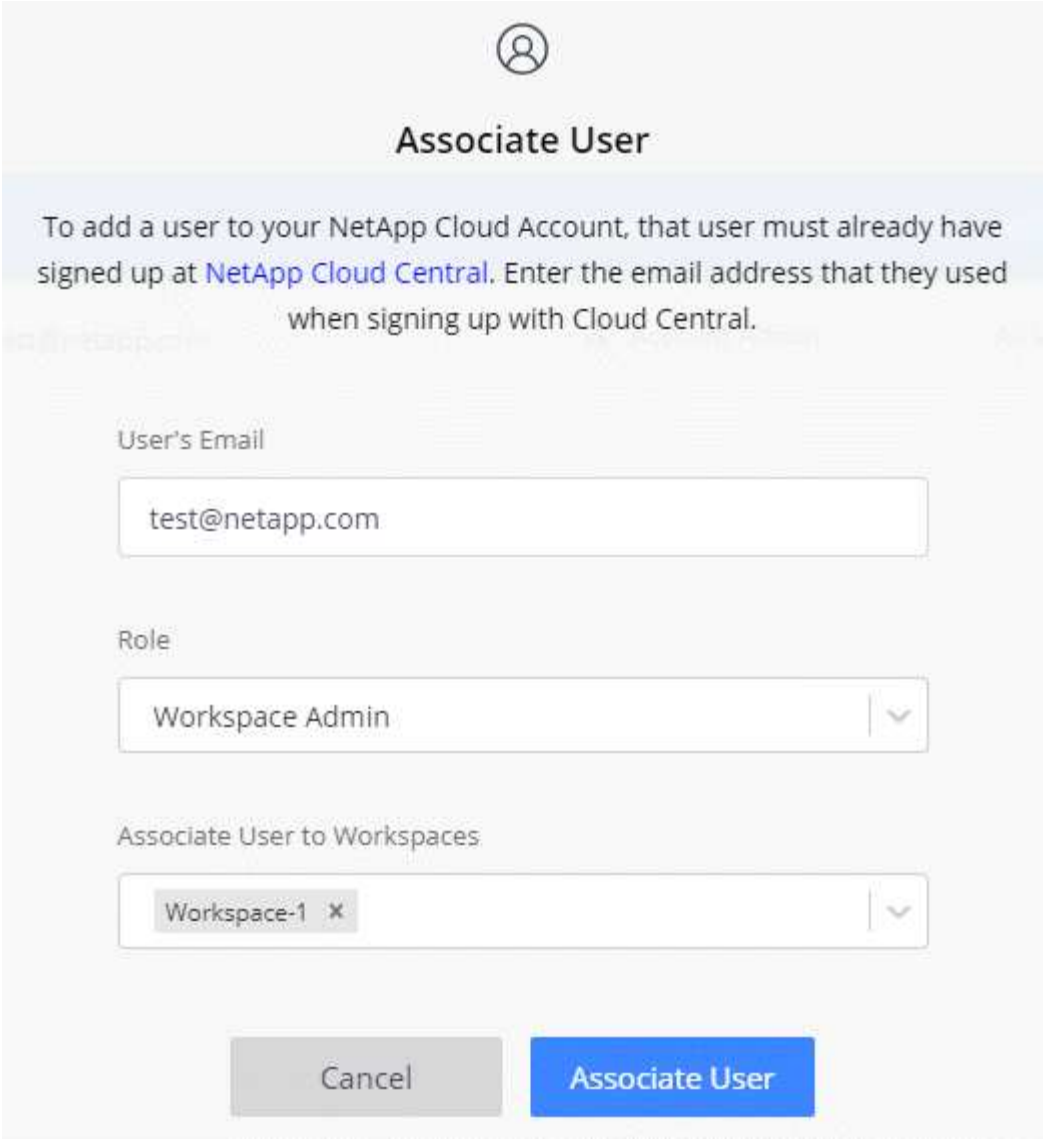
È ora possibile associare utenti e connettori di servizio allo spazio di lavoro.

Aggiunta di utenti

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

Fasi

1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "NetApp Cloud Central" e creare un account.
2. In Cloud Manager, fare clic su **Impostazioni account**.
3. Nella scheda Users (utenti), fare clic su **associate User** (Associa utente).
4. Inserire l'indirizzo e-mail dell'utente e selezionare un ruolo per l'utente:
   - **Account Admin**: Può eseguire qualsiasi azione in Cloud Manager.
   - **Workspace Admin**: Consente di creare e gestire le risorse nelle aree di lavoro assegnate.
5. Se si seleziona Workspace Admin (Amministrazione area di lavoro), selezionare una o più aree di lavoro da associare all'utente.



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

Risultato

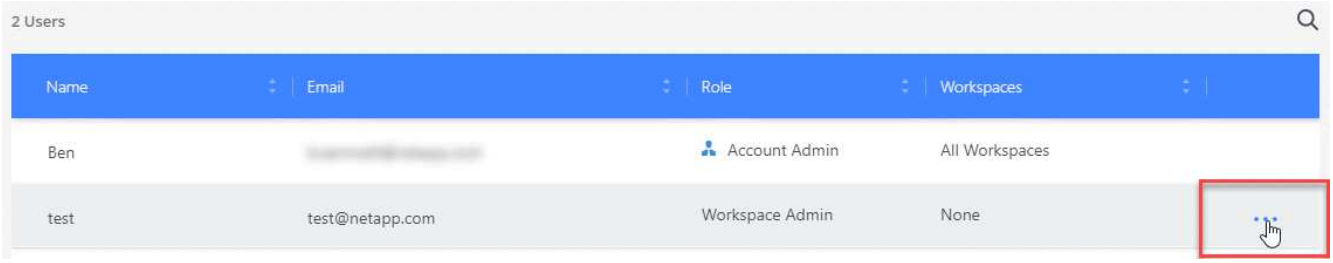
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

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

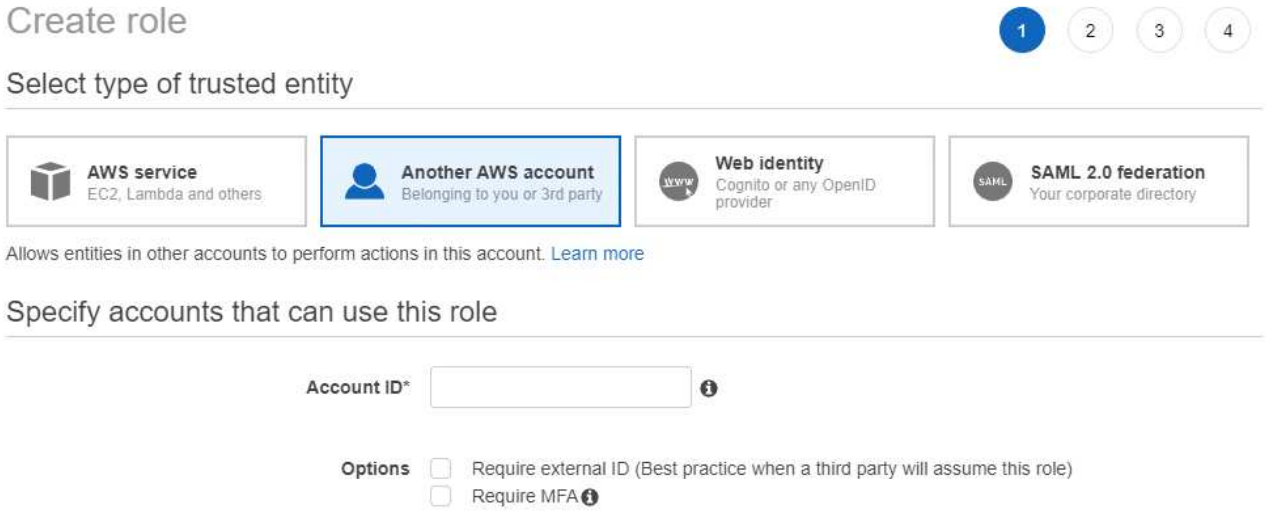
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Cloud Manager e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

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.

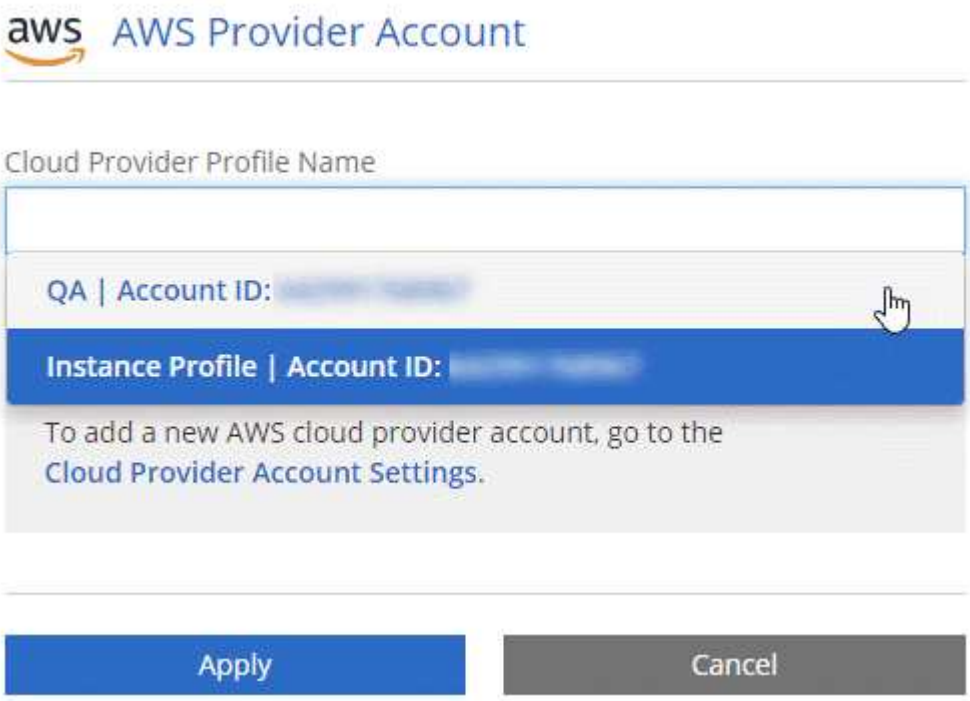
Fasi

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".

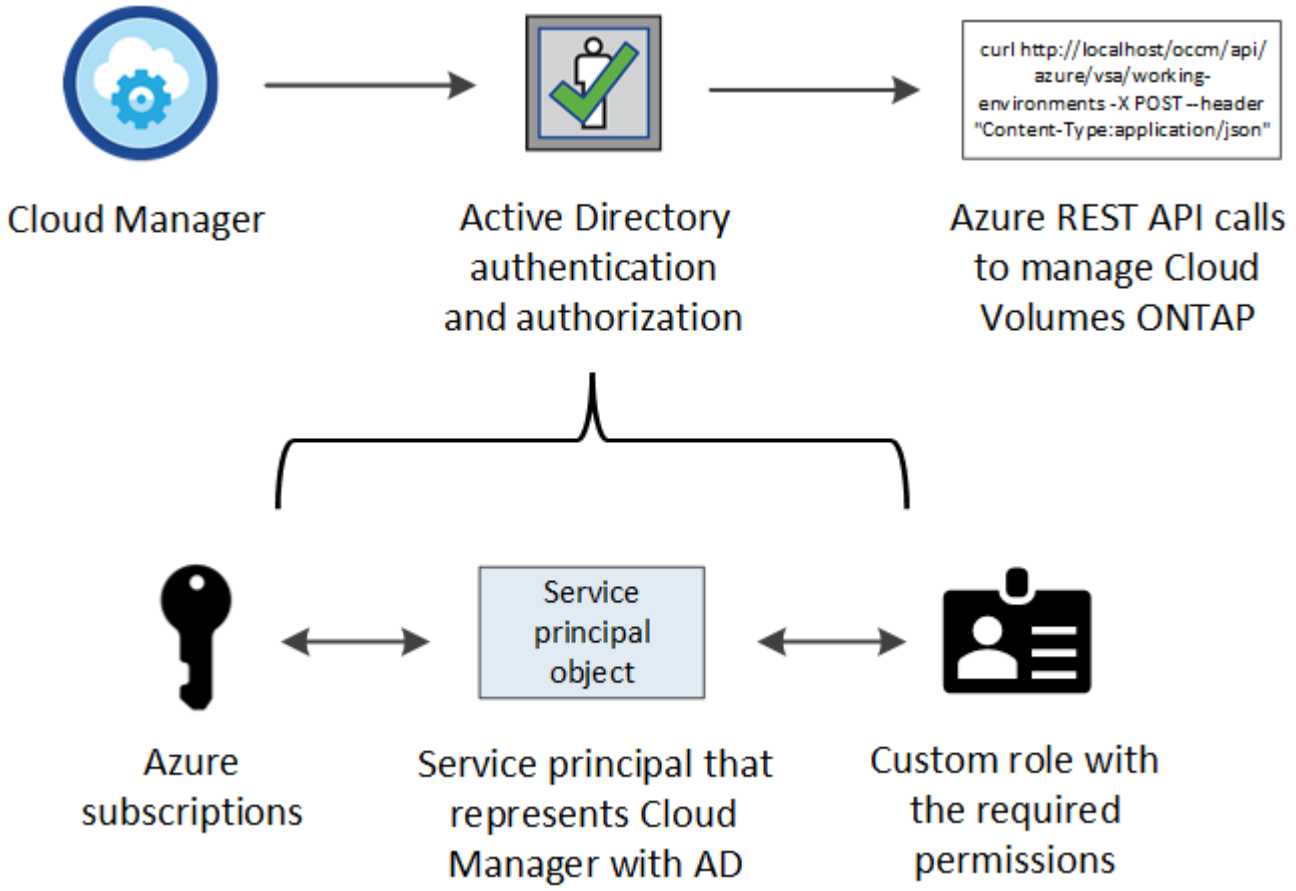
Concessione delle autorizzazioni di Azure mediante un'entità del servizio

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

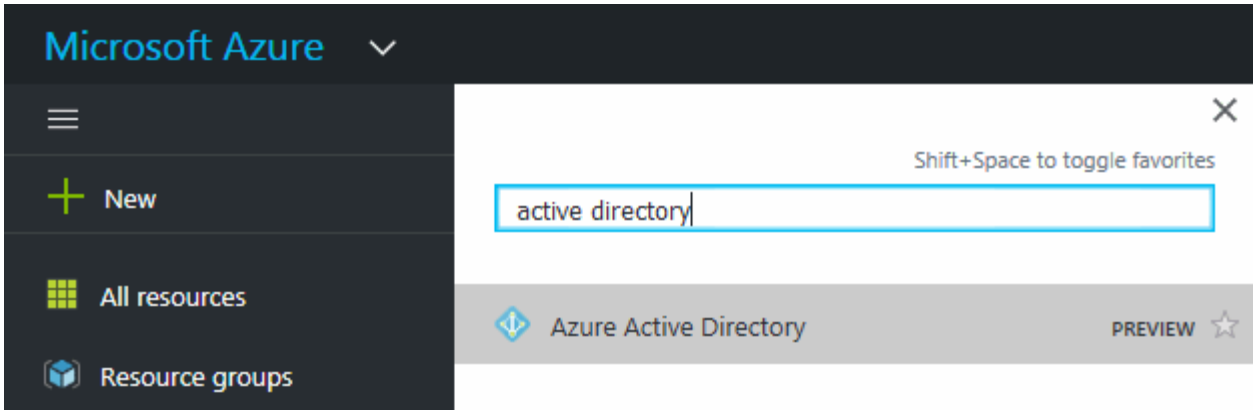
Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per il controllo degli accessi in base al ruolo.

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**.

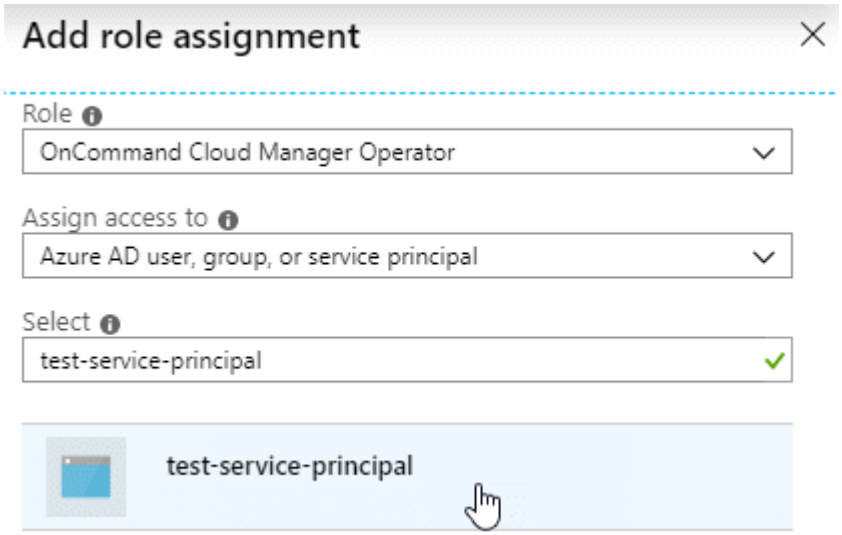
   b. Selezionare l'abbonamento.

   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.

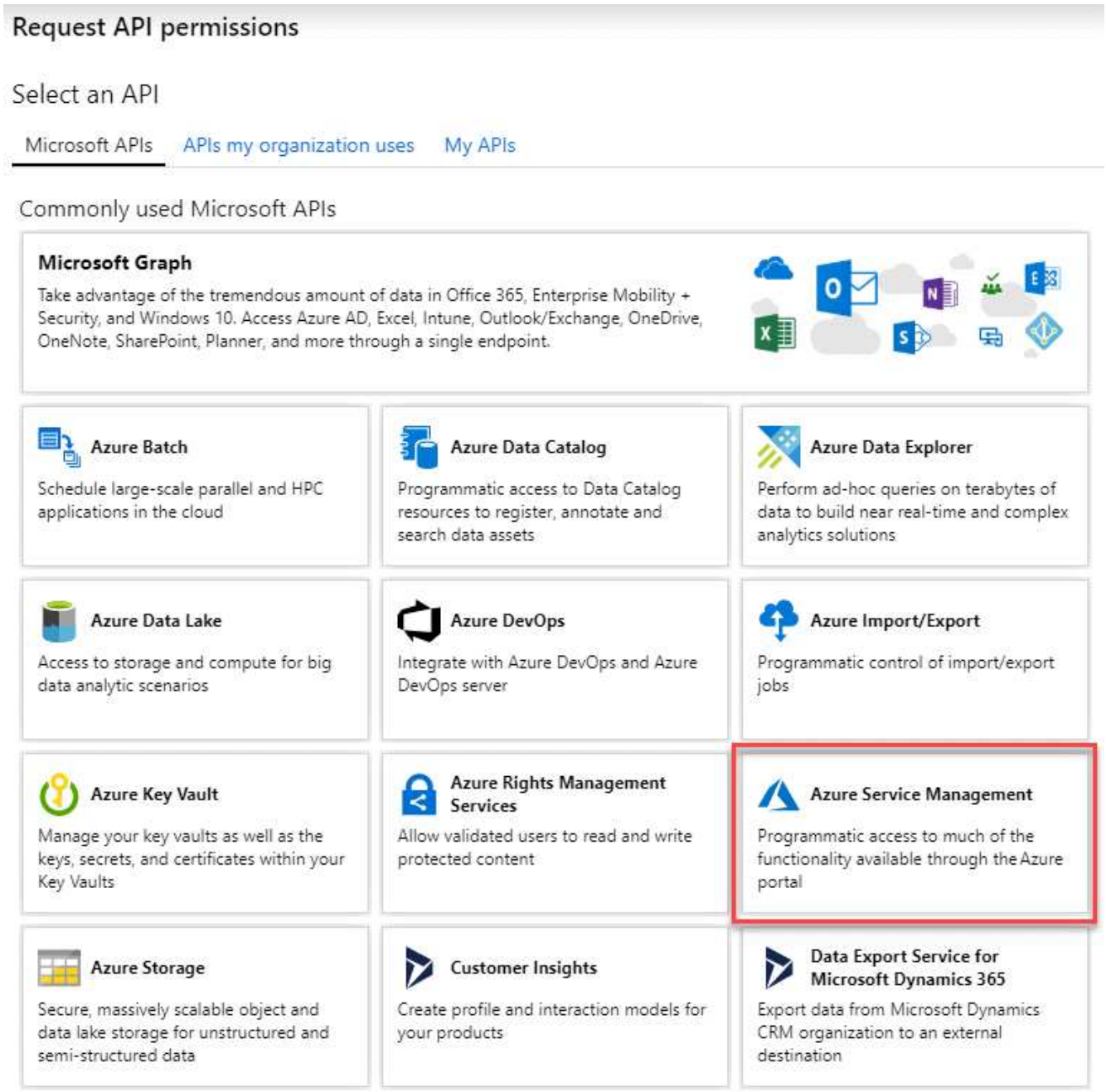
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Cloud Manager consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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

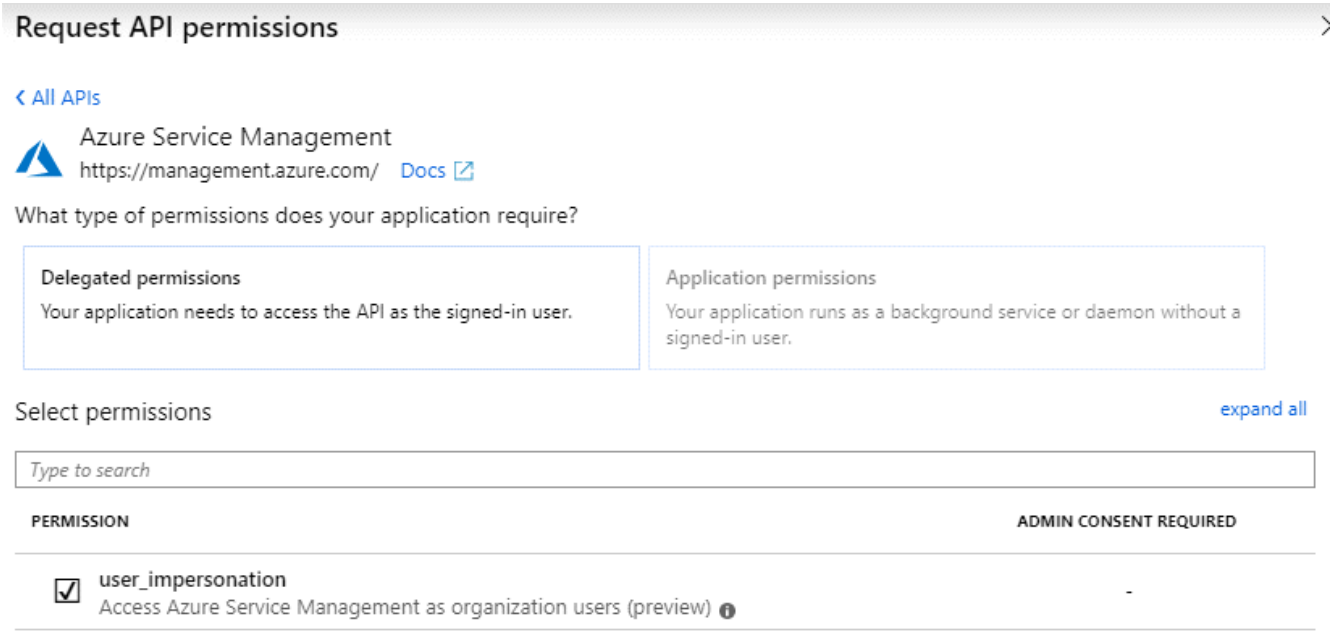
L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

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** (

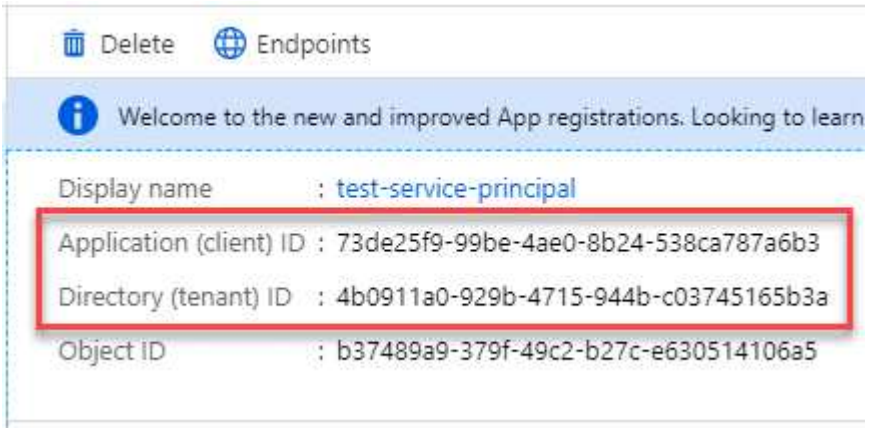


Ottenere l'ID dell'applicazione e l'ID della directory

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.

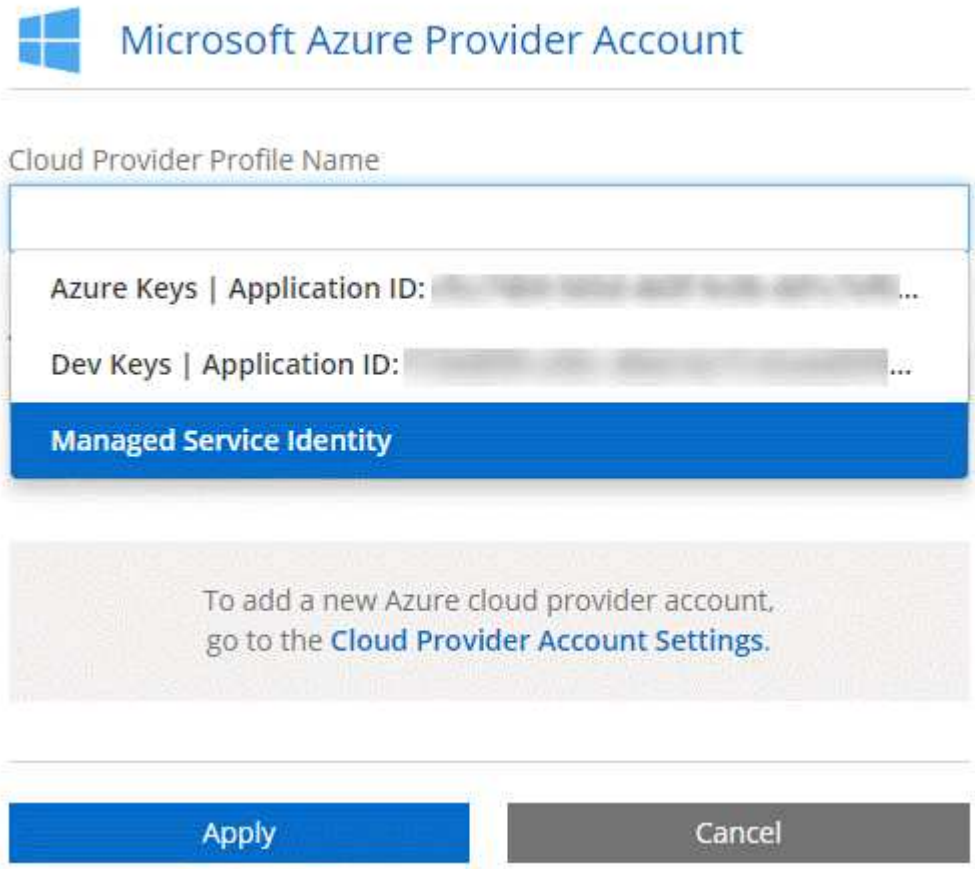
Fasi

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.

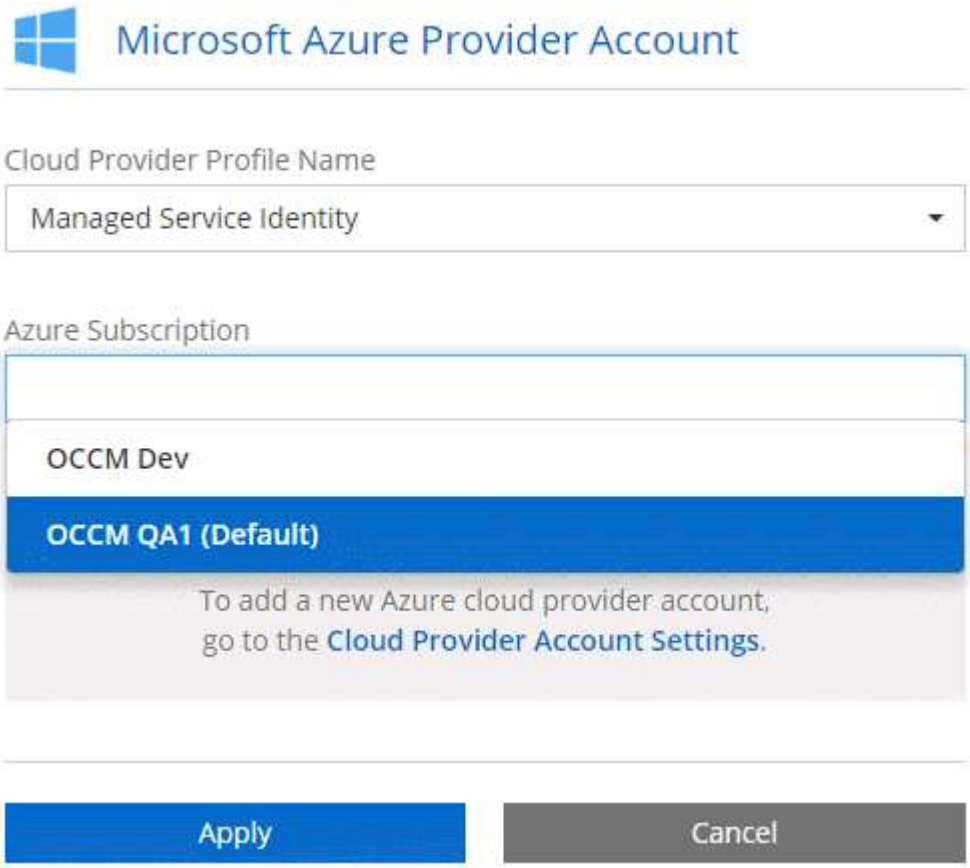
      - Assegnare l'accesso a una **macchina virtuale**.

- 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

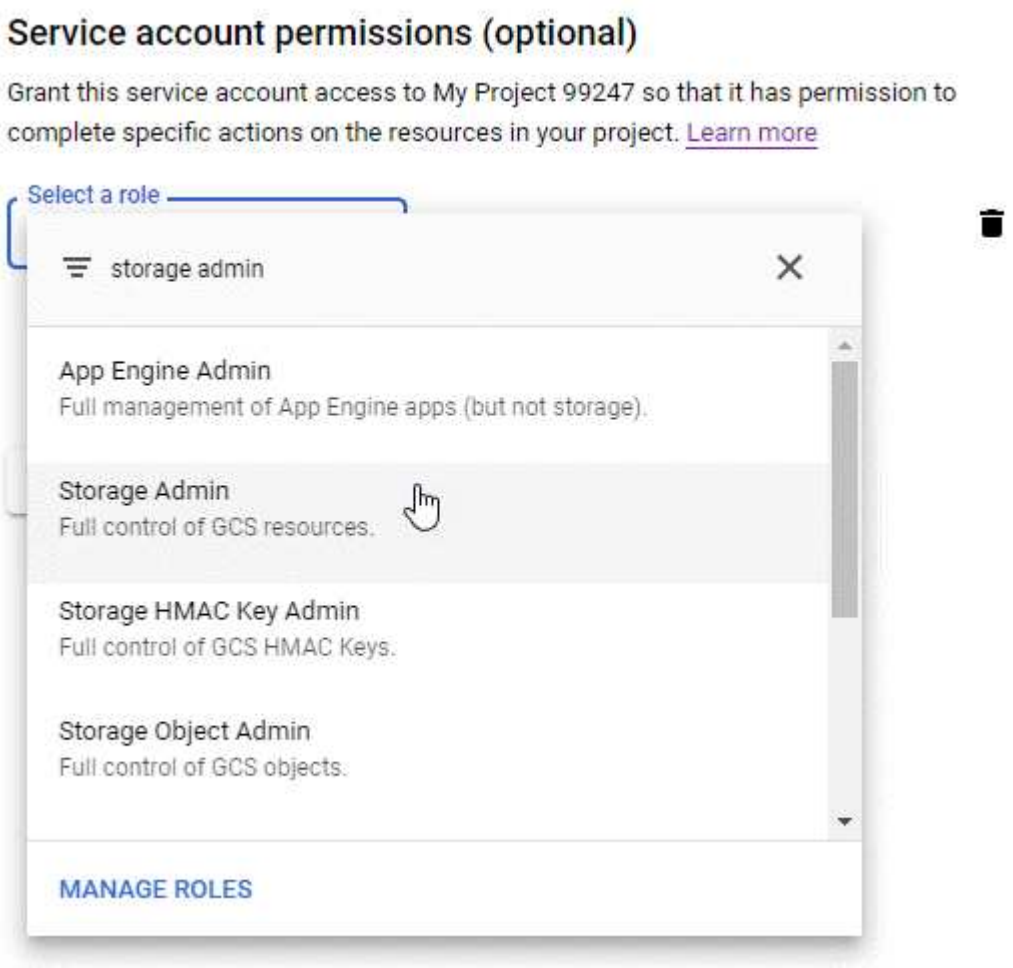
Se si desidera attivare "tiering dei dati" In un sistema Cloud Volumes ONTAP, è necessario fornire a Cloud Manager una chiave di accesso allo storage per un account di servizio che dispone delle autorizzazioni di amministratore dello storage. Cloud Manager utilizza le chiavi di accesso per configurare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

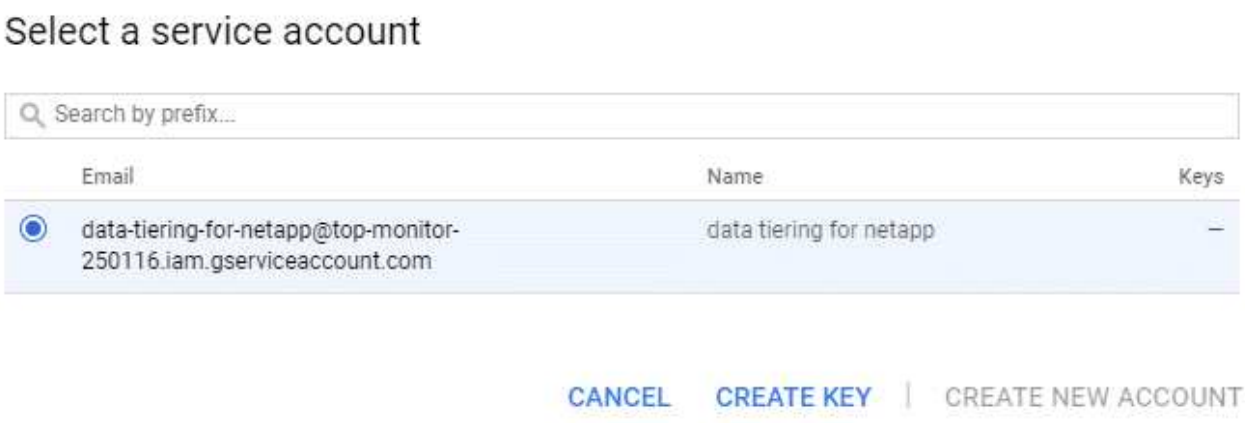
Un account di servizio consente a Cloud Manager di autenticare e accedere ai bucket Cloud Storage utilizzati per il tiering dei dati. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

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

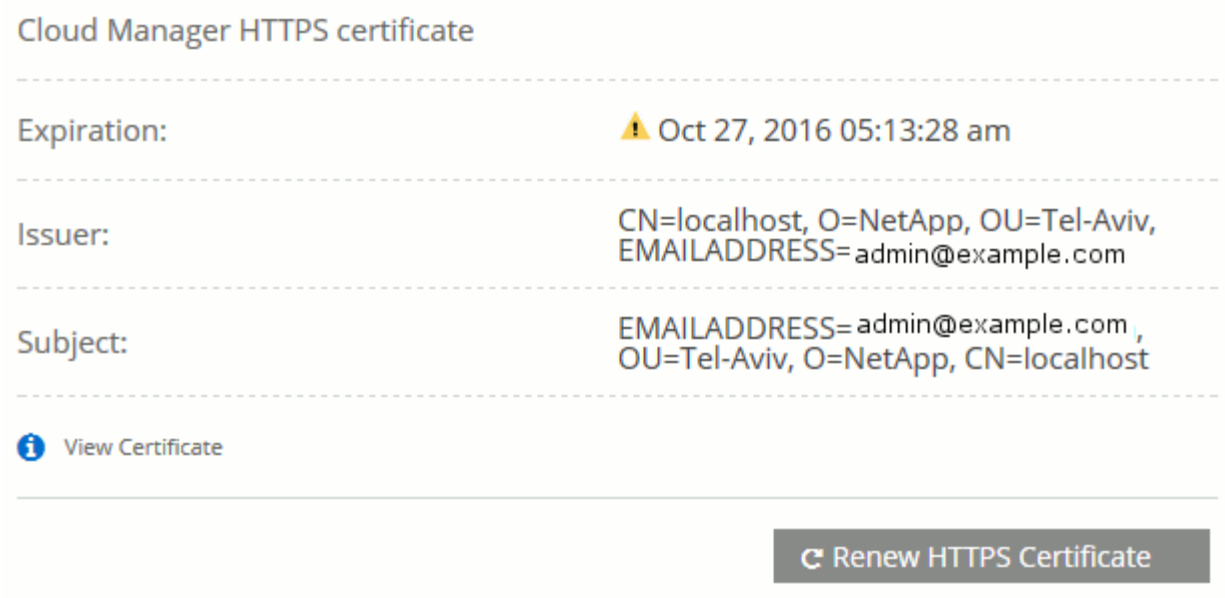
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Settings (Impostazioni) e selezionare **HTTPS Setup** (Configurazione HTTPS).

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"

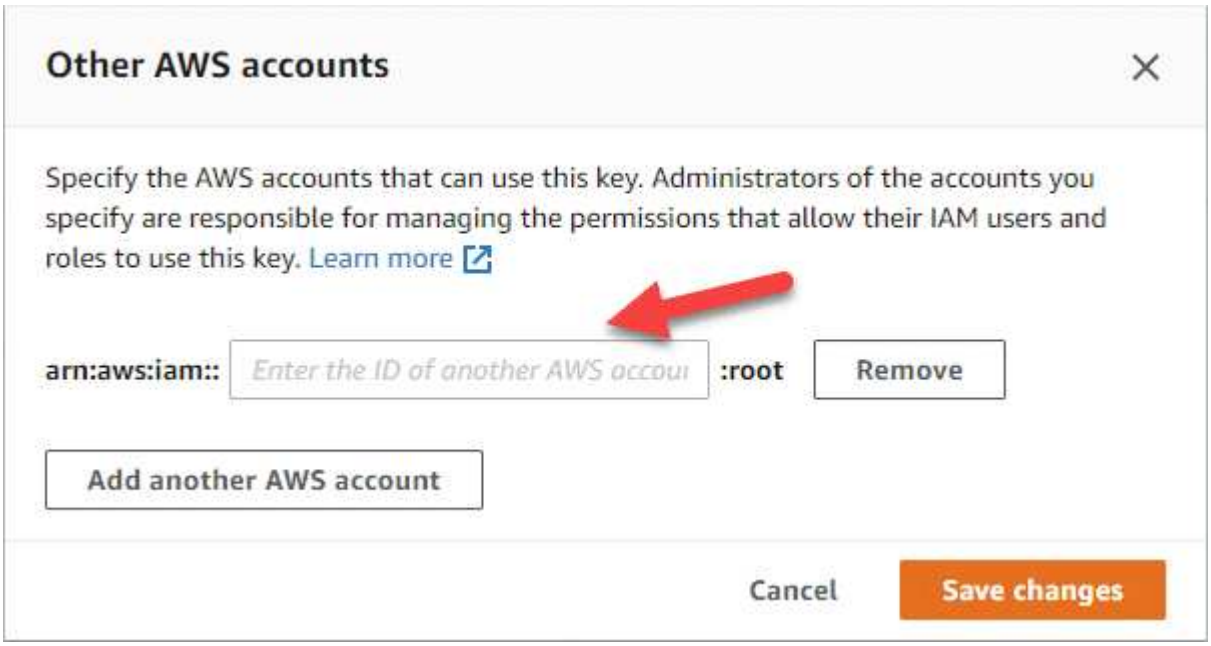
3. Se il CMK si trova in un account AWS diverso, completare la seguente procedura:

   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".

Requisiti di rete

Requisiti di rete per Cloud Manager

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

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

Connessione alle reti di destinazione

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

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

Accesso a Internet in uscita

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

Le sezioni seguenti identificano gli endpoint specifici.

Endpoint per gestire Cloud Volumes ONTAP in AWS

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

Endpoint	Scopo
Servizi AWS (amazonaws.com): • 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://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.
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 del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
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.

Endpoint per gestire Cloud Volumes ONTAP in Azure

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

Endpoint	Scopo
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.

Endpoint	Scopo
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.
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://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://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
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.

Endpoint per gestire Cloud Volumes ONTAP in GCP

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

Endpoint	Scopo
https://www.googleapis.com	Consente a Cloud Manager di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
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://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://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
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.

Endpoint a cui si accede dal browser Web

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

Endpoint	Scopo
L'host Cloud Manager	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.

Endpoint per installare Cloud Manager su un host Linux

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

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Porte e gruppi di sicurezza

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

Requisiti di rete per Cloud Volumes ONTAP in AWS

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

Requisiti generali di rete AWS per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

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

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

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

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

Accesso a Internet in uscita per il mediatore ha

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

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

Numero di indirizzi IP

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

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

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

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

Gruppi di sicurezza

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

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

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

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

In caso di problemi, vedere "AWS Support Knowledge Center: Perché non è possibile connettersi a un

bucket S3 utilizzando un endpoint VPC gateway?"

Connessioni a sistemi ONTAP in altre reti

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

DNS e Active Directory per CIFS

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

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

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

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

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

Per informazioni sul funzionamento delle coppie ha, vedere "Coppie ad alta disponibilità".

Zone di disponibilità

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

Indirizzi IP mobili per dati NAS e gestione cluster/SVM

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

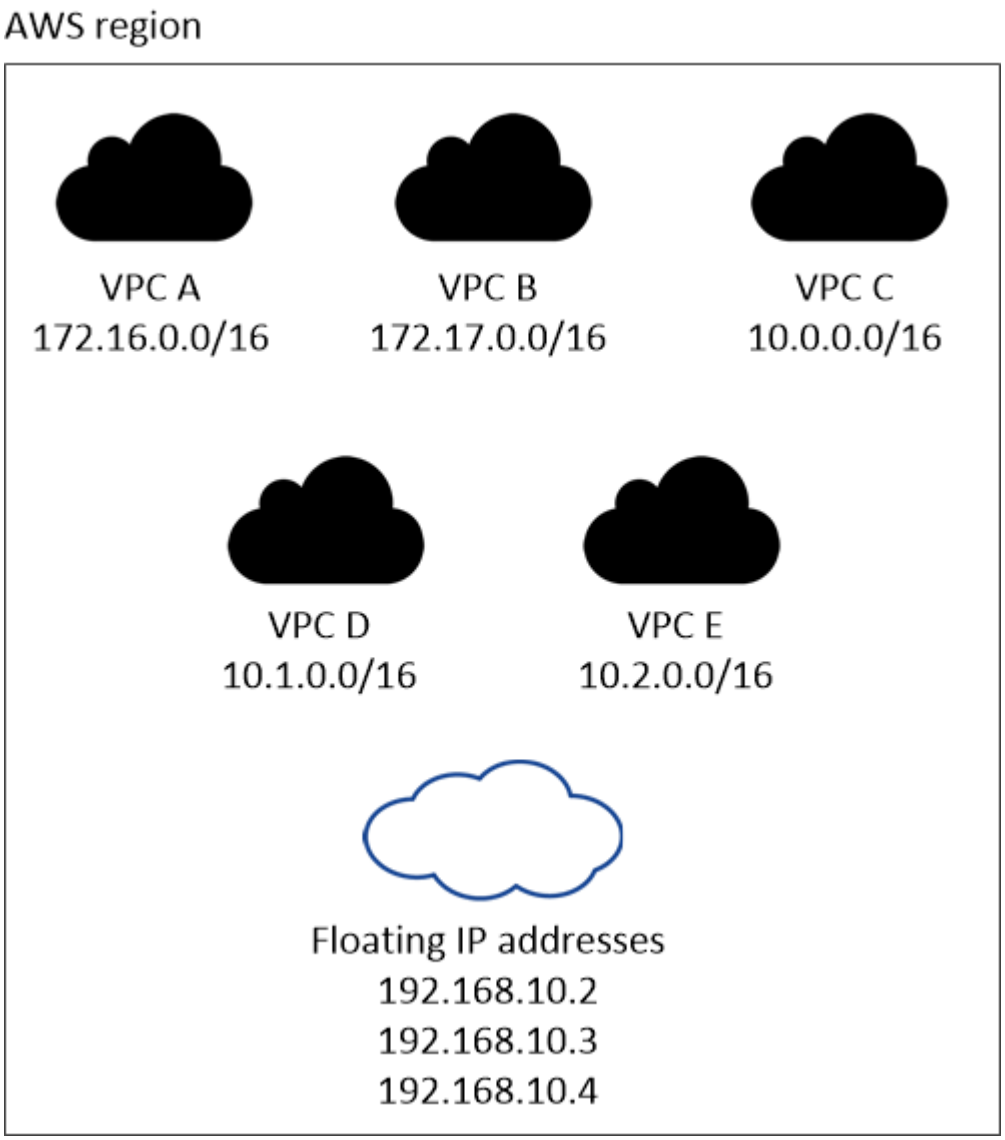
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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

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

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

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



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".

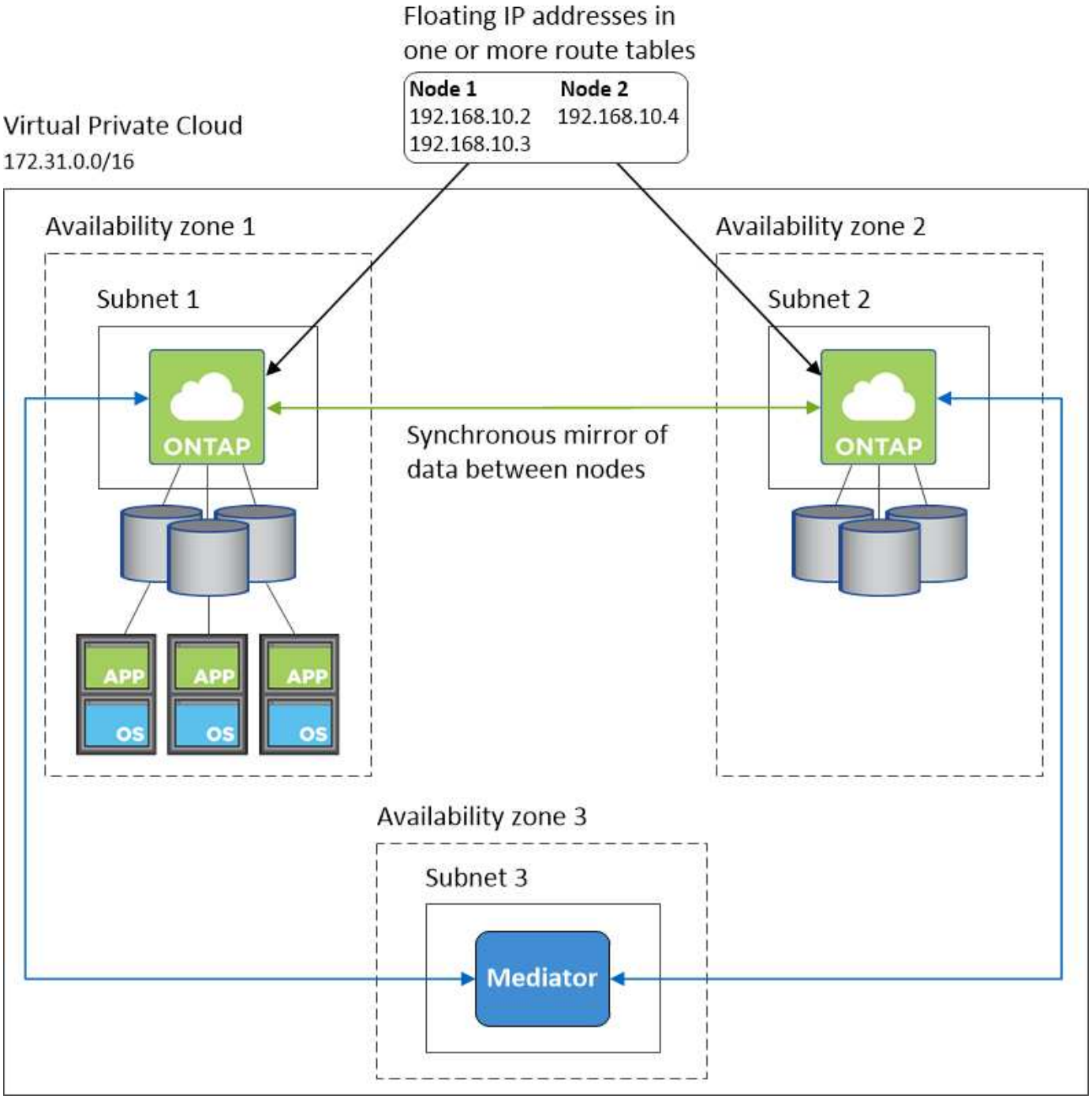
Connessione ai tool di gestione NetApp

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

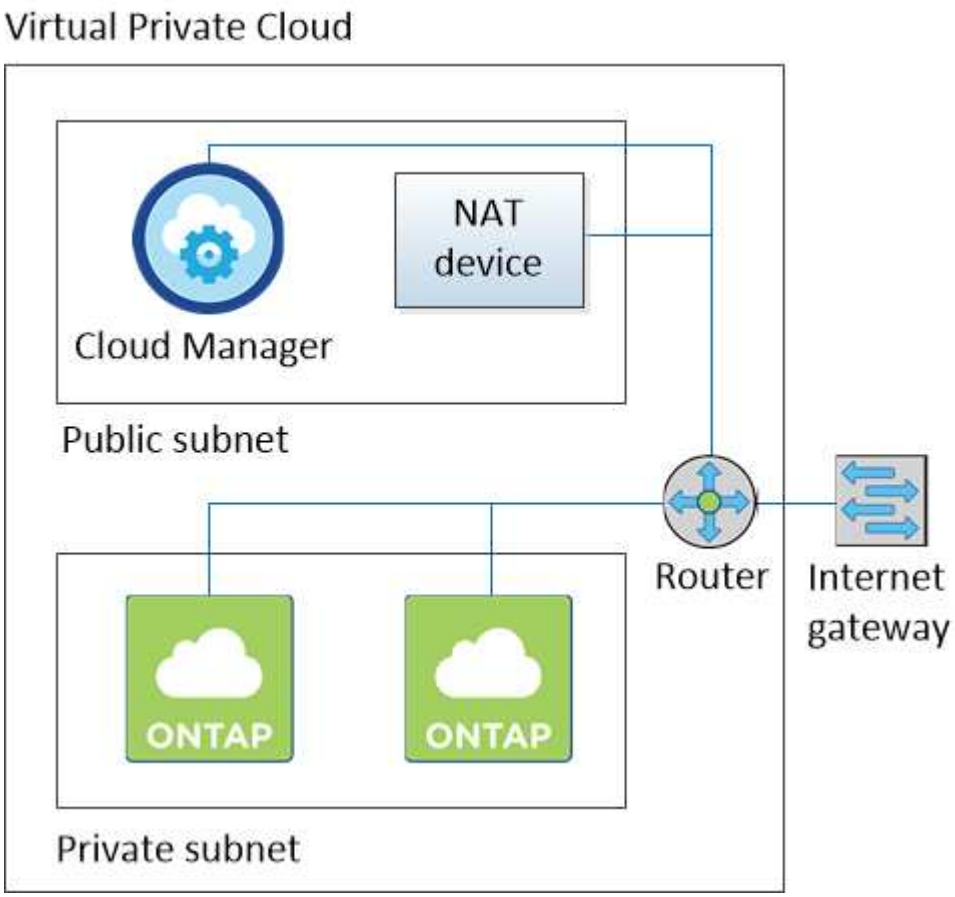
Questa configurazione VPC include subnet pubbliche e private, un gateway Internet che connette il VPC a Internet e un gateway NAT o istanza NAT nella subnet pubblica che abilita il traffico Internet in uscita dalla

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

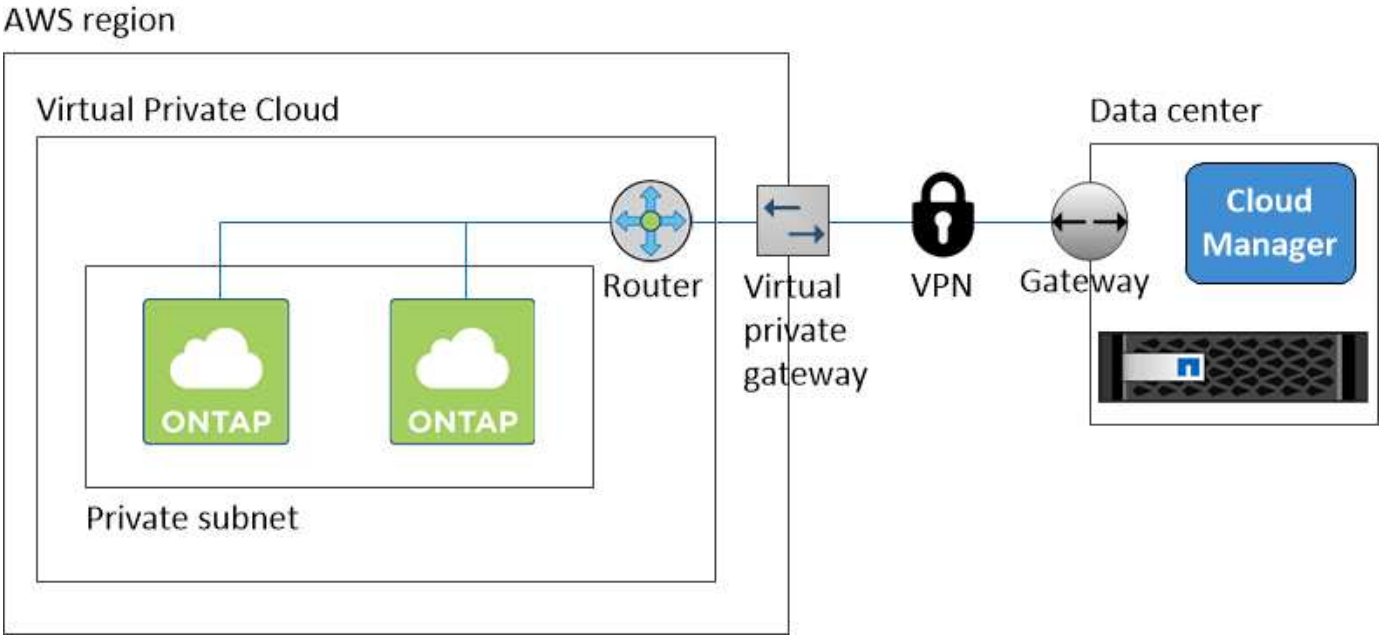
Questa configurazione VPC è una configurazione di cloud ibrido in cui Cloud Volumes ONTAP diventa un'estensione del tuo ambiente privato. La configurazione include una subnet privata e un gateway privato virtuale con una connessione VPN alla rete. Il routing attraverso il tunnel VPN consente alle istanze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

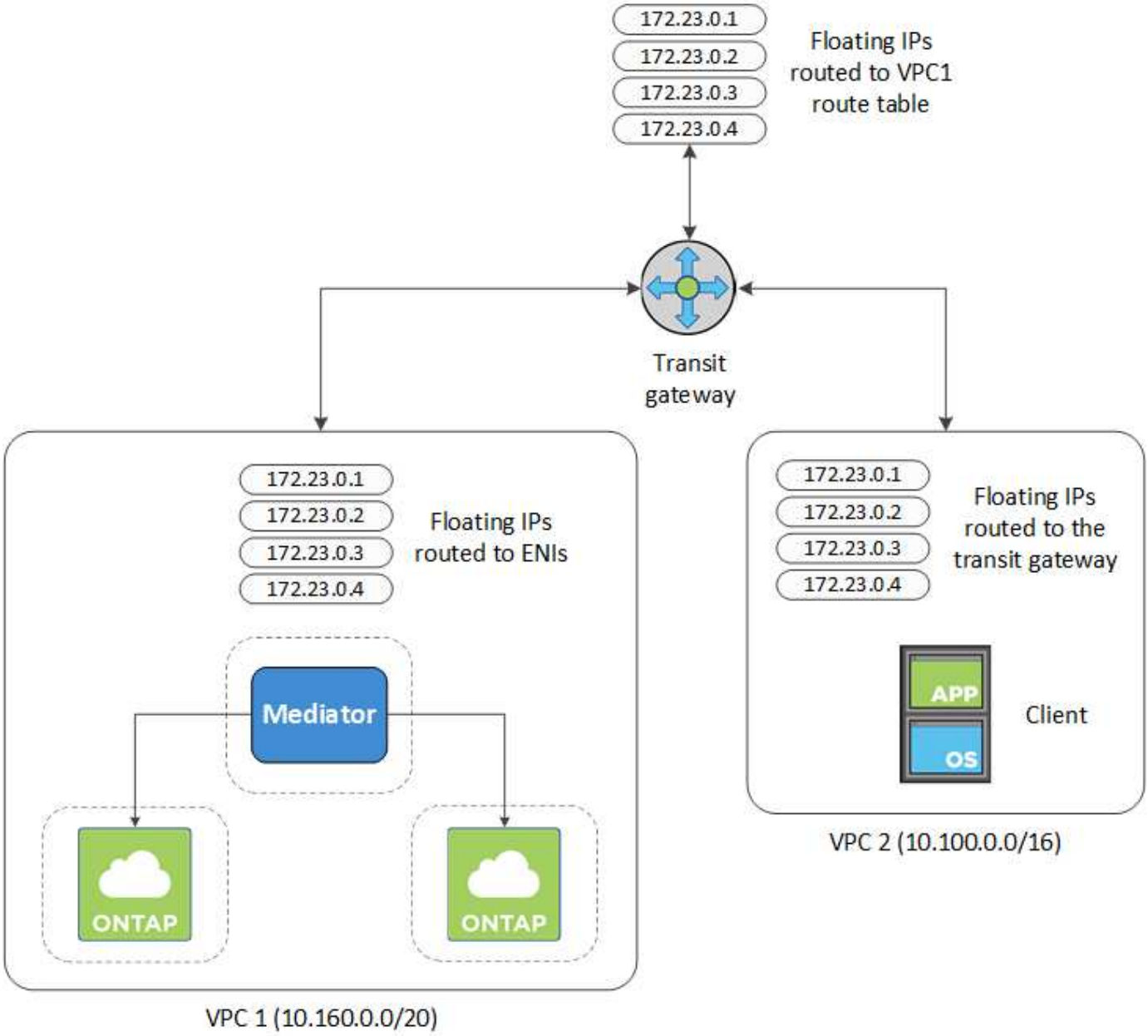
Impostare un gateway di transito AWS per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

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.

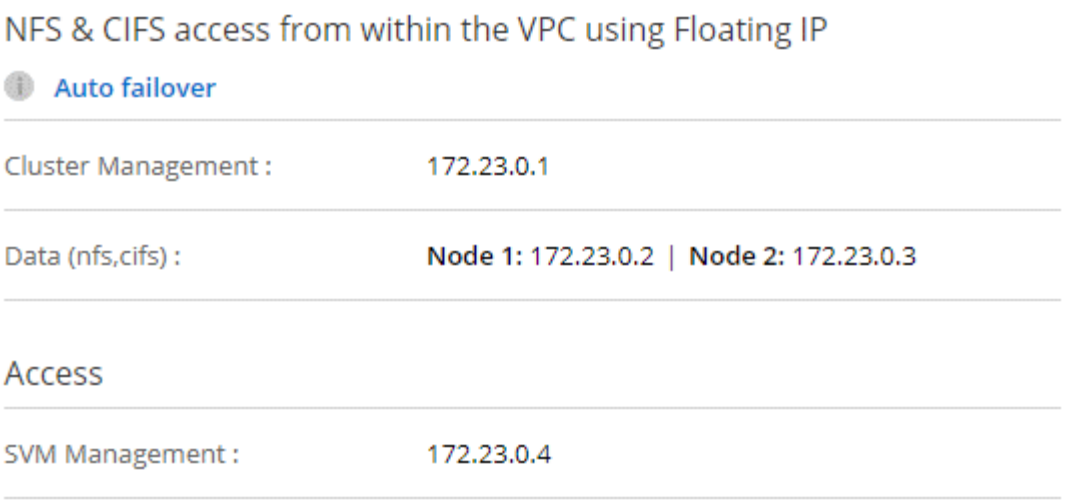


La seguente procedura illustra come configurare una configurazione simile.

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:



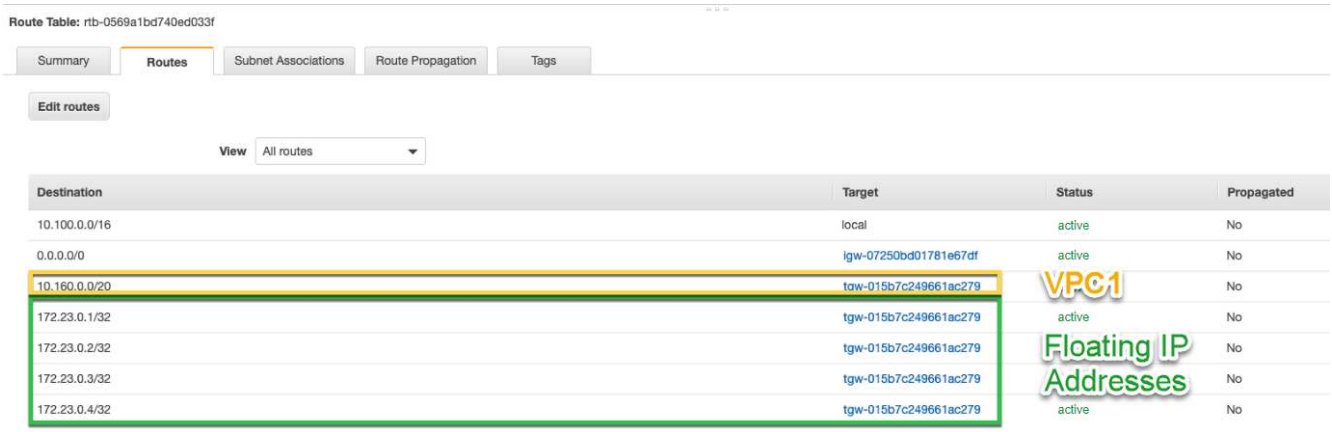
L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

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.

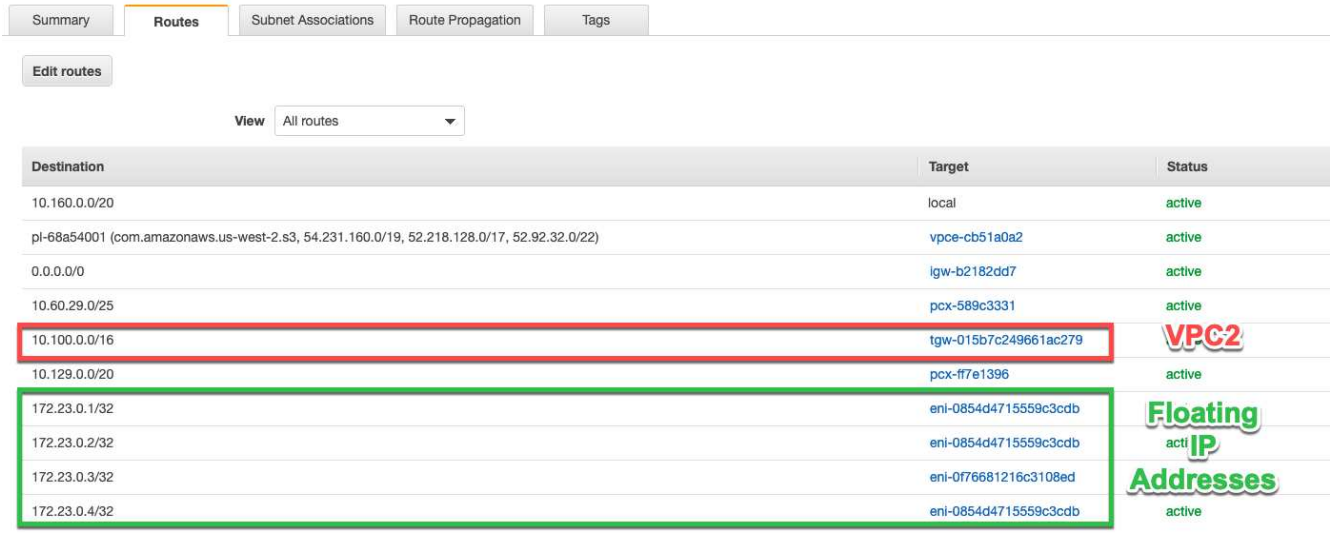
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.

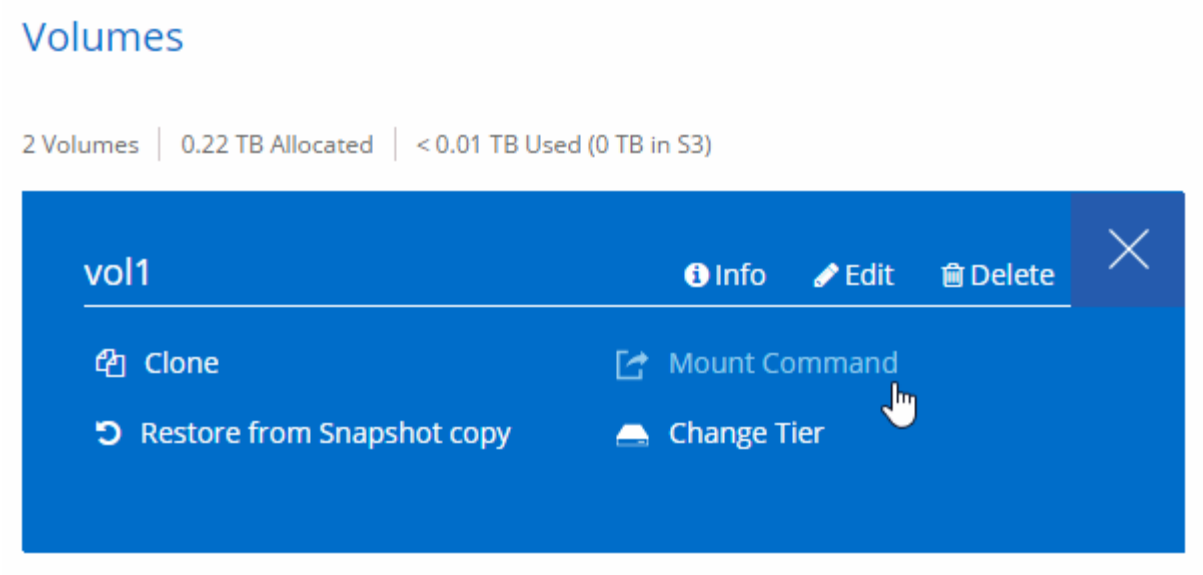
   Questo passaggio è importante perché completa il routing tra i VPC.

   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

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

Accesso a Internet in uscita per Cloud Volumes ONTAP

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

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

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

Gruppi di sicurezza

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

Numero di indirizzi IP

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

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

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

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

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

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

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

Queste autorizzazioni sono incluse nella versione più recente "Policy di Cloud Manager".

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

Connessioni a sistemi ONTAP in altre reti

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

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

Requisiti di rete per Cloud Volumes ONTAP in GCP

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

VPC condiviso

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

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

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

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

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

Accesso a Internet in uscita per Cloud Volumes ONTAP

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

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

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

Numero di indirizzi IP

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

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

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

Regole del firewall

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

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

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

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

Connessioni a sistemi ONTAP in altre reti

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

Per istruzioni, fare riferimento a. "Documentazione di Google Cloud: Panoramica di Cloud VPN".

Opzioni di implementazione aggiuntive

Requisiti degli host di Cloud Manager

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

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

È richiesto un host dedicato

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

Tipi di istanze AWS EC2 supportati

- t2.medio
- t3.medium (consigliato)

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

Dimensioni delle macchine virtuali Azure supportate

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

Tipi di macchine GCP supportati

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

Sistemi operativi supportati

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

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

  Cloud Manager è supportato dalle versioni in lingua inglese di questi sistemi operativi.

Hypervisor

Un hypervisor bare metal o in hosting certificato per l'esecuzione di CentOS o Red Hat Enterprise 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.

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

Prima di iniziare

- Un sistema Red Hat Enterprise Linux deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione di Cloud Manager.
- Il programma di installazione di Cloud Manager accede a diversi URL durante il processo di installazione. È necessario assicurarsi che l'accesso a Internet in uscita sia consentito a tali endpoint. Fare riferimento a. "Requisiti di rete per Cloud Manager".

A proposito di questa attività

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

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

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

versione.

Fasi

1. Verifica dei requisiti di rete:
   - "Requisiti di rete per Cloud Manager"
   - "Requisiti di rete per Cloud Volumes ONTAP in AWS"
   - "Requisiti di rete per Cloud Volumes ONTAP in Azure"
   - "Requisiti di rete per Cloud Volumes ONTAP in GCP"
2. Revisione "Requisiti degli host di Cloud Manager".
3. Scaricare il software dal "Sito di supporto NetApp", Quindi copiarlo sull'host Linux.

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

4. Assegnare le autorizzazioni per eseguire lo script.

   Esempio

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

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

   silent esegue l'installazione senza richiedere informazioni.

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

   proxyport è la porta del server proxy.

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

   proxypwd è la password per il nome utente specificato.

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

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

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

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

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

https://ipaddress:port

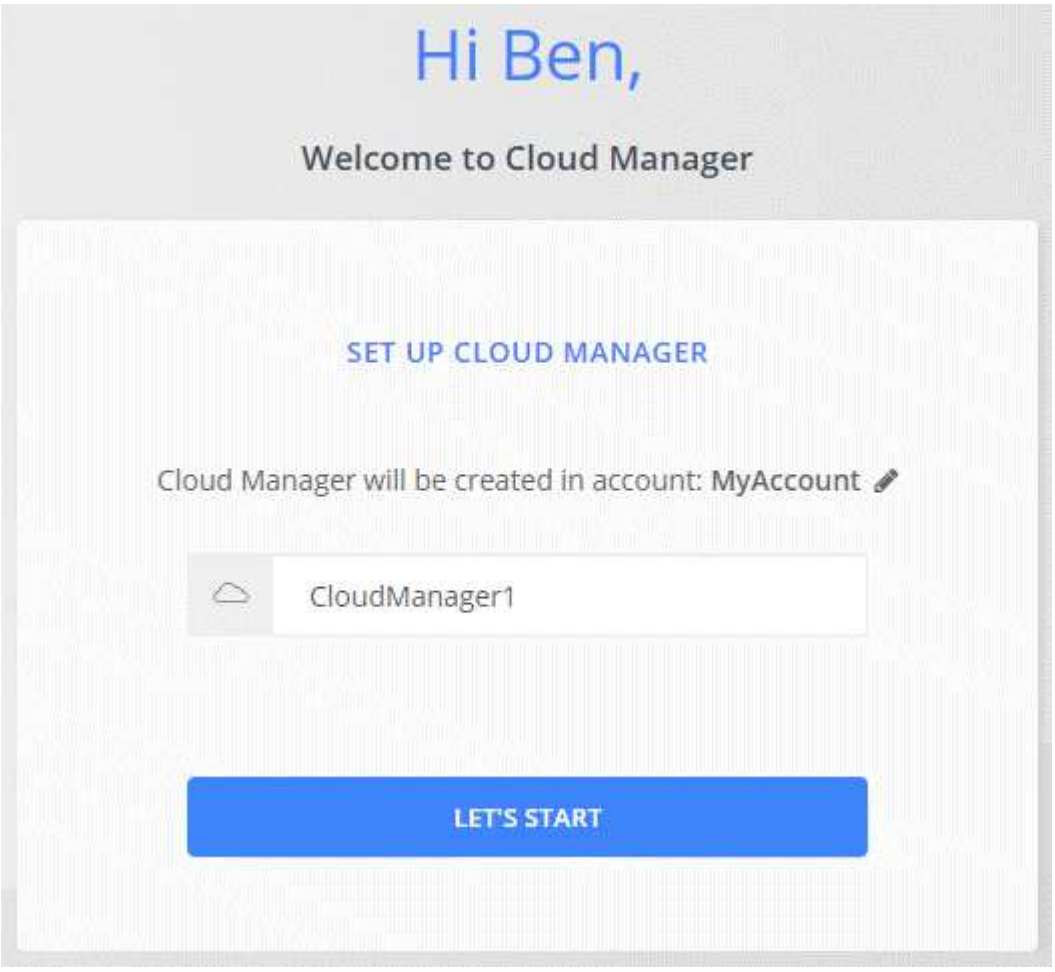
Ipaddress può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host Cloud Manager. Ad esempio, se Cloud Manager si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario inserire un indirizzo IP privato da un host che ha una connessione 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 NetApp Cloud Central o effettua l'accesso.
8. Dopo aver effettuato l'accesso, configurare Cloud Manager:
   a. Specificare l'account Cloud Central da associare al sistema Cloud Manager.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Al termine

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

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

Avvio di Cloud Manager da AWS Marketplace

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

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

A proposito di questa attività

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

Fasi

1. Creare un criterio e un ruolo IAM per l'istanza EC2:
   a. Scarica la policy IAM di Cloud Manager dal seguente percorso:

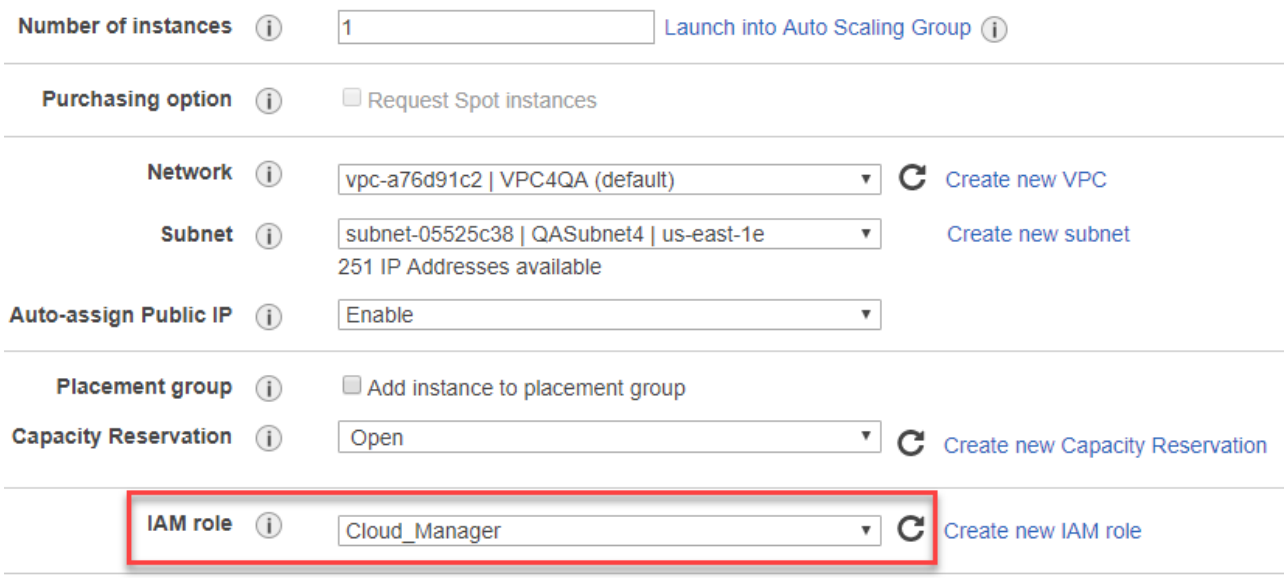
      "NetApp Cloud Manager: Policy AWS, Azure e GCP"

   b. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.
   c. Creare un ruolo IAM con il tipo di ruolo Amazon EC2 e allegare al ruolo il criterio creato nel passaggio precedente.
2. "Iscriviti a AWS Marketplace" Per garantire che non si verificano interruzioni del servizio al termine della prova gratuita di Cloud Volumes ONTAP. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata.
3. Passare alla "Pagina Cloud Manager su AWS Marketplace" Per implementare Cloud Manager da un AMI.
4. Nella pagina Marketplace, fare clic su **Continue to Subscribe**, quindi fare clic su **Continue to Configuration**.
5. Modificare una delle opzioni predefinite e fare clic su **Continue to Launch** (continua fino all'avvio).
6. In **Choose Action** (Scegli azione), selezionare **Launch through EC2** (Avvia tramite EC2*), quindi fare clic su **Launch** (Avvia).
7. Seguire le istruzioni per configurare e implementare l'istanza:
   - **Choose Instance Type** (Scegli tipo di istanza): A seconda della disponibilità della regione, scegliere

uno dei tipi di istanza supportati (si consiglia t3.medium).

"Esaminare l'elenco dei tipi di istanze supportati".

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



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

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

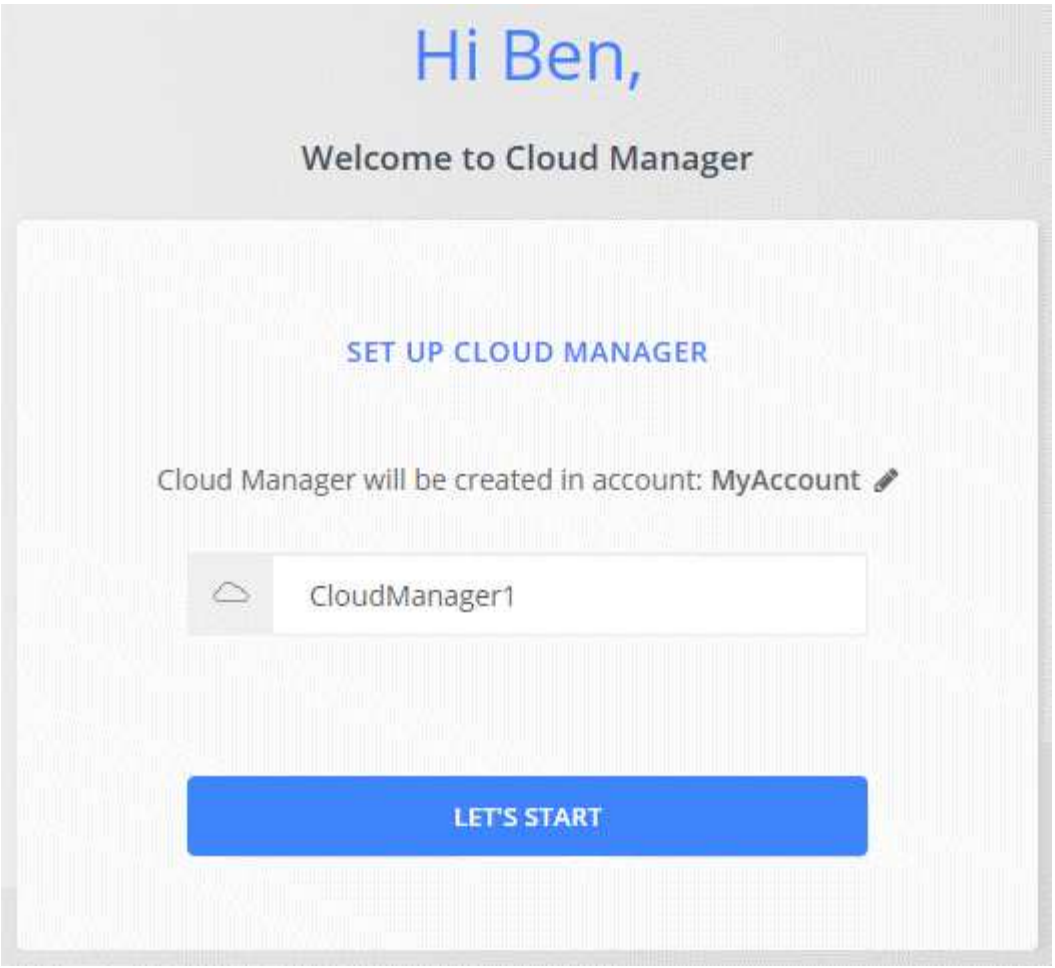
8. Aprire un browser Web da un host connesso alla macchina virtuale Cloud Manager e immettere il seguente URL:

   http://ipaddress:80

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

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Cloud Manager è ora installato e configurato.

Implementazione di Cloud Manager da Azure Marketplace

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

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

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

Implementazione di Cloud Manager in Azure

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

Fasi

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

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

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

  "Scopri di più sulle regole dei gruppi di sicurezza per Cloud Manager".

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

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

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

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

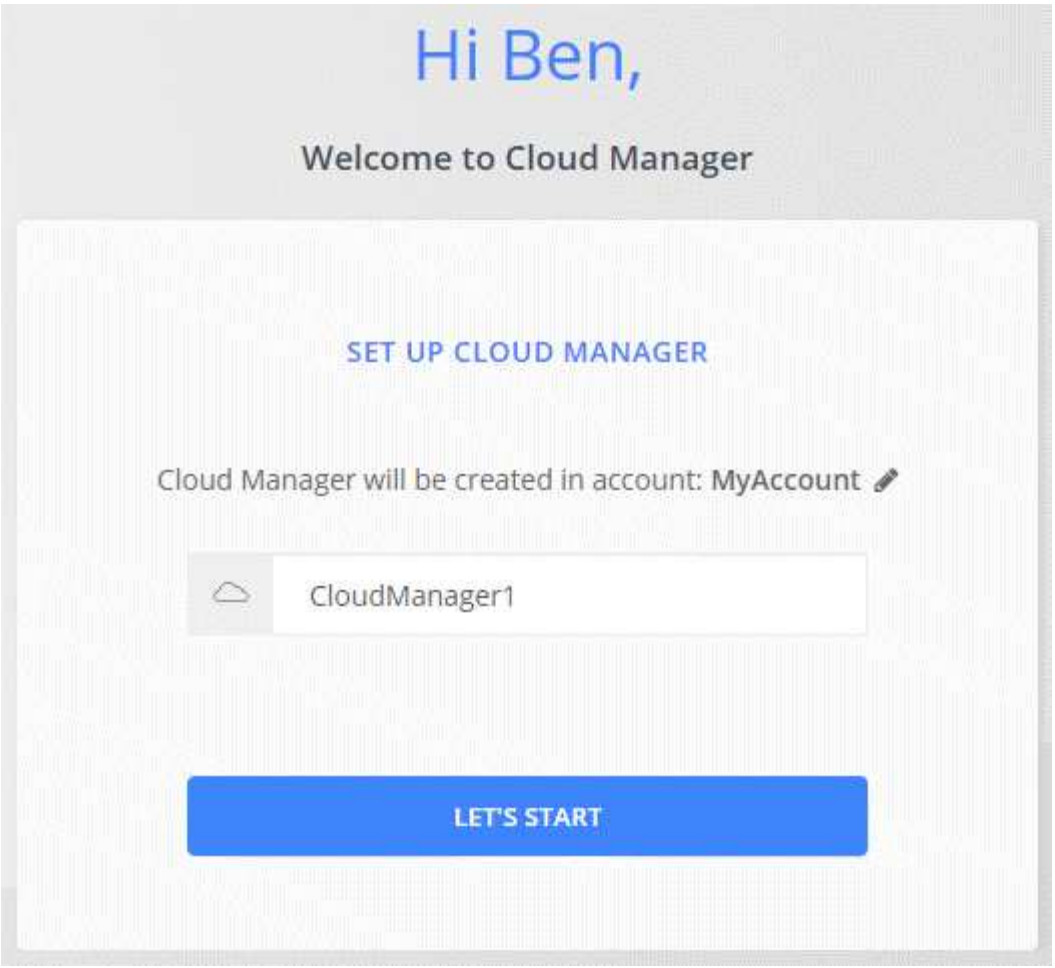
5. Aprire un browser Web da un host connesso alla macchina virtuale Cloud Manager e immettere il seguente URL:

   http://ipaddress:80

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

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

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

Concessione delle autorizzazioni Azure a Cloud Manager

Quando hai implementato Cloud Manager in Azure, dovresti aver attivato una "identità gestita assegnata dal sistema". È ora necessario concedere le autorizzazioni necessarie per Azure creando un ruolo personalizzato e assegnando il ruolo alla macchina virtuale Cloud Manager per una o più sottoscrizioni.

Fasi

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

   a. Scaricare il "Policy di Cloud Manager Azure".

   b. Modificare il file JSON aggiungendo gli ID di abbonamento Azure all'ambito assegnabile.

      È necessario aggiungere l'ID per ogni abbonamento Azure da cui gli utenti creeranno i sistemi Cloud Volumes ONTAP.

      Esempio

      "AssignableScopes": ["/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscriptions/398e471c-3b42-4ae7-9bzzbce5bzzbce5bce5bzzbce5bce5bce5b5b

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_3.7.4.json

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

2. Assegnare il ruolo alla macchina virtuale Cloud Manager per una o più sottoscrizioni:
   a. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare i sistemi Cloud Volumes ONTAP.
   b. Fare clic su **controllo di accesso (IAM)**.
   c. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
      - Selezionare il ruolo **operatore cloud OnCommand**.

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

      - Assegnare l'accesso a una **macchina virtuale**.
      - Selezionare l'abbonamento in cui è stata creata la macchina virtuale Cloud Manager.
      - Selezionare la macchina virtuale Cloud Manager.
      - Fare clic su **Save** (Salva).
   d. Se si desidera implementare Cloud Volumes ONTAP da abbonamenti aggiuntivi, passare a tale abbonamento e ripetere la procedura.

Risultato

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

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

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

Per un elenco delle regioni governative statunitensi Azure supportate, vedere "Cloud Volumes Global Regions".

Implementazione di Cloud Manager da Azure US Government Marketplace

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

Fasi

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

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

"Documentazione di Microsoft Azure: Azure Government Marketplace"

2. Cerca OnCommand Cloud Manager nel portale per il governo degli Stati Uniti.
3. Fare clic su **Create** (Crea) e seguire la procedura per configurare la macchina virtuale.

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

- Cloud Manager può funzionare in modo ottimale con dischi HDD o SSD.
- Scegliere una delle dimensioni consigliate per le macchine virtuali: A2, D2 v2 o D2 v3 (in base alla disponibilità).
- Per il gruppo di sicurezza di rete, è consigliabile scegliere **Avanzate**.

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

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

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

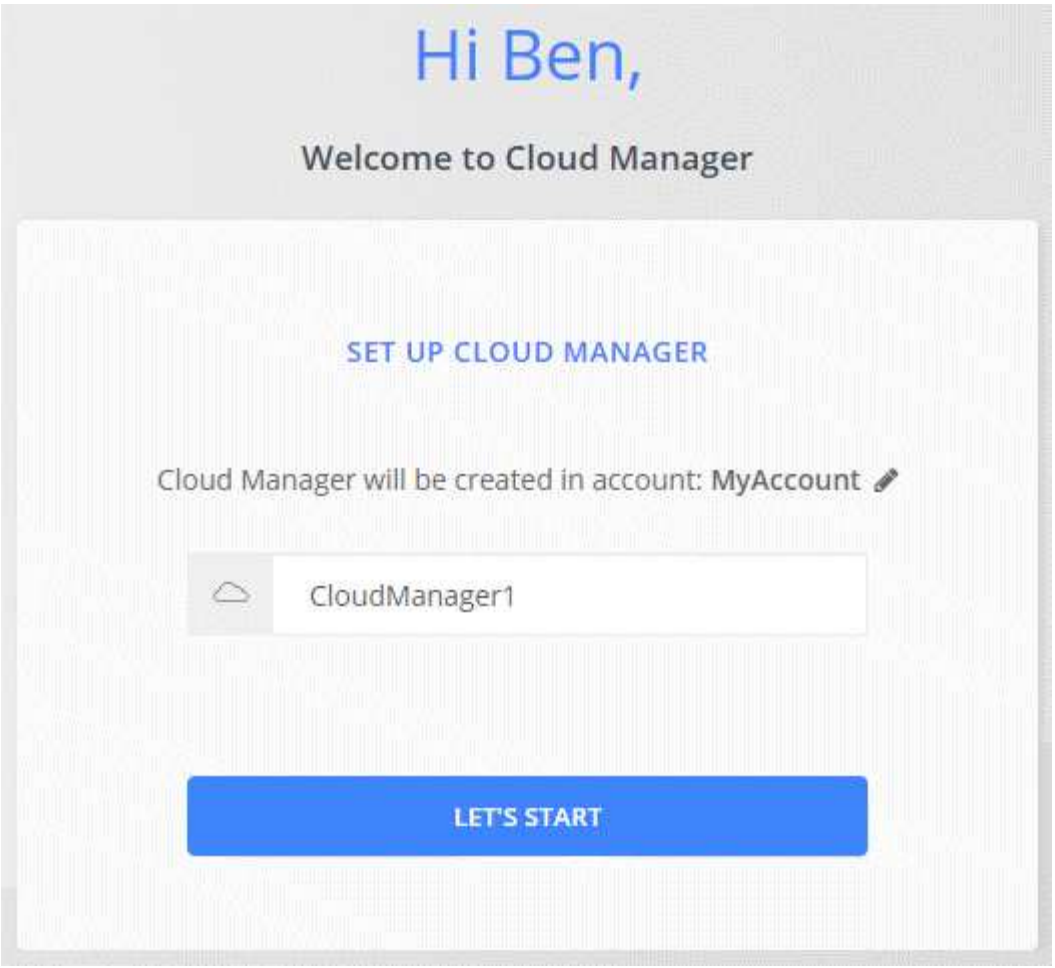
5. Aprire un browser Web da un host connesso alla macchina virtuale Cloud Manager e immettere il seguente URL:

http://ipaddress:80

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

   "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

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

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

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

Fasi

1. Abilitare un'identità gestita sulla macchina virtuale Cloud Manager:
   a. Accedere alla macchina virtuale Cloud Manager e selezionare **Identity**.
   b. In **System Assigned** (sistema assegnato), fare clic su **on**, quindi su **Save** (Salva).
2. Creare un ruolo personalizzato utilizzando la policy di Cloud Manager:
   a. Scaricare il "Policy di Cloud Manager Azure".
   b. Modificare il file JSON aggiungendo gli ID di abbonamento Azure all'ambito assegnabile.

      È necessario aggiungere l'ID per ogni abbonamento Azure da cui gli utenti creeranno i sistemi Cloud Volumes ONTAP.

Esempio

"AssignableScopes": ["/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscriptions/398e471c-3b42-4ae7-9bzzbce5bzzbce5bce5bzzbce5bce5bce5b5b

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_3.7.4.json

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

3. Assegnare il ruolo alla macchina virtuale Cloud Manager per una o più sottoscrizioni:
   a. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare i sistemi Cloud Volumes ONTAP.
   b. Fare clic su **controllo di accesso (IAM)**.
   c. Fare clic su **Aggiungi**, fare clic su **Aggiungi assegnazione ruolo**, quindi aggiungere le autorizzazioni:
      - Selezionare il ruolo **operatore cloud OnCommand**.

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

      - Assegnare l'accesso a una **macchina virtuale**.
      - Selezionare l'abbonamento in cui è stata creata la macchina virtuale Cloud Manager.
      - Digitare il nome della macchina virtuale e selezionarlo.
      - Fare clic su **Save** (Salva).
   d. Se si desidera implementare Cloud Volumes ONTAP da abbonamenti aggiuntivi, passare a tale abbonamento e ripetere la procedura.

Risultato

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

Installazione di Cloud Manager in una regione di Azure Germania

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

Fasi

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

Al termine

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

Mantenere operativo Cloud Manager

Cloud Manager deve rimanere sempre in esecuzione.

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

Implementare Cloud Volumes ONTAP

Prima di creare sistemi Cloud Volumes ONTAP

Prima di utilizzare Cloud Manager per creare e gestire i sistemi Cloud Volumes ONTAP, l'amministratore di Cloud Manager deve aver preparato il networking e installato e configurato Cloud Manager.

Prima di iniziare la distribuzione di Cloud Volumes ONTAP, devono sussistere le seguenti condizioni:

- I requisiti di rete sono stati soddisfatti per Cloud Manager e Cloud Volumes ONTAP.
- Cloud Manager dispone delle autorizzazioni necessarie per eseguire le operazioni nel cloud provider scelto.
- Per AWS, ti sei iscritto alla pagina AWS Marketplace appropriata:
  - Se si desidera implementare un sistema PAYGO o attivare una funzione aggiuntiva: "La pagina Cloud Manager (per Cloud Volumes ONTAP)".
  - Se si desidera implementare un sistema BYOL: "Il nodo singolo o la pagina ha in AWS Marketplace".
- Cloud Manager installato.

Link correlati

- "Introduzione ad AWS"
- "Introduzione ad Azure"
- "Introduzione a GCP"
- "Configurazione di Cloud Manager"

Accesso a Cloud Manager

È possibile accedere a Cloud Manager da qualsiasi browser Web che dispone di una connessione al sistema Cloud Manager. È necessario effettuare l'accesso utilizzando un "NetApp Cloud Central" account utente.

Fasi

1. Aprire un browser Web e accedere a. "NetApp Cloud Central".

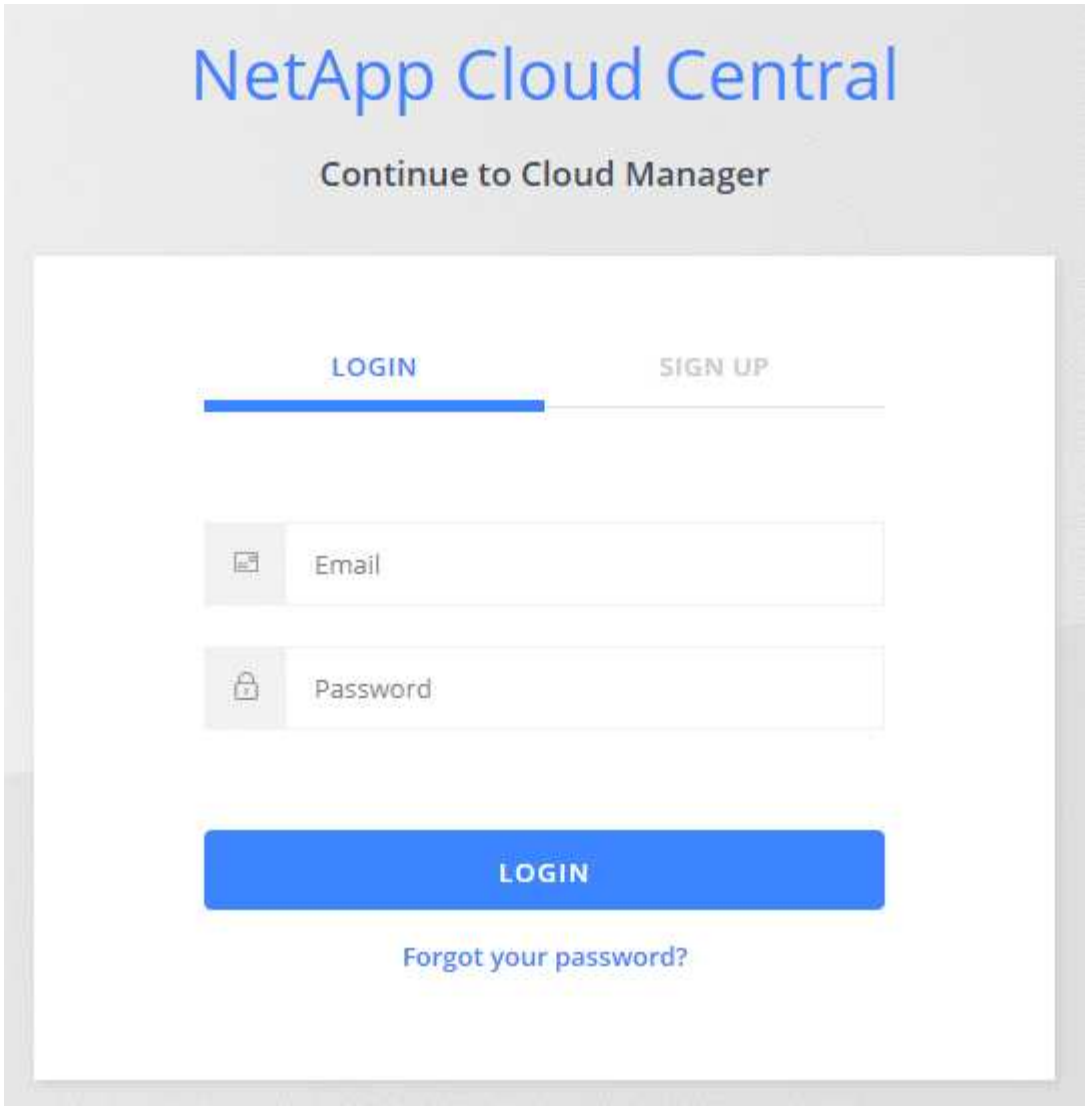
   Questo passaggio dovrebbe automaticamente essere diretto alla vista fabric. In caso contrario, fare clic su **Fabric View**.

2. Selezionare il sistema Cloud Manager a cui si desidera accedere.

   Se non vedi alcun sistema nell'elenco, assicurati che l'account Admin ti ha aggiunto all'account Cloud Central associato al sistema Cloud Manager.

3. Accedi a Cloud Manager utilizzando le credenziali di NetApp Cloud Central.



Pianificazione della configurazione di Cloud Volumes ONTAP

Quando si implementa Cloud Volumes ONTAP, è possibile scegliere un sistema preconfigurato che soddisfi i requisiti del carico di lavoro oppure creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili.

Scelta di un tipo di licenza

Cloud Volumes ONTAP è disponibile in due opzioni di prezzo: Pay-as-you-go e Bring Your Own License (BYOL). Per il pay-as-you-go, puoi scegliere tra tre licenze: Explore, Standard o Premium. Ogni licenza offre diverse capacità e opzioni di calcolo.

- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in AWS"
- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in Azure"
- "Configurazioni supportate per Cloud Volumes ONTAP 9.7 in GCP"

Comprendere i limiti dello storage

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti influiscono sulle dimensioni degli aggregati e dei volumi. Durante la pianificazione della configurazione, è necessario conoscere questi limiti.

- "Limiti di storage per Cloud Volumes ONTAP 9.7 in AWS"
- "Limiti di storage per Cloud Volumes ONTAP 9.7 in Azure"
- "Limiti di storage per Cloud Volumes ONTAP 9.7 in GCP"

Scelta della velocità di scrittura

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normali e alte e i rischi e le raccomandazioni quando si utilizza un'elevata velocità di scrittura.

Differenza tra la velocità di scrittura normale e l'alta velocità di scrittura

Quando si sceglie la normale velocità di scrittura, i dati vengono scritti direttamente su disco, riducendo così la probabilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

Quando si sceglie un'elevata velocità di scrittura, i dati vengono memorizzati nel buffer prima che vengano scritti su disco, garantendo prestazioni di scrittura più rapide. A causa di questo caching, vi è la possibilità di perdita di dati in caso di un'interruzione non pianificata del sistema.

La quantità di dati che è possibile perdere in caso di interruzione non pianificata del sistema è l'intervallo degli ultimi due punti di coerenza. Un punto di coerenza è l'azione di scrittura dei dati bufferizzati su disco. Un punto di coerenza si verifica quando il registro di scrittura è pieno o dopo 10 secondi (a seconda di quale condizione si verifica per prima). Tuttavia, le performance del volume di AWS EBS possono influire sul tempo di elaborazione dei punti di coerenza.

Quando utilizzare un'elevata velocità di scrittura

L'elevata velocità di scrittura è una buona scelta se per il carico di lavoro sono richieste prestazioni di scrittura rapide e se si può resistere al rischio di perdita di dati in caso di un'interruzione non pianificata del sistema.

Consigli quando si utilizza un'elevata velocità di scrittura

Se si attiva l'alta velocità di scrittura, è necessario garantire la protezione in scrittura a livello di applicazione.

Scelta di un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza dello storage che consentono di ridurre la quantità totale di storage necessaria. Quando crei un volume in Cloud Manager, puoi scegliere un profilo che abiliti queste funzionalità o un profilo che le disabiliti. Dovresti saperne di più su queste funzionalità per aiutarti a decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Thin provisioning

Presenta uno storage logico maggiore per gli host o gli utenti rispetto al pool di storage fisico. Invece di preallocare lo spazio di storage, lo spazio di storage viene allocato dinamicamente a ciascun volume durante la scrittura dei dati.

Deduplica

Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità dello storage eliminando blocchi di dati ridondanti che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica richiesta per memorizzare i dati comprimendo i dati all'interno di un volume su storage primario, secondario e di archivio.

Pianificazione AWS

Pianificare l'implementazione di Cloud Volumes ONTAP in AWS dimensionando il sistema ed esaminando le informazioni di rete da inserire.

- Dimensionamento del sistema in AWS
- Foglio di lavoro delle informazioni di rete AWS

Dimensionamento del sistema in AWS

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance e capacità. Quando si sceglie un tipo di istanza, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di istanza

- Abbina i requisiti di carico di lavoro al throughput massimo e agli IOPS per ogni tipo di istanza EC2.
- Se diversi utenti scrivono nel sistema contemporaneamente, scegliere un tipo di istanza con CPU sufficienti per gestire le richieste.
- Se si dispone di un'applicazione in gran parte in lettura, scegliere un sistema con una quantità di RAM sufficiente.
  - "Documentazione AWS: Tipi di istanze Amazon EC2"
  - "Documentazione AWS: Istanze ottimizzate per Amazon EBS"

Tipo di disco EBS

Gli SSD General Purpose sono il tipo di disco più comune per Cloud Volumes ONTAP. Per visualizzare i casi di utilizzo dei dischi EBS, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

Dimensione del disco EBS

Quando si avvia un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. Dopo di che, è possibile "Lascia che Cloud Manager gestisca la capacità di un sistema per te", ma se lo si desidera "costruisci gli aggregati", tenere presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Le prestazioni dei dischi EBS sono legate alle dimensioni dei dischi. La dimensione determina gli IOPS di riferimento e la durata massima del burst per i dischi SSD e il throughput di base e burst per i dischi HDD.
- In definitiva, è necessario scegliere le dimensioni del disco che offrono le *prestazioni sostenute* necessarie.
- Anche se si scelgono dischi più grandi (ad esempio, sei dischi da 4 TB), è possibile che non si ottengano tutti gli IOPS perché l'istanza EC2 può raggiungere il limite di larghezza di banda.

Per ulteriori informazioni sulle prestazioni dei dischi EBS, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

Guarda il seguente video per ulteriori dettagli sul dimensionamento del tuo sistema Cloud Volumes ONTAP in AWS:

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

Foglio di lavoro delle informazioni di rete AWS

Quando si avvia Cloud Volumes ONTAP in AWS, è necessario specificare i dettagli della rete VPC. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Informazioni di rete per Cloud Volumes ONTAP

Informazioni AWS	Il tuo valore
Regione	
VPC	
Subnet	
Gruppo di sicurezza (se si utilizza il proprio)	

Informazioni di rete per una coppia ha in più AZS

Informazioni AWS	Il tuo valore
Regione	
VPC	
Gruppo di sicurezza (se si utilizza il proprio)	
Zona di disponibilità del nodo 1	
Subnet del nodo 1	
Zona di disponibilità del nodo 2	
Subnet del nodo 2	
Area di disponibilità del mediatore	
Subnet del mediatore	
Coppia di chiavi per il mediatore	
Indirizzo IP mobile per la porta di gestione del cluster	
Indirizzo IP mobile per i dati sul nodo 1	
Indirizzo IP mobile per i dati sul nodo 2	

Informazioni AWS	Il tuo valore
Tabelle di routing per gli indirizzi IP mobili	

Pianificazione di Azure

Pianifica la tua implementazione di Cloud Volumes ONTAP in Azure dimensionando il tuo sistema ed esaminando le informazioni di rete che devi inserire.

- Dimensionamento del sistema in Azure
- Foglio di lavoro con le informazioni di rete di Azure

Dimensionamento del sistema in Azure

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance e capacità. Quando si sceglie un tipo di macchina virtuale, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di macchina virtuale

Esaminare i tipi di macchine virtuali supportati in "Note di rilascio di Cloud Volumes ONTAP" Quindi, esaminare i dettagli relativi a ciascun tipo di macchina virtuale supportato. Tenere presente che ogni tipo di macchina virtuale supporta un numero specifico di dischi dati.

- "Documentazione di Azure: Dimensioni generali delle macchine virtuali"
- "Documentazione di Azure: Dimensioni delle macchine virtuali ottimizzate per la memoria"

Tipo di disco Azure

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza come disco.

I sistemi HA utilizzano i blob di pagina Premium. Nel frattempo, i sistemi a nodo singolo possono utilizzare due tipi di dischi gestiti Azure:

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.
- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

  Per ulteriori informazioni sui casi di utilizzo di questi dischi, vedere "Documentazione di Microsoft Azure: Introduzione allo storage Microsoft Azure".

Dimensioni del disco Azure

Quando si avviano le istanze di Cloud Volumes ONTAP, è necessario scegliere la dimensione predefinita del disco per gli aggregati. Cloud Manager utilizza questa dimensione del disco per l'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa da quella predefinita di "utilizzando l'opzione di allocazione avanzata".

Tutti i dischi di un aggregato devono avere le stesse dimensioni.

Quando si sceglie una dimensione del disco, è necessario prendere in considerazione diversi fattori. Le dimensioni del disco influiscono sul costo dello storage, sulle dimensioni dei volumi che è possibile creare in un aggregato, sulla capacità totale disponibile per Cloud Volumes ONTAP e sulle performance dello storage.

Le prestazioni di Azure Premium Storage sono legate alle dimensioni del disco. I dischi più grandi offrono IOPS e throughput più elevati. Ad esempio, la scelta di dischi da 1 TB può offrire prestazioni migliori rispetto ai dischi da 500 GB, a un costo superiore.

Non esistono differenze di performance tra le dimensioni dei dischi per lo storage standard. È necessario scegliere le dimensioni del disco in base alla capacità richiesta.

Fare riferimento a Azure per IOPS e throughput in base alle dimensioni del disco:

- "Microsoft Azure: Prezzi dei dischi gestiti"
- "Microsoft Azure: Page Blobs pricing"

Foglio di lavoro con le informazioni di rete di Azure

Quando si implementa Cloud Volumes ONTAP in Azure, è necessario specificare i dettagli della rete virtuale. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Informazioni su Azure	Il tuo valore
Regione	
Rete virtuale (VNET)	
Subnet	
Gruppo di sicurezza di rete (se si utilizza il proprio)	

Pianificazione GCP

Pianifica la tua implementazione di Cloud Volumes ONTAP nella piattaforma cloud di Google dimensionando il tuo sistema ed esaminando le informazioni di rete che devi inserire.

- Dimensionamento del sistema in GCP
- Foglio di lavoro delle informazioni di rete GCP

Dimensionamento del sistema in GCP

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance e capacità. Quando si sceglie un tipo di macchina, un tipo di disco e una dimensione del disco, occorre tenere presente alcuni punti chiave:

Tipo di macchina

Esaminare i tipi di computer supportati in "Note di rilascio di Cloud Volumes ONTAP" Quindi, esamina i dettagli di Google relativi a ciascun tipo di computer supportato. Abbina i requisiti di carico di lavoro al numero di vCPU e di memoria per il tipo di computer. Si noti che ogni core della CPU aumenta le performance di rete.

Per ulteriori informazioni, fare riferimento a quanto segue:

- "Documentazione di Google Cloud: Tipi di computer standard N1"
- "Documentazione Google Cloud: Performance"

Tipo di disco GCP

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante utilizzato da Cloud Volumes ONTAP per un disco. Il tipo di disco può essere *dischi persistenti SSD Zonal* o *dischi persistenti standard Zonal*.

I dischi persistenti SSD sono ideali per i carichi di lavoro che richiedono elevati tassi di IOPS casuali, mentre i dischi persistenti standard sono economici e possono gestire operazioni di lettura/scrittura sequenziali. Per ulteriori informazioni, vedere "Documentazione di Google Cloud: Dischi persistenti zonali (Standard e SSD)".

Dimensione del disco GCP

Quando si implementa un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. In seguito, puoi lasciare che Cloud Manager gestisca la capacità di un sistema per te, ma se vuoi creare aggregati, tieni presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Determinare lo spazio necessario, tenendo in considerazione le performance.
- Le performance dei dischi persistenti si ridimensionano automaticamente in base alle dimensioni del disco e al numero di vCPU disponibili per il sistema.

  Per ulteriori informazioni, fare riferimento a quanto segue:

  - "Documentazione di Google Cloud: Dischi persistenti zonali (Standard e SSD)"
  - "Documentazione di Google Cloud: Ottimizzazione delle performance di dischi persistenti e SSD locali"

Foglio di lavoro delle informazioni di rete GCP

Quando si implementa Cloud Volumes ONTAP in GCP, è necessario specificare i dettagli della rete virtuale. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Informazioni GCP	Il tuo valore
Regione	
Zona	
Rete VPC	
Subnet	
Policy firewall (se si utilizza il proprio)	

Individuazione dell'ID di sistema di Cloud Manager

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

Fasi

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

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

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

   Esempio

Attivazione di Flash cache su Cloud Volumes ONTAP

Alcune configurazioni Cloud Volumes ONTAP in AWS e Azure includono lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance.

Cos'è Flash cache?

Flash cache accelera l'accesso ai dati attraverso il caching intelligente in tempo reale dei dati utente recentemente letti e dei metadati NetApp. È efficace per carichi di lavoro a lettura intensiva, inclusi database, e-mail e file service.

Limitazioni

- La compressione deve essere disattivata su tutti i volumi per sfruttare i miglioramenti delle prestazioni di Flash cache.
- Il ripristino della cache dopo un riavvio non è supportato con Cloud Volumes ONTAP.

Abilitazione di Flash cache su Cloud Volumes ONTAP in AWS

Flash cache è supportata con Cloud Volumes ONTAP Premium e BYOL in AWS.

Fasi

1. Selezionare uno dei seguenti tipi di istanze EC2 con un sistema Cloud Volumes ONTAP Premium o BYOL nuovo o esistente:
   - c5d.4xlarge

- c5d.9xlarge
- r5d.2xlarge

2. Disattiva la compressione su tutti i volumi per sfruttare i miglioramenti delle performance di Flash cache.

   Scegli l'assenza di efficienza dello storage durante la creazione di un volume da Cloud Manager, oppure crea un volume e poi "Disattivare la compressione dei dati utilizzando l'interfaccia CLI".

Abilitazione di Flash cache su Cloud Volumes ONTAP in Azure

Flash cache è supportata con Cloud Volumes ONTAP BYOL su sistemi a nodo singolo.

Fasi

1. Selezionare il tipo di macchina virtuale Standard_L8s_v2 con un sistema BYOL Cloud Volumes ONTAP a nodo singolo in Azure.
2. Disattiva la compressione su tutti i volumi per sfruttare i miglioramenti delle performance di Flash cache.

   Scegli l'assenza di efficienza dello storage durante la creazione di un volume da Cloud Manager, oppure crea un volume e poi "Disattivare la compressione dei dati utilizzando l'interfaccia CLI".

Avvio di Cloud Volumes ONTAP in AWS

È possibile avviare Cloud Volumes ONTAP in una configurazione a sistema singolo o come coppia ha in AWS.

Iscrizione a AWS Marketplace

Iscriviti al marketplace AWS per pagare Cloud Volumes ONTAP mentre vai o per implementare Cloud Volumes ONTAP BYOL.

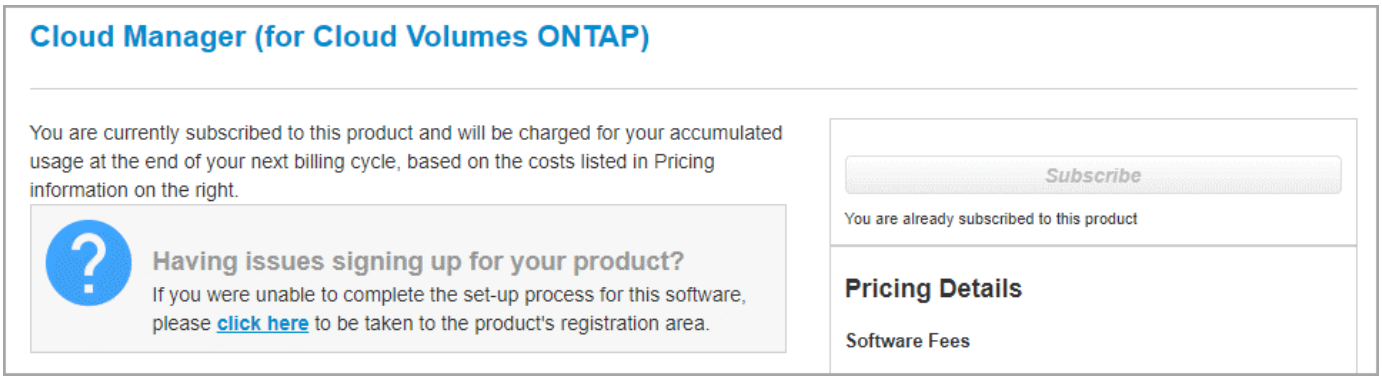
Iscrizione A PAYGO

"Iscriviti a AWS Marketplace" Per garantire che non si verificano interruzioni del servizio al termine della prova gratuita di Cloud Volumes ONTAP. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata.

Il seguente video mostra la procedura di iscrizione:

► https://docs.netapp.com/it-it/occm37//media/video_subscribing_aws.mp4 *(video)*

Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS mostra agli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l'account AWS, ciascun utente IAM deve associarsi all'abbonamento. Se viene visualizzato il messaggio riportato di seguito, fare clic sul collegamento **fare clic qui** per accedere a Cloud Central e completare il processo.



Iscrizione a BYOL

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

"Scopri di più su ogni pagina di AWS Marketplace".

Avvio di un singolo sistema Cloud Volumes ONTAP in AWS

Se si desidera avviare Cloud Volumes ONTAP in AWS, è necessario creare un nuovo ambiente di lavoro in Cloud Manager.

Prima di iniziare

- Si dovrebbe aver preparato scegliendo una configurazione e ottenendo le informazioni di rete AWS dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Se si desidera avviare un sistema BYOL, è necessario disporre del numero di serie a 20 cifre (chiave di licenza).
- Se si desidera utilizzare CIFS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP in AWS".

A proposito di questa attività

Subito dopo aver creato l'ambiente di lavoro, Cloud Manager avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, Cloud Manager termina immediatamente l'istanza e avvia l'implementazione del sistema Cloud Volumes ONTAP. Se Cloud Manager non riesce a verificare la connettività, la creazione dell'ambiente di lavoro non riesce. L'istanza di test è t2.nano (per la tenancy VPC predefinita) o m3.medium (per la tenancy VPC dedicata).

Fasi

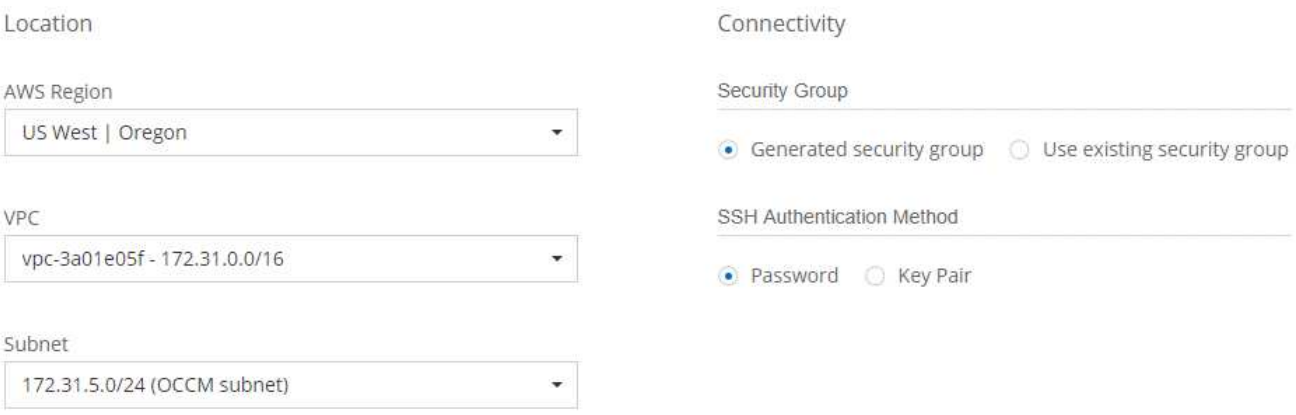
1. Nella pagina ambienti di lavoro, fare clic su **Crea Cloud Volumes ONTAP** e seguire le istruzioni.
2. **Definisci il tuo ambiente di lavoro**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Se si desidera, modificare l'account AWS e l'abbonamento al marketplace, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Account	Puoi scegliere un altro account se lo desideri "Aggiunti altri account AWS a Cloud Manager".
Abbonamento Marketplace	Selezionare un altro abbonamento se si desidera modificare l'account AWS da cui si ottiene l'addebito. Per aggiungere un nuovo abbonamento, "Vai all'offerta in AWS Marketplace".
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Aggiungere tag	I tag AWS sono metadati per le risorse AWS. Cloud Manager aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ogni risorsa AWS associata all'istanza. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione AWS: Contrassegno delle risorse Amazon EC2".
Credenziali	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema di OnCommand o la relativa CLI.

4. **Servizi**: Consente di abilitare o disabilitare i singoli servizi che non si desidera utilizzare con questo sistema Cloud Volumes ONTAP.
   - "Scopri di più su Backup in S3".
   - "Scopri di più sulla conformità al cloud".
5. **Location & Connectivity** (posizione e connettività): Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente immagine mostra la pagina compilata:



6. **Crittografia dei dati**: Non scegliere alcuna crittografia dei dati o crittografia gestita da AWS.

   Per la crittografia gestita da AWS, è possibile scegliere una chiave Customer Master Key (CMK) diversa dal proprio account o da un altro account AWS.

Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

"Scopri come configurare AWS KMS per Cloud Volumes ONTAP".

"Scopri di più sulle tecnologie di crittografia supportate".

7. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

8. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

9. **Ruolo IAM**: Devi mantenere l'opzione predefinita per consentire a Cloud Manager di creare il ruolo per te.

   Se si preferisce utilizzare la propria policy, è necessario che sia conforme "Requisiti dei criteri per i nodi Cloud Volumes ONTAP".

10. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle necessità, selezionare una licenza, un tipo di istanza e la tenancy dell'istanza.

    Se le esigenze cambiano dopo l'avvio dell'istanza, è possibile modificare il tipo di licenza o di istanza in un secondo momento.

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.4 RC1 e 9.4 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.3 a 9.4.

11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering S3.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per eventuali aggregati aggiuntivi creati da Cloud Manager quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

    Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in AWS".

12. **Write Speed & WORM**: Scegliere **Normal** o **High** write speed e attivare lo storage write once, Read Many (WORM), se lo si desidera.

    "Scopri di più sulla velocità di scrittura".

"Scopri di più sullo storage WORM".

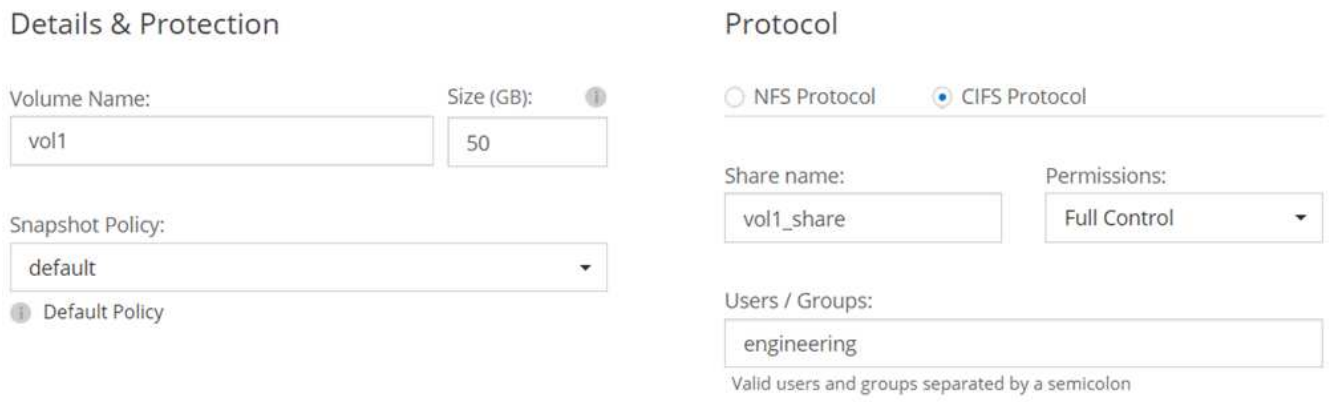
13. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    Se si desidera creare un volume per iSCSI, saltare questo passaggio. Cloud Manager imposta i volumi solo per NFS e CIFS.

    Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

    La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



14. **CIFS Setup**: Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

15. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering S3, se necessario.

    Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

16. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

Cloud Manager avvia l'istanza di Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'avvio dell'istanza di Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su Re-create environment (Crea ambiente).

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.

- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvio di una coppia Cloud Volumes ONTAP ha in AWS

Se si desidera lanciare una coppia Cloud Volumes ONTAP ha in AWS, è necessario creare un ambiente di lavoro ha in Cloud Manager.

Prima di iniziare

- Si dovrebbe aver preparato scegliendo una configurazione e ottenendo le informazioni di rete AWS dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Se sono state acquistate licenze BYOL, è necessario disporre di un numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.
- Se si desidera utilizzare CIFS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP in AWS".

A proposito di questa attività

Subito dopo aver creato l'ambiente di lavoro, Cloud Manager avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, Cloud Manager termina immediatamente l'istanza e avvia l'implementazione del sistema Cloud Volumes ONTAP. Se Cloud Manager non riesce a verificare la connettività, la creazione dell'ambiente di lavoro non riesce. L'istanza di test è t2.nano (per la tenancy VPC predefinita) o m3.medium (per la tenancy VPC dedicata).

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Crea Cloud Volumes ONTAP** e seguire le istruzioni.
2. **Definisci il tuo ambiente di lavoro**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP ha**.
3. **Dettagli e credenziali**: Se si desidera, modificare l'account AWS e l'abbonamento al marketplace, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

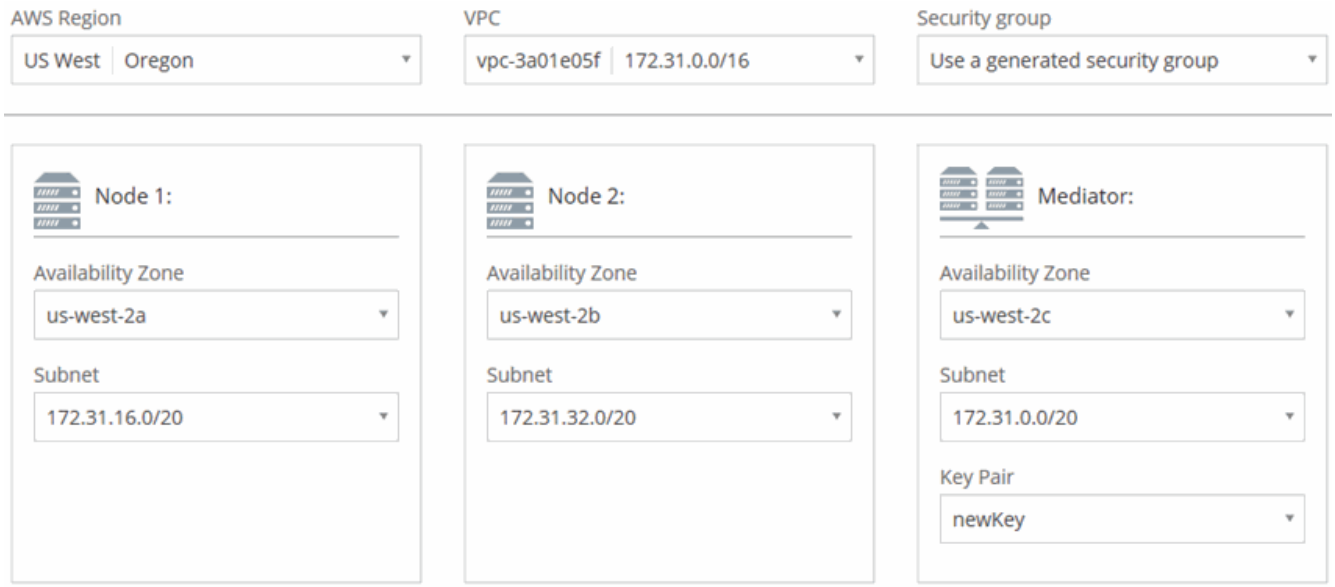
Campo	Descrizione
Account	Puoi scegliere un altro account se lo desideri "Aggiunti altri account AWS a Cloud Manager".
Abbonamento Marketplace	Selezionare un altro abbonamento se si desidera modificare l'account AWS da cui si ottiene l'addebito. Per aggiungere un nuovo abbonamento, "Vai all'offerta in AWS Marketplace".
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.

Campo	Descrizione
Aggiungere tag	I tag AWS sono metadati per le risorse AWS. Cloud Manager aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ogni risorsa AWS associata all'istanza. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione AWS: Contrassegno delle risorse Amazon EC2".
Credenziali	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema di OnCommand o la relativa CLI.

4. **Servizi**: Consente di abilitare o disabilitare i singoli servizi che non si desidera utilizzare con questo sistema Cloud Volumes ONTAP.
   - "Scopri di più su Backup in S3".
   - "Scopri di più sulla conformità al cloud".
5. **Modelli di implementazione ha**: Scegliere una configurazione ha.

   Per una panoramica dei modelli di implementazione, vedere "Cloud Volumes ONTAP ha per AWS".
6. **Regione e VPC**: Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente immagine mostra la pagina compilata per una configurazione AZ multipla:



7. **Connettività e autenticazione SSH**: Scegliere i metodi di connessione per la coppia ha e il mediatore.
8. **IP mobili**: Se si sceglie più AZS, specificare gli indirizzi IP mobili.

   Gli indirizzi IP devono essere esterni al blocco CIDR per tutti i VPC della regione. Per ulteriori informazioni, vedere "Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS".
9. **Route Table**: Se si sceglie Multiple AZS, selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili.

Se si dispone di più tabelle di percorso, è molto importante selezionare le tabelle di percorso corrette. In caso contrario, alcuni client potrebbero non avere accesso alla coppia Cloud Volumes ONTAP ha. Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a. "Documentazione AWS: Tabelle di percorso".

10. **Crittografia dei dati**: Non scegliere alcuna crittografia dei dati o crittografia gestita da AWS.

    Per la crittografia gestita da AWS, è possibile scegliere una chiave Customer Master Key (CMK) diversa dal proprio account o da un altro account AWS.

    Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

    "Scopri come configurare AWS KMS per Cloud Volumes ONTAP".

    "Scopri di più sulle tecnologie di crittografia supportate".

11. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

    Per informazioni sul funzionamento delle licenze, vedere "Licensing".

    Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

12. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

13. **Ruolo IAM**: Devi mantenere l'opzione predefinita per consentire a Cloud Manager di creare i ruoli per te.

    Se si preferisce utilizzare la propria policy, è necessario che sia conforme "Requisiti delle policy per i nodi Cloud Volumes ONTAP e il mediatore ha".

14. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle necessità, selezionare una licenza, un tipo di istanza e la tenancy dell'istanza.

    Se le esigenze cambiano dopo l'avvio delle istanze, è possibile modificare il tipo di licenza o di istanza in un secondo momento.

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.4 RC1 e 9.4 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.3 a 9.4.

15. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering S3.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per eventuali aggregati aggiuntivi

creati da Cloud Manager quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in AWS".

16. **WORM**: Attivare lo storage write once, Read Many (WORM), se lo si desidera.

    "Scopri di più sullo storage WORM".

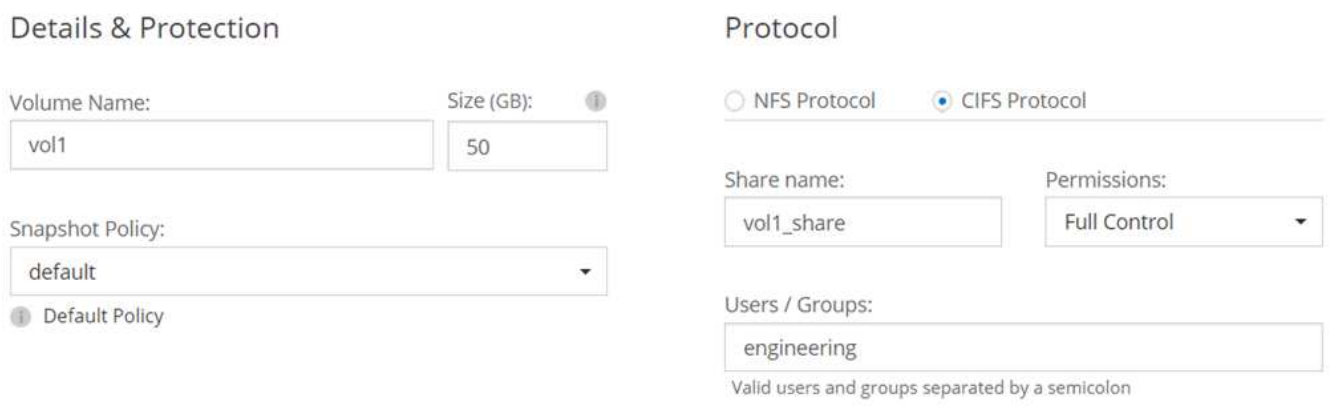
17. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    Se si desidera creare un volume per iSCSI, saltare questo passaggio. Cloud Manager imposta i volumi solo per NFS e CIFS.

    Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



18. **CIFS Setup**: Se è stato selezionato il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

19. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering S3, se necessario.

    Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

20. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

Cloud Manager lancia la coppia Cloud Volumes ONTAP ha. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'avvio della coppia ha, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su Re-create environment (Crea ambiente).

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le

cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.

- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Lancio di Cloud Volumes ONTAP in Azure

È possibile avviare un sistema a nodo singolo o una coppia ha in Azure creando un ambiente di lavoro Cloud Volumes ONTAP in Cloud Manager.

Prima di iniziare

- Assicurarsi che l'account Azure disponga delle autorizzazioni necessarie, soprattutto se si esegue l'aggiornamento da una release precedente e si sta implementando un sistema ha per la prima volta.

  Le autorizzazioni più recenti si trovano in "Policy di NetApp Cloud Central per Azure".

- È necessario aver scelto una configurazione e ottenuto le informazioni di rete di Azure dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.

A proposito di questa attività

Quando Cloud Manager crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti Azure, come un gruppo di risorse, interfacce di rete e account di storage. Al termine della procedura guidata, è possibile visualizzare un riepilogo delle risorse.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Crea Cloud Volumes ONTAP** e seguire le istruzioni.
2. **Definisci il tuo ambiente di lavoro**: Seleziona **Microsoft Azure** e scegli un singolo nodo o una coppia ha.
3. **Dettagli e credenziali**: Se si desidera, modificare l'account o l'abbonamento Azure, specificare un nome di cluster e di gruppo di risorse, aggiungere tag, se necessario, quindi specificare le credenziali.

   La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Cambia account	Puoi scegliere un account o un abbonamento diverso, se lo desideri "Configurali e aggiungili a Cloud Manager".
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome gruppo di risorse	Se si deseleziona l'opzione **Usa predefinito**, è possibile immettere il nome di un nuovo gruppo di risorse. Se si desidera utilizzare un gruppo di risorse esistente, è necessario utilizzare l'API.

Campo	Descrizione
Tag	I tag sono metadati per le risorse Azure. Cloud Manager aggiunge i tag al sistema Cloud Volumes ONTAP e a ogni risorsa Azure associata al sistema. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione di Microsoft Azure: Utilizzo di tag per organizzare le risorse di Azure".
Credenziali	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema di OnCommand o la relativa CLI.

4. **Servizi**: Mantieni abilitata la conformità cloud o disattivala se non desideri utilizzarla con questo sistema Cloud Volumes ONTAP.

   "Scopri di più sulla conformità al cloud".

5. **Location & Connectivity** (posizione e connettività): Selezionare una posizione e un gruppo di sicurezza e selezionare la casella di controllo per confermare la connettività di rete tra Cloud Manager e la posizione di destinazione.
6. **License and Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

7. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

8. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze, selezionare una licenza e selezionare un tipo di macchina virtuale.

   Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

   > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.5 RC1 e 9.5 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.4 a 9.5.

9. **Iscriviti al marketplace Azure**: Segui la procedura se Cloud Manager non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
10. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per eventuali aggregati aggiuntivi creati da Cloud Manager quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in Azure".

11. **Write Speed & WORM**: Scegliere **Normal** o **High** write speed e attivare lo storage write once, Read Many (WORM), se lo si desidera.

   La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

   "Scopri di più sulla velocità di scrittura".

   "Scopri di più sullo storage WORM".

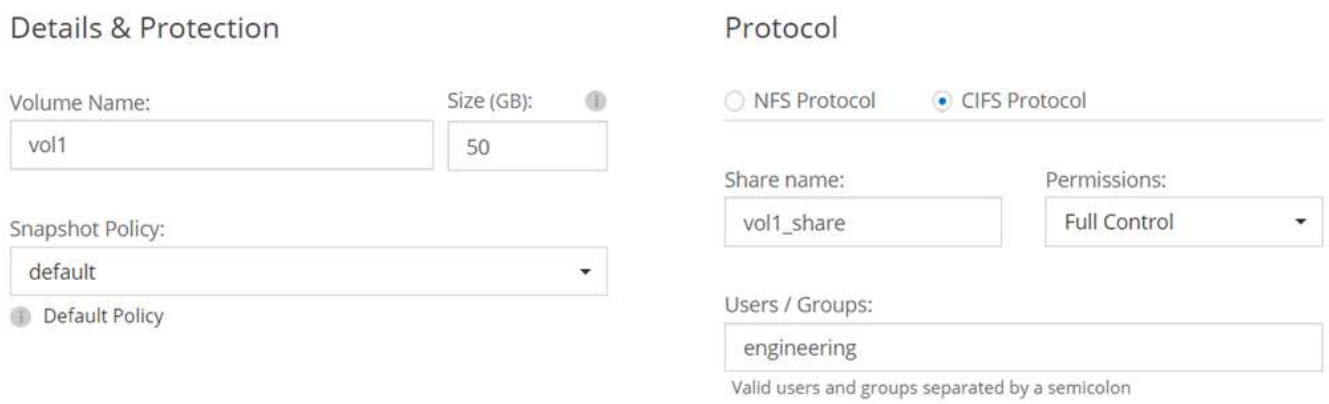
12. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

   Saltare questo passaggio se si desidera utilizzare iSCSI. Cloud Manager consente di creare volumi solo per NFS e CIFS.

   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

   La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



13. **CIFS Setup**: Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

14. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering, se necessario.

    Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

15. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.

a. Esaminare i dettagli della configurazione.

b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse di Azure che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

Risultato

Cloud Manager implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare ambiente**.

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvio di Cloud Volumes ONTAP in GCP

È possibile avviare un sistema Cloud Volumes ONTAP a nodo singolo in GCP creando un ambiente di lavoro.

Prima di iniziare

- Si dovrebbe aver scelto una configurazione e ottenuto le informazioni di rete GCP dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.

Fasi

1. nella pagina Working Environments (ambienti di lavoro), fare clic su **Create Cloud Volumes ONTAP** (Crea server) e seguire le istruzioni.
2. **Definisci l'ambiente di lavoro**: Fare clic su **continua**.
3. **Iscriviti a Cloud Volumes ONTAP**: Se ti viene richiesto, iscriviti a Cloud Volumes ONTAP nel marketplace GCP.

   Il seguente video mostra la procedura di iscrizione:

   ► https://docs.netapp.com/it-it/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, aggiungere etichette e specificare le credenziali.

   La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Progetto Google Cloud	Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede Cloud Manager. Se non vedi altri progetti nell'elenco a discesa, non hai ancora associato l'account del servizio Cloud Manager ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account di servizio con il ruolo di Cloud Manager a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Questo è l'account di servizio configurato per Cloud Manager, "come descritto nella fase 4b di questa pagina".
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza della VM GCP. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Aggiungi etichette	Le etichette sono metadati per le risorse GCP. Cloud Manager aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse GCP associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a. "Documentazione Google Cloud: Risorse per l'etichettatura".
Credenziali	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema o la relativa CLI.

5. **Posizione e connettività**: Selezionare una posizione, scegliere un criterio firewall e selezionare la casella di controllo per confermare la connettività di rete allo storage Google Cloud per il tiering dei dati.

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

6. **License & Support Site account**: Specificare se si desidera utilizzare la funzione pay-as-you-go o BYOL, quindi specificare un account NetApp Support Site.

   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

   Un account NetApp Support Site è opzionale per il pay-as-you-go, ma necessario per i sistemi BYOL. "Scopri come aggiungere account NetApp Support Site".

7. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

8. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze, selezionare una licenza e selezionare un tipo di macchina virtuale.

Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.5 RC1 e 9.5 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.4 a 9.5.

9. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati.

   Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

   Le dimensioni del disco sono per tutti i dischi nell'aggregato iniziale e per eventuali aggregati aggiuntivi creati da Cloud Manager quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

   Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in GCP".

10. **Write Speed & WORM**: Scegliere **Normal** o **High** write speed e attivare lo storage write once, Read Many (WORM), se lo si desidera.

    "Scopri di più sulla velocità di scrittura".

    "Scopri di più sullo storage WORM".

11. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

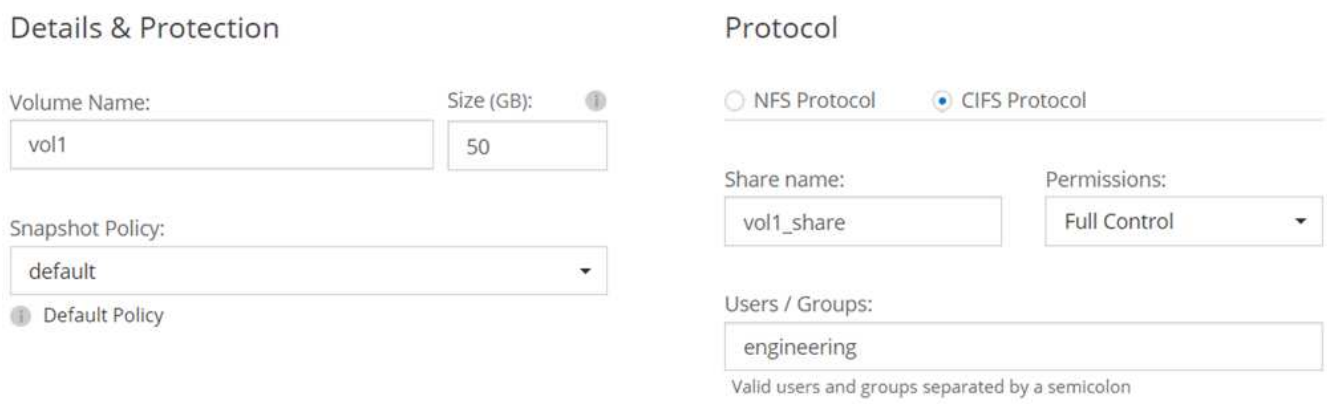
    Saltare questo passaggio se si desidera utilizzare iSCSI. Cloud Manager consente di creare volumi solo per NFS e CIFS.

    Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.

Campo	Descrizione
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



12. **CIFS Setup**: Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer.
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

13. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello

storage e modificare la policy di tiering, se necessario.

Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

14. **Google Cloud Platform account for Data Tiering**: Imposta il tiering dei dati fornendo chiavi di accesso allo storage interoperabili per un account Google Cloud Platform. Fare clic su **Ignora** per disattivare il tiering dei dati.

    Le chiavi consentono a Cloud Manager di configurare un bucket di cloud storage per il tiering dei dati. Per ulteriori informazioni, vedere "Configurazione e aggiunta di account GCP a Cloud Manager".

15. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse GCP che Cloud Manager acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

Cloud Manager implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare ambiente**.

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Registrazione di sistemi pay-as-you-go

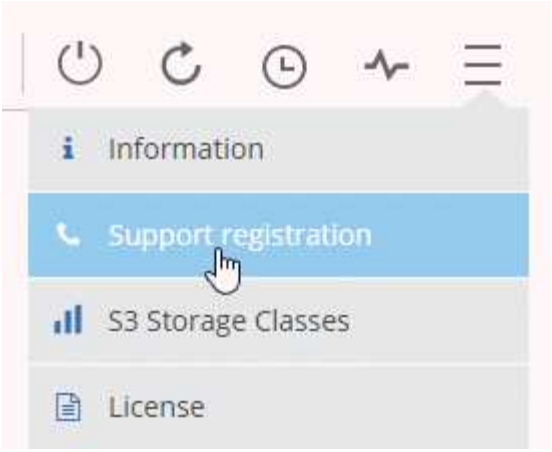
Il supporto NetApp è incluso nei sistemi Cloud Volumes ONTAP Explore, Standard e Premium, ma è necessario prima attivare il supporto registrando i sistemi con NetApp.

Fasi

1. Se non hai ancora aggiunto il tuo account NetApp Support Site a Cloud Manager, vai a **Impostazioni account** e aggiungilo ora.

   "Scopri come aggiungere account NetApp Support Site".

2. Nella pagina ambienti di lavoro, fare doppio clic sul nome del sistema che si desidera registrare.
3. Fare clic sull'icona del menu, quindi su **registrazione supporto**:



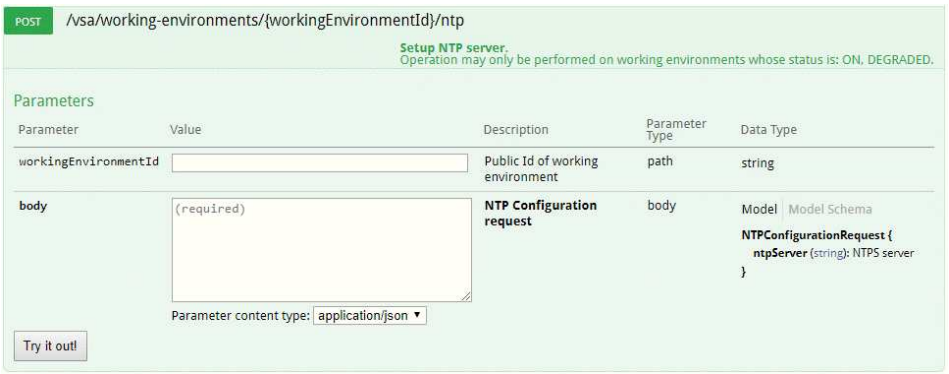
4. Selezionare un account NetApp Support Site e fare clic su **Register**.

Risultato

Cloud Manager registra il sistema con NetApp.

Configurazione di Cloud Volumes ONTAP

Dopo aver implementato Cloud Volumes ONTAP, è possibile configurarlo sincronizzando l'ora del sistema utilizzando NTP ed eseguendo alcune attività facoltative da Gestore di sistema o CLI.

Attività	Descrizione
Sincronizzare l'ora del sistema utilizzando NTP	La specifica di un server NTP sincronizza l'ora tra i sistemi della rete, evitando così problemi dovuti a differenze di tempo. Specificare un server NTP utilizzando l'API Cloud Manager o dall'interfaccia utente quando si imposta un server CIFS. • "Modifica del server CIFS" • "Guida per sviluppatori API di Cloud Manager" Ad esempio, ecco l'API per un sistema a nodo singolo in AWS: 

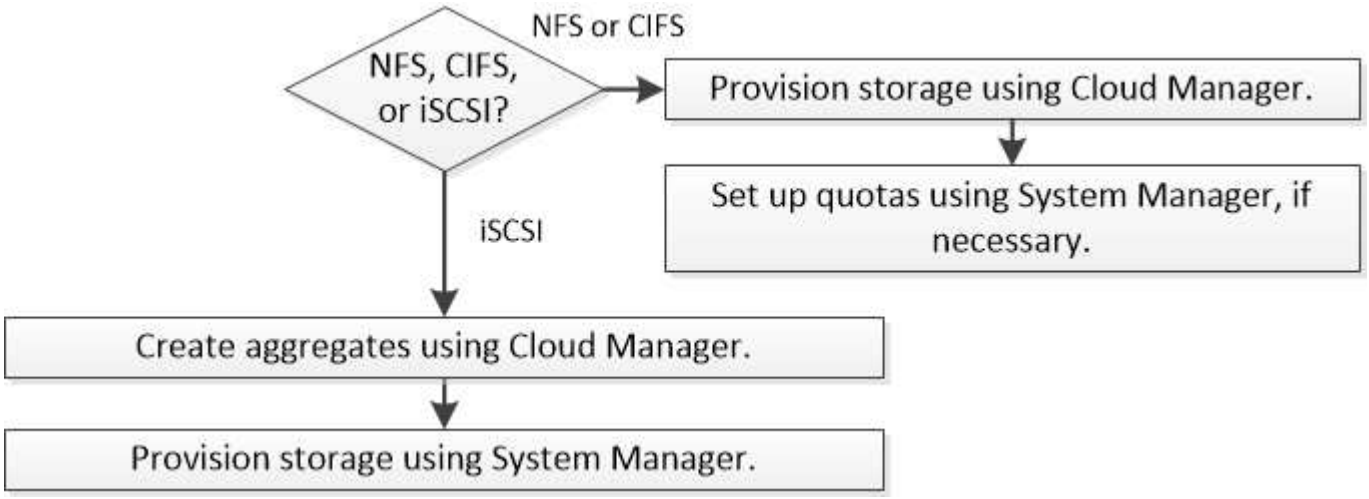
Attività	Descrizione
Facoltativo: Configurare AutoSupport	AutoSupport monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp per impostazione predefinita. Se l'amministratore dell'account ha aggiunto un server proxy a Cloud Manager prima di avviare l'istanza, Cloud Volumes ONTAP viene configurato per utilizzare tale server proxy per i messaggi AutoSupport. Verificare che AutoSupport sia in grado di inviare messaggi. Per istruzioni, consultare la Guida in linea di System Manager o il "Guida di riferimento per l'amministrazione del sistema ONTAP 9".
Opzionale: Configurare EMS	Il sistema di gestione degli eventi (EMS) raccoglie e visualizza informazioni sugli eventi che si verificano nei sistemi Cloud Volumes ONTAP. Per ricevere le notifiche degli eventi, è possibile impostare le destinazioni degli eventi (indirizzi e-mail, host di trap SNMP o server syslog) e i percorsi degli eventi per una particolare gravità degli eventi. È possibile configurare EMS utilizzando la CLI. Per istruzioni, consultare "Guida rapida alla configurazione EMS di ONTAP 9".
Opzionale: Creare un'interfaccia di rete di gestione SVM (LIF) per i sistemi ha in più zone di disponibilità AWS	Se si desidera utilizzare SnapCenter o SnapDrive per Windows con una coppia ha, è necessaria un'interfaccia di rete per la gestione delle macchine virtuali storage (SVM). La LIF di gestione SVM deve utilizzare un indirizzo IP *mobile* quando si utilizza una coppia ha in più zone di disponibilità AWS. Cloud Manager richiede di specificare l'indirizzo IP mobile quando si avvia la coppia ha. Se non è stato specificato l'indirizzo IP, è possibile creare autonomamente la LIF di gestione SVM da System Manager o dalla CLI. Nell'esempio seguente viene illustrato come creare la LIF dalla CLI: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Facoltativo: Modificare la posizione di backup dei file di configurazione	Cloud Volumes ONTAP crea automaticamente file di backup della configurazione contenenti informazioni sulle opzioni configurabili necessarie per il corretto funzionamento. Per impostazione predefinita, Cloud Volumes ONTAP esegue il backup dei file nell'host di Cloud Manager ogni otto ore. Se si desidera inviare i backup a una posizione alternativa, è possibile modificare la posizione in un server FTP o HTTP nel data center o in AWS. Ad esempio, è possibile che si disponga già di una posizione di backup per i sistemi di storage FAS. È possibile modificare la posizione di backup utilizzando l'interfaccia CLI. Vedere "Guida di riferimento per l'amministrazione del sistema ONTAP 9".

Eseguire il provisioning dello storage

Provisioning dello storage

Puoi eseguire il provisioning di storage NFS e CIFS aggiuntivi per i tuoi sistemi Cloud Volumes ONTAP da Cloud Manager attraverso la gestione di volumi e aggregati. Se è necessario creare storage iSCSI, è necessario farlo da System Manager.

Tutti i dischi e gli aggregati devono essere creati ed eliminati direttamente da Cloud Manager. Non eseguire queste azioni da un altro tool di gestione. In questo modo si può influire sulla stabilità del sistema, ostacolare la possibilità di aggiungere dischi in futuro e potenzialmente generare tariffe ridondanti per i provider di cloud.



Creazione di volumi FlexVol

Se hai bisogno di più storage dopo il lancio di un sistema Cloud Volumes ONTAP, puoi creare nuovi volumi FlexVol per NFS o CIFS da Cloud Manager.

Prima di iniziare

Se si desidera utilizzare CIFS in AWS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP per AWS".

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera eseguire il provisioning dei volumi FlexVol.
2. Creare un nuovo volume su qualsiasi aggregato o su un aggregato specifico:

Azione	Fasi
Crea un nuovo volume e lascia che Cloud Manager scelga l'aggregato contenente	Fare clic su **Add New Volume** (Aggiungi nuovo volume).

Azione	Fasi
Creare un nuovo volume su un aggregato specifico	a. Fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**. b. Fare clic sul menu per un aggregato. c. Fare clic su **Create volume** (Crea volume).

3. Inserire i dettagli del nuovo volume, quindi fare clic su **continua**.

   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

4. Se si sceglie il protocollo CIFS e il server CIFS non è stato configurato, specificare i dettagli del server nella finestra di dialogo Crea un server CIFS, quindi fare clic su **Salva e continua**:

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.

Campo	Descrizione
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. • Per configurare AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo. • Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

5. Nella pagina Usage Profile (Profilo di utilizzo), Disk Type (tipo di disco) e Tiering Policy (criterio di tiering), scegliere se attivare le funzionalità di efficienza dello storage, scegliere un tipo di disco e modificare il criterio di tiering, se necessario.

   Per assistenza, fare riferimento a quanto segue:

   ◦ "Comprensione dei profili di utilizzo dei volumi"
   ◦ "Dimensionamento del sistema in AWS"
   ◦ "Dimensionamento del sistema in Azure"
   ◦ "Panoramica sul tiering dei dati"

6. Fare clic su **Go**.

Risultato

Cloud Volumes ONTAP esegue il provisioning del volume.

Al termine

Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.

Se si desidera applicare le quote ai volumi, è necessario utilizzare System Manager o la CLI. Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Creazione di volumi FlexVol sul secondo nodo in una configurazione ha

Per impostazione predefinita, Cloud Manager crea volumi sul primo nodo in una configurazione ha. Se è necessaria una configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, è necessario creare aggregati e volumi sul secondo nodo.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi creare l'aggregato.
4. Per nodo principale, scegliere il secondo nodo della coppia ha.
5. Dopo che Cloud Manager ha creato l'aggregato, selezionarlo e fare clic su **Create volume** (Crea volume).
6. Inserire i dettagli del nuovo volume, quindi fare clic su **Create** (Crea).

Al termine

Se necessario, è possibile creare volumi aggiuntivi su questo aggregato.

Per le coppie ha implementate in più zone di disponibilità AWS, è necessario montare il volume sui client utilizzando l'indirizzo IP mobile del nodo su cui risiede il volume.

Creazione di aggregati

È possibile creare aggregati o lasciare che Cloud Manager lo faccia per te quando crea volumi. Il vantaggio della creazione di aggregati consiste nella possibilità di scegliere la dimensione del disco sottostante, che consente di dimensionare l'aggregato in base alla capacità o alle performance necessarie.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'istanza di Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi specificare i dettagli per l'aggregato.

   Per informazioni sul tipo di disco e sulle dimensioni del disco, vedere "Pianificazione della configurazione".

4. Fare clic su **Go**, quindi su **Approve and Purchase** (approva e acquista).

Provisioning dei LUN iSCSI

Se si desidera creare LUN iSCSI, è necessario farlo da System Manager.

Prima di iniziare

- Le utility host devono essere installate e configurate sugli host che si connetteranno al LUN.
- È necessario aver registrato il nome iSCSI Initiator dall'host. Specificare questo nome quando si crea un igroup per il LUN.
- Prima di creare volumi in System Manager, è necessario assicurarsi di disporre di un aggregato con spazio sufficiente. Devi creare aggregati in Cloud Manager. Per ulteriori informazioni, vedere "Creazione di aggregati".

A proposito di questa attività

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

Fasi

1. "Accedere a System Manager".
2. Fare clic su **Storage > LUN**.
3. Fare clic su **Create** (Crea) e seguire le istruzioni per creare il LUN.
4. Connettersi al LUN dagli host.

   Per istruzioni, consultare "Documentazione delle utility host" per il sistema operativo in uso.

Utilizzo di FlexCache Volumes per accelerare l'accesso ai dati

Un volume FlexCache è un volume di storage che memorizza nella cache i dati di lettura NFS da un volume di origine (o di origine). Le successive letture dei dati memorizzati nella cache consentono un accesso più rapido a tali dati.

È possibile utilizzare i volumi FlexCache per accelerare l'accesso ai dati o per trasferire il traffico dai volumi ad accesso elevato. I volumi FlexCache aiutano a migliorare le performance, soprattutto quando i client devono accedere ripetutamente agli stessi dati, perché i dati possono essere gestiti direttamente senza dover accedere al volume di origine. I volumi FlexCache funzionano bene per i carichi di lavoro di sistema che richiedono un uso intensivo della lettura.

Cloud Manager non fornisce attualmente la gestione dei volumi FlexCache, ma è possibile utilizzare l'interfaccia CLI di ONTAP o Gestione di sistema di ONTAP per creare e gestire i volumi FlexCache:

- "Guida all'alimentazione di FlexCache Volumes per un accesso più rapido ai dati"
- "Creazione di volumi FlexCache in Gestore di sistema"

A partire dalla versione 3.7.2, Cloud Manager genera una licenza FlexCache per tutti i nuovi sistemi Cloud Volumes ONTAP. La licenza include un limite di utilizzo di 500 GB.

Per generare la licenza, Cloud Manager deve accedere a https://ipa-signer.cloudmanager.netapp.com. Assicurarsi che questo URL sia accessibile dal firewall.

Tiering dei dati inattivi su storage a oggetti a basso costo

È possibile ridurre i costi di storage combinando un Tier di performance SSD o HDD per i dati hot con un Tier di capacità dello storage a oggetti per i dati inattivi. Per una panoramica generale, vedere "Panoramica sul tiering dei dati".

Per impostare il tiering dei dati, è sufficiente eseguire le seguenti operazioni:

Scegliere una configurazione supportata

Sono supportate la maggior parte delle configurazioni. Se si dispone di un sistema Cloud Volumes ONTAP standard, Premium o BYOL con la versione più recente, si consiglia di procedere. "Scopri di più".

Garantire la connettività tra Cloud Volumes ONTAP e lo storage a oggetti

- Per AWS, è necessario un endpoint VPC per S3. Scopri di più.
- Per Azure, non dovrai fare nulla finché Cloud Manager dispone delle autorizzazioni necessarie. Scopri di più.
- Per GCP, è necessario aggiungere un account GCP a Cloud Manager e configurare la subnet per Private Google Access. Scopri di più.

Scegliere un criterio di tiering quando si crea, modifica o replica un volume

Cloud Manager richiede di scegliere una policy di tiering quando si crea, modifica o si replica un volume.

- "Tiering dei dati sui volumi di lettura/scrittura"
- "Tiering dei dati sui volumi di protezione dei dati"

Cosa non è richiesto per il tiering dei dati? (8217

- Non è necessario installare una licenza per le funzionalità per abilitare il tiering dei dati.
- Non è necessario creare il Tier di capacità (un bucket S3, un container Azure Blob o un bucket GCP). Cloud Manager fa tutto questo per te.

Configurazioni che supportano il tiering dei dati

È possibile abilitare il tiering dei dati quando si utilizzano configurazioni e funzionalità specifiche:

- Il tiering dei dati è supportato con Cloud Volumes ONTAP standard, Premium e BYOL, a partire dalle seguenti versioni:
  - Versione 9.2 in AWS
  - Versione 9.4 in Azure con sistemi a nodo singolo
  - Versione 9.6 in Azure con coppie ha
  - Versione 9.6 in GCP

    Il tiering dei dati non è supportato in Azure con il tipo di macchina virtuale DS3_v2.
- In AWS, il Tier di performance può essere SSD General Purpose, SSD IOPS con provisioning o HDD ottimizzati per il throughput.
- In Azure, il Tier di performance può essere costituito da dischi gestiti da SSD Premium, dischi gestiti da SSD Standard o dischi gestiti da HDD Standard.
- In GCP, il Tier di performance può essere SSD o HDD (dischi standard).
- Il tiering dei dati è supportato dalle tecnologie di crittografia.
- Il thin provisioning deve essere attivato sui volumi.

Requisiti per il tiering dei dati cold in AWS S3

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?".

Requisiti per il tiering dei dati cold nello storage Azure Blob

Non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

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

Le autorizzazioni sono incluse nella versione più recente "Policy di Cloud Manager".

Requisiti per tierare i dati cold in un bucket di storage Google Cloud

- È necessario aggiungere un account Google Cloud Platform a Cloud Manager inserendo le chiavi di accesso allo storage per un account di servizio. Le chiavi consentono a Cloud Manager di configurare un bucket di cloud storage per il tiering dei dati. Per istruzioni, vedere "Configurazione e aggiunta di account GCP a Cloud Manager".
- La subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access".

Tiering dei dati dai volumi di lettura/scrittura

Cloud Volumes ONTAP è in grado di tierare i dati inattivi su volumi di lettura/scrittura per uno storage a oggetti conveniente, liberando il Tier di performance per i dati hot.

Fasi

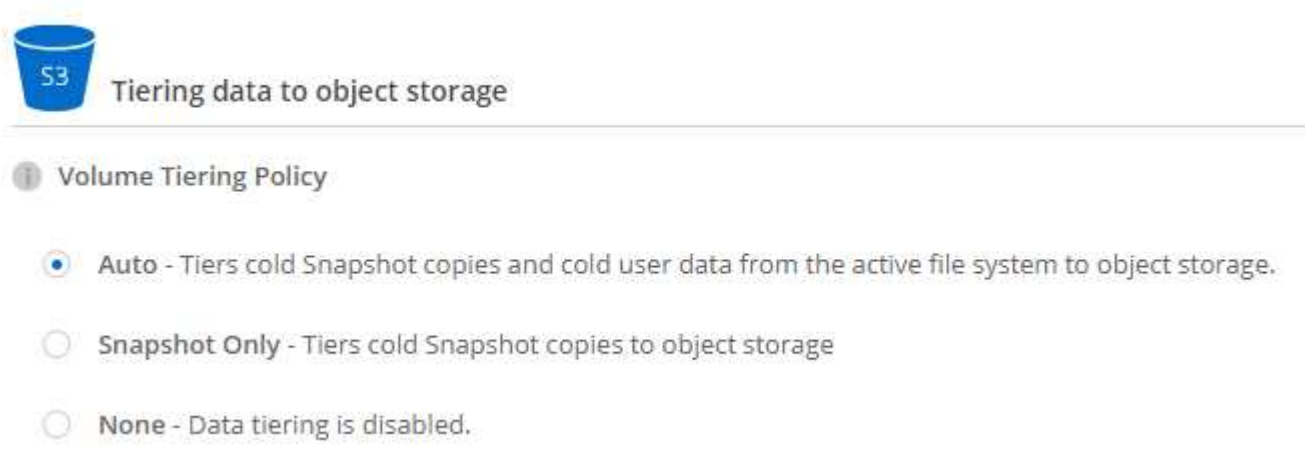
1. Nell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

Attività	Azione
Creare un nuovo volume	Fare clic su **Add New Volume** (Aggiungi nuovo volume).
Modificare un volume esistente	Selezionare il volume e fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering).

2. Selezionare la policy Snapshot Only (solo snapshot) o Auto (automatico).

   Per una descrizione di questi criteri, vedere "Panoramica sul tiering dei dati".

   Esempio



   Cloud Manager crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering

dei dati.

Se preferisci creare aggregati, puoi abilitare il tiering dei dati sugli aggregati quando li crei.

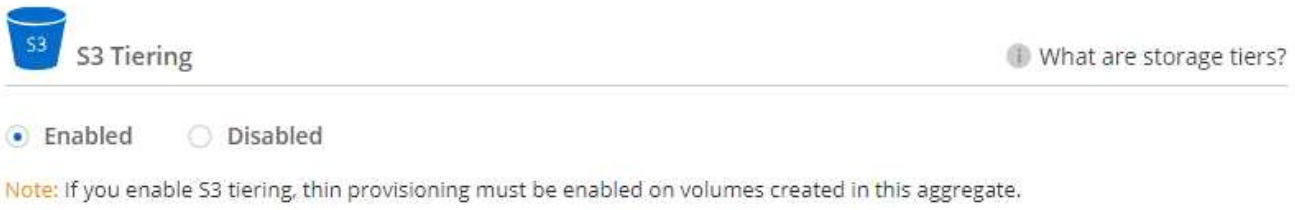
Tiering dei dati dai volumi di protezione dei dati

Cloud Volumes ONTAP può eseguire il tiering dei dati da un volume di protezione dei dati a un livello di capacità. Se si attiva il volume di destinazione, i dati si spostano gradualmente al livello di performance man mano che vengono letti.

Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume.
2. Seguire le istruzioni fino a raggiungere la pagina di tiering e abilitare il tiering dei dati allo storage a oggetti.

   Esempio



   Per assistenza nella replica dei dati, vedere "Replica dei dati da e verso il cloud".

Modifica del livello di tiering in AWS o Azure

Quando si abilita il tiering dei dati, Cloud Volumes ONTAP esegue il tiering dei dati inattivi nella classe di storage S3 *Standard* in AWS o nel Tier di storage *hot* in Azure. Dopo aver implementato Cloud Volumes ONTAP, è possibile ridurre i costi di storage modificando il livello di tiering per i dati inattivi a cui non è stato effettuato l'accesso per 30 giorni. I costi di accesso sono più elevati se si accede ai dati, quindi è necessario prendere in considerazione questo aspetto prima di modificare il livello di tiering.

Non è possibile modificare il livello di tiering in GCP perché al momento è supportata solo la classe di storage *Regional*.

A proposito di questa attività

Il livello di tiering è esteso a tutto il sistema, it non è per volume.

In AWS, è possibile modificare il livello di tiering in modo che i dati inattivi si spostino in una delle seguenti classi di storage dopo 30 giorni di inattività:

- Tiering intelligente
- Standard-infrequent Access (accesso standard-non frequente)
- Accesso non frequente a una sola zona

In Azure, è possibile modificare il livello di tiering in modo che i dati inattivi si spostino al livello di storage *COOL* dopo 30 giorni di inattività.

Per ulteriori informazioni sul funzionamento dei livelli di tiering, vedere "Panoramica sul tiering dei dati".

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **S3 Storage CLASSES** o **Blob Storage Tiering**.
2. Scegliere il livello di tiering, quindi fare clic su **Save** (Salva).

Utilizzo di ONTAP come storage persistente per Kubernetes

Cloud Manager può automatizzare l'implementazione di "Trident di NetApp" Sui cluster Kubernetes in modo da poter utilizzare ONTAP come storage persistente per i container. Funziona con cluster Cloud Volumes ONTAP e ONTAP on-premise.

Prima di completare questa procedura, è necessario "Creare un sistema Cloud Volumes ONTAP" oppure "Scopri un cluster ONTAP on-premise" Da Cloud Manager.

Se si implementano cluster Kubernetes utilizzando "Servizio NetApp Kubernetes", Cloud Manager può rilevare automaticamente i cluster dal tuo account NetApp Cloud Central. In tal caso, saltare i primi due passaggi e iniziare con il passaggio 3.

Verificare la connettività di rete

1. Deve essere disponibile una connessione di rete tra Cloud Manager e i cluster Kubernetes, dai cluster Kubernetes ai sistemi ONTAP.
2. Cloud Manager richiede una connessione Internet in uscita per accedere ai seguenti endpoint durante l'installazione di Trident:

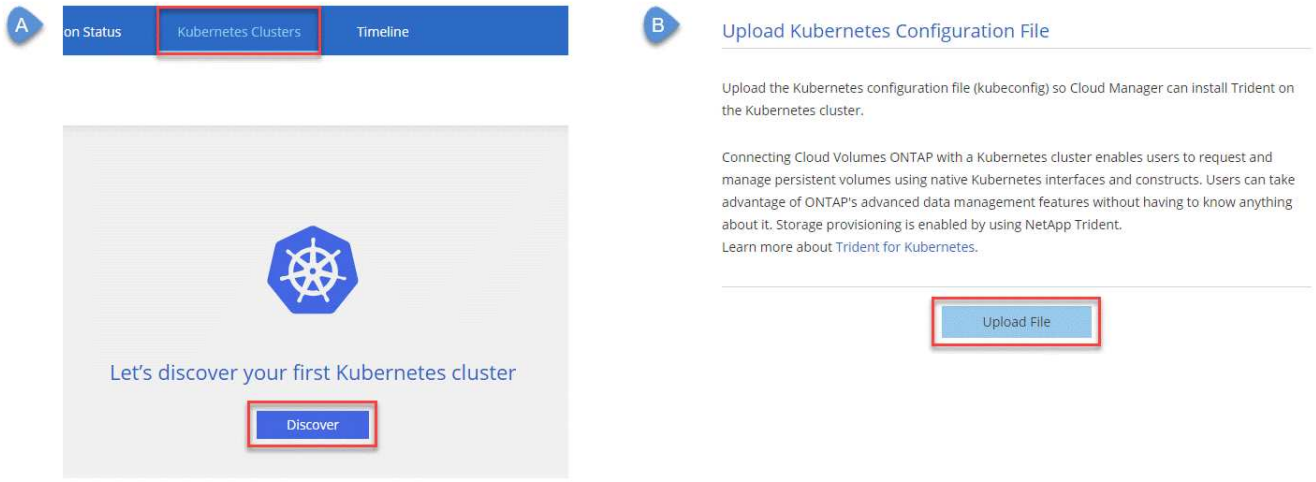
   https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

   Cloud Manager installa Trident su un cluster Kubernetes quando si connette un ambiente di lavoro al cluster.

Caricare i file di configurazione di Kubernetes in Cloud Manager

Per ogni cluster Kubernetes, l'account Admin deve caricare un file di configurazione (kubeconfig) in formato YAML. Dopo aver caricato il file, Cloud Manager verifica la connettività al cluster e salva una copia crittografata del file kubeconfig.

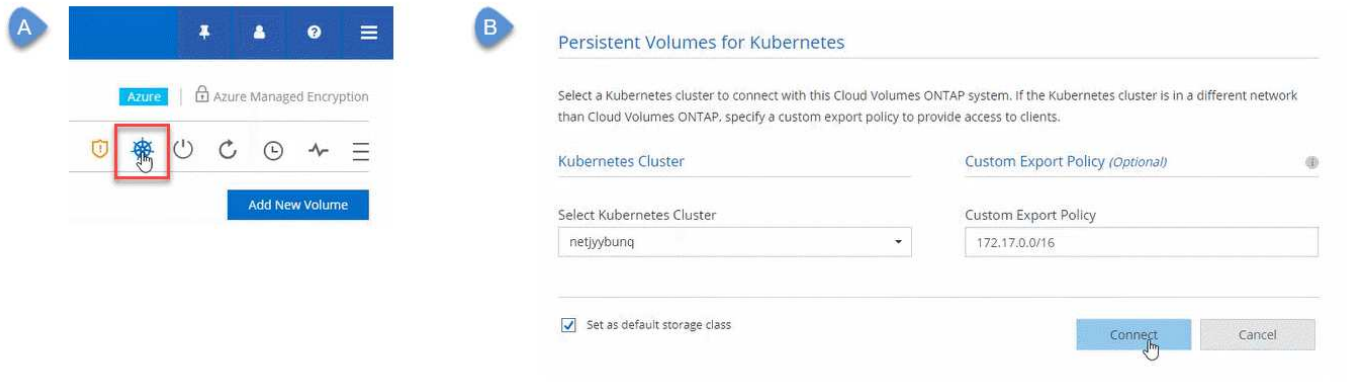
Fare clic su **Kubernetes Clusters > Discover > Upload file** e selezionare il file kubeconfig.



3 Connetti i tuoi ambienti di lavoro ai cluster Kubernetes

Dall'ambiente di lavoro, fare clic sull'icona Kubernetes e seguire le istruzioni. È possibile collegare diversi cluster a diversi sistemi ONTAP e più cluster allo stesso sistema ONTAP.

È possibile impostare la classe di storage NetApp come classe di storage predefinita per il cluster Kubernetes. Quando un utente crea un volume persistente, il cluster Kubernetes può utilizzare i sistemi ONTAP connessi come storage back-end per impostazione predefinita.



4 Avviare il provisioning dei volumi persistenti

Richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi. Cloud Manager crea quattro classi di storage Kubernetes che è possibile utilizzare per il provisioning di volumi persistenti:

- **netapp-file**: Per il binding di volumi persistenti a sistemi ONTAP a nodo singolo
- **netapp-file-san**: Per il binding di volumi persistenti iSCSI a sistemi ONTAP a nodo singolo
- **netapp-file-Redundant**: Per il binding di volumi persistenti a coppie ONTAP ha
- **netapp-file-ridondanti-san**: Per il binding di volumi persistenti iSCSI a coppie ONTAP ha

Cloud Manager configura Trident in modo che utilizzi le seguenti opzioni di provisioning per impostazione predefinita:

- Volumi sottili
- Il criterio Snapshot predefinito
- Directory Snapshot accessibile

"Scopri di più sul provisioning del tuo primo volume con Trident for Kubernetes"

Quali sono i volumi Trident_Trident?

Cloud Manager crea un volume sul primo sistema ONTAP a cui ci si connette a un cluster Kubernetes. Il nome del volume viene aggiunto con "_Trident_Trident". ONTAP utilizza questo volume per connettersi al cluster Kubernetes. Non eliminare questi volumi.

Cosa accade quando si disconnette o rimuove un cluster Kubernetes?

Cloud Manager consente di scollegare singoli sistemi ONTAP da un cluster Kubernetes. Quando si disconnette un sistema, non è più possibile utilizzarlo ONTAP come storage persistente per i container. I volumi persistenti esistenti non vengono cancellati.

Dopo aver scollegato tutti i sistemi da un cluster Kubernetes, è possibile rimuovere l'intera configurazione di Kubernetes da Cloud Manager. Cloud Manager non disinstalla Trident quando si rimuove il cluster e non elimina alcun volume persistente.

Entrambe queste azioni sono disponibili solo tramite API. Prevediamo di aggiungere le azioni all'interfaccia in una release futura."Fare clic qui per ulteriori informazioni sulle API".

Crittografia dei volumi con NetApp Volume Encryption

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. I dati, le copie Snapshot e i metadati sono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume.

A proposito di questa attività

- A partire da Cloud Manager 3.7.1, una licenza per la crittografia dei volumi NetApp viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp.
  - "Aggiunta di account NetApp Support Site a Cloud Manager"
  - "Registrazione di sistemi pay-as-you-go"

  Cloud Manager non installa la licenza NVE sui sistemi che risiedono nell'area geografica Cina.

- Attualmente, Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp con un server di gestione delle chiavi esterno. Onboard Key Manager non è supportato.
- È necessario configurare la crittografia dei volumi NetApp dall'interfaccia CLI di ONTAP.

  È quindi possibile utilizzare CLI o System Manager per attivare la crittografia su volumi specifici. Cloud Manager non supporta NetApp Volume Encryption dalla sua interfaccia utente e dalle sue API.

"Scopri di più sulle tecnologie di crittografia supportate".

Fasi

1. Esaminare l'elenco dei Key Manager supportati in "Tool di matrice di interoperabilità NetApp".

   Cercare la soluzione **Key Manager**.

2. "Connettersi all'interfaccia utente di Cloud Volumes ONTAP".
3. Installare i certificati SSL e connettersi ai server di gestione delle chiavi esterni.

   "ONTAP 9 Guida all'alimentazione per la crittografia NetApp: Configurazione della gestione esterna delle chiavi"

4. Creare un nuovo volume crittografato o convertire un volume non crittografato esistente utilizzando CLI o System Manager.
   - CLI:
     - Per i nuovi volumi, utilizzare il comando **volume create** con il parametro -Encrypt.

       "ONTAP 9 Guida all'alimentazione per la crittografia NetApp: Attivazione della crittografia su un nuovo volume"

     - Per i volumi esistenti, utilizzare il comando **volume Encryption conversion start**.

       "ONTAP 9 Guida all'alimentazione per la crittografia NetApp: Attivazione della crittografia su un volume esistente con il comando di avvio della conversione della crittografia del volume"

   - Gestore di sistema:
     - Per i nuovi volumi, fare clic su **Storage > Volumes > Create > Create FlexVol** (archiviazione > volumi > Crea volume > Crea volume), quindi selezionare **Encrypted** (crittografato).

       "Gestione dei cluster di ONTAP 9 con Gestione di sistema: Creazione di volumi FlexVol"

     - Per i volumi esistenti, selezionare il volume, fare clic su **Edit**, quindi selezionare **Encrypted**.

       "Gestione dei cluster di ONTAP 9 con Gestione di sistema: Modifica delle proprietà dei volumi"

Gestione dello storage esistente

Cloud Manager consente di gestire volumi, aggregati e server CIFS. Inoltre, richiede di spostare i volumi per evitare problemi di capacità.

Gestione dei volumi esistenti

Puoi gestire i volumi esistenti in base alle tue esigenze di storage. È possibile visualizzare, modificare, clonare, ripristinare ed eliminare i volumi.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire i volumi.
2. Gestisci i tuoi volumi:

Attività	Azione
Consente di visualizzare informazioni su un volume	Selezionare un volume, quindi fare clic su **Info**.
Modifica di un volume (solo volumi di lettura/scrittura)	a. Selezionare un volume, quindi fare clic su **Modifica**. b. Modificare la policy Snapshot del volume, l'elenco di controllo dell'accesso NFS o le autorizzazioni di condivisione, quindi fare clic su **Update** (Aggiorna). Se sono necessarie policy Snapshot personalizzate, è possibile crearle utilizzando System Manager.
Clonare un volume	a. Selezionare un volume, quindi fare clic su **Clone**. b. Modificare il nome del clone secondo necessità, quindi fare clic su **Clone**. Questo processo crea un volume FlexClone. Un volume FlexClone è una copia point-in-time scrivibile efficiente in termini di spazio, in quanto utilizza una piccola quantità di spazio per i metadati e consuma solo spazio aggiuntivo quando i dati vengono modificati o aggiunti. Per ulteriori informazioni sui volumi FlexClone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
Ripristinare i dati da una copia Snapshot a un nuovo volume	a. Selezionare un volume, quindi fare clic su **Restore from Snapshot copy** (Ripristina da copia Snapshot). b. Selezionare una copia Snapshot, immettere un nome per il nuovo volume, quindi fare clic su **Restore** (Ripristina).
Crea una copia Snapshot on-demand	a. Selezionare un volume, quindi fare clic su **Crea una copia Snapshot**. b. Modificare il nome, se necessario, quindi fare clic su **Crea**.
Scarica il comando NFS mount	a. Selezionare un volume, quindi fare clic su **comando di montaggio**. b. Fare clic su **Copy** (Copia).
Modificare il tipo di disco sottostante	a. Selezionare un volume, quindi fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering). b. Selezionare il tipo di disco, quindi fare clic su **Cambia**. Cloud Manager sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato oppure crea un nuovo aggregato per il volume.

Attività	Azione
Modificare la policy di tiering	a. Selezionare un volume, quindi fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering). b. Fare clic su **Edit Policy** (Modifica policy). c. Selezionare un altro criterio e fare clic su **Cambia**. Cloud Manager sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato con il tiering oppure crea un nuovo aggregato per il volume.
Attivare o disattivare la sincronizzazione con S3 per un volume	Selezionare un volume e fare clic su **Sync to S3** o **Delete Sync Relationship**. Prima di poter utilizzare queste opzioni, è necessario attivare la funzione di sincronizzazione con S3. Per istruzioni, vedere "Sincronizzazione dei dati con AWS S3"
Eliminare un volume	a. Selezionare un volume, quindi fare clic su **Delete** (Elimina). b. Fare nuovamente clic su **Delete** per confermare.

Gestione degli aggregati esistenti

Gestisci gli aggregati aggiungendo dischi, visualizzando informazioni sugli aggregati ed eliminandoli.

Prima di iniziare

Se si desidera eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

A proposito di questa attività

Se un aggregato sta esaurendo lo spazio, è possibile spostare i volumi in un altro aggregato utilizzando Gestione di sistema di OnCommand.

Fasi

1. Nella pagina Working Environments (ambienti di lavoro), fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Gestisci i tuoi aggregati:

Attività	Azione
Visualizzare informazioni su un aggregato	Selezionare un aggregato e fare clic su **Info**.
Creare un volume su un aggregato specifico	Selezionare un aggregato e fare clic su **Create volume** (Crea volume).

Attività	Azione
Aggiungere dischi a un aggregato	a. Selezionare un aggregato e fare clic su **Aggiungi dischi AWS** o **Aggiungi dischi Azure**. b. Selezionare il numero di dischi che si desidera aggiungere e fare clic su **Aggiungi**. Tutti i dischi di un aggregato devono avere le stesse dimensioni.
Eliminare un aggregato	a. Selezionare un aggregato che non contiene volumi e fare clic su **Delete** (Elimina). b. Fare nuovamente clic su **Delete** per confermare.

Modifica del server CIFS

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server CIFS in Cloud Volumes ONTAP in modo che possa continuare a fornire storage ai client.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > CIFS setup**.
2. Specificare le impostazioni per il server CIFS:

Attività	Azione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.

Attività	Azione
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

3. Fare clic su **Save** (Salva).

Risultato

Cloud Volumes ONTAP aggiorna il server CIFS con le modifiche.

Spostamento di un volume per evitare problemi di capacità

Cloud Manager potrebbe visualizzare un messaggio Action Required (azione richiesta) che indica che lo spostamento di un volume è necessario per evitare problemi di capacità, ma che non può fornire consigli per correggere il problema. In questo caso, è necessario identificare come correggere il problema e spostare uno o più volumi.

Fasi

1. Identificare come risolvere il problema.
2. In base alla tua analisi, sposta i volumi per evitare problemi di capacità:
   - Spostare i volumi in un altro sistema.
   - Spostare i volumi in un altro aggregato sullo stesso sistema.

Identificare come correggere i problemi di capacità

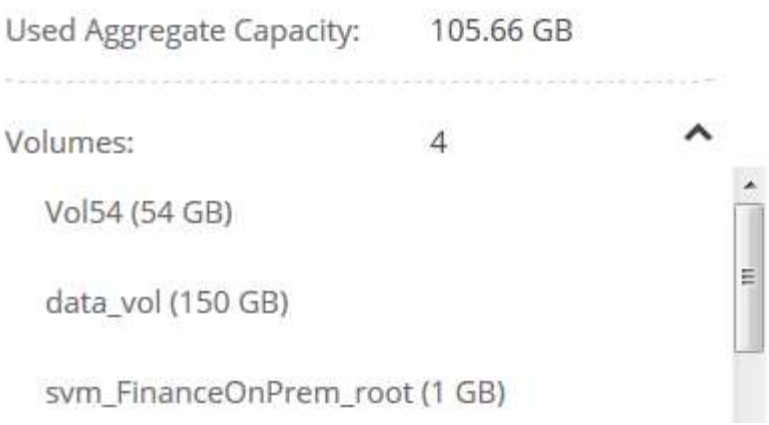
Se Cloud Manager non è in grado di fornire consigli per lo spostamento di un volume per evitare problemi di capacità, è necessario identificare i volumi da spostare e se è necessario spostarli in un altro aggregato sullo stesso sistema o in un altro sistema.

Fasi

1. Visualizzare le informazioni avanzate nel messaggio Action Required (azione richiesta) per identificare l'aggregato che ha raggiunto il limite di capacità.

   Ad esempio, le informazioni avanzate dovrebbero dire qualcosa di simile a quanto segue: L'aggregato aggr1 ha raggiunto il suo limite di capacità.

2. Identificare uno o più volumi da spostare fuori dall'aggregato:
   a. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
   b. Selezionare l'aggregato, quindi fare clic su **Info**.
   c. Espandere l'elenco dei volumi.



d. Esaminare le dimensioni di ciascun volume e scegliere uno o più volumi da spostare fuori dall'aggregato.

   È necessario scegliere volumi sufficientemente grandi da liberare spazio nell'aggregato in modo da evitare ulteriori problemi di capacità in futuro.

3. Se il sistema non ha raggiunto il limite di dischi, spostare i volumi in un aggregato esistente o in un nuovo aggregato sullo stesso sistema.

   Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro aggregato per evitare problemi di capacità".

4. Se il sistema ha raggiunto il limite di dischi, eseguire una delle seguenti operazioni:
   a. Eliminare eventuali volumi inutilizzati.
   b. Riorganizzare i volumi per liberare spazio su un aggregato.

      Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro aggregato per evitare problemi di capacità".

   c. Spostare due o più volumi in un altro sistema con spazio.

      Per ulteriori informazioni, vedere "Spostamento dei volumi in un altro sistema per evitare problemi di capacità".

Spostamento dei volumi in un altro sistema per evitare problemi di capacità

È possibile spostare uno o più volumi in un altro sistema Cloud Volumes ONTAP per evitare problemi di capacità. Potrebbe essere necessario eseguire questa operazione se il sistema ha raggiunto il limite di dischi.

A proposito di questa attività

È possibile seguire la procedura descritta in questa attività per correggere il seguente messaggio Action Required (azione richiesta):

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Fasi
. Identificare un sistema Cloud Volumes ONTAP con capacità disponibile o
implementare un nuovo sistema.
. Trascinare e rilasciare l'ambiente di lavoro di origine nell'ambiente di
lavoro di destinazione per eseguire una replica dei dati del volume una
tantum.
```

+
Per ulteriori informazioni, vedere "Replica dei dati tra sistemi".

1. Accedere alla pagina Replication Status (Stato replica), quindi interrompere la relazione SnapMirror per convertire il volume replicato da un volume di protezione dati a un volume di lettura/scrittura.

   Per ulteriori informazioni, vedere "Gestione delle pianificazioni e delle relazioni di replica dei dati".

2. Configurare il volume per l'accesso ai dati.

   Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati, consultare "Guida rapida per il disaster recovery dei volumi di ONTAP 9".

3. Eliminare il volume originale.

   Per ulteriori informazioni, vedere "Gestione dei volumi esistenti".

Spostamento dei volumi in un altro aggregato per evitare problemi di capacità

È possibile spostare uno o più volumi in un altro aggregato per evitare problemi di capacità.

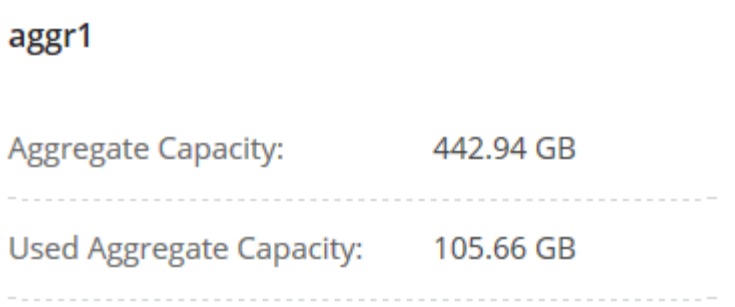
A proposito di questa attività

È possibile seguire la procedura descritta in questa attività per correggere il seguente messaggio Action Required (azione richiesta):

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Fasi
. Verificare se un aggregato esistente dispone di capacità disponibile per
i volumi da spostare:
```

+
.. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
.. Selezionare ciascun aggregato, fare clic su **Info**, quindi visualizzare la capacità disponibile (capacità aggregata meno capacità aggregata utilizzata).

+



1. Se necessario, aggiungere dischi a un aggregato esistente:
   a. Selezionare l'aggregato, quindi fare clic su **Aggiungi dischi**.
   b. Selezionare il numero di dischi da aggiungere, quindi fare clic su **Aggiungi**.
2. Se nessun aggregato dispone di capacità, creare un nuovo aggregato.

   Per ulteriori informazioni, vedere "Creazione di aggregati".
3. Utilizzare System Manager o CLI per spostare i volumi nell'aggregato.
4. Nella maggior parte dei casi, è possibile utilizzare System Manager per spostare i volumi.

   Per istruzioni, consultare "Guida rapida per lo spostamento del volume di ONTAP 9".

Replica e protezione dei dati

Rilevamento e gestione dei cluster ONTAP

Cloud Manager è in grado di rilevare i cluster ONTAP nel tuo ambiente on-premise, in una configurazione di storage privato NetApp e nel cloud IBM. La scoperta di questi cluster ti consente di replicare facilmente i dati nel tuo ambiente di cloud ibrido direttamente da Cloud Manager.

Alla scoperta dei cluster ONTAP

Il rilevamento di un cluster ONTAP in Cloud Manager ti consente di eseguire il provisioning dello storage e di replicare i dati nel cloud ibrido.

Prima di iniziare

Per aggiungere il cluster a Cloud Manager, è necessario disporre dell'indirizzo IP di gestione del cluster e della password dell'account utente admin.

Cloud Manager rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:

- L'host Cloud Manager deve consentire l'accesso HTTPS in uscita attraverso la porta 443.

  Se Cloud Manager si trova in AWS, tutte le comunicazioni in uscita sono consentite dal gruppo di sicurezza predefinito.

- Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443.

  Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questa policy predefinita è stata modificata o se è stata creata una policy firewall personalizzata, è necessario associare il protocollo HTTPS a tale policy e abilitare l'accesso dall'host Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Discover** e selezionare **cluster ONTAP**.
2. Nella pagina **Dettagli cluster ONTAP**, inserire l'indirizzo IP di gestione del cluster, la password per l'account utente admin e la posizione del cluster.

3. Nella pagina Dettagli, immettere un nome e una descrizione per l'ambiente di lavoro, quindi fare clic su **Go**.

Risultato

Cloud Manager rileva il cluster. È ora possibile creare volumi, replicare i dati da e verso il cluster e avviare Gestione di sistema di OnCommand per eseguire attività avanzate.

Provisioning di volumi su cluster ONTAP

Cloud Manager consente di eseguire il provisioning di volumi NFS e CIFS su cluster ONTAP.

Prima di iniziare

NFS o CIFS devono essere impostati sul cluster. È possibile configurare NFS e CIFS utilizzando System Manager o CLI.

A proposito di questa attività

È possibile creare volumi su aggregati esistenti. Non è possibile creare nuovi aggregati da Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome del cluster ONTAP su cui si desidera eseguire il provisioning dei volumi.
2. Fare clic su **Add New Volume** (Aggiungi nuovo volume).
3. Nella pagina Create New Volume (Crea nuovo volume), inserire i dettagli del volume, quindi fare clic su **Create** (Crea).

   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, Cloud Manager inserisce un valore che fornisce l'accesso a tutte le istanze nella subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Profilo di utilizzo	I profili di utilizzo definiscono le funzionalità di efficienza dello storage NetApp abilitate per un volume.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.

Replica dei dati tra sistemi

È possibile replicare i dati tra ambienti di lavoro scegliendo una replica dei dati una tantum per il trasferimento dei dati o una pianificazione ricorrente per il disaster recovery o la conservazione a lungo termine. Ad esempio, è possibile configurare la replica dei dati da un sistema ONTAP on-premise a Cloud Volumes ONTAP per il disaster recovery.

Cloud Manager semplifica la replica dei dati tra volumi su sistemi separati utilizzando le tecnologie SnapMirror e SnapVault. È sufficiente identificare il volume di origine e il volume di destinazione, quindi scegliere una policy e una pianificazione di replica. Cloud Manager acquista i dischi richiesti, configura le relazioni, applica la policy di replica e avvia il trasferimento di riferimento tra i volumi.

Il trasferimento di riferimento include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di origine.

Requisiti di replica dei dati

Prima di poter replicare i dati, è necessario verificare che i requisiti specifici siano soddisfatti sia per i sistemi Cloud Volumes ONTAP che per i cluster ONTAP.

Requisiti di versione

Prima di eseguire la replica dei dati, verificare che i volumi di origine e di destinazione eseguano versioni ONTAP compatibili. Per ulteriori informazioni, vedere "Guida all'alimentazione per la protezione dei dati".

Requisiti specifici di Cloud Volumes ONTAP

- Il gruppo di protezione dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 10000, 11104 e 11105.

  Queste regole sono incluse nel gruppo di protezione predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).
- Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e un sistema in Azure, è necessario disporre di una connessione VPN tra AWS VPC e Azure VNET.

Requisiti specifici dei cluster ONTAP

- È necessario installare una licenza SnapMirror attiva.
- Se il cluster si trova all'interno della propria sede, si dovrebbe disporre di una connessione dalla rete aziendale ad AWS o Azure, che in genere è una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Per ulteriori informazioni, consultare la Guida rapida di peering di cluster e SVM per la versione di ONTAP in uso.

Configurazione della replica dei dati tra sistemi

Puoi replicare i dati tra sistemi Cloud Volumes ONTAP e cluster ONTAP scegliendo una replica dei dati una tantum, che può aiutarti a spostare i dati da e verso il cloud, o una pianificazione ricorrente, che può aiutarti con il disaster recovery o la conservazione a lungo termine.

A proposito di questa attività

Cloud Manager supporta configurazioni di protezione dei dati semplici, fanout e a cascata:

- In una configurazione semplice, la replica avviene dal volume A al volume B.
- In una configurazione fanout, la replica avviene dal volume A a più destinazioni.
- In una configurazione a cascata, la replica avviene dal volume A al volume B e dal volume B al volume C.

È possibile configurare configurazioni fanout e a cascata in Cloud Manager impostando più repliche di dati tra sistemi. Ad esempio, replicando un volume dal sistema A al sistema B e replicando lo stesso volume dal sistema B al sistema C.

Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume:

2. Se vengono visualizzate le pagine Source (origine) e Destination peering Setup (Configurazione peering destinazione), selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.

   La rete intercluster deve essere configurata in modo che i peer del cluster dispongano di una *connettività full-mesh a coppie*, il che significa che ogni coppia di cluster in una relazione peer del cluster dispone di connettività tra tutte le proprie LIF intercluster.

   Queste pagine vengono visualizzate se l'origine o la destinazione è un cluster ONTAP con più LIF.

3. Nella pagina Source Volume Selection (selezione volume di origine), selezionare il volume che si desidera replicare.
4. Nella pagina Destination Volume Name and Tiering (Nome volume di destinazione e tiering), specificare il nome del volume di destinazione, scegliere un tipo di disco sottostante, modificare una delle opzioni avanzate e fare clic su **Continue** (continua).

   Se la destinazione è un cluster ONTAP, è necessario specificare anche la SVM di destinazione e l'aggregato.

5. Nella pagina velocità di trasferimento massima, specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.
6. Nella pagina Replication Policy (Criteri di replica), scegliere uno dei criteri predefiniti o fare clic su **Additional Policies** (Criteri aggiuntivi), quindi selezionare uno dei criteri avanzati.

   Per ulteriori informazioni, vedere "Scelta di un criterio di replica".

   Se si sceglie un criterio di backup personalizzato (SnapVault), le etichette associate al criterio devono corrispondere alle etichette delle copie Snapshot sul volume di origine. Per ulteriori informazioni, vedere "Come funzionano le policy di backup".

7. Nella pagina Pianificazione, scegliere una copia singola o una pianificazione ricorrente.

   Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione nel cluster *destination* utilizzando System Manager.

8. Nella pagina Review (esamina), rivedere le selezioni, quindi fare clic su **Go** (Vai).

Risultato

Cloud Manager avvia il processo di replica dei dati. È possibile visualizzare i dettagli relativi alla replica nella pagina Replication Status (Stato replica).

Gestione delle pianificazioni e delle relazioni di replica dei dati

Dopo aver configurato la replica dei dati tra due sistemi, è possibile gestire la pianificazione e la relazione della replica dei dati da Cloud Manager.

Fasi

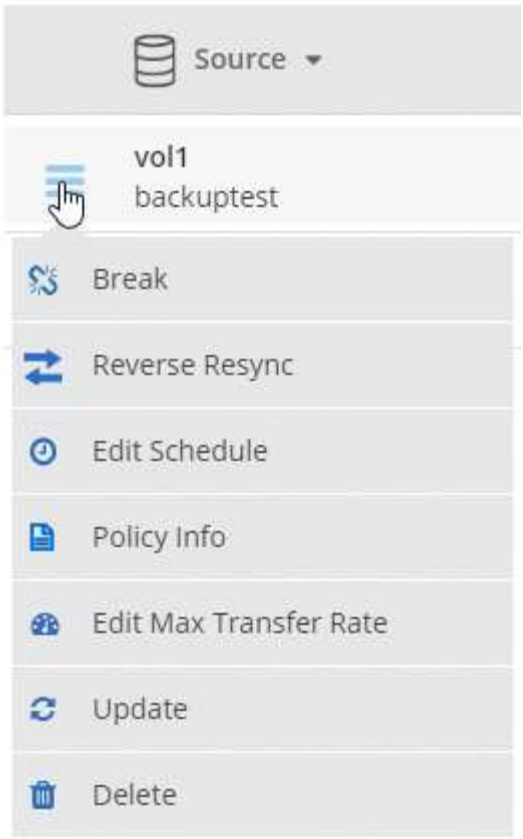
1. Nella pagina ambienti di lavoro, visualizzare lo stato della replica per tutti gli ambienti di lavoro nell'area di lavoro o per un ambiente di lavoro specifico:

Opzione	Azione
Tutti gli ambienti di lavoro nello spazio di lavoro	Nella parte superiore di Cloud Manager, fare clic su **Replication Status** (Stato replica).
Un ambiente di lavoro specifico	Aprire l'ambiente di lavoro e fare clic su **Replications** (repliche).

2. Esaminare lo stato delle relazioni di replica dei dati per verificare che siano integre.

   Se lo stato di una relazione è inattivo e lo stato di mirroring non è inizializzato, è necessario inizializzare la relazione dal sistema di destinazione per eseguire la replica dei dati in base alla pianificazione definita. È possibile inizializzare la relazione utilizzando System Manager o l'interfaccia della riga di comando (CLI). Questi stati possono essere visualizzati quando il sistema di destinazione non funziona e poi torna in linea.

3. Selezionare l'icona del menu accanto al volume di origine, quindi scegliere una delle azioni disponibili.



La seguente tabella descrive le azioni disponibili:

Azione	Descrizione
Rompere	Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati. Questa opzione viene generalmente utilizzata quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline. Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati e la riattivazione di un volume di origine, consultare la Guida rapida al disaster recovery di ONTAP 9.
Risincronizzare	Consente di ripristinare una relazione interrotta tra i volumi e di riprendere la replica dei dati in base alla pianificazione definita. Quando si risincronizzano i volumi, i contenuti del volume di destinazione vengono sovrascritti dai contenuti del volume di origine. Per eseguire una risincronizzazione inversa, che risincronizza i dati dal volume di destinazione al volume di origine, vedere la "Guida rapida per il disaster recovery dei volumi di ONTAP 9".
Risincronizzazione inversa	Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine originale viene sovrascritto dal contenuto del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline. Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.

Azione	Descrizione
Modifica pianificazione	Consente di scegliere una pianificazione diversa per la replica dei dati.
Info policy	Mostra il criterio di protezione assegnato alla relazione di replica dei dati.
Modifica velocità di trasferimento massima	Consente di modificare la velocità massima (in kilobyte al secondo) alla quale è possibile trasferire i dati.
Aggiornare	Avvia un trasferimento incrementale per aggiornare il volume di destinazione.
Eliminare	Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati. Questa azione elimina anche la relazione peer del cluster e la relazione peer SVM (Storage Virtual Machine), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, Cloud Manager aggiorna la relazione o la pianificazione.

Scelta di un criterio di replica

Quando si imposta la replica dei dati in Cloud Manager, potrebbe essere necessario un aiuto nella scelta di una policy di replica. Un criterio di replica definisce il modo in cui il sistema storage replica i dati da un volume di origine a un volume di destinazione.

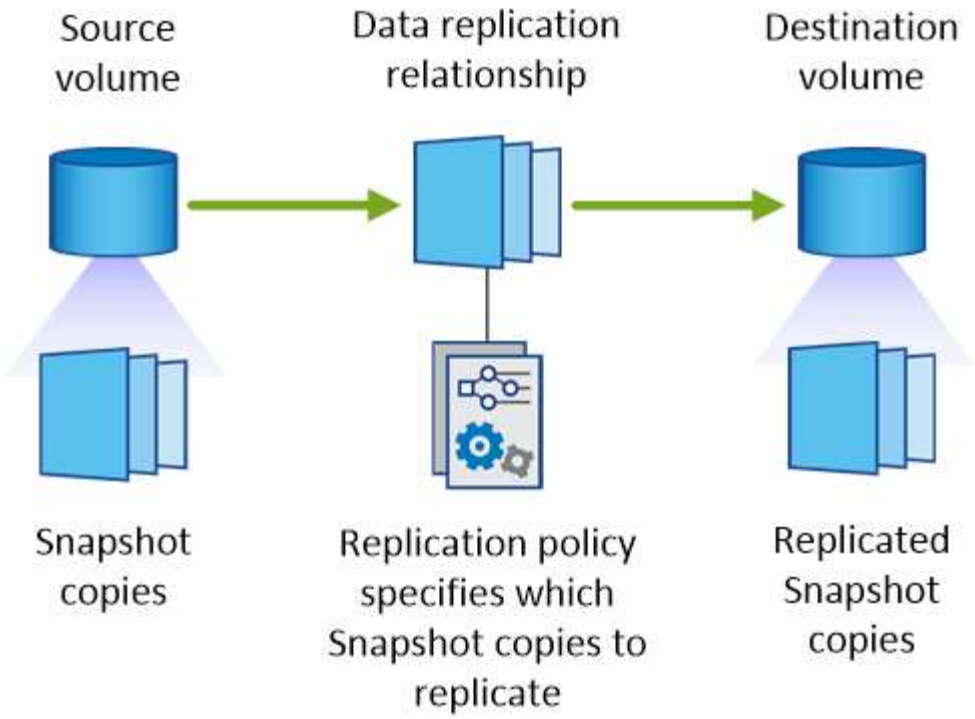
Quali sono le funzioni delle policy di replica

Il sistema operativo ONTAP crea automaticamente i backup denominati copie Snapshot. Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato del file system in un momento specifico.

Quando si replicano i dati tra sistemi, si replicano le copie Snapshot da un volume di origine a un volume di destinazione. Un criterio di replica specifica quali copie Snapshot replicare dal volume di origine al volume di destinazione.

Le policy di replica sono anche denominate policy di *protezione*, in quanto sono basate sulle tecnologie SnapMirror e SnapVault, che forniscono protezione dal disaster recovery e backup e ripristino disk-to-disk.

La seguente immagine mostra la relazione tra le copie Snapshot e i criteri di replica:



Tipi di policy di replica

Esistono tre tipi di policy di replica:

- Un criterio *Mirror* replica le nuove copie Snapshot create in un volume di destinazione.

  È possibile utilizzare queste copie Snapshot per proteggere il volume di origine in preparazione al disaster recovery o alla replica dei dati una tantum. È possibile attivare il volume di destinazione per l'accesso ai dati in qualsiasi momento.

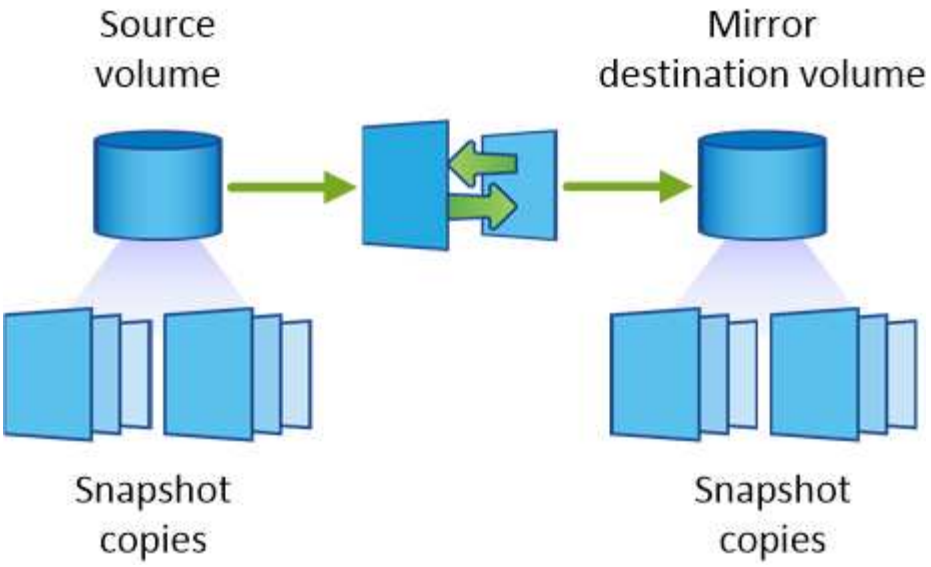
- Un criterio *Backup* replica copie Snapshot specifiche in un volume di destinazione e le conserva per un periodo di tempo più lungo rispetto al volume di origine.

  È possibile ripristinare i dati da queste copie Snapshot quando i dati vengono danneggiati o persi e conservarli per la conformità agli standard e altri scopi correlati alla governance.

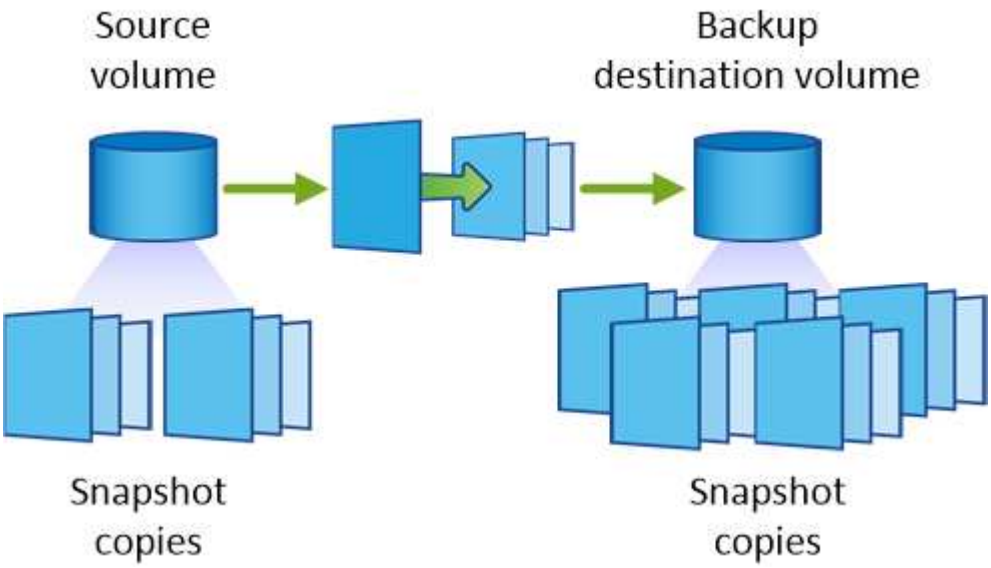
- Una policy di *Mirror e Backup* fornisce sia il disaster recovery che la conservazione a lungo termine.

  Ogni sistema include una policy di backup e mirroring predefinita, che funziona bene per molte situazioni. Se hai bisogno di policy personalizzate, puoi crearle usando System Manager.

Le seguenti immagini mostrano la differenza tra i criteri Mirror e Backup. Un criterio Mirror esegue il mirroring delle copie Snapshot disponibili sul volume di origine.



Una policy di backup conserva in genere le copie Snapshot più a lungo di quanto non vengano conservate nel volume di origine:



Come funzionano le policy di backup

A differenza dei criteri di mirroring, i criteri di backup (SnapVault) replicano copie Snapshot specifiche in un volume di destinazione. È importante comprendere il funzionamento dei criteri di backup se si desidera utilizzare i propri criteri invece dei criteri predefiniti.

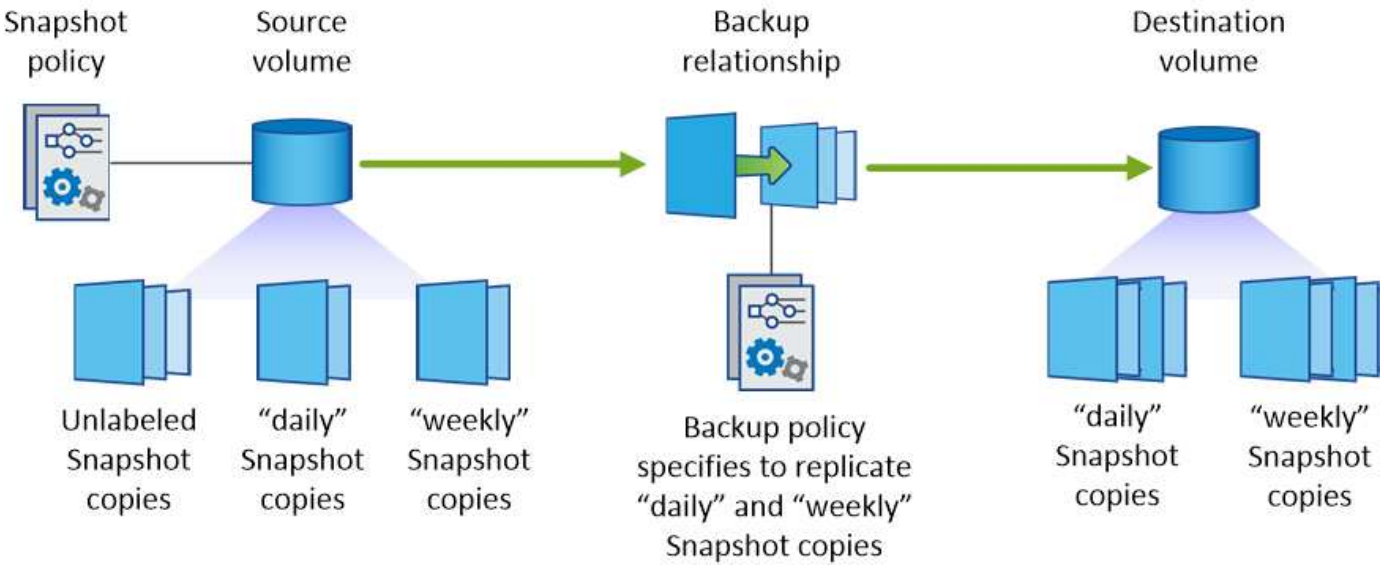
Comprensione della relazione tra le etichette delle copie Snapshot e le policy di backup

Una policy Snapshot definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare e come etichettarle. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti ed etichettarle "ogni giorno".

Un criterio di backup include regole che specificano le copie Snapshot etichettate da replicare in un volume di destinazione e il numero di copie da conservare. Le etichette definite in un criterio di backup devono corrispondere a una o più etichette definite in un criterio Snapshot. In caso contrario, il sistema non può

replicare alcuna copia Snapshot.

Ad esempio, una policy di backup che include le etichette "giornaliere" e "settimanali" produce la replica delle copie Snapshot che includono solo quelle etichette. Non vengono replicate altre copie Snapshot, come mostrato nell'immagine seguente:



Policy predefinite e policy personalizzate

La policy Snapshot predefinita crea copie Snapshot orarie, giornaliere e settimanali, conservando sei copie Snapshot orarie, due giornaliere e due copie Snapshot settimanali.

È possibile utilizzare facilmente un criterio di backup predefinito con il criterio Snapshot predefinito. Le policy di backup predefinite replicano copie Snapshot giornaliere e settimanali, conservando sette copie Snapshot giornaliere e 52 copie Snapshot settimanali.

Se si creano criteri personalizzati, le etichette definite da tali criteri devono corrispondere. È possibile creare policy personalizzate utilizzando System Manager.

Backup dei dati su Amazon S3

Backup su S3 è una funzionalità add-on per Cloud Volumes ONTAP che offre funzionalità di backup e ripristino completamente gestite per la protezione e l'archiviazione a lungo termine dei dati cloud. I backup vengono memorizzati nello storage a oggetti S3, indipendentemente dalle copie Snapshot del volume utilizzate per il ripristino o il cloning a breve termine.

Quando si attiva Backup in S3, il servizio esegue un backup completo dei dati. Tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e nuovi.

"Visita NetApp Cloud Central per i dettagli sui prezzi".

Si noti che è necessario utilizzare Cloud Manager per tutte le operazioni di backup e ripristino. Qualsiasi azione intrapresa direttamente da ONTAP o da Amazon S3 comporta una configurazione non supportata.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare il supporto per la configurazione

Verificare quanto segue:

- Cloud Volumes ONTAP 9.4 o versione successiva viene eseguito in una regione AWS supportata: N. Virginia, Oregon, Irlanda, Francoforte o Sydney
- Sei iscritto al nuovo "Offerta Cloud Manager Marketplace"
- La porta TCP 5010 è aperta per il traffico in uscita nel gruppo di sicurezza per Cloud Volumes ONTAP (è aperta per impostazione predefinita)
- La porta TCP 8088 è aperta per il traffico in uscita nel gruppo di sicurezza per Cloud Manager (è aperta per impostazione predefinita)
- Il seguente endpoint è accessibile da Cloud Manager:

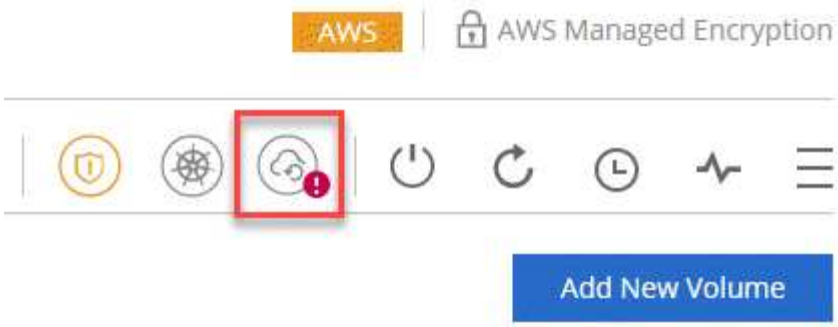
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Cloud Manager può allocare fino a due endpoint VPC di interfaccia nel VPC (il limite AWS per VPC è 20)
- Cloud Manager dispone dell'autorizzazione per utilizzare le autorizzazioni endpoint VPC elencate nella più recente "Policy di Cloud Manager":

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

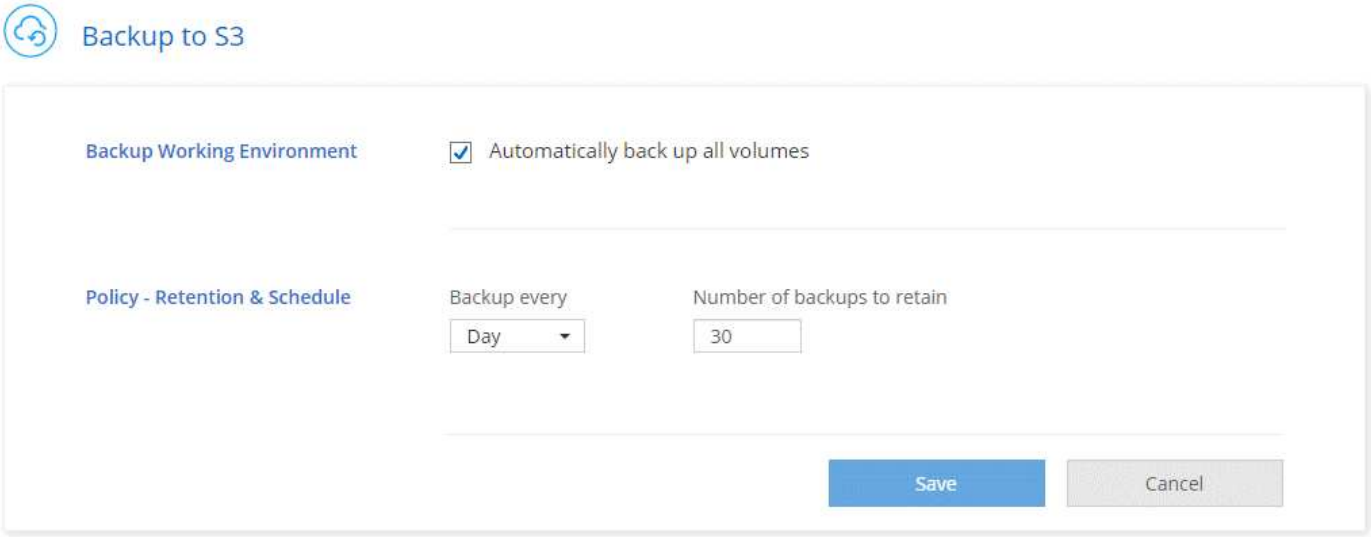
Abilitare Backup su S3 sul sistema nuovo o esistente

- Nuovi sistemi: La funzione Backup in S3 è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.
- Sistemi esistenti: Aprire l'ambiente di lavoro, fare clic sull'icona delle impostazioni di backup e abilitare i backup.



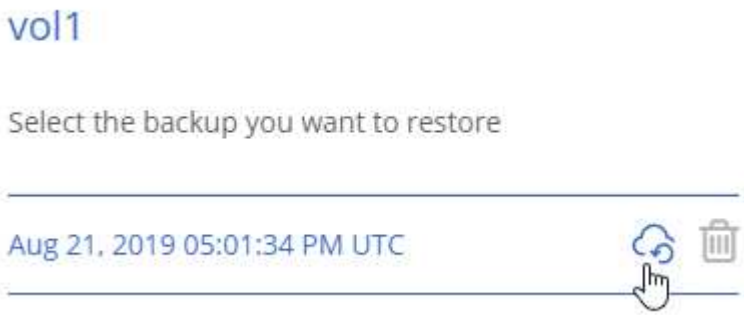
Se necessario, modificare il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva 30 copie di backup per ogni volume. Se necessario, è possibile modificare il numero di copie di backup da conservare.



Ripristinare i dati, se necessario

Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**, selezionare un volume, selezionare un backup, quindi ripristinare i dati dal backup in un nuovo volume.



Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi in S3.

Versioni di ONTAP supportate

Il backup su S3 è supportato con Cloud Volume ONTAP 9.4 e versioni successive.

Regioni AWS supportate

Il backup su S3 è supportato con Cloud Volumes ONTAP nelle seguenti aree AWS:

- US East (N. Virginia)
- STATI UNITI occidentali (Oregon)
- UE (Irlanda)
- UE (Francoforte)
- Asia Pacifico (Sydney)

Autorizzazioni AWS richieste

Il ruolo IAM che fornisce le autorizzazioni a Cloud Manager deve includere quanto segue:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Requisito di abbonamento AWS

A partire dalla versione 3.7.3, è disponibile un nuovo abbonamento a Cloud Manager in AWS Marketplace. Questo abbonamento consente l'implementazione di sistemi PAYGO Cloud Volumes ONTAP 9.6 e versioni successive e la funzionalità di backup in S3. È necessario "Iscriviti a questo nuovo abbonamento a Cloud Manager" Prima di attivare Backup su S3. La fatturazione per la funzione Backup in S3 viene effettuata tramite questo abbonamento.

Requisiti delle porte

- La porta TCP 5010 deve essere aperta per il traffico in uscita da Cloud Volumes ONTAP al servizio di backup.
- La porta TCP 8088 deve essere aperta per il traffico in uscita nel gruppo di sicurezza di Cloud Manager.

  Queste porte sono già aperte se sono stati utilizzati i gruppi di protezione predefiniti. Tuttavia, se hai utilizzato le tue, dovrai aprire queste porte.

Accesso a Internet in uscita

Assicurarsi che il seguente endpoint sia accessibile da Cloud Manager: https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager contatta questo endpoint per aggiungere il tuo ID account AWS all'elenco degli utenti autorizzati per Backup in S3.

Interfaccia endpoint VPC

Quando si attiva la funzione Backup in S3, Cloud Manager crea un endpoint VPC di interfaccia nel VPC in cui è in esecuzione Cloud Volumes ONTAP. Questo *endpoint di backup* si connette al VPC NetApp in cui è in esecuzione Backup in S3. Se ripristini un volume, Cloud Manager crea un endpoint VPC con interfaccia aggiuntiva, ovvero l' *endpoint di ripristino*.

Tutti i sistemi Cloud Volumes ONTAP aggiuntivi del VPC utilizzano questi due endpoint VPC.

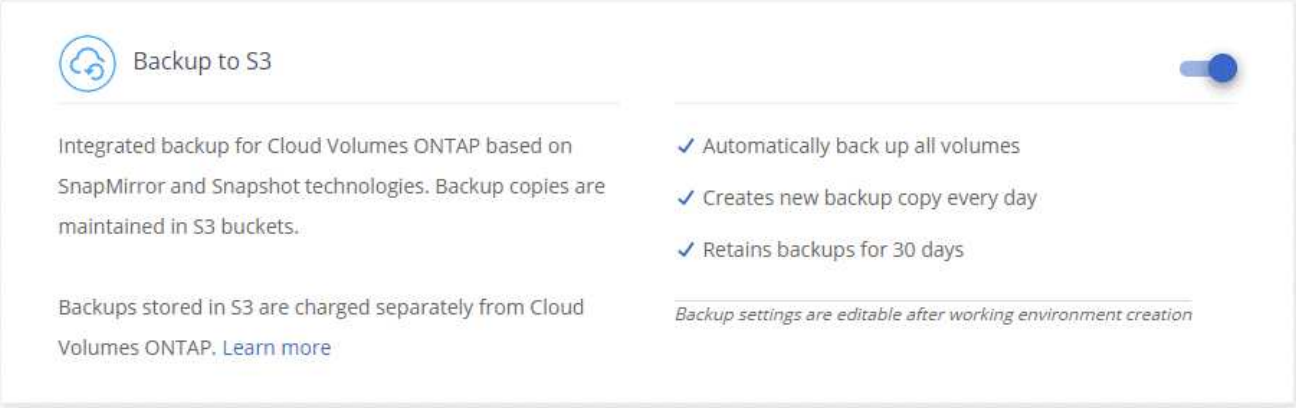
"Il limite predefinito per gli endpoint VPC dell'interfaccia è 20 per VPC". Assicurarsi che il VPC non abbia raggiunto il limite prima di attivare la funzione.

Abilitazione dei backup in S3 su un nuovo sistema

La funzione Backup in S3 è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina Backup in S3, lasciare attivata la funzione e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

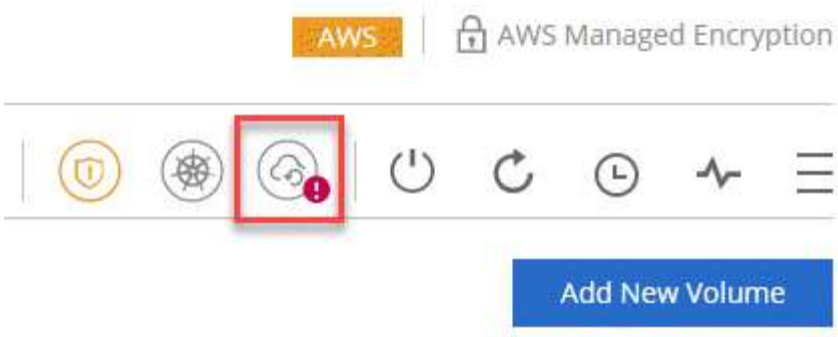
La funzione Backup in S3 è attivata sul sistema e consente di eseguire il backup dei volumi ogni giorno, conservando 30 copie di backup. Scopri come modificare la conservazione dei backup.

Abilitazione dei backup in S3 su un sistema esistente

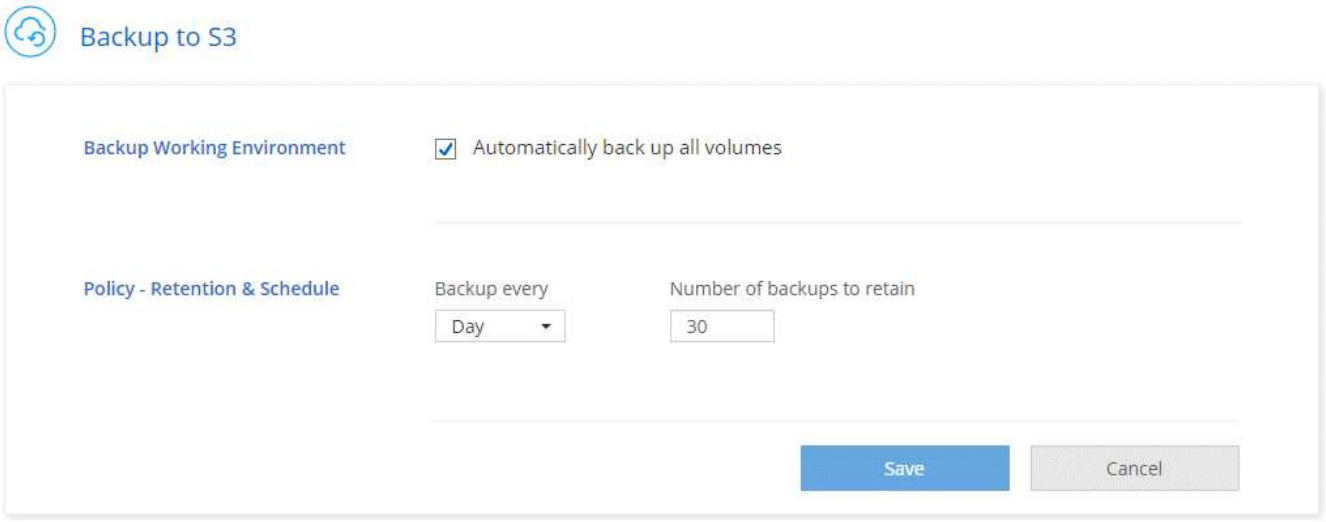
È possibile abilitare i backup in S3 su un sistema Cloud Volumes ONTAP esistente, purché sia in esecuzione una configurazione supportata. Per ulteriori informazioni, vedere Requisiti.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Selezionare **backup automatico di tutti i volumi**.
4. Scegliere la conservazione del backup e fare clic su **Save** (Salva).



Risultato

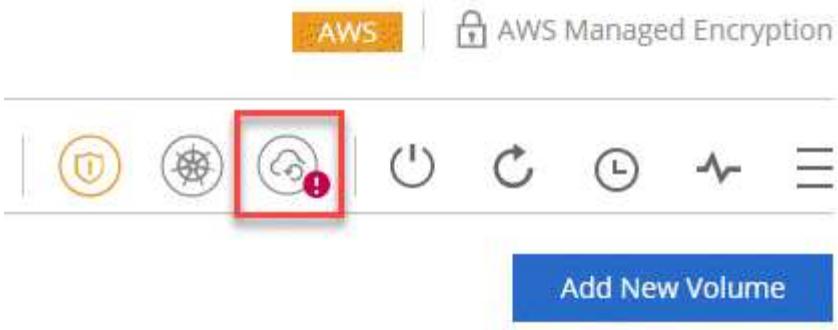
La funzionalità Backup in S3 inizia a eseguire i backup iniziali di ciascun volume.

Modifica della conservazione del backup

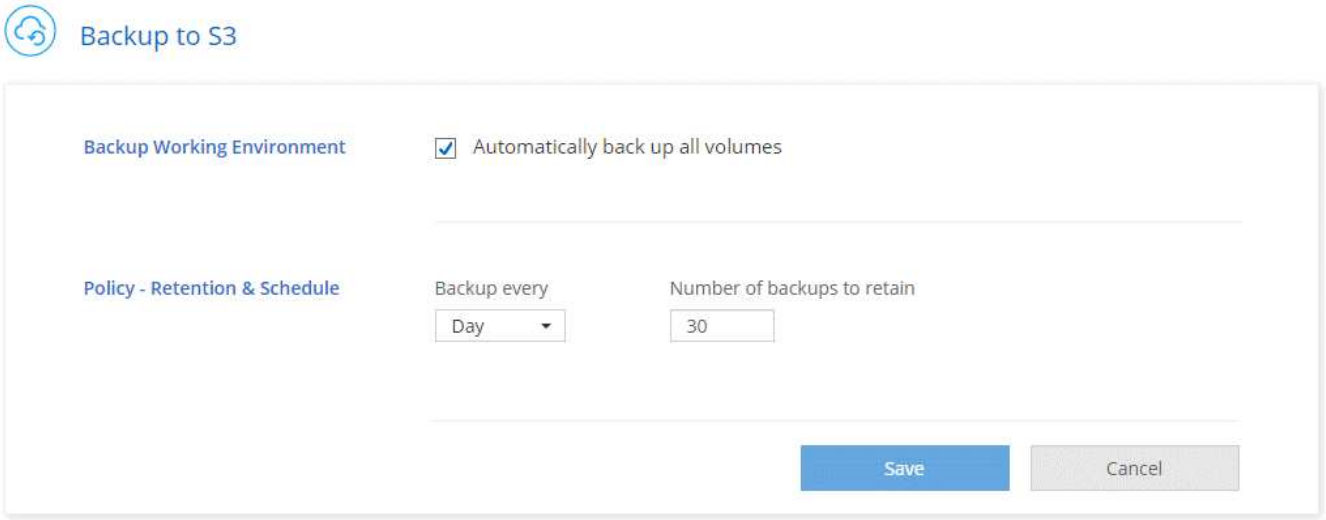
Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva 30 copie di backup per ogni volume. È possibile modificare il numero di copie di backup da conservare.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Modificare la conservazione del backup, quindi fare clic su **Save** (Salva).



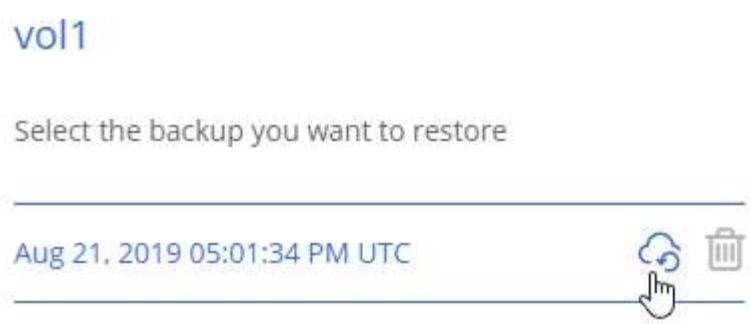
Ripristino di un volume

Quando ripristini i dati da un backup, Cloud Manager esegue un ripristino completo del volume in un volume *new*. È possibile ripristinare i dati nello stesso ambiente di lavoro o in un ambiente di lavoro diverso.

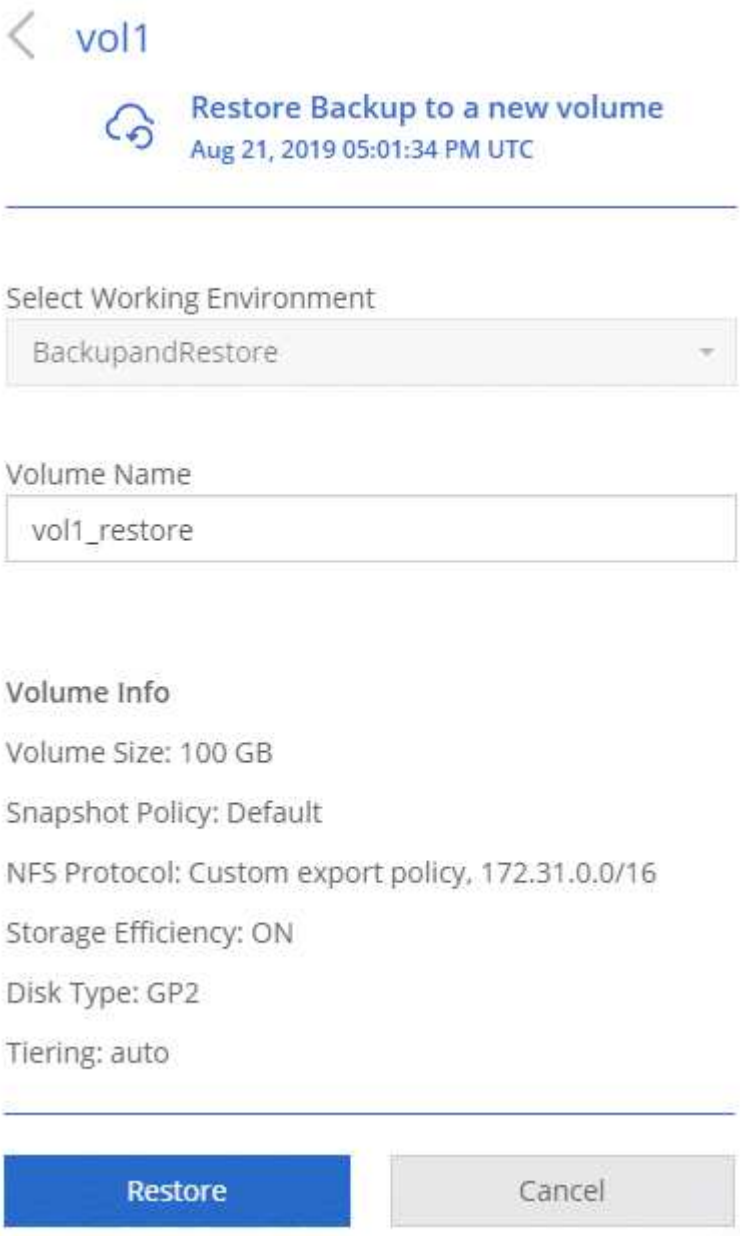
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**.
2. Selezionare il volume che si desidera ripristinare.

3. Individuare il backup da cui si desidera eseguire il ripristino e fare clic sull'icona di ripristino.



4. Selezionare l'ambiente di lavoro in cui si desidera ripristinare il volume.
5. Immettere un nome per il volume.
6. Fare clic su **Restore** (Ripristina).

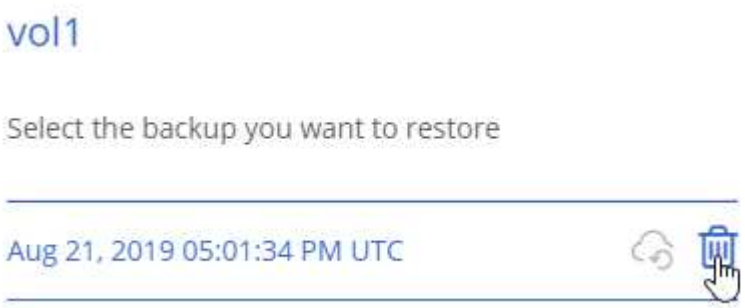


Eliminazione dei backup

Tutti i backup vengono conservati in S3 fino a quando non vengono eliminati da Cloud Manager. I backup non vengono cancellati quando si elimina un volume o quando si elimina il sistema Cloud Volumes ONTAP.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**.
2. Selezionare un volume.
3. Individuare il backup che si desidera eliminare e fare clic sull'icona di eliminazione.



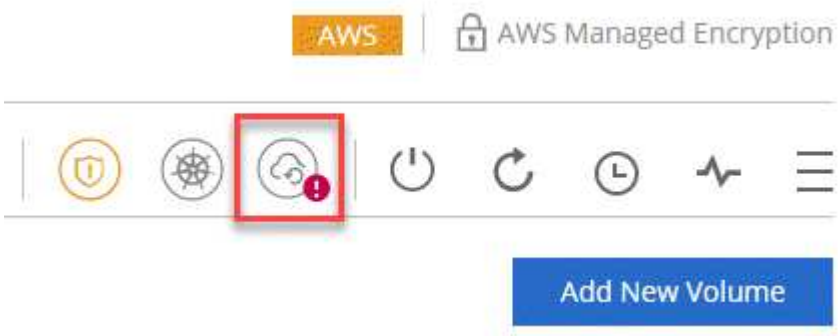
4. Confermare che si desidera eliminare il backup.

Disattivazione dei backup in S3

La disattivazione dei backup in S3 disattiva i backup di ciascun volume nel sistema. I backup esistenti non verranno eliminati.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Disattiva **Esegui automaticamente il backup di tutti i volumi**, quindi fai clic su **Salva**.

Funzionamento di Backup in S3

Le sezioni seguenti forniscono ulteriori informazioni sulla funzione Backup in S3.

Dove risiedono i backup

Le copie di backup vengono memorizzate in un bucket S3 di proprietà di NetApp, nella stessa regione in cui si trova il sistema Cloud Volumes ONTAP.

I backup sono incrementali

Dopo il backup completo iniziale dei dati, tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e dei nuovi blocchi.

I backup vengono eseguiti a mezzanotte

I backup giornalieri iniziano ogni giorno dopo la mezzanotte. Al momento, non è possibile pianificare le operazioni di backup in un orario specificato dall'utente.

Le copie di backup sono associate al tuo account Cloud Central

Le copie di backup sono associate a "Account Cloud Central" In cui risiede Cloud Manager.

Se si dispone di più sistemi Cloud Manager nello stesso account Cloud Central, ciascun sistema Cloud Manager visualizzerà lo stesso elenco di backup. Che include i backup associati alle istanze di Cloud Volumes ONTAP da altri sistemi di Cloud Manager.

Il criterio di backup è esteso a tutto il sistema

Il numero di backup da conservare viene definito a livello di sistema. Non è possibile impostare criteri diversi per ciascun volume del sistema.

Sicurezza

I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.

I dati viaggiano attraverso collegamenti protetti con Direct Connect al servizio ed è protetto da crittografia AES a 256 bit. I dati crittografati vengono quindi scritti nel cloud utilizzando connessioni HTTPS TLS 1.2. I dati viaggiano anche su Amazon S3 solo attraverso connessioni endpoint VPC sicure, quindi non viene inviato traffico su Internet.

A ciascun utente viene assegnata una chiave tenant, oltre a una chiave di crittografia generale di proprietà del servizio. Questo requisito è simile alla necessità di una coppia di chiavi per aprire un cliente in una banca. Tutte le chiavi, come credenziali cloud, sono memorizzate in modo sicuro dal servizio e sono limitate solo al personale NetApp responsabile della manutenzione del servizio.

Limitazioni

- Se si utilizza uno dei seguenti tipi di istanza, un sistema Cloud Volumes ONTAP può eseguire il backup di un massimo di 20 volumi in S3:
  - m4.xlange
  - m5.xlange
  - r4.xlange
  - r5.xlange
- Il backup dei volumi creati al di fuori di Cloud Manager non viene eseguito automaticamente su S3.

Ad esempio, se si crea un volume dall'interfaccia CLI di ONTAP, dall'API di ONTAP o da Gestore di sistema, il backup del volume non verrà eseguito automaticamente.

Se si desidera eseguire il backup di questi volumi, è necessario disattivare Backup in S3 e riattivarlo.

- Quando ripristini i dati da un backup, Cloud Manager esegue un ripristino completo del volume in un volume *new*. Il backup di questo nuovo volume non viene eseguito automaticamente su S3.

  Se si desidera eseguire il backup dei volumi creati da un'operazione di ripristino, è necessario disattivare Backup in S3 e riattivarlo.

- È possibile eseguire il backup di volumi di dimensioni pari o inferiori a 50 TB.
- Il backup su S3 può mantenere fino a 245 backup totali di un volume.
- Lo storage WORM non è supportato su un sistema Cloud Volumes ONTAP quando è attivato il backup su S3.

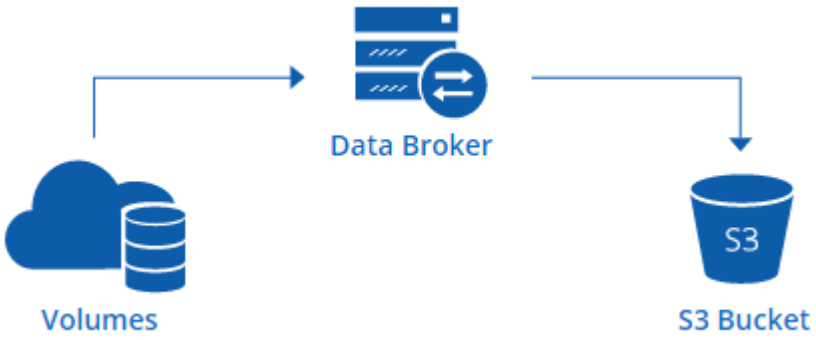
Sincronizzazione dei dati su Amazon S3

Puoi sincronizzare i dati dai volumi ONTAP a un bucket Amazon S3 integrando un ambiente di lavoro con "NetApp Cloud Sync". È quindi possibile utilizzare i dati sincronizzati come copia secondaria o per l'elaborazione dei dati utilizzando servizi AWS come EMR e Redshift.

Come funziona la funzione di sincronizzazione con S3

È possibile integrare un ambiente di lavoro con il servizio Cloud Sync in qualsiasi momento. Quando si integra un ambiente di lavoro, il servizio Cloud Sync sincronizza i dati dai volumi selezionati in un singolo bucket S3. L'integrazione funziona con gli ambienti di lavoro di Cloud Volumes ONTAP e con i cluster ONTAP on-premise o che fanno parte di una configurazione di storage privato NetApp (NPS).

Per sincronizzare i dati, il servizio avvia un'istanza del broker di dati nel VPC. Cloud Sync utilizza un data broker per ambiente di lavoro per sincronizzare i dati dai volumi a un bucket S3. Dopo la sincronizzazione iniziale, il servizio sincronizza tutti i dati modificati una volta al giorno a mezzanotte.



Se si desidera eseguire azioni Cloud Sync avanzate, accedere direttamente al servizio Cloud Sync. Da qui è possibile eseguire azioni come la sincronizzazione da S3 a un server NFS, la scelta di diversi bucket S3 per i volumi e la modifica delle pianificazioni.

14 giorni di prova gratuita

Se sei un nuovo utente Cloud Sync, i primi 14 giorni sono gratuiti. Al termine della prova gratuita, devi pagare ogni *relazione di sincronizzazione* a una tariffa oraria o acquistando licenze. Ogni volume sincronizzato con un bucket S3 è considerato una relazione di sincronizzazione. È possibile impostare entrambe le opzioni di pagamento direttamente da Cloud Sync nella pagina Impostazioni di licenza.

Come ottenere aiuto

Utilizzare le seguenti opzioni per qualsiasi supporto relativo alla funzione di sincronizzazione con S3 di Cloud Manager o per Cloud Sync in generale:

- Feedback generale sui prodotti: ng-cloudsync-contact@netapp.com
- Opzioni di supporto tecnico:
  - Community NetApp Cloud Sync
  - Chat in-product (angolo in basso a destra di Cloud Manager)

Integrazione di un ambiente di lavoro con il servizio Cloud Sync

Se si desidera sincronizzare i volumi su Amazon S3 direttamente da Cloud Manager, è necessario integrare l'ambiente di lavoro con il servizio Cloud Sync.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Fasi

1. Aprire un ambiente di lavoro e fare clic su **Sync to S3**.
2. Fare clic su **Sync** e seguire le istruzioni per sincronizzare i dati su S3.

Non è possibile sincronizzare i volumi di protezione dei dati in S3. I volumi devono essere scrivibili.

Gestione delle relazioni di sincronizzazione dei volumi

Dopo aver integrato un ambiente di lavoro con il servizio Cloud Sync, è possibile sincronizzare volumi aggiuntivi, interrompere la sincronizzazione di un volume e rimuovere l'integrazione con Cloud Sync.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sull'ambiente di lavoro su cui si desidera gestire le relazioni di sincronizzazione.
2. Se si desidera attivare o disattivare la sincronizzazione con S3 per un volume, selezionare il volume e fare clic su **Sync to S3** o **Delete Sync Relationship**.
3. Se si desidera eliminare tutte le relazioni di sincronizzazione per un ambiente di lavoro, fare clic sulla scheda **Sync to S3**, quindi fare clic su **Delete Sync** (Elimina sincronizzazione).

   Questa azione non elimina i dati sincronizzati dal bucket S3. Se il data broker non viene utilizzato in altre relazioni di sincronizzazione, il servizio Cloud Sync elimina il data broker.

Approfondimenti sulla privacy dei dati

Scopri di più sulla conformità al cloud

La conformità al cloud è un servizio di privacy e conformità dei dati per Cloud Volumes ONTAP in AWS e Azure. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili nei sistemi Cloud Volumes ONTAP.

Cloud Compliance è attualmente disponibile come release a disponibilità controllata.

"Scopri i casi di utilizzo per la conformità al cloud".

Caratteristiche

Cloud Compliance offre diversi strumenti che possono aiutarti con le tue attività di compliance. Puoi utilizzare la conformità al cloud per:

- Identificare le informazioni personali identificabili (PII)
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR, CCPA, PCI e HIPAA
- Rispondere alle richieste di accesso dei soggetti a dati (DSAR)

Costo

La conformità al cloud è un servizio add-on per Cloud Volumes ONTAP fornito da NetApp senza costi aggiuntivi. L'attivazione della conformità al cloud richiede l'implementazione di un'istanza del cloud, che verrà addebitata dal tuo cloud provider. Non sono previsti costi per l'ingresso o l'uscita dei dati perché i dati non fluiscono all'esterno della rete.

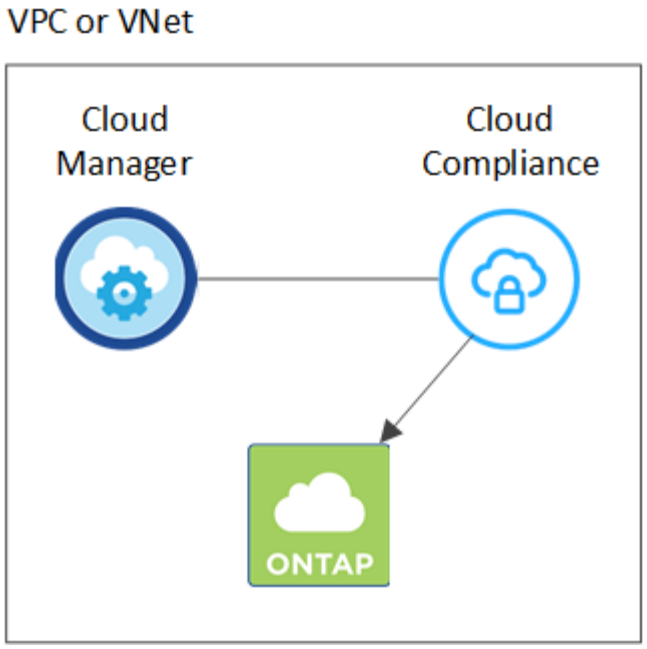
Come funziona Cloud Compliance

Ad alto livello, la conformità al cloud funziona come segue:

1. Abilita la conformità al cloud su uno o più sistemi Cloud Volumes ONTAP.
2. Cloud Compliance esegue la scansione dei dati utilizzando un processo di apprendimento ai.
3. In Cloud Manager, fai clic su **Compliance** e utilizza la dashboard e gli strumenti di reporting forniti per aiutarti nelle tue attività di compliance.

L'istanza di Cloud Compliance

Quando abiliti la conformità al cloud su uno o più sistemi Cloud Volumes ONTAP, Cloud Manager implementa un'istanza di conformità al cloud nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta.



Tenere presente quanto segue a proposito dell'istanza:

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco io1 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Per ogni sistema Cloud Manager viene implementata una sola istanza di Cloud Compliance.
- Gli aggiornamenti del software Cloud Compliance sono automatizzati e non dovrai preoccuparti di questo.

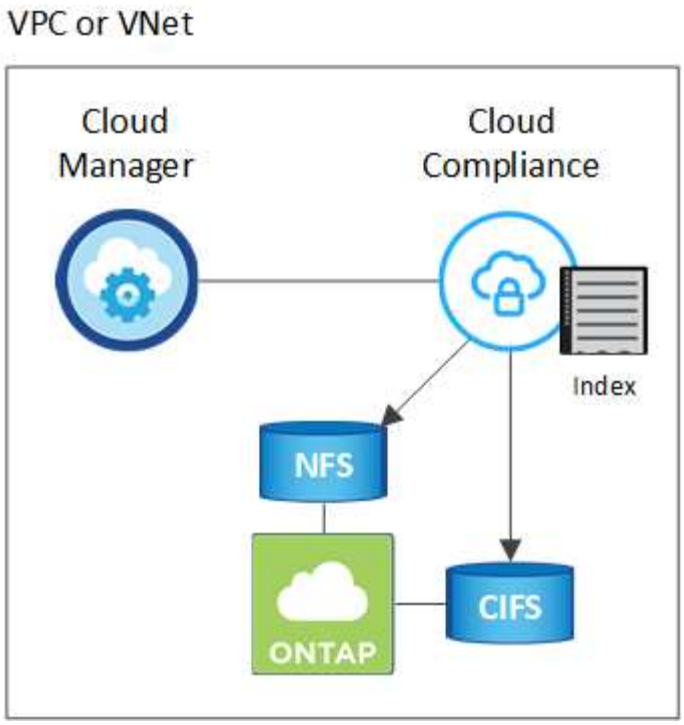
L'istanza deve rimanere sempre in esecuzione perché la conformità cloud esegue continuamente la scansione dei dati sui sistemi Cloud Volumes ONTAP.

Come funzionano le scansioni

Dopo aver attivato la conformità al cloud, inizia immediatamente la scansione dei dati per identificare i dati personali e sensibili.

La conformità al cloud si connette a Cloud Volumes ONTAP come qualsiasi altro client montando volumi NFS e CIFS. Ai volumi NFS viene automaticamente eseguito l'accesso in sola lettura, mentre è necessario fornire le credenziali Active Directory per eseguire la scansione dei volumi CIFS.

Cloud Compliance esegue la scansione dei dati non strutturati su ciascun volume per individuare una serie di informazioni personali. Mappa i dati dell'organizzazione, classifica ciascun file e identifica ed estrae entità e modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili e categorie di dati.



Dopo la scansione iniziale, Cloud Compliance esegue una scansione continua di ciascun volume per rilevare le modifiche incrementali (per questo motivo è importante mantenere l'istanza in esecuzione).

È possibile attivare e disattivare le scansioni a livello di ambiente di lavoro, ma non a livello di volume. "Scopri come".

Informazioni indicizzati dalla Cloud Compliance

Cloud Compliance raccoglie, indicizza e assegna le categorie ai dati non strutturati (file). I dati indicizzati dalla Cloud Compliance includono:

Metadati standard

Cloud Compliance raccoglie i metadati standard relativi ai file: Il tipo, le dimensioni, le date di creazione e modifica e così via.

Dati personali

Informazioni personali come indirizzi e-mail, numeri di identificazione o numeri di carta di credito. "Scopri di più sui dati personali".

Dati personali sensibili

Tipi speciali di informazioni sensibili, come dati sanitari, origine etnica o opinioni politiche, come definito dal GDPR e da altre normative sulla privacy. "Scopri di più sui dati personali sensibili".

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Scopri di più sulle categorie".

Riconoscimento entità nome

Cloud Compliance utilizza l'ai per estrarre i nomi delle persone fisiche dai documenti. "Scopri come rispondere alle richieste di accesso ai soggetti dati".

Panoramica delle reti

Cloud Manager implementa l'istanza Cloud Compliance con un indirizzo IP privato e un gruppo di sicurezza che abilita le connessioni HTTP in entrata da Cloud Manager. Questa connessione consente di accedere alla dashboard Cloud Compliance dall'interfaccia di Cloud Manager.

Le regole in uscita sono completamente aperte. L'istanza si connette ai sistemi Cloud Volumes ONTAP e a Internet tramite un proxy da Cloud Manager. L'accesso a Internet è necessario per aggiornare il software Cloud Compliance e inviare metriche di utilizzo.

Se hai requisiti di rete rigorosi, "Scopri gli endpoint che la Cloud Compliance contatta".

I dati indicizzati non lasciano mai l'istanza di Cloud Compliance: I dati non vengono inoltrati al di fuori della rete virtuale e non vengono inviati a Cloud Manager.

Accesso dell'utente alle informazioni di conformità

Gli amministratori di Cloud Manager possono visualizzare le informazioni di conformità per tutti gli ambienti di lavoro.

Gli amministratori dello spazio di lavoro possono visualizzare le informazioni di conformità solo per i sistemi ai quali sono autorizzati ad accedere. Se un amministratore dell'area di lavoro non riesce ad accedere a un ambiente di lavoro in Cloud Manager, non può visualizzare alcuna informazione di conformità per l'ambiente di lavoro nella scheda Compliance.

"Scopri di più sui ruoli di Cloud Manager".

Introduzione alla conformità cloud per Cloud Volumes ONTAP

Completa alcuni passaggi per iniziare a utilizzare la conformità cloud per Cloud Volumes ONTAP in AWS o Azure.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare che la configurazione soddisfi i requisiti

- Assicurarsi che l'istanza Cloud Compliance disponga dell'accesso a Internet in uscita.

  Cloud Manager implementa l'istanza nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta.

- Assicurarsi che gli utenti possano accedere all'interfaccia di Cloud Manager da un host che dispone di una connessione diretta ad AWS o Azure o da un host che si trova all'interno della stessa rete dell'istanza di Cloud Compliance (l'istanza avrà un indirizzo IP privato).
- Assicurarsi di poter mantenere in esecuzione l'istanza Cloud Compliance.

Abilita la conformità del cloud su Cloud Volumes ONTAP

- Nuovi ambienti di lavoro: Assicurati di mantenere la conformità cloud abilitata quando crei l'ambiente di lavoro (è attivata per impostazione predefinita).
- Ambienti di lavoro esistenti: Fare clic su **Compliance**, modificare l'elenco degli ambienti di lavoro e fare clic su **Show Compliance Dashboard** (Mostra dashboard conformità).

Garantire l'accesso ai volumi

Ora che la conformità al cloud è abilitata, assicurati che l'IT possa accedere ai volumi.

- L'istanza di conformità cloud richiede una connessione di rete a ciascuna subnet Cloud Volumes ONTAP.
- I gruppi di sicurezza per Cloud Volumes ONTAP devono consentire connessioni in entrata dall'istanza di conformità cloud.
- Le policy di esportazione dei volumi NFS devono consentire l'accesso dall'istanza Cloud Compliance.
- Cloud Compliance necessita delle credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Compliance** > **CIFS Scan Status** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali. Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere i dati che richiedono autorizzazioni elevate.

Garantire la connettività tra Cloud Manager e Cloud Compliance

- Il gruppo di sicurezza per Cloud Manager deve consentire il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.
- Se la rete AWS non utilizza un NAT o un proxy per l'accesso a Internet, il gruppo di sicurezza per Cloud Manager deve consentire il traffico in entrata sulla porta TCP 3128 dall'istanza Cloud Compliance.

Verifica dei prerequisiti

Prima di attivare la conformità al cloud, verificare di disporre di una configurazione supportata. Dopo aver attivato la conformità al cloud, dovrai garantire la connettività tra i componenti. Di seguito viene descritto.

Abilitare l'accesso a Internet in uscita

La conformità al cloud richiede l'accesso a Internet in uscita. Se la rete virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza Cloud Compliance disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint:

Endpoint	Scopo
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.

Endpoint	Scopo
https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.docker.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Consente alla conformità del cloud di accedere e scaricare manifesti e modelli e di inviare registri e metriche.

Verificare la connettività del browser Web alla conformità del cloud

L'istanza Cloud Compliance utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili a Internet. Di conseguenza, il browser Web utilizzato per accedere a Cloud Manager deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta ad AWS o Azure (ad esempio, una VPN) o da un host che si trova all'interno della stessa rete dell'istanza Cloud Compliance.

Se si accede a Cloud Manager da un indirizzo IP pubblico, probabilmente il browser Web non è in esecuzione su un host all'interno della rete.

Mantieni la conformità al cloud in esecuzione

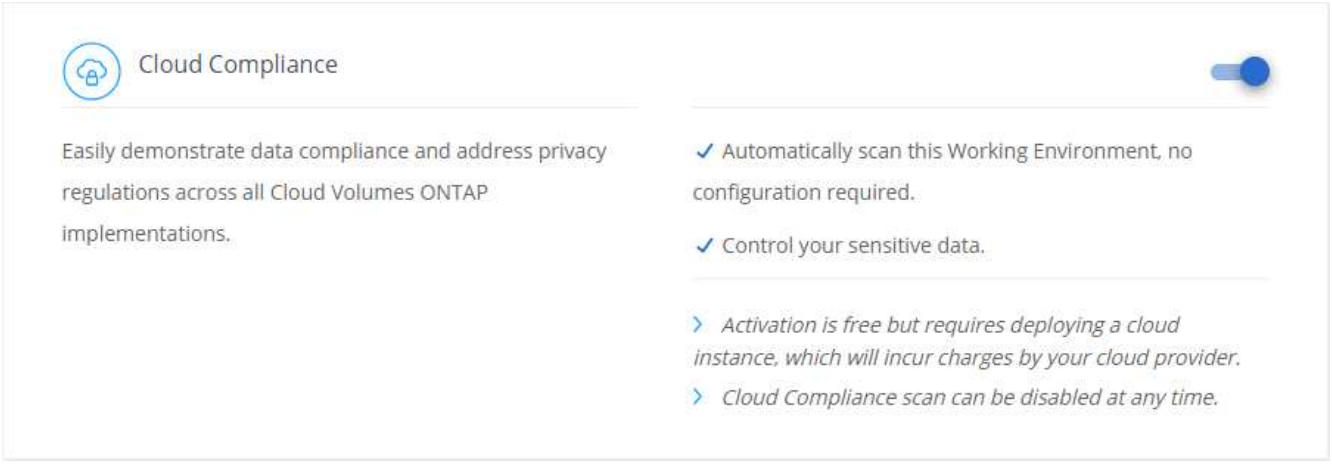
L'istanza di Cloud Compliance deve continuare a eseguire la scansione dei dati.

Abilitare la conformità al cloud in un nuovo ambiente di lavoro

La conformità cloud è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services o Microsoft Azure come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare abilitata la conformità cloud e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

   Per ulteriori informazioni, vedere "Avvio di Cloud Volumes ONTAP in AWS" e. "Lancio di Cloud Volumes ONTAP in Azure".

Risultato

La conformità al cloud è abilitata sul sistema Cloud Volumes ONTAP. Se questa è la prima volta che hai attivato la conformità al cloud, Cloud Manager implementa l'istanza di conformità al cloud nel tuo cloud provider. Non appena l'istanza è disponibile, inizia la scansione dei dati man mano che vengono scritti in ciascun volume creato.

Abilitare la conformità al cloud negli ambienti di lavoro esistenti

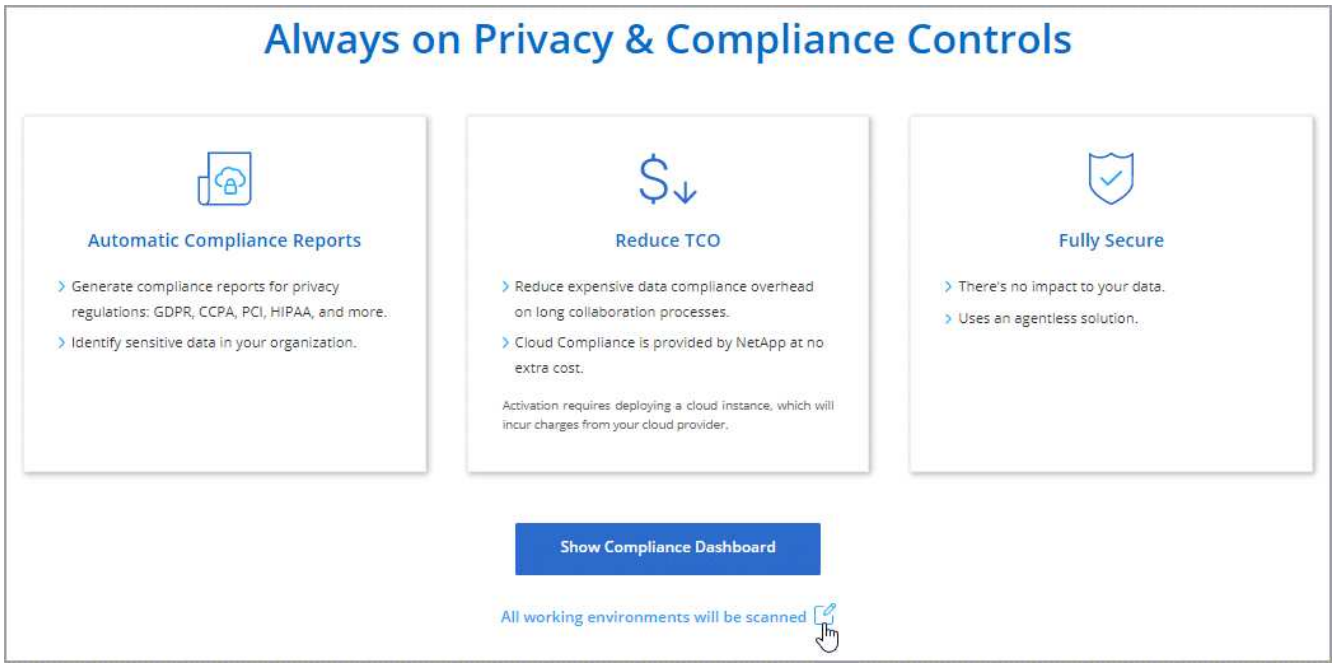
Abilita la conformità al cloud sui tuoi sistemi Cloud Volumes ONTAP esistenti dalla scheda **Compliance** di Cloud Manager.

Un'altra opzione consiste nell'attivare la conformità cloud dalla scheda **ambienti di lavoro** selezionando ciascun ambiente di lavoro singolarmente. Il completamento di questo processo richiede più tempo, a meno che non si disponga di un solo sistema.

Passaggi per ambienti di lavoro multipli

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Se si desidera attivare la conformità cloud su ambienti di lavoro specifici, fare clic sull'icona di modifica.

   In caso contrario, Cloud Manager è impostato per abilitare la conformità al cloud in tutti gli ambienti di lavoro ai quali si ha accesso.

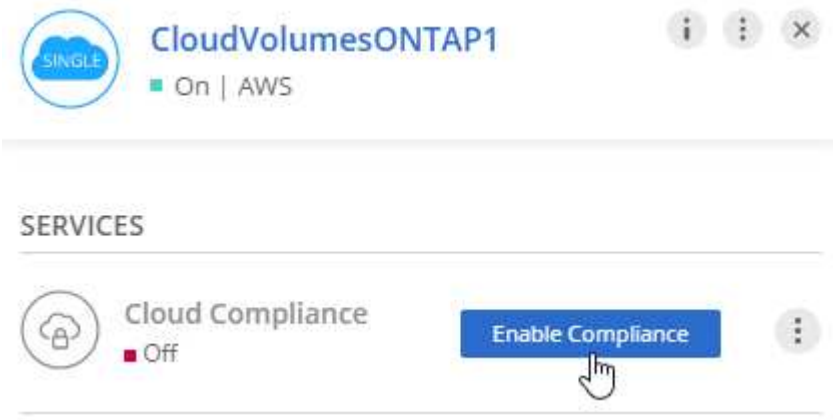


3. Fare clic su **Mostra dashboard conformità**.

Passaggi per un singolo ambiente di lavoro

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.

3. Nel riquadro a destra, fare clic su **Enable Compliance** (attiva conformità).



Risultato

Se questa è la prima volta che hai attivato la conformità al cloud, Cloud Manager implementa l'istanza di conformità al cloud nel tuo cloud provider.

Cloud Compliance inizia la scansione dei dati in ogni ambiente di lavoro. I dati saranno disponibili nella dashboard Compliance non appena la Cloud Compliance terminerà le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

Verificare che la conformità del cloud abbia accesso ai volumi

Assicurati che la conformità al cloud possa accedere ai volumi su Cloud Volumes ONTAP controllando il networking, i gruppi di sicurezza e le policy di esportazione. È necessario fornire le credenziali CIFS per la conformità al cloud in modo che possa accedere ai volumi CIFS.

Fasi

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di conformità cloud e ciascuna subnet Cloud Volumes ONTAP.

   Cloud Manager implementa l'istanza di conformità cloud nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta. Pertanto, questo passaggio è importante se alcuni sistemi Cloud Volumes ONTAP si trovano in sottoreti o reti virtuali diverse.

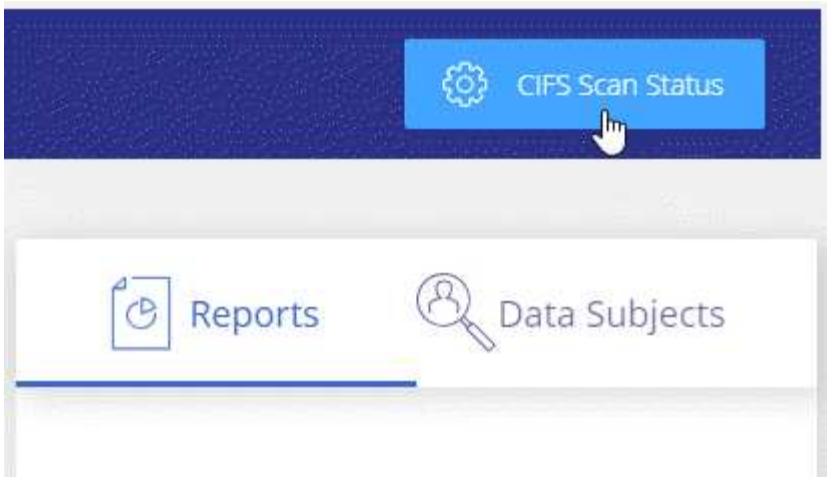
2. Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di conformità cloud.

   È possibile aprire il gruppo di sicurezza per il traffico dall'indirizzo IP dell'istanza Cloud Compliance oppure aprire il gruppo di sicurezza per tutto il traffico dall'interno della rete virtuale.

3. Assicurarsi che le policy di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza Cloud Compliance in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la conformità cloud con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

   a. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.

   b. In alto a destra, fare clic su **CIFS Scan Status** (Stato scansione CIFS).



c. Per ciascun sistema Cloud Volumes ONTAP, fare clic su **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per accedere ai volumi CIFS nel sistema.

   Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza Cloud Compliance.

   Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.

Verificare che Cloud Manager possa accedere alla conformità cloud

Assicurati la connettività tra Cloud Manager e Cloud Compliance per visualizzare le informazioni sulla conformità rilevate dalla Cloud Compliance.

Fasi

1. Assicurarsi che il gruppo di sicurezza per Cloud Manager consenta il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.

   Questa connessione consente di visualizzare le informazioni nella scheda Compliance.

2. Se la rete AWS non utilizza un NAT o un proxy per l'accesso a Internet, modificare il gruppo di sicurezza per Cloud Manager in modo da consentire il traffico in entrata sulla porta TCP 3128 dall'istanza Cloud Compliance.

   Ciò è necessario perché l'istanza Cloud Compliance utilizza Cloud Manager come proxy per accedere a Internet.

Questa porta è aperta per impostazione predefinita in tutte le nuove istanze di Cloud Manager, a partire dalla versione 3.7.5. Non è aperto sulle istanze di Cloud Manager create prima di quella versione.

Ottenere visibilità e controllo sui dati privati

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli relativi ai dati personali e ai dati personali sensibili della tua organizzazione. Puoi anche ottenere visibilità esaminando le categorie e i tipi di file che Cloud Compliance ha trovato nei tuoi dati.

Dati personali

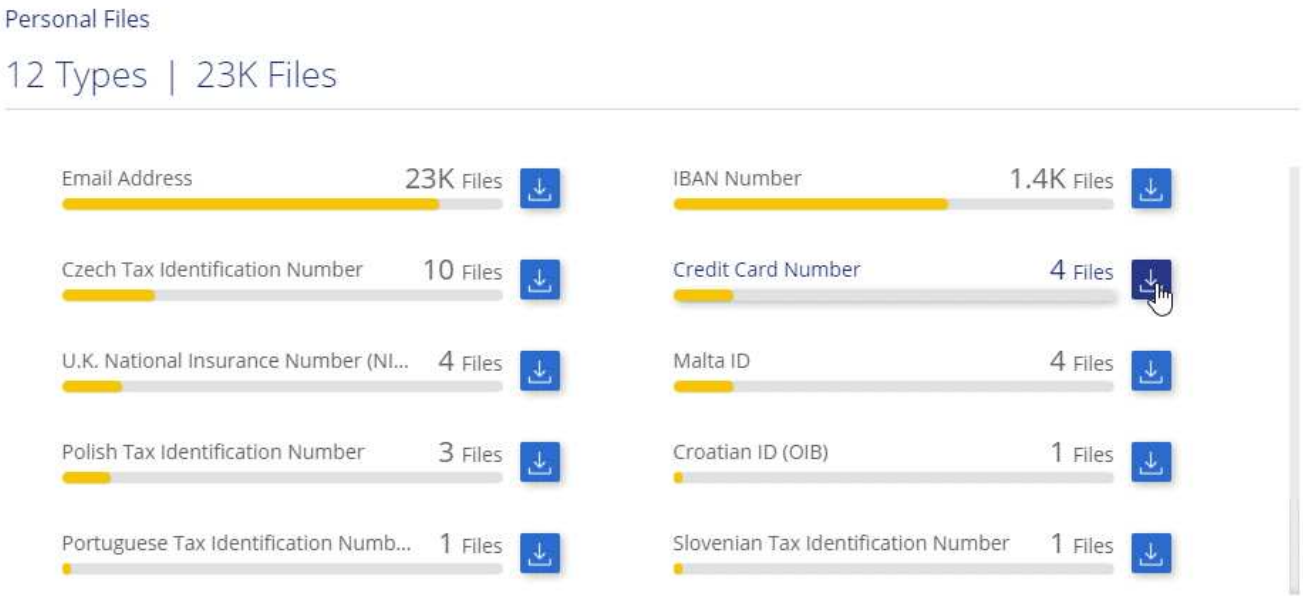
Cloud Compliance identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario e altro ancora. Consulta l'elenco completo.

Per alcuni tipi di dati personali, Cloud Compliance utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, Cloud Compliance identifica un Numero di previdenza sociale (SSN) come SSN se viene visualizzato un termine di prossimità, ad esempio *SSN* o *social Security*. L'elenco seguente Mostra quando Cloud Compliance utilizza la convalida di prossimità.

Visualizzazione di file contenenti dati personali

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 2 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi scaricare l'elenco dei tipi di dati personali trovati.



Tipi di dati personali

I dati personali contenuti nei file possono essere dati personali di carattere generale o identificativi nazionali. La terza colonna indica se la conformità al cloud utilizza convalida della prossimità per convalidare i risultati per l'identificatore.

Tipo	Identificatore	Convalida della prossimità?
Generale	Indirizzo e-mail	No
	Numero della carta di credito	No
	Numero IBAN (International Bank account Number)	No
	Indirizzo IP	Sì

Tipo	Identificatore	Convalida della prossimità?
Identificatori nazionali	ID belga (numero nazionale)	Sì
	ID bulgaro (numero civile unificato)	Sì
	Codice fiscale di Cipro (TIC)	Sì
	Codice fiscale danese (CPR)	Sì
	ID estone (Isikukood)	Sì
	ID finlandese (henkilötunnus)	Sì
	Francese Tax Identification Number (SPI)	Sì
	Codice fiscale tedesco (Steuerliche Identifikationsnummer)	Sì
	Codice fiscale ungherese (Adóazonosító jel)	Sì
	Irish ID (PPS) (ID irlandese)	Sì
	ID Israeliano	Sì
	ID italiano (Codice fiscale)	Sì
	Codice fiscale lettone	Sì
	Lituano ID (Asmens kodas)	Sì
	Lussemburgo ID	Sì
	ID Malta	Sì
	ID Paesi Bassi (BSN)	Sì
	Codice fiscale polacco	Sì
	Portoghese Tax Identification Number (NIF)	Sì
	Codice fiscale rumeno	Sì
	Numero di identificazione fiscale slovacco	Sì
	Codice fiscale sloveno	Sì
	ID sudafricano	Sì
	Codice fiscale spagnolo	Sì
	Codice fiscale svedese	Sì
	REGNO UNITO NINO (National Insurance Number)	Sì
	Numero di previdenza sociale (SSN) USA	Sì

Dati personali sensibili

Cloud Compliance identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy, ad esempio "articoli 9 e 10 del GDPR". Ad esempio, informazioni relative alla salute, all'origine etnica o all'orientamento sessuale di una persona. Consulta l'elenco completo.

Cloud Compliance utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il calcolo cognitivo (CC) per comprendere il significato dei contenuti che

scansiona al fine di estrarre le entità e classificarle di conseguenza.

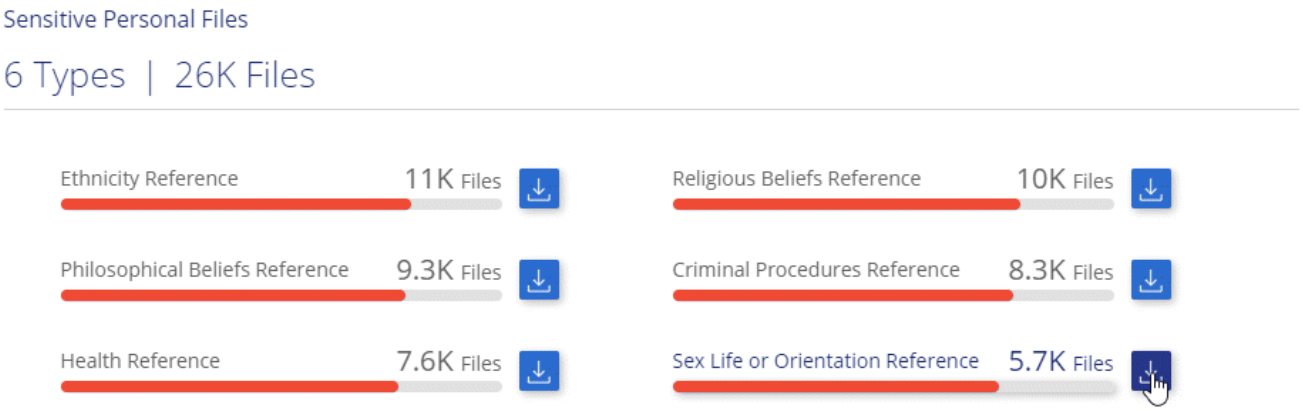
Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità di NLP, Cloud Compliance è in grado di distinguere la differenza tra una frase con la dicitura "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating Mexican Food" (George is Eating Mexican Food).

Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Visualizzazione di file contenenti dati personali sensibili

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 2 tipi di file principali direttamente dalla schermata principale oppure fare clic su **View All** (Visualizza tutto) e quindi scaricare l'elenco dei tipi di dati personali sensibili trovati.



Tipi di dati personali sensibili

I dati personali sensibili che Cloud Compliance può trovare nei file includono:

Riferimento alle procedure penali
Dati relativi alle condanne e ai reati penali di una persona fisica.

Riferimento di etnia
Dati relativi alla razza o all'origine etnica di una persona fisica.

Riferimento di salute
Dati relativi alla salute di una persona fisica.

Riferimento alle credenze filosofiche
Dati relativi alle convinzioni filosofiche di una persona naturale.

Riferimenti alle credenze religiose
Dati relativi alle convinzioni religiose di una persona fisica.

Sex Life o orientamento di riferimento

Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. Vedere l'elenco delle categorie.

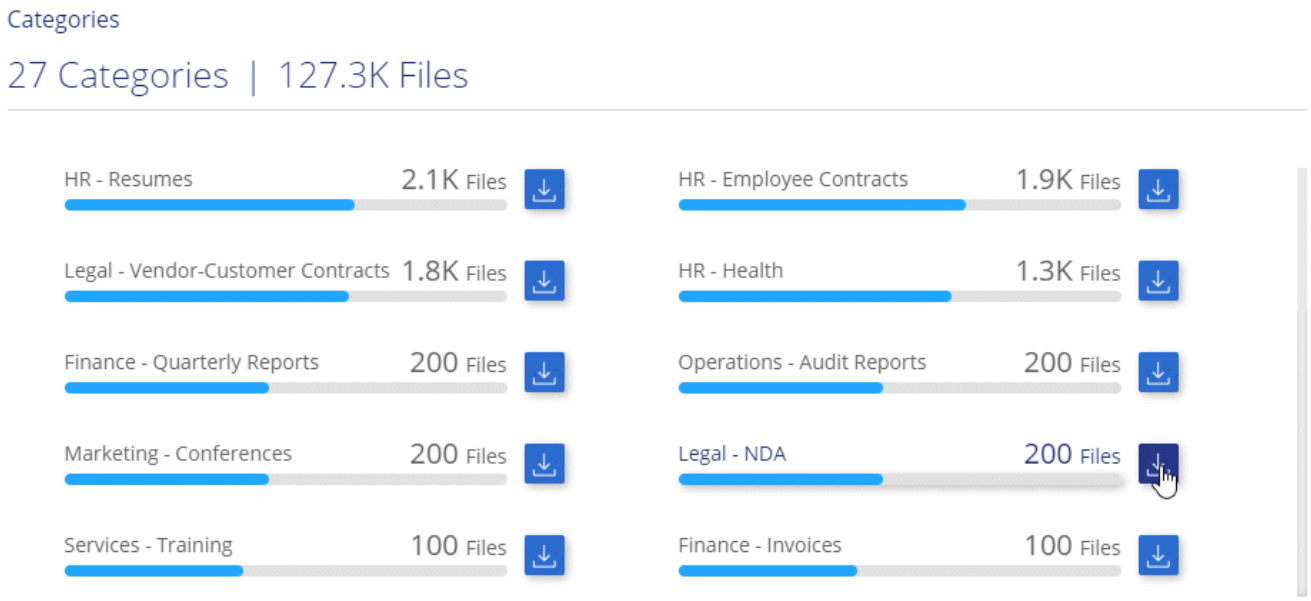
Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando il tipo di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si scarica il report CSV, i contratti dei dipendenti potrebbero essere memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Per le categorie è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Visualizzazione dei file in base alle categorie

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scarica i dettagli di uno dei primi 4 tipi di file direttamente dalla schermata principale oppure fai clic su **Visualizza tutto** e scarica l'elenco per qualsiasi categoria.



Tipi di categorie

La conformità al cloud classifica i tuoi dati nel modo seguente:

Finanza

- Bilanci
- Ordini di acquisto
- Fatture

- Report trimestrali

FC

- Controllo in background
- Piani di compensazione
- Contratti con i dipendenti
- Analisi dei dipendenti
- Salute
- Riprende

Legale

- NDA
- Contratti fornitore-cliente

Marketing

- Campagne
- Conferenze

Operazioni

- Report di audit

Vendite

- Ordini di vendita

Servizi

- RFI
- RFP
- Formazione

Supporto

- Reclami e biglietti

Altro

- Archiviare i file
- Audio
- File CAD
- Codice
- Eseguibili
- Immagini

Tipi di file

Cloud Compliance prende i dati sottoposti a scansione e li suddivide in base al tipo di file. Cloud Compliance consente di visualizzare tutti i tipi di file trovati nelle scansioni.

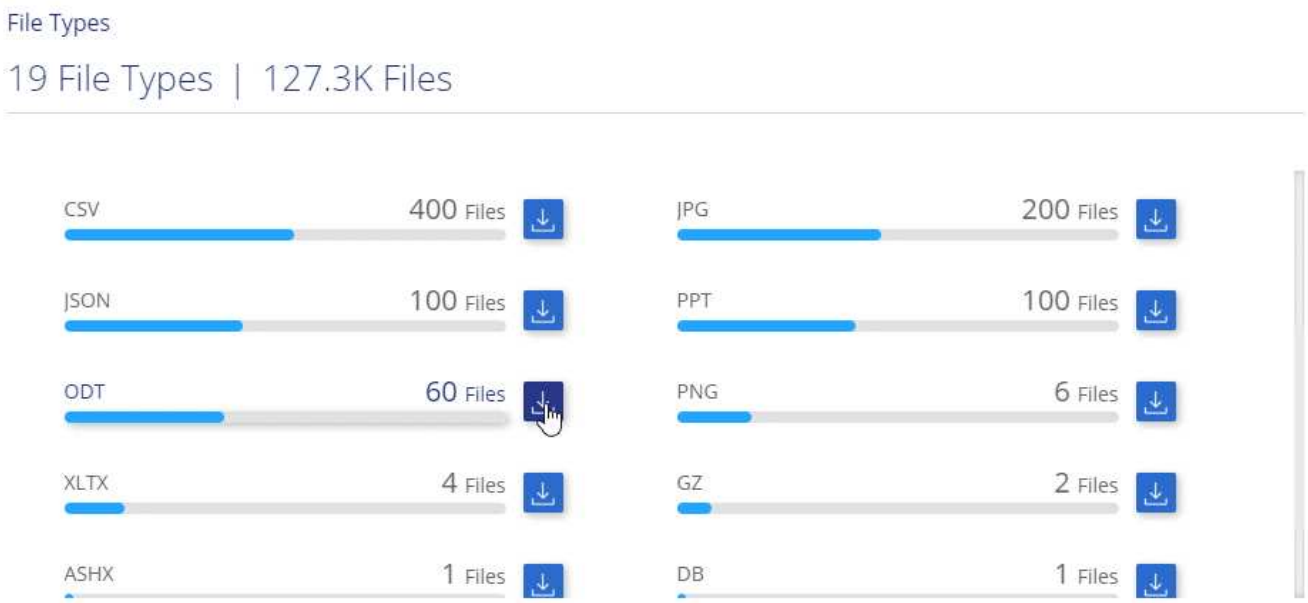
La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere

memorizzati correttamente. Ad esempio, è possibile memorizzare file CAD che includono informazioni molto sensibili sull'organizzazione. Se non sono protetti, è possibile assumere il controllo dei dati sensibili limitando le autorizzazioni o spostando i file in un'altra posizione.

Visualizzazione dei tipi di file

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. Scaricare i dettagli di uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **View All** (Visualizza tutto) e quindi scaricare l'elenco per qualsiasi tipo di file.



Accuratezza delle informazioni rilevate

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

In base ai nostri test, la tabella seguente mostra l'accuratezza delle informazioni rilevate dalla Cloud Compliance. Lo suddivideremo per *precisione* e *richiamo*:

Precisione

La probabilità che ciò che trova Cloud Compliance sia stata identificata correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali contengono effettivamente informazioni personali. 1 file su 10 sarebbe un falso positivo.

Ricorda

La probabilità che la conformità cloud trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che Cloud Compliance è in grado di identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La conformità al cloud perderebbe il 30% dei dati e non verrà visualizzata nella dashboard.

Cloud Compliance è in una release di disponibilità controllata e stiamo costantemente migliorando la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future release di Cloud Compliance.

Tipo	Precisione	Ricorda
Dati personali - Generale	90%-95%	60%-80%
Dati personali - identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Contenuto di ciascun report elenco file (file CSV)

La dashboard consente di scaricare elenchi di file (in formato CSV) che includono dettagli sui file identificati. Se sono presenti più di 10,000 risultati, nell'elenco vengono visualizzati solo i primi 10,000 risultati (il supporto per altri verrà aggiunto in seguito).

Ciascun elenco di file include le seguenti informazioni:

- Nome del file
- Tipo di ubicazione
- Posizione
- Percorso del file
- Tipo di file
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Data di rilevamento dell'eliminazione

  Una data di rilevamento dell'eliminazione identifica la data in cui il file è stato cancellato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file cancellati non fanno parte del numero di file visualizzato nella dashboard. I file vengono visualizzati solo nei report CSV.

Visualizzazione del report sulla valutazione dei rischi per la privacy

Il report sulla valutazione dei rischi per la privacy fornisce una panoramica dello stato di rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy come GDPR e CCPA.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Il report contiene le seguenti informazioni:

Stato di compliance

Un punteggio di severità (vedi sotto per ulteriori dettagli) e la distribuzione dei dati, sia che si tratti di dati non sensibili, personali o sensibili.

Panoramica della valutazione

Analisi dei tipi di dati personali rilevati, nonché delle categorie di dati.

Argomenti trattati in questa valutazione

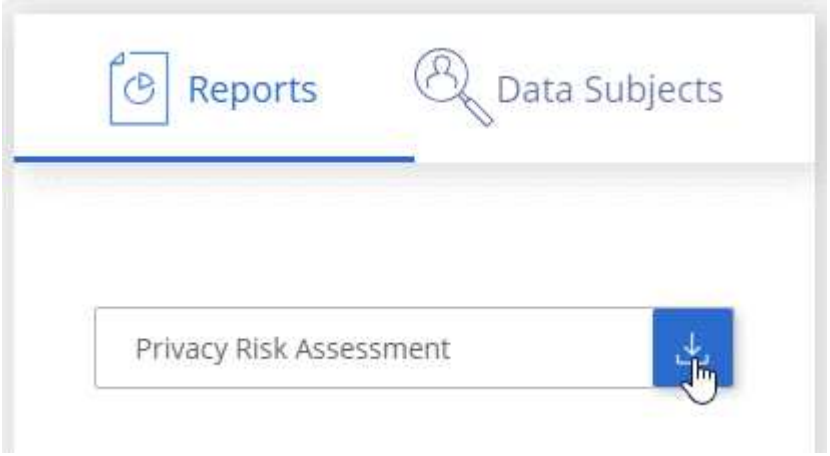
Il numero di persone per località per le quali sono stati trovati identificatori nazionali.

Generazione del report sulla valutazione dei rischi per la privacy

Accedere alla scheda Compliance per generare il report.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.
2. In **Report**, fare clic sull'icona di download accanto a **Privacy Risk Assessment**.



Risultato

Cloud Compliance genera un report PDF che puoi rivedere e inviare ad altri gruppi in base alle esigenze.

Punteggio di severità

Cloud Compliance calcola il punteggio di severità per il report di valutazione dei rischi per la privacy sulla base di tre variabili:

- La percentuale di dati personali su tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.
- La percentuale di file che includono soggetti dati, determinata da identificatori nazionali come ID nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di severità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%

Punteggio di severità	Logica
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono più grandi del 6%
7	Tre delle variabili sono più grandi del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono più grandi del 15%
10	Tre delle variabili sono più grandi del 15%

Risposta a una richiesta di accesso soggetto a dati

Rispondere a una richiesta di accesso soggetto a dati (DSAR) cercando il nome completo o l'identificatore noto di un soggetto (ad esempio un indirizzo e-mail) e scaricando un report. Il report è stato progettato per aiutare l'organizzazione a rispettare il GDPR o leggi simili sulla privacy dei dati.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Che cos'è una richiesta di accesso ai dati?

Le normative sulla privacy, come il GDPR europeo, concedono ai soggetti interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, queste vengono denominate DSAR (data subject access request). Le organizzazioni devono rispondere a queste richieste "senza ritardi indebito" e al più tardi entro un mese dalla ricezione.

In che modo la Cloud Compliance può aiutarti a rispondere a una DSAR?

Quando esegui una ricerca dell'oggetto dati, Cloud Compliance trova tutti i file che contengono il nome o l'identificatore della persona. Cloud Compliance verifica i dati pre-indicizzati più recenti per il nome o l'identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l'elenco dei file o un report Data Subject Access Request. Il report aggrega le informazioni dei dati e le inserisce in termini legali che è possibile inviare alla persona.

Ricerca di dati e download di report

Cercare il nome completo o l'identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a. "qualsiasi tipo di informazione personale".

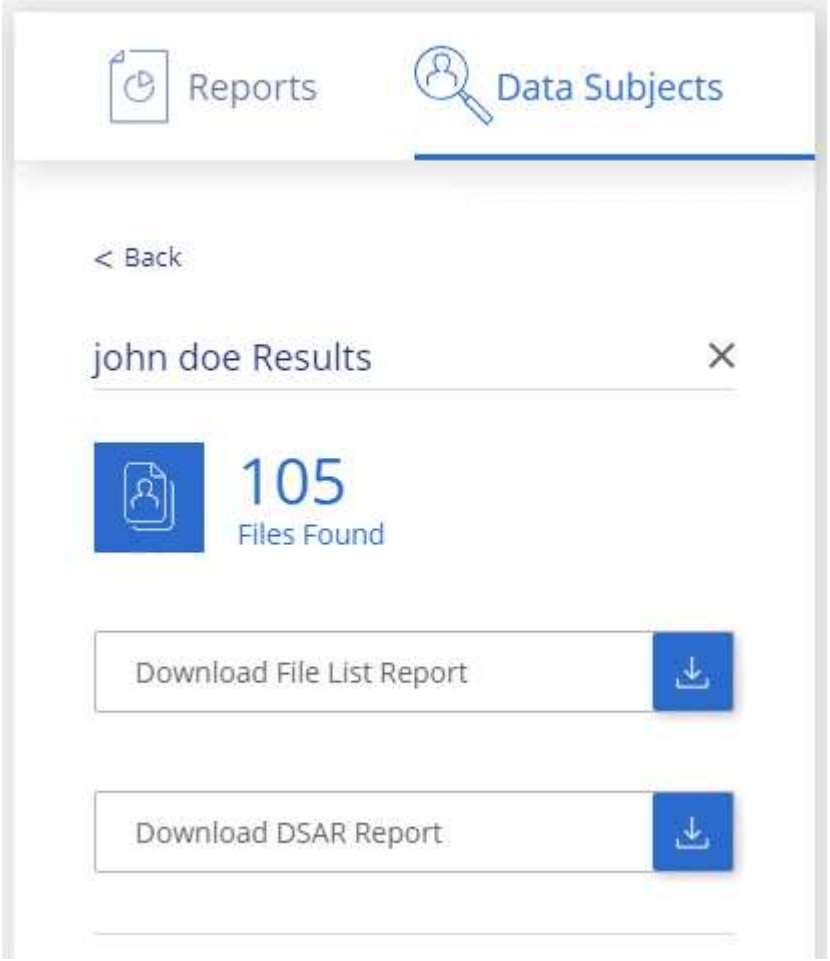
Quando si ricercano i nomi dei soggetti dati, è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Compliance**.

2. Fare clic su **Data subjects**.
3. Cercare il nome completo o l'identificativo noto dell'interessato.

   Ecco un esempio che mostra una ricerca per il nome *john Doe*:



4. Scegliere una delle opzioni disponibili:
   - **Download file List Report**: Un elenco dei file che contengono informazioni sull'oggetto dei dati.

     Se sono presenti più di 10,000 risultati, nel report vengono visualizzati solo i primi 10,000 risultati (il supporto per altri verrà aggiunto in seguito).

   - **Download del report DSAR**: Una risposta formale alla richiesta di accesso che è possibile inviare al soggetto interessato. Questo report contiene informazioni generate automaticamente in base ai dati rilevati dalla Cloud Compliance nell'oggetto dei dati ed è progettato per essere utilizzato come modello. Completare il modulo e esaminarlo internamente prima di inviarlo al soggetto interessato.

Disattivazione della conformità al cloud

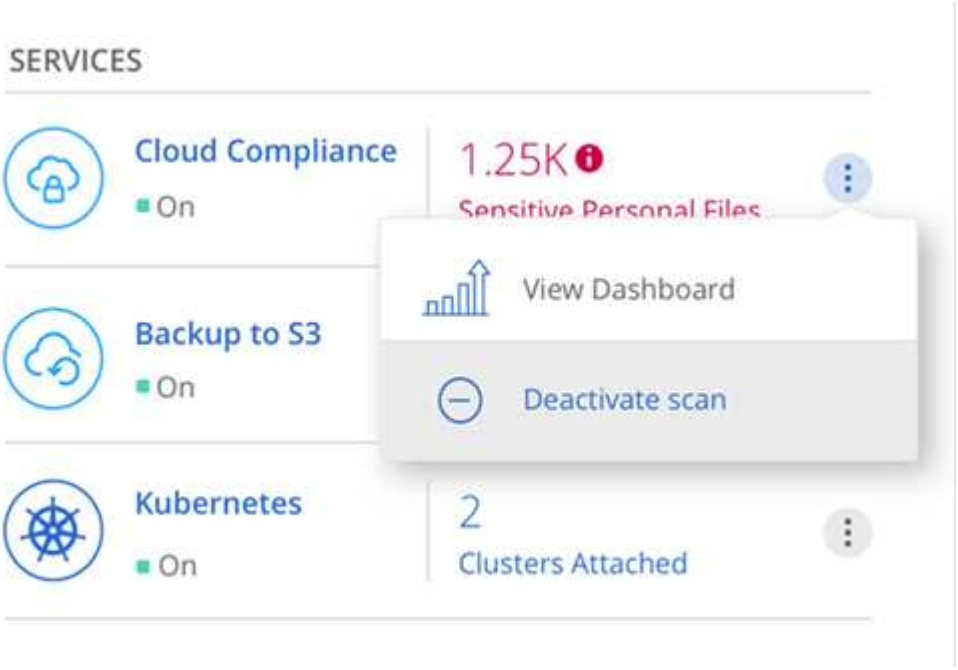
Se necessario, puoi impedire alla conformità cloud di eseguire la scansione di uno o più ambienti di lavoro. Puoi anche eliminare l'istanza di conformità cloud se non desideri più utilizzare la conformità cloud con i tuoi sistemi Cloud Volumes ONTAP.

Disattivazione delle scansioni di compliance per un ambiente di lavoro

Quando si disattivano le scansioni, Cloud Compliance non esegue più la scansione dei dati sul sistema e rimuove le informazioni indicizzate sulla compliance dall'istanza Cloud Compliance (i dati dell'ambiente di lavoro stesso non vengono cancellati).

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare l'ambiente di lavoro.
3. Nel pannello di destra, fare clic sull'icona dell'azione relativa al servizio Cloud Compliance e selezionare **Disattiva scansione**.



Eliminazione dell'istanza di Cloud Compliance

Se non si desidera più utilizzare la conformità cloud con Cloud Volumes ONTAP, è possibile eliminare l'istanza di conformità cloud. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati.

Fase

1. Accedere alla console del provider di servizi cloud ed eliminare l'istanza Cloud Compliance.

   L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

Domande frequenti sulla conformità al cloud

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Che cos'è la conformità al cloud?

Cloud Compliance è una nuova offerta cloud di NetApp. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili nei sistemi Cloud Volumes ONTAP ospitati in AWS o Azure.

Cloud Compliance offre parametri predefiniti (ad esempio tipi e categorie di informazioni sensibili) per soddisfare le nuove normative sulla conformità dei dati per la privacy e la sensibilità dei dati, come GDPR, CCPA e altro ancora.

Perché dovrei utilizzare Cloud Compliance?

La conformità al cloud può aiutarti con i dati per aiutarti a:

- Rispettare le normative sulla privacy e sulla conformità dei dati.
- Rispettare le policy di conservazione dei dati.
- Individuare e creare report su dati specifici in risposta a soggetti interessati, come richiesto dal GDPR, dal CCPA e da altre normative sulla privacy dei dati.

Quali sono i casi di utilizzo più comuni per la conformità al cloud?

- Identificare le informazioni personali identificabili (PII).
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR e CCPA.
- Rispettare le nuove e future normative sulla privacy dei dati.

"Scopri di più sui casi di utilizzo per la conformità al cloud".

Quali tipi di dati è possibile sottoporre a scansione con la conformità al cloud?

Cloud Compliance supporta la scansione di dati non strutturati su protocolli NFS e CIFS. Attualmente, la conformità al cloud esegue la scansione dei dati gestiti da Cloud Volumes ONTAP.

"Scopri come funzionano le scansioni".

Quali cloud provider sono supportati?

Cloud Compliance opera come parte di Cloud Manager e attualmente supporta AWS e Azure. In questo modo, la tua organizzazione potrà ottenere una visibilità unificata della privacy tra diversi cloud provider. Il supporto per Google Cloud Platform (GCP) verrà aggiunto a breve.

Come posso accedere alla conformità cloud?

La conformità al cloud viene gestita e gestita tramite Cloud Manager. Puoi accedere alle funzionalità Cloud Compliance dalla scheda **Compliance** di Cloud Manager.

Come funziona Cloud Compliance?

La conformità al cloud implementa un altro livello di intelligenza artificiale insieme al sistema Cloud Manager e alle istanze di Cloud Volumes ONTAP. Quindi, esegue la scansione dei dati su Cloud Volumes ONTAP e indicizza le informazioni rilevate.

"Scopri di più sul funzionamento della conformità al cloud".

Quanto costa la Cloud Compliance?

La conformità al cloud viene offerta come parte di Cloud Volumes ONTAP e non richiede costi aggiuntivi. In futuro potrebbero essere necessari costi aggiuntivi per le funzionalità personalizzate.

La conformità al cloud richiede l'implementazione di un'istanza nel tuo cloud provider, per la quale ti verrà addebitato il costo del tuo cloud provider.

Con quale frequenza la Cloud Compliance esegue la scansione dei miei dati?

I dati cambiano di frequente, pertanto la conformità del cloud esegue una scansione continua dei dati senza alcun impatto sui dati. Anche se la scansione iniziale dei dati potrebbe richiedere più tempo, le scansioni successive eseguono solo la scansione delle modifiche incrementali, riducendo i tempi di scansione del sistema.

"Scopri come funzionano le scansioni".

Cloud Compliance offre report?

Sì. Le informazioni offerte dalla Cloud Compliance possono essere rilevanti per gli altri stakeholder delle tue organizzazioni, pertanto ti consentiamo di generare report per condividere le informazioni.

Per la conformità al cloud sono disponibili i seguenti report:

Report sulla valutazione dei rischi per la privacy
: Fornisce informazioni sulla privacy dai dati e un punteggio di rischio per la privacy. "Scopri di più".

Report Data Subject Access Request
: Consente di estrarre un report di tutti i file che contengono informazioni relative al nome specifico o all'identificativo personale di un soggetto. "Scopri di più".

Report su un tipo di informazioni specifico
: Sono disponibili report che includono dettagli sui file identificati che contengono dati personali e dati personali sensibili. È inoltre possibile visualizzare i file suddivisi per categoria e tipo di file. "Scopri di più".

Quale tipo di istanza o macchina virtuale è richiesto per la conformità al cloud?

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco io1 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

"Scopri di più sul funzionamento della conformità al cloud".

Le prestazioni di scansione variano?

Le performance di scansione possono variare in base alla larghezza di banda della rete e alle dimensioni medie dei file nel tuo ambiente cloud.

Come posso abilitare la conformità al cloud?

Puoi abilitare la conformità al cloud quando crei un nuovo ambiente di lavoro. È possibile abilitarla negli ambienti di lavoro esistenti dalla scheda **Compliance** (solo alla prima attivazione) o selezionando un ambiente di lavoro specifico.

"Scopri come iniziare".

L'attivazione della conformità cloud comporta una scansione iniziale immediata. I risultati della compliance vengono visualizzati poco dopo.

Come si disattiva la conformità al cloud?

Dopo aver selezionato un singolo ambiente di lavoro, è possibile disattivare Cloud Compliance dalla pagina Working Environments (ambienti di lavoro).

"Scopri di più".

Per rimuovere completamente l'istanza di Cloud Compliance, puoi rimuovere manualmente l'istanza di Cloud Compliance dal portale del tuo cloud provider.

Cosa succede se il tiering dei dati è attivato su Cloud Volumes ONTAP?

Potresti voler abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP che esegue il Tier dei dati cold sullo storage a oggetti. Se il tiering dei dati è attivato, Cloud Compliance esegue la scansione di tutti i dati presenti sui dischi e cold data tiered in storage a oggetti.

La scansione di compliance non riscalda i dati cold, ma rimane fredda e viene tierata per lo storage a oggetti.

Posso utilizzare la conformità al cloud per eseguire la scansione dello storage ONTAP on-premise?

No La conformità al cloud è attualmente disponibile come parte di Cloud Manager e supporta Cloud Volumes ONTAP. Stiamo pianificando di supportare la conformità al cloud con offerte cloud aggiuntive come Cloud Volumes Service e Azure NetApp Files.

Cloud Compliance può inviare notifiche alla mia organizzazione?

No, ma è possibile scaricare i report di stato che è possibile condividere internamente all'organizzazione.

Posso personalizzare il servizio in base alle esigenze della mia organizzazione?

La conformità al cloud offre informazioni pronte all'uso ai tuoi dati. Queste informazioni possono essere estratte e utilizzate per le esigenze della tua organizzazione.

Posso limitare le informazioni sulla conformità al cloud a utenti specifici?

Sì, la conformità del cloud è completamente integrata con Cloud Manager. Gli utenti di Cloud Manager possono visualizzare le informazioni solo per gli ambienti di lavoro che possono visualizzare in base ai privilegi dell'area di lavoro.

"Scopri di più".

Amministrare Cloud Volumes ONTAP

Connessione a Cloud Volumes ONTAP

Se è necessario eseguire una gestione avanzata di Cloud Volumes ONTAP, è possibile farlo utilizzando Gestione di sistema di OnCommand o l'interfaccia della riga di comando.

Connessione a Gestore di sistema di OnCommand

Potrebbe essere necessario eseguire alcune attività di Cloud Volumes ONTAP da Gestore di sistema di OnCommand, uno strumento di gestione basato su browser che viene eseguito sul sistema Cloud Volumes ONTAP. Ad esempio, se si desidera creare LUN, è necessario utilizzare System Manager.

Prima di iniziare

Il computer da cui si accede a Cloud Manager deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario effettuare l'accesso a Cloud Manager da un host jump in AWS o Azure.

> Quando vengono implementate in più zone di disponibilità AWS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

Fasi

1. Dalla pagina ambienti di lavoro, fare doppio clic sul sistema Cloud Volumes ONTAP che si desidera gestire con Gestione sistema.
2. Fare clic sull'icona del menu, quindi fare clic su **Advanced > System Manager**.
3. Fare clic su **Avvia**.

   System Manager viene caricato in una nuova scheda del browser.

4. Nella schermata di accesso, inserire **admin** nel campo User Name (Nome utente), immettere la password specificata al momento della creazione dell'ambiente di lavoro, quindi fare clic su **Sign in** (Accedi).

Risultato

Viene caricata la console di System Manager. Ora puoi utilizzarlo per gestire Cloud Volumes ONTAP.

Connessione all'interfaccia utente di Cloud Volumes ONTAP

La CLI di Cloud Volumes ONTAP consente di eseguire tutti i comandi amministrativi ed è una buona scelta per attività avanzate o se si è più comodi nell'utilizzo della CLI. È possibile connettersi all'interfaccia CLI utilizzando Secure Shell (SSH).

Prima di iniziare

L'host da cui si utilizza SSH per connettersi a Cloud Volumes ONTAP deve disporre di una connessione di rete a Cloud Volumes ONTAP. Ad esempio, potrebbe essere necessario utilizzare SSH da un host jump in AWS o Azure.

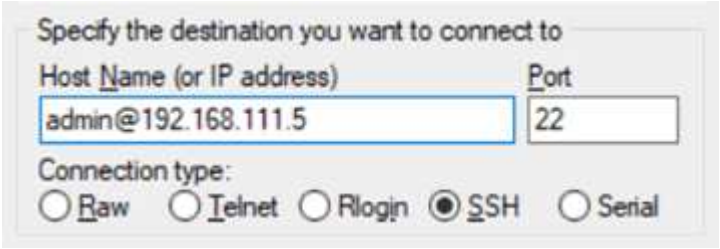
Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

Fasi

1. In Cloud Manager, identificare l'indirizzo IP dell'interfaccia di gestione del cluster:
   a. Nella pagina ambienti di lavoro, selezionare il sistema Cloud Volumes ONTAP.
   b. Copiare l'indirizzo IP di gestione del cluster visualizzato nel riquadro di destra.
2. Utilizzare SSH per connettersi all'indirizzo IP dell'interfaccia di gestione del cluster utilizzando l'account admin.

   Esempio

   L'immagine seguente mostra un esempio di utilizzo di PuTTY:

3. Al prompt di login, inserire la password per l'account admin.

   Esempio

   ```
   Password: ********
   COT2::>
   ```

Aggiornamento del software Cloud Volumes ONTAP

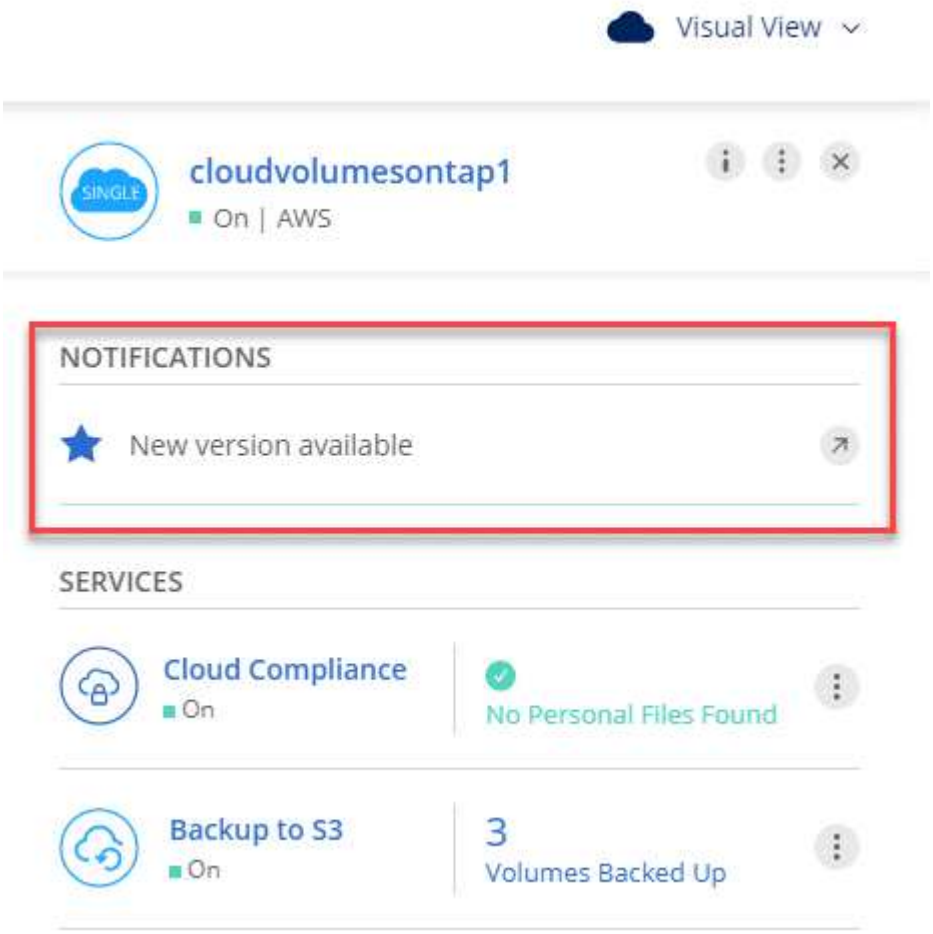
Cloud Manager include diverse opzioni che è possibile utilizzare per eseguire l'aggiornamento alla release corrente di Cloud Volumes ONTAP o per eseguire il downgrade di Cloud Volumes ONTAP a una release precedente. È necessario preparare i sistemi Cloud Volumes ONTAP prima di aggiornare o eseguire il downgrade del software.

Gli aggiornamenti software devono essere completati da Cloud Manager

Gli aggiornamenti di Cloud Volumes ONTAP devono essere completati da Cloud Manager. Non aggiornare Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI. In questo modo si può influire sulla stabilità del sistema.

Metodi per aggiornare Cloud Volumes ONTAP

Cloud Manager visualizza una notifica negli ambienti di lavoro Cloud Volumes ONTAP quando è disponibile una nuova versione di Cloud Volumes ONTAP:



È possibile avviare il processo di aggiornamento da questa notifica, che automatizza il processo ottenendo l'immagine software da un bucket S3, installando l'immagine e riavviando il sistema. Per ulteriori informazioni, vedere Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager.

Per i sistemi ha in AWS, Cloud Manager potrebbe aggiornare il mediatore ha come parte del processo di aggiornamento.

Opzioni avanzate per gli aggiornamenti software

Cloud Manager offre inoltre le seguenti opzioni avanzate per l'aggiornamento del software Cloud Volumes ONTAP:

- Aggiornamenti software utilizzando un'immagine su un URL esterno

  Questa opzione è utile se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software, se è stata fornita una patch o se si desidera eseguire il downgrade del software a una versione specifica.

  Per ulteriori informazioni, vedere Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP.

- Aggiornamenti software utilizzando l'immagine alternativa sul sistema

  È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente, rendendo l'immagine software alternativa l'immagine predefinita. Questa opzione non è disponibile per le coppie ha.

  Per ulteriori informazioni, vedere Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale.

Preparazione all'aggiornamento del software Cloud Volumes ONTAP

Prima di eseguire un upgrade o un downgrade, è necessario verificare che i sistemi siano pronti ed eseguire le modifiche di configurazione richieste.

- Pianificazione del downtime
- Revisione dei requisiti di versione
- Verificare che il giveback automatico sia ancora attivato
- Sospensione dei trasferimenti SnapMirror
- Verificare che gli aggregati siano online

Pianificazione del downtime

Quando si aggiorna un sistema a nodo singolo, il processo di aggiornamento porta il sistema offline per un massimo di 25 minuti, durante i quali l'i/o viene interrotto.

L'aggiornamento di una coppia ha è senza interruzioni e l'i/o è ininterrotto. Durante questo processo di aggiornamento senza interruzioni, ogni nodo viene aggiornato in tandem per continuare a fornire i/o ai client.

Revisione dei requisiti di versione

La versione di ONTAP che è possibile aggiornare o eseguire il downgrade varia in base alla versione di ONTAP attualmente in esecuzione nel sistema.

Per informazioni sui requisiti di versione, fare riferimento a. "Documentazione di ONTAP 9: Requisiti per l'aggiornamento del cluster".

Verificare che il giveback automatico sia ancora attivato

Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

"Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

Sospensione dei trasferimenti SnapMirror

Se un sistema Cloud Volumes ONTAP dispone di relazioni SnapMirror attive, si consiglia di sospendere i trasferimenti prima di aggiornare il software Cloud Volumes ONTAP. La sospensione dei trasferimenti impedisce gli errori di SnapMirror. È necessario sospendere i trasferimenti dal sistema di destinazione.

A proposito di questa attività

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

Fasi

1. "Accedere a System Manager" dal sistema di destinazione.
2. Fare clic su **protezione > Relazioni**.
3. Selezionare la relazione e fare clic su **operazioni > Quiesce**.

Verificare che gli aggregati siano online

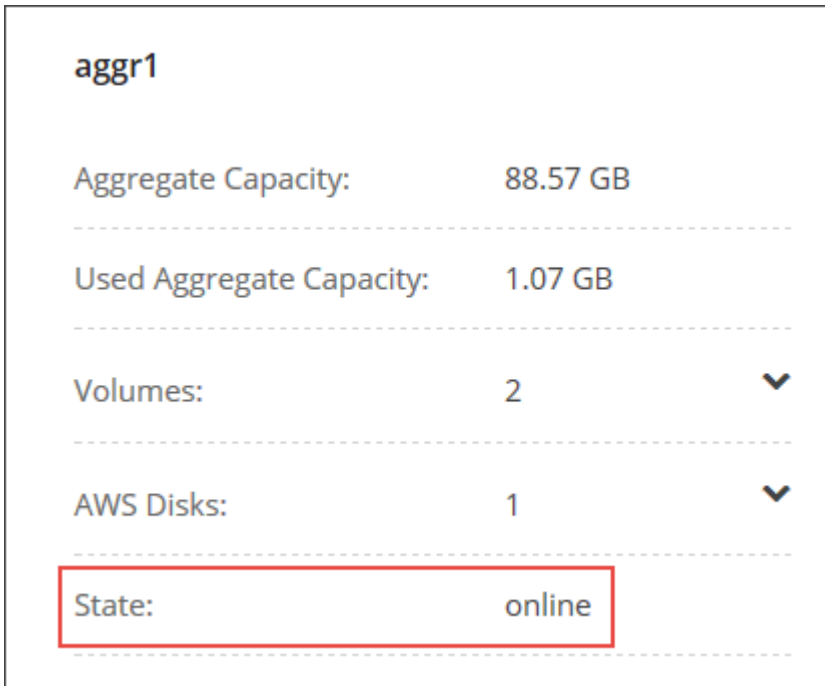
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

A proposito di questa attività

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

Fasi

1. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
2. Selezionare un aggregato, fare clic su **Info**, quindi verificare che lo stato sia online.



3. Se l'aggregato non è in linea, utilizzare System Manager per portare l'aggregato online:
   a. "Accedere a System Manager".
   b. Fare clic su **Storage > Aggregates & Disks > Aggregates**.
   c. Selezionare l'aggregato, quindi fare clic su **altre azioni > Stato > Online**.

Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager

Cloud Manager ti avvisa quando è disponibile una nuova versione di Cloud Volumes ONTAP. Fare clic sulla notifica per avviare il processo di aggiornamento.

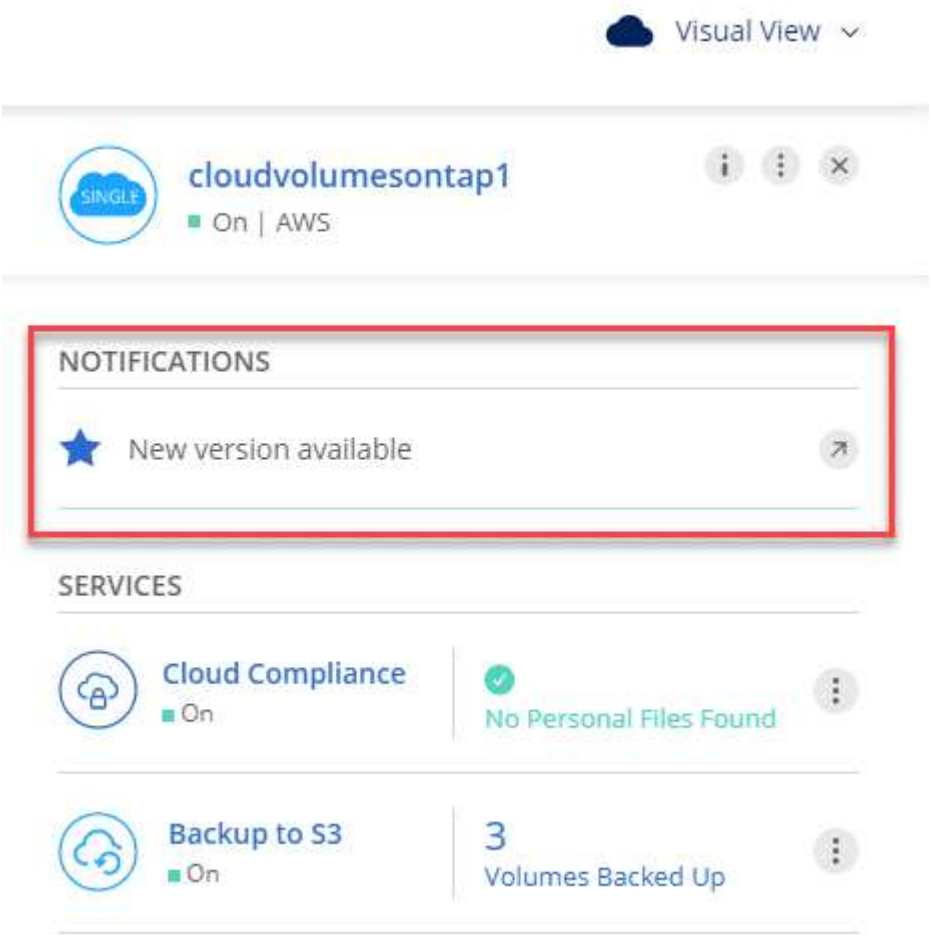
Prima di iniziare

Le operazioni di Cloud Manager, come la creazione di volumi o aggregati, non devono essere in corso per il sistema Cloud Volumes ONTAP.

Fasi

1. Fare clic su **ambienti di lavoro**.
2. Selezionare un ambiente di lavoro.

   Se è disponibile una nuova versione, nel riquadro di destra viene visualizzata una notifica:



3. Se è disponibile una nuova versione, fare clic su **Upgrade** (Aggiorna).
4. Nella pagina Release Information (informazioni sulla release), fare clic sul collegamento per leggere le Note sulla release per la versione specificata, quindi selezionare la casella di controllo **ho letto…**.
5. Nella pagina del Contratto di licenza con l'utente finale (EULA), leggere il Contratto e selezionare **i Read and Approve the EULA** (Leggi e approva il Contratto di licenza con l'utente finale).
6. Nella pagina Review and Approve (esamina e approva), leggere le note importanti, selezionare **i cape…**, quindi fare clic su **Go**.

Risultato

Cloud Manager avvia l'aggiornamento del software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP

È possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP e avviare l'aggiornamento software da Cloud Manager. È possibile utilizzare questa opzione se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software o se si desidera eseguire il downgrade del software.

Fasi

1. Configurare un server HTTP o FTP in grado di ospitare l'immagine del software Cloud Volumes ONTAP.
2. Se si dispone di una connessione VPN alla rete virtuale, è possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP nella propria rete. In caso contrario, è necessario posizionare il file su un server HTTP o FTP nel cloud.
3. Se si utilizza il proprio gruppo di protezione per Cloud Volumes ONTAP, assicurarsi che le regole in uscita consentano connessioni HTTP o FTP in modo che Cloud Volumes ONTAP possa accedere all'immagine software.

   Per impostazione predefinita, il gruppo di protezione Cloud Volumes ONTAP predefinito consente le connessioni HTTP e FTP in uscita.

4. Ottenere l'immagine software da "Il sito di supporto NetApp".
5. Copiare l'immagine del software nella directory del server HTTP o FTP da cui verrà servito il file.
6. Dall'ambiente di lavoro in Cloud Manager, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
7. Nella pagina di aggiornamento del software, scegliere **selezionare un'immagine disponibile da un URL**, immettere l'URL, quindi fare clic su **Cambia immagine**.
8. Fare clic su **Procedi** per confermare.

Risultato

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale

La transizione di Cloud Volumes ONTAP a una release precedente nella stessa famiglia di release (ad esempio, da 9.5 a 9.4) viene definita downgrade. È possibile eseguire il downgrade senza assistenza durante il downgrade di cluster nuovi o di test, ma è necessario contattare il supporto tecnico se si desidera eseguire il downgrade di un cluster di produzione.

Ogni sistema Cloud Volumes ONTAP può contenere due immagini software: L'immagine corrente in esecuzione e un'immagine alternativa che è possibile avviare. Cloud Manager può modificare l'immagine alternativa in modo che sia l'immagine predefinita. È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente di Cloud Volumes ONTAP, in caso di problemi con l'immagine corrente.

A proposito di questa attività

Questo processo di downgrade è disponibile solo per sistemi Cloud Volumes ONTAP singoli. Non è disponibile per le coppie ha.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
2. Nella pagina di aggiornamento del software, selezionare l'immagine alternativa, quindi fare clic su **Cambia immagine**.
3. Fare clic su **Procedi** per confermare.

Risultato

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Modifica dei sistemi Cloud Volumes ONTAP

Potrebbe essere necessario modificare la configurazione delle istanze di Cloud Volumes ONTAP in base alle esigenze di storage. Ad esempio, è possibile passare da una configurazione pay-as-you-go all'altra, modificare l'istanza o il tipo di macchina virtuale e passare a un abbonamento alternativo.

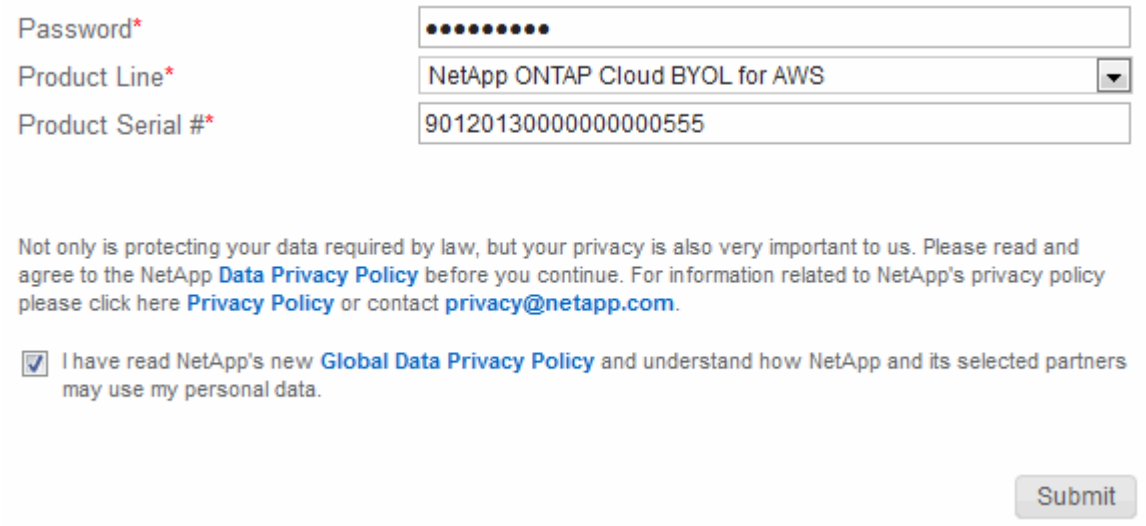
Installazione dei file di licenza sui sistemi Cloud Volumes ONTAP BYOL

Se Cloud Manager non riesce a ottenere un file di licenza BYOL da NetApp, è possibile ottenerlo da solo e caricarlo manualmente in Cloud Manager in modo che possa installare la licenza sul sistema Cloud Volumes ONTAP.

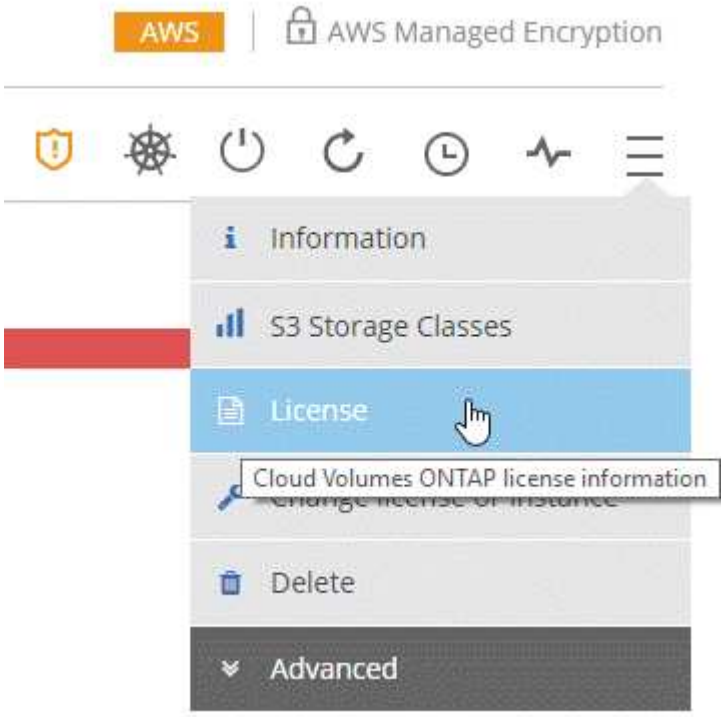
Fasi

1. Accedere alla "NetApp License file Generator" Ed effettua l'accesso utilizzando le credenziali del sito di supporto NetApp.
2. Inserire la password, scegliere il prodotto, inserire il numero di serie, confermare di aver letto e accettato l'informativa sulla privacy, quindi fare clic su **Invia**.

Esempio



3. Scegliere se si desidera ricevere il file serialnumber.NLF JSON tramite e-mail o download diretto.
4. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
5. Fare clic sull'icona del menu, quindi su **licenza**.



6. Fare clic su **carica file di licenza**.
7. Fare clic su **Upload**, quindi selezionare il file.

Risultato

Cloud Manager installa il nuovo file di licenza sul sistema Cloud Volumes ONTAP.

Modifica dell'istanza o del tipo di macchina per Cloud Volumes ONTAP

Quando si avvia Cloud Volumes ONTAP in AWS, Azure o GCP, è possibile scegliere tra diversi tipi di istanze o computer. È possibile modificare l'istanza o il tipo di macchina in qualsiasi momento se si determina che è sottodimensionato o sovradimensionato per le proprie esigenze.

A proposito di questa attività

- Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

  "Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Se si utilizza una configurazione pay-as-you-go, è possibile scegliere una licenza diversa.
3. Selezionare un'istanza o un tipo di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Passaggio da una configurazione pay-as-you-go all'altra

Dopo aver lanciato i sistemi Cloud Volumes ONTAP pay-as-you-go, è possibile passare da una configurazione Explore a una configurazione standard e a una configurazione Premium in qualsiasi momento modificando la licenza. La modifica della licenza aumenta o diminuisce il limite di capacità raw e consente di scegliere tra diversi tipi di istanze AWS o tipi di macchine virtuali Azure.

In GCP, è disponibile un singolo tipo di macchina per ogni configurazione pay-as-you-go. Non è possibile scegliere tra diversi tipi di computer.

A proposito di questa attività

Tenere presente quanto segue circa il passaggio da una licenza pay-as-you-go all'altra:

- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Selezionare un tipo di licenza e un tipo di istanza o di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova licenza, il tipo di istanza o il tipo di macchina o entrambi.

Passaggio a una configurazione Cloud Volumes ONTAP alternativa

Se si desidera passare da un abbonamento pay-as-you-go a un abbonamento BYOL o tra un singolo sistema Cloud Volumes ONTAP e una coppia ha, è possibile implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

Fasi

1. Creare un nuovo ambiente di lavoro Cloud Volumes ONTAP.

   "Avvio di Cloud Volumes ONTAP in AWS"
   "Lancio di Cloud Volumes ONTAP in Azure"

"Avvio di Cloud Volumes ONTAP in GCP"

2. "Configurare la replica dei dati una tantum" tra i sistemi per ciascun volume da replicare.
3. Terminare il sistema Cloud Volumes ONTAP di cui non si ha più bisogno "eliminazione dell'ambiente di lavoro originale".

Modifica dell'abbonamento a AWS Marketplace

Modificare l'abbonamento AWS Marketplace per il sistema Cloud Volumes ONTAP se si desidera modificare l'account AWS da cui si riceve l'addebito.

Fasi

1. Se non l'hai ancora fatto, Aggiungi un nuovo abbonamento da "L'offerta Cloud Manager in AWS Marketplace".
2. Dall'ambiente di lavoro in Cloud Manager, fare clic sull'icona del menu, quindi su **Marketplace Subscription**.
3. Selezionare un abbonamento dall'elenco a discesa.
4. Fare clic su **Save** (Salva).

Modifica della velocità di scrittura su normale o alta

La velocità di scrittura predefinita per Cloud Volumes ONTAP è normale. È possibile passare a un'elevata velocità di scrittura se sono richieste prestazioni di scrittura rapide per il carico di lavoro. Prima di modificare la velocità di scrittura, è necessario "comprendere le differenze tra le impostazioni normali e quelle alte".

A proposito di questa attività

- Assicurarsi che operazioni come la creazione di volumi o aggregati non siano in corso.
- Tenere presente che questa modifica riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > Writing Speed** (Avanzate > velocità di scrittura).
2. Selezionare **normale** o **alta**.

   Se scegli High, allora devi leggere il messaggio "capisco…" e confermare selezionando la casella.

3. Fare clic su **Save** (Salva), controllare il messaggio di conferma, quindi fare clic su **Proceed** (Procedi).

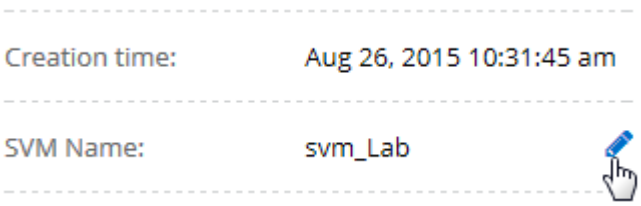
Modifica del nome della macchina virtuale di storage

Cloud Manager assegna automaticamente un nome alla macchina virtuale di storage (SVM) per Cloud Volumes ONTAP. È possibile modificare il nome della SVM se si dispone di standard di denominazione rigorosi. Ad esempio, è possibile che corrisponda al nome delle SVM per i cluster ONTAP.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **informazioni**.

2. Fare clic sull'icona di modifica a destra del nome SVM.



3. Nella finestra di dialogo Modify SVM Name (Modifica nome SVM), modificare il nome SVM, quindi fare clic su **Save** (Salva).

Modifica della password per Cloud Volumes ONTAP

Cloud Volumes ONTAP include un account di amministrazione del cluster. Se necessario, puoi modificare la password per questo account da Cloud Manager.

> Non modificare la password per l'account admin tramite System Manager o CLI. La password non verrà riflessa in Cloud Manager. Di conseguenza, Cloud Manager non è in grado di monitorare correttamente l'istanza.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Imposta password**.
2. Inserire due volte la nuova password, quindi fare clic su **Save** (Salva).

   La nuova password deve essere diversa da una delle ultime sei password utilizzate.

Modifica della MTU di rete per istanze di grandi dimensioni c4.4x4 e c4.8x

Per impostazione predefinita, Cloud Volumes ONTAP è configurato per l'utilizzo di 9,000 MTU (detti anche frame jumbo) quando si sceglie l'istanza c4.4xlarge o l'istanza c4.8xlarge in AWS. È possibile modificare l'MTU di rete a 1,500 byte, se più appropriato per la configurazione di rete.

A proposito di questa attività

Un'unità MTU (Network Maximum Transmission Unit) di 9,000 byte può fornire il massimo throughput di rete possibile per configurazioni specifiche.

9,000 MTU è una buona scelta se i client nello stesso VPC comunicano con il sistema Cloud Volumes ONTAP e alcuni o tutti questi client supportano anche 9,000 MTU. Se il traffico lascia il VPC, può verificarsi la frammentazione dei pacchetti, che peggiora le performance.

Una MTU di rete di 1,500 byte è una buona scelta se client o sistemi esterni al VPC comunicano con il sistema Cloud Volumes ONTAP.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > Network Utilization** (Avanzate > utilizzo rete).
2. Selezionare **Standard** o **Jumbo Frame**.
3. Fare clic su **Cambia**.

Modifica delle tabelle di percorso associate alle coppie ha in più AWS AZS

È possibile modificare le tabelle di routing AWS che includono i percorsi verso gli indirizzi IP mobili per una coppia ha. È possibile eseguire questa operazione se i nuovi client NFS o CIFS devono accedere a una coppia ha in AWS.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **informazioni**.
2. Fare clic su **Route Tables**.
3. Modificare l'elenco delle tabelle di percorso selezionate, quindi fare clic su **Save** (Salva).

Risultato

Cloud Manager invia una richiesta AWS per modificare le tabelle di routing.

Gestione dello stato di Cloud Volumes ONTAP

Puoi arrestare e avviare Cloud Volumes ONTAP da Cloud Manager per gestire i costi di calcolo del cloud.

Pianificazione degli arresti automatici di Cloud Volumes ONTAP

Per ridurre i costi di calcolo, potrebbe essere necessario arrestare Cloud Volumes ONTAP durante intervalli di tempo specifici. Invece di eseguire questa operazione manualmente, è possibile configurare Cloud Manager in modo che arresti e riavvii automaticamente i sistemi in orari specifici.

A proposito di questa attività

Quando si pianifica un arresto automatico del sistema Cloud Volumes ONTAP, Cloud Manager posticipa l'arresto se è in corso un trasferimento di dati attivo. Cloud Manager arresta il sistema al termine del trasferimento.

Questa attività pianifica gli arresti automatici di entrambi i nodi in una coppia ha.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona dell'orologio:

2. Specificare il programma di arresto:

   a. Scegliere se si desidera spegnere il sistema ogni giorno, ogni giorno feriale, ogni fine settimana o qualsiasi combinazione delle tre opzioni.

   b. Specificare quando si desidera spegnere il sistema e per quanto tempo si desidera disattivarlo.

      Esempio

      La seguente immagine mostra un programma che indica a Cloud Manager di spegnere il sistema ogni sabato alle 12:00 per 48 ore. Cloud Manager riavvia il sistema ogni lunedì alle 12:00

3. Fare clic su **Save** (Salva).

Risultato

Cloud Manager salva la pianificazione. L'icona dell'orologio cambia per indicare che è stata impostata una pianificazione: 

Arresto di Cloud Volumes ONTAP

L'arresto di Cloud Volumes ONTAP consente di risparmiare sui costi di calcolo e di creare snapshot dei dischi root e di boot, che possono essere utili per la risoluzione dei problemi.

A proposito di questa attività

Quando si interrompe una coppia ha, Cloud Manager arresta entrambi i nodi.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona **Spegni**.

2. Mantenere l'opzione per creare snapshot abilitata, in quanto le snapshot possono abilitare il ripristino del sistema.
3. Fare clic su **Spegni**.

   L'arresto del sistema può richiedere fino a qualche minuto. È possibile riavviare i sistemi in un secondo momento dalla pagina ambiente di lavoro.

Monitoraggio dei costi delle risorse AWS

Cloud Manager consente di visualizzare i costi delle risorse associati all'esecuzione di Cloud Volumes ONTAP in AWS. Puoi anche vedere quanto denaro hai risparmiato utilizzando le funzionalità di NetApp che possono ridurre i costi di storage.

A proposito di questa attività

Cloud Manager aggiorna i costi quando aggiorni la pagina. Fare riferimento ad AWS per i dettagli sui costi finali.

Fase

1. Verificare che Cloud Manager possa ottenere informazioni sui costi da AWS:
   a. Assicurarsi che il criterio IAM che fornisce le autorizzazioni a Cloud Manager includa le seguenti azioni:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Queste azioni sono incluse nella versione più recente "Policy di Cloud Manager". I nuovi sistemi implementati da NetApp Cloud Central includono automaticamente queste autorizzazioni.

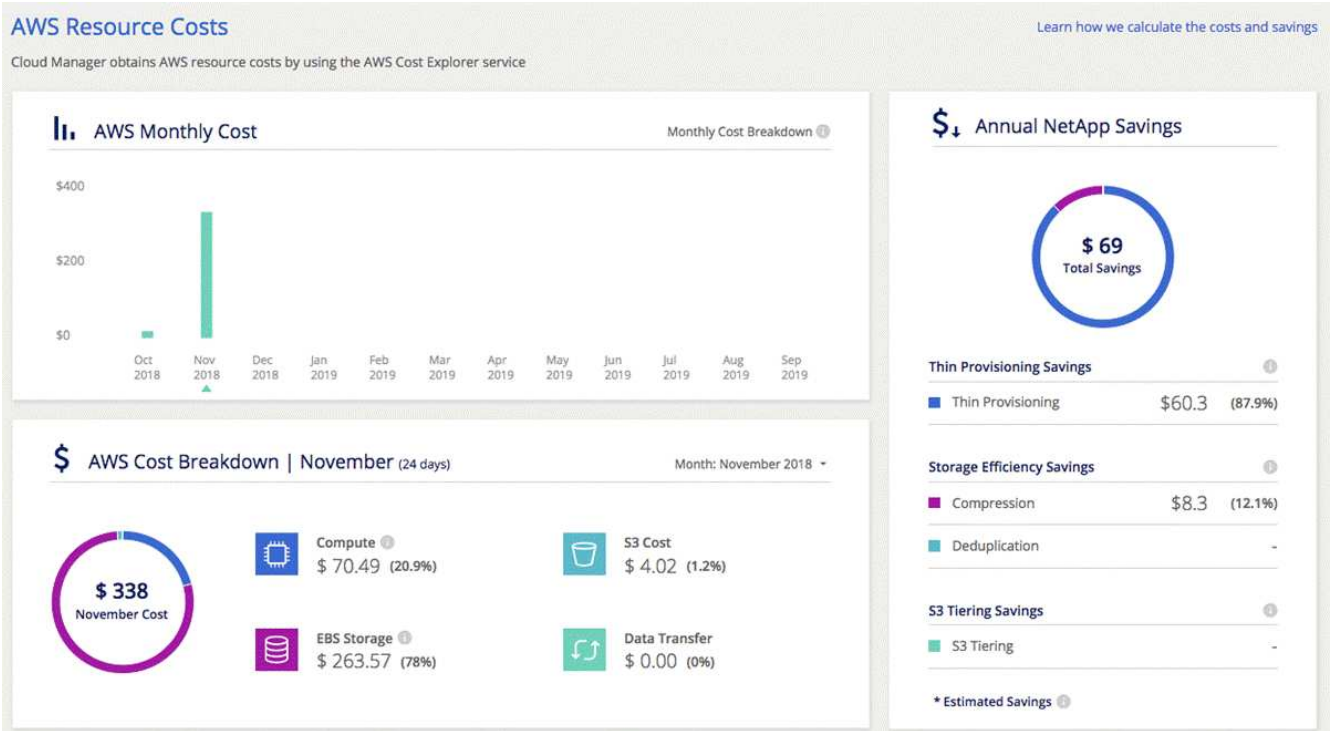
   b. "Attivare il tag **WorkingEnvironmentId**".

      Per tenere traccia dei costi AWS, Cloud Manager assegna un tag di allocazione dei costi alle istanze di Cloud Volumes ONTAP. Dopo aver creato il primo ambiente di lavoro, attivare il tag **WorkingEnvironmentId**. I tag definiti dall'utente non vengono visualizzati nei report di fatturazione AWS finché non vengono attivati nella console di fatturazione e gestione dei costi.

2. Nella pagina Working Environments (ambienti di lavoro), selezionare un ambiente di lavoro Cloud Volumes ONTAP e fare clic su **Cost** (costo).

   La pagina dei costi visualizza i costi per i mesi correnti e precedenti e mostra i risparmi annuali di NetApp, se hai abilitato le funzionalità di risparmio sui volumi di NetApp.

   La seguente immagine mostra una pagina di costo di esempio:

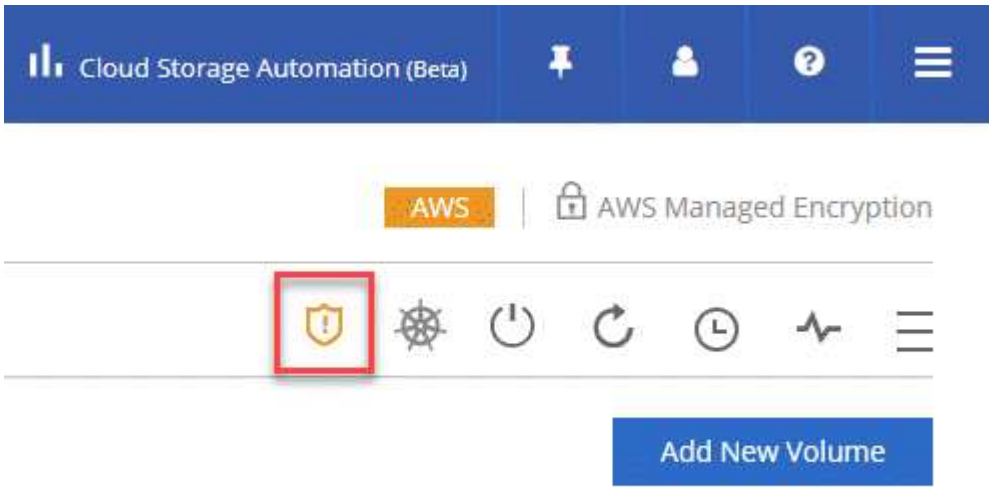


Miglioramento della protezione contro ransomware

Gli attacchi ransomware possono costare tempo di business, risorse e reputazione. Cloud Manager consente di implementare la soluzione NetApp per ransomware, che fornisce strumenti efficaci per visibilità, rilevamento e risoluzione dei problemi.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona **ransomware**.

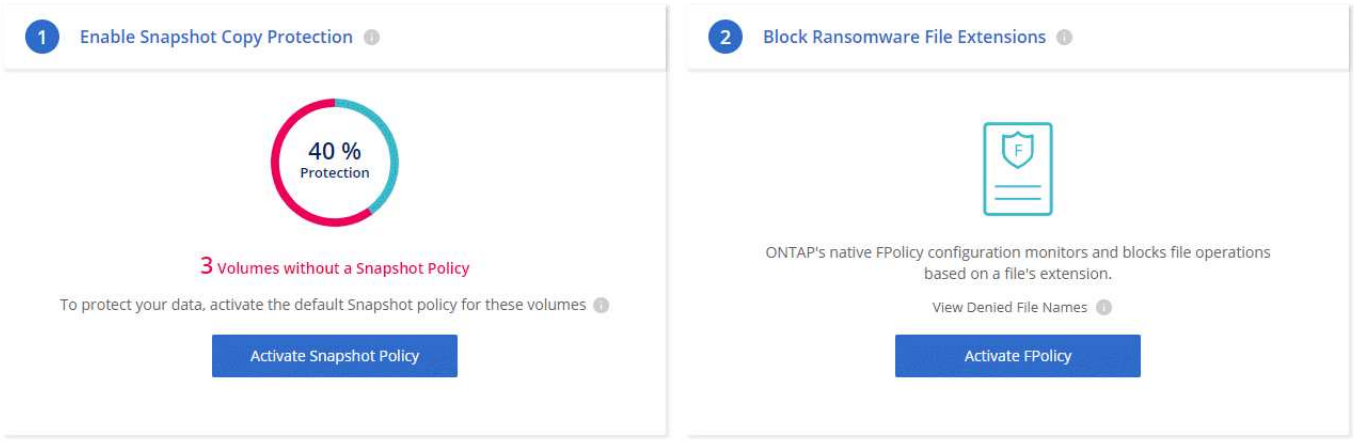


2. Implementare la soluzione NetApp per ransomware:
   a. Fare clic su **Activate Snapshot Policy** (attiva policy Snapshot) se si dispone di volumi che non hanno una policy Snapshot attivata.

      La tecnologia Snapshot di NetApp offre la migliore soluzione del settore per la risoluzione dei problemi ransomware. La chiave per un ripristino corretto è il ripristino da backup non infetti. Le copie Snapshot sono di sola lettura, impedendo la corruzione del ransomware. Possono inoltre offrire la granularità necessaria per creare immagini di una singola copia di file o di una soluzione completa di disaster recovery.

   b. Fare clic su **Activate FPolicy** (attiva FPolicy) per attivare la soluzione FPolicy di ONTAP, che può bloccare le operazioni sui file in base all'estensione di un file.

      Questa soluzione preventiva migliora la protezione dagli attacchi ransomware bloccando i tipi di file ransomware più comuni.



Aggiunta di sistemi Cloud Volumes ONTAP esistenti a Cloud Manager

Puoi scoprire e aggiungere sistemi Cloud Volumes ONTAP esistenti a Cloud Manager. Puoi farlo se hai implementato un nuovo sistema Cloud Manager.

Prima di iniziare

È necessario conoscere la password dell'account utente amministratore di Cloud Volumes ONTAP.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Discover** e selezionare **Cloud Volumes ONTAP**.
2. Selezionare il provider cloud in cui risiede il sistema.
3. Nella pagina Area, scegliere l'area in cui sono in esecuzione le istanze, quindi selezionare le istanze.
4. Nella pagina credenziali, immettere la password per l'utente amministratore di Cloud Volumes ONTAP, quindi fare clic su **Go**.

Risultato

Cloud Manager aggiunge le istanze di Cloud Volumes ONTAP allo spazio di lavoro.

Eliminazione di un ambiente di lavoro Cloud Volumes ONTAP

Si consiglia di eliminare i sistemi Cloud Volumes ONTAP da Cloud Manager, piuttosto che dalla console del provider di cloud. Ad esempio, se si termina un'istanza di Cloud Volumes ONTAP con licenza da AWS, non è possibile utilizzare la chiave di licenza per un'altra istanza. Per rilasciare la licenza, è necessario eliminare l'ambiente di lavoro da Cloud Manager.

A proposito di questa attività

Quando si elimina un ambiente di lavoro, Cloud Manager termina le istanze, elimina dischi e snapshot.

Le istanze di Cloud Volumes ONTAP dispongono di una protezione di terminazione abilitata per prevenire la terminazione accidentale da parte di AWS. Tuttavia, se si interrompe un'istanza di Cloud Volumes ONTAP da AWS, è necessario accedere alla console di AWS CloudFormation ed eliminare lo stack dell'istanza. Il nome dello stack è il nome dell'ambiente di lavoro.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Delete** (Elimina).
2. Digitare il nome dell'ambiente di lavoro, quindi fare clic su **Delete** (Elimina).

   L'eliminazione dell'ambiente di lavoro può richiedere fino a 5 minuti.

Amministrare Cloud Manager

Aggiornamento di Cloud Manager

È possibile aggiornare Cloud Manager alla versione più recente o con una patch condivisa dal personale NetApp.

Attivazione degli aggiornamenti automatici

Cloud Manager può aggiornarsi automaticamente quando è disponibile una nuova versione. In questo modo si garantisce l'esecuzione della versione più recente.

A proposito di questa attività

Cloud Manager si aggiorna automaticamente alle 12:00 se non sono in esecuzione operazioni.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **Impostazioni Cloud Manager**.
2. Selezionare la casella di controllo nella sezione aggiornamenti automatici di Cloud Manager, quindi fare clic su **Salva**.

Aggiornamento di Cloud Manager alla versione più recente

È necessario attivare gli aggiornamenti automatici di Cloud Manager, ma è sempre possibile eseguire un aggiornamento manuale direttamente dalla console Web. Cloud Manager ottiene l'aggiornamento software da un bucket S3 di proprietà di NetApp in AWS.

Prima di iniziare

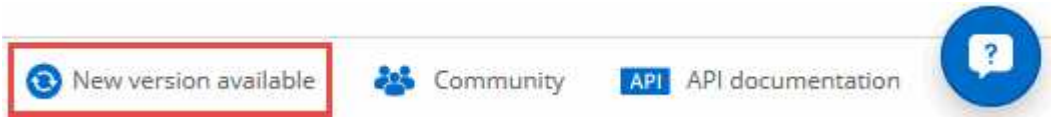
Dovresti aver esaminato "novità della release" identificare nuovi requisiti e modifiche nel supporto.

A proposito di questa attività

L'aggiornamento del software richiede alcuni minuti. Cloud Manager non sarà disponibile durante l'aggiornamento.

Fasi

1. Controllare se è disponibile una nuova versione osservando l'angolo inferiore destro della console:



2. Se è disponibile una nuova versione, fare clic su **Timeline** per determinare se sono in corso attività.

   Se sono in corso attività, attendere che vengano completate prima di passare alla fase successiva.

3. Nella parte inferiore destra della console, fare clic su **Nuova versione disponibile**.
4. Nella pagina Cloud Manager Software Update, fare clic su **Update** accanto alla versione desiderata.
5. Completare la finestra di dialogo di conferma, quindi fare clic su **OK**.

Risultato

Cloud Manager avvia il processo di aggiornamento. È possibile accedere alla console dopo alcuni minuti.

Aggiornamento di Cloud Manager con una patch

Se NetApp ha condiviso una patch con te, puoi aggiornare Cloud Manager con la patch fornita direttamente dalla console Web di Cloud Manager.

A proposito di questa attività

L'aggiornamento delle patch in genere richiede alcuni minuti. Cloud Manager non sarà disponibile durante l'aggiornamento.

Fasi

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

2. Fare clic sul collegamento per aggiornare Cloud Manager con la patch fornita.

3. Completare la finestra di dialogo di conferma, quindi fare clic su **OK**.
4. Selezionare la patch fornita.

Risultato

Cloud Manager applica la patch. È possibile accedere alla console dopo alcuni minuti.

Gestione degli spazi di lavoro e degli utenti nell'account Cloud Central

"Dopo aver eseguito la configurazione iniziale", potrebbe essere necessario gestire in seguito utenti, aree di lavoro e connettori di servizio.

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

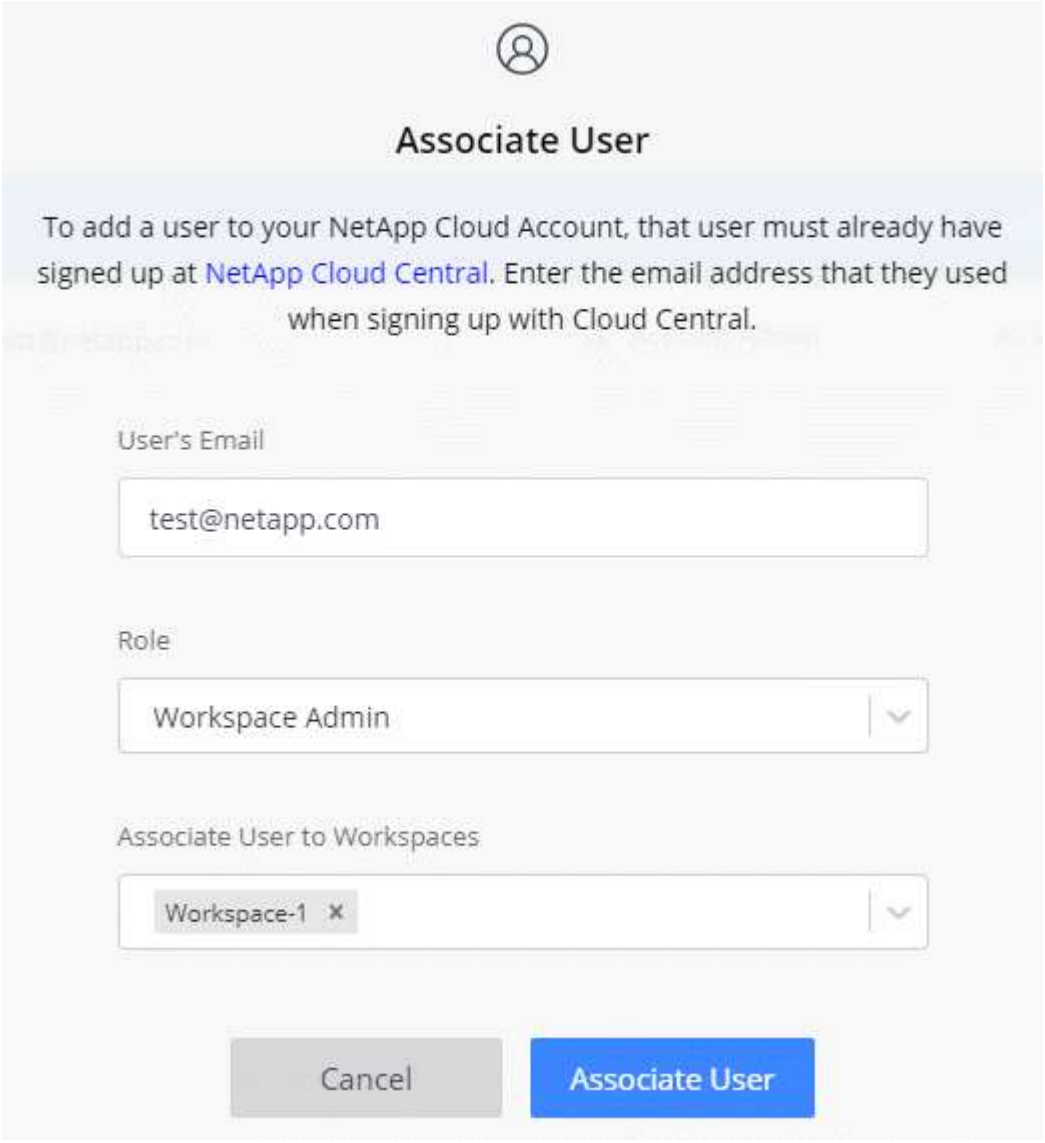
Aggiunta di utenti

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

Fasi

1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "NetApp Cloud Central" e 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.

Risultato

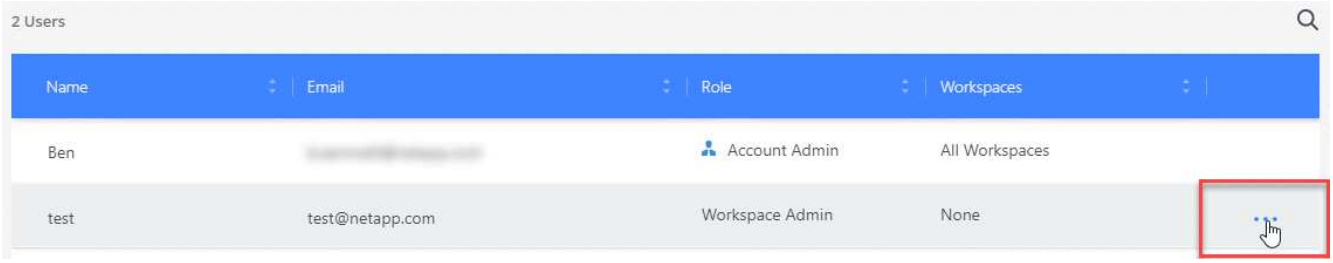
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

Rimozione degli utenti

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

Fasi

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



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

Risultato

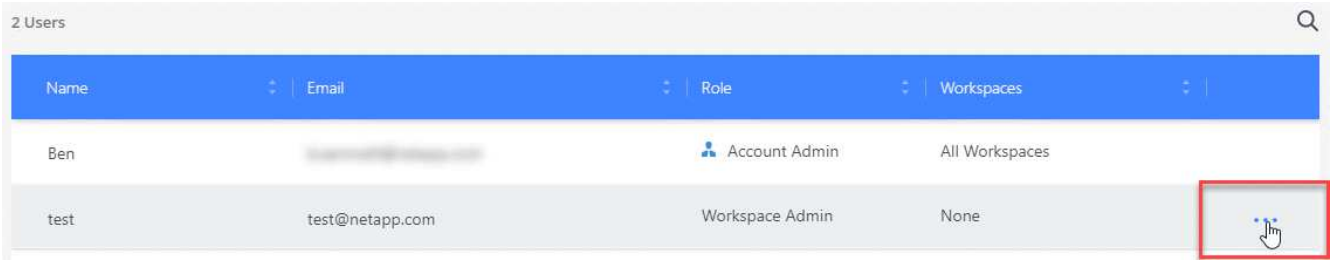
L'utente non può più accedere alle risorse di questo account Cloud Central.

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

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

Fasi

1. 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 le aree di lavoro da associare all'utente e fare clic su **Apply** (Applica).

Risultato

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

Gestione delle aree di lavoro

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

Fasi

1. Fare clic su **Impostazioni account**.
2. Fare clic su **Workspaces**.
3. Scegliere una delle seguenti opzioni:
    - Fare clic su **Add New Workspace** (Aggiungi nuova area di lavoro) per creare una nuova area di lavoro.
    - Fare clic su **Rename** (Rinomina) per rinominare l'area di lavoro.
    - Fare clic su **Delete** (Elimina) per eliminare l'area di lavoro.

Gestione delle aree di lavoro di un Service Connector

È necessario associare il 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 le aree di lavoro da associare al connettore di servizio e fare clic su **Apply** (Applica).

Rimozione degli ambienti di lavoro Cloud Volumes ONTAP

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

A proposito di questa attività

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

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

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

Fasi

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

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

Risultato

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

Configurazione di Cloud Manager per l'utilizzo di un server proxy

Quando si implementa Cloud Manager per la prima volta, viene richiesto di inserire un server proxy se il sistema non dispone di accesso a Internet. Puoi anche inserire e modificare manualmente il proxy dalle impostazioni di Cloud Manager.

A proposito di questa attività

Se le policy aziendali impongono di utilizzare un server proxy per tutte le comunicazioni HTTP a Internet, è necessario configurare Cloud Manager per l'utilizzo di tale server proxy. Il server proxy può trovarsi nel cloud o nella rete.

Quando si configura Cloud Manager per l'utilizzo di un server proxy, Cloud Manager, Cloud Volumes ONTAP e il mediatore ha utilizzano tutti il server proxy.

Fasi

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

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

   Cloud Manager non supporta password che includono il carattere @.

Risultato

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

Rinnovo del certificato HTTPS di Cloud Manager

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

Fasi

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

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

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

Risultato

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

Ripristino di Cloud Manager

Il tuo "Account NetApp Cloud Central" Semplifica il ripristino di una configurazione di Cloud Manager. L'account è un servizio in esecuzione in Cloud Central in modo che gli utenti, le aree di lavoro e i connettori di servizio associati all'account siano sempre accessibili. Anche se il tuo sistema Cloud Manager è stato accidentalmente cancellato.

A partire dalla versione 3.7.1, Cloud Manager non supporta più il download e l'utilizzo di un backup per ripristinare la configurazione. Per ripristinare Cloud Manager, devi seguire questa procedura.

Fasi

1. Implementa un nuovo sistema Cloud Manager nel tuo account Cloud Central esistente.

   "Opzioni di implementazione"

2. Aggiungi i tuoi account cloud provider e gli account NetApp Support Site a Cloud Manager.

   Questa fase prepara Cloud Manager per creare sistemi Cloud Volumes ONTAP aggiuntivi nel tuo cloud provider.

   È importante completare questo passaggio se si utilizzano le chiavi AWS per implementare un sistema Cloud Volumes ONTAP esistente che si desidera scoprire su questo nuovo sistema Cloud Manager. Cloud Manager ha bisogno delle chiavi AWS per rilevare e gestire correttamente Cloud Volumes ONTAP.

   - "Aggiunta di account AWS a Cloud Manager"
   - "Aggiunta di account Azure a Cloud Manager"
   - "Aggiunta di account NetApp Support Site a Cloud Manager"

3. Riscopri i tuoi ambienti di lavoro: Sistemi Cloud Volumes ONTAP, cluster on-premise e configurazioni di storage privato NetApp per il cloud.

- "Aggiunta di sistemi Cloud Volumes ONTAP esistenti a Cloud Manager"
- "Alla scoperta dei cluster ONTAP"

Risultato

La configurazione di Cloud Manager viene ora ripristinata con account, impostazioni e ambienti di lavoro.

Disinstallazione di Cloud Manager

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

Fasi

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

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

   silent esegue lo script senza richiedere conferma.

Provisioning dei volumi per i file service

Gestione dei volumi per Azure NetApp Files

Visualizzare e creare volumi NFS per "Azure NetApp Files" Direttamente da Cloud Manager.

Impostazione della configurazione

La tua configurazione deve soddisfare alcuni requisiti prima di poter gestire i volumi per Azure NetApp Files da Cloud Manager.

1. Azure NetApp Files deve essere configurato completando le seguenti operazioni dal portale Azure:
   - "Registrati a Azure NetApp Files"
   - "Creare un account NetApp"
   - "Impostare un pool di capacità"
   - "Delegare una subnet a Azure NetApp Files"
2. Cloud Manager deve essere configurato come segue:
   - Cloud Manager deve essere in esecuzione in Azure, nell'account in cui è stato configurato Azure NetApp Files.
   - La macchina virtuale Cloud Manager deve ricevere le autorizzazioni tramite un "identità gestita".

     Se hai implementato Cloud Manager da Cloud Central, sei tutto a posto. Cloud Central abilita automaticamente un'identità gestita assegnata dal sistema sulla macchina virtuale Cloud Manager.

   Se hai implementato Cloud Manager da Azure Marketplace, dovresti aver seguito questa operazione "istruzioni per abilitare un'identità gestita".

   - Il ruolo Azure assegnato alla macchina virtuale Cloud Manager deve includere le autorizzazioni elencate nella più recente "Policy di Cloud Manager per Azure":

     ```
     "Microsoft.NetApp/netAppAccounts/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
     ```

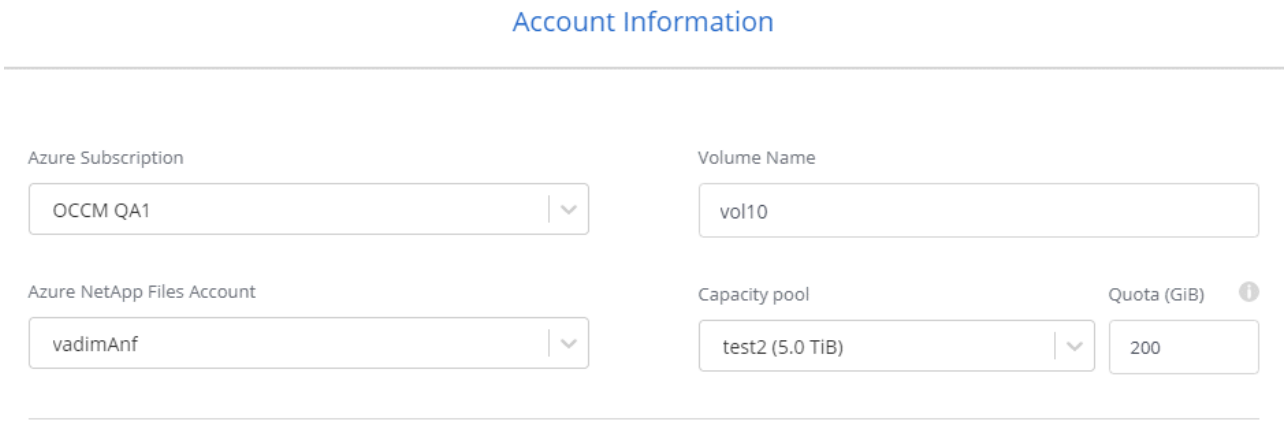
Una volta configurata la configurazione, Cloud Manager visualizza automaticamente Azure NetApp Files nella pagina Working Environments (ambienti di lavoro):

Creazione di volumi

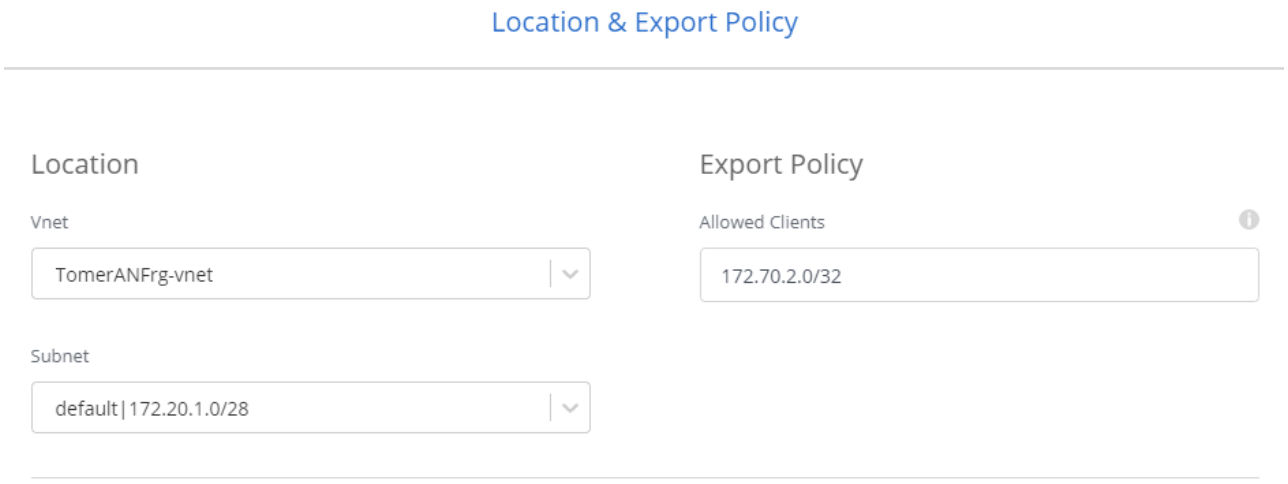
Cloud Manager consente di creare volumi NFSv3 per Azure NetApp Files.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic su **Add New Volume** (Aggiungi nuovo volume).
3. Inserire i dettagli di base sul volume nella pagina **informazioni account**:
   a. Seleziona un abbonamento Azure e un account Azure NetApp Files.
   b. Immettere un nome per il volume.
   c. Selezionare un pool di capacità e specificare una quota, ovvero la quantità di storage logico allocata al volume.



4. Compila la pagina **Location & Export Policy**:
   a. Selezionare un VNET e una subnet.
   b. Configurare un criterio di esportazione per controllare l'accesso al volume.



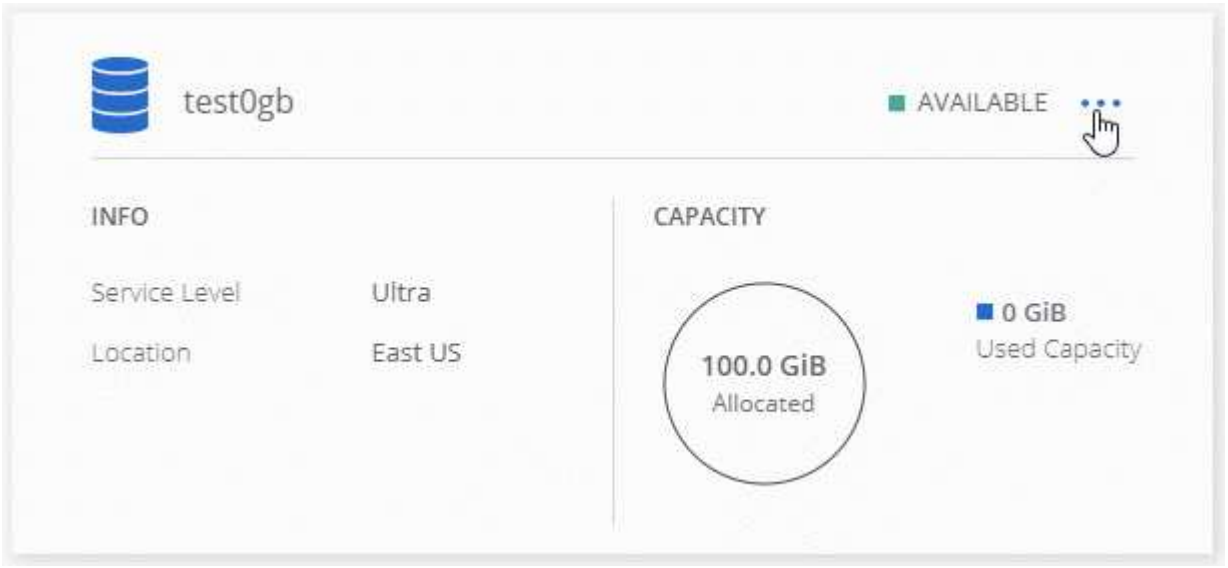
5. Fare clic su **Go**.

Ottenere il percorso di montaggio di un volume

Copiare il percorso di montaggio di un volume in modo da poter montare il volume su una macchina Linux.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic sul menu.



3. Fare clic su **Mount Command**.

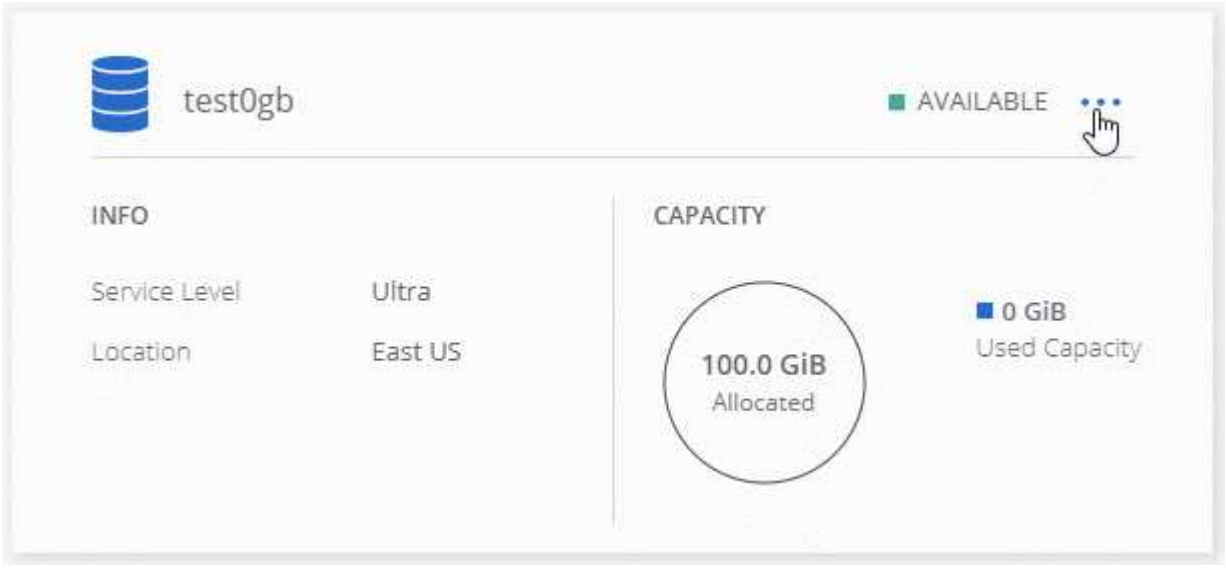
4. Copiare il percorso di montaggio e utilizzare il testo copiato per montare il volume su una macchina Linux.

Eliminazione di volumi

Eliminare i volumi non più necessari.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic sul menu.



3. Fare clic su **Delete** (Elimina).
4. Confermare che si desidera eliminare il volume.

Assistenza

USA la chat di Cloud Manager per domande generali sull'assistenza.

Per problemi di supporto tecnico associati a Azure NetApp Files, utilizzare il portale Azure per registrare una

richiesta di supporto a Microsoft. Selezionare l'abbonamento Microsoft associato e il nome del servizio **Azure NetApp Files** sotto **Storage.** fornire le informazioni rimanenti necessarie per creare la richiesta di supporto Microsoft.

Cloud Manager fornisce un download AutoSupport locale sotto l'opzione di menu **pannello di supporto**. Questo file 7z contiene un file di debug Azure per mostrare le comunicazioni in entrata e in uscita verso il tuo account Azure NetApp Files.

Limitazioni

- Cloud Manager non supporta i volumi SMB.
- Cloud Manager non consente di gestire pool di capacità o snapshot di volumi.
- È possibile creare volumi con una dimensione iniziale e una singola policy di esportazione. La modifica di un volume deve essere eseguita dall'interfaccia Azure NetApp Files nel portale Azure.
- Cloud Manager non supporta la replica dei dati verso o da Azure NetApp Files.

Link correlati

- "Cloud Central di NetApp: Azure NetApp Files"
- "Documentazione Azure NetApp Files"

Gestione di Cloud Volumes Service per AWS

Cloud Manager ti consente di scoprire i volumi cloud NFS nel tuo "Cloud Volumes Service per AWS" iscrizione. Dopo il rilevamento, puoi aggiungere altri volumi cloud NFS direttamente da Cloud Manager.

Cloud Manager non supporta volumi SMB o a doppio protocollo con Cloud Volumes Service per AWS.

Prima di iniziare

- Cloud Manager consente di rilevare le sottoscrizioni *esistenti* Cloud Volumes Service per AWS. Vedere "Guida alla configurazione dell'account NetApp Cloud Volumes Service per AWS" se non hai ancora configurato l'abbonamento.

  Devi seguire questo processo di configurazione per ciascuna regione ed eseguire il provisioning del tuo primo volume da Cloud Volumes Service prima di scoprire la regione in Cloud Manager.

- È necessario ottenere la chiave API e la chiave segreta Cloud Volumes per poterli fornire a Cloud Manager. "Per istruzioni, consultare la documentazione di Cloud Volumes Service per AWS".

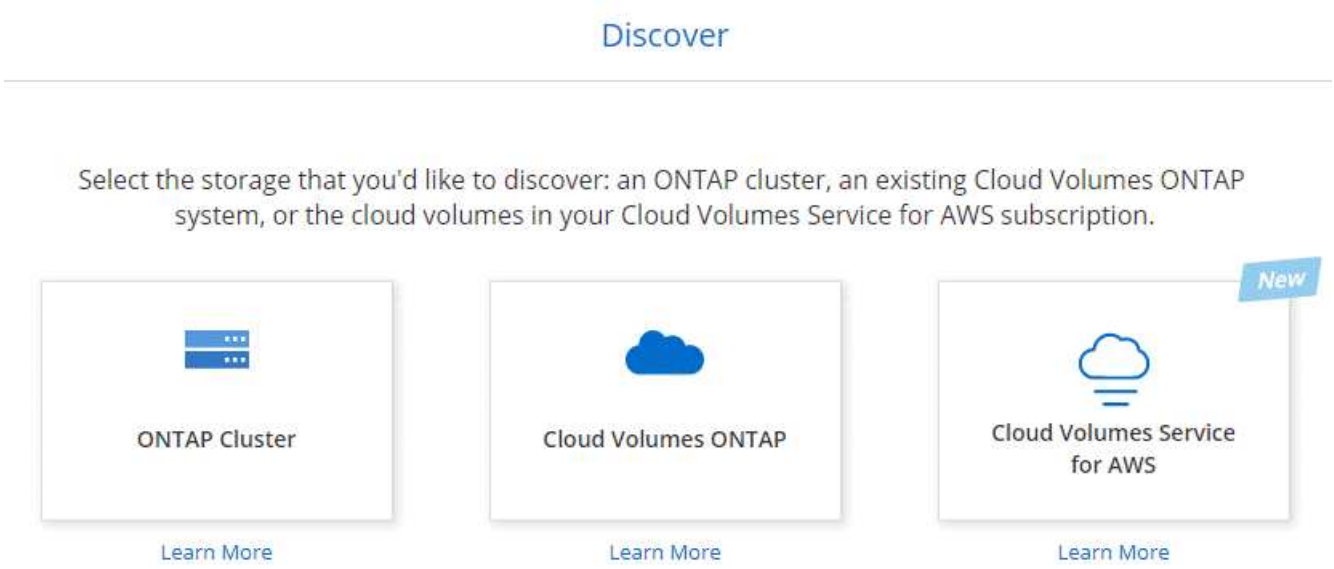
Rilevamento dell'abbonamento a Cloud Volumes Service per AWS

Per iniziare, devi scoprire i volumi cloud in una regione AWS. È possibile scoprire altre regioni in un secondo momento.

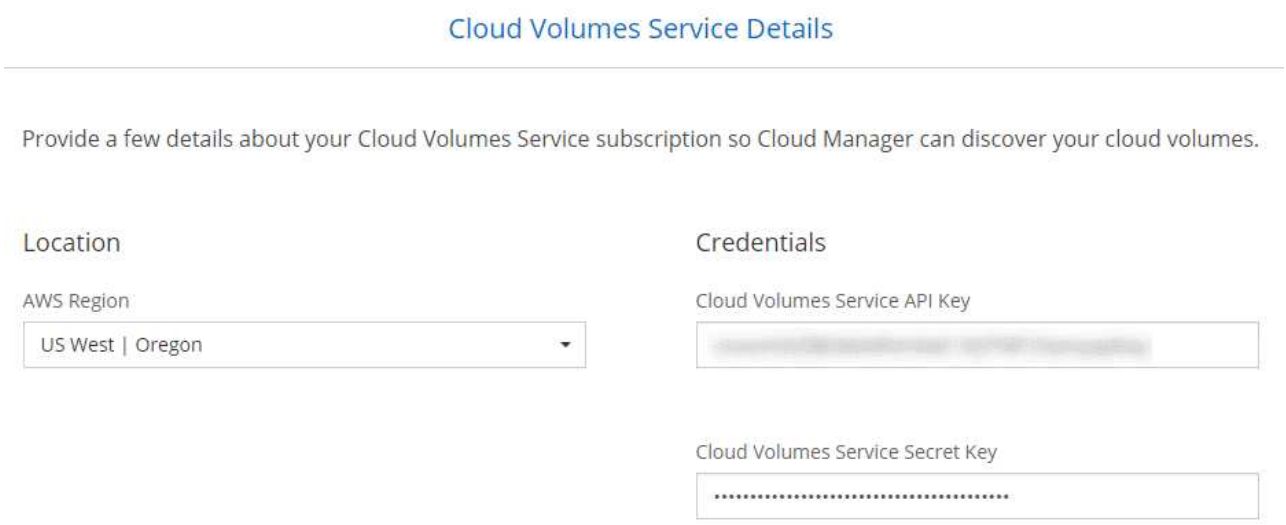
Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Scopri**.

2. Selezionare **Cloud Volumes Service per AWS**.



3. Fornisci informazioni sull'abbonamento a Cloud Volumes Service:
   a. Selezionare la regione AWS in cui risiedono i volumi cloud.
   b. Immettere la chiave API e la chiave segreta dei volumi cloud. "Per istruzioni, consultare la documentazione di Cloud Volumes Service per AWS".
   c. Fare clic su **Go**.



Risultato

Cloud Manager dovrebbe ora visualizzare la configurazione di Cloud Volumes Service per AWS nella pagina Working Environments (ambienti di lavoro).

Rilevamento di altre regioni

Se hai volumi cloud in altre regioni, devi scoprire ogni singola regione.

Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro (ma non aprirlo facendo doppio clic).
2. Nel riquadro di destra, fare clic su **Discover Cloud Volumes Service in another region** (Scopri il mondo in un'altra regione)

3. Fornisci informazioni sull'abbonamento a Cloud Volumes Service:
   a. Selezionare la regione AWS in cui risiedono i volumi cloud.
   b. Immettere la chiave API e la chiave segreta dei volumi cloud. "Per istruzioni, consultare la documentazione di Cloud Volumes Service per AWS".
   c. Fare clic su **Go**.

Risultato

Cloud Manager rileva le informazioni sui volumi cloud nella regione selezionata.

Creazione di volumi cloud

Cloud Manager consente di creare volumi cloud NFSv3. Puoi creare volumi cloud solo con una dimensione iniziale e una singola policy di esportazione. La modifica del volume deve essere eseguita dall'interfaccia utente di Cloud Volume Service.

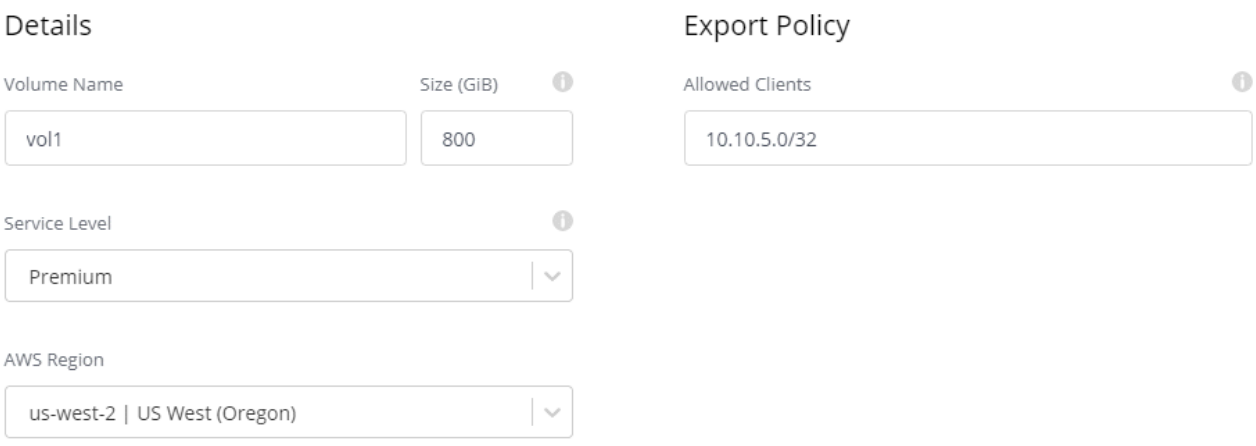
1. Aprire l'ambiente di lavoro.
2. Fare clic su **Add New Volume** (Aggiungi nuovo volume).
3. Inserire i dettagli relativi al volume:
   a. Immettere un nome per il volume.
   b. Specificare una dimensione compresa nell'intervallo da 100 GiB a 90,000 GiB (equivalente a 88 Tibs).

      Cloud Manager visualizza i volumi in GiB, mentre Cloud Volumes Service visualizza i volumi in GB.

   c. Specificare un livello di servizio: Standard, Premium o Extreme.

      "Scopri di più su questi livelli di servizio".

   d. Scegli una regione. È possibile creare il volume in una regione rilevata da Cloud Manager.
   e. Limitare l'accesso al client specificando un indirizzo IP o CIDR (Classless Inter-Domain Routing).



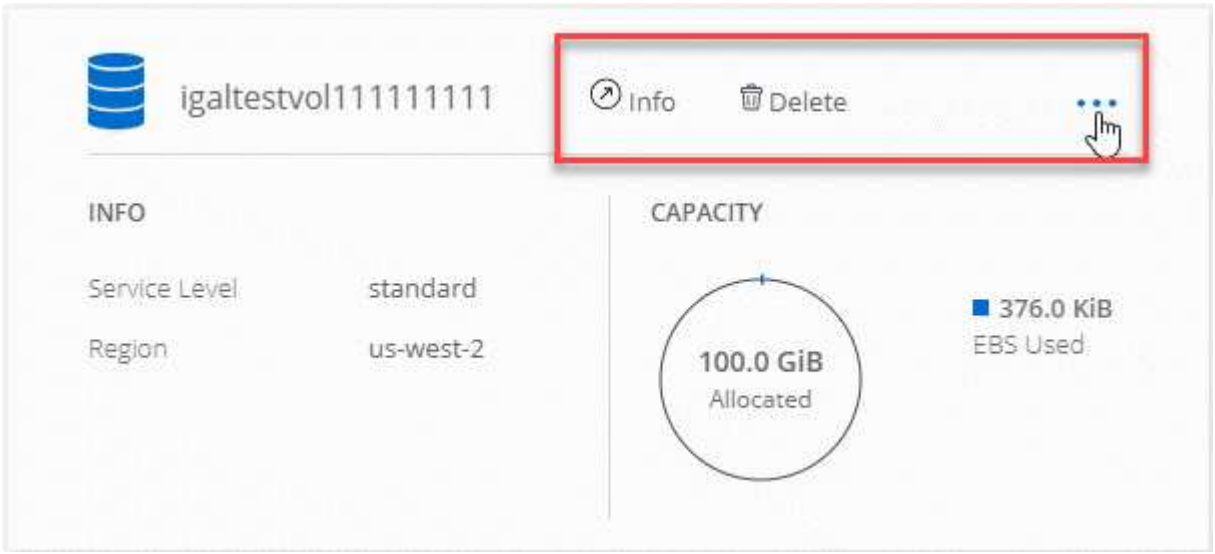
4. Fare clic su **Go**.

Eliminazione dei volumi cloud

Elimina i volumi cloud di cui non hai più bisogno.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic sul menu. Fare clic su **Delete** (Elimina).



3. Confermare che si desidera eliminare il volume.

Assistenza

USA la chat di Cloud Manager per domande generali sull'assistenza.

Per problemi di supporto tecnico associati ai volumi cloud, utilizza il numero di serie a 20 cifre "930" nella scheda "supporto" dell'interfaccia utente di Cloud Volumes Service. Utilizzare questo ID di supporto per aprire un ticket Web o per chiamare il supporto. Assicurarsi di attivare il numero di serie di Cloud Volumes Service per il supporto dall'interfaccia utente di Cloud Volumes Service. "Questi passaggi sono spiegati qui".

Limitazioni

- Cloud Manager non supporta volumi SMB o a doppio protocollo.
- Puoi creare volumi cloud solo con una dimensione iniziale e una singola policy di esportazione. La modifica del volume deve essere eseguita dall'interfaccia utente di Cloud Volume Service.
- Cloud Manager non supporta la replica dei dati da o verso un abbonamento a Cloud Volumes Service per AWS.
- La rimozione dell'abbonamento a Cloud Volumes Service per AWS da Cloud Manager non è supportata. Non ci sono costi per scoprire una regione da Cloud Manager.

Link correlati

- "NetApp Cloud Central: Cloud Volumes Service per AWS"
- "Documentazione di NetApp Cloud Volumes Service per AWS"

API e automazione

Esempi di automazione per l'infrastruttura come codice

Utilizza le risorse di questa pagina per ottenere assistenza nell'integrazione di Cloud Manager e Cloud Volumes ONTAP con il "infrastruttura come codice".

I team DevOps utilizzano una vasta gamma di strumenti per automatizzare la configurazione di nuovi ambienti, consentendo loro di trattare l'infrastruttura come codice. Due di questi strumenti sono Ansible e Terraform. Abbiamo sviluppato esempi di Ansible e Terraform che il team DevOps può utilizzare con Cloud Manager per automatizzare e integrare Cloud Volumes ONTAP con l'infrastruttura come codice.

"Visualizza gli esempi di automazione".

Ad esempio, puoi utilizzare i playbook Ansible di esempio per implementare Cloud Manager e Cloud Volumes ONTAP, creare un aggregato e creare un volume. Modifica i campioni per il tuo ambiente o crea nuovi playbook in base ai campioni.

Link correlati

- "NetApp Cloud Blog: Utilizzo delle API REST di Cloud Manager con accesso federato"
- "Blog sul cloud di NetApp: Automazione del cloud con Cloud Volumes ONTAP e REST"
- "NetApp Cloud Blog: Clonazione automatica dei dati per il test basato sul cloud delle applicazioni software"
- "NetApp Blog: Accelerazione dell'infrastruttura come codice (IAC) con Ansible + NetApp"
- "NetApp thePub: Configuration Management Automation with Ansible"
- "NetApp thePub: Ruoli per l'utilizzo di Ansible ONTAP"

Riferimento

Domande frequenti: Integrazione di Cloud Manager con NetApp Cloud Central

Quando si esegue l'aggiornamento da Cloud Manager 3.4 o versioni precedenti, NetApp sceglierà sistemi Cloud Manager specifici da integrare con NetApp Cloud Central, se non sono già integrati. Queste FAQ possono rispondere alle domande che potresti avere sul processo.

Che cos'è NetApp Cloud Central?

NetApp Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi ti consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il backup dei dati SaaS e migrare e controllare in modo efficace i dati su più cloud.

Perché NetApp sta integrando il mio sistema Cloud Manager con Cloud Central?

L'integrazione di Cloud Manager con NetApp Cloud Central offre diversi vantaggi, tra cui un'esperienza di implementazione semplificata, un'unica posizione per visualizzare e gestire più sistemi Cloud Manager e autenticazione utente centralizzata.

Cosa succede durante il processo di integrazione?

NetApp esegue la migrazione di tutti gli account utente locali nel sistema Cloud Manager all'autenticazione utente centralizzata disponibile in Cloud Central.

Come funziona l'autenticazione utente centralizzata?

Con l'autenticazione utente centralizzata, è possibile utilizzare lo stesso set di credenziali nei sistemi Cloud Manager e tra Cloud Manager e altri servizi dati, come Cloud Sync. È anche facile reimpostare la password se la si dimentica.

Devo iscrivermi a un account utente Cloud Central?

NetApp creerà un account utente Cloud Central per te quando integreremo il tuo sistema Cloud Manager con Cloud Central. Per completare il processo di registrazione, è sufficiente reimpostare la password.

Cosa fare se si dispone già di un account utente Cloud Central?

Se l'indirizzo e-mail utilizzato per accedere a Cloud Manager corrisponde all'indirizzo e-mail di un account utente Cloud Central, puoi accedere direttamente al tuo sistema Cloud Manager.

Cosa succede se il sistema Cloud Manager dispone di più account utente?

NetApp esegue la migrazione di tutti gli account utente locali verso gli account utente di Cloud Central. Ogni utente deve reimpostare la propria password.

Cosa succede se si dispone di un account utente che utilizza lo stesso indirizzo e-mail su più sistemi Cloud Manager?

Devi solo reimpostare la password una volta per poter utilizzare lo stesso account utente di Cloud Central per accedere a ciascun sistema Cloud Manager.

Cosa fare se l'account utente locale utilizza un indirizzo e-mail non valido?

La reimpostazione della password richiede un indirizzo e-mail valido. Contattaci tramite l'icona della chat disponibile nell'angolo inferiore destro dell'interfaccia di Cloud Manager.

Cosa succede se si dispone di script di automazione per le API Cloud Manager?

Tutte le API sono compatibili con le versioni precedenti. Sarà necessario aggiornare gli script che utilizzano le password, se si modifica la password al momento della reimpostazione.

Cosa succede se il sistema Cloud Manager utilizza LDAP?

Se il sistema utilizza LDAP, NetApp non può integrare automaticamente il sistema con Cloud Central. È necessario eseguire manualmente i seguenti passaggi:

1. Implementa un nuovo sistema Cloud Manager da "NetApp Cloud Central".
2. "Configurare LDAP con il nuovo sistema".
3. "Scopri i sistemi Cloud Volumes ONTAP esistenti" Dal nuovo sistema Cloud Manager.
4. Eliminare il vecchio sistema Cloud Manager.

È importante dove ho installato il sistema Cloud Manager?

No NetApp integrerà i sistemi con Cloud Central indipendentemente da dove risiedono, sia in AWS, Azure o on-premise.

L'unica eccezione è l'ambiente di servizi cloud commerciali AWS.

Regole del gruppo di sicurezza per AWS

Cloud Manager crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Manager

Il gruppo di sicurezza per Cloud Manager richiede regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host Cloud Manager
HTTP	80	Fornisce accesso HTTP dai browser Web client alla console Web Cloud Manager e connessioni da Cloud Compliance
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager
TCP	3128	Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

Regole in uscita per Cloud Manager

Il gruppo di sicurezza predefinito per Cloud Manager apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Manager include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Manager.

L'indirizzo IP di origine è l'host Cloud Manager.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager
Conformità al cloud	HTTP	80	Istanza di Cloud Compliance	Conformità del cloud per Cloud Volumes ONTAP

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole inbound per Cloud Volumes ONTAP

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita per Cloud Volumes ONTAP

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory					

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
	TCP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
Backup su S3	TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole per il gruppo di sicurezza esterno del mediatore ha

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP ha include le seguenti regole in entrata e in uscita.

Regole in entrata

L'origine delle regole in entrata è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Connessioni SSH al mediatore ha
TCP	3000	Accesso API RESTful da Cloud Manager

Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore ha apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il mediatore ha include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita dal mediatore ha.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP di Cloud Manager	Scarica gli aggiornamenti per il mediatore
HTTPS	443	Servizi API AWS	Assistenza per il failover dello storage
UDP	53	Servizi API AWS	Assistenza per il failover dello storage

Anziché aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

Regole per il gruppo di sicurezza interno del mediatore ha

Il gruppo di sicurezza interno predefinito per il mediatore ha Cloud Volumes ONTAP include le seguenti regole. Cloud Manager crea sempre questo gruppo di sicurezza. Non hai la possibilità di utilizzare il tuo.

Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole in uscita

Il gruppo di protezione predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore ha e i nodi ha

Regole del gruppo di sicurezza per Azure

Cloud Manager crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Manager

Il gruppo di sicurezza per Cloud Manager richiede regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Porta	Protocollo	Scopo
22	SSH	Fornisce l'accesso SSH all'host Cloud Manager
80	HTTP	Fornisce l'accesso HTTP dai browser Web client alla console Web di Cloud Manager
443	HTTPS	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager

Regole in uscita per Cloud Manager

Il gruppo di sicurezza predefinito per Cloud Manager apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Manager include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Manager.

L'indirizzo IP di origine è l'host Cloud Manager.

Servizio	Porta	Protocollo	Destinazione	Scopo
Active Directory	88	TCP	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	139	TCP	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP	Insieme di strutture di Active Directory	LDAP
	445	TCP	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	137	UDP	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	464	UDP	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos

Servizio	Porta	Protocollo	Destinazione	Scopo
Chiamate API e AutoSupport	443	HTTPS	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	3000	TCP	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	53	UDP	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata per sistemi a nodo singolo

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
1001 inbound_http	80 TCP	Qualsiasi a qualsiasi	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1002 inbound_111_tcp	111 TCP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Blocca tutto il traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

I sistemi HA hanno meno regole in entrata rispetto ai sistemi a nodo singolo perché il traffico dati in entrata passa attraverso il bilanciamento del carico standard di Azure. Per questo motivo, il traffico proveniente dal bilanciamento del carico deve essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in uscita per Cloud Volumes ONTAP

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
Active Directory					

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
	389	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	445	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	464	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
DHCP	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	67	UDP	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	53	UDP	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	25	TCP	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	161	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	161	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	11104	TCP	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	11105	TCP	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	514	UDP	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole firewall per GCP

Cloud Manager crea regole firewall GCP che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Manager

Le regole firewall per Cloud Manager richiedono regole sia in entrata che in uscita.

Regole in entrata per Cloud Manager

L'origine delle regole in entrata nelle regole firewall predefinite è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host Cloud Manager
HTTP	80	Fornisce l'accesso HTTP dai browser Web client alla console Web di Cloud Manager
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client alla console Web di Cloud Manager

Regole in uscita per Cloud Manager

Le regole predefinite del firewall per Cloud Manager aprono tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Le regole firewall predefinite per Cloud Manager includono le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Manager.

L'indirizzo IP di origine è l'host Cloud Manager.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API a GCP e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole inbound per Cloud Volumes ONTAP

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita per Cloud Volumes ONTAP

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory					

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
	TCP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Pagine del marketplace AWS per Cloud Manager e Cloud Volumes ONTAP

Nel marketplace AWS sono disponibili diverse offerte per Cloud Manager e Cloud Volumes ONTAP. Se non sei sicuro di quale pagina devi utilizzare, leggi di seguito e ti indirizzeremo alla pagina giusta in base al tuo obiettivo.

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

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Abilitare l'implementazione DI Cloud Volumes ONTAP PAYGO per le versioni 9.6 e successive	"Cloud Manager (per Cloud Volumes ONTAP)"	Questa pagina di AWS Marketplace consente di addebitare la versione PAYGO di Cloud Volumes ONTAP 9.6 e versioni successive. Consente inoltre di addebitare le funzioni aggiuntive di Cloud Volumes ONTAP. Questa pagina non consente di avviare Cloud Manager in AWS. Questo dovrebbe essere fatto da "NetApp Cloud Central", O in alternativa utilizzando l'AMI elencato nella riga 4 di questa tabella.
Abilitare le funzionalità add-on per Cloud Volumes ONTAP (PAYGO o BYOL)		
Consentire l'implementazione di Cloud Volumes ONTAP utilizzando una licenza acquistata da NetApp (BYOL)	• "Cloud Volumes ONTAP per AWS (BYOL)" • "Cloud Volumes ONTAP per AWS - alta disponibilità (BYOL)"	Queste pagine del marketplace AWS consentono di iscriversi alle versioni a nodo singolo o ha di Cloud Volumes ONTAP BYOL.
Implementare Cloud Manager da AWS Marketplace utilizzando un AMI	"NetApp Cloud Manager (per NetApp Cloud Volumes ONTAP)"	Si consiglia di avviare Cloud Manager in AWS da "NetApp Cloud Central", Ma è possibile avviarlo da questa pagina di AWS Marketplace, se si preferisce.

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Implementazione di Cloud Volumes ONTAP PAYGO (9.5 o precedente)	• "Cloud Volumes ONTAP per AWS" • "Cloud Volumes ONTAP per AWS - alta disponibilità"	Queste pagine di AWS Marketplace consentono di sottoscrivere le versioni a nodo singolo o ha di Cloud Volumes ONTAP PAYGO per le versioni 9.5 e precedenti. A partire dalla versione 9.6, è necessario iscriversi alla pagina AWS Marketplace elencata nella riga 1 di questa tabella per le implementazioni PAYGO.

In che modo Cloud Manager utilizza le autorizzazioni del cloud provider

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

Cosa fa Cloud Manager con le autorizzazioni AWS

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

Azioni	Scopo
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescripbeInstances", "ec2:DescripbeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Avvia un'istanza di Cloud Volumes ONTAP e interrompe, avvia e monitora l'istanza.
"ec2:DescripbeInstanceAttribute",	Verifica che la rete avanzata sia abilitata per i tipi di istanze supportati.
"ec2:DescripbeRouteTable", "ec2:DescripbeImages",	Avvia una configurazione Cloud Volumes ONTAP ha.
"ec2:CreateTags",	Contrassegna ogni risorsa creata da Cloud Manager con i tag "WorkingEnvironment" e "WorkingEnvironmentId". Cloud Manager utilizza questi tag per la manutenzione e l'allocazione dei costi.
"ec2:CreateVolume", "ec2:DescripbeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestisce i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end.

Azioni	Scopo
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescripbeSecurityGroups", "ec2:RevokeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupErgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea gruppi di protezione predefiniti per Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescripbeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"ec2:DescripbeSubnet", "ec2:DescripbeVpcs",	Ottiene l'elenco delle subnet di destinazione e dei gruppi di protezione necessari per la creazione di un nuovo ambiente di lavoro per Cloud Volumes ONTAP.
"ec2:DescripbeDhcpOptions",	Determina i server DNS e il nome di dominio predefinito quando si avviano le istanze di Cloud Volumes ONTAP.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescripbeSnapshot",	Esegue snapshot dei volumi EBS durante la configurazione iniziale e ogni volta che un'istanza di Cloud Volumes ONTAP viene arrestata.
"ec2:GetConsoleOutput",	Acquisisce la console Cloud Volumes ONTAP, che è collegata ai messaggi AutoSupport.
"ec2:DescripbeKeyPairs",	Ottiene l'elenco delle coppie di chiavi disponibili quando si avviano le istanze.
"ec2:DescripbeRegions",	Ottiene un elenco delle regioni AWS disponibili.
"ec2:DeleteTags", "ec2:DescripteTags",	Gestisce i tag per le risorse associate alle istanze di Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "Cloudformation:DeleteStack", "Cloudformation:DescripbeStack", "Cloudformation:DescripbeStackEvents", "Cloudformation:ValidateTemplate",	Avvia le istanze di Cloud Volumes ONTAP.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Avvia una configurazione Cloud Volumes ONTAP ha.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescripbeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Gestisce i profili di istanza per le istanze di Cloud Volumes ONTAP.

Azioni	Scopo
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBucket", "s3:ListBucket"	Ottiene informazioni sui bucket AWS S3 in modo che Cloud Manager possa integrarsi con il servizio NetApp Data Fabric Cloud Sync.
"s3:Createbucket", "s3:Deletebucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions",	Gestisce il bucket S3 utilizzato da un sistema Cloud Volumes ONTAP come Tier di capacità.
"Kms:List*", "kms:descrivi*"	Ottiene informazioni sulle chiavi da AWS Key Management Service.
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Ottiene i dati dei costi AWS per Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	Quando si implementa una configurazione ha in una singola AWS Availability zone, Cloud Manager lancia i due nodi ha e il mediatore in un gruppo di posizionamento AWS Spread.

Cosa fa Cloud Manager con le autorizzazioni Azure

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

Azioni	Scopo
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Crea Cloud Volumes ONTAP e arresta, avvia, elimina e ottiene lo stato del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Consente l'implementazione di Cloud Volumes ONTAP da un VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/Read", "Microsoft.Storage/Operations/Read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/Read", "Microsoft.Storage/storageAccounts/rigeneratekey/action", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/uses/Read",	Gestisce gli account e i dischi dello storage Azure e li collega a Cloud Volumes ONTAP.

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

Azioni	Scopo
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Gestisce un bilanciamento del carico Azure per le coppie ha.
"Microsoft.Authorization/Blocks/*"	Consente la gestione dei blocchi sui dischi Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestisce il failover per le coppie ha.

Cosa fa Cloud Manager con le autorizzazioni GCP

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

Azioni	Scopo
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Per creare e gestire dischi per Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Per creare regole firewall per Cloud Volumes ONTAP.
- Compute.globalOperations.get	Per ottenere lo stato delle operazioni.
- Compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Per ottenere immagini per istanze di macchine virtuali.
- compute.instances.attachDisk - compute.instances.detachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Per creare ed eliminare istanze di Cloud Volumes ONTAP VM.
- compute.instances.get	Per elencare le istanze di macchine virtuali.
- compute.instances.getSerialPortOutput	Per ottenere i log della console.
- compute.instances.list	Per recuperare l’elenco di istanze in una zona.
- compute.instances.setDeletionProtection	Per impostare la protezione di eliminazione sull’istanza.
- compute.instances.setLabels	Per aggiungere etichette.

Azioni	Scopo
- compute.instances.setMachineType	Per modificare il tipo di macchina per Cloud Volumes ONTAP.
- compute.instances.setMetadata	Per aggiungere metadati.
- compute.instances.setTags	Per aggiungere tag per le regole del firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Per avviare e arrestare Cloud Volumes ONTAP.
- Compute.machineTypes.get	Per ottenere il numero di core per controllare le qoutas.
- compute.projects.get	Per supportare progetti multipli.
- Compute.Snapshot.create - compute.snapshots.delete - compute.Snapshot.get - compute.Snapshot.list - compute.snapshots.setLabels	Per creare e gestire snapshot di dischi persistenti.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zone.list	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.typeopers.get.get.get - deploymentmanager.get.list	Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Per ottenere unità di log stack.
- resourcemanager.projects.get	Per supportare progetti multipli.
- storage.bucket.create - storage.buckets.delete - storage.bucket.get - storage.bucket.list	Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptKeys.get - cloudkms.cryptKeys.list - cloudkms.keyrings.list	Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP.

Configurazioni predefinite

I dettagli sulla configurazione predefinita di Cloud Manager e Cloud Volumes ONTAP possono aiutare l'amministratore dei sistemi.

Configurazione predefinita per Cloud Manager su Linux

Se hai bisogno di risolvere i problemi di Cloud Manager o del tuo host Linux, potrebbe aiutarti a capire come è configurato Cloud Manager.

- Se hai implementato Cloud Manager da NetApp Cloud Central (o direttamente dal mercato di un cloud provider), prendi nota di quanto segue:
  - In AWS, il nome utente per l'istanza EC2 Linux è ec2-user.
  - Il sistema operativo per l'immagine Cloud Manager è Red Hat Enterprise Linux 7.4 (HVM).

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

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

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

  Se il servizio MySQL non è attivo, anche il servizio occm è inattivo.
- Cloud Manager installa i seguenti pacchetti sull'host Linux, se non sono già installati:
  - 7zip
  - AWSCLI
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Wget

Configurazione predefinita per Cloud Volumes ONTAP

La configurazione predefinita di Cloud Volumes ONTAP consente di configurare e amministrare i sistemi, in particolare se si conosce ONTAP perché la configurazione predefinita di Cloud Volumes ONTAP è diversa da ONTAP.

- Cloud Volumes ONTAP è disponibile come sistema a nodo singolo in AWS, Azure e GCP e come coppia ha in AWS e Azure.
- Cloud Manager crea una SVM per il servizio dei dati quando implementa Cloud Volumes ONTAP. Non è supportato l'utilizzo di più SVM per la distribuzione dei dati.
- Cloud Manager installa automaticamente le seguenti licenze ONTAP Feature su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache

- FlexClone
- ISCSI
- NetApp Volume Encryption (solo per sistemi BYOL o PAYGO registrati)
- NFS
- SnapMirror
- SnapRestore
- SnapVault

- Per impostazione predefinita, vengono create diverse interfacce di rete:
  - Una LIF di gestione del cluster
  - Un LIF intercluster
  - LIF di gestione SVM su sistemi ha in Azure, sistemi a nodo singolo in AWS e, facoltativamente, su sistemi ha in più zone di disponibilità AWS
  - Una LIF di gestione dei nodi
  - Una LIF di dati iSCSI
  - Una LIF di dati CIFS e NFS

> Il failover LIF è disattivato per impostazione predefinita per Cloud Volumes ONTAP a causa dei requisiti EC2. La migrazione di una LIF a una porta diversa interrompe la mappatura esterna tra gli indirizzi IP e le interfacce di rete sull'istanza, rendendo la LIF inaccessibile.

- Cloud Volumes ONTAP invia i backup della configurazione a Cloud Manager utilizzando HTTPS.

  Una volta effettuato l'accesso a Cloud Manager, i backup sono accessibili da https://ipaddress/occm/offboxconfig/

- Cloud Manager imposta alcuni attributi di volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio, System Manager o CLI).

  La tabella seguente elenca gli attributi del volume impostati da Cloud Manager in modo diverso dai valori predefiniti:

Attributo	Valore stabilito da Cloud Manager
Modalità di dimensionamento automatico	crescere
Dimensionamento automatico massimo	1,000% L'amministratore dell'account può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno

Attributo	Valore stabilito da Cloud Manager
Autorizzazioni UNIX (solo NFS)	777

Per informazioni su questi attributi, consulta la pagina man *volume create*.

Dati di boot e root per Cloud Volumes ONTAP

Oltre allo storage per i dati degli utenti, Cloud Manager acquista anche lo storage cloud per i dati di boot e root su ogni sistema Cloud Volumes ONTAP.

AWS

- Due dischi SSD General Purpose:
  - Un disco da 140 GB per i dati root (uno per nodo)
  - 9.6 e versioni successive: Un disco da 86 GB per i dati di avvio (uno per nodo)
  - 9.5 e versioni precedenti: Un disco da 45 GB per i dati di avvio (uno per nodo)
- Un'istantanea EBS per ogni disco di boot e disco root
- Per le coppie ha, un volume EBS per l'istanza Mediator, che è di circa 8 GB

Azure (nodo singolo)

- Due dischi SSD Premium:
  - Un disco da 90 GB per i dati di avvio
  - Un disco da 140 GB per i dati root
- Uno snapshot Azure per ogni disco di boot e disco root

Azure (coppie ha)

- Due dischi SSD Premium da 90 GB per il volume di boot (uno per nodo)
- Due blob di pagina Premium Storage da 140 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 128 GB per il risparmio di core (uno per nodo)
- Uno snapshot Azure per ogni disco di boot e disco root

GCP

- Un disco persistente standard da 10 GB per i dati di avvio
- Un disco persistente standard da 64 GB per i dati root
- Un disco persistente standard da 500 GB per NVRAM
- Un disco persistente standard da 216 GB per il risparmio dei core
- Uno snapshot GCP per il disco di boot e il disco root

Dove risiedono i dischi

Cloud Manager definisce lo storage come segue:

- I dati di avvio risiedono su un disco collegato all'istanza o alla macchina virtuale.

  Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.

- I dati root, che contengono la configurazione del sistema e i log, risiedono in aggr0.
- Il volume root della macchina virtuale di storage (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

Crittografia

I dischi di boot e root sono sempre crittografati in Azure e Google Cloud Platform perché la crittografia è attivata per impostazione predefinita in tali provider cloud.

Quando si attiva la crittografia dei dati in AWS utilizzando il servizio di gestione delle chiavi (KMS), vengono crittografati anche i dischi di avvio e i dischi root per Cloud Volumes ONTAP. Questo include il disco di boot per l'istanza del mediatore in una coppia ha. I dischi vengono crittografati utilizzando la CMK selezionata quando si crea l'ambiente di lavoro.

Ruoli

I ruoli account Admin (Amministratore account) e Workspace Admin (Amministratore area di lavoro) forniscono autorizzazioni specifiche agli utenti.

Attività	Amministratore account	Amministratore dello spazio di lavoro
Gestire gli ambienti di lavoro	Sì	Sì, per le aree di lavoro associate
Visualizzare lo stato della replica dei dati	Sì	Sì, per le aree di lavoro associate
Visualizza la timeline	Sì	Sì, per le aree di lavoro associate
Eliminare gli ambienti di lavoro	Sì	No
Connettere i cluster Kubernetes a Cloud Volumes ONTAP	Sì	No
Ricevere il report Cloud Volumes ONTAP	Sì	No
Gestire gli account Cloud Central	Sì	No
Gestire gli account dei cloud provider	Sì	No
Modificare le impostazioni di Cloud Manager	Sì	No
Visualizza e gestisci la dashboard di supporto	Sì	No

Attività	Amministratore account	Amministratore dello spazio di lavoro
Rimuovere gli ambienti di lavoro da Cloud Manager	Sì	No
Aggiorna Cloud Manager	Sì	No
Installare un certificato HTTPS	Sì	No
Configurare Active Directory	Sì	No

Link correlati

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

Dove trovare assistenza e ulteriori informazioni

Puoi ottenere aiuto e ottenere ulteriori informazioni su Cloud Manager e Cloud Volumes ONTAP attraverso varie risorse, tra cui video, forum e supporto.

- "Video per Cloud Manager e Cloud Volumes ONTAP"

  Guarda i video che mostrano come implementare e gestire Cloud Volumes ONTAP e come replicare i dati nel tuo cloud ibrido.

- "Policy per Cloud Manager"

  Scarica i file JSON che includono le autorizzazioni necessarie a Cloud Manager per eseguire azioni in un cloud provider.

- "Guida per sviluppatori API di Cloud Manager"

  Leggi una panoramica delle API, esempi di come utilizzarle e un riferimento API.

- Training per Cloud Volumes ONTAP
  - "Nozioni di base su Cloud Volumes ONTAP"
  - "Implementazione e gestione di Cloud Volumes ONTAP per Azure"
  - "Implementazione e gestione di Cloud Volumes ONTAP per AWS"
- Report tecnici
  - "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni"
  - "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi"
- Disaster recovery SVM

  Il disaster recovery SVM è il mirroring asincrono dei dati SVM e della configurazione da una SVM di origine a una SVM di destinazione. È possibile attivare rapidamente una SVM di destinazione per l'accesso ai dati se la SVM di origine non è più disponibile.

  - "Guida rapida alla preparazione del disaster recovery per Cloud Volumes ONTAP 9 SVM"

Descrive come configurare rapidamente una SVM di destinazione in preparazione al disaster recovery.

  - "Guida rapida al disaster recovery di Cloud Volumes ONTAP 9 SVM"

    Descrive come attivare rapidamente una SVM di destinazione dopo un disastro e riattivare la SVM di origine.

- "Guida all'alimentazione di FlexCache Volumes per un accesso più rapido ai dati"

  Viene descritto come creare e gestire volumi FlexCache nello stesso cluster o in un cluster diverso del volume di origine per accelerare i dati access.es come attivare rapidamente una SVM di destinazione dopo un disastro, quindi riattivare la SVM di origine.

- "Avvisi di sicurezza"

  Identificare le vulnerabilità note (CVE) per i prodotti NetApp, incluso ONTAP. Si noti che è possibile correggere le vulnerabilità di sicurezza per Cloud Volumes ONTAP seguendo la documentazione di ONTAP.

- "Centro documentazione di ONTAP 9"

  Accedi alla documentazione del prodotto per ONTAP, che può aiutarti a utilizzare Cloud Volumes ONTAP.

- "Supporto NetApp Cloud Volumes ONTAP"

  Accedi alle risorse di supporto per ottenere assistenza e risolvere i problemi relativi a Cloud Volumes ONTAP.

- "Community NetApp: Servizi dati cloud"

  Connettiti con i colleghi, fai domande, scambia idee, trova risorse e condividi le Best practice.

- "NetApp Cloud Central"

  Informazioni su ulteriori prodotti e soluzioni NetApp per il cloud.

- "Documentazione sui prodotti NetApp"

  Cerca nella documentazione dei prodotti NetApp istruzioni, risorse e risposte.

Versioni precedenti della documentazione di Cloud Manager

La documentazione relativa alle release precedenti di Cloud Manager è disponibile nel caso in cui non si stia utilizzando la versione più recente.

"Cloud Manager 3.6"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

http://www.netapp.com/us/legal/netapptmlist.aspx

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/us/media/patents-page.pdf

Direttiva sulla privacy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Cloud Manager 3.7.4"
- "Avviso per Cloud Manager 3.7.1"
- "Avviso per Cloud Manager 3.7"
- "Avviso per Cloud Backup Service"

Informazioni sul copyright

Informazioni sul marchio commerciale