Cloud Manager e documentazione Cloud Volumes ONTAP

Cloud Manager 3.6

NetApp
March 25, 2024

Sommario

Cloud Manager e documentazione Cloud Volumes ONTAP

OnCommand 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"
- "Trova le configurazioni supportate per Cloud Volumes ONTAP"
- "Esamina i requisiti di rete dettagliati per Cloud Manager"
- "Consulta i requisiti di rete dettagliati per Cloud Volumes ONTAP per AWS"
- "Consulta i requisiti di rete dettagliati per Cloud Volumes ONTAP for Azure"
- "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 3.6

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

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

Supporto per l'ambiente AWS C2S (2 maggio 2019)

Cloud Volumes ONTAP 9.5 e Cloud Manager 3.6.4 sono ora disponibili negli Stati Uniti Intelligence Community (IC) attraverso l'ambiente AWS Commercial Cloud Services (C2S). È possibile implementare coppie ha e sistemi a nodo singolo in C2S.

"Guida rapida per l'ambiente di servizi cloud commerciali AWS"

Cloud Manager 3.6.6 (1 maggio 2019)

- Supporto per dischi da 6 TB in AWS
- Supporto per nuove dimensioni di dischi con sistemi a nodo singolo in Azure
- Supporto per SSD standard con sistemi a nodo singolo in Azure
- Rilevamento automatico dei cluster Kubernetes creati con NetApp Kubernetes Service
- Possibilità di configurare un server NTP

Supporto per dischi da 6 TB in AWS

Ora puoi scegliere un disco EBS di 6 TB con Cloud Volumes ONTAP per AWS. Con il recente "Migliori performance degli SSD General Purpose", Un disco da 6 TB è ora la scelta migliore per ottenere le massime prestazioni.

Questa modifica è supportata con Cloud Volumes ONTAP 9.5, 9.4 e 9.3.

Supporto per nuove dimensioni di dischi con sistemi a nodo singolo in Azure

Ora puoi utilizzare dischi da 8 TB, 16 TB e 32 TB con sistemi a nodo singolo in Azure. Le maggiori dimensioni dei dischi consentono di raggiungere fino a 368 TB di capacità di sistema con i soli dischi utilizzando le licenze Premium o BYOL.

Questa modifica è supportata con Cloud Volumes ONTAP 9.5, 9.4 e 9.3.

Supporto per SSD standard con sistemi a nodo singolo in Azure

I dischi gestiti SSD standard sono ora supportati con i sistemi a nodo singolo in Azure. Questi dischi offrono un livello di performance tra SSD Premium e HDD standard.

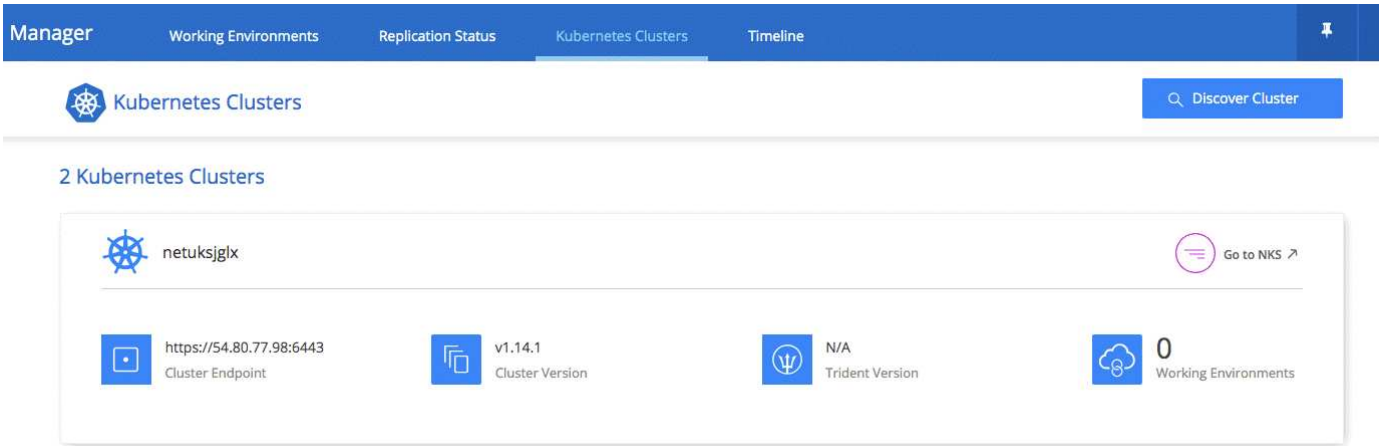
Questa modifica è supportata con Cloud Volumes ONTAP 9.5, 9.4 e 9.3.

"Scopri di più sugli SSD standard".

Rilevamento automatico dei cluster Kubernetes creati con NetApp Kubernetes Service

Cloud Manager è ora in grado di rilevare automaticamente i cluster Kubernetes implementati utilizzando NetApp Kubernetes Service. In questo modo è possibile collegare i cluster Kubernetes ai sistemi Cloud Volumes ONTAP in modo da utilizzarli come storage persistente per i container.

L'immagine seguente mostra un cluster Kubernetes rilevato automaticamente. Il collegamento "Go to NKS" (Vai a NKS) consente di accedere direttamente al NetApp Kubernetes Service.



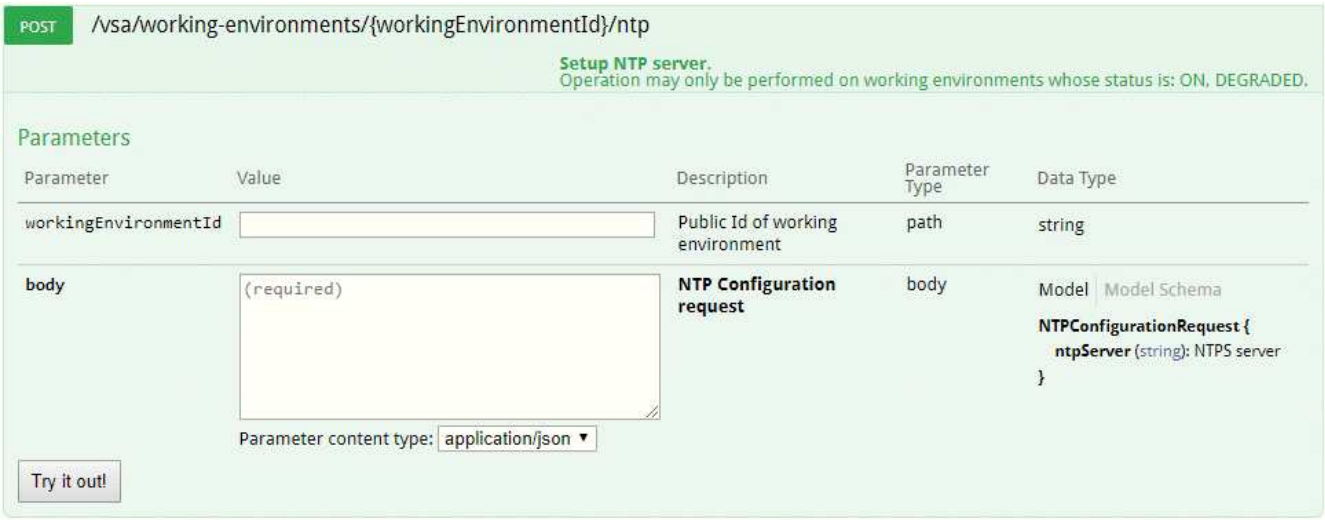
"Scopri come connettere i tuoi ambienti di lavoro ai cluster Kubernetes".

Possibilità di configurare un server NTP

È ora possibile configurare Cloud Volumes ONTAP in modo che utilizzi un server NTP (Network Time Protocol). La specifica di un server NTP sincronizza l'ora tra i sistemi della rete, evitando così problemi dovuti a differenze di tempo.

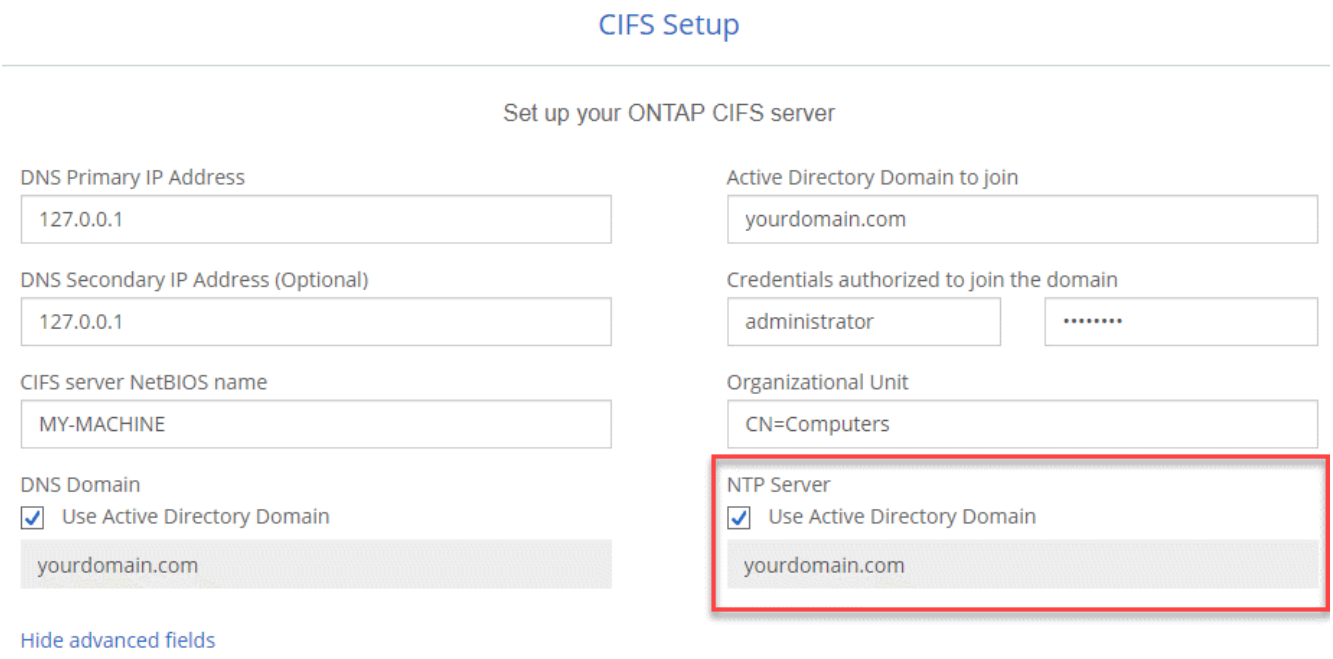
Specificare un server NTP utilizzando l'API Cloud Manager o dall'interfaccia utente quando si imposta un server CIFS:

- Il "API di Cloud Manager" Consente di specificare qualsiasi indirizzo per il server NTP. Ecco l'API per un sistema a nodo singolo in AWS:



- Quando si configura un server CIFS, l'interfaccia utente di Cloud Manager consente di specificare un server NTP che utilizza il dominio Active Directory. Se è necessario utilizzare un indirizzo diverso, utilizzare l'API.

  L'immagine seguente mostra il campo Server NTP, disponibile durante l'impostazione di CIFS.



Cloud Manager 3.6.5 (2 aprile 2019)

Cloud Manager 3.6.5 include i seguenti miglioramenti.

- Miglioramenti di Kubernetes
- Gli account NetApp Support Site sono ora gestiti a livello di sistema
- I gateway di transito AWS possono consentire l'accesso a indirizzi IP mobili
- I gruppi di risorse Azure sono ora bloccati
- NFS 4 e NFS 4.1 sono ora abilitati per impostazione predefinita
- Una nuova API consente di eliminare le copie Snapshot di ONTAP

Miglioramenti di Kubernetes

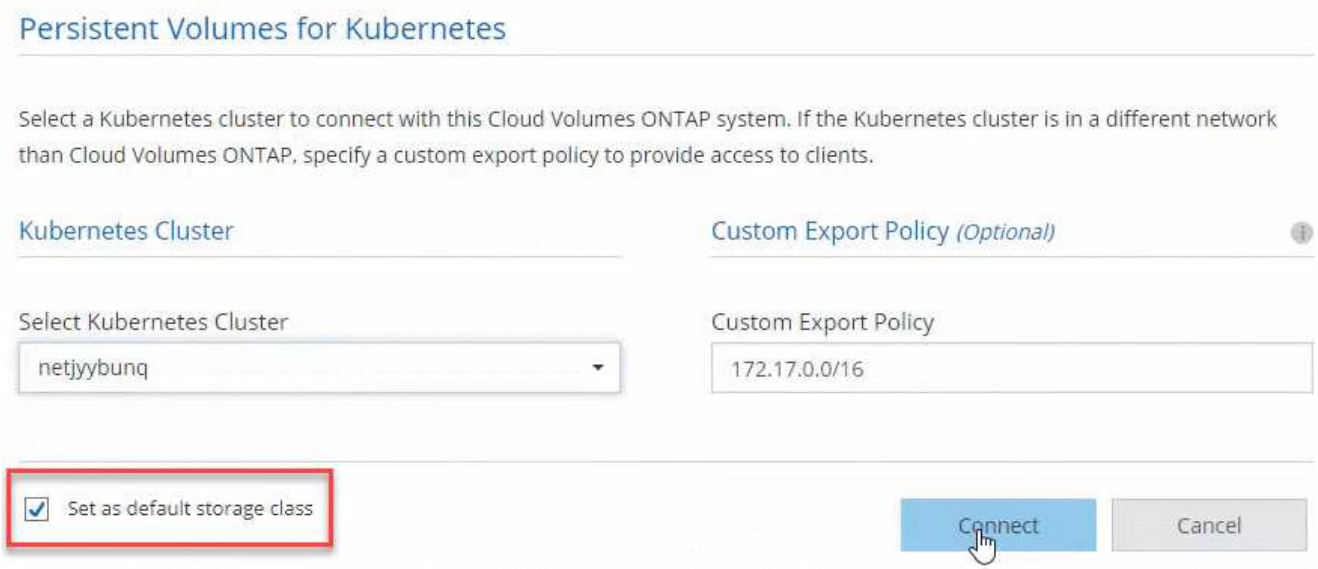
Abbiamo apportato alcuni miglioramenti che semplificano l'utilizzo di Cloud Volumes ONTAP come storage persistente per i container:

- Ora puoi aggiungere più cluster Kubernetes a Cloud Manager.

  In questo modo è possibile collegare diversi cluster a diversi sistemi Cloud Volumes ONTAP e più cluster allo stesso sistema Cloud Volumes ONTAP.

- Quando si connette un cluster, è ora possibile impostare Cloud Volumes ONTAP come classe di storage predefinita per il cluster Kubernetes.

  Quando un utente crea un volume persistente, il cluster Kubernetes può utilizzare Cloud Volumes ONTAP come storage back-end per impostazione predefinita:



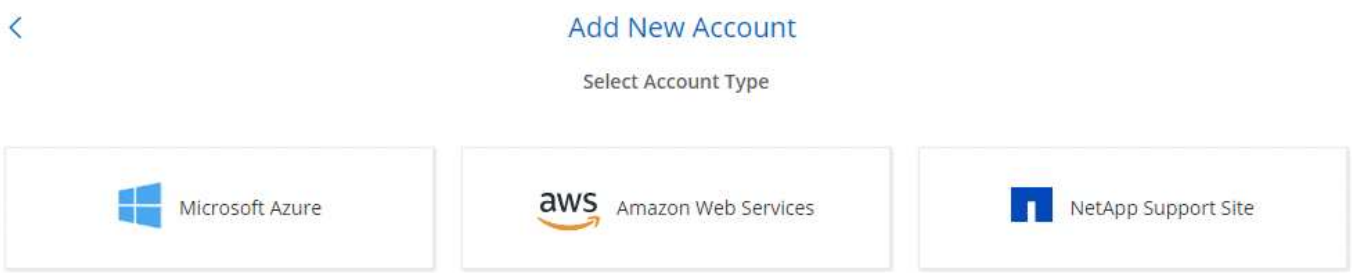
- Abbiamo modificato il modo in cui Cloud Manager nomina le classi di storage Kubernetes in modo che siano più facilmente identificabili:
  - **netapp-file**: Per associare un volume persistente a un sistema Cloud Volumes ONTAP a nodo singolo
  - **netapp-file-Redundant**: Per associare un volume persistente a una coppia Cloud Volumes ONTAP ha
- La versione di NetApp Trident installata da Cloud Manager è stata aggiornata alla versione più recente.

"Scopri come utilizzare Cloud Volumes ONTAP come storage persistente per Kubernetes".

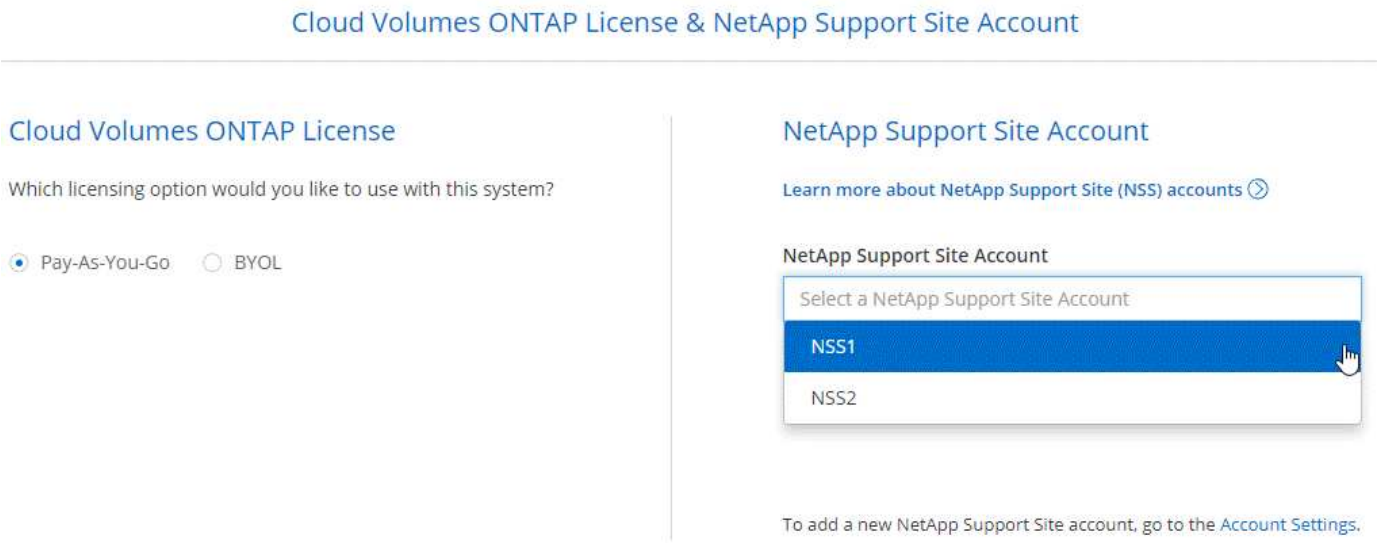
Gli account NetApp Support Site sono ora gestiti a livello di sistema

Ora è più semplice gestire gli account NetApp Support Site in Cloud Manager.

Nelle versioni precedenti, era necessario collegare un account NetApp Support Site a un tenant specifico. Gli account vengono ora gestiti a livello di sistema Cloud Manager nello stesso posto in cui si gestiscono gli account dei provider di cloud. Questa modifica offre la flessibilità di scegliere tra più account del sito di supporto NetApp durante la registrazione dei sistemi Cloud Volumes ONTAP.



Quando si crea un nuovo ambiente di lavoro, è sufficiente selezionare l'account del sito di supporto NetApp per registrare il sistema Cloud Volumes ONTAP con:



Quando Cloud Manager esegue l'aggiornamento alla versione 3.6.5, aggiunge automaticamente gli account NetApp Support Site, se in precedenza si erano collegati i tenant con un account.

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

I gateway di transito AWS possono consentire l'accesso a indirizzi IP mobili

Una coppia ha in più zone di disponibilità AWS utilizza *indirizzi IP mobili* per l'accesso ai dati NAS e per le interfacce di gestione. Fino ad ora, gli indirizzi IP mobili non sono stati accessibili dall'esterno del VPC in cui risiede la coppia ha.

Abbiamo verificato che puoi utilizzare un "Gateway di transito AWS" Per abilitare l'accesso agli indirizzi IP mobili dall'esterno del VPC. Ciò significa che i tool di gestione NetApp e i client NAS esterni al VPC possono accedere agli IP mobili e sfruttare il failover automatico.

"Scopri come configurare un gateway di transito AWS per coppie ha in più AZS".

I gruppi di risorse Azure sono ora bloccati

Cloud Manager ora blocca i gruppi di risorse Cloud Volumes ONTAP in Azure quando li crea. Il blocco dei gruppi di risorse impedisce agli utenti di eliminare o modificare accidentalmente le risorse critiche.

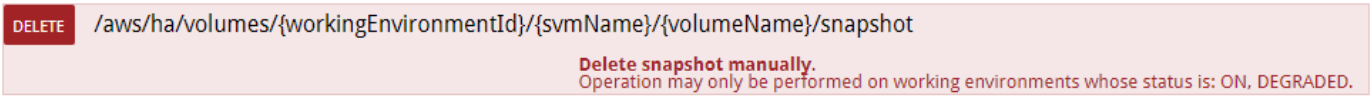
NFS 4 e NFS 4.1 sono ora abilitati per impostazione predefinita

Cloud Manager ora abilita i protocolli NFS 4 e NFS 4.1 su ogni nuovo sistema Cloud Volumes ONTAP creato. Questa modifica consente di risparmiare tempo perché non è più necessario attivare manualmente tali protocolli.

Una nuova API consente di eliminare le copie Snapshot di ONTAP

È ora possibile eliminare le copie Snapshot dei volumi di lettura/scrittura utilizzando una chiamata API di Cloud Manager.

Ecco un esempio della chiamata API per un sistema ha in AWS:



Chiamate API simili sono disponibili per i sistemi a nodo singolo in AWS e per i sistemi a nodo singolo e ha in Azure.

"Guida per sviluppatori API di Cloud Manager OnCommand"

Aggiornamento di Cloud Manager 3.6.4 (18 marzo 2019)

Cloud Manager è stato aggiornato per supportare la release di patch 9.5 P1 per Cloud Volumes ONTAP. Con questa release di patch, le coppie ha in Azure sono ora generalmente disponibili (GA).

Vedere "Note sulla versione di Cloud Volumes ONTAP 9.5" Per ulteriori dettagli, incluse informazioni importanti sul supporto della regione Azure per le coppie ha.

Cloud Manager 3.6.4 (3 marzo 2019)

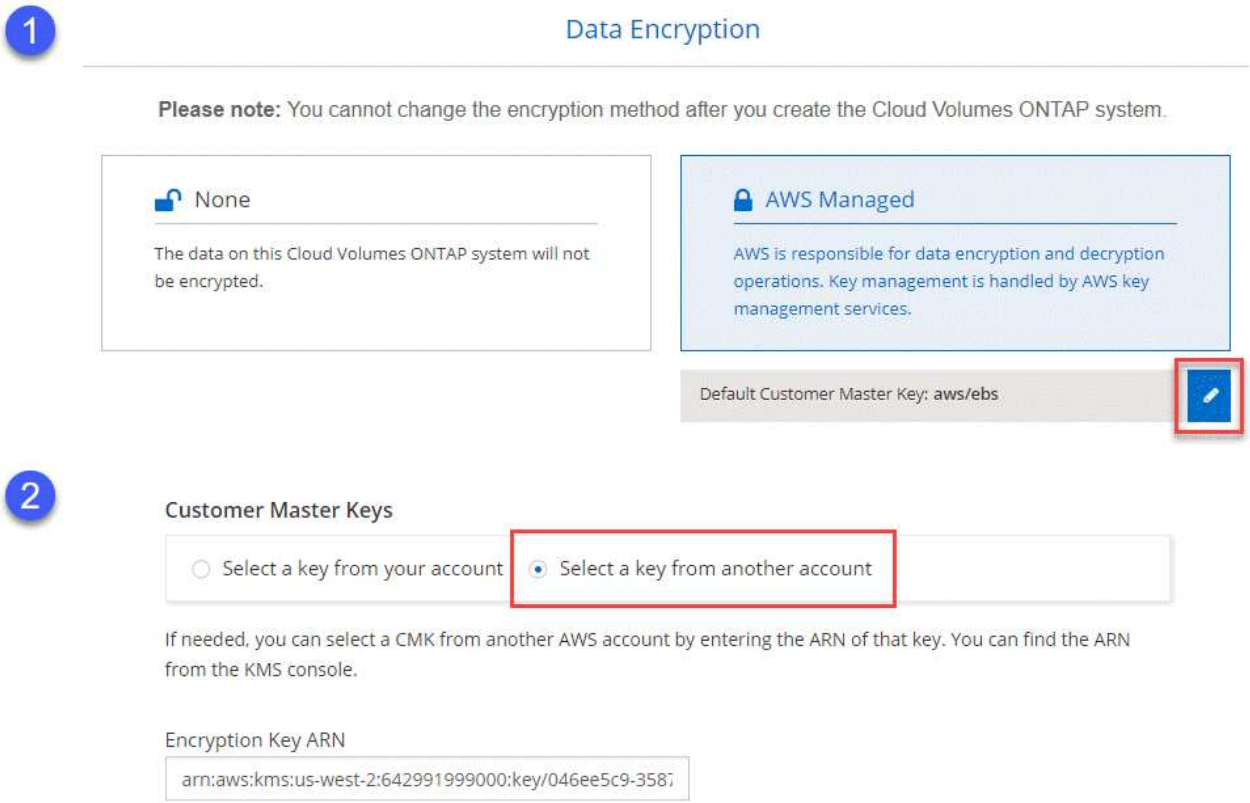
Cloud Manager 3.6.4 include i seguenti miglioramenti.

- Crittografia gestita da AWS con una chiave di un altro account
- Ripristino dei dischi guasti
- Gli account di storage Azure sono abilitati per HTTPS quando si esegue il tiering dei dati nei container Blob

Crittografia gestita da AWS con una chiave di un altro account

Quando si avvia un sistema Cloud Volumes ONTAP in AWS, è possibile attivarlo "Crittografia gestita da AWS" Utilizzo di una chiave master cliente (CMK) da un altro account utente AWS.

Le seguenti immagini mostrano come selezionare l'opzione quando si crea un nuovo ambiente di lavoro:



"Scopri di più sulle tecnologie di crittografia supportate".

Ripristino dei dischi guasti

Cloud Manager tenta ora di ripristinare i dischi guasti dai sistemi Cloud Volumes ONTAP. I tentativi riusciti vengono annotati nei report di notifica via email. Ecco un esempio di notifica:

È possibile attivare i report di notifica modificando l'account utente.

Gli account di storage Azure sono abilitati per HTTPS quando si esegue il tiering dei dati nei container Blob

Quando si imposta un sistema Cloud Volumes ONTAP per il Tier dei dati inattivi in un container di Azure Blob, Cloud Manager crea un account di storage Azure per quel container. A partire da questa release, Cloud Manager ora abilita nuovi account storage con trasferimento sicuro (HTTPS). Gli account di storage esistenti continuano a utilizzare HTTP.

Cloud Manager 3.6.3 (4 febbraio 2019)

Cloud Manager 3.6.3 include i seguenti miglioramenti.

- Supporto per Cloud Volumes ONTAP 9.5 GA
- Limite di capacità di 368 TB per tutte le configurazioni Premium e BYOL
- Supporto per nuove regioni AWS
- Supporto di S3 Intelligent-Tiering
- Possibilità di disattivare il tiering dei dati sull'aggregato iniziale
- Tipo di istanza EC2 consigliato ora t3.medium per Cloud Manager
- Rinvio degli arresti pianificati durante i trasferimenti di dati

Supporto per Cloud Volumes ONTAP 9.5 GA

Cloud Manager ora supporta la release di disponibilità generale (GA) di Cloud Volumes ONTAP 9.5. Questo include il supporto per le istanze M5 e R5 in AWS. Per ulteriori informazioni sulla versione 9.5, vedere "Note sulla versione di Cloud Volumes ONTAP 9.5".

Limite di capacità di 368 TB per tutte le configurazioni Premium e BYOL

Il limite di capacità del sistema per Cloud Volumes ONTAP Premium e BYOL è ora di 368 TB in tutte le configurazioni: Nodo singolo e ha in AWS e Azure. Questa modifica si applica a Cloud Volumes ONTAP 9.5, 9.4 e 9.3 (AWS solo con 9.3).

Per alcune configurazioni, i limiti dei dischi impediscono di raggiungere il limite di capacità di 368 TB utilizzando solo i dischi. In questi casi, è possibile raggiungere il limite di capacità di 368 TB di "tiering dei dati inattivi sullo storage a oggetti". Ad esempio, un sistema a nodo singolo in Azure potrebbe avere 252 TB di capacità basata su disco, che consentirebbe fino a 116 TB di dati inattivi nello storage Azure Blob.

Per informazioni sui limiti dei dischi, fare riferimento ai limiti di storage nella "Note di rilascio di Cloud Volumes ONTAP".

Supporto per nuove regioni AWS

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

- Europa (Stoccolma)

  Solo sistemi a nodo singolo. Le coppie HA non sono attualmente supportate.

- GovCloud (USA-Est)

  Oltre al supporto per l'area AWS GovCloud (USA-ovest).

"Consulta l'elenco completo delle regioni supportate".

Supporto di S3 Intelligent-Tiering

Quando si attiva il tiering dei dati in AWS, Cloud Volumes ONTAP esegue il tiering dei dati inattivi nella classe di storage S3 Standard per impostazione predefinita. È ora possibile modificare il livello di tiering nella classe di storage *Intelligent Tiering*. Questa classe di storage ottimizza i costi di storage spostando i dati tra due livelli in base al cambiamento dei modelli di accesso ai dati. Un livello è per l'accesso frequente e l'altro per l'accesso non frequente.

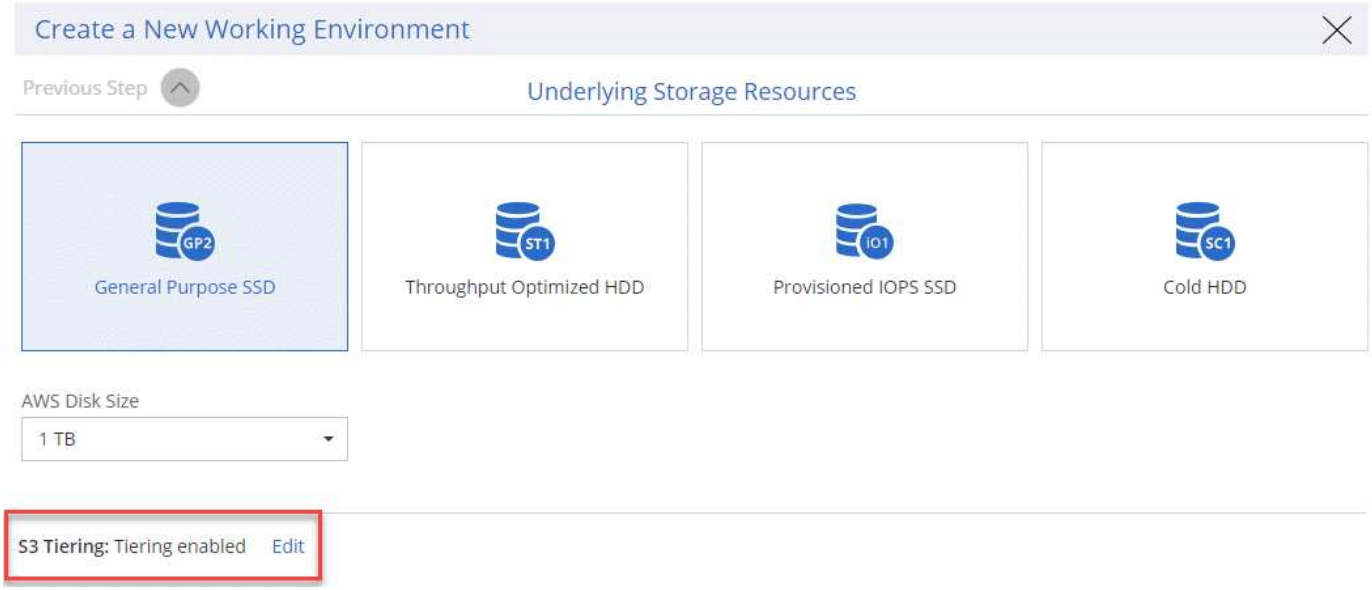
Come nelle release precedenti, è possibile utilizzare anche il Tier di accesso standard-non frequente e il Tier di accesso one zone-non frequente.

"Scopri di più sul tiering dei dati" e. "scopri come cambiare la classe di storage".

Possibilità di disattivare il tiering dei dati sull'aggregato iniziale

Nelle versioni precedenti, Cloud Manager ha attivato automaticamente il tiering dei dati sull'aggregato Cloud Volumes ONTAP iniziale. È ora possibile scegliere di disattivare il tiering dei dati su questo aggregato iniziale. È possibile attivare o disattivare il tiering dei dati anche sugli aggregati successivi.

Questa nuova opzione è disponibile quando si scelgono le risorse di storage sottostanti. L'immagine seguente mostra un esempio quando si avvia un sistema in AWS:



Tipo di istanza EC2 consigliato ora t3.medium per Cloud Manager

Il tipo di istanza per Cloud Manager è ora t3.medium quando si implementa Cloud Manager in AWS da NetApp Cloud Central. È anche il tipo di istanza consigliato in AWS Marketplace. Questa modifica consente il supporto nelle regioni AWS più recenti e riduce i costi delle istanze. Il tipo di istanza consigliato in precedenza era t2.medium, che è ancora supportato.

Rinvio degli arresti pianificati durante i trasferimenti di dati

Se è stato pianificato 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.

Cloud Manager 3.6.2 (2 gennaio 2019)

Cloud Manager 3.6.2 include nuove funzionalità e miglioramenti.

- Gruppo di posizionamento AWS Spread per Cloud Volumes ONTAP ha in un singolo AZ
- Protezione ransomware
- Nuove policy di replica dei dati
- Controllo dell'accesso al volume per Kubernetes

Gruppo di posizionamento AWS Spread per Cloud Volumes ONTAP ha in un singolo AZ

Quando si implementa Cloud Volumes ONTAP ha in una singola area di disponibilità AWS, ora viene creato 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.

Cloud Manager richiede nuove autorizzazioni per questa funzionalità. Assicurarsi che il criterio IAM che fornisce le autorizzazioni a Cloud Manager includa le seguenti azioni:

```
"ec2:CreatePlacementGroup",
"ec2:DeletePlacementGroup"
```

L'elenco completo delle autorizzazioni richieste è disponibile nella "Policy AWS più recente per Cloud Manager".

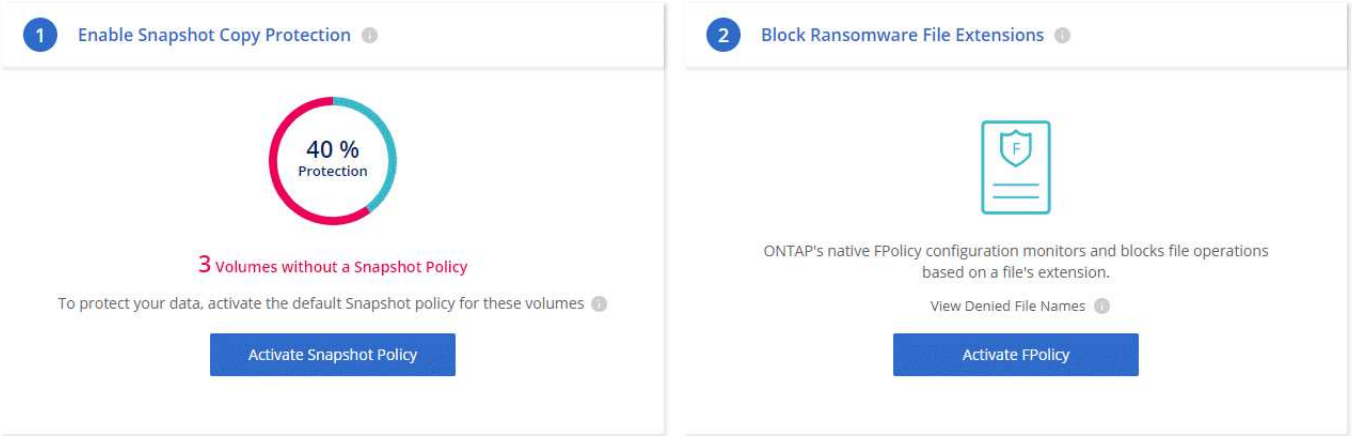
Protezione ransomware

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

Nuove policy di replica dei dati

Cloud Manager include cinque nuove policy di replica dei dati che è possibile utilizzare per la protezione dei dati.

Tre dei criteri configurano il disaster recovery e la conservazione a lungo termine dei backup sullo stesso volume di destinazione. Ogni policy offre un diverso periodo di conservazione del backup:

- Mirror e backup (7 anni di conservazione)
- Mirror e backup (7 anni di conservazione con più backup settimanali)
- Mirror e backup (1 anno di conservazione, mensile)

Le restanti policy offrono più opzioni per la conservazione a lungo termine dei backup:

- Backup (1 mese di conservazione)
- Backup (conservazione di 1 settimana)

È sufficiente trascinare un ambiente di lavoro per selezionare una delle nuove policy.

Controllo dell'accesso al volume per Kubernetes

È ora possibile configurare il criterio di esportazione per i volumi persistenti Kubernetes. Il criterio di esportazione può consentire l'accesso ai client se il cluster Kubernetes si trova in una rete diversa da quella del sistema Cloud Volumes ONTAP.

È possibile configurare il criterio di esportazione quando si connette un ambiente di lavoro a un cluster Kubernetes e modificando un volume esistente.

Cloud Manager 3.6.1 (4 dicembre 2018)

Cloud Manager 3.6.1 include nuove funzionalità e miglioramenti.

- Supporto per Cloud Volumes ONTAP 9.5 in Azure
- Account Cloud Provider
- Miglioramenti al report dei costi AWS
- Supporto per nuove aree Azure

Supporto per Cloud Volumes ONTAP 9.5 in Azure

Cloud Manager ora supporta la release Cloud Volumes ONTAP 9.5 in Microsoft Azure, che include un'anteprima delle coppie ad alta disponibilità (ha). Puoi richiedere una licenza di anteprima per una coppia Azure ha contattandoci all'indirizzo ng-Cloud-Volume-ONTAP-preview@netapp.com.

Per ulteriori informazioni sulla versione 9.5, vedere "Note sulla versione di Cloud Volumes ONTAP 9.5".

Nuove autorizzazioni Azure richieste per Cloud Volumes ONTAP 9.5

Cloud Manager richiede nuove autorizzazioni Azure per le funzionalità chiave della release Cloud Volumes ONTAP 9.5. Per garantire che Cloud Manager possa implementare e gestire i sistemi Cloud Volumes ONTAP 9.5, è necessario aggiornare la policy di Cloud Manager aggiungendo le seguenti autorizzazioni:

```
"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",
"Microsoft.Network/routeTables/join/action"
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",
"Microsoft.Web/sites/*"
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/usages/read",
```

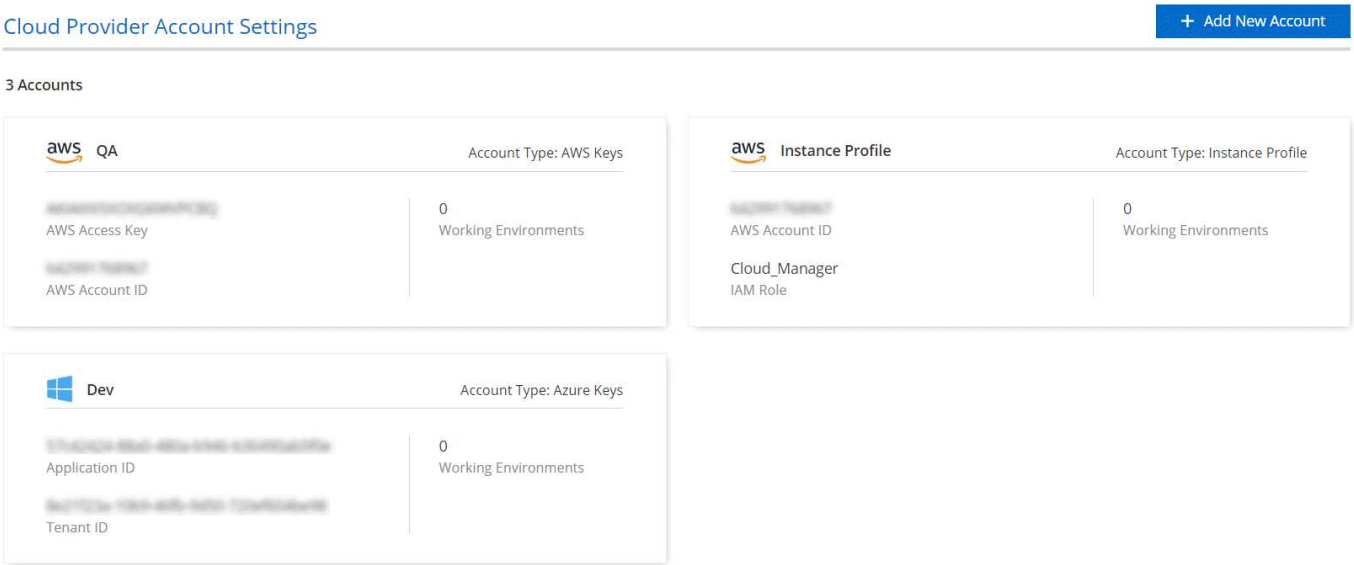
L'elenco completo delle autorizzazioni richieste è disponibile nella "Ultima policy di Azure per Cloud Manager".

"Scopri come Cloud Manager utilizza queste autorizzazioni".

Account Cloud Provider

Ora è più semplice gestire più account AWS e Azure in Cloud Manager utilizzando gli account Cloud Provider.

Nelle versioni precedenti, era necessario specificare le autorizzazioni del provider cloud per ciascun account utente di Cloud Manager. Le autorizzazioni vengono ora gestite a livello di sistema Cloud Manager utilizzando gli account Cloud Provider.



Quando si crea un nuovo ambiente di lavoro, è sufficiente selezionare l'account in cui si desidera implementare il sistema Cloud Volumes ONTAP:

Quando esegui l'aggiornamento alla versione 3.6.1, Cloud Manager crea automaticamente account Cloud Provider in base alla configurazione corrente. Se si dispone di script, la compatibilità con le versioni precedenti è attiva, quindi non si verifica alcuna interruzione.

- "Scopri come funzionano gli account e le autorizzazioni dei provider cloud"
- "Scopri come configurare e aggiungere account Cloud Provider a Cloud Manager"

Miglioramenti al report dei costi AWS

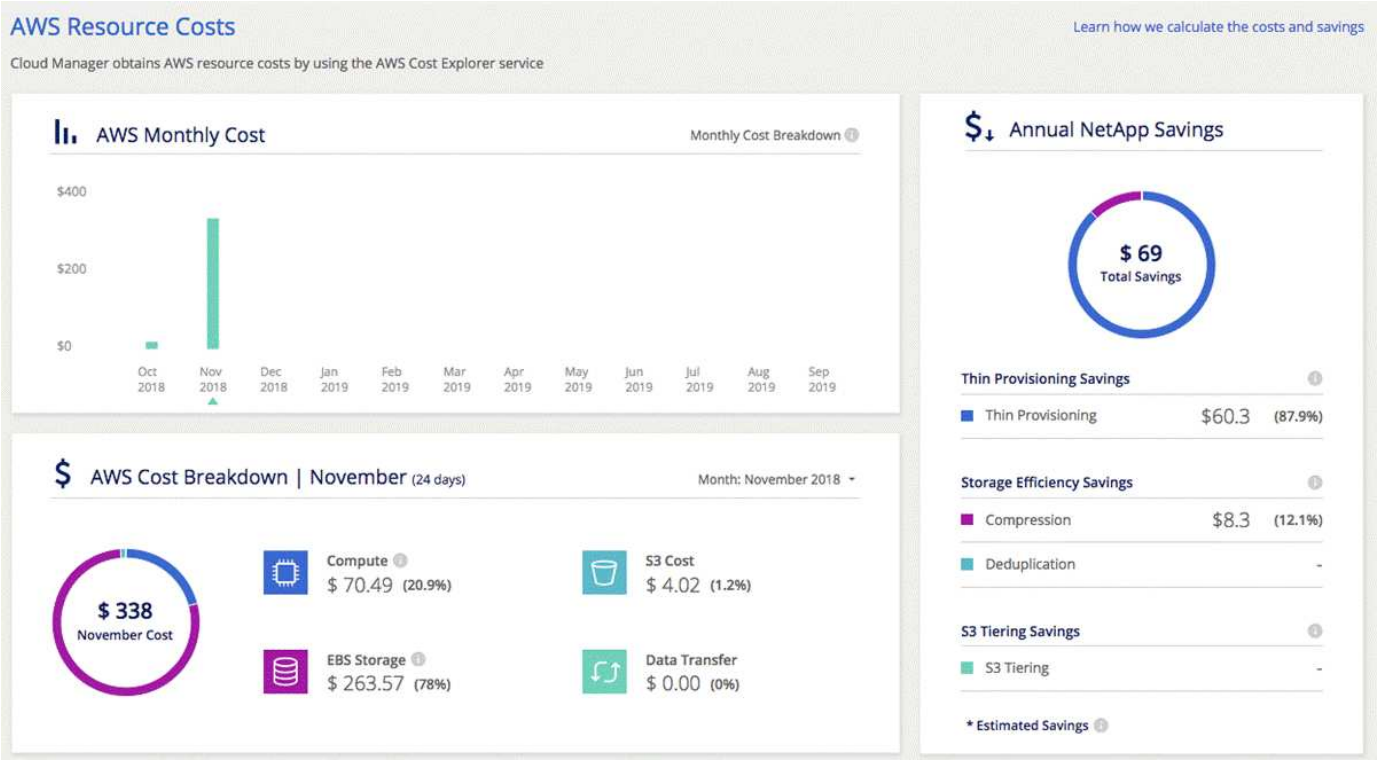
Il report dei costi AWS ora fornisce ulteriori informazioni ed è più semplice da configurare.

- Il report suddivide i costi mensili delle risorse associati all'esecuzione di Cloud Volumes ONTAP in AWS. È possibile visualizzare i costi mensili per calcolo, storage EBS (incluse le snapshot EBS), storage S3 e trasferimenti di dati.
- Il report mostra ora i risparmi sui costi quando si esegue il tiering dei dati inattivi in S3.
- Abbiamo anche semplificato il modo in cui Cloud Manager ottiene i dati sui costi da AWS.

  Cloud Manager non ha più bisogno di accedere ai report di fatturazione memorizzati in un bucket S3. Cloud Manager utilizza invece l'API di Cost Explorer. Devi solo assicurarti che la policy 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 fornita da NetApp". I nuovi sistemi implementati da NetApp Cloud Central includono automaticamente queste autorizzazioni.



Supporto per nuove aree Azure

Ora puoi implementare Cloud Manager e Cloud Volumes ONTAP nella regione centrale della Francia.

Cloud Manager 3.6 (4 novembre 2018)

Cloud Manager 3.6 include una nuova funzionalità.

Utilizzo di Cloud Volumes ONTAP come storage persistente per un cluster Kubernetes

Cloud Manager può ora automatizzare l'implementazione di "Trident di NetApp" Su un singolo cluster Kubernetes in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container. Gli utenti possono quindi richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi, sfruttando al contempo le funzionalità avanzate di gestione dei dati di ONTAP senza doverne conoscere nulla.

"Scopri come connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes"

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 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.

Limitazioni di Volume View

- La vista volume non è supportata nell'area AWS GovCloud (USA), nell'ambiente AWS Commercial Cloud Services e in Microsoft Azure.
- La vista volume consente di creare solo volumi NFS.
- Cloud Manager non avvia le istanze di Cloud Volumes ONTAP BYOL nella vista volume.

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.

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

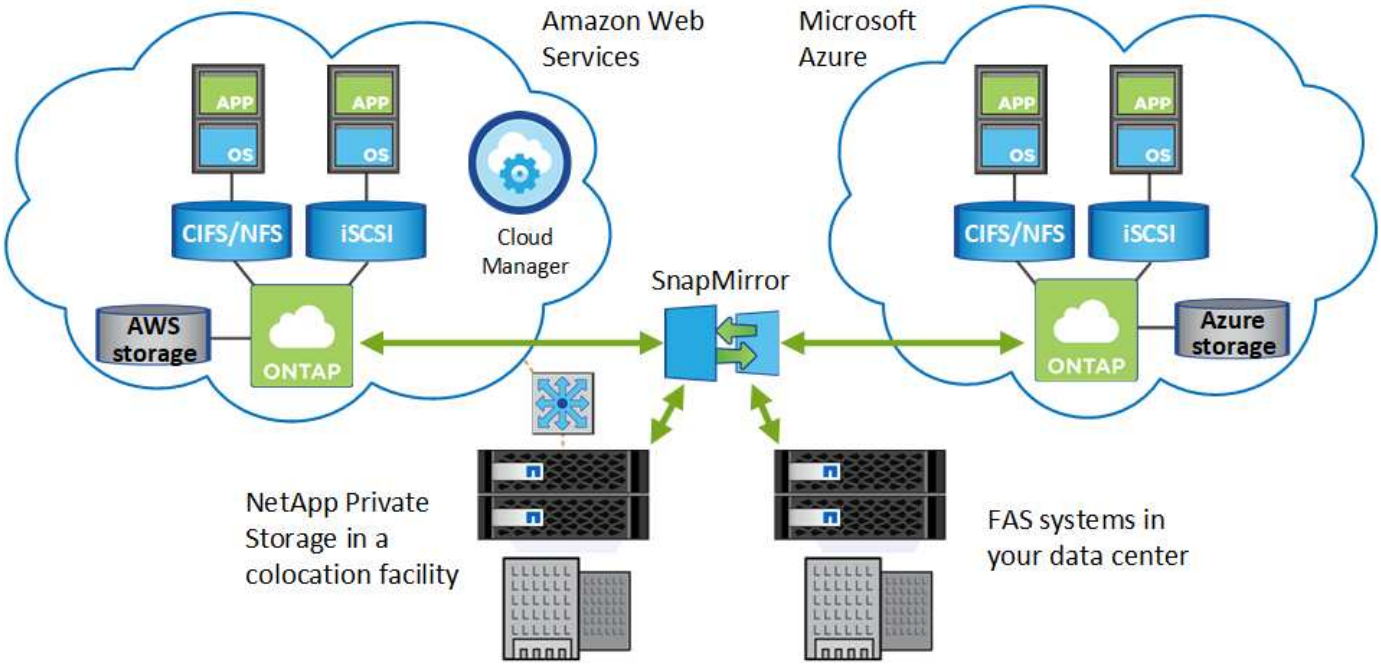
Cloud Manager di OnCommand ti consente di implementare Cloud Volumes ONTAP, che offre funzionalità di livello Enterprise per il tuo cloud storage, e di replicare facilmente i dati tra cloud ibridi basati su NetApp.

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 in esecuzione in AWS e la gestione dei sistemi Cloud Volumes ONTAP in AWS e Azure. 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, ad eccezione di NetApp Volume Encryption.

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

"Scopri di più su Cloud Volumes ONTAP"

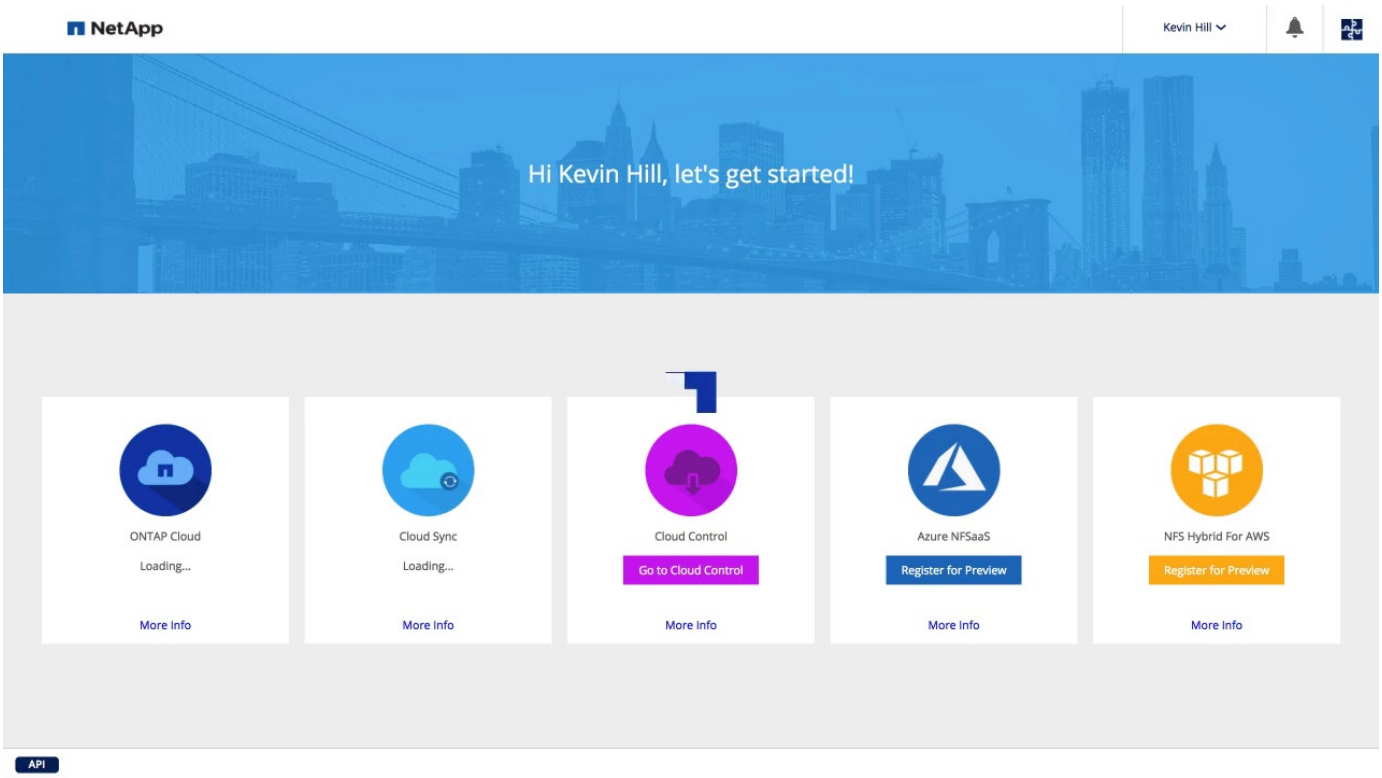
NetApp Cloud Central

"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.

Il seguente video offre una panoramica di NetApp Cloud Central:



Account e permessi dei provider di cloud

Cloud Manager ti consente di scegliere l' *account del cloud provider* in cui desideri implementare un sistema Cloud Volumes ONTAP. Prima di aggiungere gli account a Cloud Manager, è necessario comprendere i requisiti di autorizzazione.

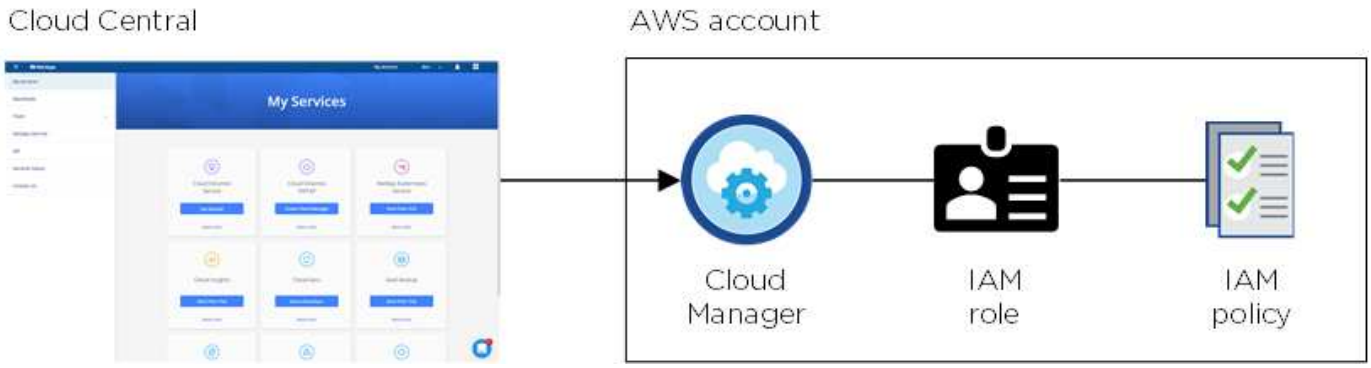
Account e autorizzazioni AWS

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".

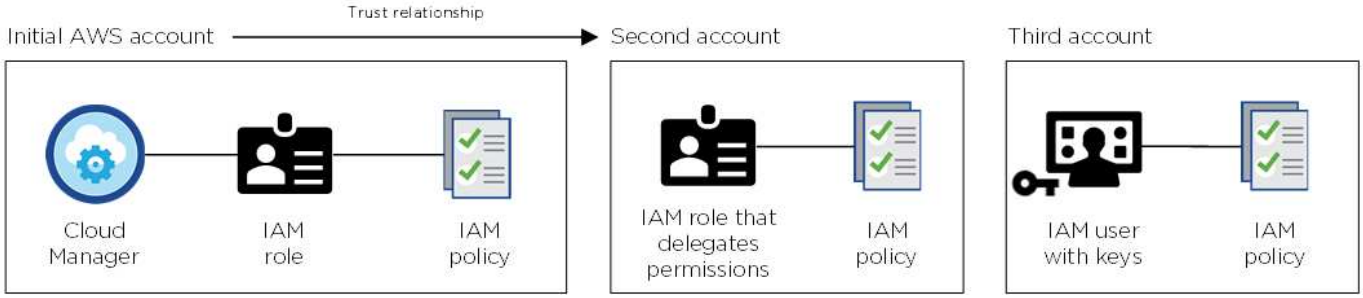
Quando Cloud Central avvia l'istanza di Cloud Manager in AWS, crea un ruolo IAM e un profilo di istanza per l'istanza. Allega inoltre una policy che fornisce a Cloud Manager le autorizzazioni per implementare e gestire Cloud Volumes ONTAP in quell'account AWS. "Analisi dell'utilizzo delle autorizzazioni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



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

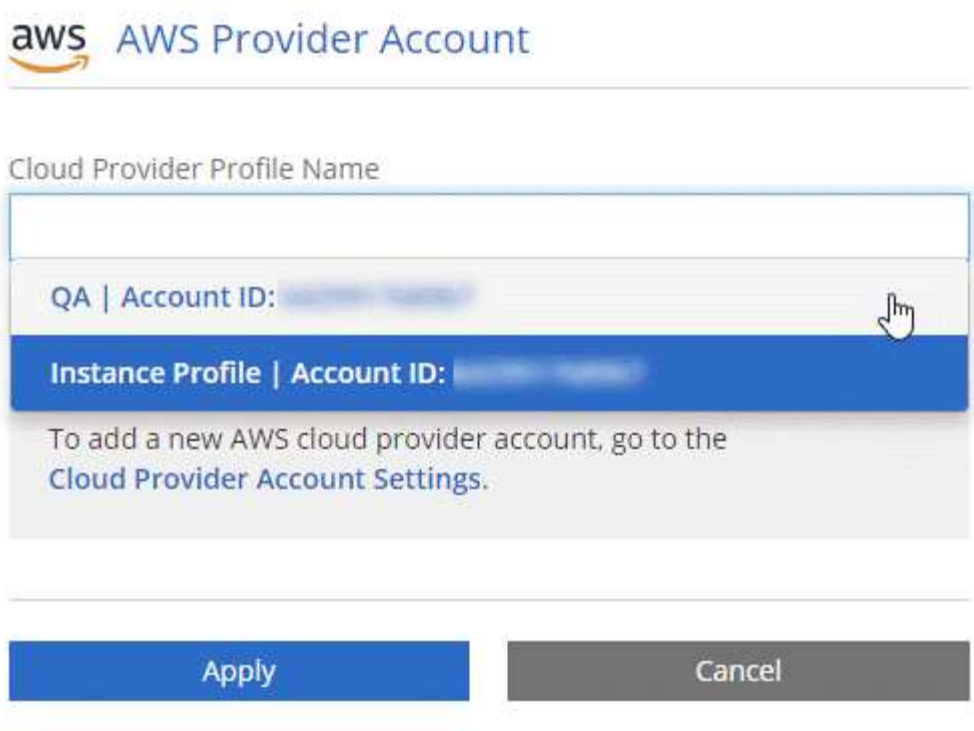
Account AWS aggiuntivi

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:



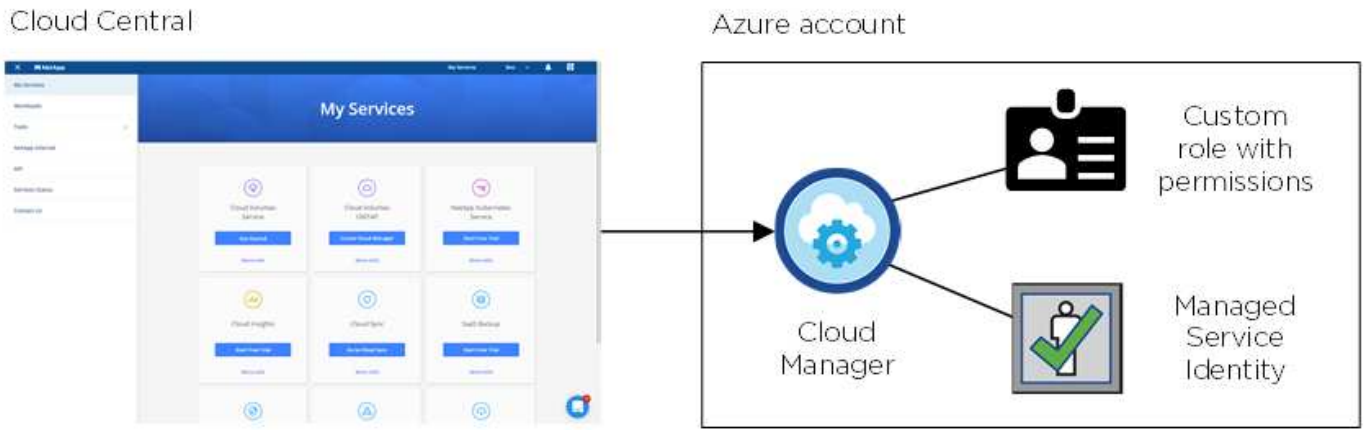
Account e autorizzazioni Azure

Puoi implementare tutti i tuoi sistemi Cloud Volumes ONTAP nell'account Azure iniziale oppure puoi impostare altri account.

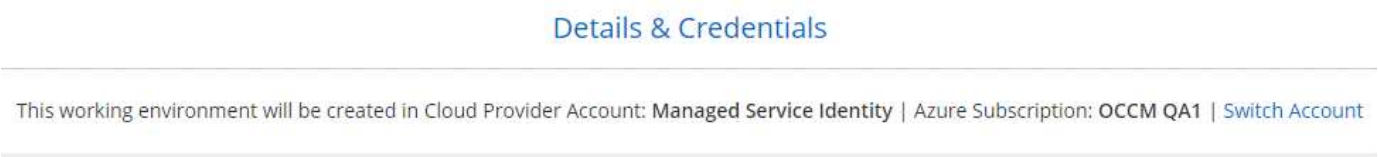
L'account Azure iniziale

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:

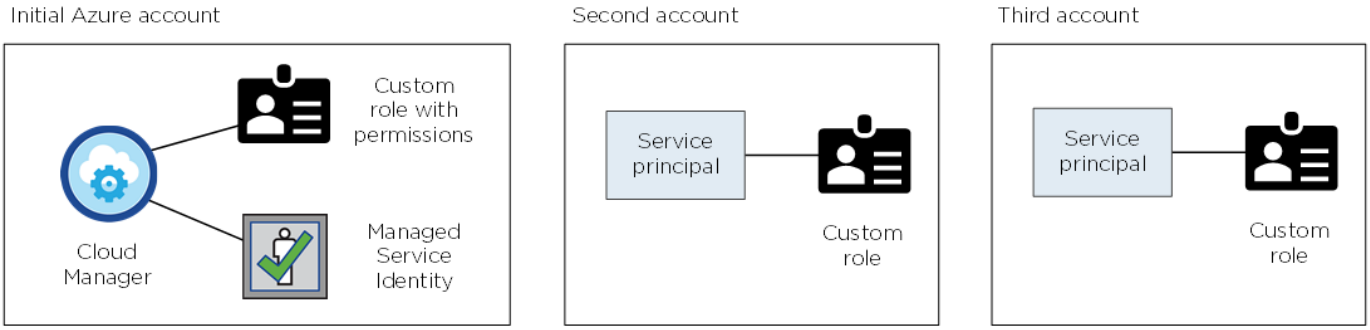


Abbonamenti Azure aggiuntivi per l'account iniziale

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".

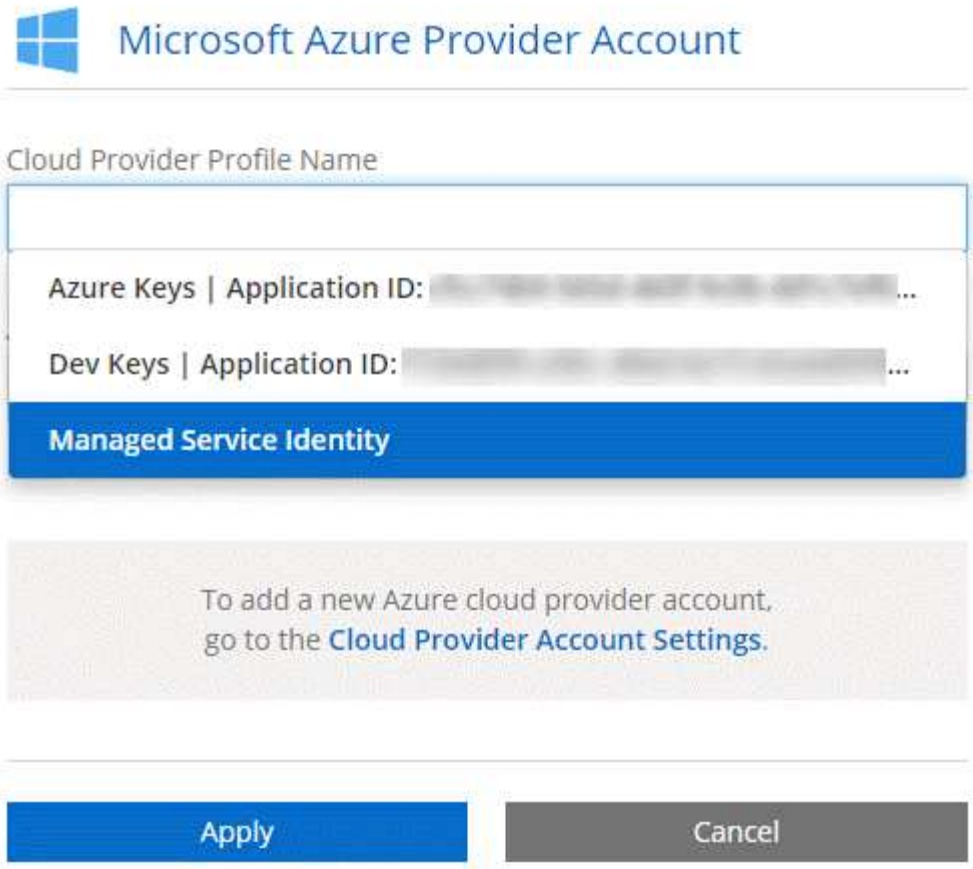
Altri account Azure

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 da "Mercato AWS", il "Azure Marketplace"e puoi farlo "Installazione di Cloud Manager on-premise".

Se si utilizza uno dei mercati, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente il ruolo IAM o l'identità gestita per Cloud Manager, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

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

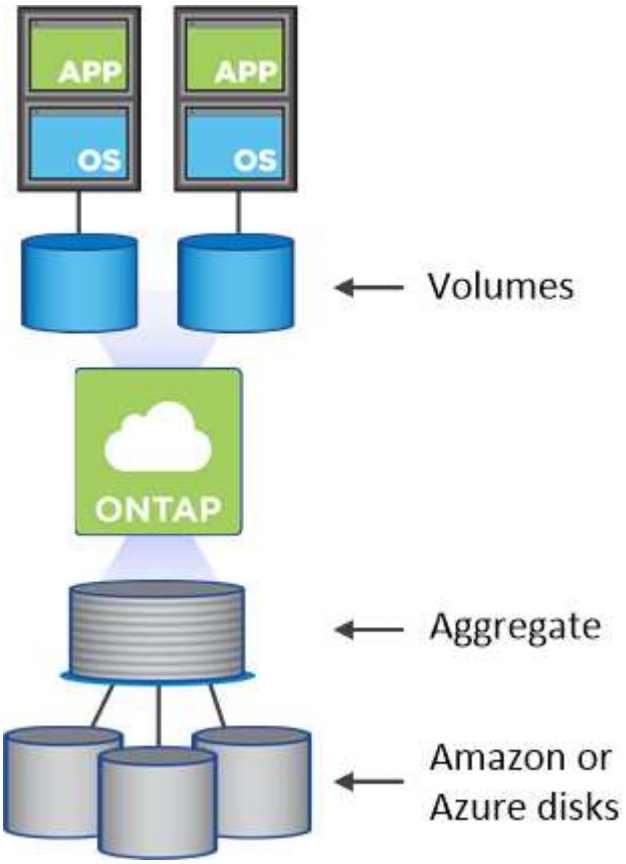
Storage

In che modo Cloud Volumes ONTAP utilizza lo storage cloud

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

Panoramica

Cloud Volumes ONTAP utilizza i volumi AWS e Azure come storage back-end. Questi volumi vengono quindi utilizzati come dischi e raggruppati in uno o più aggregati. Gli aggregati forniscono storage a uno o più volumi.



Sono supportati diversi tipi di dischi cloud. Quando si implementa Cloud Volumes ONTAP, si sceglie il tipo di disco per la creazione dei volumi e la dimensione predefinita del disco.

> La quantità totale di storage acquistata da AWS o Azure 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, 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 inoltre possibile associare un disco EBS con Amazon S3 per "tiering dei dati".

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.

Per ulteriori informazioni sui casi di utilizzo di questi dischi, fare riferimento a. "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".

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 per "tiering dei dati".

Coppie HA

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

Per ulteriori informazioni sui casi di utilizzo di questi dischi, vedere "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".

Panoramica sul tiering dei dati

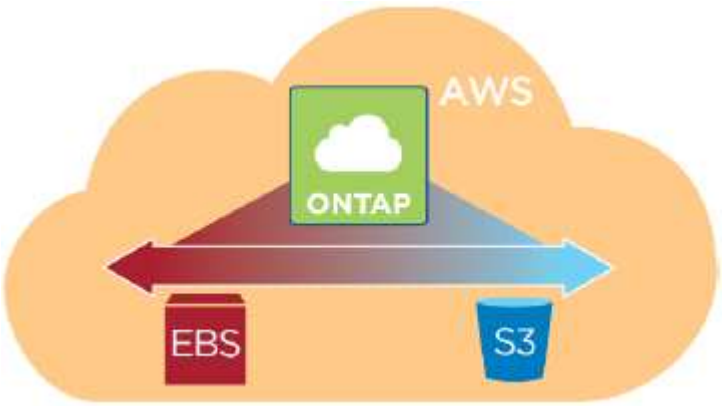
Puoi ridurre i costi di storage abilitando il tiering automatizzato dei dati inattivi su storage a oggetti a basso costo. I dati attivi rimangono in SSD o HDD ad alte prestazioni (il Tier di performance), mentre i dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo (il Tier di capacità). 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 e in Microsoft Azure. Il tiering dei dati è basato sulla tecnologia FabricPool.

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

Funzionamento del 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:



Tier di performance in AWS

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

Tier di capacità in AWS

Per impostazione predefinita, Cloud Volumes ONTAP esegue il Tier dei dati inattivi nella classe di storage S3 *Standard*. Standard è ideale per i dati ad accesso frequente memorizzati in più zone di disponibilità.

Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di storage modificando il livello di tiering di un sistema in uno dei seguenti modi, dopo aver implementato Cloud Volumes ONTAP:

Tiering intelligente
: Ottimizza i costi dello storage spostando i dati tra due livelli man mano che cambiano i modelli di accesso ai dati. Un livello è per l'accesso frequente e l'altro per l'accesso non frequente.

Accesso non frequente a una sola zona
: Per i dati ad accesso non frequente memorizzati in una singola zona di disponibilità.

Standard-infrequent Access (accesso standard-non frequente)
: Per i dati ad accesso non frequente memorizzati in più zone di disponibilità.

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. Per ulteriori informazioni sulle classi di storage S3, fare riferimento a. "Documentazione AWS".

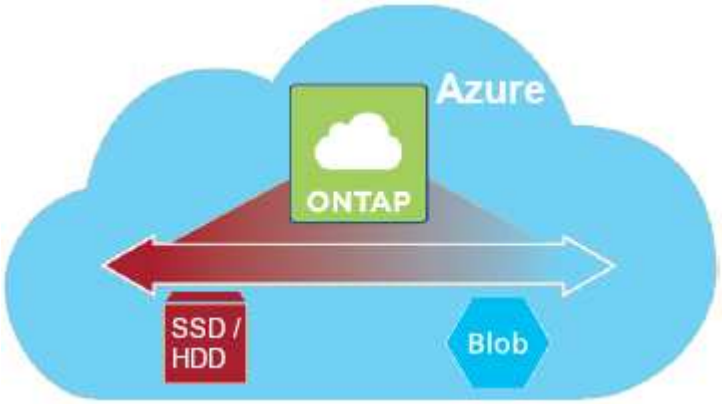
Quando si modifica il livello di tiering, i dati inattivi iniziano nella classe di storage Standard e vengono spostati nella classe di storage selezionata, se non si accede ai dati dopo 30 giorni. Per ulteriori informazioni sulla modifica del livello di tiering, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

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

Un ambiente di lavoro Cloud Volumes ONTAP utilizza un bucket S3 per tutti i dati a più livelli del sistema. Non viene utilizzato un bucket S3 diverso per ciascun volume. Ciò include un ambiente di lavoro ha. Cloud Manager crea un bucket S3 e lo nomina fabric-pool-*cluster unique identifier*.

Funzionamento del tiering dei dati in Microsoft 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 Azure Blob come Tier di capacità per i dati inattivi:



Tier di performance in Azure

Il Tier di performance può essere Premium Storage (SSD) o Standard Storage (HDD).

Tier di capacità in Azure

Per impostazione predefinita, Cloud Volumes ONTAP esegue il Tier dei dati inattivi nel Tier di storage Azure *hot*, ideale per i dati ad accesso frequente.

Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di storage modificando il livello di tiering di un sistema nel Tier di storage Azure *COOL* dopo aver implementato Cloud Volumes ONTAP. Il cool Tier è ideale per i dati ad accesso non frequente che risiedono nel Tier per almeno 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. Per ulteriori informazioni sui Tier di storage Azure Blob, fare riferimento a. "Documentazione di Azure".

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. Per ulteriori informazioni sulla modifica del livello di tiering, 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.

Un ambiente di lavoro Cloud Volumes ONTAP utilizza un container di Azure Blob per tutti i dati a più livelli del sistema. Non viene utilizzato un container diverso per ciascun volume. Cloud Manager crea un nuovo account storage con un container per ogni sistema Cloud Volumes ONTAP. Il nome dell'account di storage è casuale.

In che modo il tiering dei dati influisce sui 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 Volumes ONTAP supporta i seguenti criteri di tiering:

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.

Backup

Quando si replica un volume per il disaster recovery o la conservazione a lungo termine, i dati del volume di destinazione iniziano nel Tier di capacità. Se si attiva il volume di destinazione, i dati si spostano gradualmente al livello di performance man mano che vengono letti.

Nessuno

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

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 di Cloud Manager 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'amministratore di Cloud Manager 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

Se l'amministratore di Cloud Manager imposta la modalità di gestione della capacità su automatica, 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 manuale della capacità

Se Cloud Manager 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.

Isolamento dello storage con tenant

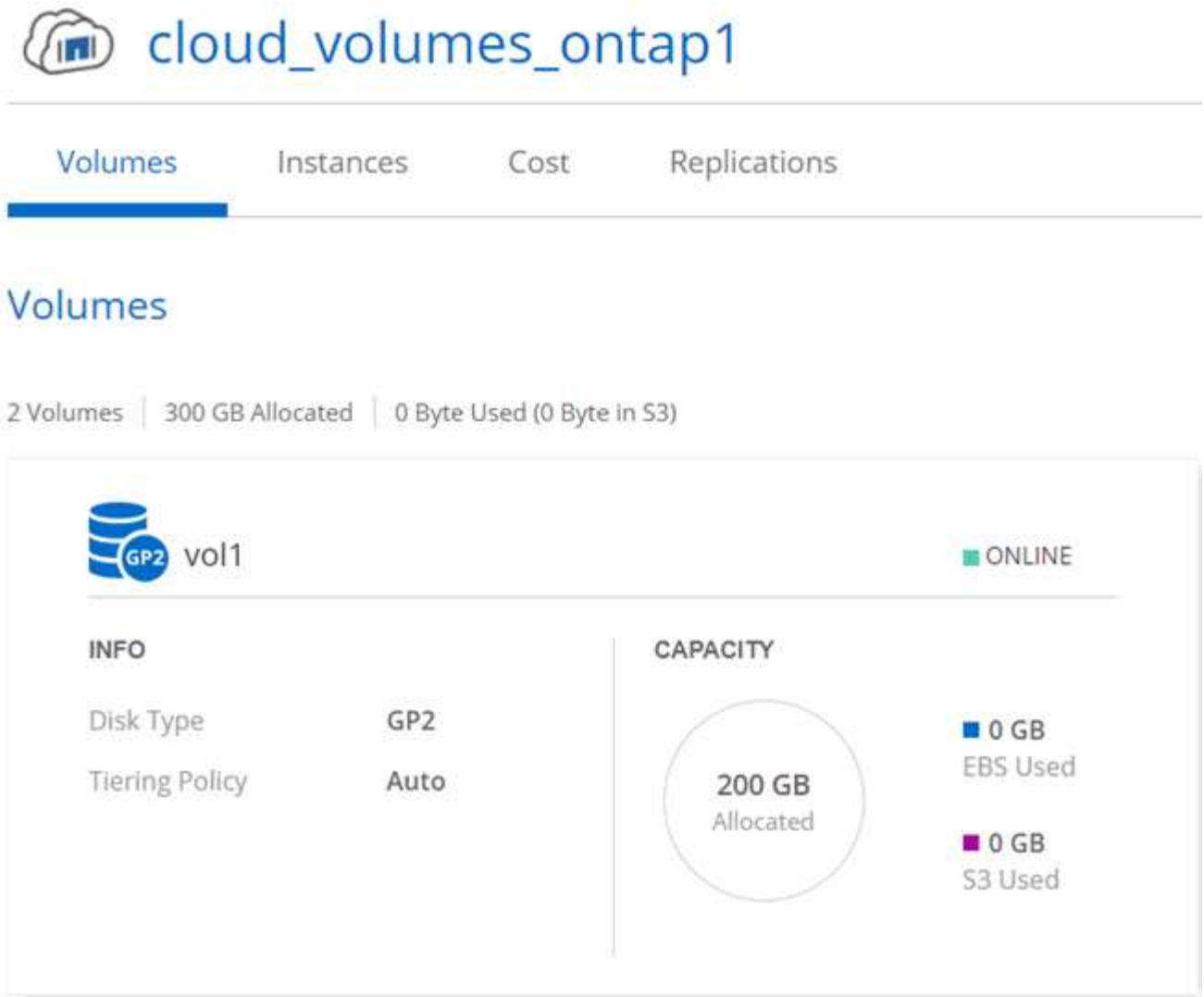
Cloud Manager consente di eseguire il provisioning e la gestione dello storage in gruppi isolati chiamati tenant. Devi decidere come organizzare gli utenti di Cloud Manager e i loro ambienti di lavoro tra i tenant.

Ambienti di lavoro

Cloud Manager rappresenta i sistemi storage come *ambienti di lavoro*. Un ambiente di lavoro è uno dei seguenti:

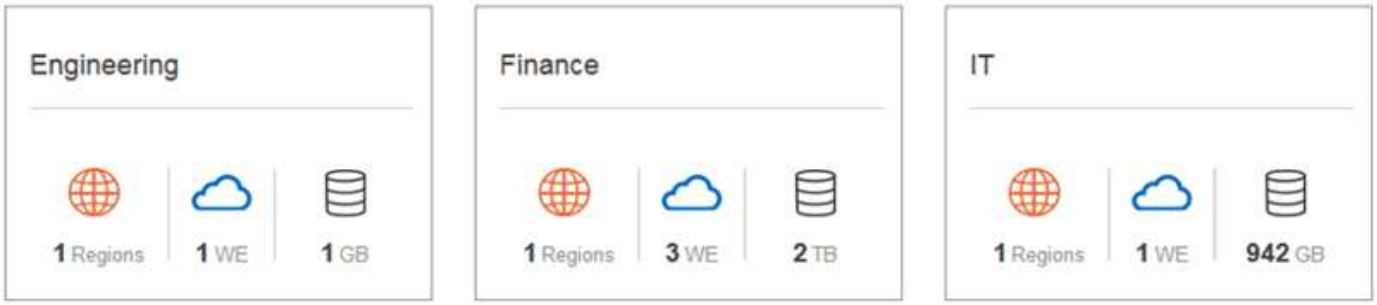
- Un singolo sistema Cloud Volumes ONTAP o una coppia ha
- Un cluster ONTAP on-premise nella rete
- Un cluster ONTAP in una configurazione di storage privato NetApp

La seguente immagine mostra un ambiente di lavoro Cloud Volumes ONTAP:



Tenant

Un *tenant* isola gli ambienti di lavoro in gruppi. Si creano uno o più ambienti di lavoro all'interno di un tenant. La seguente immagine mostra tre tenant definiti in Cloud Manager:



Gestione degli utenti di tenant e ambienti di lavoro

I tenant e gli ambienti di lavoro che gli utenti di Cloud Manager possono gestire dipendono dal ruolo e dalle assegnazioni degli utenti. I tre ruoli utente distinti sono i seguenti:

Amministratore di Cloud Manager

Amministra il prodotto e può accedere a tutti i tenant e a tutti gli ambienti di lavoro.

Amministratore tenant

Amministra un singolo tenant. Può creare e gestire tutti gli ambienti di lavoro e gli utenti del tenant.

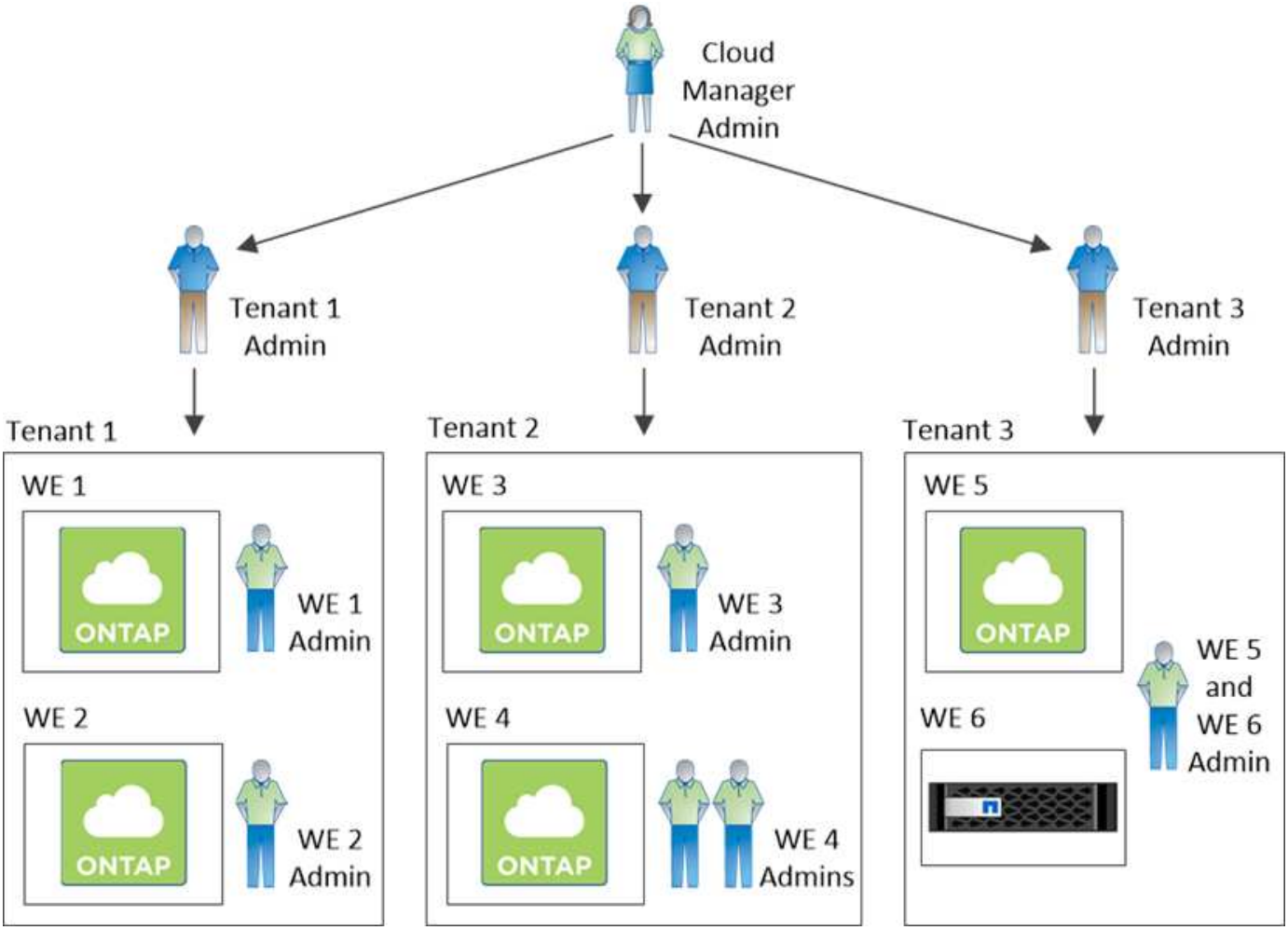
Amministratore dell'ambiente di lavoro

Può creare e gestire uno o più ambienti di lavoro in un tenant.

Esempio di come creare tenant e utenti

Se l'organizzazione dispone di reparti che operano in modo indipendente, è consigliabile disporre di un tenant per ciascun reparto.

Ad esempio, è possibile creare tre tenant per tre reparti separati. Creare quindi un amministratore tenant per ciascun tenant. All'interno di ciascun tenant si troverebbero uno o più amministratori dell'ambiente di lavoro che gestiscono gli ambienti di lavoro. La seguente immagine mostra questo scenario:



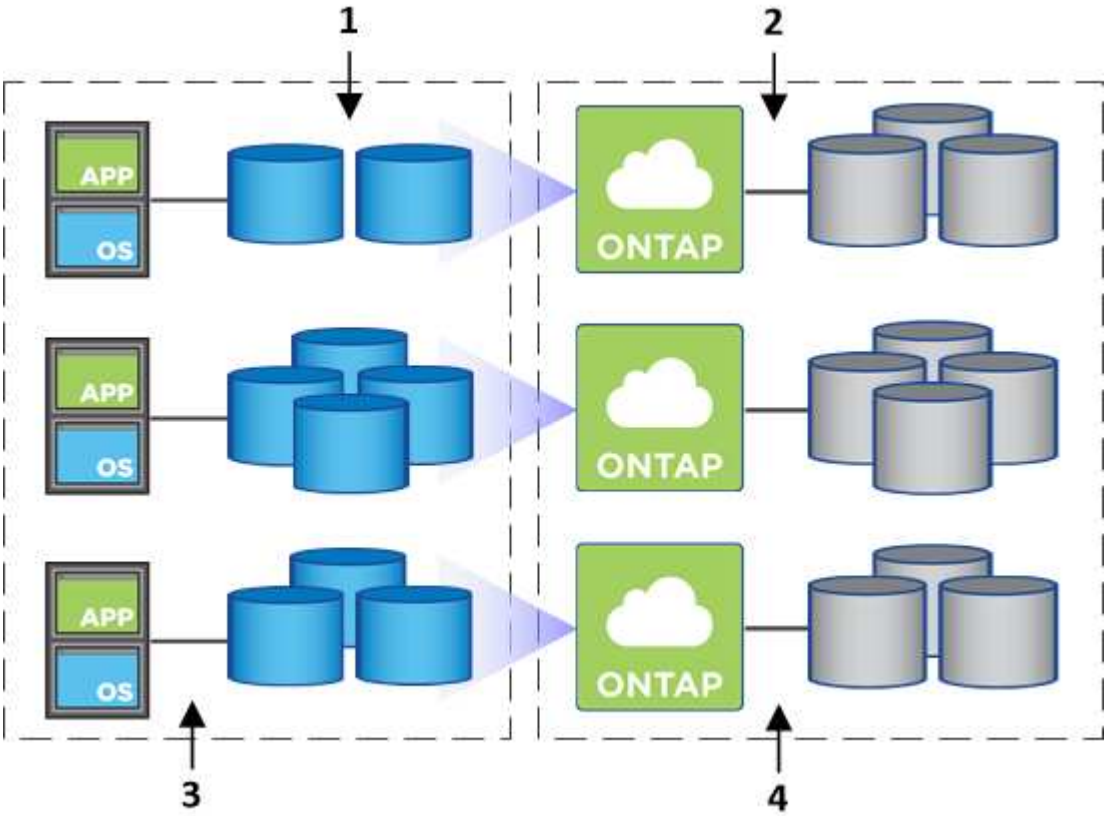
Gestione dello storage semplificata grazie a Volume View

Cloud Manager offre una vista di gestione separata denominata *Volume View*, che semplifica ulteriormente la gestione dello storage in AWS.

La vista volume consente di specificare semplicemente i volumi NFS necessari in AWS, quindi Cloud Manager

gestisce il resto: Implementa i sistemi Cloud Volumes ONTAP in base alle esigenze e prende decisioni di allocazione della capacità in base all'aumento dei volumi. Questa vista offre i vantaggi dello storage di livello Enterprise nel cloud con una gestione dello storage molto ridotta.

La seguente immagine mostra come interagire con Cloud Manager nella vista volume:

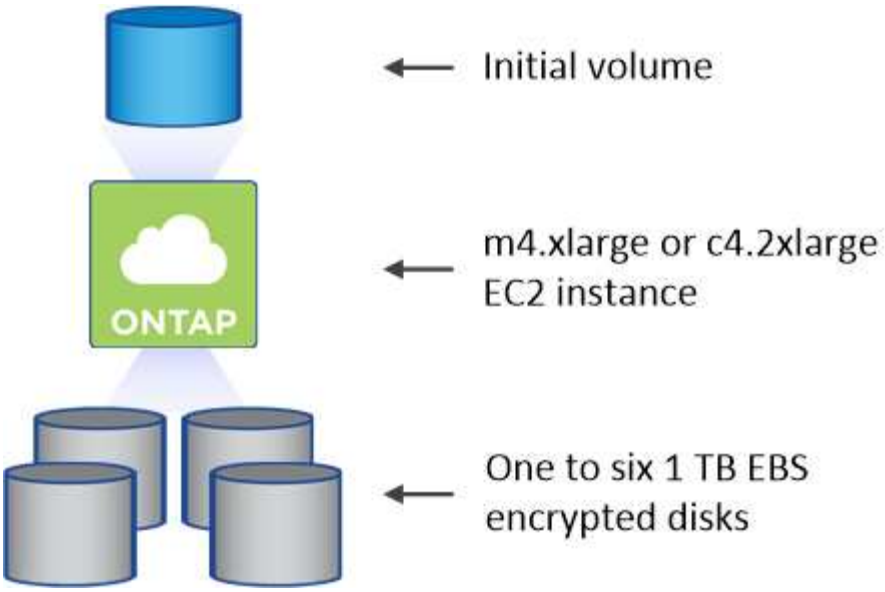


1. I volumi NFS vengono creati.
2. Cloud Manager lancia le istanze di Cloud Volumes ONTAP in AWS per nuovi volumi o crea volumi su istanze esistenti. Inoltre, acquista lo storage EBS fisico per i volumi.
3. I volumi vengono resi disponibili per gli host e le applicazioni.
4. Cloud Manager prende le decisioni di allocazione della capacità man mano che i volumi crescono.

   Ciò significa che è sufficiente interagire con i volumi (l'immagine a sinistra), mentre Cloud Manager interagisce con il sistema di storage e lo storage sottostante (l'immagine a destra).

Allocazione delle risorse cloud per il volume iniziale

Quando crei il tuo primo volume, Cloud Manager lancia un'istanza di Cloud Volumes ONTAP o una coppia di Cloud Volumes ONTAP ha in AWS e acquista lo storage Amazon EBS per il volume:



La dimensione del volume iniziale determina il tipo di istanza EC2 e il numero di dischi EBS.

> Cloud Manager avvia un'istanza Cloud Volumes ONTAP Explore o Standard, a seconda delle dimensioni iniziali del volume. Con l'aumentare dei volumi, Cloud Manager potrebbe richiedere di modificare un'istanza di AWS, il che significa che deve aggiornare la licenza dell'istanza a Standard o Premium. L'aggiornamento aumenta il limite di capacità raw di EBS, consentendo la crescita dei volumi.

> Cloud Manager non avvia le istanze di Cloud Volumes ONTAP BYOL nella vista volume. Se hai acquistato una licenza Cloud Volumes ONTAP, dovresti utilizzare Cloud Manager nella visualizzazione del sistema di storage.

Allocazione delle risorse cloud per volumi aggiuntivi

Quando si creano volumi aggiuntivi, Cloud Manager crea i volumi sulle istanze di Cloud Volumes ONTAP esistenti o sulle nuove istanze di Cloud Volumes ONTAP. Cloud Manager può creare un volume su un'istanza esistente se la posizione AWS e il tipo di disco dell'istanza corrispondono al volume richiesto e se lo spazio è sufficiente.

Funzionalità di efficienza dello storage NetApp e costi dello storage

Cloud Manager abilita automaticamente le funzionalità di efficienza dello storage NetApp su tutti i volumi. Queste efficienze possono ridurre la quantità totale di storage di cui hai bisogno. È possibile che si riscontri una differenza tra la capacità allocata e la capacità AWS acquistata, con conseguente risparmio sui costi di storage.

Decisioni di allocazione della capacità gestite automaticamente da Cloud Manager

- Cloud Manager acquista dischi EBS aggiuntivi quando vengono superate le soglie di capacità. Questo accade con la crescita dei volumi.
- Cloud Manager elimina i set inutilizzati di dischi EBS se i dischi non contengono volumi per 12 ore.
- Cloud Manager sposta i volumi tra set di dischi per evitare problemi di capacità.

  In alcuni casi, ciò richiede l'acquisto di dischi EBS aggiuntivi. Consente inoltre di liberare spazio sul set di dischi originale per i volumi nuovi ed esistenti.

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.

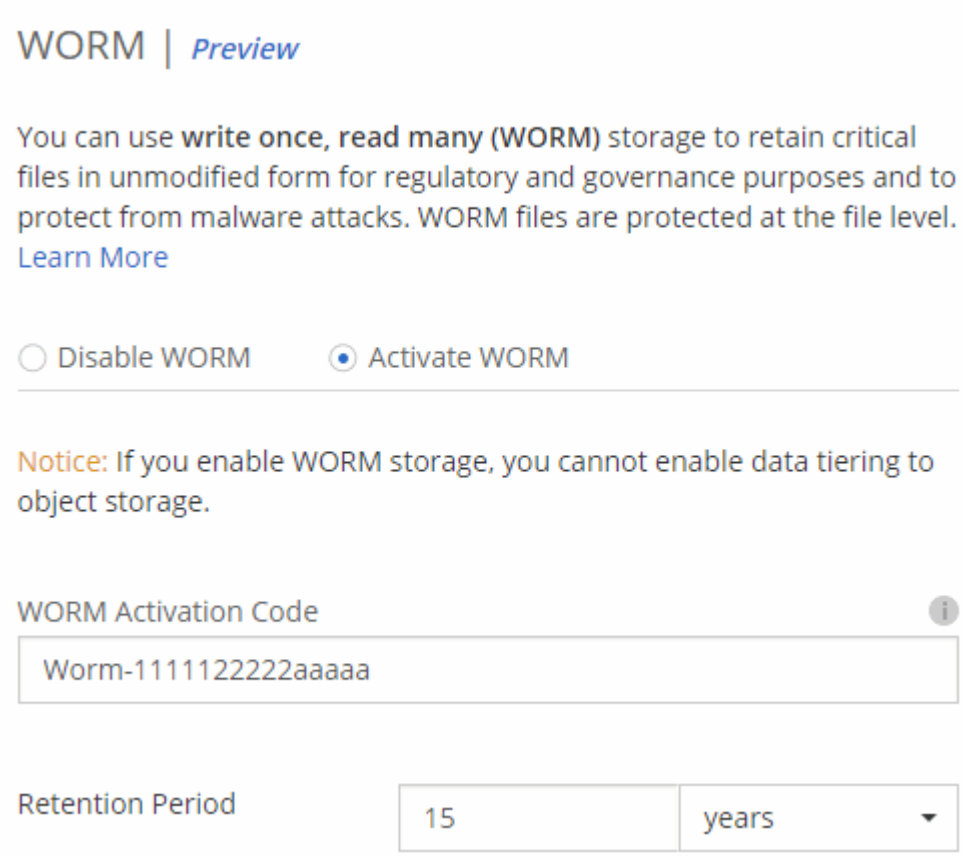
Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari.

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.

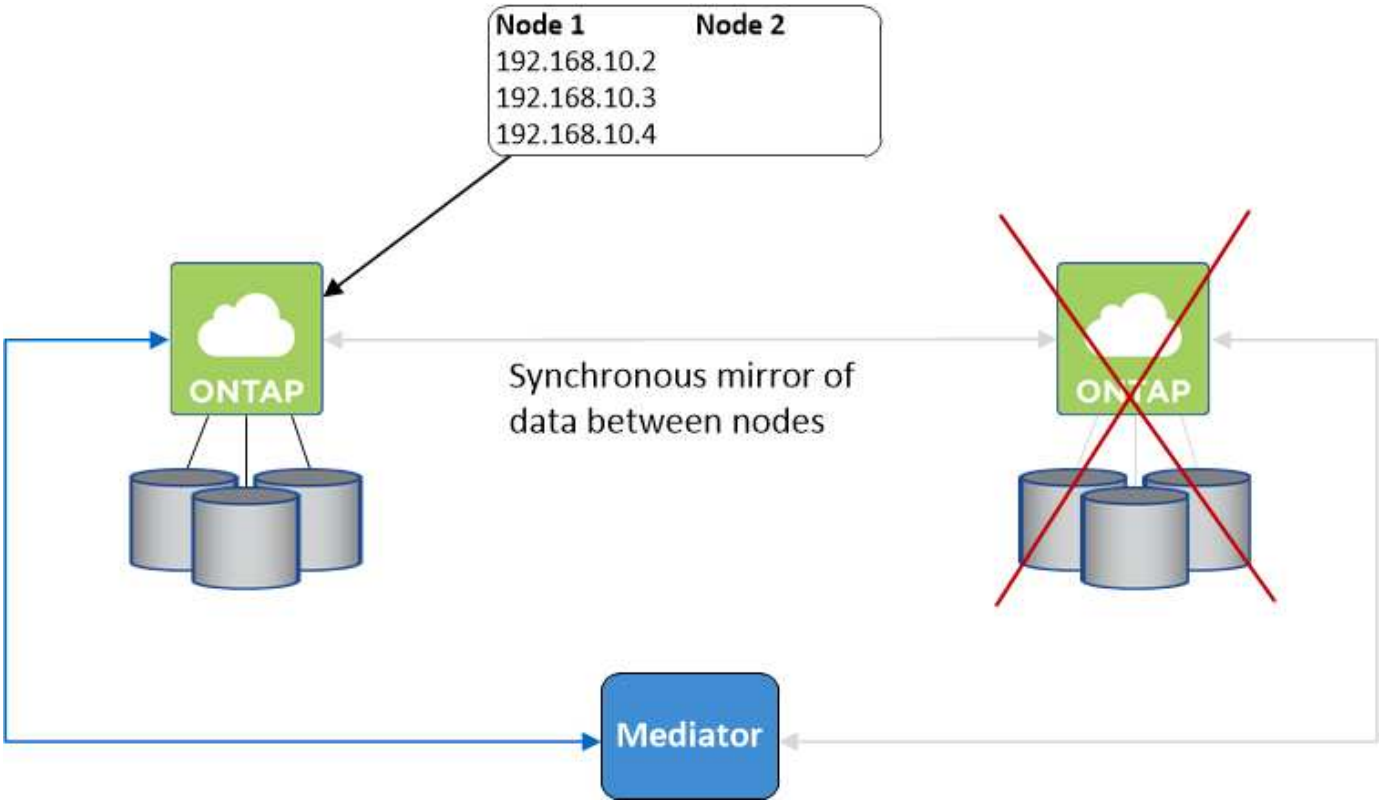
Takeover e giveback dello storage per iSCSI

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

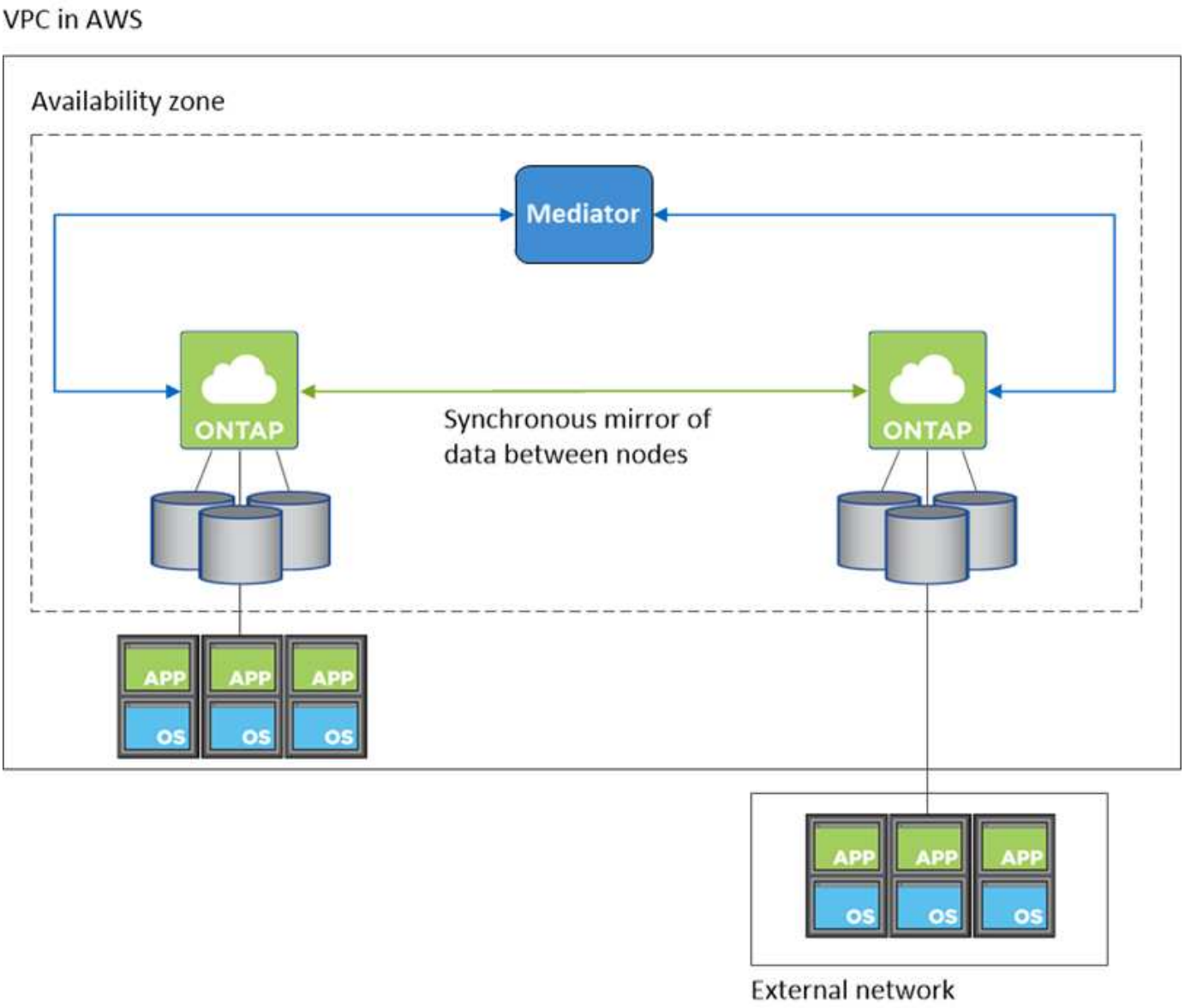
L'implementazione di una configurazione ha in una singola zona di disponibilità (AZ) può garantire un'elevata disponibilità dei dati in caso di guasto di un'istanza che esegue un nodo Cloud Volumes ONTAP. Tutti i dati sono accessibili in modo nativo dall'esterno del VPC.

> 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.

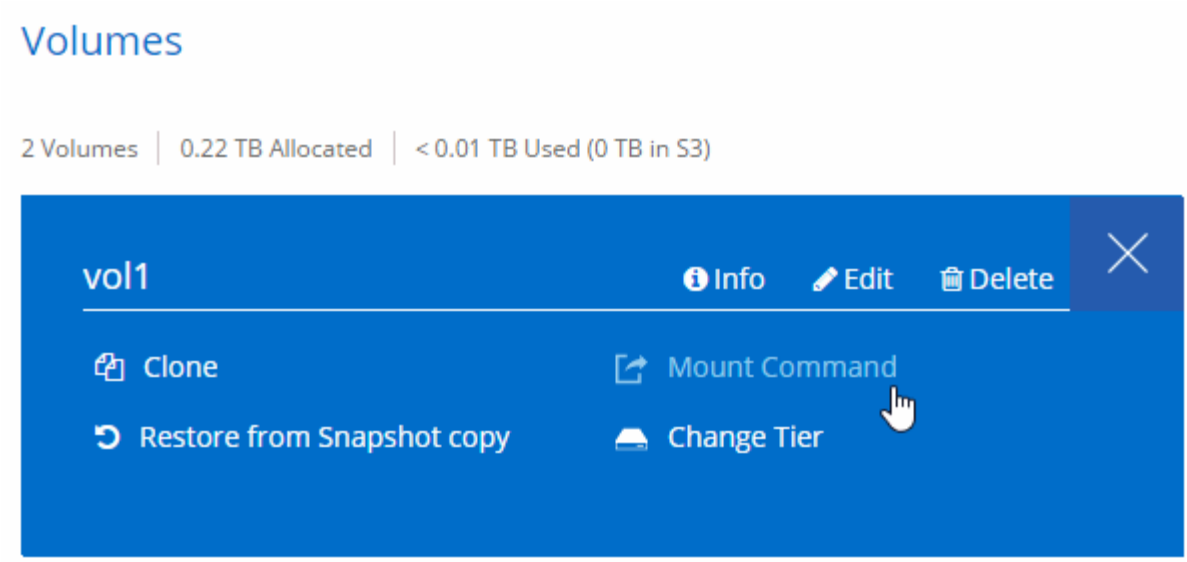
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, vedere "Performance".

Accesso client allo storage

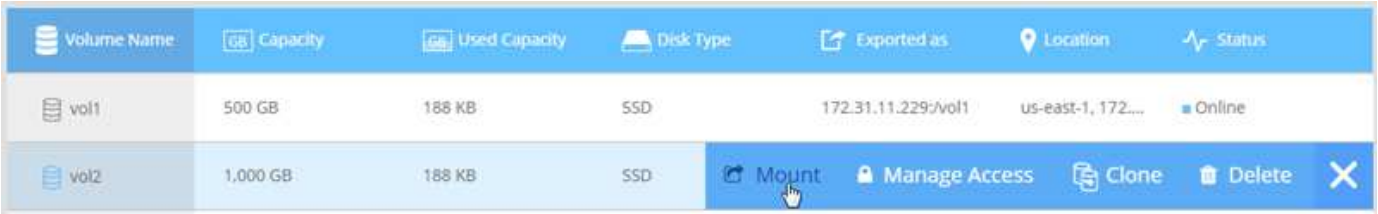
I client devono accedere ai volumi NFS e CIFS utilizzando l'indirizzo IP dei dati del nodo su cui risiede il volume. Se i client NAS accedono a un volume utilizzando l'indirizzo IP del nodo partner, il traffico passa tra entrambi i nodi, riducendo le performance.

> 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. La seguente immagine mostra la vista del sistema di storage:



La seguente immagine mostra la vista volume:

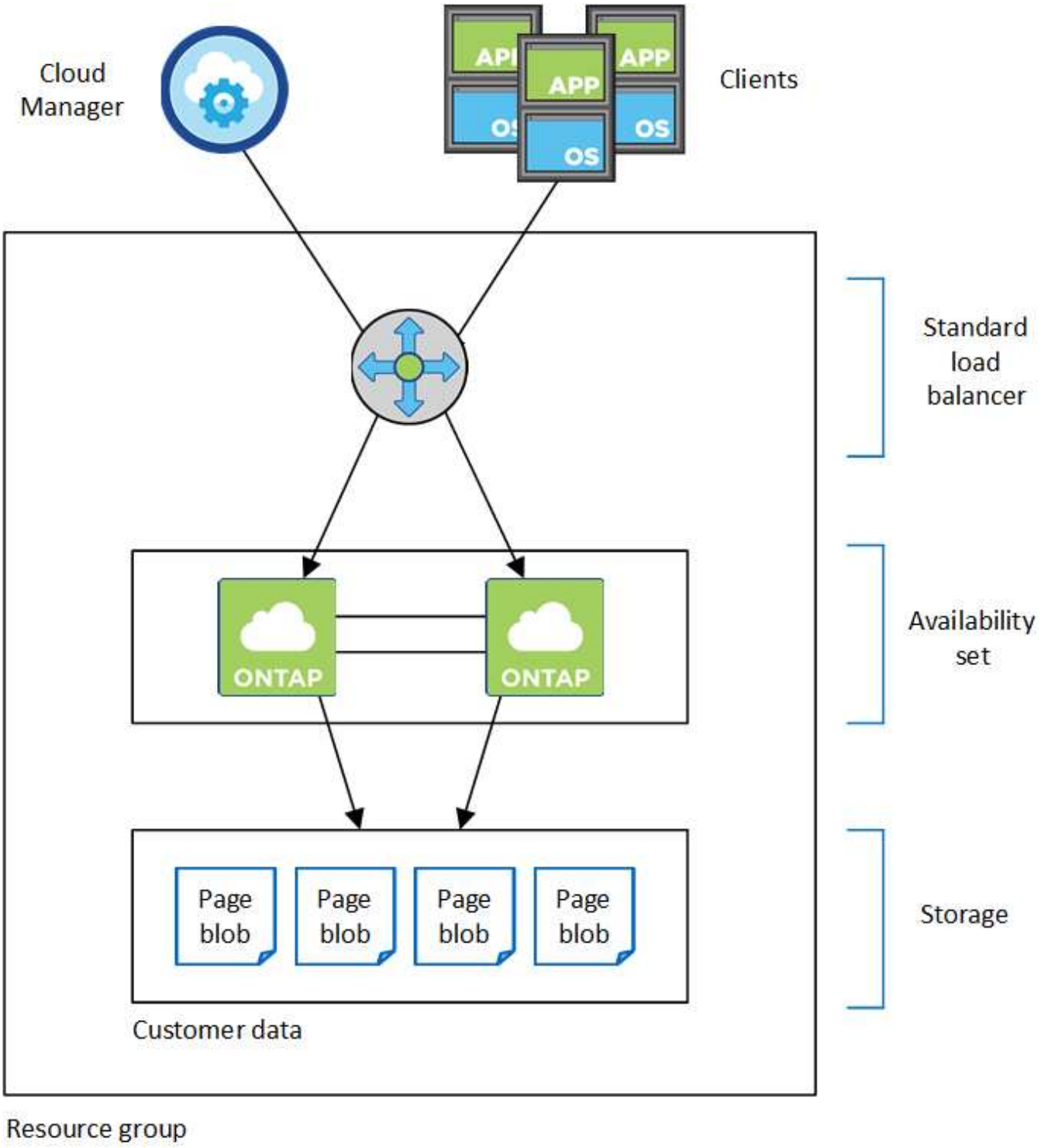


Coppie ad alta disponibilità in Azure

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.

Storage

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

- I dati di avvio di un nodo risiedono su un disco gestito SSD Premium.
- I dati root di un nodo risiedono in un blob di pagina Premium 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.
- Il tiering dei dati 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

È possibile utilizzare NetApp Volume Encryption con crittografia AWS e Azure nativa, che crittografano 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).

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.

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".

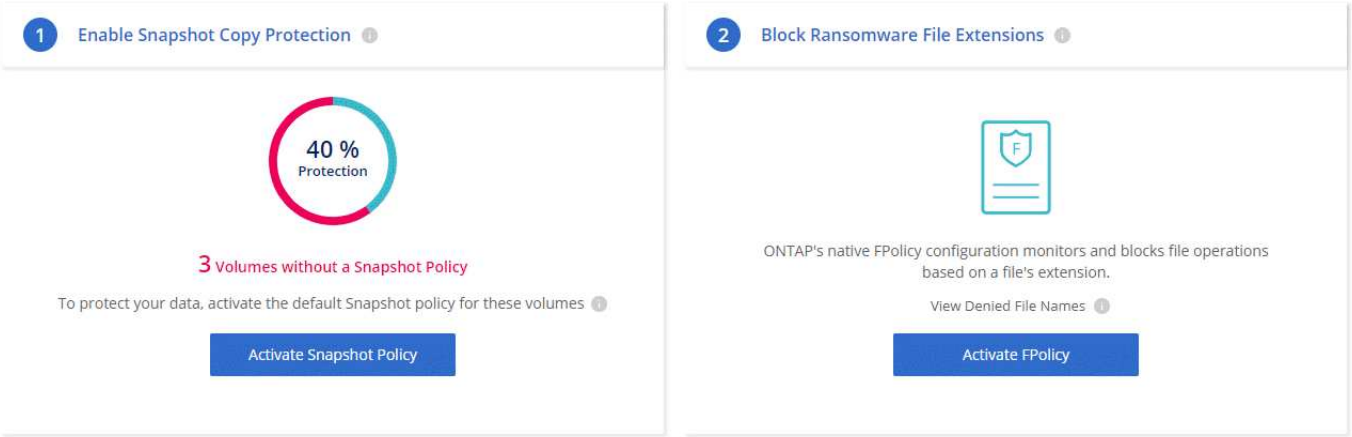
Protezione ransomware

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".

Per iniziare

Panoramica dell'implementazione

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

Installazione di Cloud Manager

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

- Amazon Web Services (AWS)
- Microsoft Azure
- Cloud IBM
- Nella tua rete

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

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

Configurazione di Cloud Manager

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

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

Implementazione di Cloud Volumes ONTAP

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

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

- "Configurazioni supportate per Cloud Volumes ONTAP 9.5"
- "Pianificazione della configurazione"
- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"

Introduzione a Cloud Volumes ONTAP in AWS

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

1 Configurare la rete

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

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

2. Impostare un endpoint VPC sul servizio S3.

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

2 Iscriviti a Cloud Volumes ONTAP dal marketplace AWS

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

3 Fornire le autorizzazioni AWS richieste

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

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

4 Lanciate Cloud Manager da NetApp Cloud Central

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

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

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

Link correlati

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

Introduzione a Cloud Volumes ONTAP in Azure

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

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 Cloud Provider a Cloud Manager"
- "Cosa fa Cloud Manager con le autorizzazioni Azure"
- "Lancio di Cloud Volumes ONTAP in Azure"
- "Lancio di Cloud Manager da Azure Marketplace"

Configurazione di Cloud Manager

Aggiunta di account cloud provider a Cloud Manager

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

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

Impostazione e aggiunta di account AWS a Cloud Manager

Se si desidera implementare Cloud Volumes ONTAP in diversi account AWS, è necessario fornire le autorizzazioni necessarie a tali account e aggiungere i dettagli a Cloud Manager. La modalità di fornitura delle autorizzazioni dipende dal fatto che si desideri fornire a Cloud Manager le chiavi AWS o l'ARN di un ruolo in un account attendibile.

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

Concessione delle autorizzazioni quando si forniscono le chiavi AWS

Se si desidera fornire a Cloud Manager le chiavi AWS per un utente IAM, è necessario concedere le

autorizzazioni necessarie a tale utente. La policy IAM di Cloud Manager definisce le azioni e le risorse AWS che Cloud Manager può utilizzare.

Fasi

1. Scarica la policy IAM di Cloud Manager da "Pagina delle policy di Cloud Manager".
2. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.

   "Documentazione AWS: Creazione di policy IAM"

3. Allegare il criterio a un ruolo IAM o a un utente IAM.
   - "Documentazione AWS: Creazione dei ruoli IAM"
   - "Documentazione di AWS: Aggiunta e rimozione dei criteri IAM"

Risultato

L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Concessione delle autorizzazioni assumendo ruoli IAM in altri account

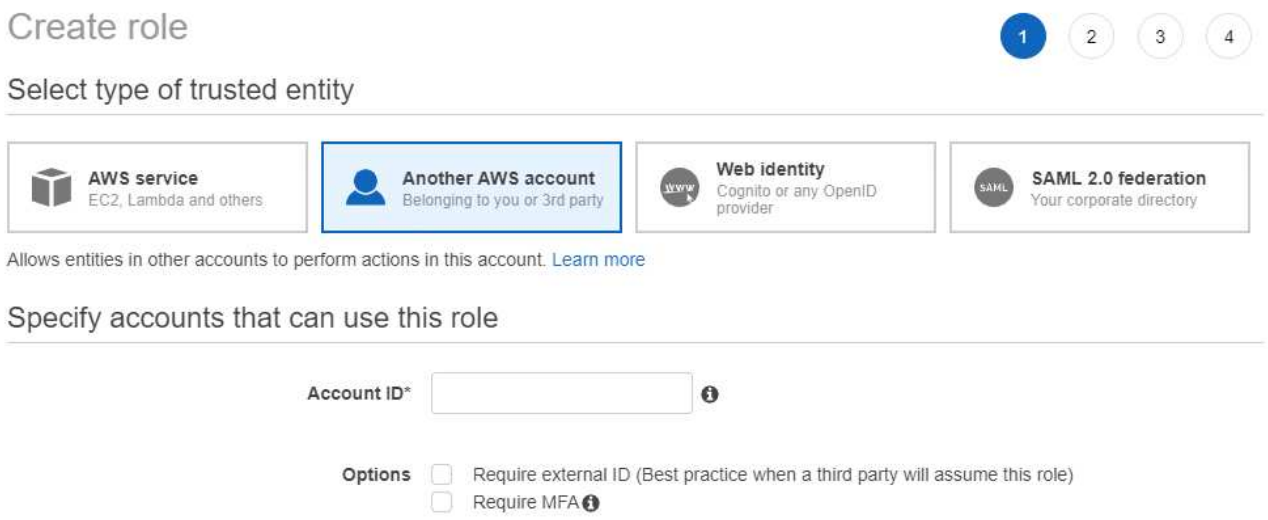
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Cloud Manager e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

Fasi

1. Accedere all'account di destinazione in cui si desidera implementare Cloud Volumes ONTAP e creare un ruolo IAM selezionando **un altro account AWS**.

   Assicurarsi di effettuare le seguenti operazioni:

   - Inserire l'ID dell'account in cui risiede l'istanza di Cloud Manager.
   - Allegare la policy IAM di Cloud Manager, disponibile in "Pagina delle policy di Cloud Manager".



2. Accedere all'account di origine in cui risiede l'istanza di Cloud Manager e selezionare il ruolo IAM associato all'istanza.

a. Fare clic su **Trust Relationship > Edit trust relationship**.

b. Aggiungi l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

Esempio

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Risultato

L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Aggiunta di account AWS a Cloud Manager

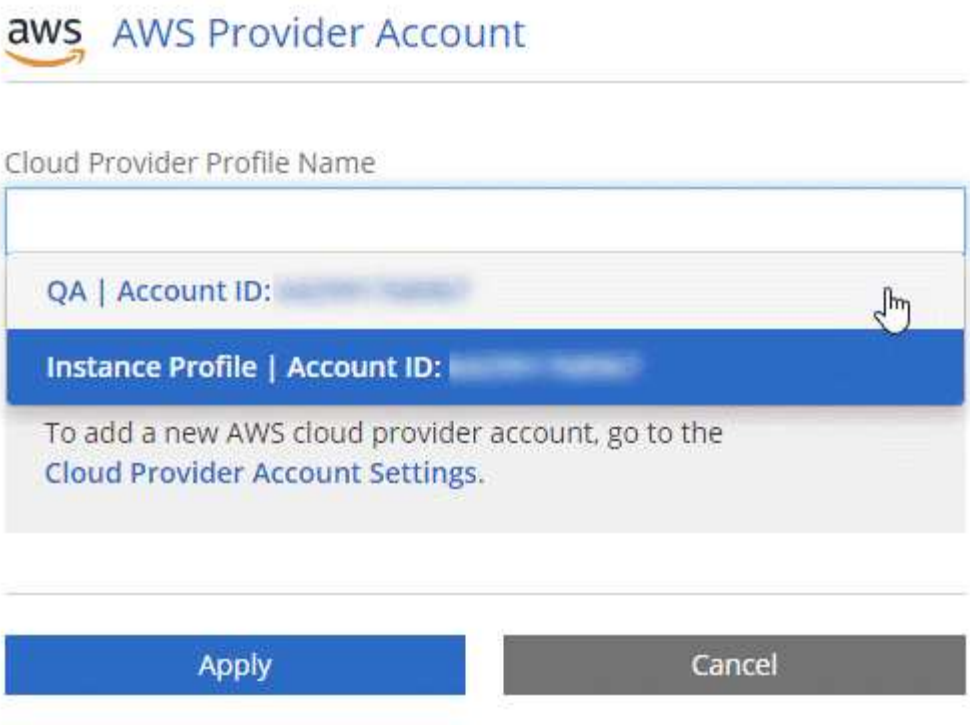
Dopo aver fornito un account AWS con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Impostazioni account**.
2. Fare clic su **Add New account** (Aggiungi nuovo account) e selezionare **AWS**.
3. Scegliere se si desidera fornire le chiavi AWS o l'ARN di un ruolo IAM attendibile.
4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

Risultato

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



Configurazione e aggiunta di account Azure a Cloud Manager

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

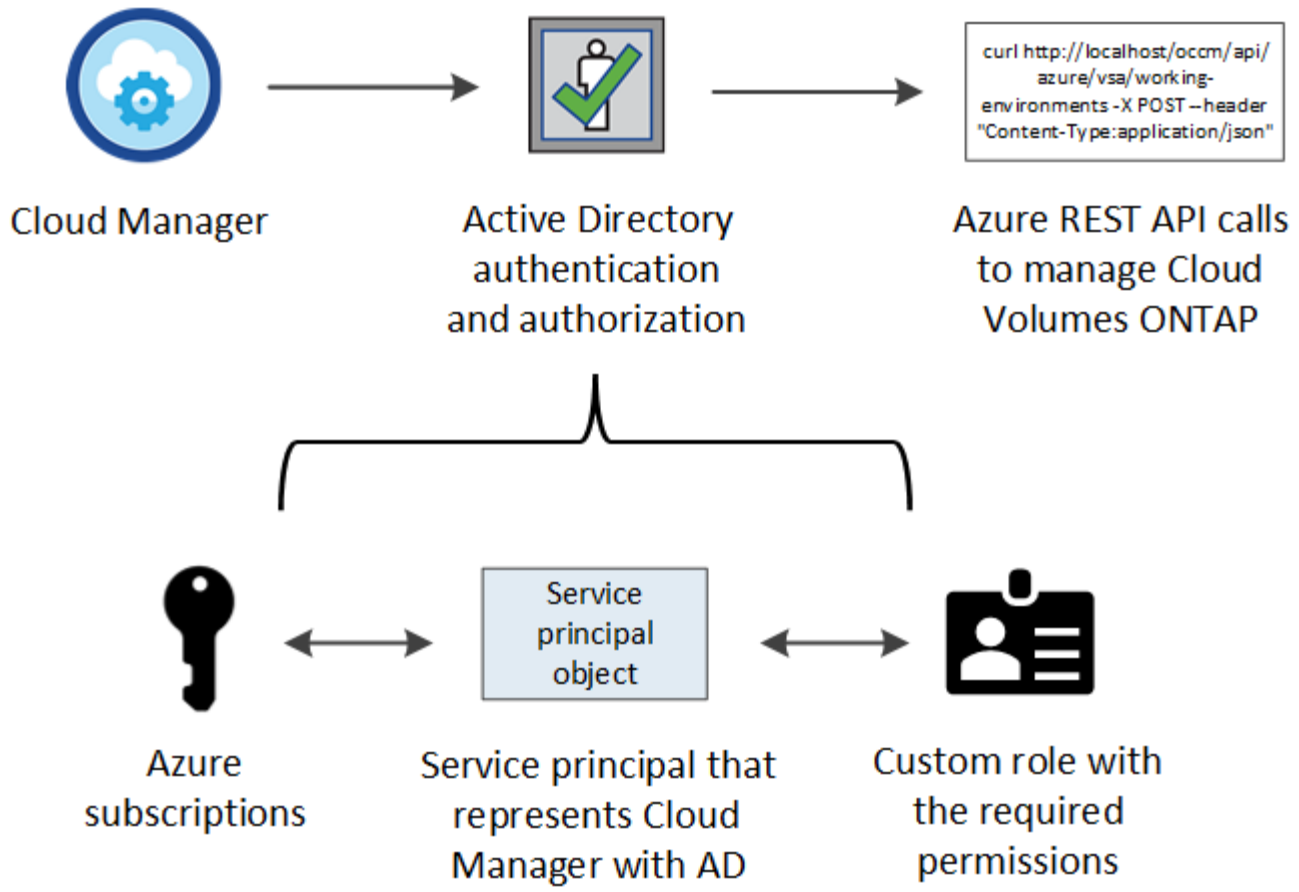
- Concessione delle autorizzazioni di Azure mediante un'entità del servizio
- Aggiunta di account Azure a Cloud Manager

Concessione delle autorizzazioni di Azure mediante un'entità del servizio

Cloud Manager ha bisogno delle autorizzazioni per eseguire azioni in Azure. È possibile concedere le autorizzazioni richieste a un account Azure creando e impostando un'entità di servizio in Azure Active Directory e ottenendo le credenziali Azure di cui Cloud Manager ha bisogno.

A proposito di questa attività

La seguente immagine mostra come Cloud Manager ottiene le autorizzazioni per eseguire operazioni in Azure. Un oggetto principale del servizio, legato a una o più sottoscrizioni Azure, rappresenta Cloud Manager in Azure Active Directory e viene assegnato a un ruolo personalizzato che consente le autorizzazioni richieste.



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

Fasi

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

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

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

Fasi

1. Scaricare il "Policy di Cloud Manager Azure".
2. Modificare il file JSON aggiungendo gli ID di abbonamento Azure all'ambito assegnabile.

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

   Esempio

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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

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

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

Risultato

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

Creazione di un'entità del servizio Active Directory

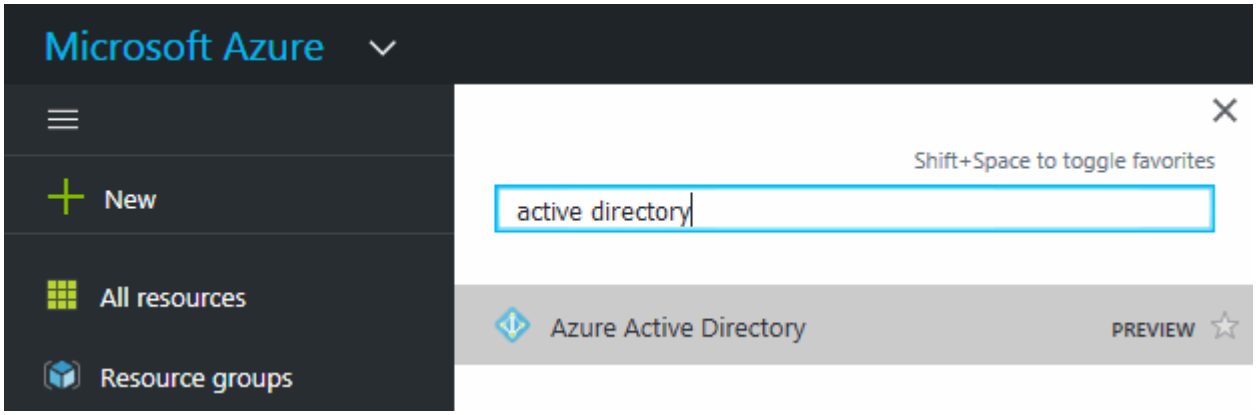
È necessario creare un'entità del servizio Active Directory in modo che Cloud Manager possa autenticarsi con Azure Active Directory.

Prima di iniziare

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

Fasi

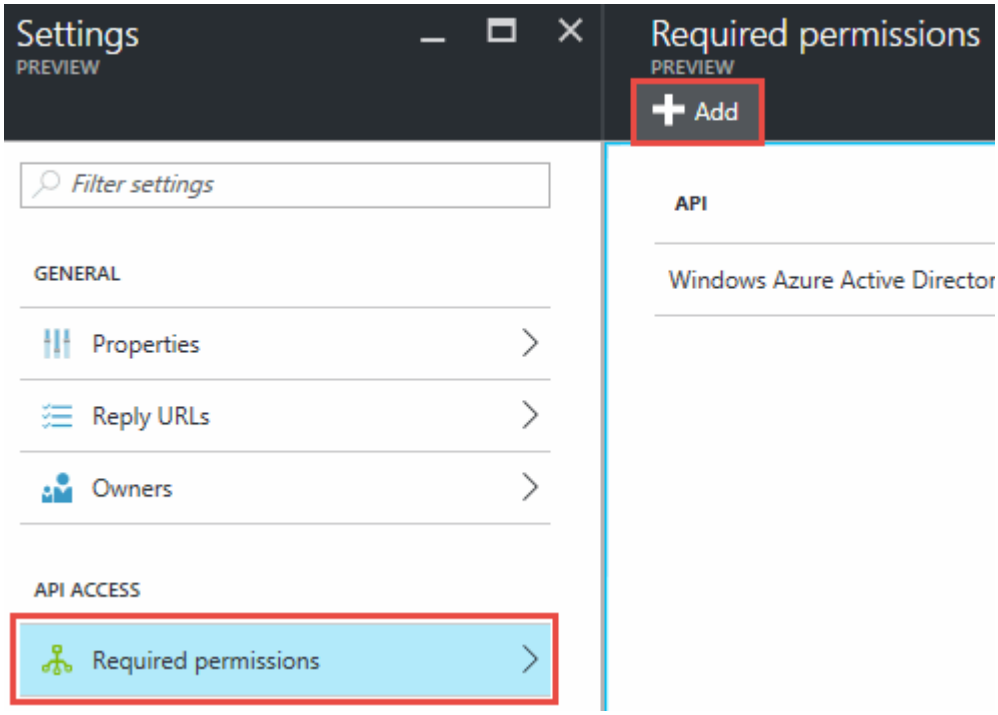
1. Dal portale Azure, aprire il servizio **Azure Active Directory**.



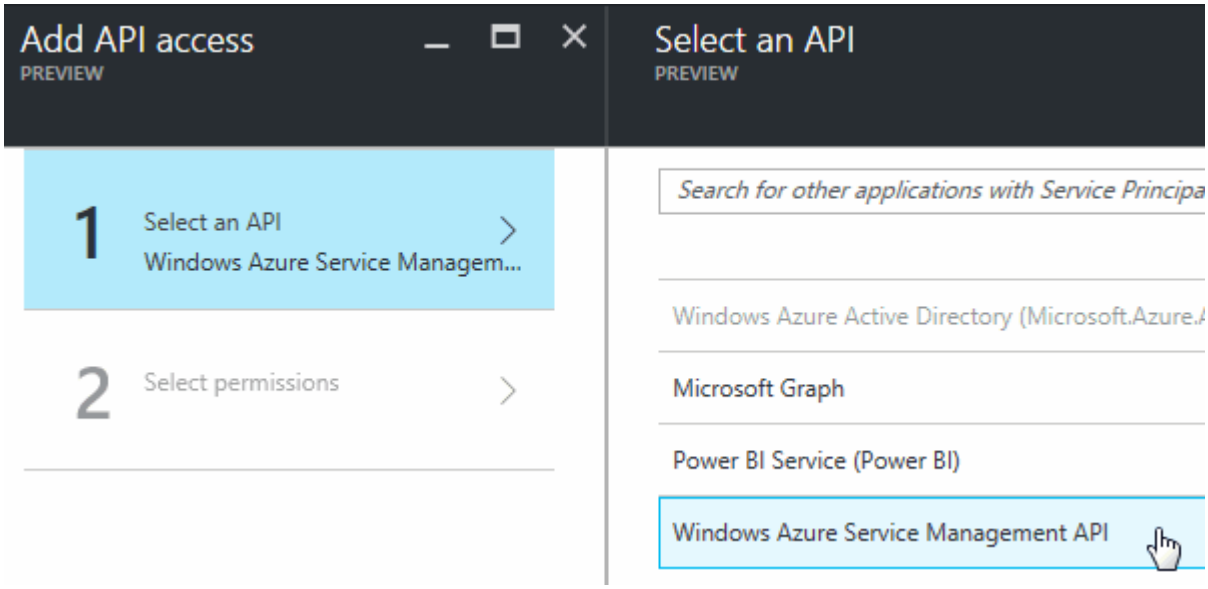
2. Nel menu, fare clic su **App Registrations (Legacy)**.
3. Creare l'entità del servizio:
   a. Fare clic su **Nuova registrazione applicazione**.
   b. Immettere un nome per l'applicazione, mantenere selezionata l'opzione **Web app/API**, quindi immettere un URL, ad esempio http://url
   c. Fare clic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

a. Selezionare l'applicazione creata.

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



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



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

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

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

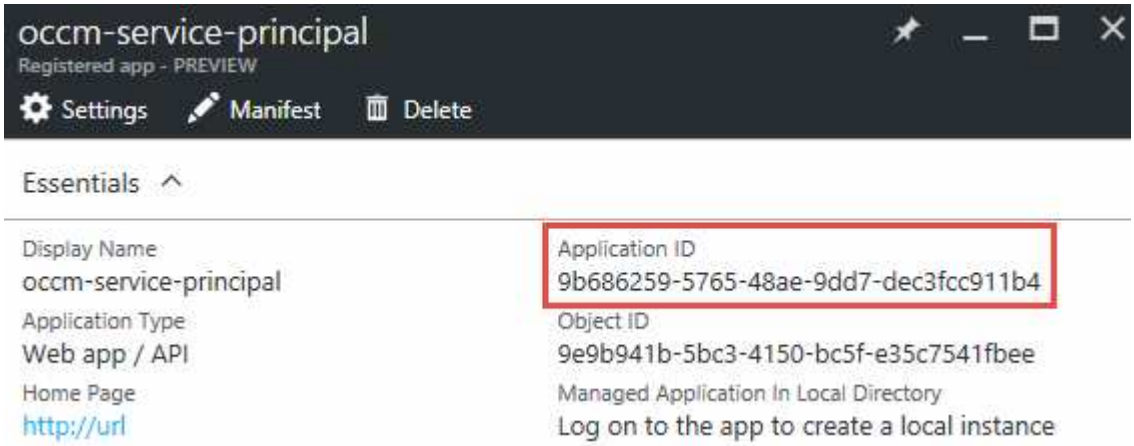
b. Inserire una descrizione, selezionare una durata, quindi fare clic su **Salva**.

c. Copiare il valore della chiave.

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

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

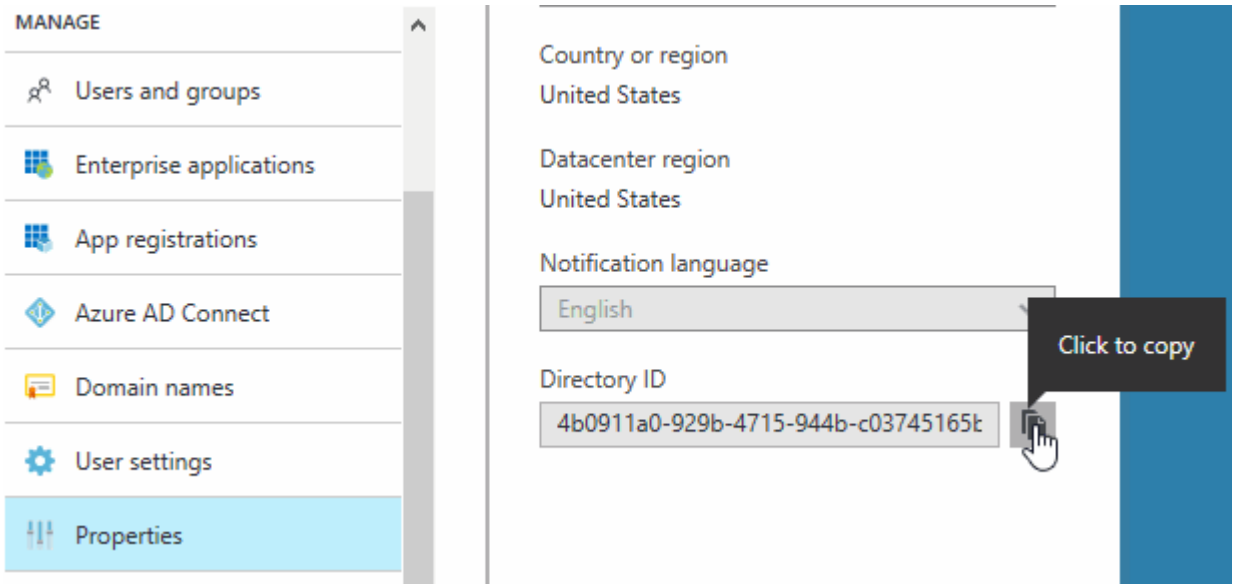
Analogamente al valore della chiave, è necessario inserire l'ID dell'applicazione in Cloud Manager quando si aggiunge un account del provider cloud a Cloud Manager.



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

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

b. Copiare l'ID della directory.



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

Risultato

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

Assegnazione del ruolo Cloud Manager Operator all'entità del servizio

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

A proposito di questa attività

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

Fasi

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

Risultato

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

Aggiunta di account Azure a Cloud Manager

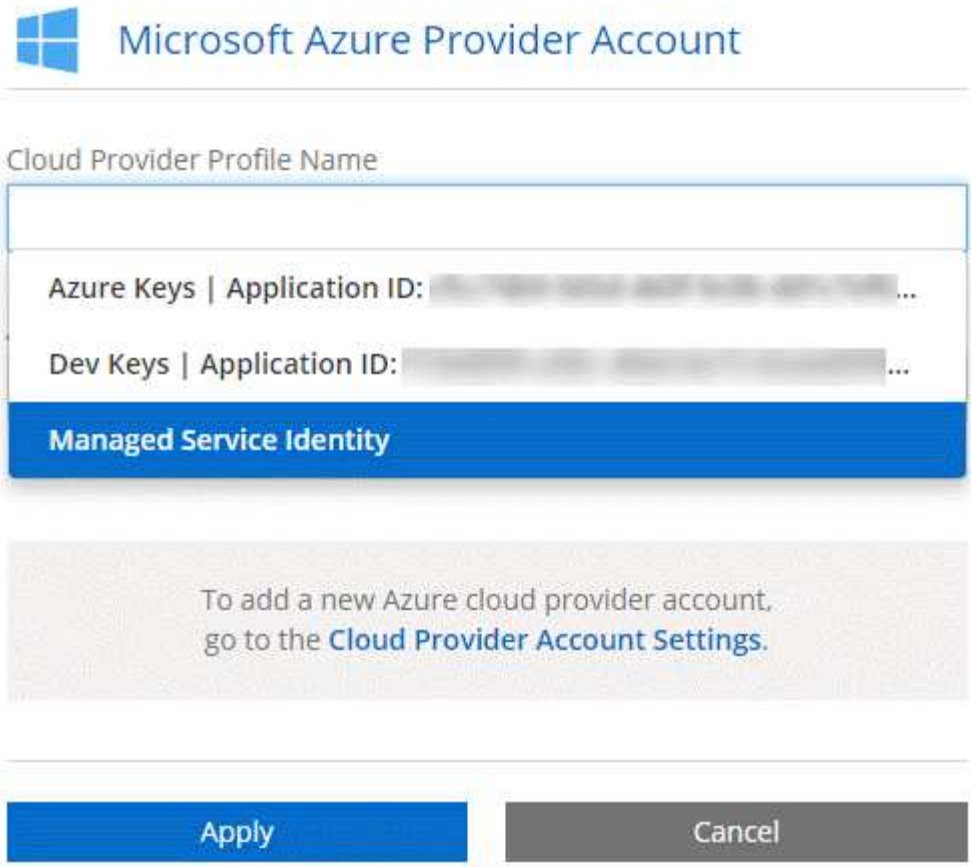
Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungerlo a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Impostazioni account**.
2. Fare clic su **Aggiungi nuovo account** e selezionare **Microsoft Azure**.
3. Immettere le informazioni sull'entità del servizio Azure Active Directory che concede le autorizzazioni richieste.
4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

Risultato

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



Associazione di sottoscrizioni Azure aggiuntive a un'identità gestita

Cloud Manager consente di scegliere l'account e l'abbonamento Azure in cui si desidera implementare Cloud Volumes ONTAP. Non è possibile selezionare un'altra sottoscrizione Azure per il profilo di identità gestita, a meno che non venga associato a. "identità gestita" con questi abbonamenti.

A proposito di questa attività

Un'identità gestita è l'iniziale "account cloud provider" Quando si implementa Cloud Manager da NetApp Cloud Central. Quando hai implementato Cloud Manager, Cloud Central ha creato il ruolo di operatore di Cloud Manager di OnCommand e lo ha assegnato alla macchina virtuale di Cloud Manager.

Fasi

1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare i sistemi Cloud Volumes ONTAP.
3. Fare clic su **controllo di accesso (IAM)**.
   a. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
      - Selezionare il ruolo **operatore cloud OnCommand**.

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

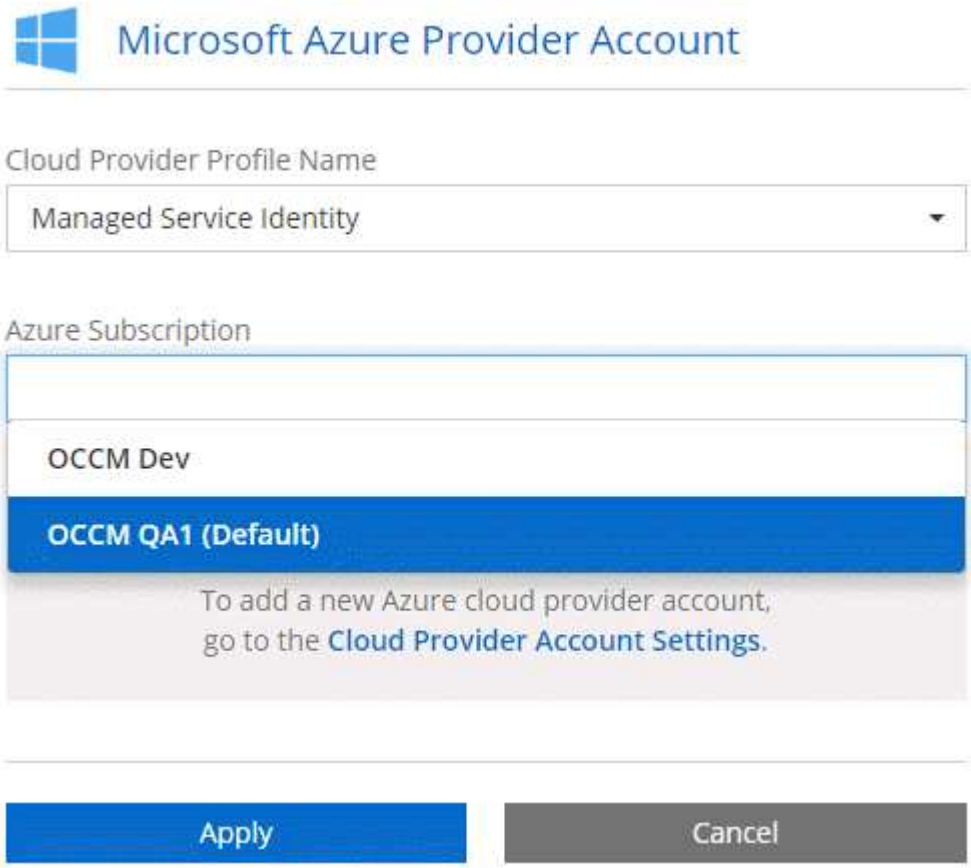
      - Assegnare l'accesso a una **macchina virtuale**.

- Selezionare l'abbonamento in cui è stata creata la macchina virtuale Cloud Manager.
- Selezionare la macchina virtuale Cloud Manager.
- Fare clic su **Save** (Salva).

4. Ripetere questa procedura per gli abbonamenti aggiuntivi.

Risultato

Quando crei un nuovo ambiente di lavoro, dovresti ora avere la possibilità di scegliere tra più sottoscrizioni Azure per il profilo di identità gestito.



Aggiunta di account NetApp Support Site a Cloud Manager

Per implementare un sistema BYOL, è necessario aggiungere il tuo account NetApp Support Site a Cloud Manager. È inoltre necessario registrare i sistemi pay-as-you-go e aggiornare il software ONTAP.

Guarda il video seguente per scoprire come aggiungere gli account NetApp Support Site a Cloud Manager. In alternativa, scorrere verso il basso per leggere i passaggi.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Fasi

1. Se non disponi ancora di un account NetApp Support Site, "registratevi per uno".
2. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività,

quindi selezionare **Impostazioni account**.

3. Fare clic su **Add New account** (Aggiungi nuovo account) e selezionare **NetApp Support Site** (Sito di supporto NetApp).
4. Specificare un nome per l'account, quindi immettere il nome utente e la password.
    - L'account deve essere un account a livello di cliente (non un account guest o temporaneo).
    - Se si prevede di implementare sistemi BYOL:
        - L'account deve essere autorizzato ad accedere ai numeri di serie dei sistemi BYOL.
        - Se hai acquistato un abbonamento BYOL sicuro, è necessario un account NSS sicuro.
5. Fare clic su **Crea account.**

Quali sono le prossime novità?

Gli utenti possono ora selezionare l'account durante la creazione di nuovi sistemi Cloud Volumes ONTAP e la registrazione di sistemi esistenti.

- "Avvio di Cloud Volumes ONTAP in AWS"
- "Lancio di Cloud Volumes ONTAP in Azure"
- "Registrazione di sistemi pay-as-you-go"
- "Scopri come Cloud Manager gestisce i file di licenza"

Installazione di un certificato HTTPS per un accesso sicuro

Per impostazione predefinita, Cloud Manager utilizza un certificato autofirmato per l'accesso HTTPS alla console Web. È possibile installare un certificato firmato da un'autorità di certificazione (CA), che offre una protezione migliore rispetto a un certificato autofirmato.

Fasi

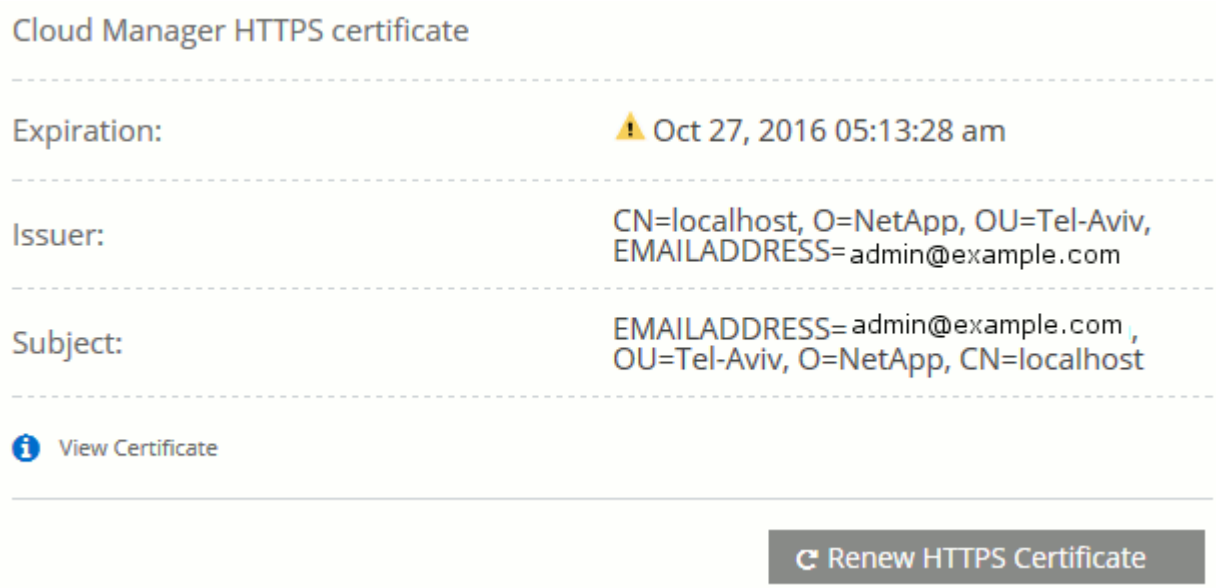
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **HTTPS Setup**.
2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio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

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

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

Risultato

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



Configurazione di utenti e tenant

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

Aggiunta di utenti a Cloud Manager

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

Fasi

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

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

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

Quali sono le prossime novità?

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

Creazione di tenant

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

Fasi

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

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

Quali sono le prossime novità?

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

Configurazione di AWS KMS

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

Fasi

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

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

   "Documentazione AWS: Customer Master Keys (CMK)"

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

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

"Documentazione AWS: Modifica delle chiavi"

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

   a. Accedere alla console KMS dall'account in cui risiede il CMK.

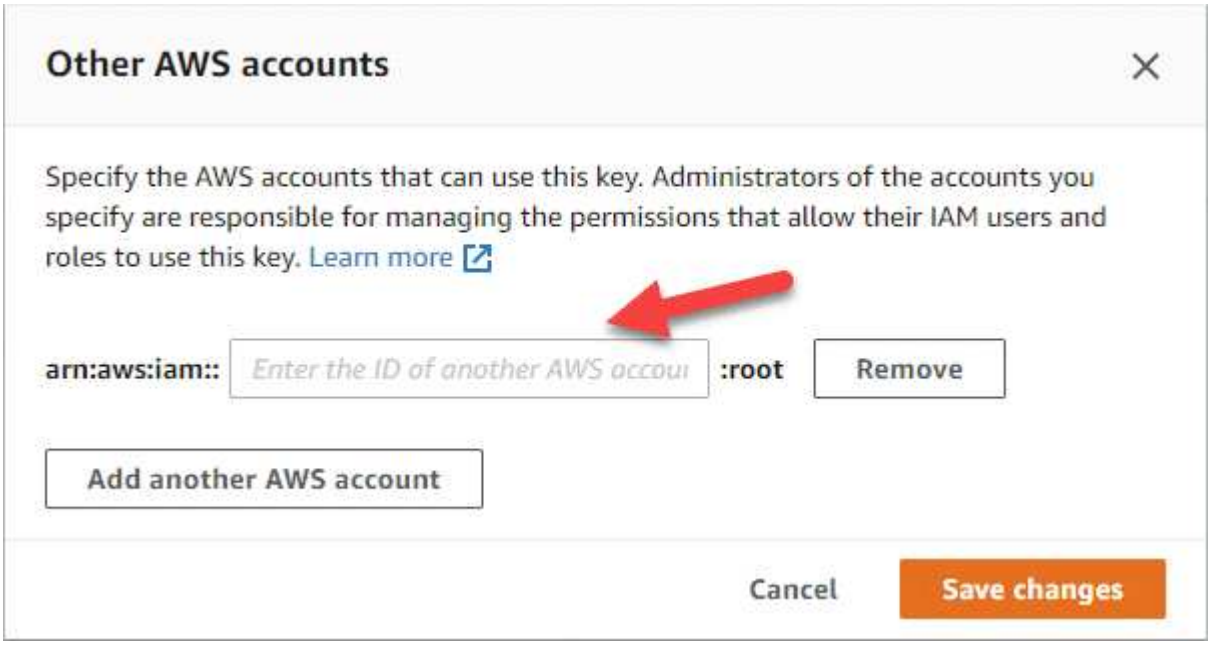
   b. Selezionare la chiave.

   c. Nel riquadro **General Configuration** (Configurazione generale), copiare l'ARN della chiave.

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

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

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



   e. Passare ora all'account AWS che fornisce le autorizzazioni a Cloud Manager e aprire la console IAM.

   f. Creare un criterio IAM che includa le autorizzazioni elencate di seguito.

   g. Allegare il criterio al ruolo IAM o all'utente IAM che fornisce le autorizzazioni a Cloud Manager.

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

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

+
Per ulteriori informazioni su questo processo, vedere "Documentazione AWS: Consentire agli account AWS esterni di accedere a un CMK".

Requisiti di rete

Requisiti di rete per Cloud Manager

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

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

Connessione alle reti di destinazione

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

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

Accesso a Internet in uscita

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

Le sezioni seguenti identificano gli endpoint specifici.

Accesso a Internet in uscita per gestire Cloud Volumes ONTAP in AWS

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

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

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

Accesso a Internet in uscita per gestire Cloud Volumes ONTAP in Azure

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

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

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

Accesso a Internet in uscita dal browser Web

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

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

Accesso a Internet in uscita per installare Cloud Manager su un host Linux

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

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

Porte e gruppi di sicurezza

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

Requisiti di rete per Cloud Volumes ONTAP in AWS

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

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

Requisiti generali di rete AWS per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

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

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

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

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

Accesso a Internet in uscita per il mediatore ha

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

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

Gruppi di sicurezza

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

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

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

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

In caso di problemi, vedere "AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"

Connessioni a sistemi ONTAP in altre reti

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

DNS e Active Directory per CIFS

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

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

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

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

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

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

Zone di disponibilità

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

Indirizzi IP mobili per dati NAS e gestione cluster/SVM

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

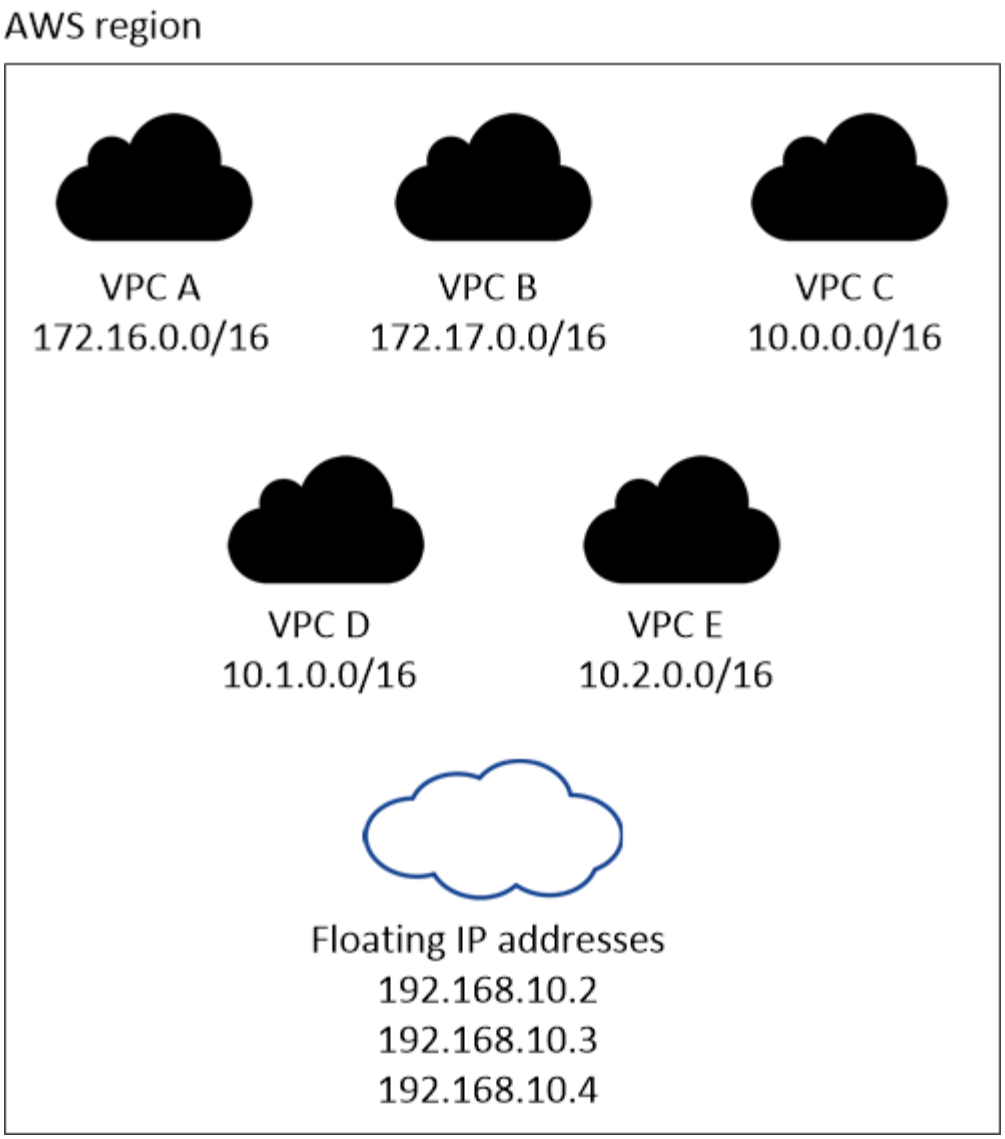
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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

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

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

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



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

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

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

Tabelle di percorso

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

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

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

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

Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a. "Documentazione AWS: Tabelle di percorso".

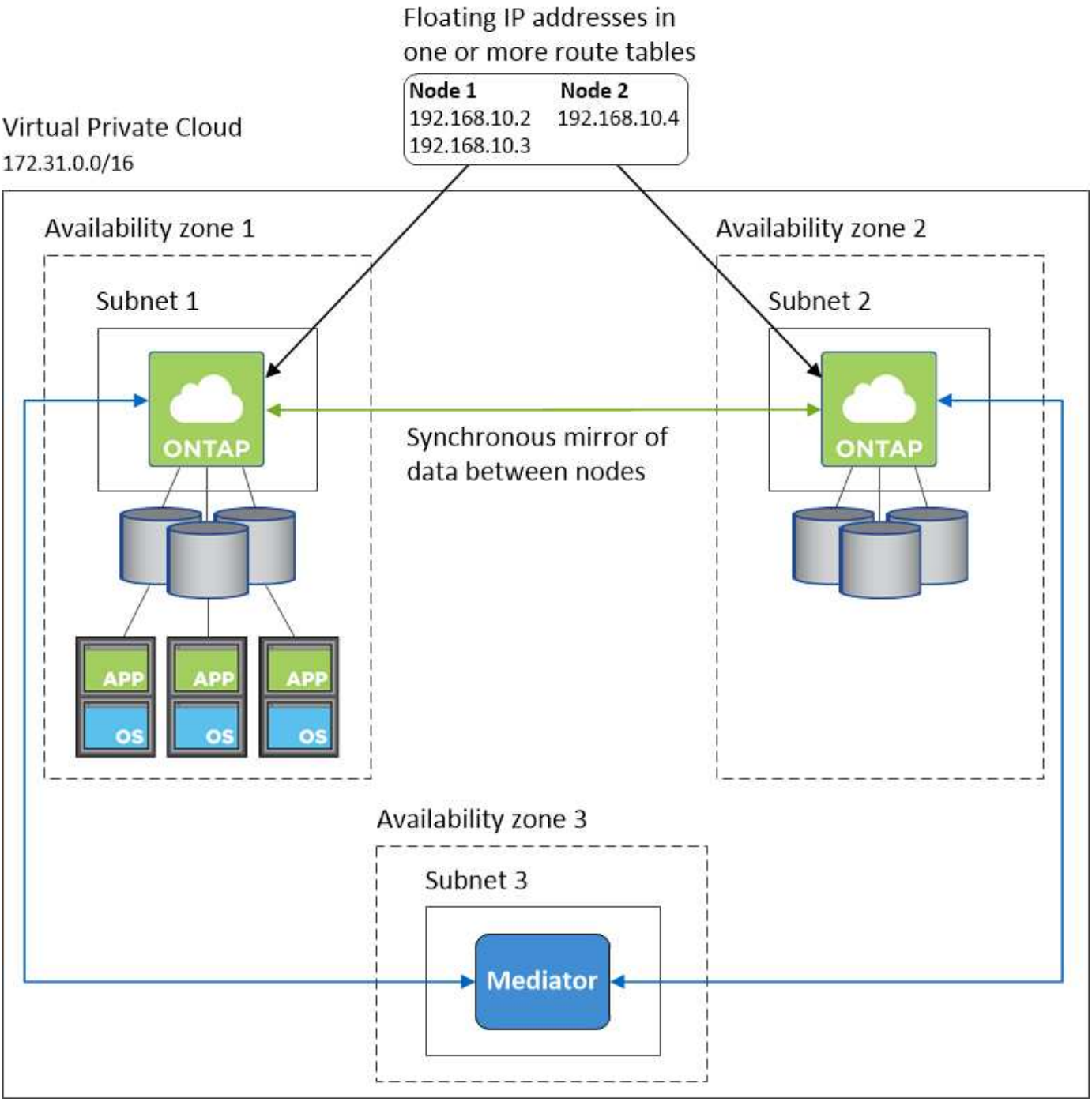
Connessione ai tool di gestione NetApp

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

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

Configurazione di esempio

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



Configurazioni VPC di esempio

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

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

Un VPC con subnet pubbliche e private e un dispositivo NAT

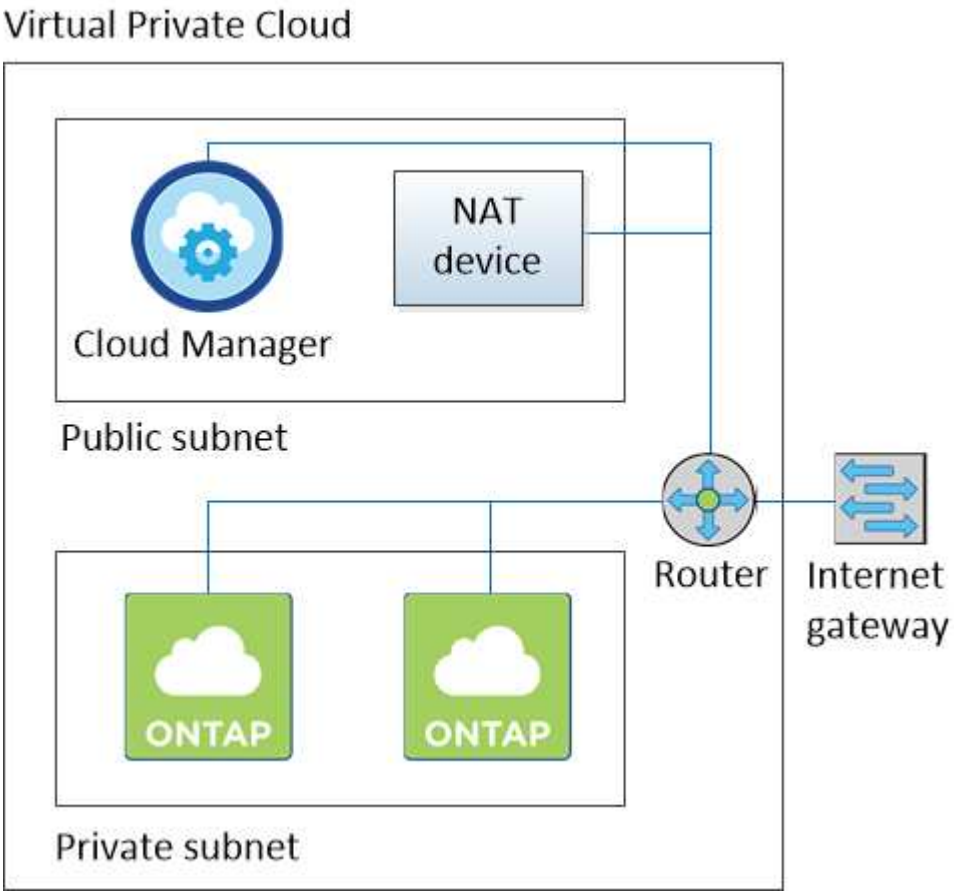
Questa configurazione VPC include subnet pubbliche e private, un gateway Internet che connette il VPC a Internet e un gateway NAT o istanza NAT nella subnet pubblica che abilita il traffico Internet in uscita dalla

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

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

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

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



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

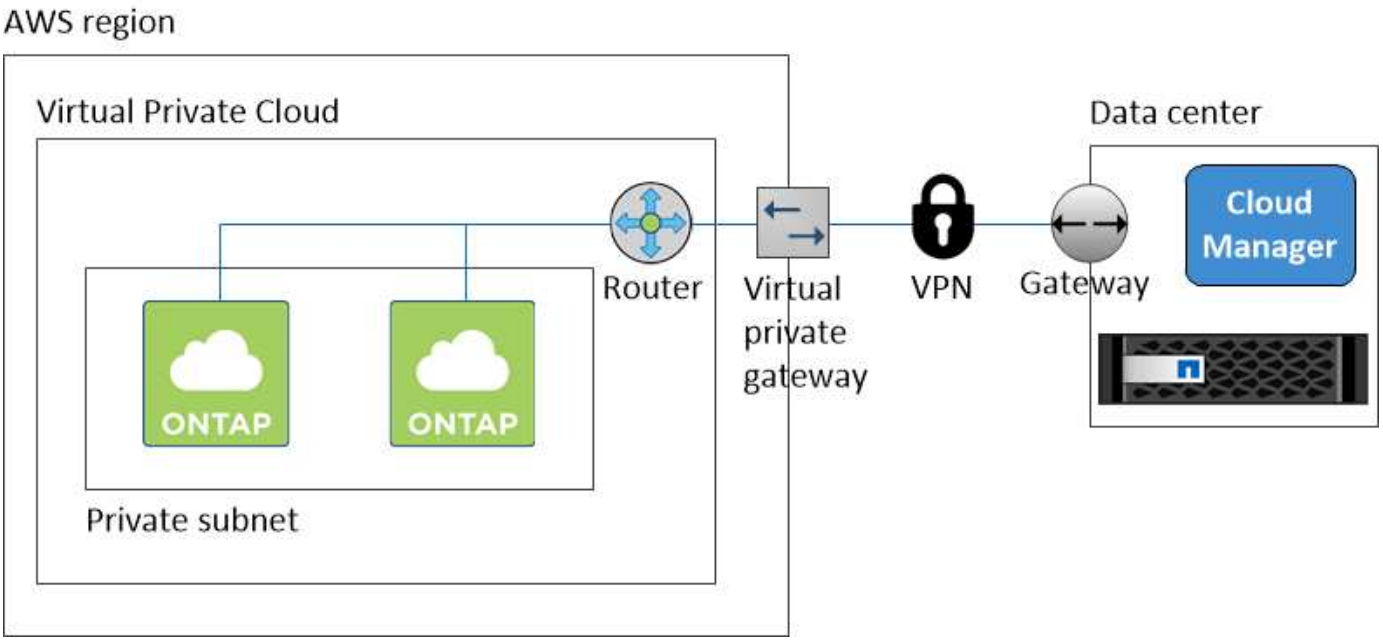
Questa configurazione VPC è una configurazione di cloud ibrido in cui Cloud Volumes ONTAP diventa un'estensione del tuo ambiente privato. La configurazione include una subnet privata e un gateway privato virtuale con una connessione VPN alla rete. Il routing attraverso il tunnel VPN consente alle istanze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

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

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

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

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



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

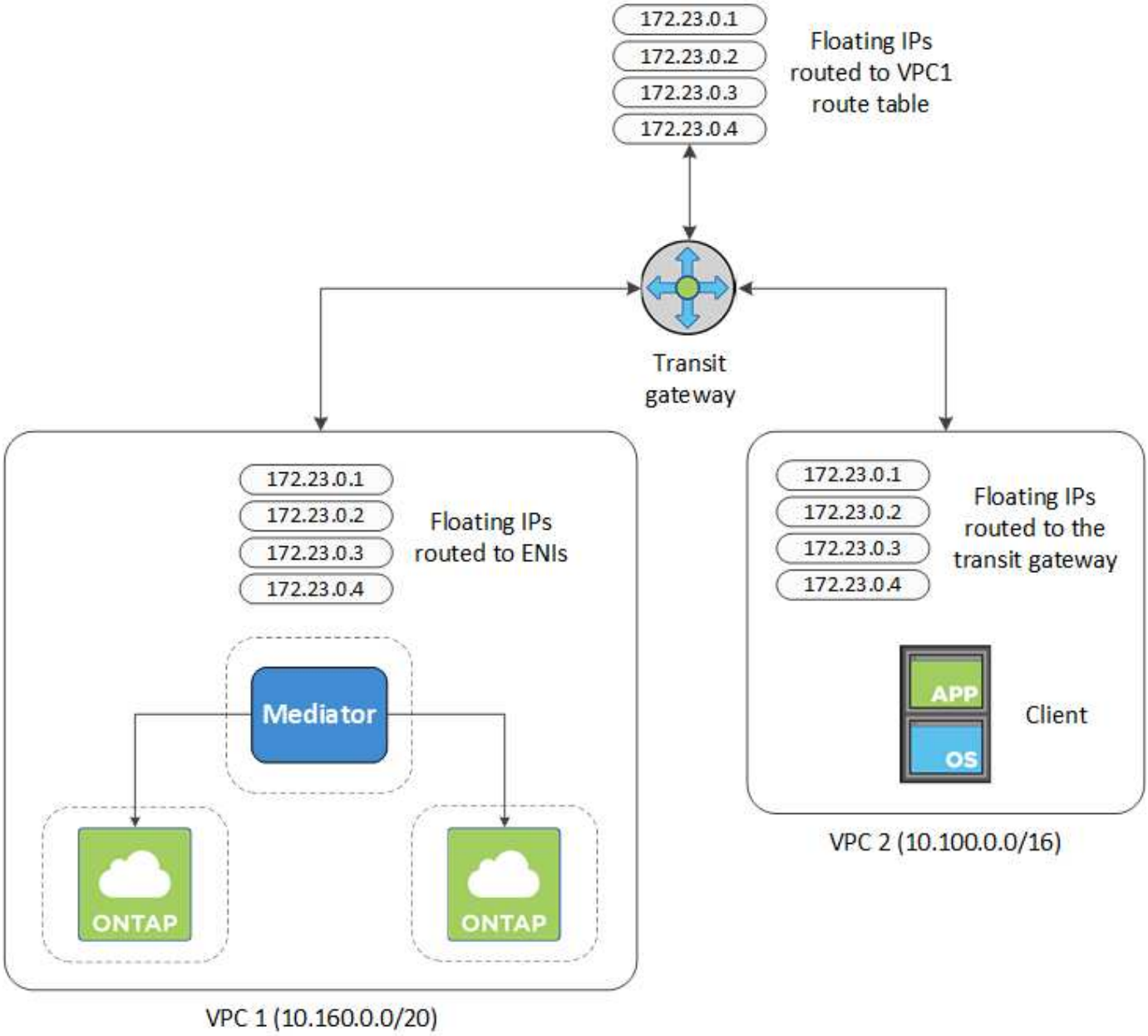
Impostare un gateway di transito AWS per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

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

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

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

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

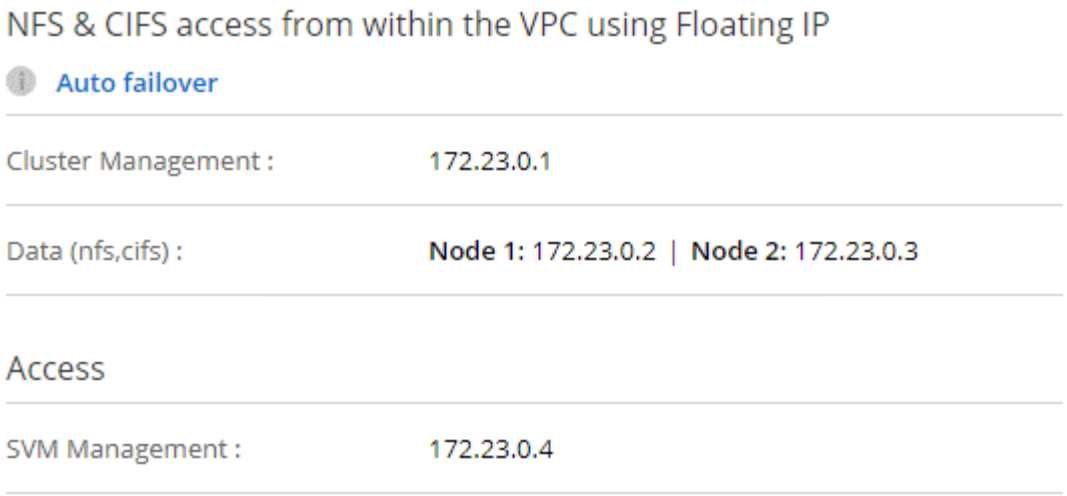


La seguente procedura illustra come configurare una configurazione simile.

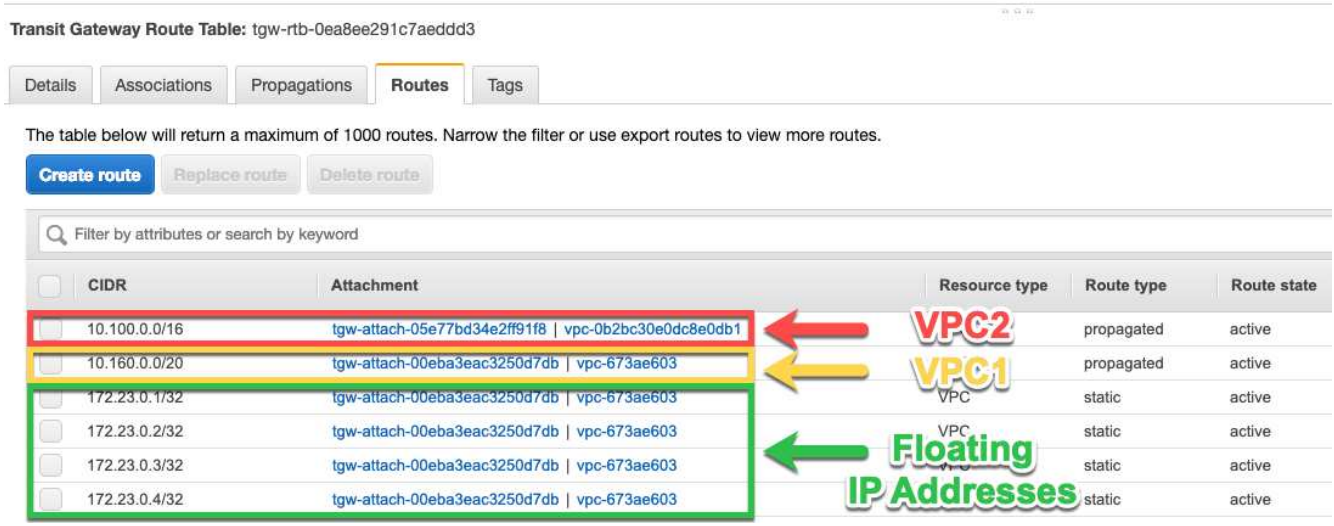
Fasi

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

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



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.

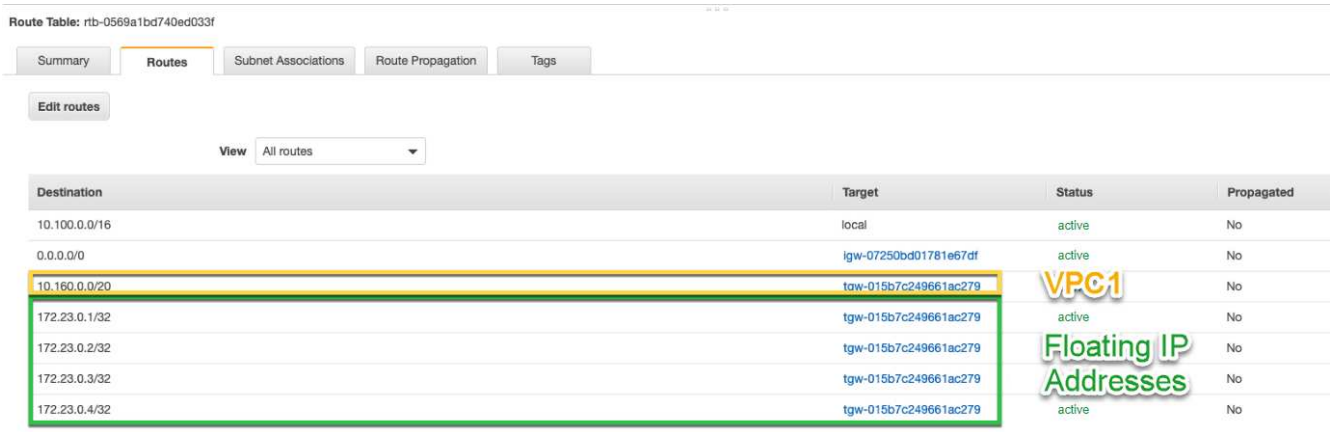


3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

   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.

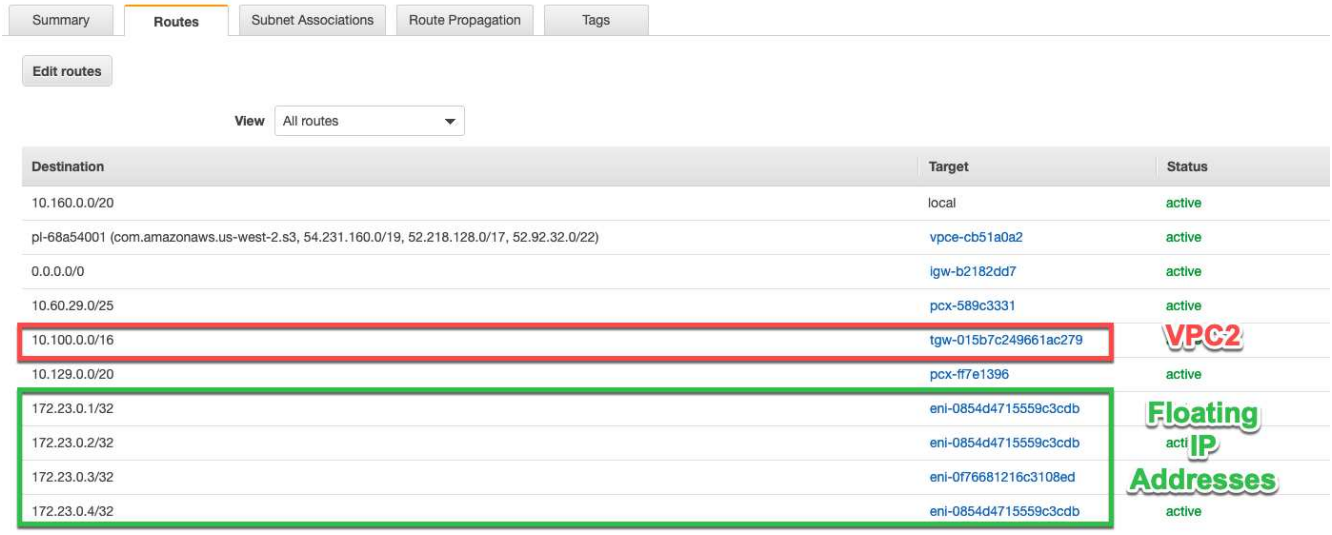
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.

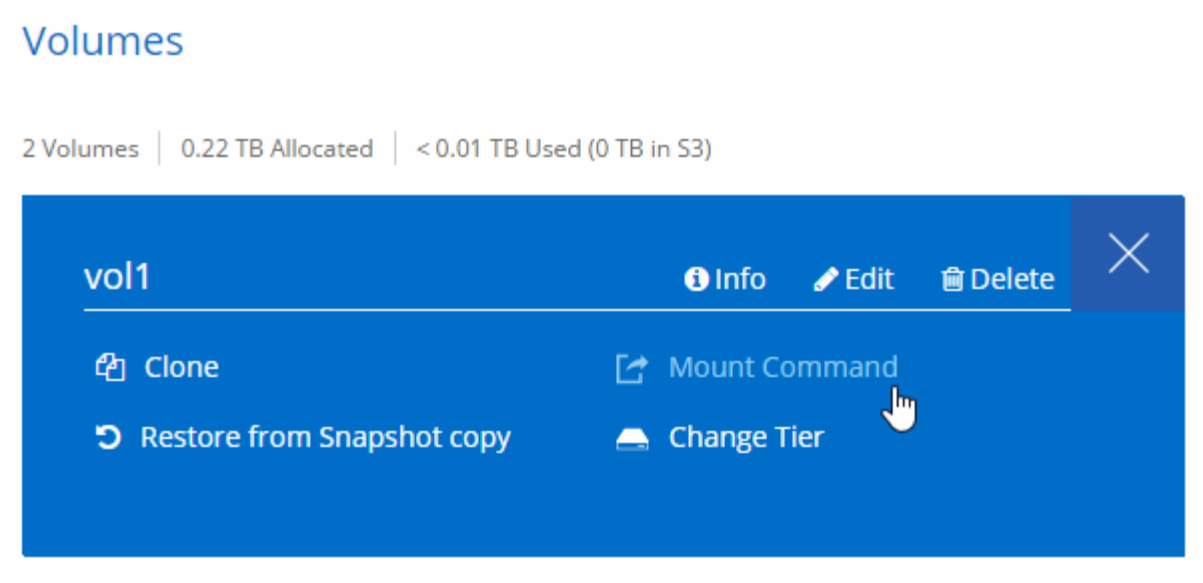
   Questo passaggio è importante perché completa il routing tra i VPC.

   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

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

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

Accesso a Internet in uscita per Cloud Volumes ONTAP

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

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

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

Gruppi di sicurezza

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

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

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

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

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

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

Connessioni a sistemi ONTAP in altre reti

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

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

Opzioni di implementazione aggiuntive

Requisiti degli host di Cloud Manager

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

Tipi di istanze AWS EC2 supportati

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

Dimensioni delle macchine virtuali Azure supportate

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

Sistemi operativi supportati

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

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

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

Hypervisor

Un hypervisor bare metal o in hosting certificato per l'esecuzione di CentOS o Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Soluzione Red Hat: Quali hypervisor sono certificati

per eseguire Red Hat Enterprise Linux?"^]

CPU

2.27 GHz o superiore con due core

RAM

4 GB

Spazio libero su disco

50 GB

Accesso a Internet in uscita

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

Porte

Devono essere disponibili le seguenti porte:

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

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

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

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

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

Installazione di Cloud Manager su un host Linux esistente

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

Prima di iniziare

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

"Requisiti di rete per Cloud Manager".

A proposito di questa attività

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

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

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

Fasi

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

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

4. Assegnare le autorizzazioni per eseguire lo script.

   Esempio

   ```
    chmod +x OnCommandCloudManager-V3.6.3.sh
   . Eseguire lo script di installazione:
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent esegue l'installazione senza richiedere informazioni.

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

   proxyport è la porta del server proxy.

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

   proxypwd è la password per il nome utente specificato.

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

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

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

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

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

   https://ipaddress:port

   Ipaddress può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host Cloud Manager. Ad esempio, se Cloud Manager si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario inserire un indirizzo IP privato da un host che ha una connessione all'host Cloud Manager.

   Port è obbligatorio se sono state modificate le porte HTTP (80) o HTTPS (443) predefinite. Ad esempio, se la porta HTTPS è stata modificata in 8443, immettere https://ipaddress:8443

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

Al termine

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

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

Avvio di Cloud Manager da AWS Marketplace

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

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

A proposito di questa attività

La seguente procedura descrive come avviare l'istanza dalla console EC2 perché la console consente di associare un ruolo IAM all'istanza di Cloud Manager. Ciò non è possibile utilizzando l'opzione 1-click.

Fasi

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

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

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

b. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.

c. Creare un ruolo IAM con il tipo di ruolo Amazon EC2 e allegare al ruolo il criterio creato nel passaggio precedente.

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

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

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

   c. Mantenere le opzioni di storage predefinite.

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

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

   f. Fare clic su **Avvia**.

Risultato

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

Al termine

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

Implementazione di Cloud Manager da Azure Marketplace

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

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

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

Implementazione di Cloud Manager in Azure

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

Fasi

1. "Vai alla pagina di Azure Marketplace per Cloud Manager".
2. Fare clic su **Get it now** (scarica ora), quindi su **Continue** (continua).

3. Dal portale Azure, fare clic su **Create** (Crea) e seguire la procedura per configurare la macchina virtuale.

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

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

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

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

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

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

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

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

   http://ipaddress:80

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

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

Risultato

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

Concessione delle autorizzazioni Azure a Cloud Manager

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

Fasi

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

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

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

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

      Esempio

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

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

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

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

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

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

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

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

Risultato

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

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

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

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

Implementazione di Cloud Manager da Azure US Government Marketplace

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

Fasi

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

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

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

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

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

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

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

   http://ipaddress:80

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

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

Risultato

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

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

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

Fasi

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

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

Volumes ONTAP.

Esempio

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

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

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

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

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

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

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

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

Risultato

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

Installazione di Cloud Manager in una regione di Azure Germania

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

Fasi

1. "Esaminare i requisiti di rete per Azure".
2. "Esaminare i requisiti degli host di Cloud Manager".

3. "Scarica e installa Cloud Manager".
4. "Concedere le autorizzazioni Azure a Cloud Manager utilizzando un'entità del servizio".

Al termine

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

Implementazione di 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.

L'amministratore dovrebbe aver seguito le istruzioni per iniziare a utilizzare il sistema "In AWS" oppure "In Azure", e facoltativamente "Configurare Cloud Manager".

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

- I requisiti di rete AWS e Azure sono stati soddisfatti per Cloud Manager e Cloud Volumes ONTAP.
- Cloud Manager dispone delle autorizzazioni necessarie per eseguire operazioni in AWS e Azure per conto dell'utente.
- Ogni prodotto Cloud Volumes ONTAP che gli utenti implementeranno è stato sottoscritto dal marketplace AWS.
- Cloud Manager installato.
- (Facoltativo) sono stati definiti tenant aggiuntivi.
- (Facoltativo) sono stati creati ulteriori account utente, che possono includere gli amministratori tenant e gli amministratori dell'ambiente di lavoro.

Accesso a Cloud Manager

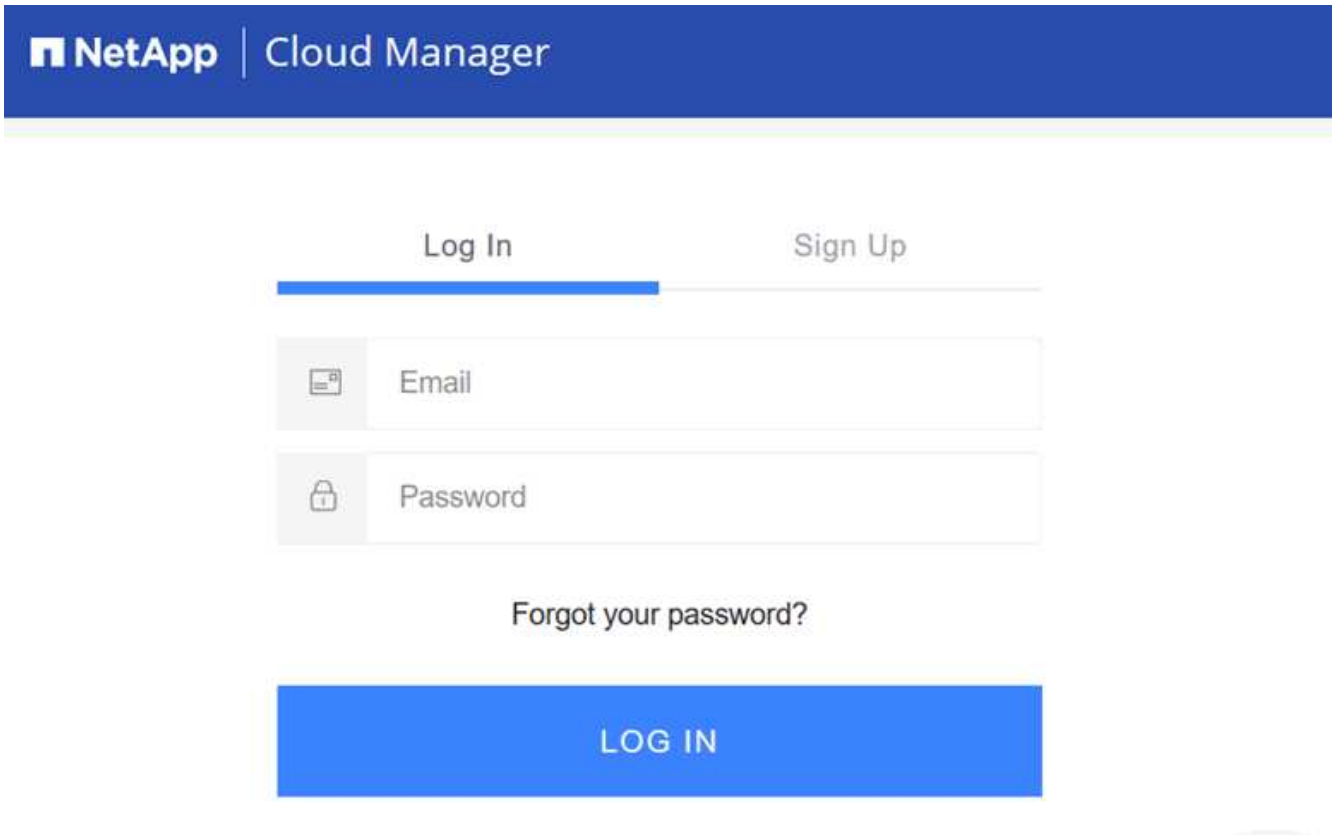
È possibile accedere a Cloud Manager da qualsiasi browser Web che dispone di una connessione al sistema Cloud Manager. È necessario effettuare l'accesso utilizzando un "NetApp Cloud Central" account utente.

Fasi

1. Aprire un browser Web e accedere a. "NetApp Cloud Central".
2. Fare clic su **Vai ai servizi dati cloud** e selezionare **Cloud Volumes ONTAP**.
3. Fare clic su **Vai a Cloud Manager** per il sistema Cloud Manager a cui si desidera accedere.

   Se non compare alcun sistema nell'elenco, assicurarsi che l'amministratore di Cloud Manager abbia aggiunto il proprio account NetApp Cloud Central al sistema.

4. Accedi a Cloud Manager utilizzando il tuo account 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 AWS e Azure 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 9.5"
- "Configurazioni supportate per Cloud Volumes ONTAP 9.4"
- "Configurazioni supportate per il cloud ONTAP 9.3"

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 9.5"

- "Limiti di storage per Cloud Volumes ONTAP 9.4"
- "Limiti di storage per il cloud ONTAP 9.3"

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*

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"

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.

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	
Tabelle di routing per gli indirizzi IP mobili	

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)	

Abilitazione di Flash cache su Cloud Volumes ONTAP in AWS

Alcuni tipi di istanze EC2 includono lo storage NVMe locale, utilizzato da Cloud Volumes ONTAP come *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.

Il ripristino della cache dopo un riavvio non è supportato con Cloud Volumes ONTAP.

Fasi

1. Selezionare uno dei seguenti tipi di istanze EC2, disponibili con le licenze Premium e BYOL:
   - c5d.4xlarge
   - c5d.9xlarge
   - r5d.2xlarge
2. Disattiva la compressione su tutti i volumi.

   La compressione deve essere disattivata su tutti i volumi per sfruttare i miglioramenti delle prestazioni di Flash cache. Quando crei un volume da Cloud Manager, puoi scegliere di non utilizzare l'efficienza dello storage, oppure creare 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.

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 **Aggiungi ambiente di lavoro**.
2. In Crea, selezionare **Cloud Volumes ONTAP**.
3. Nella pagina Dettagli e credenziali, modificare l'account AWS, immettere un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi immettere una password.

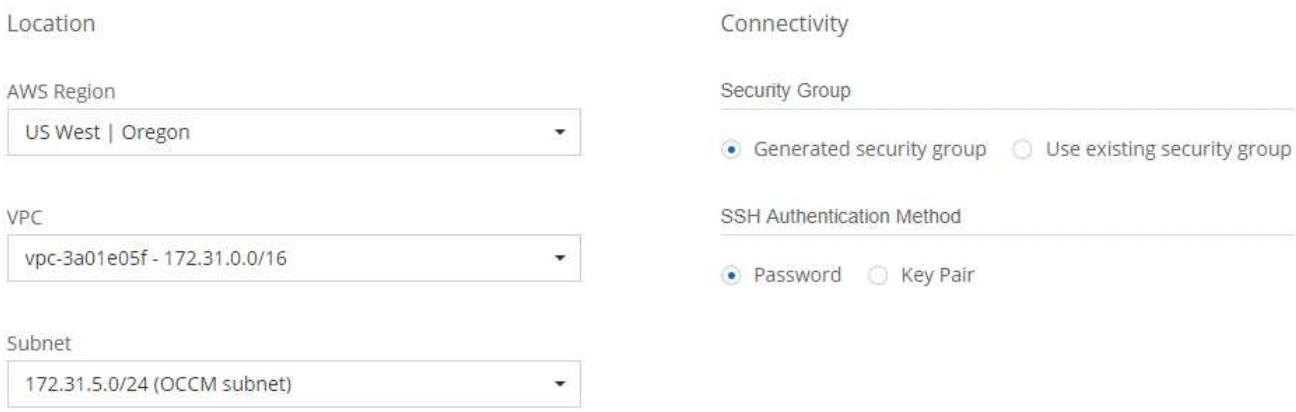
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Cambia account	Puoi scegliere un altro account se hai aggiunto altri account Cloud Provider. Per ulteriori informazioni, vedere "Aggiunta di account Cloud Provider 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 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.

   Se le chiavi AWS non sono state specificate per l'account Cloud Manager, viene richiesto di immetterle dopo aver fatto clic su Continue (continua). È necessario immetterli prima di procedere.

4. Nella pagina Location & Connectivity (posizione e connettività), inserire le informazioni di rete registrate nel foglio di lavoro AWS, quindi fare clic su **Continue** (continua).

   La seguente immagine mostra la pagina Location & Connectivity compilata:



5. Nella pagina Data Encryption (crittografia dati), scegliere NO data Encryption (Nessuna crittografia dati) o AWS-Managed Encryption (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.

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

   "Scopri di più sulle tecnologie di crittografia supportate".

6. Nella pagina 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. Nella pagina Preconfigured Packages (pacchetti preconfigurati), selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Create my own Configuration** (Crea configurazione personalizzata).

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

8. Nella pagina ruolo IAM, è necessario 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".

9. Nella pagina licenze, modificare la versione di Cloud Volumes ONTAP in base alle necessità, selezionare una licenza, un tipo di istanza, la tenancy dell'istanza, quindi fare clic su **continua**.

   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.

10. Nella pagina risorse storage sottostante, 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".

11. Nella pagina 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".

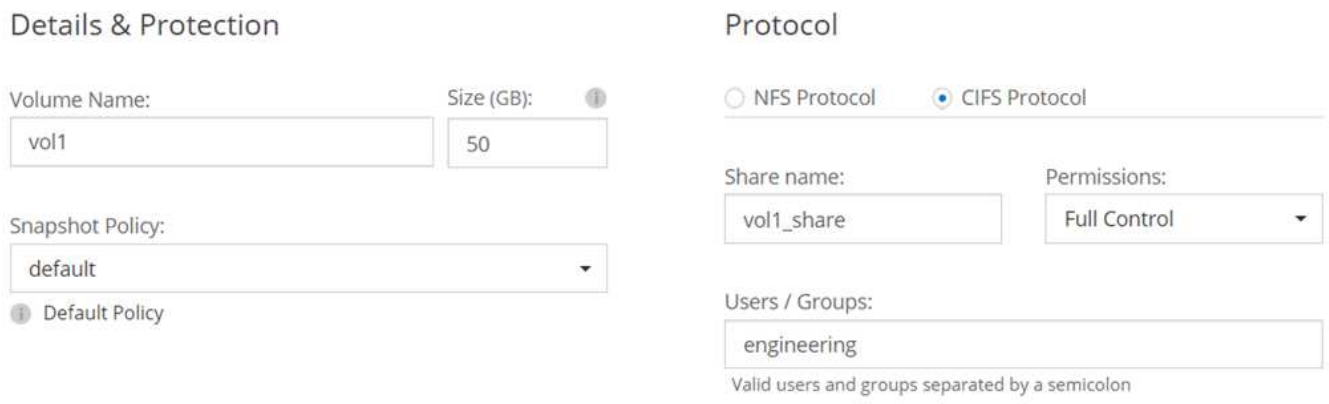
12. Nella pagina Create Volume (Crea volume), inserire i dettagli del nuovo volume, quindi fare clic su **Continue** (continua).

    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:



13. Se si sceglie il protocollo CIFS, impostare un server CIFS nella pagina CIFS Setup:

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.

14. 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 e modificare il criterio di tiering S3, se necessario.

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

15. Nella pagina Review & Approve (esamina e approva), 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 **Aggiungi ambiente di lavoro**.
2. In Crea, selezionare **Cloud Volumes ONTAP ha**.
3. Nella pagina Dettagli e credenziali, modificare l'account AWS, immettere un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi immettere 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
Cambia account	Puoi scegliere un altro account se hai aggiunto altri account Cloud Provider. Per ulteriori informazioni, vedere "Aggiunta di account Cloud Provider 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 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. 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.

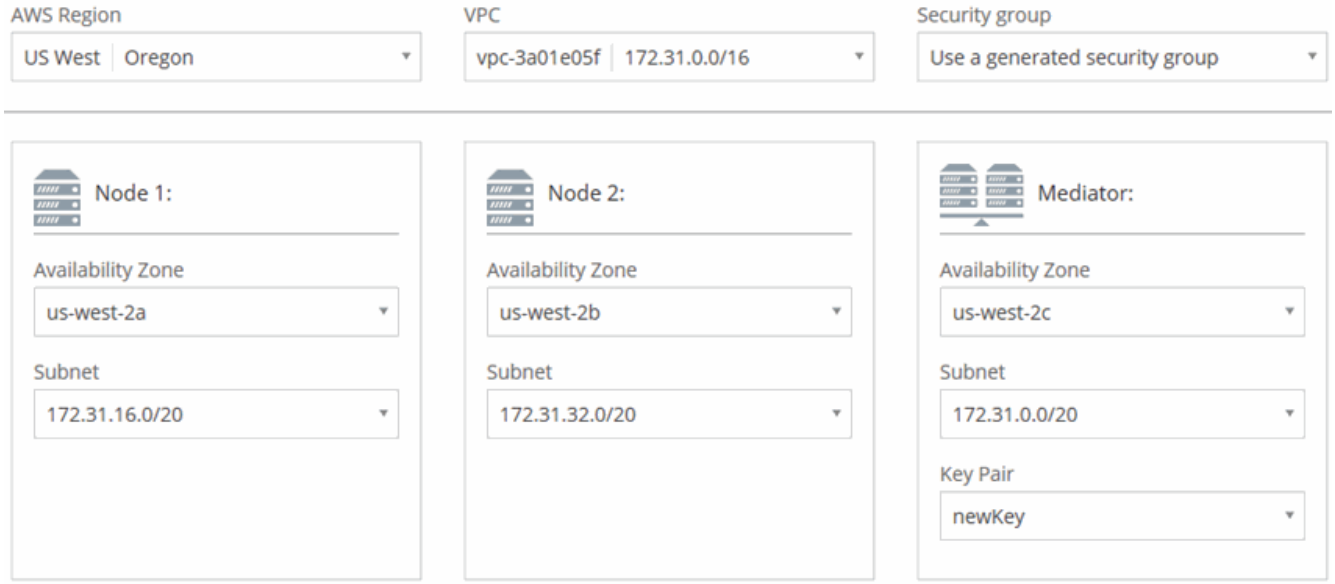
Se le chiavi AWS non sono state specificate per l'account Cloud Manager, viene richiesto di immetterle dopo aver fatto clic su Continue (continua). Prima di procedere, immettere i tasti AWS.

4. Nella pagina ha Deployment Models (modelli di implementazione ha), scegliere una configurazione ha.

   Per una panoramica dei modelli di implementazione, vedere "Cloud Volumes ONTAP ha per AWS".

5. Nella pagina Region & VPC (Regione e VPC), inserire le informazioni di rete registrate nel foglio di lavoro AWS, quindi fare clic su **Continue** (continua).

   La seguente immagine mostra la pagina Location (posizione) compilata per una configurazione AZ multipla:



6. Nella pagina Connectivity and SSH Authentication (connettività e autenticazione SSH), scegliere i metodi di connessione per la coppia ha e il mediatore.

7. Se si sceglie più AZS, specificare gli indirizzi IP mobili e fare clic su **continua**.

   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".

8. Se si sceglie più indirizzi AZS, selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili, quindi fare clic su **continua**.

   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".

9. Nella pagina Data Encryption (crittografia dati), scegliere NO data Encryption (Nessuna crittografia dati) o AWS-Managed Encryption (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.

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

   "Scopri di più sulle tecnologie di crittografia supportate".

10. Nella pagina 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".

11. Nella pagina Preconfigured Packages (pacchetti preconfigurati), selezionare uno dei pacchetti per avviare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Create my own Configuration** (Crea configurazione personale).

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

12. Nella pagina ruolo IAM, è necessario 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".

13. Nella pagina licenze, modificare la versione di Cloud Volumes ONTAP in base alle necessità, selezionare una licenza, un tipo di istanza, la tenancy dell'istanza, quindi fare clic su **continua**.

    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.

14. Nella pagina risorse storage sottostante, 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".

15. Nella pagina WORM, attivare lo storage write once, Read Many (WORM), se lo si desidera.

    "Scopri di più sullo storage WORM".

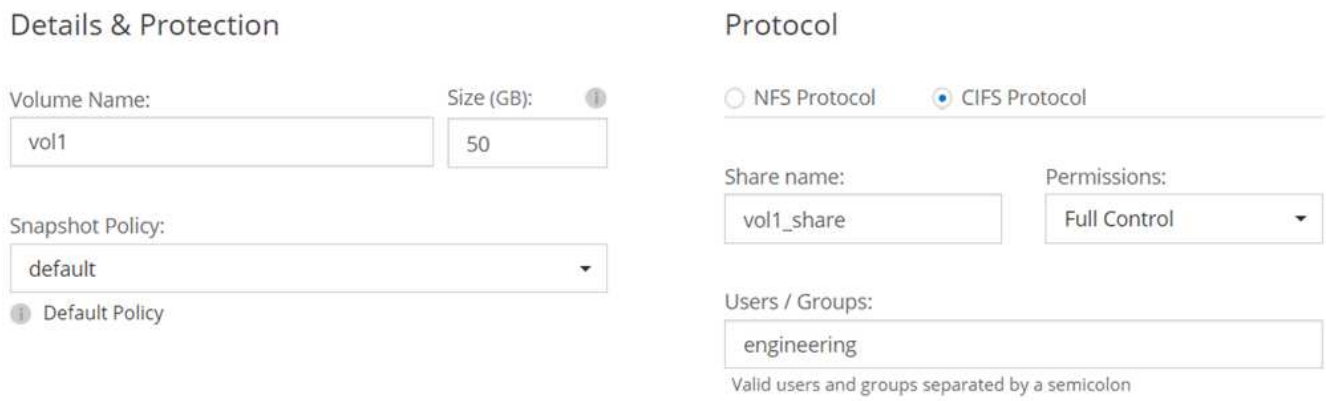
16. Nella pagina Create Volume (Crea volume), inserire i dettagli del nuovo volume, quindi fare clic su **Continue** (continua).

    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:



17. Se è stato selezionato il protocollo CIFS, configurare un server CIFS nella pagina CIFS Setup:

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.

18. 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 e modificare il criterio di tiering S3, se necessario.

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

19. Nella pagina Review & Approve (esamina e approva), 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.

  "Scopri le nuove autorizzazioni necessarie per implementare i sistemi ha".

- 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 **Aggiungi ambiente di lavoro**
2. In Crea, selezionare un sistema a nodo singolo in Azure o una coppia ha in Azure.
3. Nella pagina Dettagli e credenziali, modificare l'account o l'abbonamento Azure, specificare un nome di cluster e un nome 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 "Aggiunti altri account Cloud Provider".
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.
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. Nella pagina Location (posizione), selezionare una posizione e un gruppo di sicurezza, selezionare la casella di controllo per confermare la connettività di rete, quindi fare clic su **Continue** (continua).
5. Nella pagina 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".

6. Nella pagina Preconfigured Packages (pacchetti preconfigurati), selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Create my own Configuration** (Crea configurazione personale).

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

7. Nella pagina licenze, modificare la versione di Cloud Volumes ONTAP in base alle necessità, selezionare una licenza e un tipo di macchina virtuale, quindi fare clic su **continua**.

   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.

8. Nella pagina di Azure Marketplace, seguire i passaggi se Cloud Manager non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
9. Nella pagina risorse storage sottostante, 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 Azure".

10. Nella pagina 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".

11. Nella pagina Create Volume (Crea volume), inserire i dettagli del nuovo volume, quindi fare clic su **Continue** (continua).

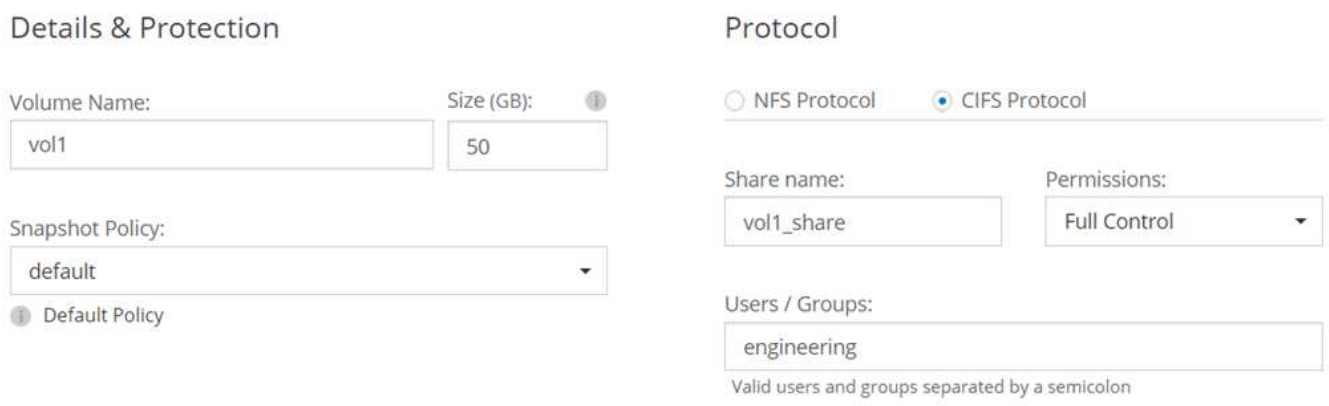
    Saltare questo passaggio se si desidera utilizzare iSCSI. Cloud Manager consente di creare volumi solo per NFS e CIFS.

    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. Se si sceglie il protocollo CIFS, impostare un server CIFS nella pagina CIFS Setup:

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. 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 e modificare la policy di tiering, se necessario.

> Il tiering dello storage è supportato solo con sistemi a nodo singolo.

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

14. Nella pagina Review & Approve (esamina e approva), 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.

Registrazione di sistemi pay-as-you-go

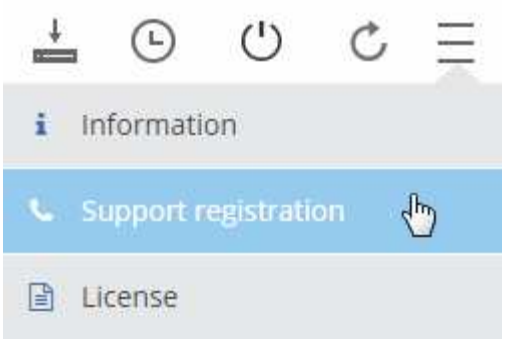
Il supporto NetApp è incluso nei sistemi Cloud Volumes ONTAP Explore, Standard e Premium, ma è necessario prima attivare il supporto registrando i sistemi con NetApp.

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:
	
	POST /vsa/working-environments/{workingEnvironmentId}/ntp
	Setup NTP server.
	Operation may only be performed on working environments whose status is: ON, DEGRADED.
	
	Parameters
	Parameter | Value | Description | Parameter Type | Data Type
	workingEnvironmentId | | Public Id of working environment | path | string
	body | (required) | NTP Configuration request | body | Model | Model Schema
	NTPConfigurationRequest {
	ntpServer (string): NTPS server
	}
	Parameter content type: application/json
	Try it out!

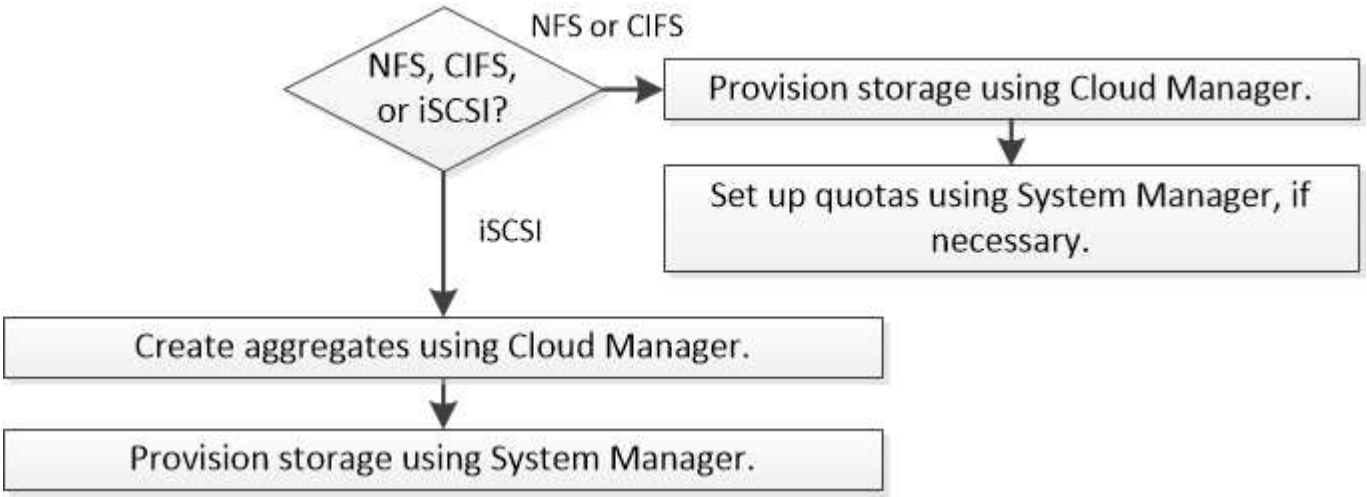
Attività	Descrizione
Facoltativo: Configurare AutoSupport	AutoSupport monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp per impostazione predefinita. Se l'amministratore di Cloud Manager ha aggiunto un server proxy a Cloud Manager prima 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".

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.



Volumi di provisioning

Se hai bisogno di più storage dopo il lancio di un sistema Cloud Volumes ONTAP, puoi eseguire il provisioning di nuovi volumi NFS e 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.
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.
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 S3, 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.

Provisioning dei volumi 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

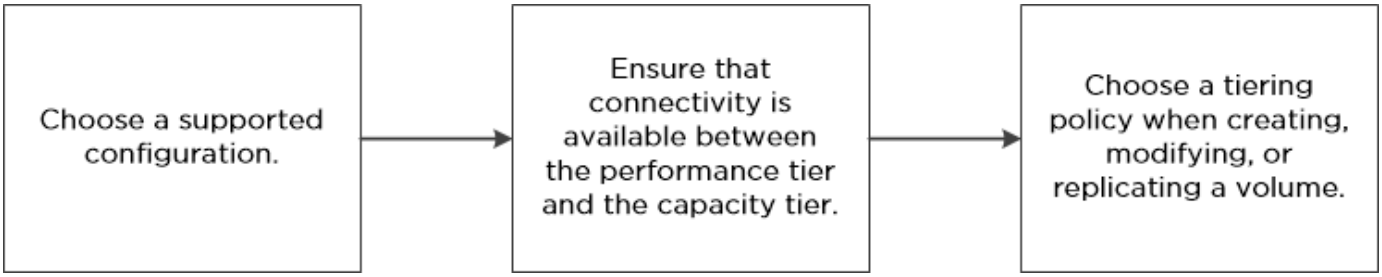
1. "Accedere a System Manager".
2. Fare clic su **Storage > LUN**.
3. Fare clic su **Create** (Crea) e seguire le istruzioni per creare il LUN.
4. Connettersi al LUN dagli host.

   Per istruzioni, consultare "Documentazione delle utility host" per il sistema operativo in uso.

Tiering dei dati inattivi su storage a oggetti a basso costo

È possibile ridurre i costi di storage in AWS e Azure 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:



Cosa non è richiesto per il tiering dei dati? (8217

- Non è necessario installare una licenza per le funzionalità per attivare il tiering dei dati.
- Non è necessario creare il Tier di capacità (un bucket S3 o un container Azure Blob). 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 dalla versione 9.2 in AWS e dalla versione 9.4 in Microsoft Azure.
  - Il tiering dei dati non è supportato con le coppie ha in Microsoft Azure.
  - 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.
- Il tiering dei dati è supportato dalle tecnologie di crittografia.
- Il thin provisioning deve essere attivato sui volumi.

Requisiti per il tiering dei dati in AWS

Assicurarsi che Cloud Volumes ONTAP sia connesso 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 in Microsoft Azure

Non è necessario impostare 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 dell'autorizzazione appropriata:

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

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

Tiering dei dati sui 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

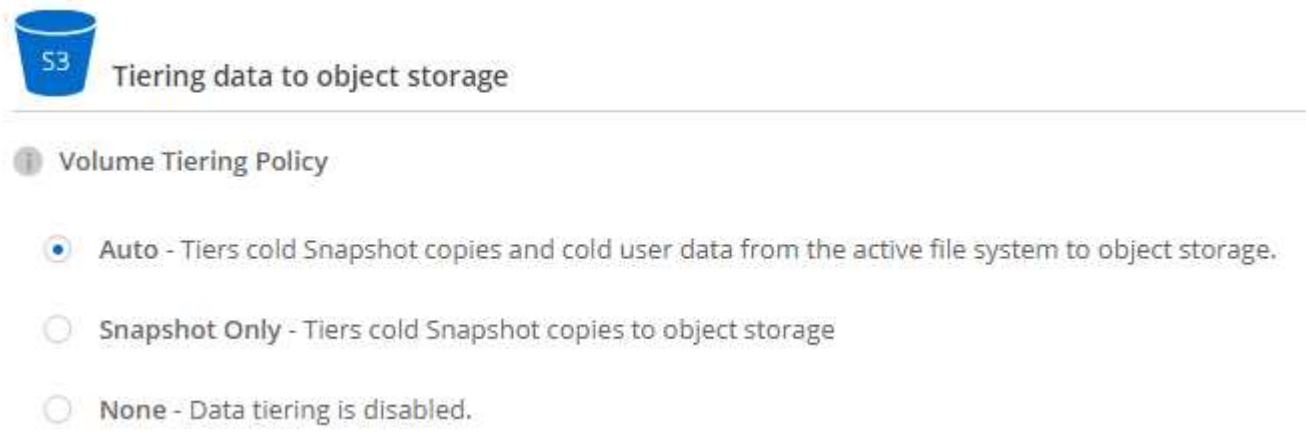
1. Nell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

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.

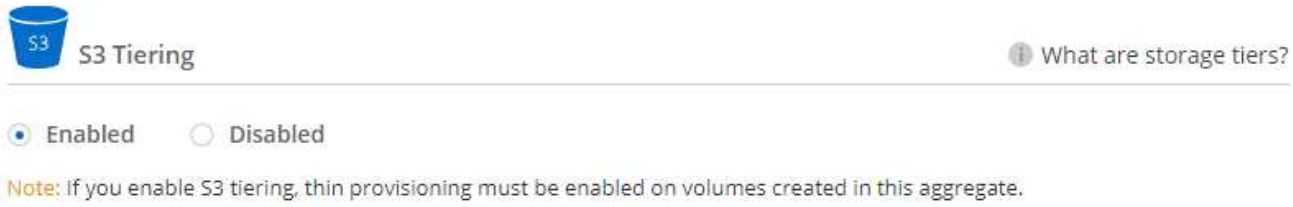
Tiering dei dati sui volumi di protezione dei dati

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

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.

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 su **livello di Tier**.

2. Scegliere il livello di tiering, quindi fare clic su **Save** (Salva).

Utilizzo di Cloud Volumes ONTAP come storage persistente per Kubernetes

Cloud Manager può automatizzare l'implementazione di "Trident di NetApp" Sui cluster Kubernetes in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container. La guida introduttiva include alcuni passaggi.

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.

1 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 Cloud Volumes ONTAP.
2. Cloud Manager richiede una connessione Internet in uscita per accedere ai seguenti endpoint durante l'installazione di Trident:

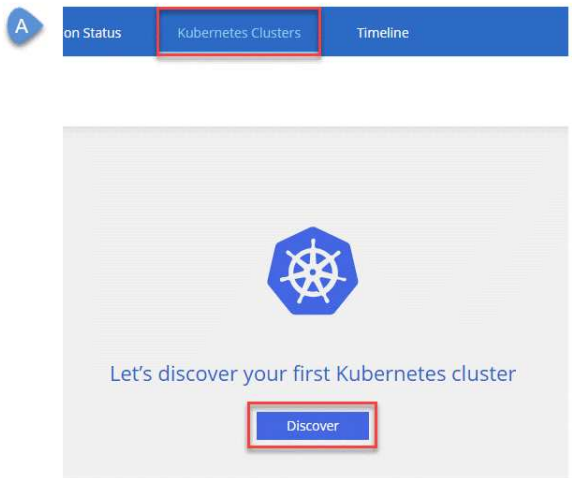
   https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

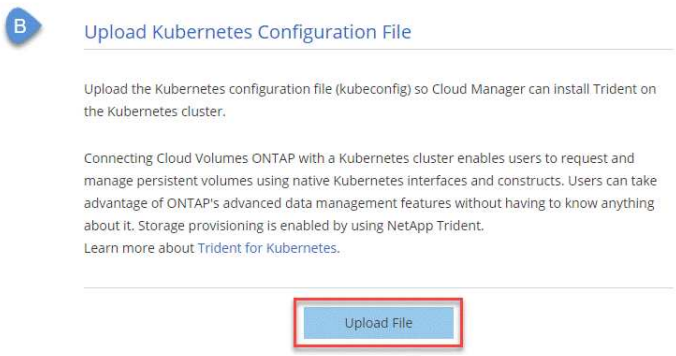
   Cloud Manager installa Trident su un cluster Kubernetes quando si connette un ambiente di lavoro al cluster.

2 Caricare i file di configurazione di Kubernetes in Cloud Manager

Per ogni cluster Kubernetes, l'amministratore di Cloud Manager 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.

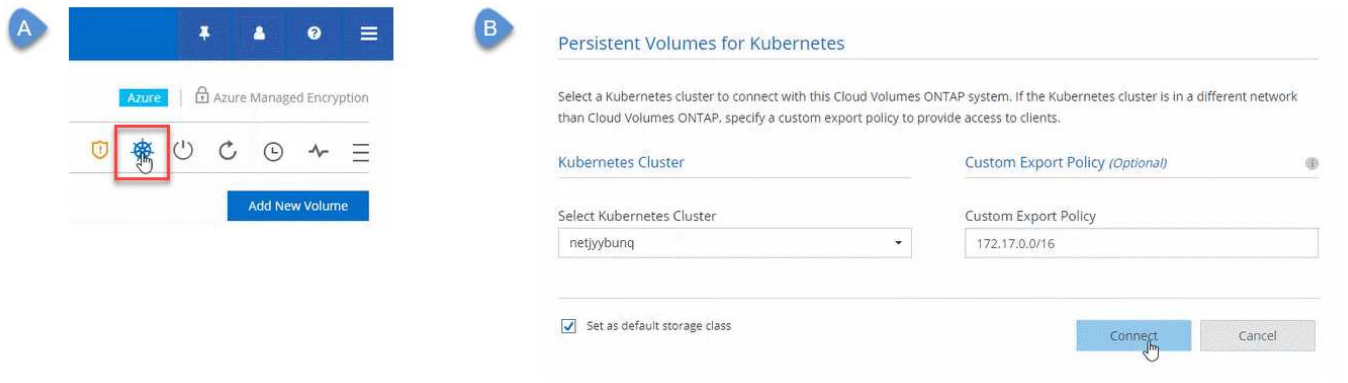




Connetti i tuoi ambienti di lavoro ai cluster Kubernetes

Dall'ambiente di lavoro, fare clic sull'icona Kubernetes e seguire le istruzioni. È possibile collegare diversi cluster a diversi sistemi Cloud Volumes ONTAP e più cluster allo stesso sistema Cloud Volumes 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 Cloud Volumes ONTAP connessi come storage back-end per impostazione predefinita.



Avviare il provisioning dei volumi persistenti

Richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi. Cloud Manager crea due classi di storage Kubernetes che è possibile utilizzare per il provisioning di volumi persistenti:

- **netapp-file**: Per il binding di volumi persistenti a sistemi Cloud Volumes ONTAP a nodo singolo
- **netapp-file-Redundant**: Per il binding di volumi persistenti a coppie Cloud Volumes 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 Cloud Volumes ONTAP a cui ci si connette a un cluster Kubernetes. Il nome del volume viene aggiunto con "_Trident_Trident". I sistemi Cloud Volumes ONTAP utilizzano 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 Cloud Volumes ONTAP da un cluster Kubernetes. Quando si disconnette un sistema, non è più possibile utilizzarlo Cloud Volumes 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

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 una licenza per la crittografia dei volumi NetApp sul sistema Cloud Volumes ONTAP.

   "Guida all'alimentazione per la crittografia NetApp di ONTAP 9: Installazione della licenza"

4. 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"

5. 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).

Attività	Azione
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.
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.

Attività	Azione
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).
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.

Attività	Azione
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.
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.

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

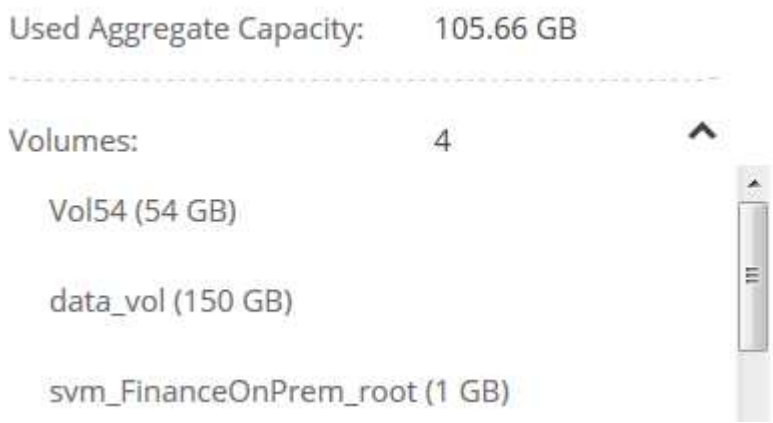
Se Cloud Manager non è in grado di fornire consigli per lo spostamento di un volume per evitare problemi di capacità, è necessario identificare i volumi da spostare e se è necessario spostarli in un altro aggregato sullo stesso sistema o in un altro sistema.

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.

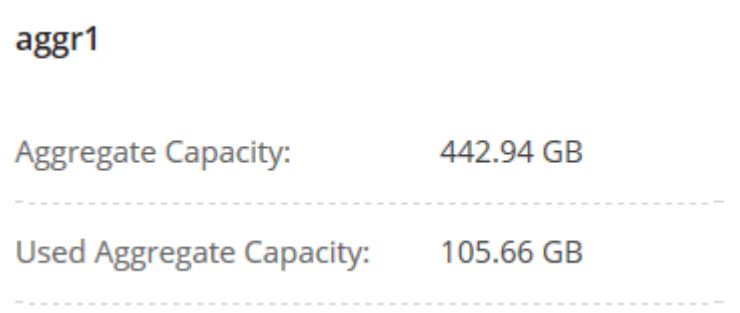
A proposito di questa attività

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".

Provisioning dei volumi NFS da Volume View

Passaggio alla vista volume

Cloud Manager offre due viste di gestione: La vista del sistema di storage per la gestione dei sistemi storage in un cloud ibrido e la vista del volume per la creazione di volumi in AWS senza dover gestire i sistemi storage. È possibile passare da una vista all'altra, ma tali istanze dovrebbero essere rare perché una singola vista dovrebbe soddisfare le proprie esigenze.

Per ulteriori informazioni su Volume View, vedere "Gestione dello storage semplificata grazie a Volume View".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sul menu, quindi su **View Selection** (Visualizza selezione).
2. Nella pagina View Selection, selezionare **Storage System View**, quindi fare clic su **Switch**.

Risultato

Cloud Manager passa alla vista volume.

Creazione e montaggio di volumi NFS

È possibile utilizzare Cloud Manager per creare volumi NFS che offrono funzionalità di livello Enterprise oltre allo storage AWS.

Creazione di volumi NFS

È possibile creare un volume collegato a una singola istanza di AWS o a un'istanza che viene sottoposta a mirroring su un'altra istanza per garantire una disponibilità elevata.

Fasi

1. Nella scheda Volumes (volumi), fare clic su **Create New Volume** (Crea nuovo volume).
2. Nella pagina Create New Volume (Crea nuovo volume), selezionare un tipo di volume:

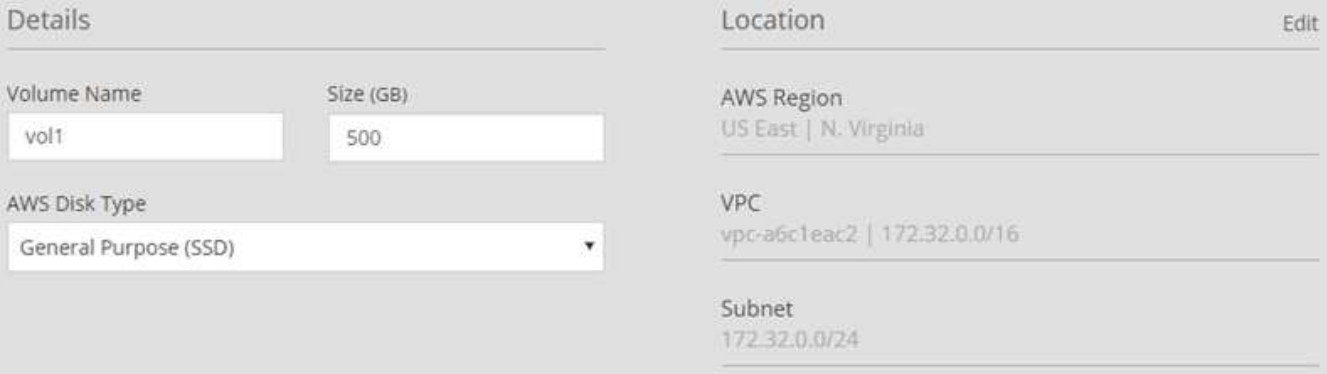
Opzione	Descrizione
Crea volume	Crea un volume collegato a una singola istanza di AWS.
Creare un volume ha	Crea un volume collegato a una singola istanza di AWS e mirrorato a un'altra istanza per garantire un'elevata disponibilità in caso di errori. Fare clic sull'icona Info per visualizzare ulteriori dettagli sulle istanze richieste per un volume ha.

3. Se si seleziona Create Volume (Crea volume), specificare i dettagli del primo volume, quindi fare clic su **Create** (Crea).

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

Campo	Descrizione
Dimensione	Le dimensioni massime del volume dipendono dalla capacità disponibile nei sistemi di storage esistenti. Il thin provisioning viene attivato automaticamente sul volume, consentendo di creare un volume più grande dello storage fisico attualmente disponibile. Invece di preallocare lo spazio di storage, lo spazio viene allocato a ciascun volume durante la scrittura dei dati.
Tipo di disco AWS	Devi scegliere il disco che soddisfa i tuoi requisiti in termini di performance e costi. • I dischi SSD General Purpose bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS. • I dischi HDD ottimizzati per il throughput sono destinati a carichi di lavoro con accesso frequente che richiedono un throughput rapido e coerente a un prezzo inferiore. • I dischi rigidi a freddo 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. Per ulteriori informazioni, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

La seguente immagine mostra la pagina Create Volume compilata:



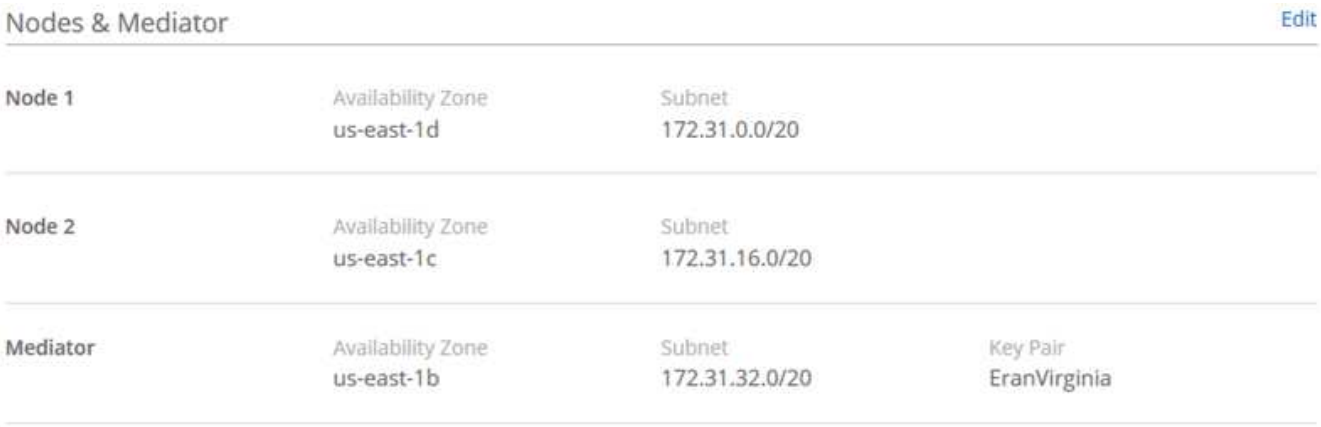
4. Se si sceglie Create ha volume (Crea volume ha), specificare i dettagli per il volume, quindi fare clic su **Create** (Crea).

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

Campo	Descrizione
Dimensione	Le dimensioni massime del volume dipendono dalla capacità disponibile nei sistemi di storage esistenti. Il thin provisioning viene attivato automaticamente sul volume, consentendo di creare un volume più grande dello storage fisico attualmente disponibile. Invece di preallocare lo spazio di storage, lo spazio viene allocato a ciascun volume durante la scrittura dei dati.

Campo	Descrizione
Tipo di disco AWS	Devi scegliere il disco che soddisfa i tuoi requisiti in termini di performance e costi. • I dischi SSD General Purpose bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS. • I dischi HDD ottimizzati per il throughput sono destinati a carichi di lavoro con accesso frequente che richiedono un throughput rapido e coerente. Per ulteriori informazioni, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".
Posizione	Scegliere un VPC che includa tre subnet in tre zone di disponibilità separate.
Nodi e mediatore	Se possibile, Cloud Manager sceglie zone di disponibilità separate per ogni istanza perché è la configurazione ottimale e supportata.
IP mobile	Gli indirizzi IP devono essere esterni al blocco CIDR per tutti i VPC della regione.
Tabella di routing	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 ha. Per ulteriori informazioni, fare riferimento a. "Documentazione AWS: Tabelle di percorso".

L'immagine seguente mostra la pagina nodi e mediatore. Ogni istanza si trova in un'area di disponibilità separata.



Risultato

Cloud Manager crea il volume su un sistema esistente o su un nuovo sistema. Se è necessario un nuovo sistema, la creazione del volume può richiedere circa 25 minuti.

Montaggio di volumi su host Linux

Dopo aver creato un volume, è necessario montarlo sugli host in modo che possano accedere al volume.

Fasi

1. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu, quindi fare clic su **Mount**.
2. Fare clic su **Copy** (Copia).
3. Sugli host Linux, modificare il testo copiato cambiando la directory di destinazione, quindi immettere il

comando per montare il volume.

Gestione dei volumi NFS

Puoi gestire i volumi NFS clonandoli, gestendo l'accesso ai dati, modificando il tipo di disco sottostante e molto altro ancora.

Cloning dei volumi

Se è necessaria una copia istantanea dei dati senza utilizzare molto spazio su disco, è possibile creare un clone di un volume esistente.

A proposito di questa attività

Il volume clonato 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.

Fasi

1. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu, quindi fare clic su **Clone**.
2. Modificare il nome del volume clonato, se necessario, quindi fare clic su **Clone**.

Risultato

Cloud Manager crea un nuovo volume che è un clone di un volume esistente.

Gestione dell'accesso ai dati ai volumi

Quando si crea un volume, Cloud Manager rende il volume disponibile per tutte le istanze EC2 nel VPC in cui è stato creato il volume. È possibile modificare questo valore predefinito se si desidera limitare l'accesso ai dati al volume.

Fasi

1. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu, quindi fare clic su **Manage Access** (Gestisci accesso).
2. Modificare l'elenco di accesso al volume, quindi fare clic su **Save** (Salva).

Modifica del disco AWS sottostante per un volume

È possibile modificare il disco AWS sottostante utilizzato da un volume per fornire lo storage. Ad esempio, se sono necessarie prestazioni più elevate, è possibile passare da un disco rigido ottimizzato per il throughput a un SSD General Purpose.

Fasi

1. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu, quindi fare clic su **Change Disk** (Modifica disco).
2. Selezionare il tipo di disco AWS e fare clic su **Change** (Modifica).

Risultato

Cloud Manager sposta il volume in un aggregato esistente che utilizza il tipo di disco selezionato oppure crea un nuovo aggregato per il volume.

Visualizzazione e modifica delle risorse AWS

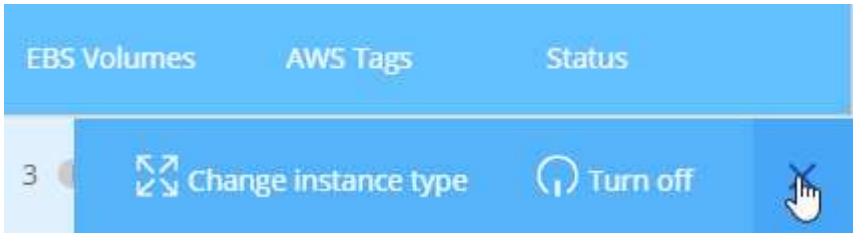
Quando si crea un nuovo volume, Cloud Manager assegna le istanze AWS e lo storage EBS necessari per quel volume. Se necessario, è possibile visualizzare i dettagli relativi alle istanze di AWS e allo storage EBS, modificare i tipi di istanze e attivare e disattivare le istanze.

Fasi

1. Fare clic su **risorse AWS**.

   Viene visualizzato l'elenco delle istanze di AWS. È possibile visualizzare dettagli quali il tipo di istanza, la posizione AWS e i volumi associati all'istanza.

2. Se necessario, selezionare l'icona del menu accanto alla colonna Status (Stato), quindi scegliere una delle azioni disponibili:



Eliminazione di volumi

È possibile eliminare volumi non più necessari.

Fasi

1. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu, quindi fare clic su **Delete** (Elimina).
2. Fare clic su **Delete** (Elimina) per confermare che si desidera eliminare il volume.

Gestione dei dati in un cloud ibrido

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.

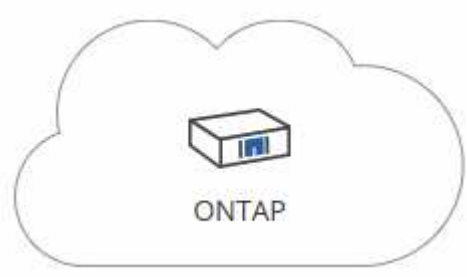
- Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443.

  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.

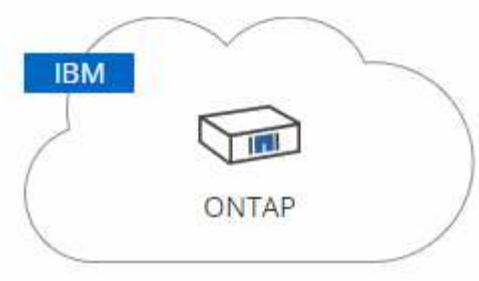
Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. In **Discover**, selezionare una delle icone per rilevare un cluster ONTAP.

   La seguente icona consente di individuare un cluster on-premise o una configurazione di NetApp Private Storage:

   La seguente icona consente di scoprire ONTAP nel cloud IBM:



3. Nella pagina **Dettagli cluster ONTAP**, inserire l'indirizzo IP di gestione del cluster e la password per l'account utente admin.

   Se è stata selezionata la prima icona, è necessario scegliere anche il tipo di ambiente di lavoro: Un cluster on-premise o una configurazione NetApp Private Storage.

4. 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.

Campo	Descrizione
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 da e verso il cloud

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.

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.

Scelta di un criterio 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. Quando si imposta la replica dei dati in Cloud Manager, è necessario scegliere un criterio di replica.

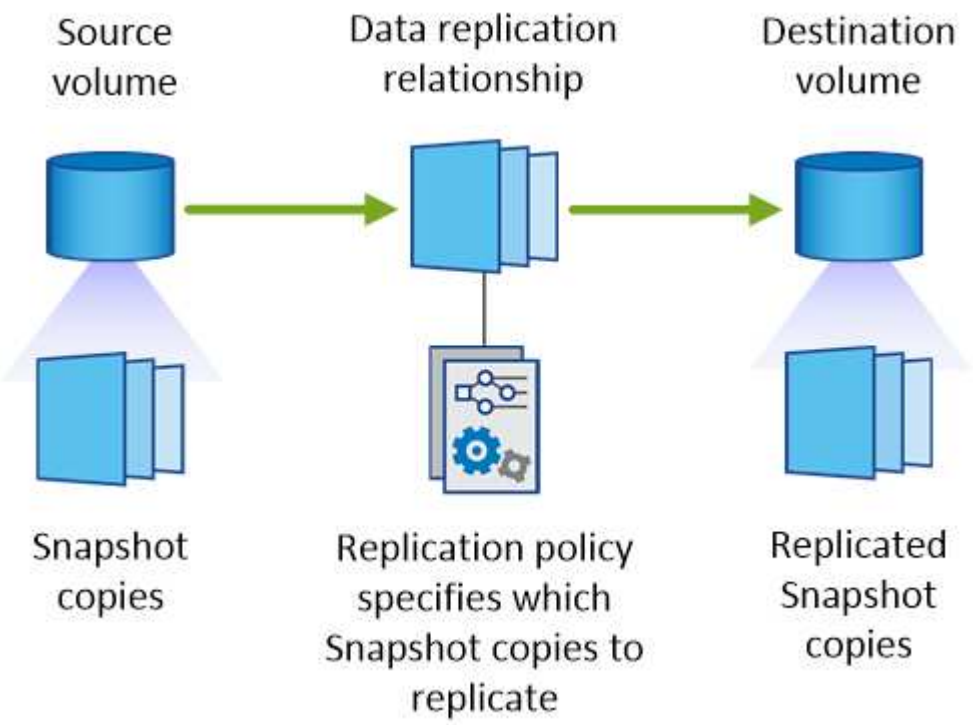
Quali sono le funzioni delle policy di replica

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.

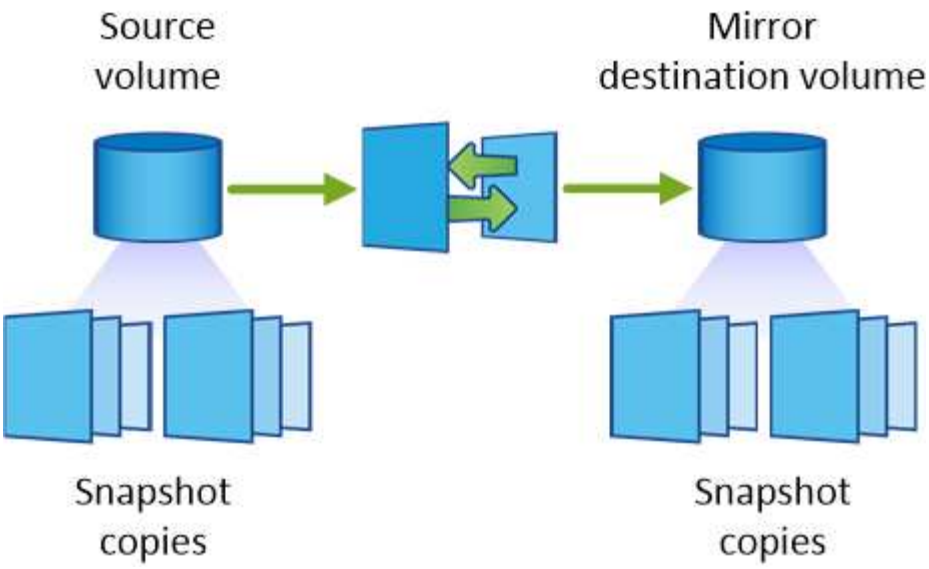
- Un criterio *Backup* replica copie Snapshot specifiche in un volume di destinazione e le conserva per un periodo di tempo più lungo rispetto al volume di origine.

  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.

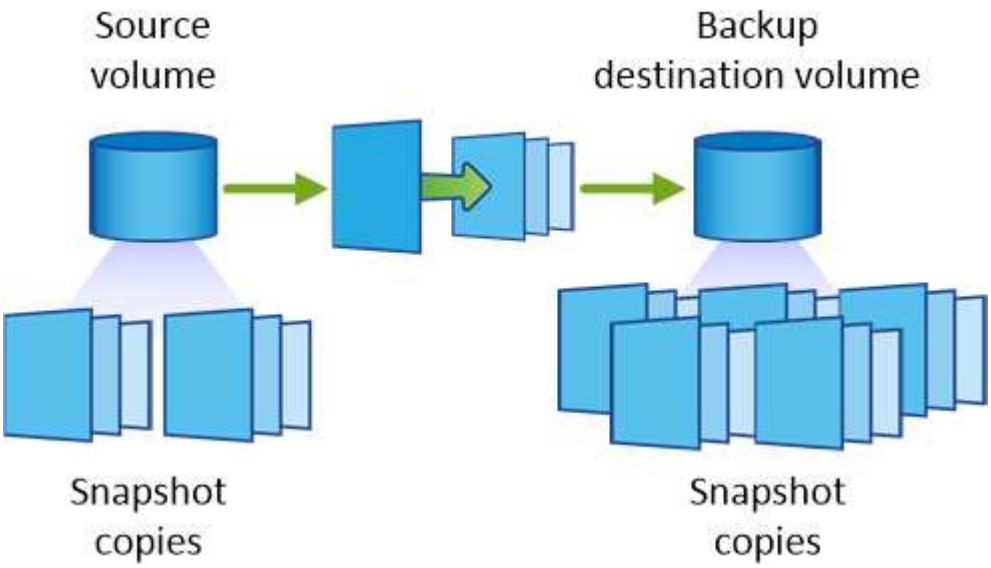
- Una policy di *Mirror e Backup* fornisce sia il disaster recovery che la conservazione a lungo termine.

  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.

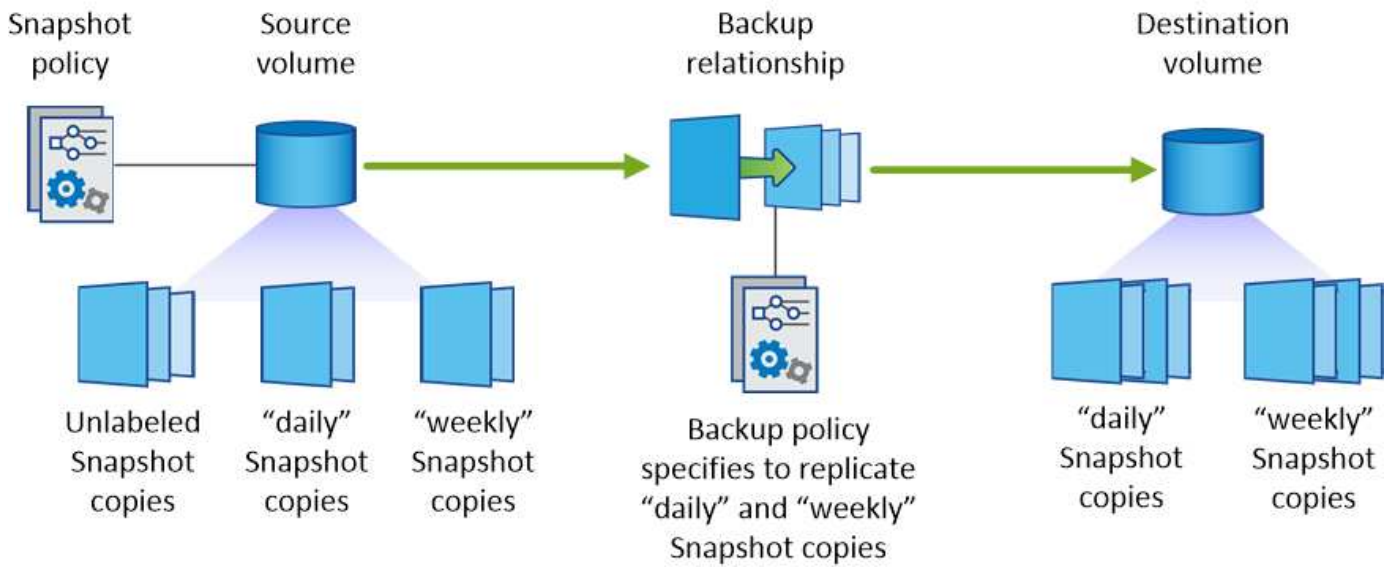
Comprensione della relazione tra le etichette delle copie Snapshot e le policy di backup

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.

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.

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).

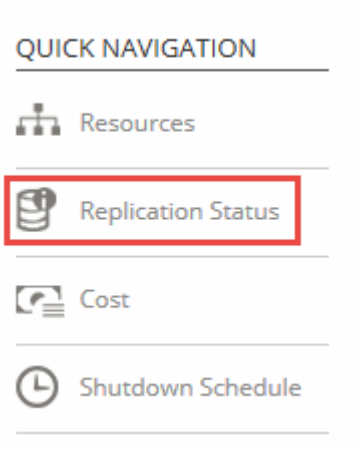
Gestione delle pianificazioni e delle relazioni di replica dei dati

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 assegnati nel tenant o per un ambiente di lavoro specifico:

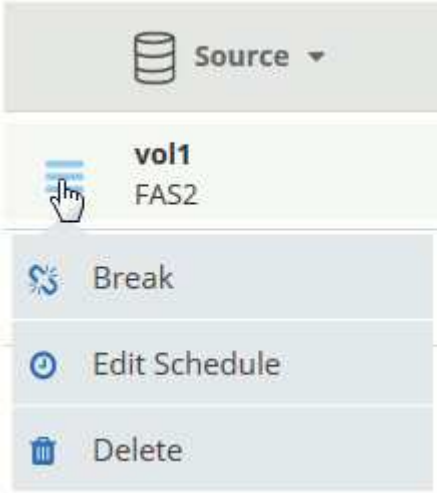
Opzione	Azione
Tutti gli ambienti di lavoro assegnati nel tenant	Fare clic su Replication Status (Stato replica) nella barra di navigazione. 

Opzione	Azione
Un ambiente di lavoro specifico	Selezionare l'ambiente di lavoro, quindi fare clic su Replication Status (Stato replica). 

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.
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.
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.

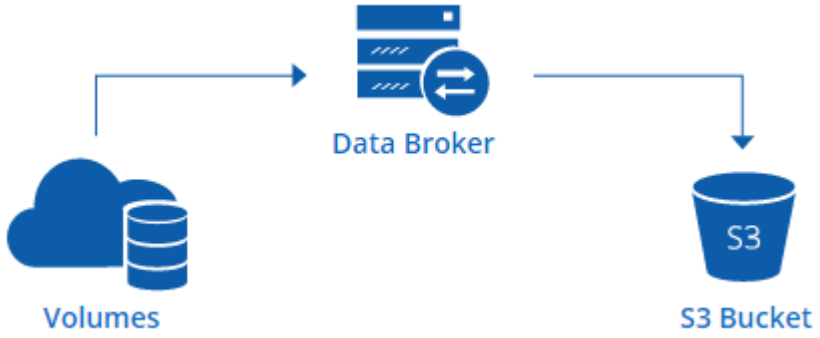
Sincronizzazione dei dati con AWS S3

È possibile sincronizzare i dati dai volumi ONTAP a un bucket AWS 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.

> La funzione di sincronizzazione con S3 è disponibile solo per gli amministratori Cloud Manager e gli amministratori tenant.

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 AWS 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.

Amministrazione di 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.

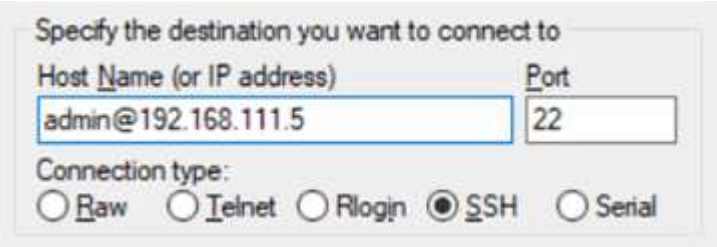
Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

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

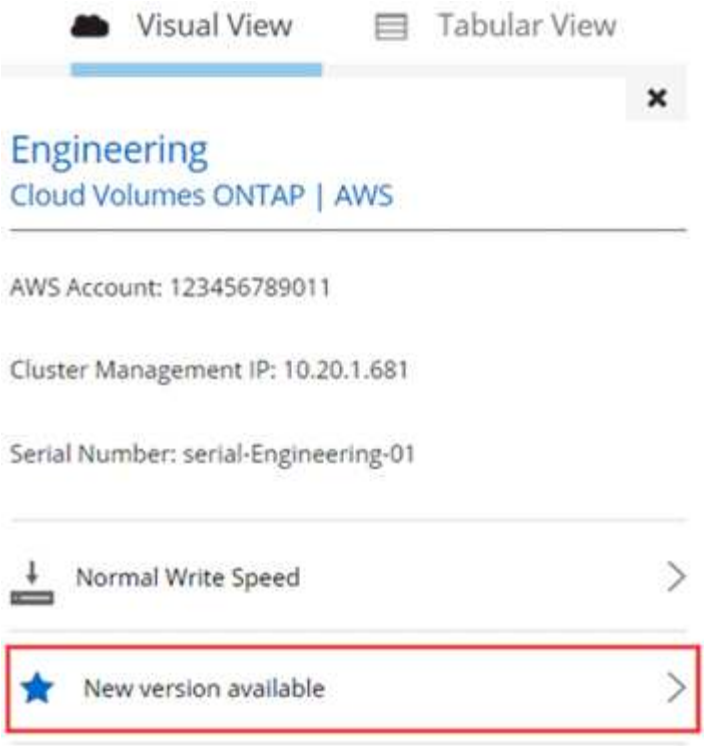
```
Password: ********
COT2::>
```

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.

Panoramica

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 alla versione più recente.

> Per i sistemi ha, 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
- 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.

Gli aggiornamenti delle coppie ha non sono disgregativi. Un upgrade senza interruzioni aggiorna contemporaneamente entrambi i nodi di una coppia ha mantenendo il servizio 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".

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

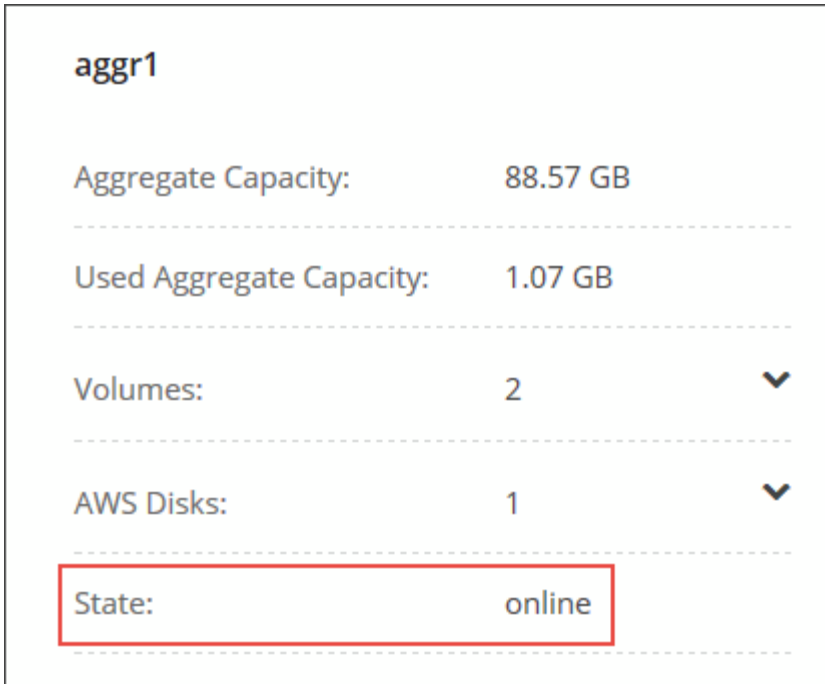
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

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 alla versione più recente

Puoi eseguire l'aggiornamento alla versione più recente di Cloud Volumes ONTAP direttamente da Cloud Manager. Cloud Manager ti avvisa quando è disponibile una nuova versione.

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.

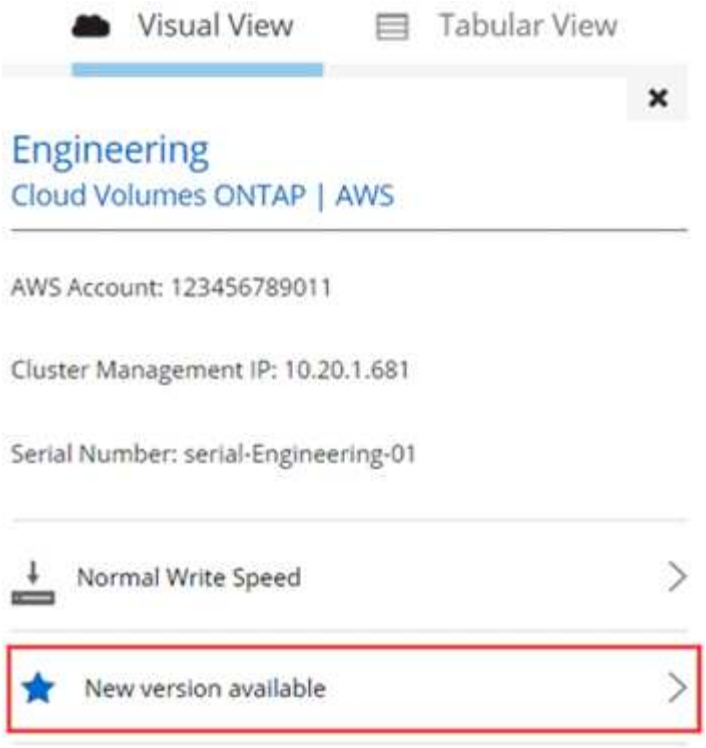
A proposito di questa attività

- 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.
- Gli aggiornamenti delle coppie ha non sono disgregativi. Un upgrade senza interruzioni aggiorna contemporaneamente entrambi i nodi di una coppia ha mantenendo il servizio ai client.

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.

A proposito di questa attività

- 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.
- Gli aggiornamenti delle coppie ha non sono disgregativi. Un upgrade senza interruzioni aggiorna contemporaneamente entrambi i nodi di una coppia ha mantenendo il servizio ai client.

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 al VPC, 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 in AWS.
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. Il processo richiede che il sistema Cloud Volumes ONTAP non sia in linea per un massimo di 25 minuti.

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.

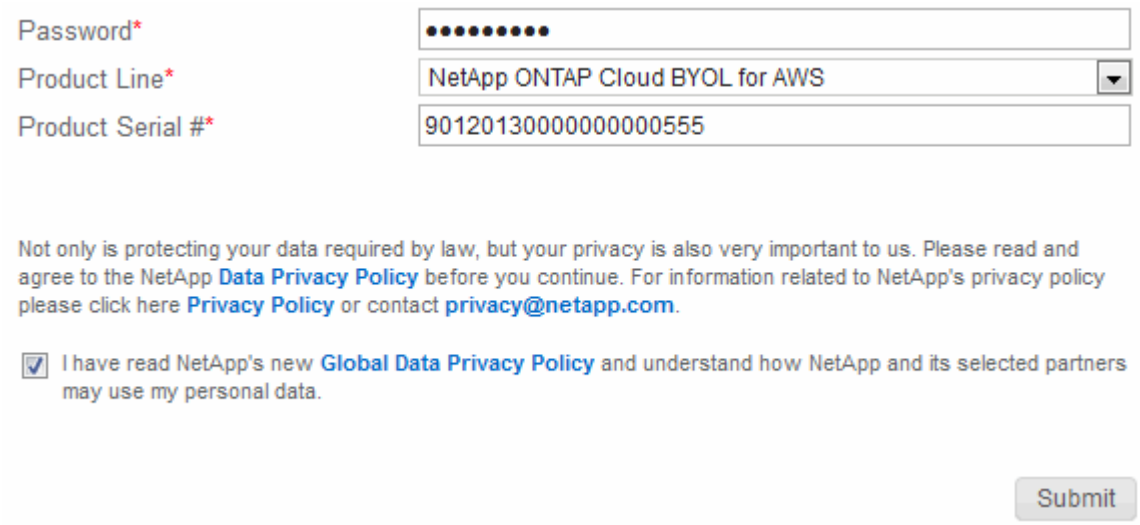
Installazione dei file di licenza sui sistemi Cloud Volumes ONTAP BYOL

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

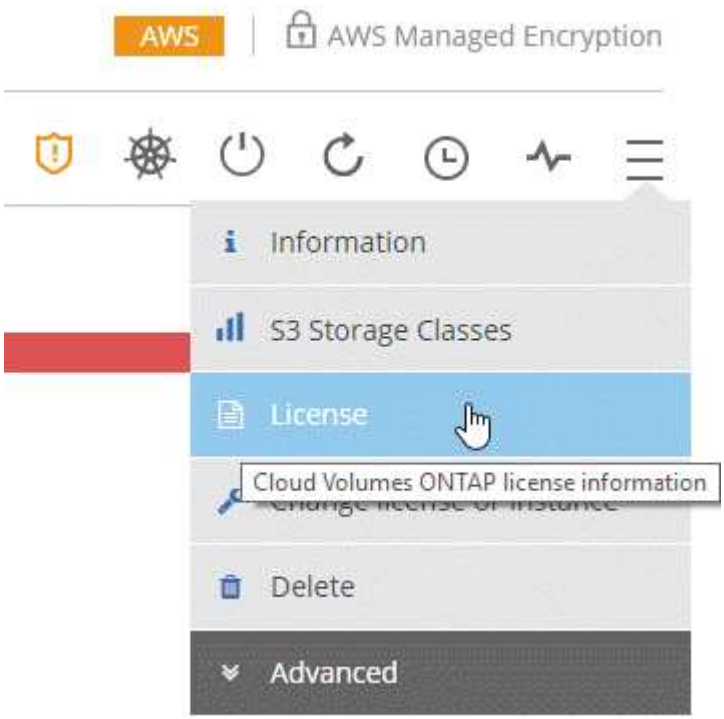
1. Accedere alla "NetApp License file Generator" Ed effettua l'accesso utilizzando le credenziali del sito di supporto NetApp.
2. Inserire la password, scegliere il prodotto (**NetApp Cloud Volumes ONTAP BYOL per AWS**, **NetApp Cloud Volumes ONTAP BYOL per Azure** o **NetApp Cloud Volumes ONTAP BYOL ha per AWS**), 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 virtuale per Cloud Volumes ONTAP

È possibile scegliere tra diversi tipi di istanze o macchine virtuali quando si avvia Cloud Volumes ONTAP in AWS o Azure. È possibile modificare il tipo di istanza o macchina virtuale in qualsiasi momento se si determina che è sottodimensionato o sovradimensionato per le proprie esigenze.

A proposito di questa attività

- 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 del tipo di istanza o macchina virtuale influisce sui costi del servizio AWS o Azure.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS (Cambia licenza o istanza) o su **Change License or VM** for Azure (Cambia licenza o macchina virtuale* per Azure).
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 virtuale, 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 EC2 o tipi di macchine virtuali Azure.

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 del tipo di istanza o macchina virtuale influisce sui costi del servizio AWS o Azure.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS (Cambia licenza o istanza) o su **Change License or VM** for Azure (Cambia licenza o macchina virtuale* per Azure).
2. Selezionare un tipo di licenza e un tipo di istanza o di macchina virtuale, 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 virtuale 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"

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".

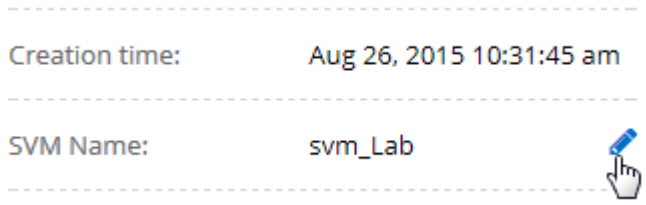
Modifica del nome della macchina virtuale di storage

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.

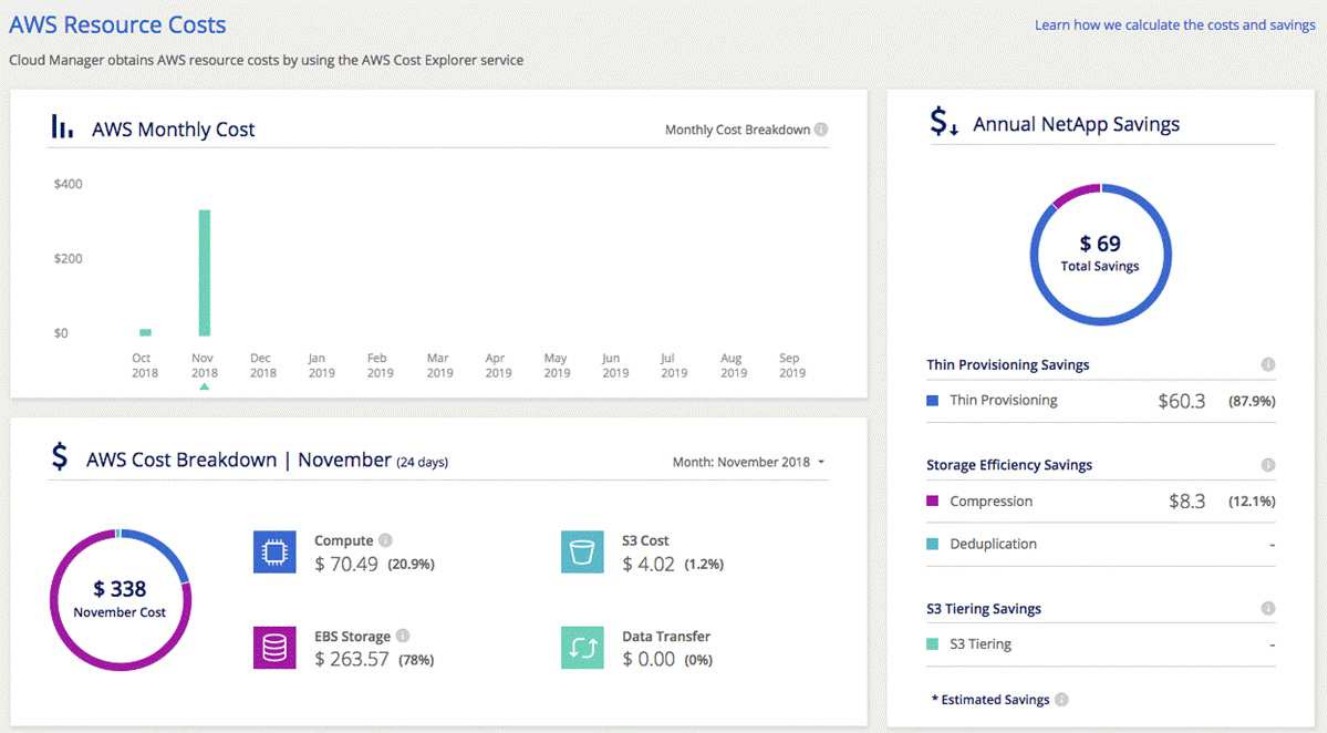
   b. "Attivare il tag **WorkingEnvironmentId**".

   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:

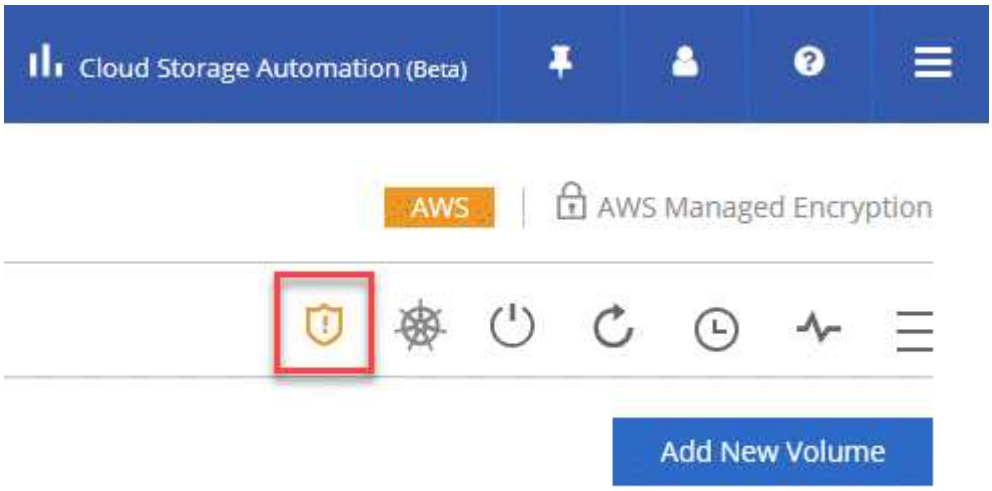


Miglioramento della protezione contro ransomware

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**.

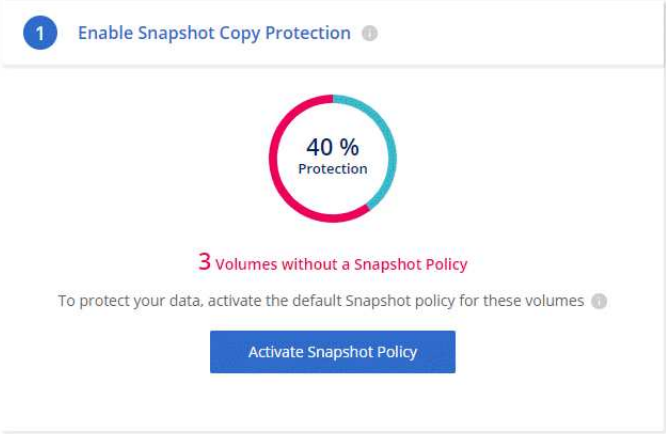


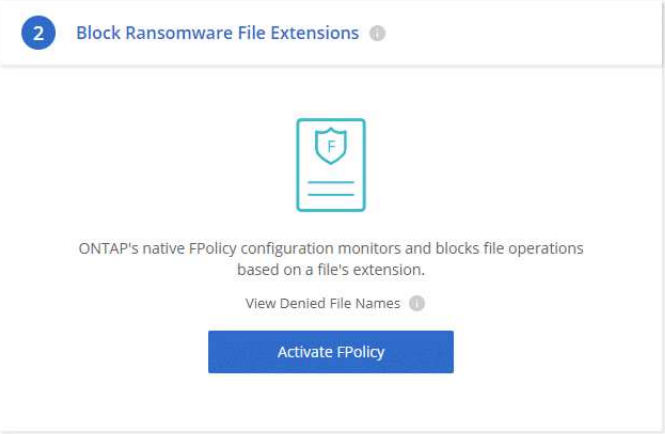
2. Implementare la soluzione NetApp per ransomware:
   a. Fare clic su **Activate Snapshot Policy** (attiva policy Snapshot) se si dispone di volumi che non hanno una policy Snapshot attivata.

      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. Questa operazione potrebbe essere eseguita se il sistema Cloud Manager è diventato inutilizzabile e si è avviato un nuovo sistema, ma non è stato possibile ripristinare tutti i sistemi Cloud Volumes ONTAP da un backup recente di 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 **Aggiungi ambiente di lavoro**.
2. In Discover (rileva), selezionare **Cloud Volumes ONTAP**.

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 al tenant.

Eliminazione di un ambiente di lavoro Cloud Volumes ONTAP

Si consiglia di eliminare i sistemi Cloud Volumes ONTAP da Cloud Manager, piuttosto che da AWS o Azure. 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.

Amministrazione di 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'elenco a discesa delle attività, quindi selezionare **Impostazioni**.
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

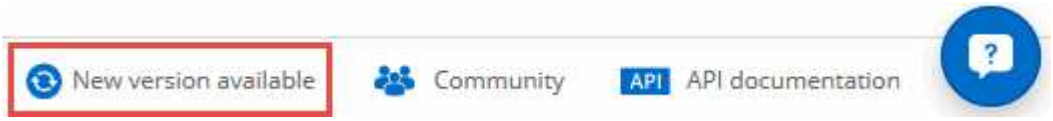
Dovresti aver esaminato "novità della release" identificare nuovi requisiti e modifiche nel supporto.

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**:
   a. Mantieni l'opzione di scaricare un backup perché puoi utilizzarlo per ripristinare la configurazione di

Cloud Manager, se necessario.

b. Leggere i termini e le condizioni, quindi selezionare la casella di controllo **ho letto e approvato i termini e le condizioni (EULA)**.

6. Quando richiesto, salvare il backup di Cloud Manager.

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. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Aggiorna**.
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**:
   a. Mantieni l'opzione per scaricare un backup abilitato perché puoi utilizzarlo per ripristinare la configurazione di Cloud Manager, se necessario.
   b. Leggere i termini e le condizioni, quindi selezionare la casella di controllo **ho letto e approvato i termini e le condizioni (EULA)**.
4. Selezionare la patch fornita.
5. Quando richiesto, salvare il backup di Cloud Manager.

Risultato

Cloud Manager applica la patch. È possibile accedere alla console dopo alcuni minuti.

Backup e ripristino di Cloud Manager

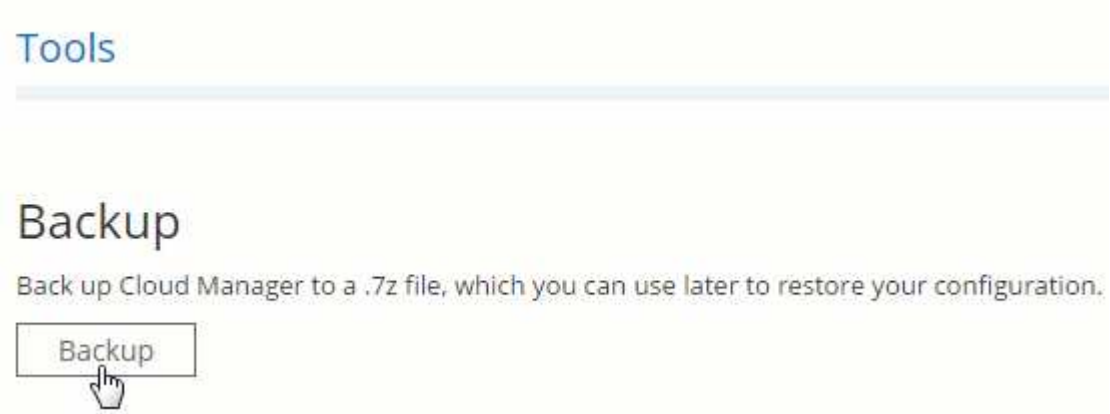
Cloud Manager consente di eseguire il backup e il ripristino del database per proteggere la configurazione e risolvere i problemi.

Backup di Cloud Manager

È buona norma eseguire il backup periodico del database Cloud Manager. In caso di problemi, è possibile ripristinare Cloud Manager da un backup precedente.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Strumenti**.
2. Fare clic su **Backup**.



3. Quando richiesto, salvare il file di backup in una posizione sicura in modo da poterlo recuperare quando necessario.

Ripristino di Cloud Manager da un backup

Il ripristino di Cloud Manager da un backup sostituisce i dati esistenti con quelli del backup.

Fasi

1. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Strumenti**.
2. Fare clic su **Restore** (Ripristina).
3. Fare clic su **OK** per confermare.
4. Selezionare il backup.

Risultato

Cloud Manager ripristina il database dal file di backup.

Rimozione degli ambienti di lavoro Cloud Volumes ONTAP

L'amministratore di Cloud Manager 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 tenant
- Riscoprilo da un altro sistema Cloud Manager
- Riscoprirla se si sono verificati problemi durante il rilevamento iniziale

Fasi

1. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi 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.

Modifica degli account utente

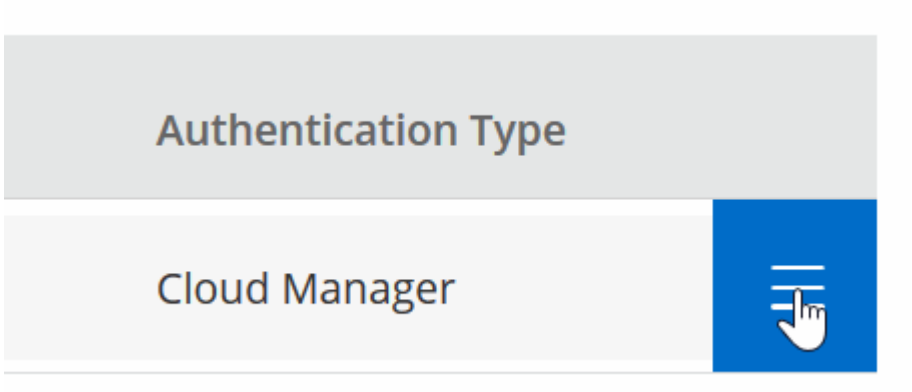
Puoi modificare gli account utente in Cloud Manager attivando e disattivando il report di notifica.

A proposito di questa attività

La password e le informazioni dell'utente devono essere modificate in "NetApp Cloud Central".

Fasi

1. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'icona dell'utente, quindi selezionare **View Users** (Visualizza utenti).
2. Selezionare l'icona del menu alla fine della riga e fare clic su **Edit User** (Modifica utente).



3. Nella pagina User Settings (Impostazioni utente), modificare l'account utente.

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. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Impostazioni**.
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'elenco a discesa delle attività, quindi selezionare **HTTPS Setup**.

   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.

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. Se si intende reinstallare Cloud Manager, eseguire il backup del database prima di disinstallare il software:
   a. Nell'angolo in alto a destra della console di Cloud Manager, fare clic sull'elenco a discesa delle attività, quindi selezionare **Strumenti**.

b. Fare clic su **Backup** e salvare il file di backup sul computer locale.

2. Eseguire lo script di disinstallazione dall'host Linux:

   /opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]

   silent esegue lo script senza richiedere conferma.

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

Durante l'aggiornamento a Cloud Manager 3.5, 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 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

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
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
			CIFS)	strutture di Active Directory	
	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

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.

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

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

Servizio	Protocollo	Porta	Destinazione	Scopo
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
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 in entrata per sistemi a nodo singolo

Priorità	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
1000	inbound_ssh	22	TCP	Qualsiasi	Qualsiasi	Consentire	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	Qualsiasi	Consentire	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	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
1003	inbound_111_udp	111	UDP	Qualsiasi	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
1004	inbound_139	139	TCP	Qualsiasi	Qualsiasi	Consentire	Sessione del servizio NetBIOS per CIFS
1005	inbound_161-162 _tcp	161-162	TCP	Qualsiasi	Qualsiasi	Consentire	Protocollo di gestione di rete semplice
1006	inbound_161-162 _udp	161-162	UDP	Qualsiasi	Qualsiasi	Consentire	Protocollo di gestione di rete semplice
1007	inbound_443	443	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1008	inbound_445	445	TCP	Qualsiasi	Qualsiasi	Consentire	Microsoft SMB/CIFS su TCP con frame NetBIOS

Priorità	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
1009	inbound_635_tcp	635	TCP	Qualsiasi	Qualsiasi	Consentire	Montaggio NFS
1010	inbound_635_udp	635	TCP	Qualsiasi	Qualsiasi	Consentire	Montaggio NFS
1011	inbound_749	749	TCP	Qualsiasi	Qualsiasi	Consentire	Kerberos
1012	inbound_2049_tcp	2049	TCP	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
1013	inbound_2049_udp	2049	UDP	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
1014	inbound_3260	3260	TCP	Qualsiasi	Qualsiasi	Consentire	Accesso iSCSI tramite LIF dei dati iSCSI
1015	inbound_4045-4046_tcp	4045-4046	TCP	Qualsiasi	Qualsiasi	Consentire	NFS lock daemon e network status monitor
1016	inbound_4045-4046_udp	4045-4046	UDP	Qualsiasi	Qualsiasi	Consentire	NFS lock daemon e network status monitor
1017	inbound_10000	10000	TCP	Qualsiasi	Qualsiasi	Consentire	Backup con NDMP
1018	inbound_11104-11105	11104-11105	TCP	Qualsiasi	Qualsiasi	Consentire	Trasferimento dei dati SnapMirror
3000	inbound_deny _all_tcp	Qualsiasi	TCP	Qualsiasi	Qualsiasi	Negare	Blocca tutto il traffico TCP in entrata
3001	inbound_deny _all_udp	Qualsiasi	UDP	Qualsiasi	Qualsiasi	Negare	Blocca tutto il traffico UDP in entrata
65000	AllowVnetInBound	Qualsiasi	Qualsiasi	VirtualNetwork	VirtualNetwork	Consentire	Traffico in entrata dall'interno di VNET
65001	AllowAzureLoad BalancerInBound	Qualsiasi	Qualsiasi	AzureLoadBalancer	Qualsiasi	Consentire	Traffico di dati dal bilanciamento del carico standard di Azure
65500	DenyAllInBound	Qualsiasi	Qualsiasi	Qualsiasi	Qualsiasi	Negare	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

> 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	Nome	Porta	Protocollo	Origine	Destinazione	Azione	Descrizione
100	inbound_443	443	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101	inbound_111_tcp	111	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Chiamata a procedura remota per NFS
102	inbound_2049_tcp	2049	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Daemon del server NFS
111	inbound_ssh	22	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121	inbound_53	53	Qualsiasi	Qualsiasi	Qualsiasi	Consentire	DNS e CIFS
65000	AllowVnetInBound	Qualsiasi	Qualsiasi	VirtualNetwork	VirtualNetwork	Consentire	Traffico in entrata dall'interno di VNET
65001	AllowAzureLoad BalancerInBound	Qualsiasi	Qualsiasi	AzureLoadBalancer	Qualsiasi	Consentire	Traffico di dati dal bilanciamento del carico standard di Azure
65500	DenyAllInBound	Qualsiasi	Qualsiasi	Qualsiasi	Qualsiasi	Negare	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.

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 Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory					
188					

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
			CIFS)	strutture di Active Directory	
	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)
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
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

Autorizzazioni AWS e Azure per Cloud Manager

Cloud Manager richiede autorizzazioni per eseguire azioni in AWS e Azure per conto dell'utente. 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.
"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.

Azioni	Scopo
"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.
"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.
"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.

Azioni	Scopo
"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.
"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.

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 da AWS Marketplace o Azure Marketplace), tieni presente quanto segue:
  - In AWS, il nome utente per l'istanza EC2 Linux è ec2-user.
  - Per AWS e Azure, 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 e come coppia ha in AWS e Azure.
- Cloud Manager crea una SVM per il servizio dei dati quando implementa Cloud Volumes ONTAP. Anche se è possibile creare un'altra SVM per la gestione dei dati da System Manager o CLI, l'utilizzo di più SVM per la gestione dei dati non è supportato.
- Per impostazione predefinita, vengono create diverse interfacce di rete:

- Una LIF di gestione del cluster
- Un LIF intercluster
- 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 di Cloud Manager può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno
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

- Un disco SSD IOPS con provisioning per i dati di avvio Cloud Volumes ONTAP, che è di circa 45 GB e 1,250 PIOPS
- Un disco SSD General Purpose per i dati root Cloud Volumes ONTAP, che è di circa 140 GB
- Un'istantanea EBS per ogni disco di boot e disco root

In una coppia ha, entrambi i nodi Cloud Volumes ONTAP replicano il proprio disco root nel nodo partner.

Azure

- Un disco SSD Premium Storage per i dati di avvio Cloud Volumes ONTAP, pari a circa 73 GB
- Un disco SSD Premium Storage per i dati root Cloud Volumes ONTAP, pari a circa 140 GB
- Uno snapshot Azure per ogni disco di boot e disco root

Dove risiedono i dischi

Cloud Manager definisce lo storage di AWS e Azure come segue:

- I dati di avvio risiedono su un disco collegato all'istanza EC2 o alla macchina virtuale Azure.

  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.

Ruoli utente

A ciascun account utente di Cloud Manager viene assegnato un ruolo che definisce le autorizzazioni.

Attività	Amministratore di Cloud Manager	Amministratore tenant	Amministratore dell'ambiente di lavoro
Gestire i tenant	Sì	No	No
Gestire gli ambienti di lavoro	Sì	Sì, per il tenant assegnato	Sì, per ambienti di lavoro assegnati
Integra un ambiente di lavoro con Cloud Sync	Sì	Sì	No
Visualizzare lo stato della replica dei dati	Sì	Sì, per il tenant assegnato	Sì, per ambienti di lavoro assegnati
Visualizza la timeline	Sì	Sì	Sì
Creare ed eliminare gli account utente	Sì	Sì, per il tenant assegnato	No
Modificare gli account utente	Sì	Sì, per il tenant assegnato	Sì, per il proprio account

Attività	Amministratore di Cloud Manager	Amministratore tenant	Amministratore dell'ambiente di lavoro
Gestire le impostazioni dell'account	Sì	No	No
Configurare Kubernetes	Sì	No	No
Passare dalla visualizzazione del sistema di storage a quella del volume	Sì	No	No
Modificare le impostazioni	Sì	No	No
Visualizza e gestisci la dashboard di supporto	Sì	No	No
Backup e ripristino di Cloud Manager	Sì	No	No
Rimuovere un ambiente di lavoro	Sì	No	No
Aggiorna Cloud Manager	Sì	No	No
Installare un certificato HTTPS	Sì	No	No
Configurare Active Directory	Sì	No	No
Attiva il Cloud Storage Automation Report	Sì	No	No

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 in AWS e Azure 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 AWS e Azure.

- "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"
- 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"
- "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.

- "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.

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 OnCommand Cloud Manager 3.6.6"
- "Avviso per OnCommand Cloud Manager 3.6.1"
- "Avviso per OnCommand Cloud Manager 3.6"