Cloud Manager e documentazione Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

Sommario

Cloud Manager e documentazione Cloud Volumes ONTAP

Cloud Manager consente agli esperti IT e agli architetti del cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud di NetApp.

BlueXP

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

"Consulta la documentazione BlueXP"

Scopri le novità

- "Modifiche importanti in Cloud Manager"
- "Novità di Cloud Manager"
- "Novità di Cloud Volumes ONTAP"

Inizia subito

- "Cloud Manager"
- "Impostazioni dell'account"
- "Cloud Volumes ONTAP per AWS"
- "Cloud Volumes ONTAP per Azure"
- "Cloud Volumes ONTAP per Google Cloud"
- "Azure NetApp Files"
- "Cloud Volumes Service per AWS"
- "Cloud Volumes Service per Google Cloud"
- "Conformità al cloud"
- "Global file cache"
- "Backup su cloud"
- "Cloud Insights"

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 3.8

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

Cerchi una release precedente?"Novità del 3.7"
"Novità del 3.6"
"Novità del 3.5"

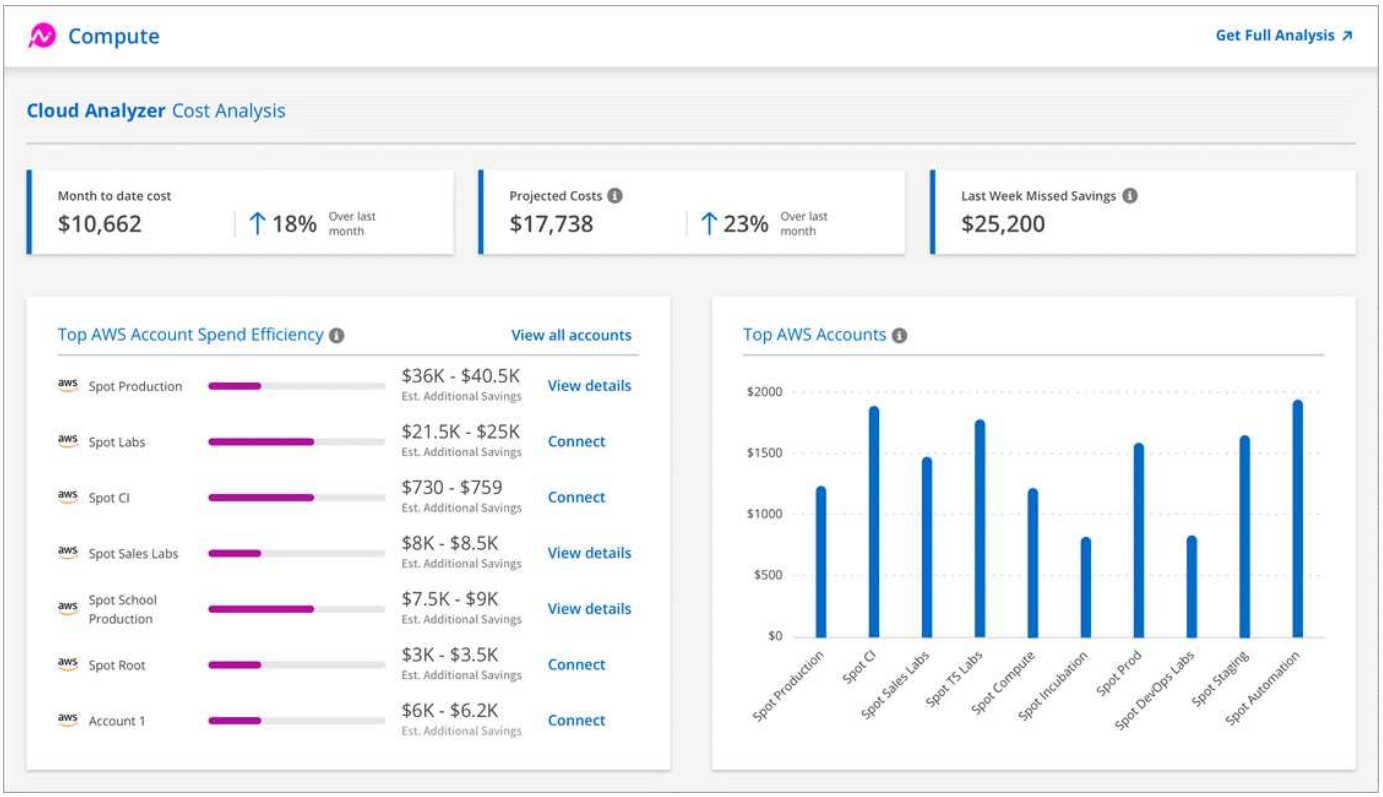
Nuovo provider Terraform (19 ottobre 2020)

Abbiamo sviluppato un nuovo provider di terraform che i team DevOps possono utilizzare con Cloud Manager per automatizzare e integrare Cloud Volumes ONTAP con l'infrastruttura come codice.

"Visualizza il provider netapp-cloud manager".

Aggiornamento di Cloud Manager 3.8.9 (18 ottobre 2020)

Sfruttando "Spot's Cloud Analyzer", Cloud Manager può ora fornire un'analisi dei costi di alto livello delle spese di calcolo del cloud e identificare i potenziali risparmi. Queste informazioni sono disponibili nel servizio **Compute** di Cloud Manager. "Scopri di più".



Aggiornamento di Cloud Manager 3.8.9 (13 ottobre 2020)

Abbiamo rilasciato due aggiornamenti di Cloud Tiering:

- Le licenze per il Cloud Tiering sono ora disponibili in Cloud Manager.

  Paga il tiering dei dati da un cluster ONTAP on-premise al cloud attraverso un abbonamento pay-as-you-go, una licenza di tiering ONTAP denominata *FabricPool* o una combinazione di entrambi.

- Il servizio standalone di Cloud Tiering è stato ritirato. Ora dovresti accedere al Cloud Tiering direttamente da Cloud Manager, dove sono disponibili tutte le stesse funzionalità.

Cloud Manager 3.8.9 (4 ottobre 2020)

- Miglioramenti della conformità al cloud
- Miglioramenti di Cloud Volumes Service per AWS
- Integrazione di Cloud Sync
- Miglioramenti alla gestione degli account
- Modifiche per le regioni governative

Miglioramenti della conformità al cloud

- In Cloud Manager è disponibile un nuovo ruolo **Cloud Compliance Viewer**.

  Gli utenti a cui è stato assegnato questo ruolo possono visualizzare solo le informazioni di conformità e generare report per le aree di lavoro a cui sono autorizzati ad accedere. Non possono gestire le impostazioni di conformità del cloud e non possono accedere ad altre funzionalità e servizi di Cloud Manager. Questo potrebbe essere il ruolo perfetto per il tuo team legale, in modo che possa monitorare i risultati della scansione Cloud Compliance. Vedere "ruoli utente" per ulteriori informazioni.

- Aggiunto supporto per la scansione degli schemi di database MongoDB e PostgreSQL. Vedere "scansione degli schemi del database" per ulteriori informazioni.
- I prezzi per la conformità al cloud stanno cambiando a partire dal 7 ottobre.

  I primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Sono inclusi i dati provenienti da volumi Cloud Volumes ONTAP, volumi Azure NetApp Files, bucket Amazon S3 e schemi di database. È necessario un abbonamento per eseguire la scansione di eventuali dati aggiuntivi dopo aver raggiunto 1 TB. Vedere "prezzi" per ulteriori informazioni.

Miglioramenti di Cloud Volumes Service per AWS

Quando si crea un nuovo volume, è possibile scegliere di basarlo su una copia Snapshot esistente di un altro volume.

Integrazione di Cloud Sync

Il servizio Cloud Sync di NetApp è ora disponibile all'interno di Cloud Manager. Cloud Sync offre un metodo semplice, sicuro e automatizzato per migrare i dati da qualsiasi destinazione di origine a qualsiasi destinazione di destinazione, nel cloud o on-premise. "Scopri di più".

Miglioramenti alla gestione degli account

Abbiamo aggiunto altri modi per gestire il tuo account.

- È ora disponibile una panoramica delle risorse del tuo account.

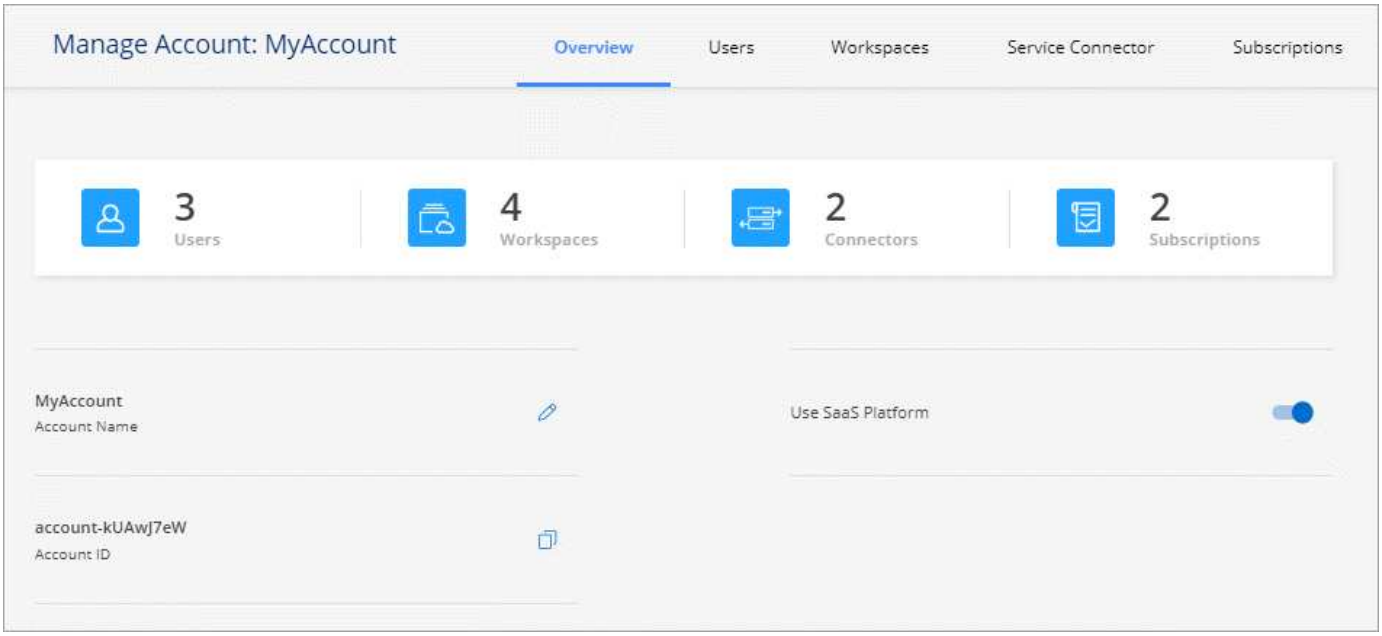
  È possibile visualizzare rapidamente il numero di utenti, aree di lavoro, connettori e sottoscrizioni nel proprio account.

- È possibile modificare il nome dell'account.
- È possibile copiare l'ID account, l'ID area di lavoro o l'ID connettore.

  La copia di questi ID aiuterà con le funzionalità di automazione che stiamo pianificando.

- È possibile disattivare l'utilizzo della piattaforma SaaS.

  Si consiglia di non disattivare la piattaforma SaaS a meno che non sia necessario per rispettare le policy di sicurezza della propria azienda. La disattivazione della piattaforma SaaS limita la tua capacità di utilizzare i servizi cloud integrati di NetApp. "Scopri di più".



Modifiche per le regioni governative

Se si implementa un connettore in un'area AWS GovCloud, Azure Gov o Azure DoD, l'accesso a Cloud Manager è ora disponibile solo tramite l'indirizzo IP host di un connettore. L'accesso alla piattaforma SaaS è disattivato per l'intero account.

Ciò significa che solo gli utenti con privilegi che possono accedere al VPC/VNET interno dell'utente finale possono utilizzare l'interfaccia utente o l'API di Cloud Manager.

"Scopri di più su questo limite".

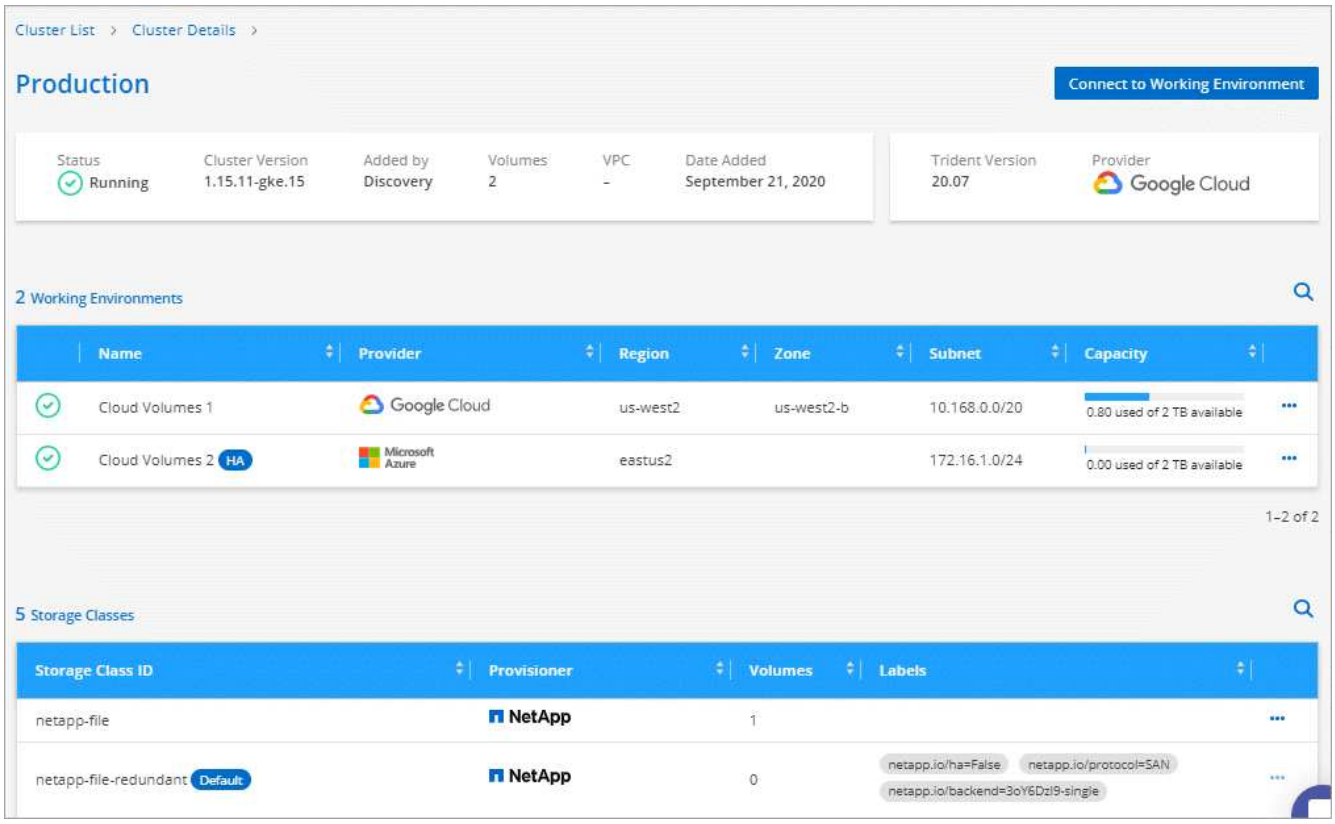
Aggiornamento di Cloud Manager 3.8.8 (22 settembre 2020)

Abbiamo migliorato il servizio Kubernetes per semplificarne l'utilizzo e fornire funzionalità aggiuntive:

- Abbiamo semplificato la scoperta dei cluster Kubernetes in esecuzione nel servizio Kubernetes gestito dal tuo cloud provider.

  Basta fare clic su **Discover Clusters** e Cloud Manager rileverà i cluster gestiti utilizzando le autorizzazioni del provider cloud già fornite.

- È ora possibile visualizzare ulteriori informazioni su un cluster Kubernetes scoperto, tra cui lo stato, il numero di volumi, le classi di storage e altro ancora.



- Abbiamo aggiunto il controllo delle risorse e degli errori per garantire la disponibilità della comunicazione tra il cluster e Cloud Volumes ONTAP. Se non lo è, ti faremo sapere.

"Scopri come iniziare".

Si noti che l'account di servizio per un connettore richiede le seguenti autorizzazioni per rilevare e gestire i cluster Kubernetes in esecuzione in Google Kubernetes Engine (GKE):

```
- container.*
```

Aggiornamento di Cloud Manager 3.8.8 (10 settembre 2020)

I seguenti miglioramenti sono disponibili quando si implementa Global file cache tramite Cloud Manager:

- Una coppia Cloud Volumes ONTAP ha in AWS è ora supportata come piattaforma di storage back-end per lo storage centrale.
- È possibile implementare più istanze Global file cache Core in un progetto Load Distributed.

"Scopri di più su Global file cache".

Cloud Manager 3.8.8 (9 settembre 2020)

- Supporto per Cloud Volumes Service per Google Cloud
- Backup su cloud ora supporta cluster ONTAP on-premise
- Miglioramenti del backup su cloud
- Miglioramenti della conformità al cloud
- Navigazione aggiornata
- Miglioramenti dell'amministrazione

Supporto per Cloud Volumes Service per Google Cloud

- Aggiungere un ambiente di lavoro per gestire i volumi Cloud Volumes Service per GCP esistenti e creare nuovi volumi. "Scopri come".
- Creare e gestire volumi NFSv3 e NFSv4.1 per client Linux e UNIX e volumi SMB 3.x per client Windows.
- Creare, eliminare e ripristinare le snapshot dei volumi.

Backup su cloud ora supporta cluster ONTAP on-premise

Avvia il backup dei dati dai sistemi ONTAP on-premise al cloud. Abilita Backup su cloud negli ambienti di lavoro on-premise per eseguire il backup dei volumi nello storage Azure Blob. "Scopri di più".

Miglioramenti del backup su cloud

Abbiamo rivisto l'interfaccia utente per una migliore usabilità:

- Pagina dell'elenco dei volumi per visualizzare facilmente i volumi di cui viene eseguito il backup insieme ai backup disponibili
- Pagina delle impostazioni di backup per visualizzare le impostazioni di backup per ciascun ambiente di lavoro

Miglioramenti della conformità al cloud

- Possibilità di eseguire la scansione dei dati dai database

  Eseguire la scansione dei database per identificare i dati personali e sensibili presenti in ogni schema. I database supportati includono Oracle, SAP HANA e SQL Server (MSSQL). "Scopri di più sulla scansione dei database".

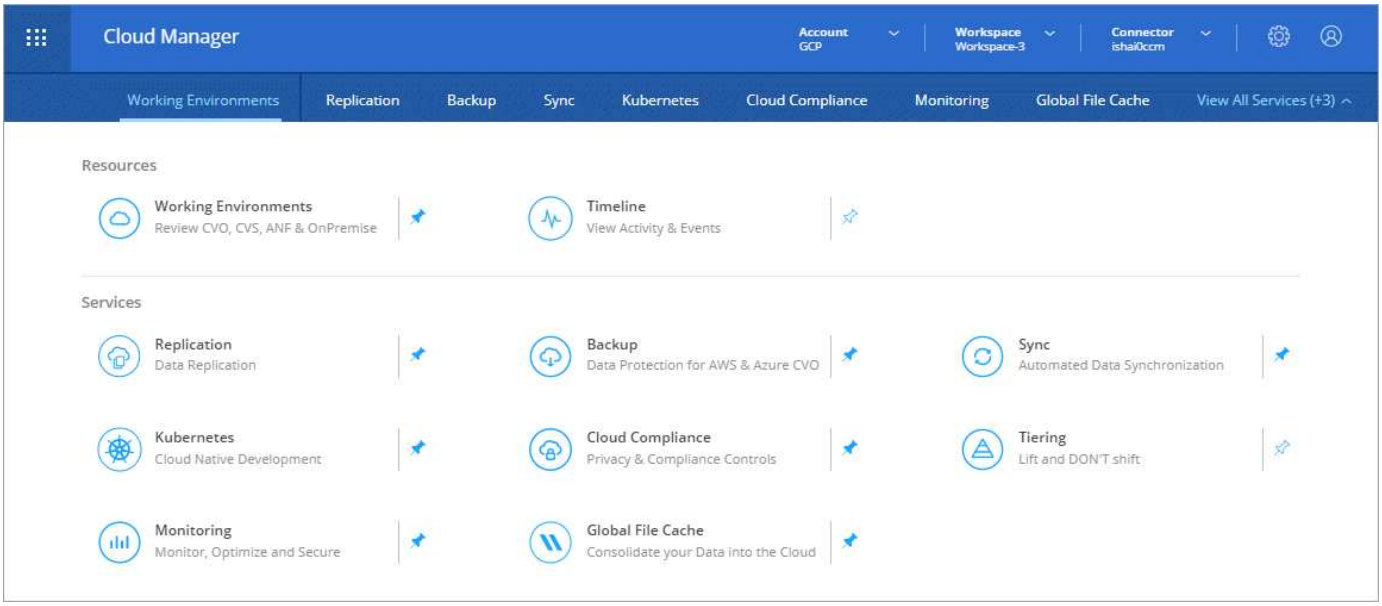
- Possibilità di eseguire la scansione di volumi DP (Data Protection)

  I volumi DP sono volumi di destinazione delle operazioni SnapMirror, in genere dei cluster ONTAP on-premise. Ora puoi identificare facilmente i dati personali e sensibili che risiedono in questi file on-premise. "Scopri come".

Navigazione aggiornata

Abbiamo aggiornato l'intestazione in Cloud Manager per semplificare la navigazione tra i servizi cloud di NetApp.

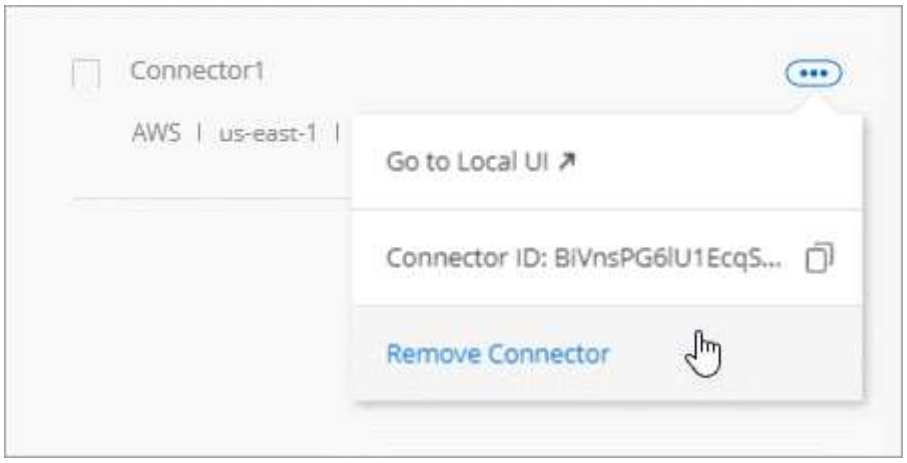
Fare clic su **View All Services** (Visualizza tutti i servizi) per aggiungere e rimuovere i servizi che si desidera visualizzare nella navigazione.



Come puoi vedere, abbiamo anche aggiornato i menu a discesa account, Workspace e Connector, in modo da semplificare la visualizzazione delle selezioni correnti.

Miglioramenti dell'amministrazione

- Ora puoi rimuovere i connettori inattivi da Cloud Manager. "Scopri come".



- Ora puoi sostituire l'abbonamento Marketplace attualmente associato alle credenziali del tuo cloud provider. Se hai bisogno di modificare l'addebito, questa modifica può aiutarti a assicurarti di ricevere l'addebito tramite l'abbonamento corretto a Marketplace.

  Scopri come "In AWS", "In Azure", e. "In GCP".

Aggiornamento delle autorizzazioni Azure richieste (6 agosto 2020)

Per evitare errori di implementazione di Azure, assicurati che la tua policy di Cloud Manager in Azure includa la seguente autorizzazione:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

Azure ora richiede questa autorizzazione per alcune implementazioni di macchine virtuali (dipende dall'hardware fisico sottostante utilizzato durante l'implementazione).

"Visualizza l'ultima policy di Cloud Manager per Azure".

Cloud Manager 3.8.7 (3 agosto 2020)

- Nuova esperienza software-as-a-service
- Miglioramenti di Cloud Volumes ONTAP
- Miglioramenti di Azure NetApp Files
- Miglioramenti di Cloud Volumes Service per AWS
- Miglioramenti della conformità al cloud
- Miglioramenti del backup su cloud
- Supporto per Global file cache

Nuova esperienza software-as-a-service

Abbiamo introdotto un'esperienza software-as-a-service per Cloud Manager. Questa nuova esperienza semplifica l'utilizzo di Cloud Manager e ci consente di fornire funzionalità aggiuntive per la gestione della tua infrastruttura di cloud ibrido.

Cloud Manager include un "Interfaccia basata su SaaS" Integrato con NetApp Cloud Central e connettori che consentono a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. (Il connettore è in realtà lo stesso del software Cloud Manager esistente installato).

Nella maggior parte dei casi è necessario un connettore, ma non è necessario utilizzare Azure NetApp Files, Cloud Volumes Service o Cloud Sync da Cloud Manager.

Come indicato in precedenza in queste note di rilascio, sarà necessario aggiornare il tipo di computer per i connettori per accedere alle nuove funzionalità che offriamo. Cloud Manager richiede di modificare il tipo di macchina. "Scopri di più".

Miglioramenti di Cloud Volumes ONTAP

Sono disponibili due miglioramenti per Cloud Volumes ONTAP.

- **Licenze BYOL multiple per allocare capacità aggiuntiva**

  È ora possibile acquistare più licenze per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TB di capacità. Ad esempio, è possibile acquistare due licenze per allocare fino a 736 TB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare quattro licenze per ottenere fino a 1.4 PB.

  Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia ha è illimitato.

  Tenere presente che i limiti dei dischi possono impedire di raggiungere il limite di capacità utilizzando solo i dischi. È possibile superare il limite di dischi di "tiering dei dati inattivi sullo storage a oggetti". Per informazioni sui limiti dei dischi, fare riferimento a. "Limiti di storage nelle note di rilascio di Cloud Volumes ONTAP".

  "Scopri come aggiungere una nuova licenza di sistema".

- **Crittografa i dischi gestiti da Azure utilizzando chiavi esterne**

È ora possibile crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. Questa funzionalità è supportata tramite API.

È sufficiente aggiungere quanto segue alla richiesta API quando si crea il sistema a nodo singolo:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

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

```
"Microsoft.Compute/diskEncryptionSets/read"
```

Miglioramenti di Azure NetApp Files

Questa versione include diversi miglioramenti nel supporto di Azure NetApp Files.

- **Configurazione Azure NetApp Files**

  Ora puoi configurare e gestire Azure NetApp Files direttamente da Cloud Manager. "Scopri come".

- **Nuovo supporto del protocollo**

  È ora possibile creare volumi NFSv4.1 e volumi SMB.

- **Gestione dello snapshot del volume e del pool di capacità**

  Cloud Manager consente di creare, eliminare e ripristinare snapshot di volumi. È inoltre possibile creare nuovi pool di capacità e specificarne i livelli di servizio.

- **Possibilità di modificare i volumi**

  È possibile modificare un volume modificandone le dimensioni e gestendo i tag.

Miglioramenti di Cloud Volumes Service per AWS

In Cloud Manager sono stati apportati numerosi miglioramenti a supporto di Cloud Volumes Service per AWS.

- **Nuovo supporto del protocollo**

  Ora è possibile creare volumi NFSv4.1, volumi SMB e volumi a doppio protocollo. In precedenza era possibile creare e scoprire volumi NFSv3 solo in Cloud Manager.

- **Supporto Snapshot**

  È possibile creare policy di snapshot per automatizzare la creazione di snapshot di volumi, creare uno snapshot on-demand, ripristinare un volume da uno snapshot, creare un nuovo volume in base a uno snapshot esistente e molto altro ancora. Vedere "Gestione delle snapshot dei volumi cloud" per ulteriori informazioni.

- **Creare il volume iniziale in una regione da Cloud Manager**

  Prima di questa release, era necessario creare il primo volume in ciascuna regione nell'interfaccia Cloud Volumes Service per AWS. Ora puoi iscriverti a. "Una delle offerte NetApp Cloud Volumes Service sul marketplace AWS" Quindi creare il primo volume da Cloud Manager.

Miglioramenti della conformità al cloud

I seguenti miglioramenti sono ora disponibili per la conformità cloud.

- **Processo di implementazione rivisto per la tua istanza di Cloud Compliance**

  L'istanza di Cloud Compliance viene configurata e implementata utilizzando una nuova procedura guidata in Cloud Manager. Una volta completata l'implementazione, attivare il servizio per ogni ambiente di lavoro che si desidera sottoporre a scansione.

- **Possibilità di selezionare i volumi da sottoporre a scansione in un ambiente di lavoro**

  Ora è possibile attivare e disattivare la scansione di singoli volumi in un ambiente di lavoro Cloud Volumes ONTAP o Azure NetApp Files. Se non è necessario eseguire la scansione di determinati volumi per verificarne la conformità, disattivarli.

  "Scopri di più sulla disattivazione della scansione per volumi."

- **Schede di navigazione per passare rapidamente alla tua area di interesse**

  Le nuove schede per Dashboard, Investigation e Configuration consentono di accedere più facilmente a queste sezioni.

- **Report HIPAA**

  È ora disponibile un nuovo report HIPAA (Health Insurance Portability and Accountability Act). Il presente report è stato progettato per aiutare l'organizzazione a rispettare le leggi sulla privacy dei dati HIPAA.

  "Scopri di più sul report HIPAA."

- **Nuovo tipo di dati personali sensibili**

  Cloud Compliance può ora trovare i codici medici ICD-9-CM nei file.

- **Nuovo tipo di dati personali**

  Cloud Compliance può ora trovare due nuovi identificatori nazionali nei file: Croatian ID (OIB) e Greek ID.

Miglioramenti del backup su cloud

I seguenti miglioramenti sono ora disponibili per il backup nel cloud.

- **La licenza BYOL (Bring Your Own License) è ora disponibile**

  Backup su cloud è disponibile solo con una licenza Pay as You Go (PAYGO). Una licenza BYOL consente di acquistare una licenza da NetApp per utilizzare Backup to Cloud per un determinato periodo di tempo e per una quantità massima di spazio di backup. Una volta raggiunto il limite, è necessario rinnovare la licenza.

"Scopri di più sulla nuova licenza BYOL per il backup nel cloud."

- **Supporto per volumi DP (Data Protection)**

  Ora è possibile eseguire il backup e il ripristino dei volumi di protezione dei dati.

Supporto per Global file cache

NetApp Global file cache consente di consolidare silos di file server distribuiti in un unico footprint di storage globale e coerente nel cloud pubblico. In questo modo si crea un file system accessibile a livello globale nel cloud che tutte le ubicazioni distribuite possono utilizzare come se fossero locali.

A partire da questa release, l'istanza Global file cache Management e l'istanza Core possono essere implementate e gestite tramite Cloud Manager. Ciò consente di risparmiare molte ore durante il processo di implementazione iniziale e offre un singolo pannello di controllo tramite Cloud Manager per questo e altri sistemi implementati. Le istanze di Global file cache Edge vengono ancora implementate localmente presso le sedi remote.

Vedere "Panoramica della Global file cache" per ulteriori informazioni.

La configurazione iniziale che può essere implementata utilizzando Cloud Manager deve soddisfare i seguenti requisiti. Altre configurazioni come Cloud Volumes Service, Azure NetApp Files e Cloud Volumes Service per AWS e GCP continuano a essere implementate utilizzando le procedure legacy. "Scopri di più".

- La piattaforma di storage back-end utilizzata come storage centrale deve essere un ambiente operativo in cui è stata implementata una coppia di Cloud Volumes ONTAP ha in Azure.

  Altre piattaforme storage e altri cloud provider non sono attualmente supportati con Cloud Manager, ma possono essere implementati utilizzando procedure di implementazione legacy.

- Il core GFC può essere implementato solo come istanza autonoma.

  Se è necessario utilizzare una progettazione distribuita con carico che include più istanze Core, è necessario utilizzare le procedure legacy.

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

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Un'esperienza migliore richiede un tipo di macchina più potente (15 luglio 2020)

Mentre miglioriamo l'esperienza di Cloud Manager, dovrai aggiornare il tuo tipo di computer per accedere alle

nuove funzionalità che offriremo. I miglioramenti includeranno un "Esperienza software-as-a-service per Cloud Manager" e integrazioni di servizi cloud nuove e migliorate.

Cloud Manager richiede di modificare il tipo di macchina.

Ecco alcuni dettagli:

1. Per garantire la disponibilità di risorse adeguate per la corretta funzionalità delle nuove funzionalità di Cloud Manager, abbiamo modificato l'istanza predefinita, la macchina virtuale e il tipo di macchina come segue:
   - AWS: t3.xlarge
   - Azure: DS3 v2
   - GCP: n1-standard-4

   Questi formati predefiniti sono quelli minimi supportati "In base ai requisiti di CPU e RAM".
2. Nell'ambito di questa transizione, Cloud Manager richiede l'accesso al seguente endpoint per ottenere immagini software dei componenti container per un'infrastruttura Docker:

   https://cloudmanagerinfraprod.azurecr.io

   Assicurati che il firewall consenta l'accesso a questo endpoint da Cloud Manager.

Cloud Manager 3.8.6 (6 luglio 2020)

- Supporto per volumi iSCSI
- Supporto per la policy di tiering completo

Supporto per volumi iSCSI

Cloud Manager consente ora di creare volumi iSCSI per cluster Cloud Volumes ONTAP e ONTAP on-premise direttamente dall'interfaccia utente.

Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.

Supporto per la policy di tiering completo

È ora possibile scegliere il criterio di tutti i livelli quando si crea o si modifica un volume per Cloud Volumes ONTAP. Quando si utilizza la policy di tiering completo, i dati vengono immediatamente contrassegnati come cold e tiered per lo storage a oggetti il più presto possibile. "Scopri di più sul tiering dei dati".

Transizione di Cloud Manager a SaaS (22 giugno 2020)

Stiamo introducendo un'esperienza software-as-a-service per Cloud Manager. Questa nuova esperienza semplifica l'utilizzo di Cloud Manager e ci consente di fornire funzionalità aggiuntive per la gestione della tua infrastruttura di cloud ibrido. "Scopri di più".

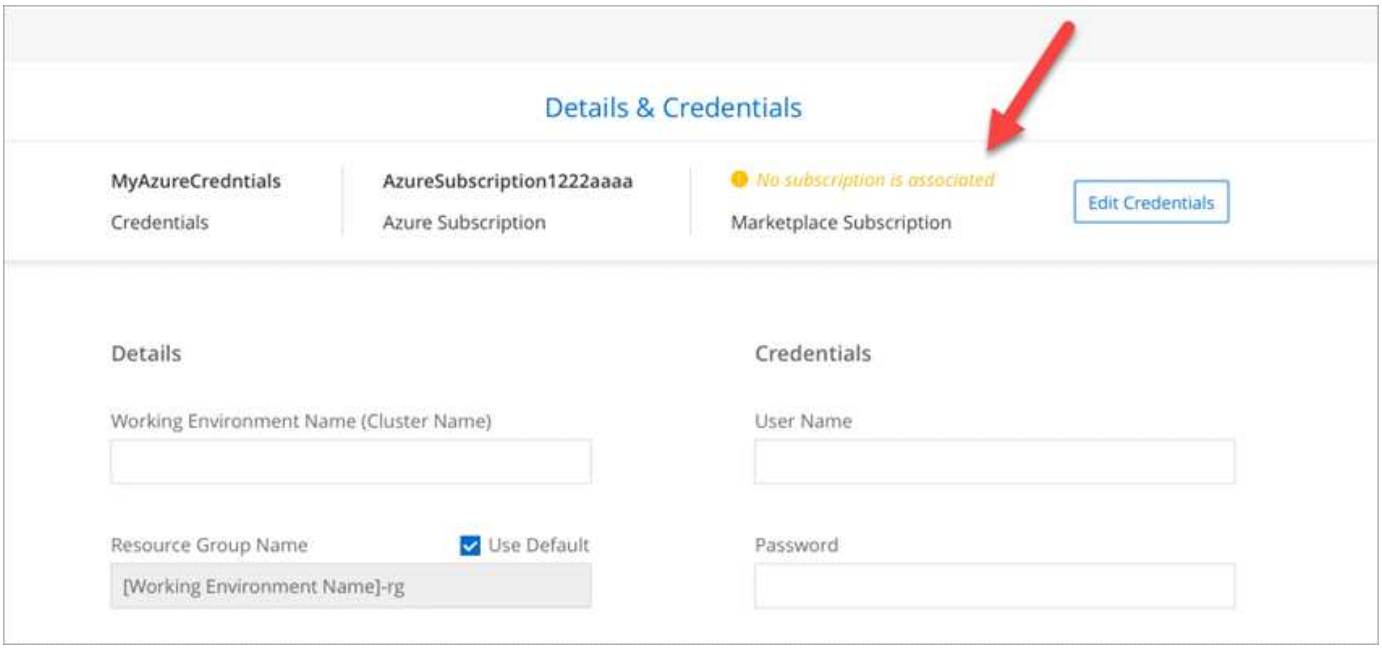
Cloud Manager 3.8.5 (31 maggio 2020)

- È richiesto un nuovo abbonamento in Azure Marketplace
- Miglioramenti del backup su cloud
- Miglioramenti della conformità al cloud

È richiesto un nuovo abbonamento in Azure Marketplace

Un nuovo abbonamento è disponibile in Azure Marketplace. Questo abbonamento una tantum è necessario per implementare Cloud Volumes ONTAP 9.7 PAYGO (ad eccezione del sistema in prova gratuita per 30 giorni). L'abbonamento ci consente inoltre di offrire funzionalità aggiuntive per Cloud Volumes ONTAP PAYGO e BYOL. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP creato e di ogni funzione aggiuntiva abilitata.

Cloud Manager ti chiederà di iscriverti a questa offerta al momento dell'implementazione di un nuovo sistema Cloud Volumes ONTAP (9.7 P1 o successivo).



Miglioramenti del backup su cloud

I seguenti miglioramenti sono ora disponibili per il backup nel cloud.

- In Azure, è ora possibile creare un nuovo gruppo di risorse o selezionare un gruppo di risorse esistente invece di fare in modo che Cloud Manager ne crei uno per te. Non è possibile modificare il gruppo di risorse dopo aver attivato Backup su cloud.
- In AWS, è ora possibile eseguire il backup delle istanze di Cloud Volumes ONTAP che risiedono su un account AWS diverso rispetto all'account AWS di Cloud Manager.
- Sono ora disponibili opzioni aggiuntive quando si seleziona la pianificazione di backup per i volumi. Oltre alle opzioni di backup giornaliere, settimanali e mensili, è ora possibile selezionare una delle policy definite dal sistema che fornisce policy di combinazione come 30 backup giornalieri, 13 settimanali e 12 mensili.
- Dopo aver eliminato tutti i backup di un volume, è possibile iniziare a creare nuovamente i backup per tale volume. Questo era un limite noto nella release precedente.

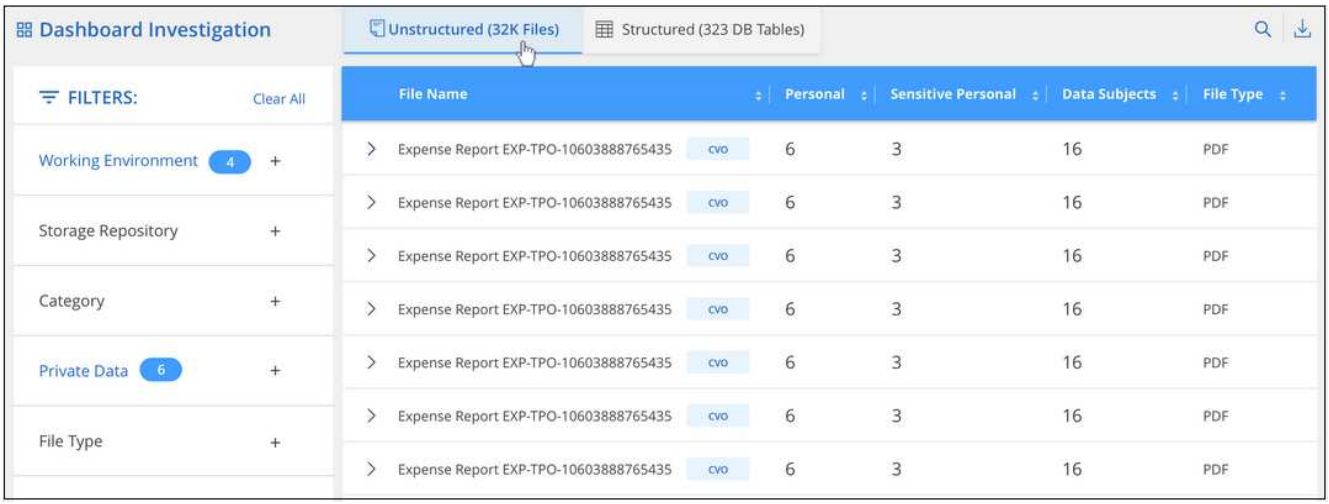
Miglioramenti della conformità al cloud

Per la conformità al cloud sono disponibili i seguenti miglioramenti.

- È ora possibile eseguire la scansione dei bucket S3 che si trovano in account AWS diversi rispetto all'istanza Cloud Compliance. Devi solo creare un ruolo sul nuovo account in modo che l'istanza esistente di Cloud Compliance possa connettersi a tali bucket. "Scopri di più".

  Se hai configurato Cloud Compliance prima della release 3.8.5, dovrai modificare la versione esistente "Ruolo IAM per l'istanza Cloud Compliance" per utilizzare questa funzionalità.

- È ora possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati che si desidera visualizzare. I filtri includono ambiente di lavoro, categoria, dati privati, tipo di file, data dell'ultima modifica, E se le autorizzazioni dell'oggetto S3 sono aperte all'accesso pubblico.



- Ora puoi attivare e disattivare Cloud Compliance in un ambiente di lavoro direttamente dalla scheda Cloud Compliance.

Aggiornamento di Cloud Manager 3.8.4 (10 maggio 2020)

Abbiamo rilasciato un miglioramento di Cloud Manager 3.8.4.

Integrazione di Cloud Insights

Sfruttando il servizio Cloud Insights di NetApp, Cloud Manager ti offre informazioni sullo stato di salute e sulle performance delle tue istanze di Cloud Volumes ONTAP e ti aiuta a risolvere i problemi e ottimizzare le performance del tuo ambiente di cloud storage. "Scopri di più".

Cloud Manager 3.8.4 (3 maggio 2020)

Cloud Manager 3.8.4 include i seguenti miglioramenti.

Miglioramenti del backup su cloud

Sono ora disponibili i seguenti miglioramenti per il backup nel cloud (precedentemente chiamato *Backup in S3* per AWS):

- **Backup su storage Azure Blob**

  Backup su cloud è ora disponibile per Cloud Volumes ONTAP in Azure. Backup su cloud offre funzionalità

di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud. "Scopri di più".

- **Eliminazione dei backup**

  Ora puoi eliminare tutti i backup di un volume specifico direttamente dall'interfaccia di Cloud Manager. "Scopri di più".

Cloud Manager 3.8.3 (5 aprile 2020)

- Integrazione del cloud tiering
- Migrazione dei dati a Azure NetApp Files
- Miglioramenti della conformità al cloud
- Miglioramenti del backup su S3
- Volumi iSCSI che utilizzano API

Integrazione del cloud tiering

Il servizio Cloud Tiering di NetApp è ora disponibile all'interno di Cloud Manager. Il tiering del cloud ti consente di tierare i dati da un cluster ONTAP on-premise a uno storage a oggetti a basso costo nel cloud. In questo modo si libera spazio di storage ad alte performance sul cluster per un maggior numero di carichi di lavoro.

"Scopri di più".

Migrazione dei dati a Azure NetApp Files

Ora puoi migrare i dati NFS o SMB su Azure NetApp Files direttamente da Cloud Manager. Le sincronizzazioni dei dati sono basate sul servizio Cloud Sync di NetApp.

"Scopri come migrare i dati su Azure NetApp Files".

Miglioramenti della conformità al cloud

I seguenti miglioramenti sono ora disponibili per la conformità cloud.

- **30 giorni di prova gratuita per Amazon S3**

  È ora disponibile una versione di prova gratuita di 30 giorni per eseguire la scansione dei dati Amazon S3 con Cloud Compliance. Se in precedenza hai abilitato Cloud Compliance su Amazon S3, la tua prova gratuita di 30 giorni è attiva a partire da oggi (5 aprile 2020).

  È necessario un abbonamento a AWS Marketplace per continuare la scansione di Amazon S3 al termine della prova gratuita. "Scopri come iscriverti".

  "Scopri i prezzi per la scansione di Amazon S3".

- **Nuovo tipo di dati personali**

  Cloud Compliance può ora trovare un nuovo identificativo nazionale nei file: Brazilian ID (CPF).

  "Scopri di più sui tipi di dati personali".

- **Supporto per ulteriori categorie di metadati**

La conformità al cloud è ora in grado di classificare i tuoi dati in nove categorie di metadati aggiuntive. "Consulta l'elenco completo delle categorie di metadati supportate".

Miglioramenti del backup su S3

Sono ora disponibili i seguenti miglioramenti per il servizio Backup in S3.

- **S3 Lifecycle policy per i backup**

  I backup iniziano con la classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.

- **Eliminazione dei backup**

  È ora possibile eliminare i backup utilizzando un'API Cloud Manager. "Scopri di più".

- **Bloccare l'accesso pubblico**

  Cloud Manager ora abilita "Funzione di accesso pubblico a blocchi Amazon S3" Nel bucket S3 in cui sono memorizzati i backup.

Volumi iSCSI che utilizzano API

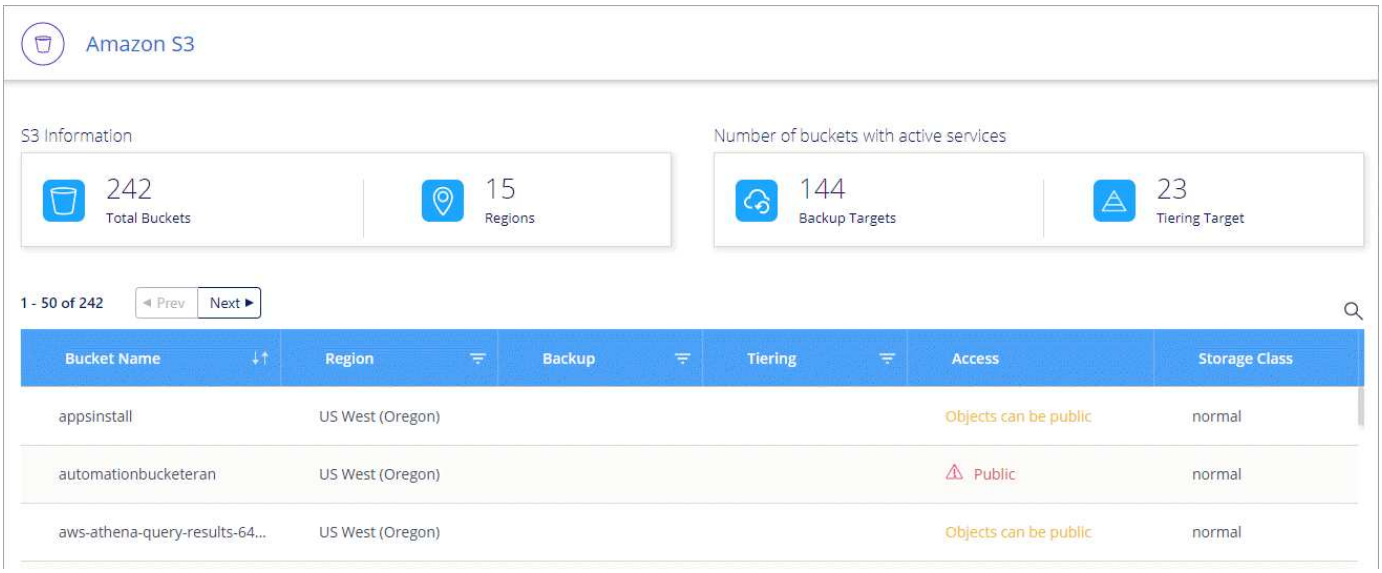
Le API Cloud Manager consentono ora di creare volumi iSCSI. "Visualizza un esempio qui".

Cloud Manager 3.8.2 (1 marzo 2020)

- Ambienti di lavoro Amazon S3
- Miglioramenti della conformità al cloud
- Versione NFS per volumi
- Supporto per le regioni Azure US Gov

Ambienti di lavoro Amazon S3

Cloud Manager ora rileva automaticamente le informazioni sui bucket Amazon S3 che risiedono nell'account AWS in cui è installato. Ciò consente di visualizzare facilmente i dettagli sui bucket S3, tra cui regione, livello di accesso, classe di storage e se il bucket viene utilizzato con Cloud Volumes ONTAP per backup o tiering dei dati. Inoltre, puoi eseguire la scansione dei bucket S3 con la conformità al cloud, come descritto di seguito.



Miglioramenti della conformità al cloud

I seguenti miglioramenti sono ora disponibili per la conformità cloud.

- **Supporto per Amazon S3**

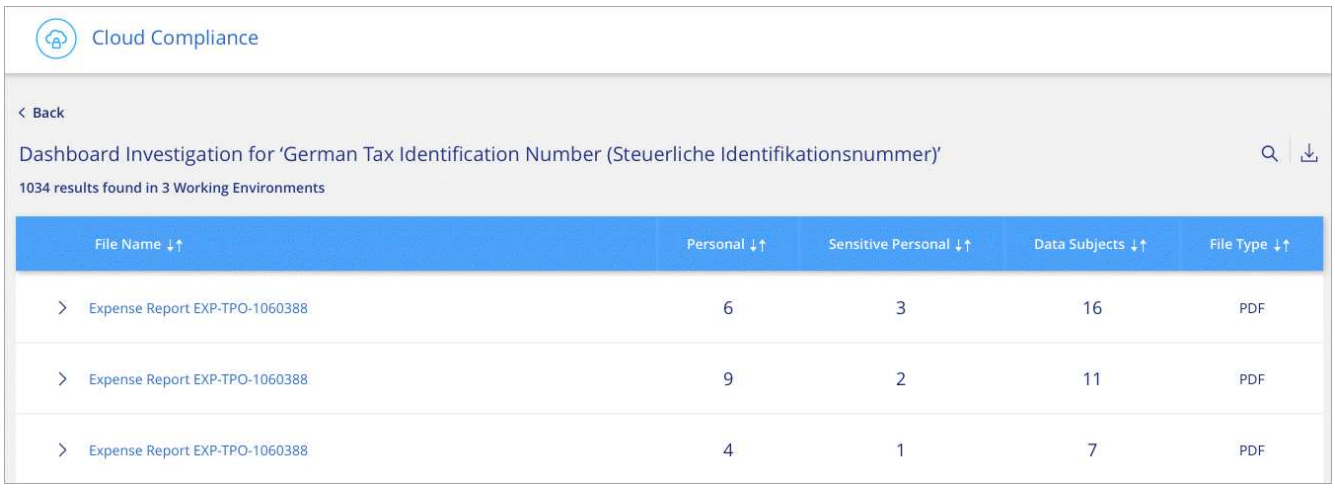
  Cloud Compliance è ora in grado di eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili che risiedono nello storage a oggetti S3. Cloud Compliance può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

  "Scopri come iniziare".

- **Pagina delle indagini**

  È ora disponibile una nuova pagina di analisi per ogni tipo di file personale, file personale sensibile, categoria e tipo di file. La pagina mostra i dettagli dei file interessati e consente di ordinare in base ai file che includono la maggior parte dei dati personali, i dati personali sensibili e i nomi degli interessati. Questa pagina sostituisce il report CSV precedentemente disponibile.

  Ecco un esempio:



  "Scopri di più sulla pagina delle indagini".

- **Report PCI DSS**

  È ora disponibile un nuovo report PCI DSS (Payment Card Industry Data Security Standard). Questo report può aiutarti a identificare la distribuzione delle informazioni sulla carta di credito nei tuoi file. È possibile visualizzare il numero di file contenenti informazioni sulla carta di credito, se gli ambienti di lavoro sono protetti da crittografia o protezione ransomware, dettagli di conservazione e altro ancora.

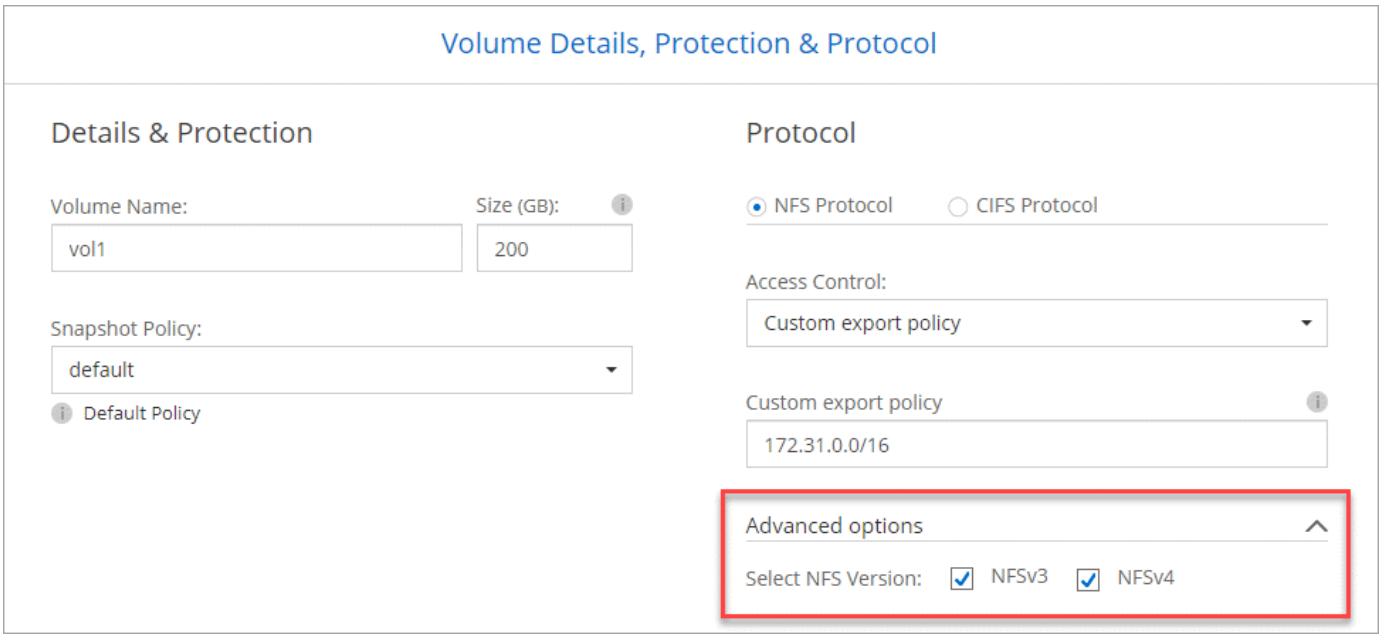
  "Scopri di più sul report PCI DSS".

- **Nuovo tipo di dati personali sensibili**

  Cloud Compliance è ora in grado di trovare i codici medici ICD-10-CM, utilizzati nel settore medico e sanitario.

Versione NFS per volumi

È ora possibile selezionare la versione di NFS da abilitare su un volume quando si crea o si modifica un volume per Cloud Volumes ONTAP.



Supporto per le regioni Azure US Gov

Le coppie Cloud Volumes ONTAP ha sono ora supportate nelle regioni Azure US Gov.

"Consulta l'elenco delle aree Azure supportate".

Aggiornamento di Cloud Manager 3.8.1 (16 febbraio 2020)

Abbiamo rilasciato alcuni miglioramenti a Cloud Manager 3.8.1.

Miglioramenti del backup su S3

- Le copie di backup sono ora memorizzate in un bucket S3 creato da Cloud Manager nel tuo account AWS, con un bucket per ogni ambiente di lavoro Cloud Volumes ONTAP.
- Il backup su S3 è ora supportato in tutte le regioni AWS "Dove è supportato Cloud Volumes ONTAP".

- È possibile impostare la pianificazione del backup su giornaliera, settimanale o mensile.
- Cloud Manager non deve più configurare *collegamenti privati* per il servizio Backup in S3.

Per questi miglioramenti sono necessarie autorizzazioni S3 aggiuntive. Il ruolo IAM che fornisce le autorizzazioni a Cloud Manager deve includere le autorizzazioni più recenti "Policy di Cloud Manager".

"Scopri di più su Backup in S3".

Aggiornamenti AWS

Abbiamo introdotto il supporto per le nuove istanze EC2 e una modifica nel numero di dischi dati supportati per Cloud Volumes ONTAP 9.6 e 9.7. Leggi le modifiche nelle note di rilascio di Cloud Volumes ONTAP.

- "Note sulla versione di Cloud Volumes ONTAP 9.7"
- "Note sulla versione di Cloud Volumes ONTAP 9.6"

Cloud Manager 3.8.1 (2 febbraio 2020)

- Miglioramenti della conformità al cloud
- Miglioramenti agli account e alle sottoscrizioni
- Miglioramenti della tempistica

Miglioramenti della conformità al cloud

I seguenti miglioramenti sono ora disponibili per la conformità cloud.

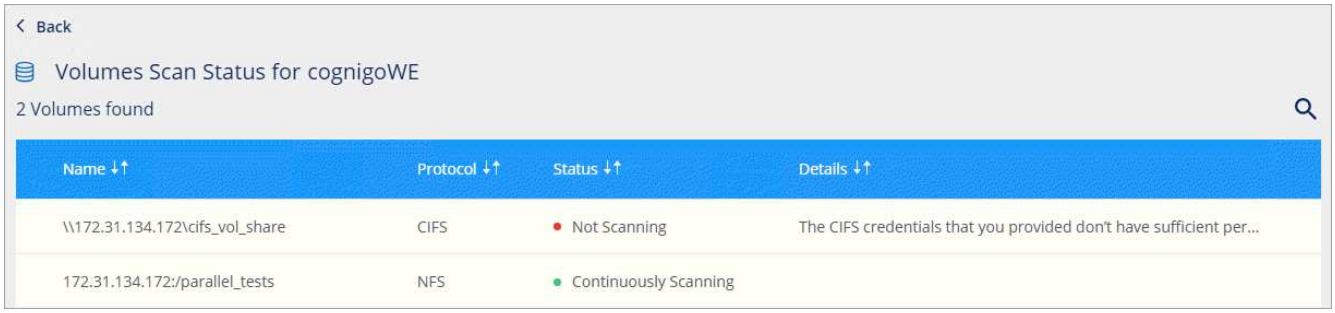
- **Supporto per Azure NetApp Files**

  Siamo lieti di annunciare che la conformità al cloud è ora in grado di eseguire la scansione di Azure NetApp Files per identificare i dati personali e sensibili che risiedono sui volumi.

  "Scopri come iniziare".

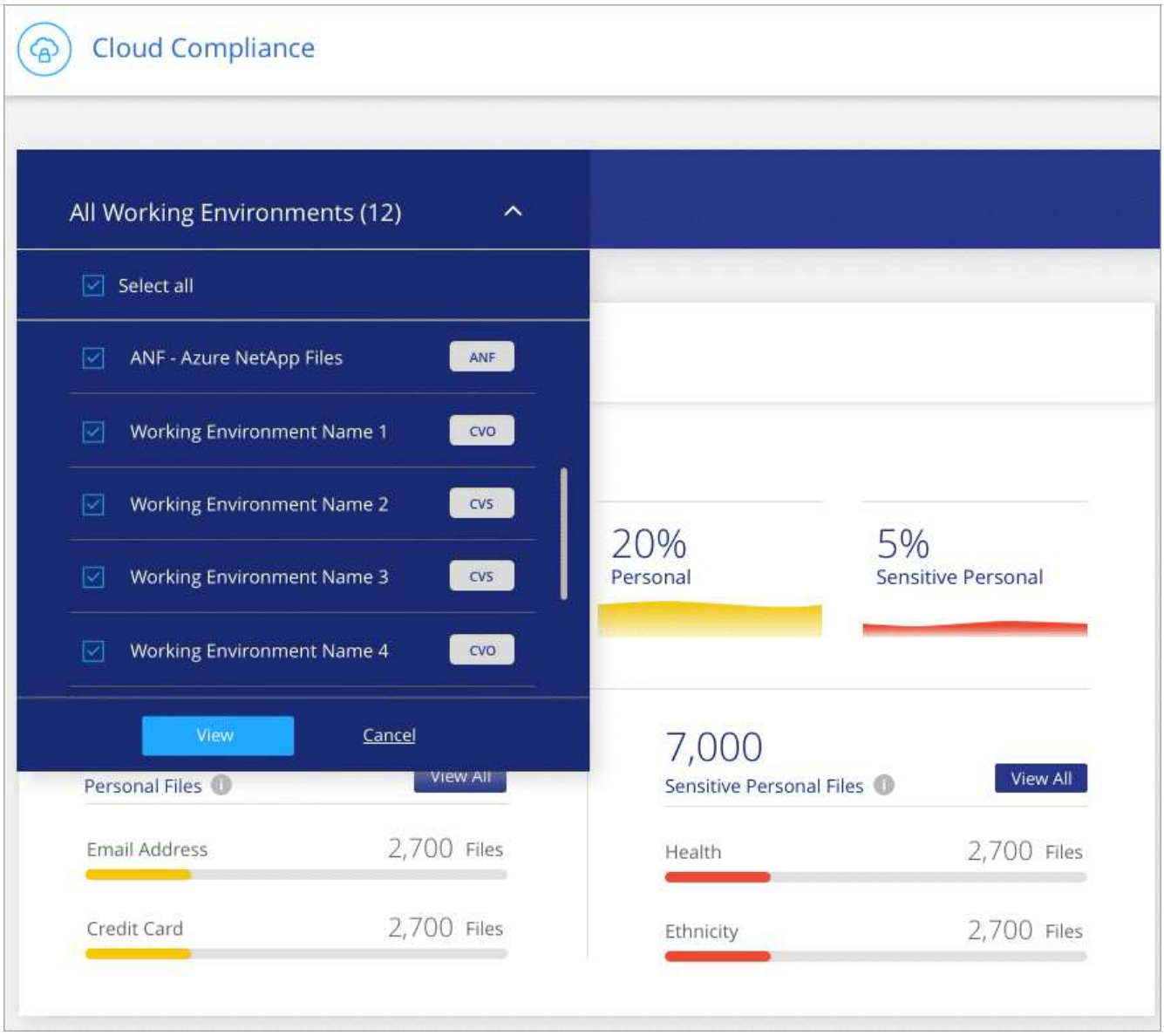
- **Stato scansione**

  Cloud Compliance mostra ora lo stato di scansione per ogni volume CIFS e NFS, inclusi i messaggi di errore che è possibile utilizzare per correggere eventuali problemi.



- **Filtra dashboard in base all'ambiente di lavoro**

  Ora puoi filtrare i contenuti della dashboard Cloud Compliance per visualizzare i dati di conformità per specifici ambienti di lavoro.



- **Nuovo tipo di dati personali**

  Cloud Compliance è ora in grado di identificare una licenza per il conducente della California durante la scansione dei dati.

- **Supporto per categorie aggiuntive**

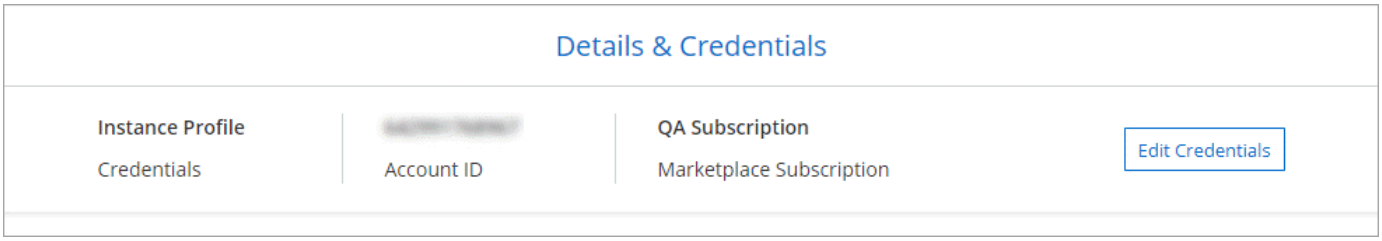
  Sono supportate tre categorie aggiuntive: Dati dell'applicazione, log, database e file di indice.

  "Scopri di più sulle categorie".

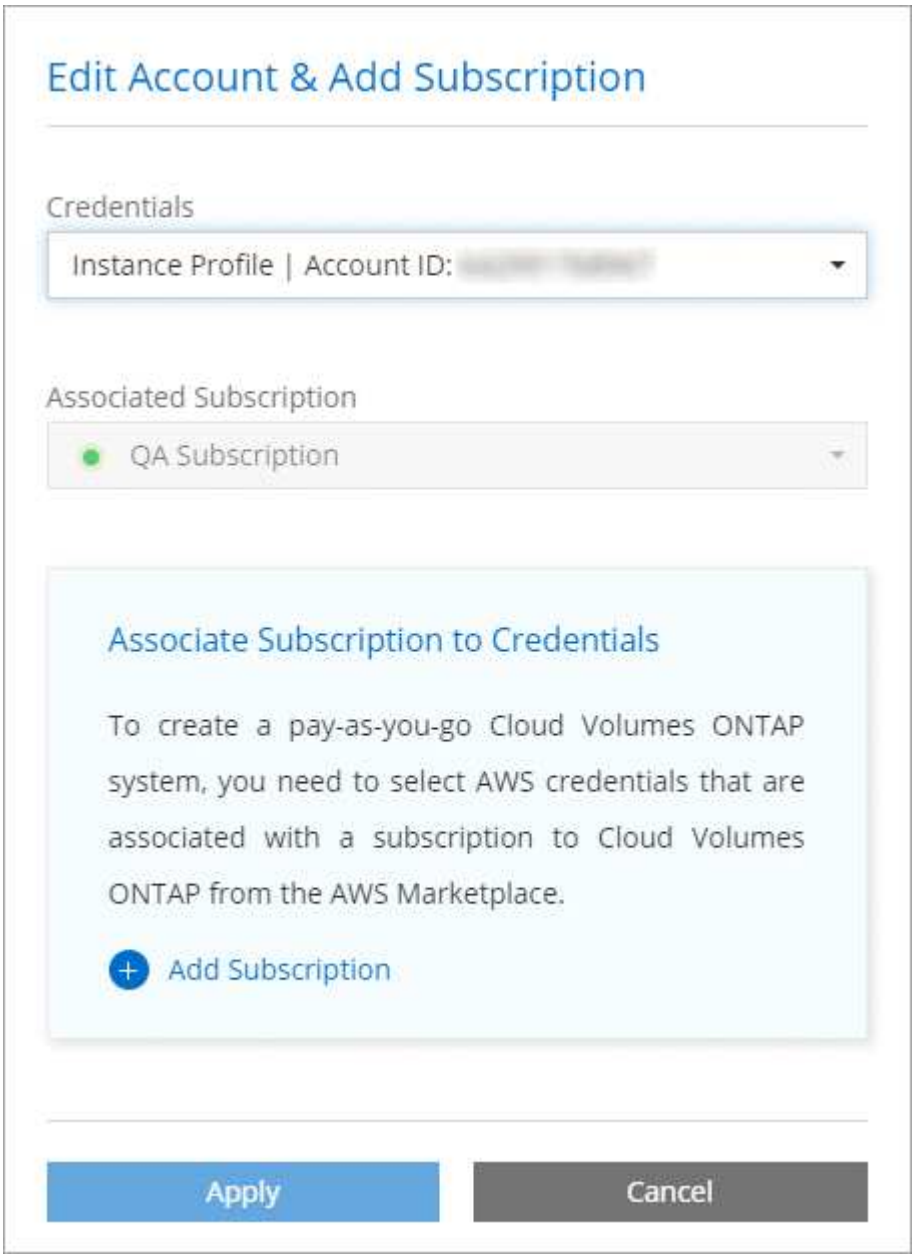
Miglioramenti agli account e alle sottoscrizioni

Abbiamo semplificato la scelta di un account AWS o di un progetto GCP e di un abbonamento al marketplace associato per un sistema Cloud Volumes ONTAP pay-as-you-go. Questi miglioramenti ti aiutano a pagare con il giusto account o progetto.

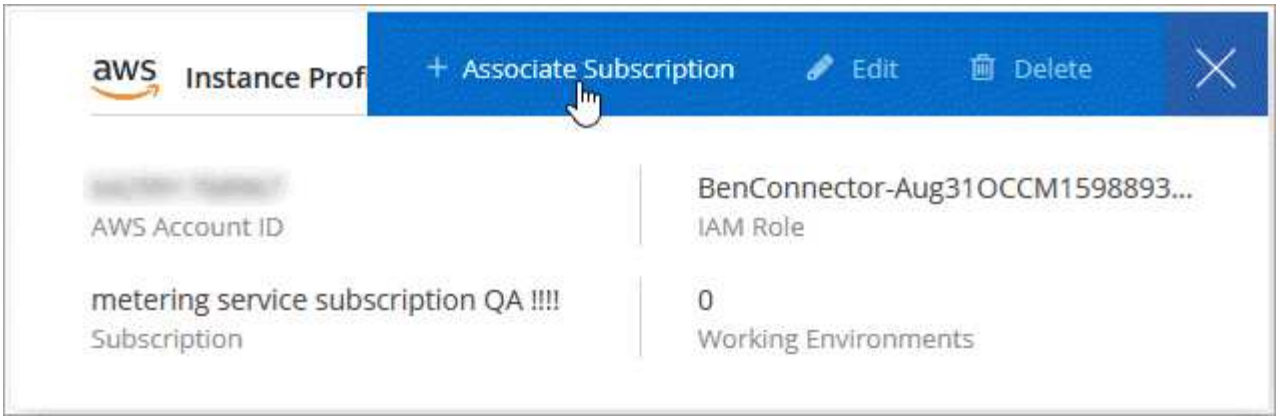
Ad esempio, quando si crea un sistema in AWS, fare clic su **Edit Credentials** (Modifica credenziali) se non si desidera utilizzare l'account e l'abbonamento predefiniti:



Da qui, è possibile scegliere le credenziali dell'account che si desidera utilizzare e l'abbonamento AWS Marketplace associato. Puoi anche aggiungere un abbonamento al marketplace, se necessario.



Inoltre, se si gestiscono più sottoscrizioni AWS, è possibile assegnarle a diverse credenziali AWS dalla pagina credenziali nelle impostazioni:

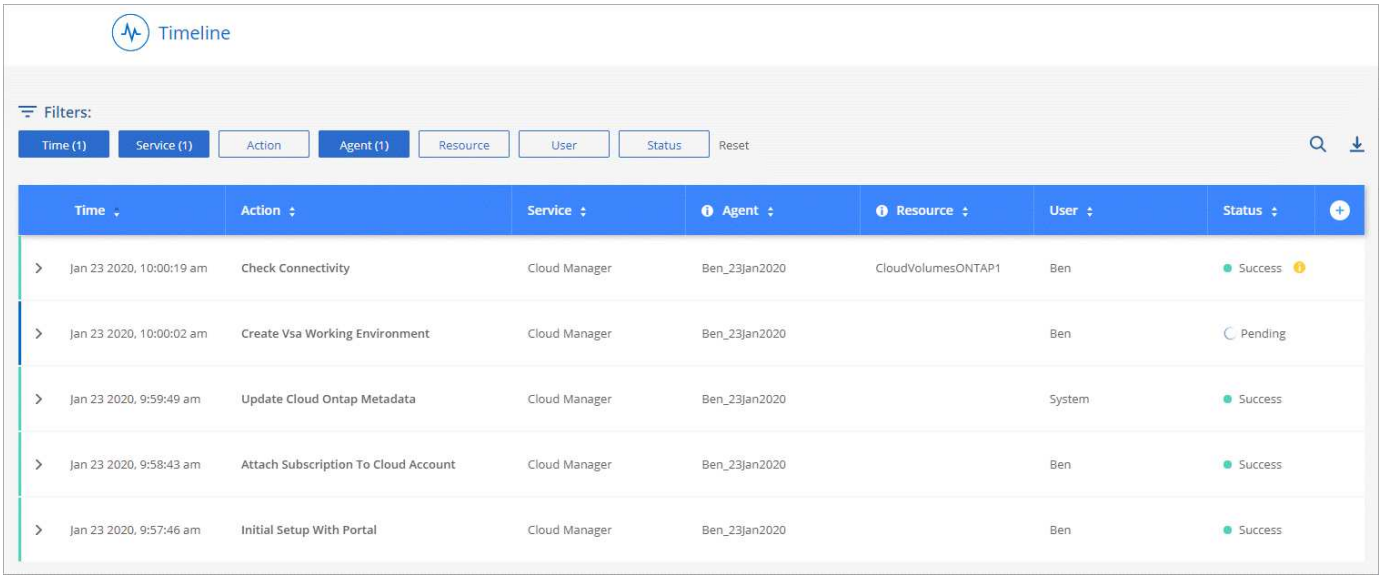


"Scopri come gestire le credenziali AWS in Cloud Manager".

Miglioramenti della tempistica

La cronologia è stata migliorata per fornire ulteriori informazioni sui servizi cloud NetApp che utilizzi.

- La cronologia mostra ora le azioni per tutti i sistemi Cloud Manager all'interno dello stesso account Cloud Central
- Ora puoi trovare le informazioni più facilmente filtrando, cercando e aggiungendo e rimuovendo colonne
- Ora puoi scaricare i dati della timeline in formato CSV
- In futuro, la cronologia mostrerà le azioni per ogni servizio cloud NetApp utilizzato (ma è possibile filtrare le informazioni in base a un singolo servizio)



Cloud Manager 3.8 (8 gennaio 2020)

- Miglioramenti HA in Azure
- Miglioramenti del tiering dei dati in GCP

Miglioramenti HA in Azure

I seguenti miglioramenti sono ora disponibili per le coppie Cloud Volumes ONTAP ha in Azure.

- **Ignora blocchi CIFS per Cloud Volumes ONTAP ha in Azure**

  Ora puoi attivare un'impostazione in Cloud Manager che impedisce i problemi di failover dello storage Cloud Volumes ONTAP durante gli eventi di manutenzione Azure. Quando si attiva questa impostazione, Cloud Volumes ONTAP esegue il veto di CIFS e ripristina le sessioni CIFS attive. "Scopri di più".

- **Connessione HTTPS da Cloud Volumes ONTAP agli account storage**

  È ora possibile attivare una connessione HTTPS da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage Azure durante la creazione di un ambiente di lavoro. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

- **Supporto per gli account storage Azure General-purpose v2**

  Gli account storage creati da Cloud Manager per le coppie ha di Cloud Volumes ONTAP 9.7 sono ora account storage v2 generici.

Miglioramenti del tiering dei dati in GCP

I seguenti miglioramenti sono disponibili per il tiering dei dati Cloud Volumes ONTAP in GCP.

- **Classi di storage Google Cloud per il tiering dei dati**

  È ora possibile scegliere una classe di storage per i dati che Cloud Volumes ONTAP esegue il Tier per lo storage cloud di Google:

  - Storage standard (impostazione predefinita)
  - Storage nearline
  - Storage Coldline

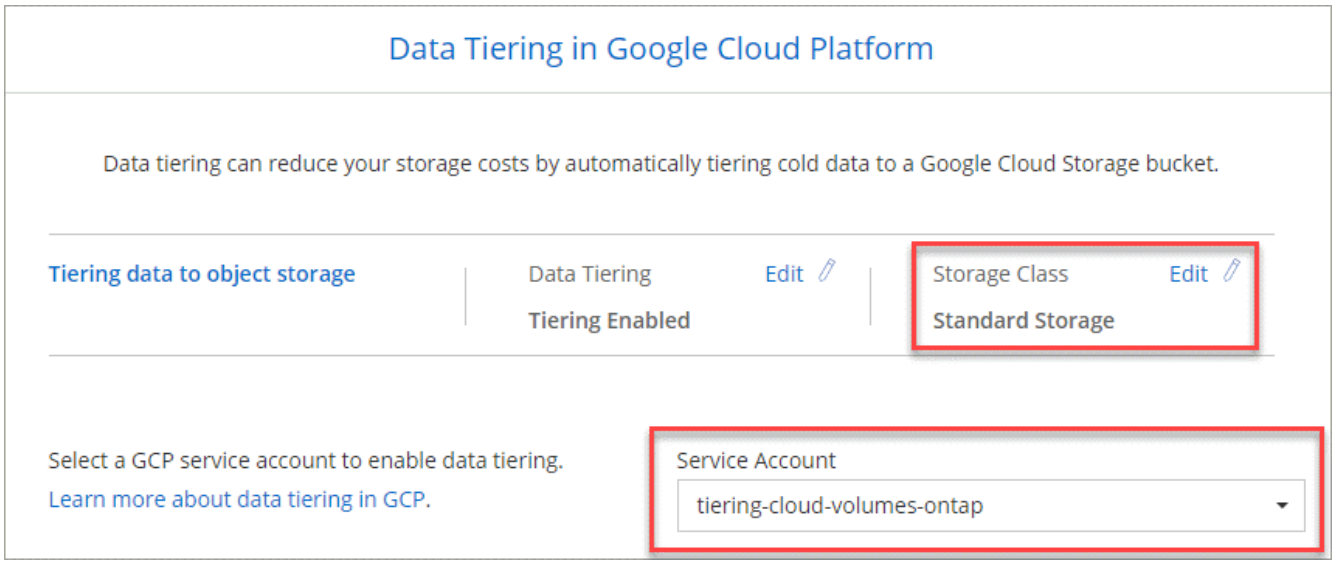
    "Scopri di più sulle classi di storage di Google Cloud".

  "Scopri come modificare la classe di storage per Cloud Volumes ONTAP".

- **Tiering dei dati con un account di servizio**

  A partire dalla versione 9.7, Cloud Manager imposta ora un account di servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Questa modifica offre maggiore sicurezza e richiede meno configurazione. Per istruzioni dettagliate sull'implementazione di un nuovo sistema, "vedere il punto 4 di questa pagina".

  L'immagine seguente mostra la procedura guidata ambiente di lavoro, in cui è possibile selezionare una classe di storage e un account di servizio:



Cloud Manager richiede le seguenti autorizzazioni GCP per questi miglioramenti, come mostrato nella più recente "Policy di Cloud Manager per GCP".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Transizione di Cloud Manager a SaaS

Abbiamo introdotto un'esperienza software-as-a-service per Cloud Manager. Questa nuova esperienza semplifica l'utilizzo di Cloud Manager e ci consente di fornire funzionalità aggiuntive per la gestione della tua infrastruttura di cloud ibrido.

La precedente esperienza di Cloud Manager

In precedenza, il software Cloud Manager era costituito da un'interfaccia utente e da un livello di gestione che inviava richieste ai cloud provider. Per iniziare, devi implementare Cloud Manager nella tua rete cloud o on-premise e accedere all'interfaccia utente che viene eseguita in quell'istanza.

Questa esperienza è cambiata.

La nuova esperienza SaaS

L'interfaccia di Cloud Manager è ora accessibile tramite un'interfaccia utente basata su SaaS a cui si accede da NetApp Cloud Central. Non è più necessario accedere a un'interfaccia utente dal software in esecuzione nella rete.

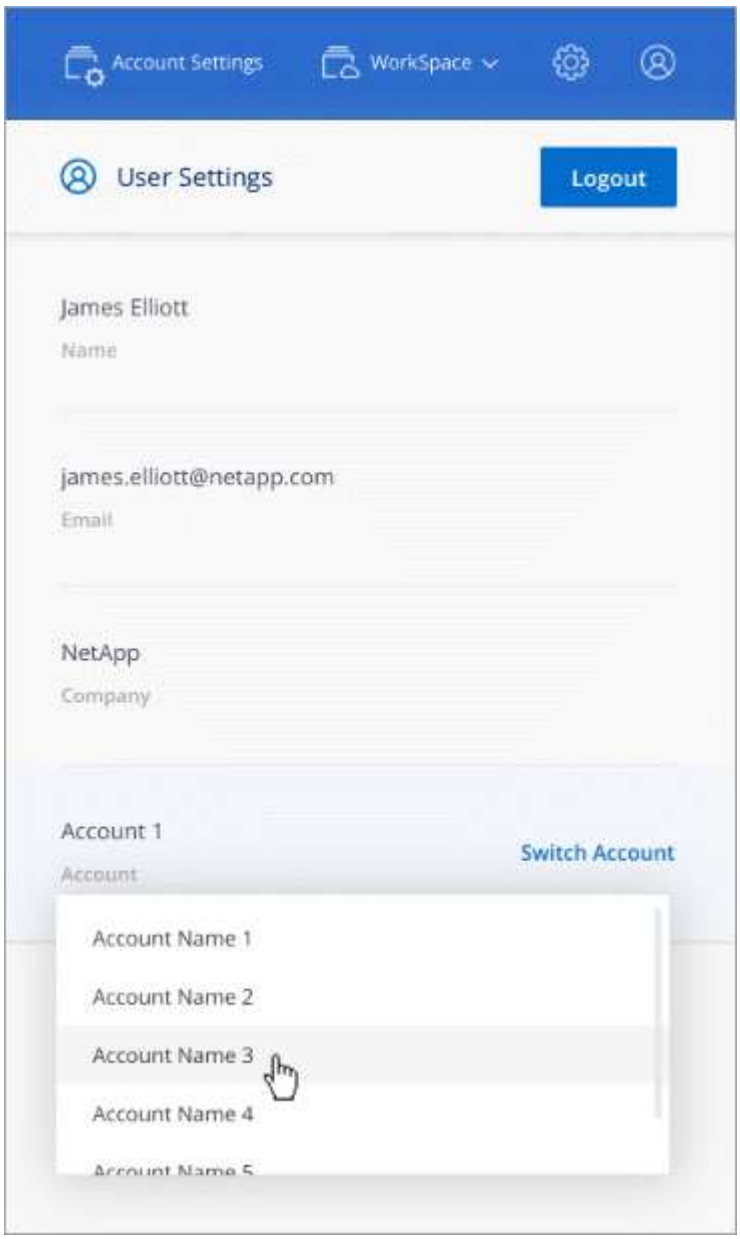
Nella maggior parte dei casi, è necessario implementare un *connettore* nel cloud o nella rete on-premise. Il connettore è un software necessario per gestire Cloud Volumes ONTAP e altri servizi dati cloud. (Il connettore è in realtà lo stesso del software Cloud Manager esistente installato).

Benefici

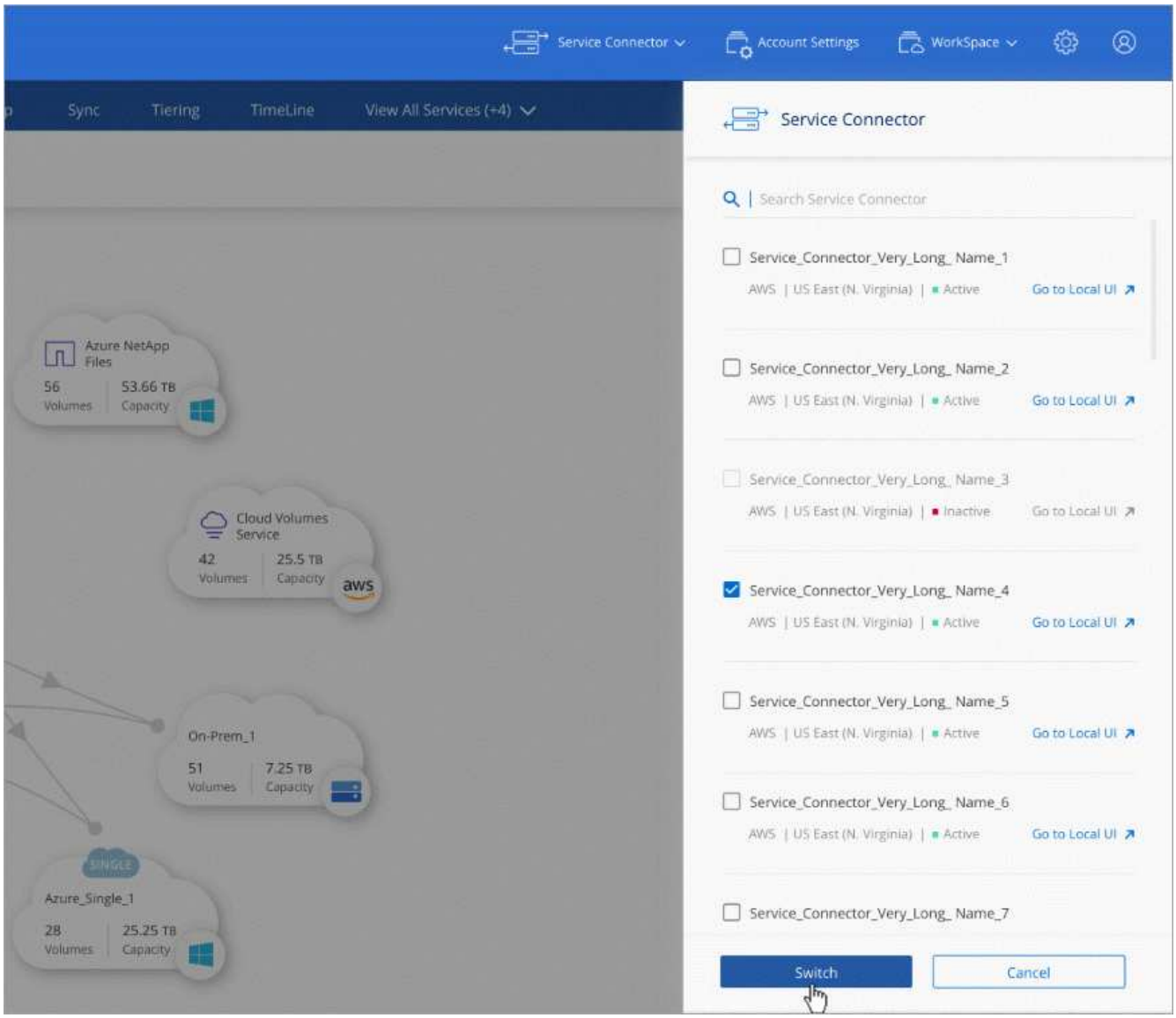
Questo approccio basato su SaaS offre diversi vantaggi:

- Ci consente di offrire funzionalità di gestione aggiuntive per Azure NetApp Files e Cloud Volumes Service senza la necessità di implementare software nel tuo ambiente.
- Puoi passare facilmente da un account Cloud Central all'altro.

  Se un utente è associato a più account Cloud Central, può passare a un altro account in qualsiasi momento dal menu Impostazioni utente. Possono quindi visualizzare i connettori e gli ambienti di lavoro associati a tale account.



- Puoi passare facilmente da un connettore all'altro (quello che oggi conosci come il software Cloud Manager) che sono installati in reti diverse o in diversi cloud provider.

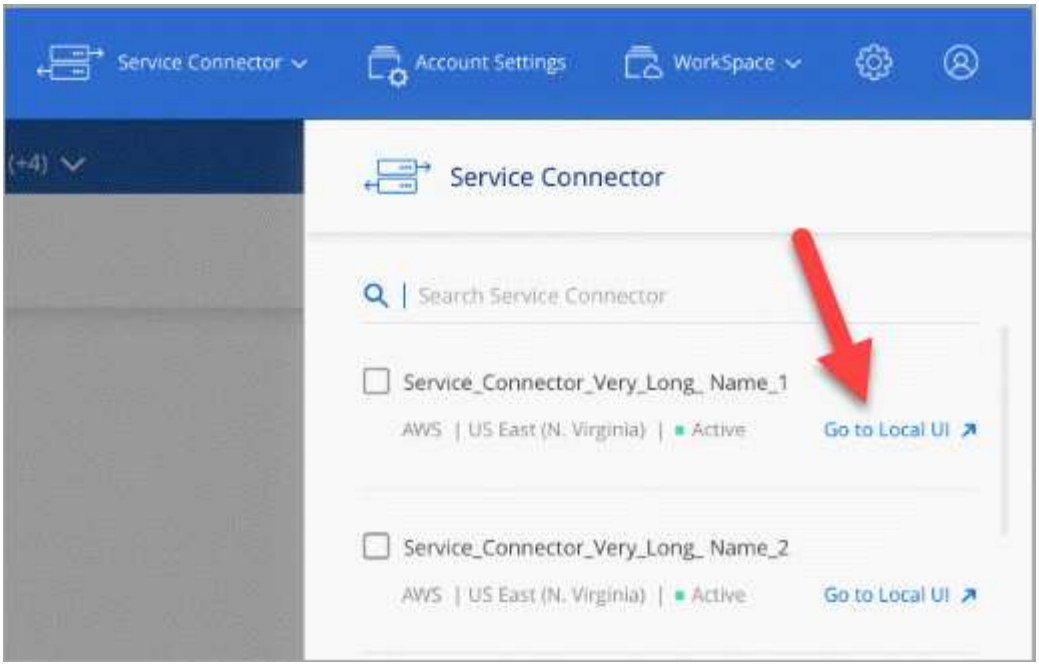


L’interfaccia utente locale

Sebbene sia necessario eseguire quasi tutte le attività dall’interfaccia utente SaaS, sul connettore è ancora disponibile un’interfaccia utente locale. Questa interfaccia è necessaria per alcune attività che devono essere eseguite dal connettore stesso:

- Impostazione di un server proxy
- Installazione di una patch
- Download dei messaggi AutoSupport in corso

È possibile accedere all’interfaccia utente locale direttamente dall’interfaccia utente SaaS:



Modifiche a istanze, macchine virtuali e tipi di computer

Per garantire che siano disponibili risorse adeguate per le nuove e future funzionalità di Cloud Manager, abbiamo modificato l'istanza minima richiesta, la macchina virtuale e il tipo di macchina come segue:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-standard-4

Quando si aggiorna il tipo di computer, si ottiene l'accesso a funzionalità come la nuova esperienza di Kubernetes, Global file cache, Monitoring e molto altro ancora.

Questi formati predefiniti sono quelli minimi supportati "In base ai requisiti di CPU e RAM".

Cloud Manager richiederà di modificare il tipo di macchina del connettore.

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.

I connettori devono rimanere in funzione

Un connettore deve rimanere sempre in funzione. È importante per la salute e il funzionamento continui dei servizi che si abilitano.

Ad esempio, un connettore è un componente chiave per lo stato e il funzionamento dei sistemi PAYGO di Cloud Volumes ONTAP. Se un connettore viene spento, i sistemi PAYGO di Cloud Volumes ONTAP si spegneranno dopo aver perso la comunicazione con un connettore per più di 14 giorni.

La piattaforma SaaS è disattivata per le regioni governative

Se si implementa un connettore in un'area AWS GovCloud, Azure Gov o Azure DoD, l'accesso a Cloud Manager è disponibile solo tramite l'indirizzo IP host di un connettore. L'accesso alla piattaforma SaaS è disattivato per l'intero account.

Ciò significa che solo gli utenti con privilegi che possono accedere al VPC/VNET interno dell'utente finale possono utilizzare l'interfaccia utente o l'API di Cloud Manager.

Significa inoltre che i seguenti servizi non sono disponibili da Cloud Manager:

- Conformità al cloud
- Kubernetes
- Tiering nel cloud
- Global file cache
- Monitoraggio (Cloud Insights)

Per utilizzare questi servizi è necessaria la piattaforma SaaS.

Gli host Linux condivisi non sono supportati

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

Cloud Manager non supporta i volumi FlexGroup

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

Modifiche importanti in Cloud Manager

Questa pagina evidenzia importanti modifiche in Cloud Manager che possono aiutarti a utilizzare il servizio mentre introduciamo nuovi miglioramenti. Si consiglia di continuare a leggere il "Novità" per scoprire tutte le nuove funzionalità e i miglioramenti.

Modifiche SaaS

Abbiamo introdotto un'esperienza software-as-a-service per Cloud Manager. Questa nuova esperienza semplifica l'utilizzo di Cloud Manager e ci consente di fornire funzionalità aggiuntive per la gestione della tua infrastruttura di cloud ibrido.

- "Transizione di Cloud Manager a SaaS"
- "Scopri come funziona Cloud Manager"

Modifiche al tipo di macchina

Per garantire che siano disponibili risorse adeguate per le nuove e future funzionalità di Cloud Manager, abbiamo modificato l'istanza minima richiesta, la macchina virtuale e il tipo di macchina come segue:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-standard-4

Quando si aggiorna il tipo di computer, si ottiene l'accesso a funzionalità come la nuova esperienza di Kubernetes, Global file cache, Monitoring e molto altro ancora.

Questi formati predefiniti sono quelli minimi supportati "In base ai requisiti di CPU e RAM".

Cloud Manager richiederà di modificare il tipo di macchina del connettore.

Impostazioni dell'account

Abbiamo introdotto gli account Cloud Central per fornire la multi-tenancy, per aiutarti a organizzare utenti e risorse in aree di lavoro isolate e per gestire l'accesso a connettori e sottoscrizioni.

- "Scopri di più sugli account Cloud Central: Utenti, aree di lavoro, connettori e sottoscrizioni"
- "Scopri come iniziare a utilizzare il tuo account"
- "Scopri come gestire il tuo account dopo averlo configurato"

Nuove autorizzazioni

Cloud Manager richiede occasionalmente autorizzazioni aggiuntive per i provider di cloud man mano che introduciamo nuove funzionalità e miglioramenti. Questa sezione identifica le nuove autorizzazioni richieste.

È possibile trovare l'elenco più recente delle autorizzazioni su "Pagina delle policy di Cloud Manager".

AWS

A partire dalla versione 3.8.1, per utilizzare il backup nel cloud con Cloud Volumes ONTAP sono necessarie le seguenti autorizzazioni. "Scopri di più".

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Per evitare errori di implementazione di Azure, assicurati che la tua policy di Cloud Manager in Azure includa la seguente autorizzazione:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- A partire dalla versione 3.8.7, è richiesta la seguente autorizzazione per crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. "Scopri di più".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- Per attivare Global file cache su Cloud Volumes ONTAP sono necessarie le seguenti autorizzazioni. "Scopri di più".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

GCP

Nuove autorizzazioni per la gestione di Kubernetes

A partire dalla versione 3.8.8, l'account di servizio per un connettore richiede le seguenti autorizzazioni per rilevare e gestire i cluster Kubernetes in esecuzione in Google Kubernetes Engine (GKE):

```
- container.*
```

Nuove autorizzazioni per il tiering dei dati

A partire dalla versione 3.8, sono necessarie le seguenti autorizzazioni per utilizzare un account di servizio per il tiering dei dati. "Scopri di più".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Nuovi endpoint

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Questa sezione identifica i nuovi endpoint richiesti.

È possibile trovare il "elenco completo degli endpoint a cui si accede dal browser web" e a. "Elenco completo degli endpoint a cui si accede dal connettore".

- Gli utenti devono accedere a Cloud Manager da un browser Web contattando il seguente endpoint:

  https://cloudmanager.netapp.com

- I connettori richiedono l'accesso al seguente endpoint per ottenere immagini software dei componenti container per un'infrastruttura Docker:

  https://cloudmanagerinfraprod.azurecr.io

Assicurarsi che il firewall consenta l’accesso a questo endpoint dal connettore.

Inizia subito con Cloud Manager

Scopri di più su Cloud Manager

Cloud Manager consente agli esperti IT e agli architetti del cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud di NetApp.

Caratteristiche

Cloud Manager è una piattaforma di gestione di livello Enterprise basata su SaaS che ti mantiene in controllo sui tuoi dati, indipendentemente da dove si trovano.

- Configurazione e utilizzo "Cloud Volumes ONTAP" per una gestione dei dati efficiente e multiprotocollo tra i cloud.
- Configurazione e utilizzo dei servizi di file storage: "Azure NetApp Files", "Cloud Volumes Service per AWS", e. "Cloud Volumes Service per Google Cloud".
- Scopri e gestisci i tuoi cluster ONTAP on-premise creando volumi, eseguendo il backup nel cloud, replicando i dati nel cloud ibrido e tiering dei dati cold nel cloud.
- Abilita servizi cloud integrati e software come "Conformità al cloud", "Cloud Insights", "Cloud Backup Service", "Trident"e molto altro ancora.

"Scopri di più su Cloud Manager".

Provider di storage a oggetti supportati

Cloud Manager consente di gestire lo storage cloud e utilizzare i servizi cloud in Amazon Web Services, Microsoft Azure e Google Cloud.

Costo

Il software Cloud Manager è gratuito di NetApp.

Per la maggior parte delle attività, Cloud Manager ti chiede di implementare un connettore nella tua rete cloud, il che comporta addebiti da parte del tuo cloud provider per l'istanza di calcolo e lo storage associato. È possibile eseguire il software Connector on-premise.

Come funziona Cloud Manager

Cloud Manager include un'interfaccia basata su SaaS integrata con NetApp Cloud Central e connettori che gestiscono Cloud Volumes ONTAP e altri servizi cloud.

Software-as-a-service

Cloud Manager è accessibile tramite un "Interfaccia utente basata su SaaS" E API. Questa esperienza SaaS ti consente di accedere automaticamente alle funzionalità più recenti non appena vengono rilasciate e di passare facilmente da un account Cloud Central a un altro.

NetApp Cloud Central

"NetApp Cloud Central" fornisce una posizione centralizzata per l'accesso e la gestione "Servizi cloud di NetApp". Con l'autenticazione utente centralizzata, puoi utilizzare lo stesso set di credenziali per accedere a

Cloud Manager e ad altri servizi cloud come Cloud Insights.

Quando accedi a Cloud Manager per la prima volta, ti viene richiesto di creare un *account Cloud Central*. Questo account offre multi-tenancy e consente di organizzare utenti e risorse in *aree di lavoro* isolate.

Connettori

Nella maggior parte dei casi, un account Admin dovrà implementare un *connettore* nel cloud o nella rete on-premise. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Un connettore deve rimanere sempre in funzione. È importante per la salute e il funzionamento continui dei servizi che si abilitano.

Ad esempio, un connettore è un componente chiave per lo stato e il funzionamento dei sistemi PAYGO di Cloud Volumes ONTAP. Se un connettore viene spento, i sistemi PAYGO di Cloud Volumes ONTAP si spegneranno dopo aver perso la comunicazione con un connettore per più di 14 giorni.

"Scopri di più su quando sono necessari i connettori e sul loro funzionamento".

Panoramica delle reti

Prima che gli utenti accedano a Cloud Manager, è necessario assicurarsi che i browser Web possano accedere a endpoint specifici. Successivamente, è necessario verificare i requisiti di rete per il tipo specifico di ambiente di lavoro e di servizi che verranno utilizzati.

Endpoint a cui si accede dal browser Web

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

Endpoint	Scopo
https://cloudmanager.cloud.netapp.com	Per connetterti all'interfaccia SaaS di Cloud Manager.
https://api.services.cloud.netapp.com	Per contattare le API Cloud Central.
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.

Indice dei requisiti di rete

- "Connettori"
- "Cloud Volumes ONTAP per AWS"
- "Cloud Volumes ONTAP per Azure"
- "Cloud Volumes ONTAP per GCP"
- "Replica dei dati tra sistemi ONTAP"

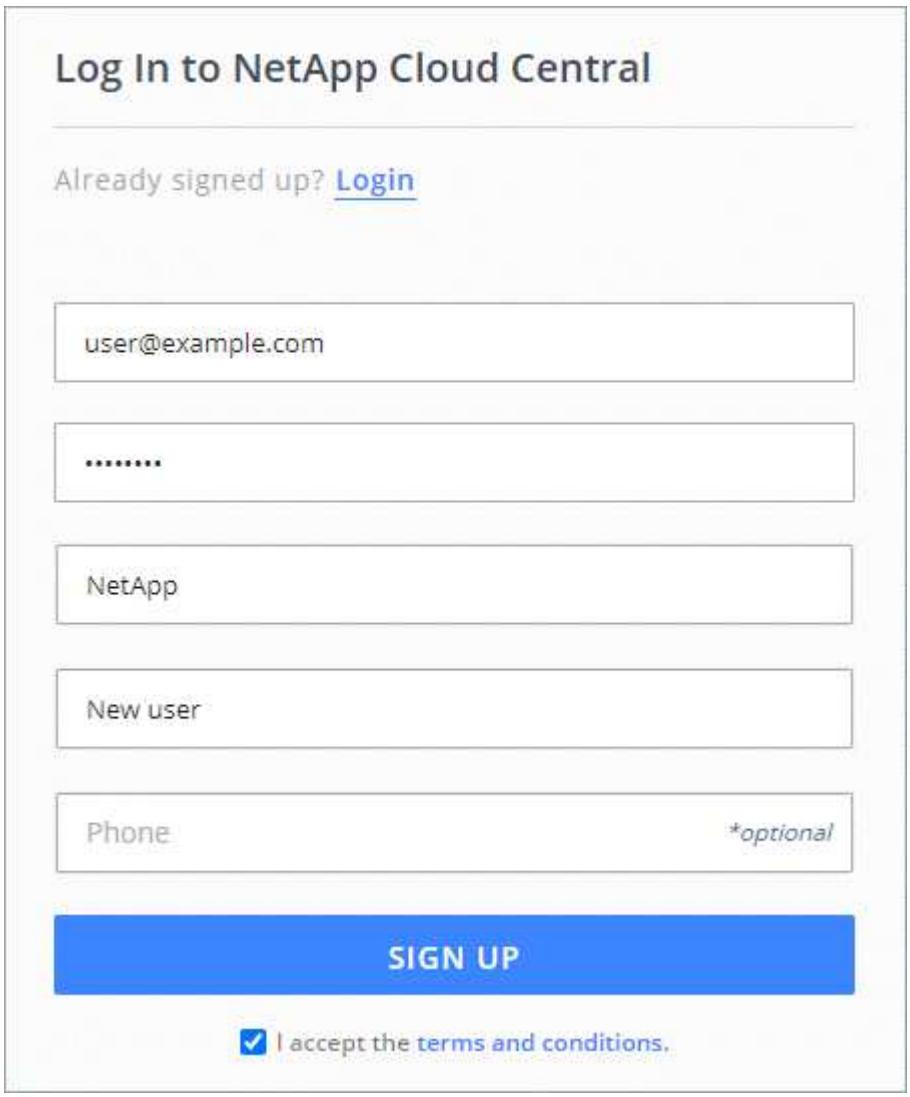
- "Conformità del cloud per Cloud Volumes ONTAP o Azure NetApp Files"
- "Conformità del cloud per Amazon S3"
- "Cluster ONTAP on-premise"
  - "Tiering dei dati dai cluster ONTAP ad Amazon S3"
  - "Tiering dei dati dai cluster ONTAP allo storage Azure Blob"
  - "Tiering dei dati dai cluster ONTAP allo storage cloud Google"
  - "Tiering dei dati dai cluster ONTAP a StorageGRID"

Iscrizione a NetApp Cloud Central

Iscriviti a NetApp Cloud Central per accedere ai servizi cloud di NetApp.

Fasi

1. Aprire un browser Web e visitare il sito Web all'indirizzo "NetApp Cloud Central".
2. Fare clic su **Registrati**.
3. Compila il modulo e fai clic su **Registrati**.



4. Attendi un'e-mail da NetApp Cloud Central.
5. Fare clic sul collegamento nell'e-mail per verificare l'indirizzo e-mail.

Risultato

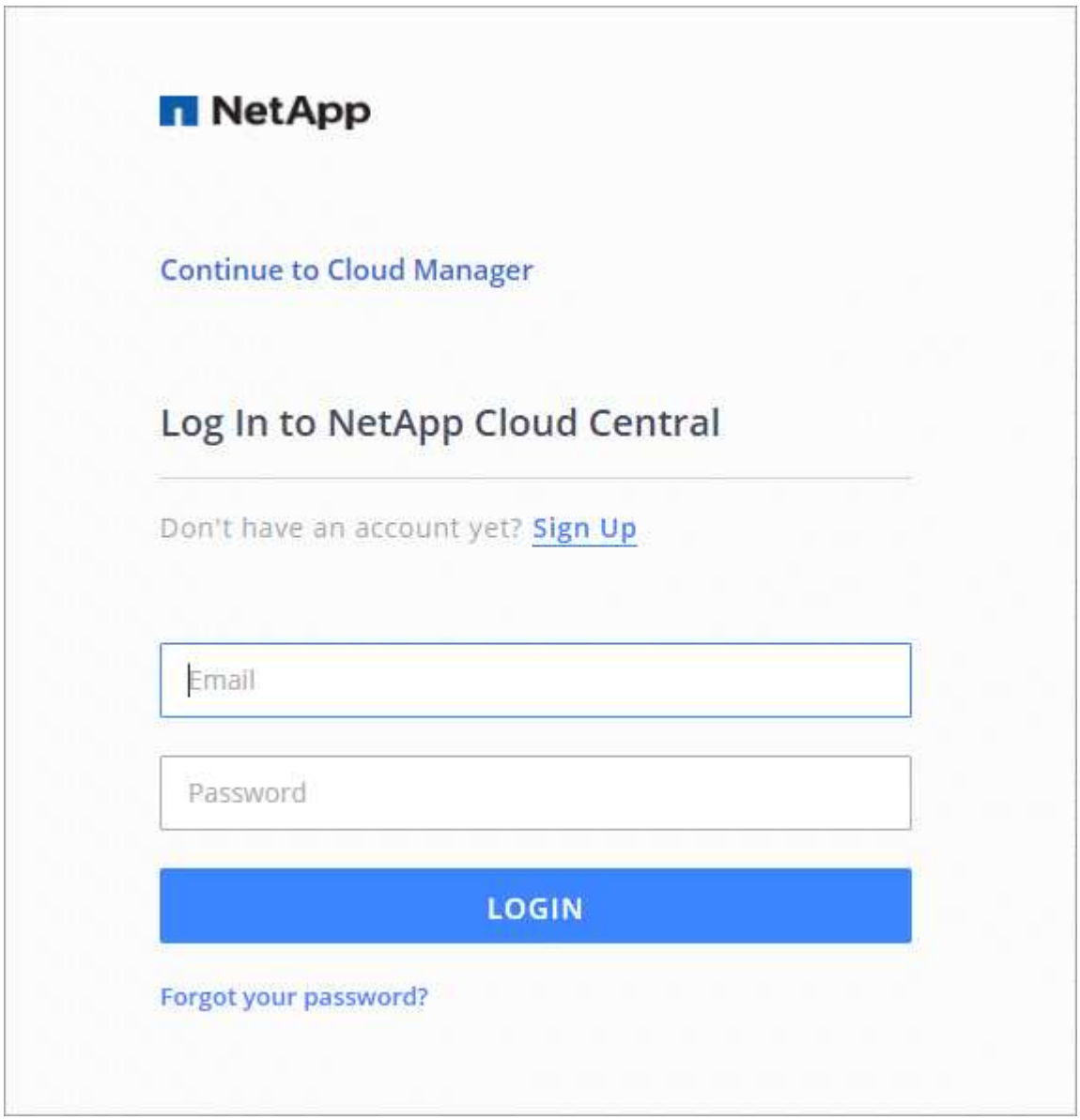
Ora disponi di un account di accesso utente attivo di Cloud Central.

Accesso a Cloud Manager

L'interfaccia di Cloud Manager è accessibile tramite un'interfaccia utente basata su SaaS visitando il sito https://cloudmanager.netapp.com.

Fasi

1. Aprire un browser Web e visitare il sito Web all'indirizzo https://cloudmanager.netapp.com.
2. Effettua l'accesso utilizzando le credenziali di NetApp Cloud Central.



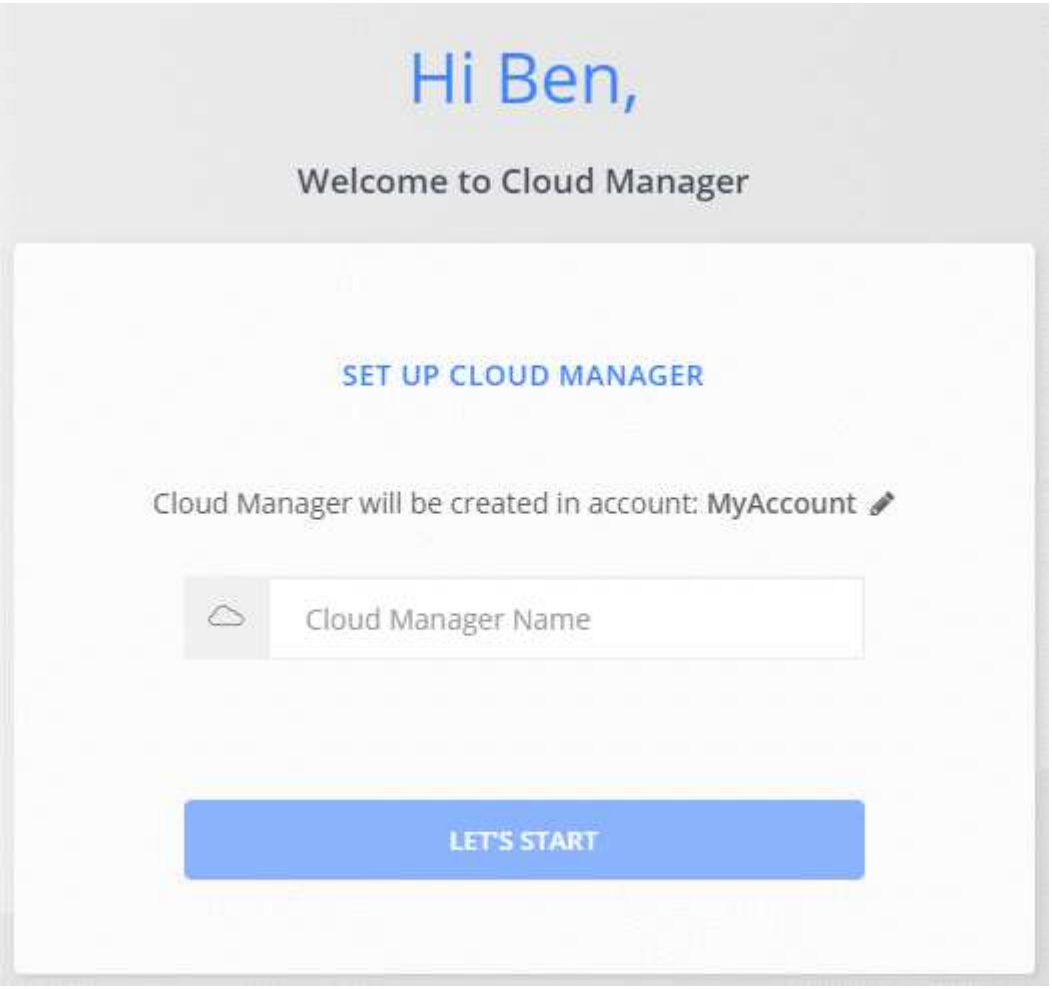
Configurare un account Cloud Central

Impostazioni dell'account: Utenti, aree di lavoro, connettori e sottoscrizioni

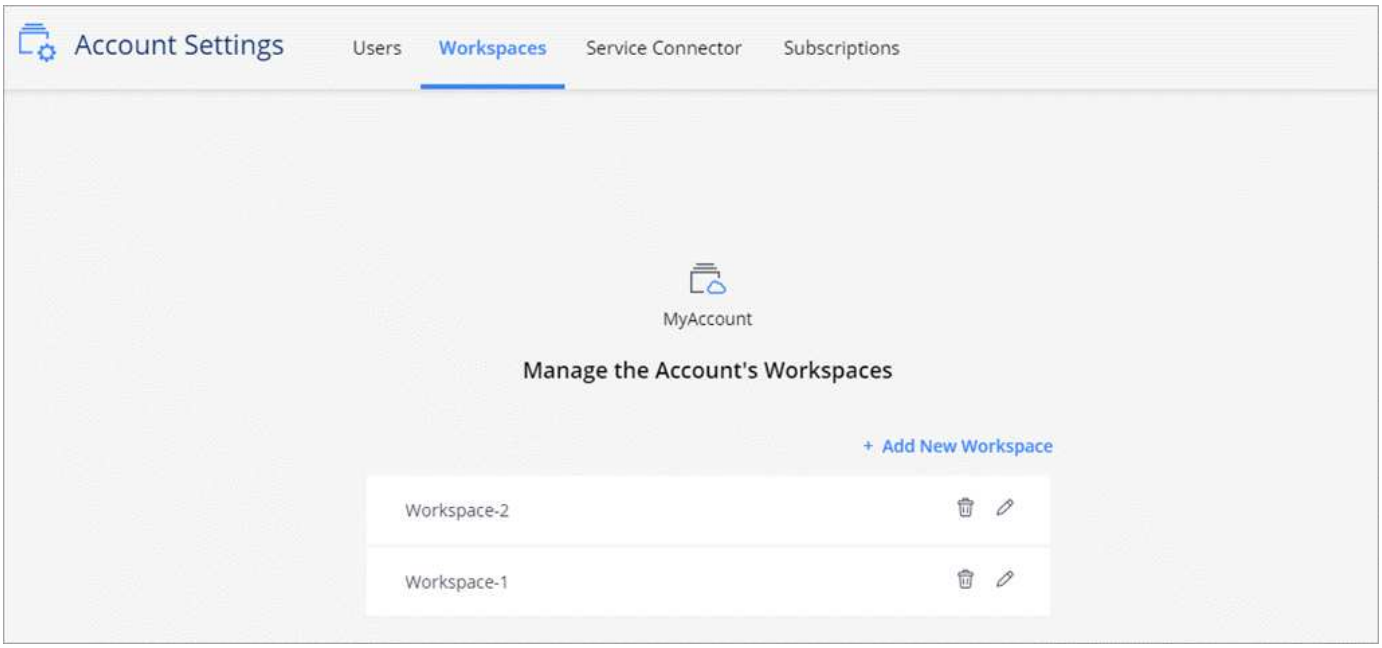
Un *account Cloud Central* offre multi-tenancy e consente di organizzare utenti e risorse in aree di lavoro isolate da Cloud Manager.

Ad esempio, più utenti possono implementare e gestire i sistemi Cloud Volumes ONTAP in ambienti isolati denominati *workspaces*. Queste aree di lavoro sono invisibili agli altri utenti, a meno che non siano condivise.

Quando accedi per la prima volta a Cloud Manager, ti viene richiesto di selezionare o creare un account Cloud Central:



Gli amministratori dell'account possono quindi modificare le impostazioni di questo account gestendo utenti, aree di lavoro, connettori e sottoscrizioni:



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

Impostazioni dell'account

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

Utenti

Gli utenti visualizzati nelle Impostazioni account sono gli utenti di NetApp Cloud Central associati al tuo account Cloud Central. L'associazione di un utente a un account e a una o più aree di lavoro in tale account consente a tali utenti di creare e gestire ambienti di lavoro in Cloud Manager.

Quando si associa un utente, viene assegnato un ruolo:

- *Account Admin*: Può eseguire qualsiasi azione in Cloud Manager.
- *Workspace Admin*: Consente di creare e gestire le risorse nell'area di lavoro assegnata.
- *Cloud Compliance Viewer*: È in grado di visualizzare solo le informazioni di conformità e generare report per i sistemi ai quali è consentito l'accesso.

Aree di lavoro

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

Un ambiente di lavoro rappresenta un sistema storage:

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

Connettori

Un connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Il connettore viene eseguito su un'istanza di macchina virtuale implementata nel provider cloud o su un host on-premise configurato.

È possibile utilizzare un connettore con più di un servizio dati cloud NetApp. Ad esempio, se disponi già di un connettore per Cloud Manager, puoi selezionarlo quando configuri il servizio Cloud Tiering.

Abbonamenti

Il widget Impostazioni account mostra gli abbonamenti NetApp associati all'account selezionato.

Quando ti iscrivi a Cloud Manager dal marketplace di un cloud provider, verrai reindirizzato a Cloud Central dove dovrai salvare l'abbonamento e associarlo a account specifici.

Dopo aver effettuato l'iscrizione, ogni abbonamento è disponibile dal widget Impostazioni account. Verranno visualizzati solo gli abbonamenti associati all'account attualmente visualizzato.

È possibile rinominare un abbonamento e disassociarlo da uno o più account.

Ad esempio, supponiamo di avere due account e di fatturarvi ciascuno tramite abbonamenti separati. Potresti disassociare un abbonamento da uno degli account, in modo che gli utenti di quell'account non scelgano accidentalmente l'abbonamento sbagliato quando crei un ambiente di lavoro Cloud Volume ONTAP.

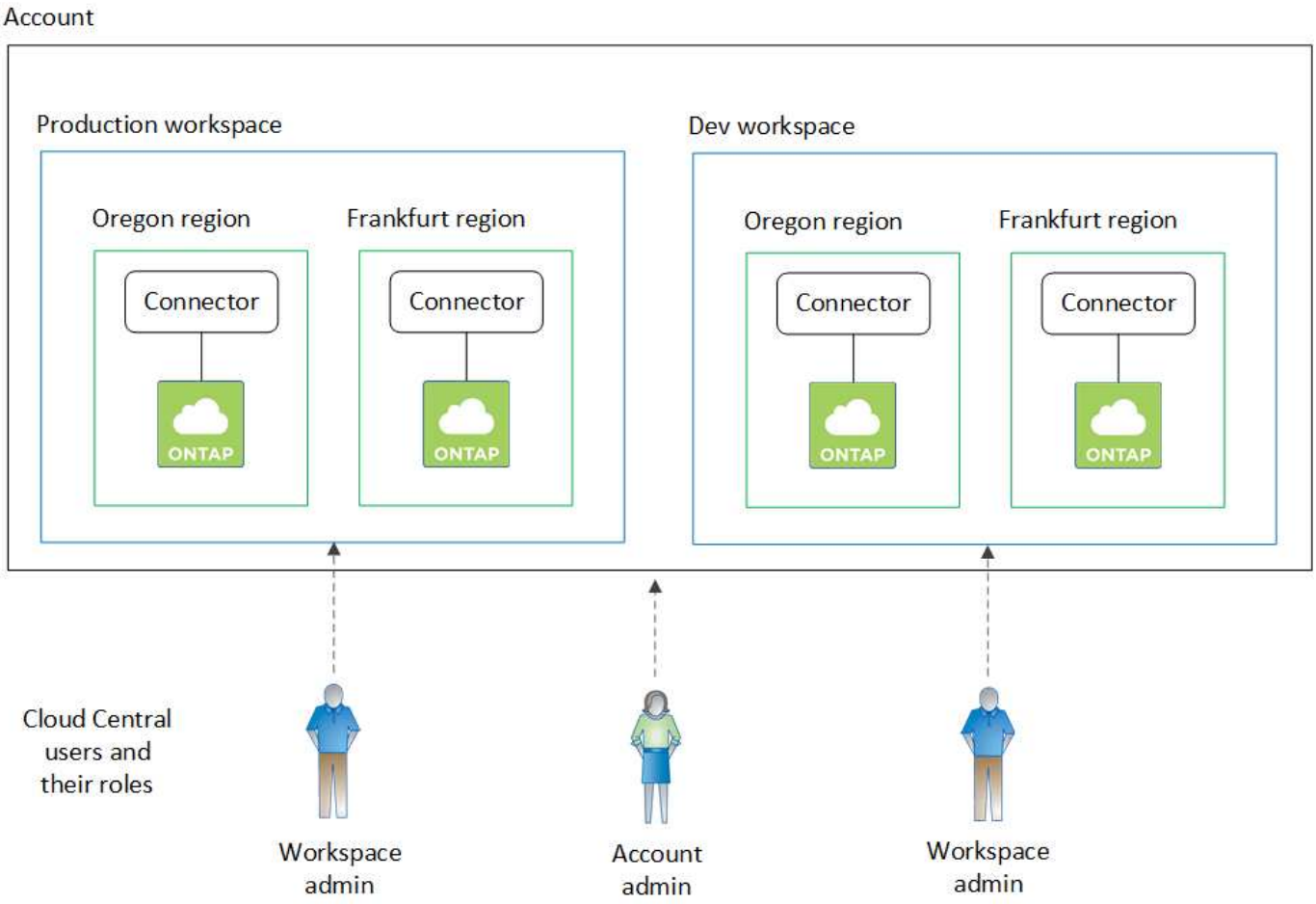
Esempi

I seguenti esempi illustrano come configurare gli account.

> In entrambe le immagini di esempio che seguono, il connettore e i sistemi Cloud Volumes ONTAP non risiedono effettivamente _nell'account NetApp Cloud Central, ma vengono eseguiti in un cloud provider. Si tratta di una rappresentazione concettuale della relazione tra ciascun componente.

Esempio 1

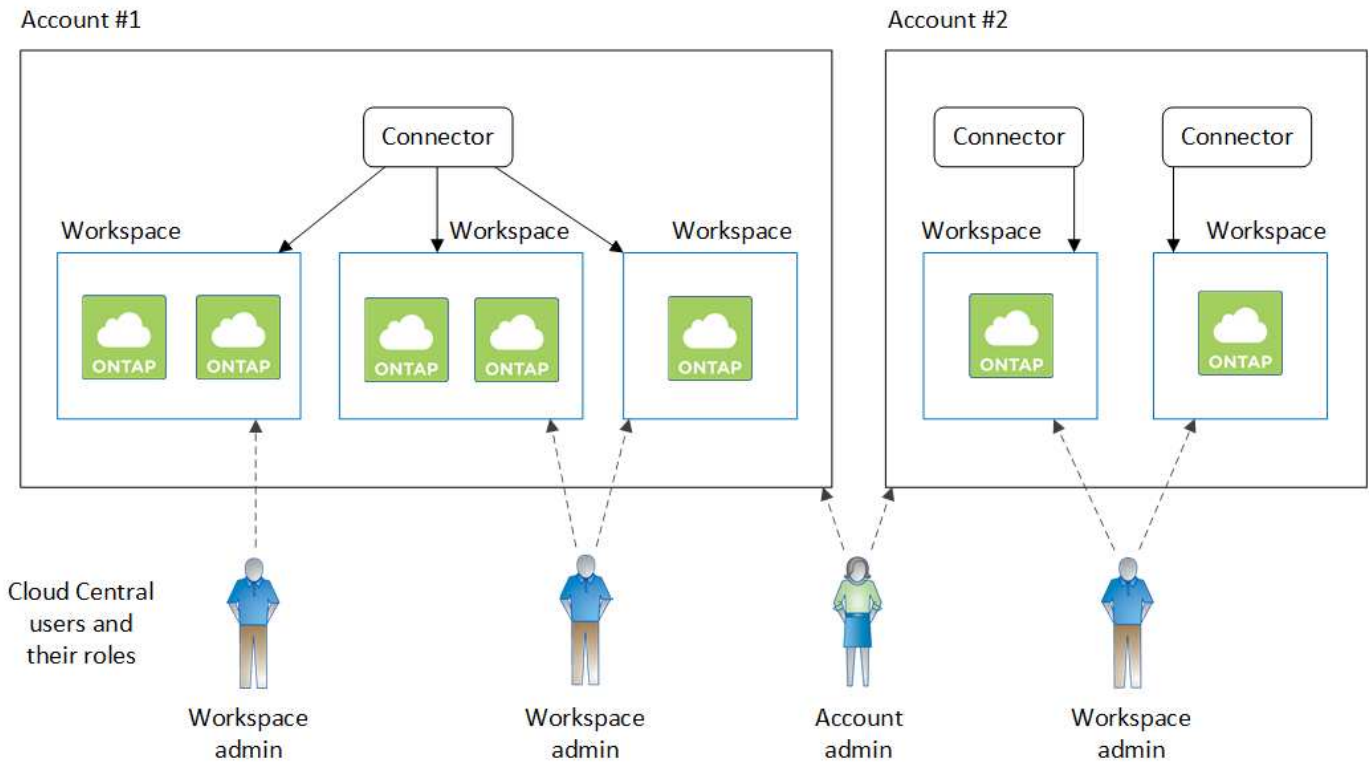
Nell'esempio riportato di seguito viene illustrato un account che utilizza due aree di lavoro per creare ambienti isolati. Il primo spazio di lavoro è per un ambiente di produzione e il secondo per un ambiente di sviluppo.



Esempio 2

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

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



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

Quando accedi a Cloud Manager per la prima volta, ti viene richiesto di creare un *account NetApp Cloud Central*. Questo account offre multi-tenancy e consente di organizzare utenti e risorse in *aree di lavoro* isolate.

"Scopri di più sul funzionamento degli account Cloud Central".

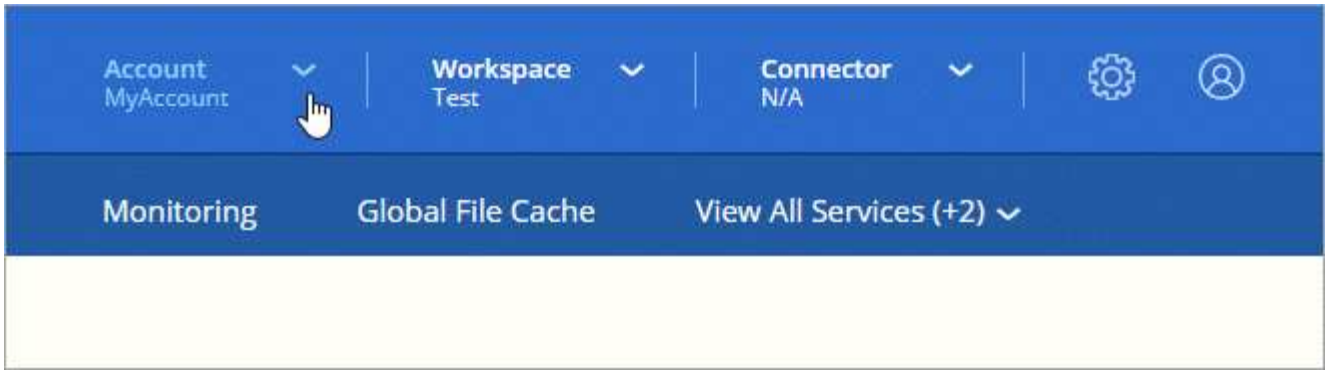
Configura il tuo account Cloud Central in modo che gli utenti possano accedere a Cloud Manager e agli ambienti di lavoro in un'area di lavoro. Basta aggiungere un singolo utente o più utenti e aree di lavoro.

Aggiunta di aree di lavoro

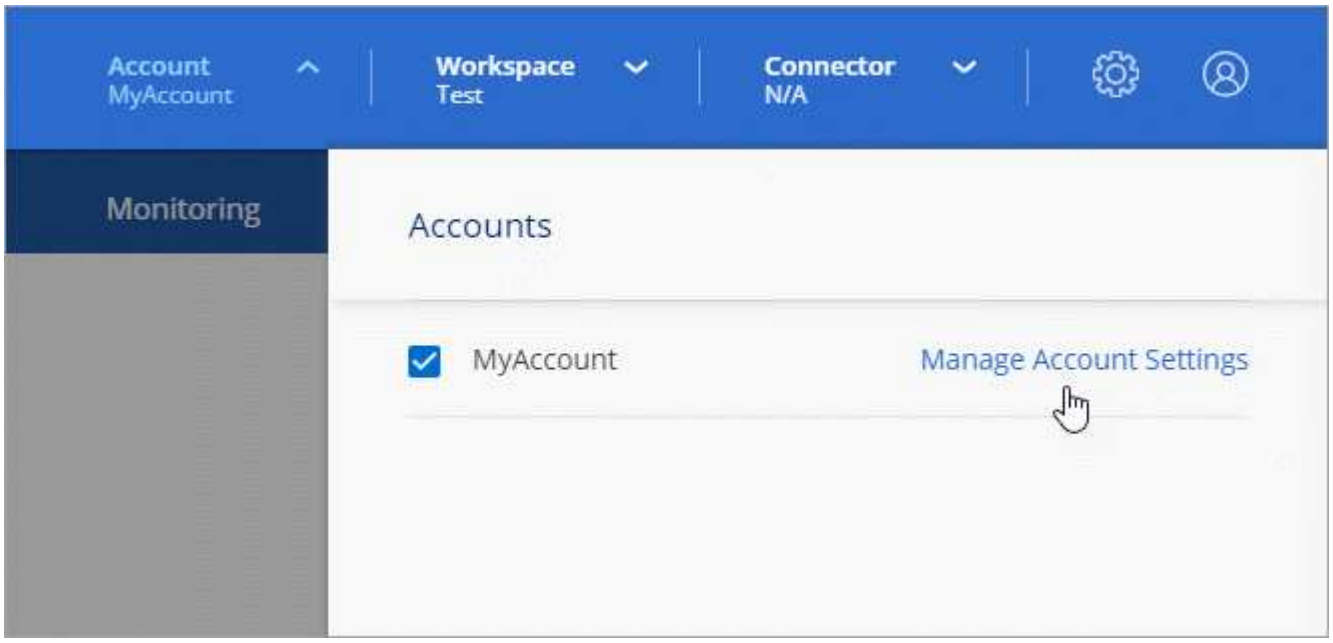
In Cloud Manager, le aree di lavoro consentono di isolare un set di ambienti di lavoro da altri ambienti di lavoro e da altri utenti. Ad esempio, è possibile creare due aree di lavoro e associare utenti separati a ciascuna area di lavoro.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account**.



2. Fare clic su **Manage account** (Gestisci account) accanto all'account attualmente selezionato.



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

Al termine

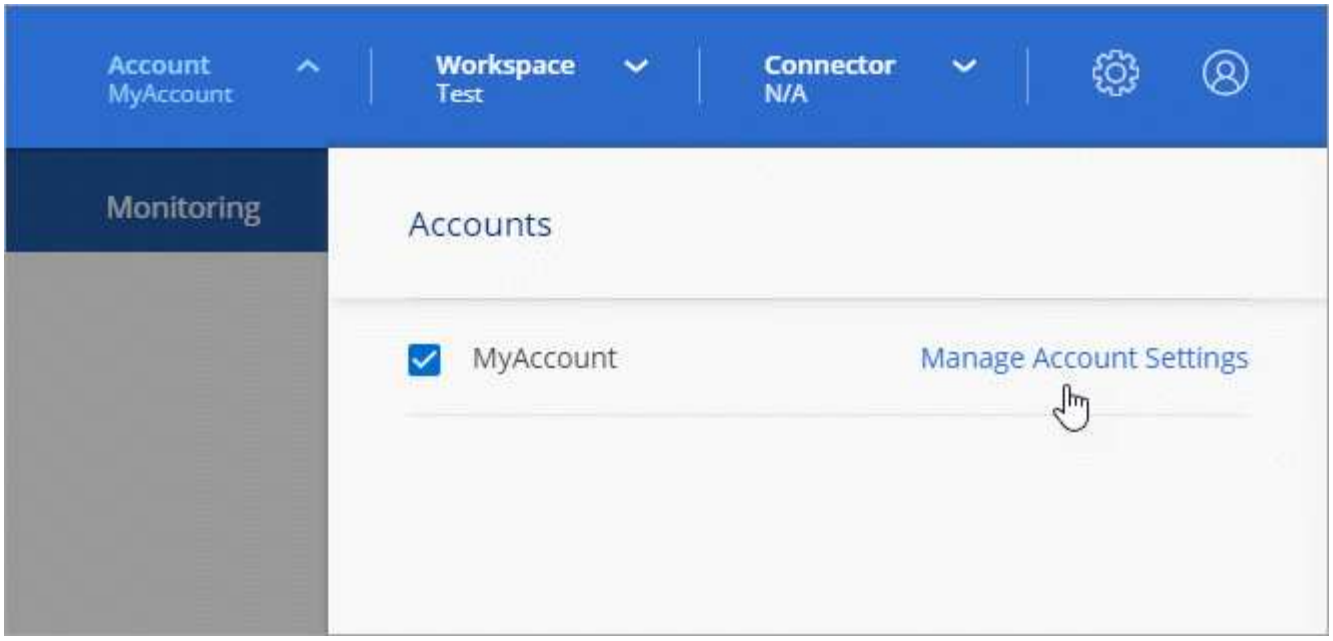
Se un amministratore dell'area di lavoro ha bisogno di accedere a questa area di lavoro, sarà necessario associare l'utente. Inoltre, dovrai associare i connettori allo spazio di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzarli.

Aggiunta di utenti

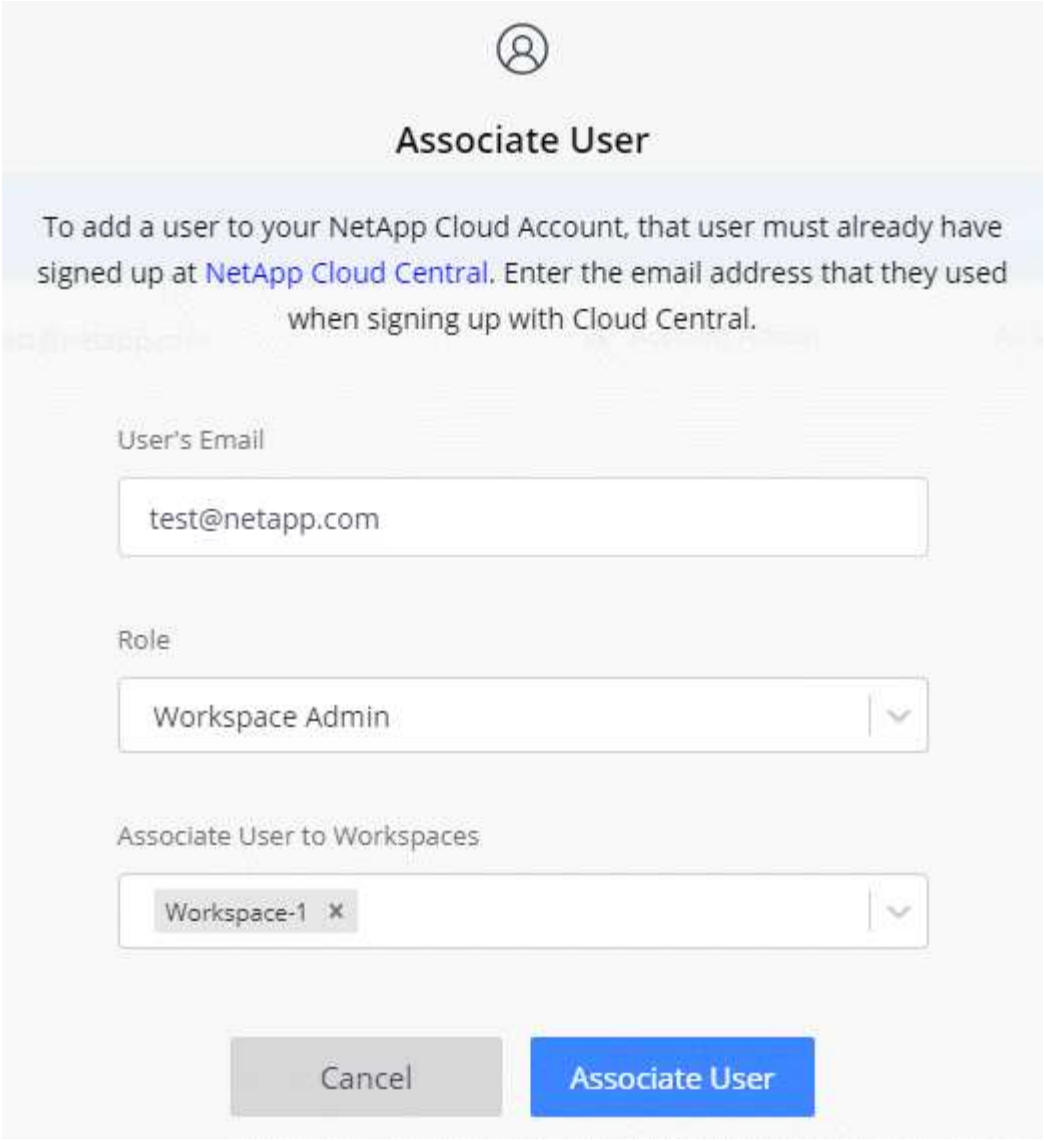
Associa gli utenti di Cloud Central all'account Cloud Central in modo che questi utenti possano creare e gestire ambienti di lavoro in Cloud Manager.

Fasi

1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "NetApp Cloud Central" e iscriverti.
2. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



3. Dalla scheda Users (utenti), fare clic su **associate User** (Associa utente).
4. Inserire l'indirizzo e-mail dell'utente e selezionare un ruolo per l'utente:
   - **Account Admin**: Può eseguire qualsiasi azione in Cloud Manager.
   - **Workspace Admin**: Consente di creare e gestire le risorse nelle aree di lavoro assegnate.
   - **Compliance Viewer**: È in grado di visualizzare solo le informazioni di conformità e generare report per le aree di lavoro a cui sono autorizzati ad accedere.
5. Se si seleziona Workspace Admin (Amministratore area di lavoro) o Compliance Viewer (Visualizzatore conformità), selezionare una o più aree di lavoro da associare all'utente.



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

Risultato

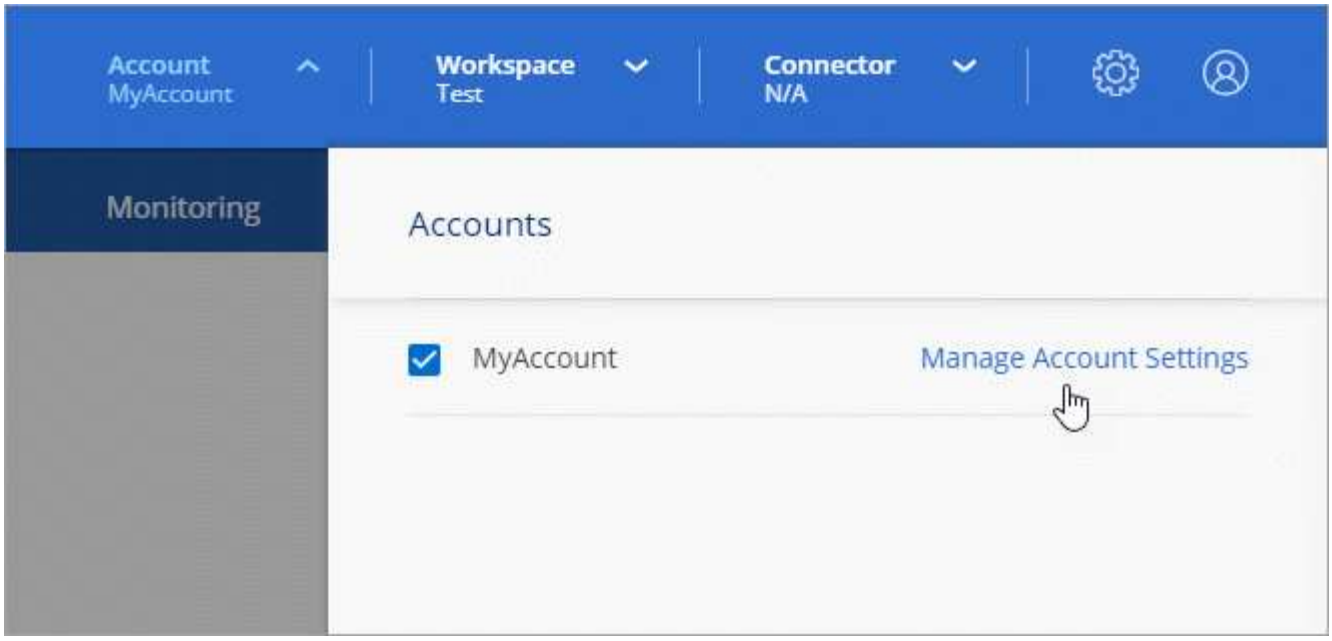
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

Associazione di Workspace Admins alle aree di lavoro

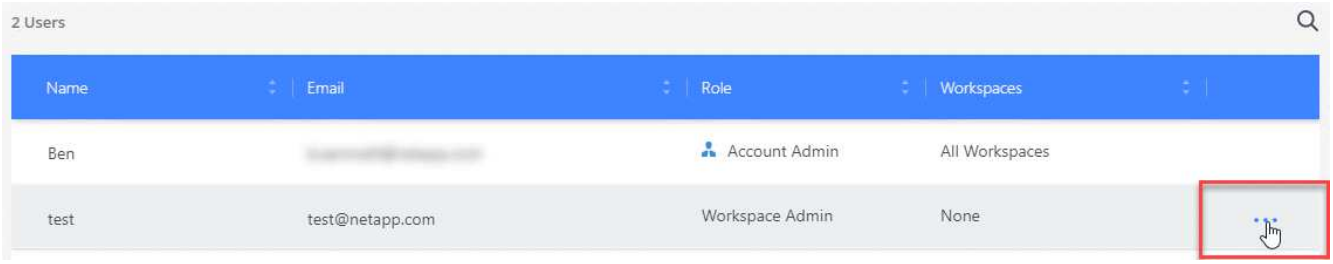
È possibile associare gli amministratori Workspace a aree di lavoro aggiuntive in qualsiasi momento. L'associazione dell'utente consente di creare e visualizzare gli ambienti di lavoro in tale area di lavoro.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Dalla scheda Users (utenti), fare clic sul menu delle azioni nella riga corrispondente all'utente.



3. Fare clic su **Gestisci aree di lavoro**.
4. Selezionare una o più aree di lavoro e fare clic su **Applica**.

Risultato

L'utente può ora accedere a tali aree di lavoro da Cloud Manager, purché il connettore sia stato associato anche alle aree di lavoro.

Associazione di connettori alle aree di lavoro

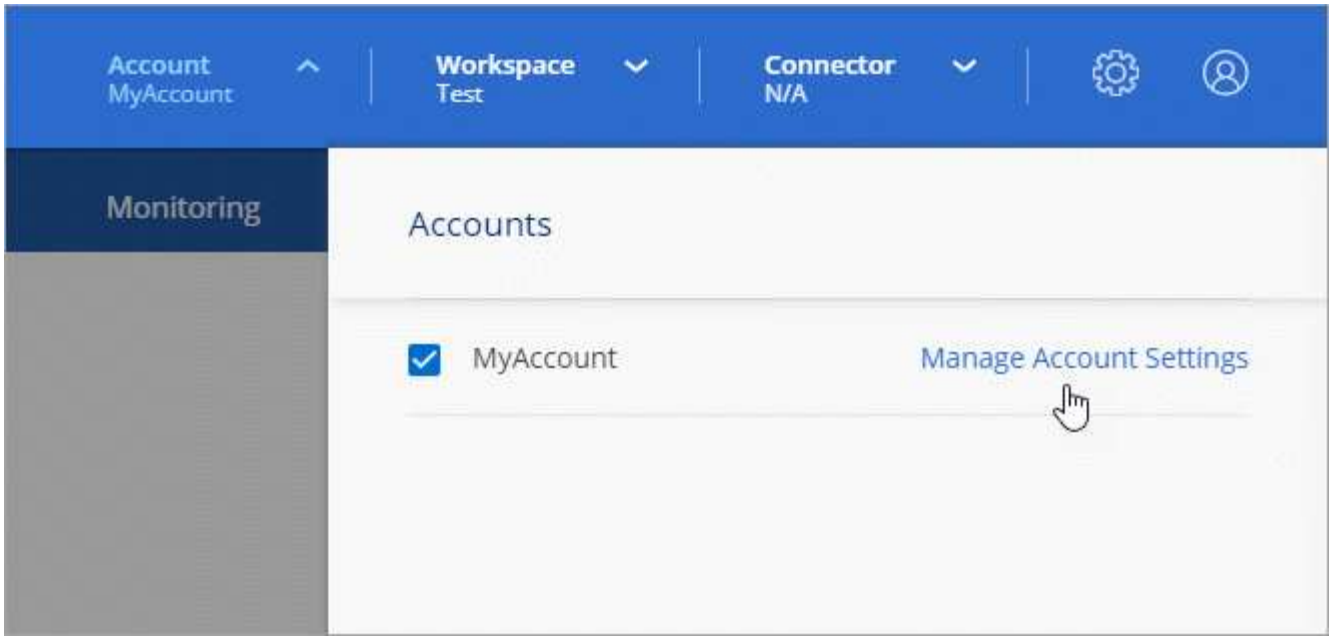
È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP.

Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita.

"Scopri di più su utenti, aree di lavoro e connettori".

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Fare clic su **Connector** (connettore).
3. Fare clic su **Manage Workspaces** (Gestisci aree di lavoro) per il connettore che si desidera associare.
4. Selezionare una o più aree di lavoro e fare clic su **Applica**.

Risultato

Gli amministratori dell'area di lavoro possono ora utilizzare questi connettori per creare sistemi Cloud Volumes ONTAP.

Quali sono le prossime novità?

Ora che hai configurato il tuo account, puoi gestirlo in qualsiasi momento rimuovendo utenti, gestendo aree di lavoro, connettori e sottoscrizioni. "Scopri di più".

Configurare un connettore

Scopri di più sui connettori

Nella maggior parte dei casi, un account Admin dovrà implementare un *connettore* nel cloud o nella rete on-premise. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Quando è necessario un connettore

È necessario un connettore per utilizzare una delle seguenti funzionalità in Cloud Manager:

- Cloud Volumes ONTAP
- Cluster ONTAP on-premise
- Conformità al cloud
- Kubernetes
- Backup su cloud

- Monitoraggio
- Tiering on-premise
- Global file cache
- Discovery bucket Amazon S3

Un connettore è ***not*** necessario per Azure NetApp Files, Cloud Volumes Service o Cloud Sync.

> Sebbene non sia necessario un connettore per configurare e gestire Azure NetApp Files, è necessario un connettore per utilizzare la conformità cloud per eseguire la scansione dei dati Azure NetApp Files.

Posizioni supportate

Un connettore è supportato nelle seguenti posizioni:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On-premise

> Se si desidera creare un sistema Cloud Volumes ONTAP in Google Cloud, è necessario disporre di un connettore in esecuzione anche in Google Cloud. Non è possibile utilizzare un connettore in esecuzione in un'altra posizione.

I connettori devono rimanere in funzione

Un connettore deve rimanere sempre in funzione. È importante per la salute e il funzionamento continui dei servizi che si abilitano.

Ad esempio, un connettore è un componente chiave per lo stato e il funzionamento dei sistemi PAYGO di Cloud Volumes ONTAP. Se un connettore viene spento, i sistemi PAYGO di Cloud Volumes ONTAP si spegneranno dopo aver perso la comunicazione con un connettore per più di 14 giorni.

Come creare un connettore

Un amministratore dell'account deve creare un connettore prima che un amministratore dell'area di lavoro possa creare un ambiente di lavoro Cloud Volumes ONTAP e utilizzare una qualsiasi delle altre funzionalità sopra elencate.

Un account Admin può creare un connettore in diversi modi:

- Direttamente da Cloud Manager (consigliato)
  - "Creare in AWS"
  - "Crea in Azure"
  - "Creare in GCP"
- "Da AWS Marketplace"
- "Da Azure Marketplace"
- "Scaricando e installando il software su un host Linux esistente"

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

Permessi

Sono necessarie autorizzazioni specifiche per creare il connettore e un altro set di autorizzazioni per l'istanza stessa del connettore.

Autorizzazioni per creare un connettore

L'utente che crea un connettore da Cloud Manager ha bisogno di autorizzazioni specifiche per implementare l'istanza nel provider cloud scelto. Cloud Manager ti ricorderà i requisiti di autorizzazione quando crei un connettore.

"Visualizza le policy per ogni cloud provider".

Permessi per l'istanza del connettore

Il connettore necessita di autorizzazioni specifiche per il cloud provider per eseguire le operazioni per conto dell'utente. Ad esempio, per implementare e gestire Cloud Volumes ONTAP.

Quando crei un connettore direttamente da Cloud Manager, Cloud Manager crea il connettore con le autorizzazioni necessarie. Non c'è niente da fare.

Se si crea il connettore da AWS Marketplace, Azure Marketplace o installando manualmente il software, è necessario assicurarsi di disporre delle autorizzazioni corrette.

"Visualizza le policy per ogni cloud provider".

Quando utilizzare connettori multipli

In alcuni casi, potrebbe essere necessario un solo connettore, ma potrebbero essere necessari due o più connettori.

Ecco alcuni esempi:

- Stai utilizzando un ambiente multi-cloud (AWS e Azure), quindi hai un connettore in AWS e un altro in Azure. Ciascuno di essi gestisce i sistemi Cloud Volumes ONTAP in esecuzione in tali ambienti.
- Un provider di servizi potrebbe utilizzare un account Cloud Central per fornire servizi ai propri clienti, mentre utilizza un altro account per fornire il disaster recovery per una delle proprie business unit. Ciascun account dispone di connettori separati.

Quando passare da un connettore all'altro

Quando crei il primo connettore, Cloud Manager utilizza automaticamente tale connettore per ogni ambiente di lavoro aggiuntivo creato. Una volta creato un connettore aggiuntivo, è necessario passare da un connettore all'altro per visualizzare gli ambienti di lavoro specifici di ciascun connettore.

"Scopri come passare da un connettore all'altro".

L'interfaccia utente locale

Mentre è necessario eseguire quasi tutte le attività di "Interfaccia utente SaaS", Un'interfaccia utente locale è ancora disponibile sul connettore. Questa interfaccia è necessaria per alcune attività che devono essere eseguite dal connettore stesso:

- "Impostazione di un server proxy"
- Installazione di una patch (in genere collaborerete con il personale NetApp per installare una patch)
- Download dei messaggi AutoSupport (solitamente indirizzati dal personale NetApp in caso di problemi)

"Scopri come accedere all'interfaccia utente locale".

Aggiornamenti del connettore

Il connettore aggiorna automaticamente il software alla versione più recente, a patto che sia disponibile "accesso a internet in uscita" per ottenere l'aggiornamento software.

Requisiti di rete per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. 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, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

Connessione alle reti di destinazione

Un connettore richiede una connessione di rete al tipo di ambiente di lavoro che si sta creando e ai servizi che si intende abilitare.

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

Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. L'accesso a Internet in uscita è necessario anche se si desidera installare manualmente il connettore su un host Linux o accedere all'interfaccia utente locale in esecuzione sul connettore.

Le sezioni seguenti identificano gli endpoint specifici.

Endpoint per gestire le risorse in AWS

Un connettore contatta i seguenti endpoint durante la gestione delle risorse 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 al connettore di implementare e gestire Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.

Endpoint	Scopo
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint per la gestione delle risorse in Azure

Un connettore contatta i seguenti endpoint durante la gestione delle risorse in 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.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP.

Endpoint	Scopo
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
*.blob.core.windows.net	Richiesto per coppie ha quando si utilizza un proxy.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint per la gestione delle risorse in GCP

Un connettore contatta i seguenti endpoint durante la gestione delle risorse in GCP:

Endpoint	Scopo
https://www.googleapis.com	Consente al connettore di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Consente a NetApp di raccogliere le informazioni necessarie per risolvere i problemi di supporto.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.

Endpoint	Scopo
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint per installare il connettore su un host Linux

È possibile installare manualmente il software del connettore sul proprio host Linux. In tal caso, il programma di installazione del connettore 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

L'host potrebbe tentare di aggiornare i pacchetti del sistema operativo durante l'installazione. L'host può contattare diversi siti di mirroring per questi pacchetti di sistemi operativi.

Endpoint a cui si accede dal browser Web quando si utilizza l'interfaccia utente locale

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	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.

Porte e gruppi di sicurezza

Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

Regole per il connettore in AWS

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

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 del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale e alle connessioni da Cloud Compliance
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore 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 la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager
Conformità al cloud	HTTP	80	Istanza di Cloud Compliance	Conformità del cloud per Cloud Volumes ONTAP

Regole per il connettore in Azure

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Porta	Protocollo	Scopo
22	SSH	Fornisce l'accesso SSH all'host del connettore
80	HTTP	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
443	HTTPS	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Porta	Protocollo	Destinazione	Scopo
Active Directory	88	TCP	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	139	TCP	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP	Insieme di strutture di Active Directory	LDAP
	445	TCP	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	137	UDP	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	464	UDP	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	443	HTTPS	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	3000	TCP	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	53	UDP	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Regole per il connettore in GCP

Le regole firewall per il connettore richiedono regole sia in entrata che in uscita.

Regole in entrata

L'origine delle regole in entrata nelle regole firewall predefinite è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Le regole firewall predefinite per il connettore aprono tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Le regole firewall predefinite per il connettore includono le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API a GCP e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Creazione di un connettore in AWS da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in AWS direttamente da Cloud Manager. È inoltre possibile scegliere di "Creare il connettore da AWS Marketplace", o a. "scaricare il software e installarlo sul proprio

host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

Impostazione delle autorizzazioni AWS per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, è necessario assicurarsi che l'account AWS disponga delle autorizzazioni corrette.

Fasi

1. Scaricare la policy di Connector IAM dal seguente percorso:

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

2. Dalla console AWS IAM, creare una policy personalizzata copiando e incollando il testo dal criterio IAM del connettore.
3. Collegare il criterio creato nel passaggio precedente all'utente IAM che creerà il connettore da Cloud Manager.

Risultato

L'utente AWS dispone ora delle autorizzazioni necessarie per creare il connettore da Cloud Manager. Quando richiesto da Cloud Manager, devi specificare le chiavi di accesso AWS per questo utente.

Creazione di un connettore in AWS

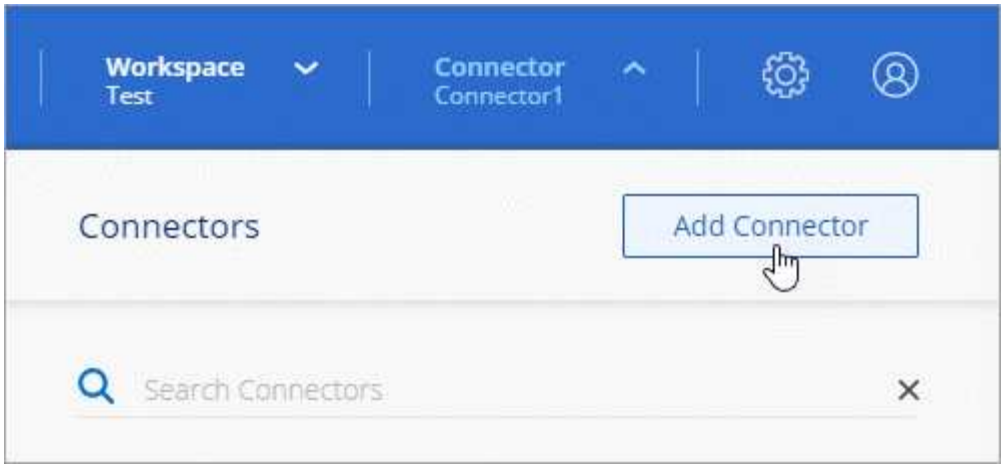
Cloud Manager consente di creare un connettore in AWS direttamente dalla relativa interfaccia utente.

Di cosa hai bisogno

- Una chiave di accesso AWS e una chiave segreta per un utente IAM che dispone di "autorizzazioni richieste".
- VPC, subnet e coppia di chiavi nella regione AWS desiderata.

Fasi

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).



2. Fare clic su **Let's Start**.
3. Scegli **Amazon Web Services** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".
4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Fornire le informazioni richieste:
   - **AWS Credentials**: Immettere un nome per l'istanza e specificare la chiave di accesso AWS e la chiave segreta che soddisfano i requisiti di autorizzazione.
   - **Location**: Specificare una regione AWS, un VPC e una subnet per l'istanza.
   - **Rete**: Selezionare la coppia di chiavi da utilizzare con l'istanza, se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

     Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.
6. Fare clic su **Create** (Crea).

   L'istanza dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

Al termine

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".

Creazione di un connettore in Azure da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior

parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in Azure direttamente da Cloud Manager. È inoltre possibile scegliere di "Creare il connettore da Azure Marketplace", o a. "scaricare il software e installarlo sul proprio host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

Impostazione delle autorizzazioni Azure per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, devi assicurarti che il tuo account Azure disponga delle autorizzazioni corrette.

Fasi

1. Creare un ruolo personalizzato utilizzando il criterio Azure per il connettore:

   a. Scaricare il "Policy di Azure per il connettore".

   Fare clic con il pulsante destro del mouse sul collegamento e fare clic su **Save link as…** (Salva collegamento con nome…) per scaricare il file.

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

   Esempio

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   ],
   ```

   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_Setup_As_Service_Azure.json
   ```

   Ora dovresti avere un ruolo personalizzato chiamato *Azure SetupAsService*.

2. Assegnare il ruolo all'utente che implementerà il connettore da Cloud Manager:

   a. Aprire il servizio **Subscriptions** e selezionare l'abbonamento dell'utente.

   b. Fare clic su **controllo di accesso (IAM)**.

   c. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:

      - Selezionare il ruolo **Azure SetupAsService**.

Azure SetupAsService è il nome predefinito fornito in "Policy di implementazione del connettore per Azure". Se si sceglie un nome diverso per il ruolo, selezionare il nome desiderato.

- Assegnare l'accesso a un utente, un gruppo o un'applicazione * di Azure ad.
- Selezionare l'account utente.
- Fare clic su **Save** (Salva).

Risultato

L'utente Azure dispone ora delle autorizzazioni necessarie per implementare il connettore da Cloud Manager.

Creazione di un connettore in Azure

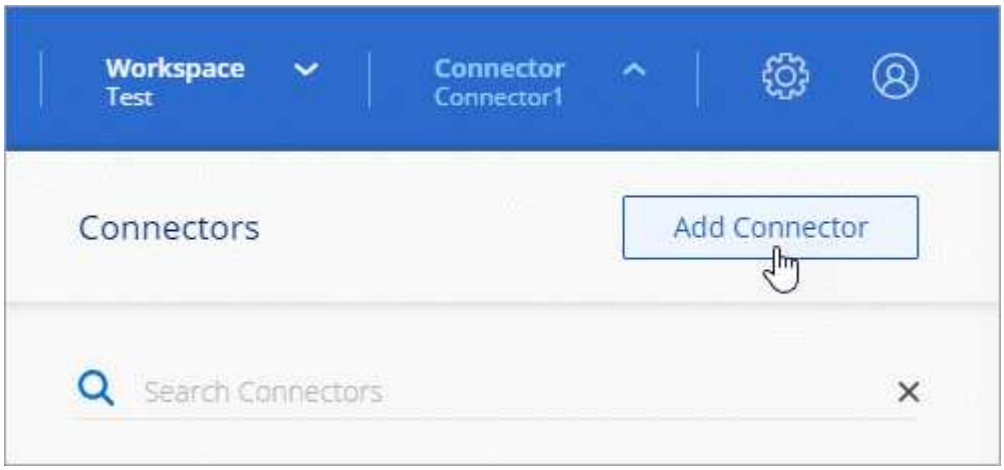
Cloud Manager consente di creare un connettore in Azure direttamente dalla sua interfaccia utente.

Di cosa hai bisogno

- Il "autorizzazioni richieste" Per il tuo account Azure.
- Un abbonamento Azure.
- Una VNET e una subnet nella regione Azure desiderata.

Fasi

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).



2. Fare clic su **Let's Start**.
3. Scegli **Microsoft Azure** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".

4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Se richiesto, accedere all'account Microsoft, che dovrebbe disporre delle autorizzazioni necessarie per creare la macchina virtuale.

Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.

Se hai già effettuato l'accesso a un account Azure, Cloud Manager utilizzerà automaticamente tale account. Se disponi di più account, potrebbe essere necessario prima disconnettersi per assicurarsi di utilizzare l'account corretto.

6. Fornire le informazioni richieste:
   - **VM Authentication**: Immettere un nome per la macchina virtuale e un nome utente e una password o una chiave pubblica.
   - **Basic Settings** (Impostazioni di base): Scegliere un abbonamento Azure, un'area Azure e se creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse esistente.
   - **Rete**: Scegliere un VNET e una subnet, se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Security Group**: Scegliere se creare un nuovo gruppo di sicurezza o se selezionare un gruppo di sicurezza esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

     Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

7. Fare clic su **Create** (Crea).

   La macchina virtuale dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

Al termine

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".

Creazione di un connettore in GCP da Cloud Manager

Un account Admin deve implementare un *connettore* prima di poter utilizzare la maggior parte delle funzionalità di Cloud Manager. "Scopri quando è necessario un connettore". Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Questa pagina descrive come creare un connettore in GCP direttamente da Cloud Manager. È inoltre possibile scegliere di "scaricare il software e installarlo sul proprio host".

Questi passaggi devono essere completati da un utente che ha il ruolo di amministratore dell'account. Un amministratore dell'area di lavoro non può creare un connettore.

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiederà di creare un connettore se non ne hai ancora uno.

Impostazione delle autorizzazioni GCP per creare un connettore

Prima di poter implementare un connettore da Cloud Manager, è necessario assicurarsi che l'account GCP disponga delle autorizzazioni corrette e che sia impostato un account di servizio per la macchina virtuale del connettore.

Fasi

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

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

2. Impostare un account di servizio che disponga delle autorizzazioni necessarie per creare e gestire i sistemi Cloud Volumes ONTAP nei progetti.

   Questo account del servizio verrà associato alla macchina virtuale del connettore quando lo si crea da Cloud Manager.

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

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

   b. "Creare un account di servizio GCP e applicare il ruolo personalizzato appena creato".

   c. Se si desidera implementare Cloud Volumes ONTAP in altri progetti, "Concedere l'accesso aggiungendo l'account di servizio con il ruolo Cloud Manager a quel progetto". Dovrai ripetere questo passaggio per ogni progetto.

Risultato

L'utente GCP dispone ora delle autorizzazioni necessarie per creare il connettore da Cloud Manager e l'account del servizio per la macchina virtuale del connettore è impostato.

Abilitazione delle API di Google Cloud

Per implementare il connettore e Cloud Volumes ONTAP sono necessarie diverse API.

Fase

1. "Abilita le seguenti API di Google Cloud nel tuo progetto".
   - API di Cloud Deployment Manager V2
   - API Cloud Logging
   - API Cloud Resource Manager
   - API di Compute Engine
   - API IAM (Identity and Access Management)

Creazione di un connettore in GCP

Cloud Manager consente di creare un connettore in GCP direttamente dalla sua interfaccia utente.

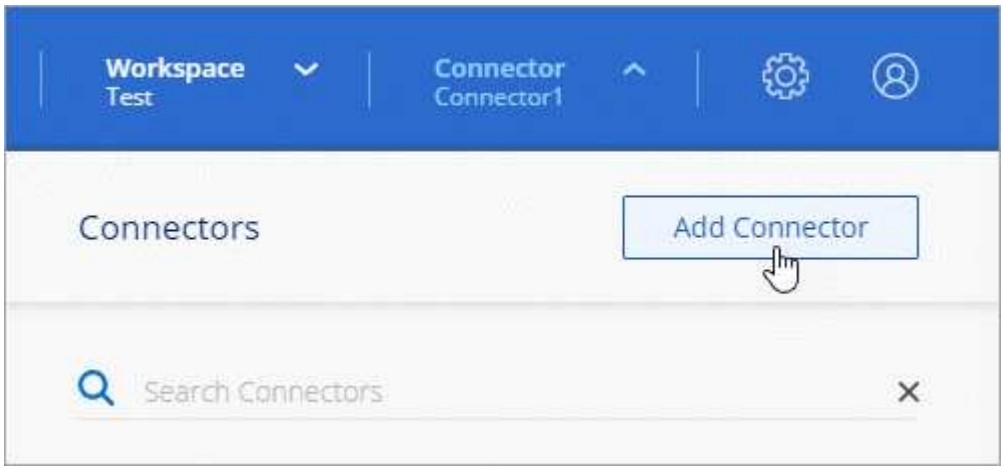
Di cosa hai bisogno

- Il "autorizzazioni richieste" Per il tuo account Google Cloud.

- Un progetto Google Cloud.
- Account di servizio che dispone delle autorizzazioni necessarie per creare e gestire Cloud Volumes ONTAP.
- Un VPC e una subnet nell'area di Google Cloud desiderata.

Fasi

1. Se si sta creando il primo ambiente di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni. In caso contrario, fare clic sull'elenco a discesa **Connector** e selezionare **Add Connector** (Aggiungi connettore).



2. Fare clic su **Let's Start**.
3. Scegli **Google Cloud Platform** come tuo cloud provider.

   Tenere presente che il connettore deve disporre di una connessione di rete con il tipo di ambiente di lavoro che si sta creando e con i servizi che si intende abilitare.

   "Scopri di più sui requisiti di rete per il connettore".

4. Consulta le informazioni necessarie e fai clic su **continua**.
5. Se richiesto, accedere all'account Google, che dovrebbe disporre delle autorizzazioni necessarie per creare l'istanza della macchina virtuale.

   Il modulo è di proprietà e ospitato da Google. Le tue credenziali non vengono fornite a NetApp.

6. Fornire le informazioni richieste:
   - **Basic Settings** (Impostazioni di base): Immettere un nome per l'istanza della macchina virtuale e specificare un account di progetto e servizio con le autorizzazioni richieste.
   - **Location**: Specificare una regione, una zona, un VPC e una subnet per l'istanza.
   - **Network** (rete): Scegliere se attivare un indirizzo IP pubblico e, facoltativamente, specificare una configurazione proxy.
   - **Firewall Policy**: Scegliere se creare una nuova policy firewall o se selezionare una policy firewall esistente che consenta l'accesso HTTP, HTTPS e SSH in entrata.

     Non c'è traffico in entrata verso il connettore, a meno che non venga avviato. HTTP e HTTPS forniscono l'accesso a "UI locale", che utilizzerai in rare circostanze. SSH è necessario solo se è necessario connettersi all'host per la risoluzione dei problemi.

7. Fare clic su **Create** (Crea).

   L'istanza dovrebbe essere pronta in circa 7 minuti. Si consiglia di rimanere sulla pagina fino al completamento del processo.

Al termine

È necessario associare un connettore alle aree di lavoro in modo che gli amministratori dell'area di lavoro possano utilizzare tali connettori per creare sistemi Cloud Volumes ONTAP. Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita. "Scopri di più".

Dove andare

Dopo aver effettuato l'accesso e configurato Cloud Manager, gli utenti possono iniziare a creare e scoprire ambienti di lavoro.

- "Inizia a utilizzare Cloud Volumes ONTAP per AWS"
- "Inizia a utilizzare Cloud Volumes ONTAP per Azure"
- "Inizia a utilizzare Cloud Volumes ONTAP per Google Cloud"
- "Configurare Azure NetApp Files"
- "Impostare Cloud Volumes Service per AWS"
- "Scopri un cluster ONTAP on-premise"
- "Scopri i bucket Amazon S3"

Se sei un amministratore, puoi gestire le impostazioni di Cloud Manager dopo aver creato il primo connettore.

- "Scopri di più sui connettori"
- "Gestire un certificato HTTPS per un accesso sicuro"
- "Configurare le impostazioni del proxy"

Gestire Cloud Volumes ONTAP

Scopri

Scopri di più su Cloud Volumes ONTAP

Cloud Volumes ONTAP consente di ottimizzare i costi e le performance del cloud storage, migliorando al contempo protezione, sicurezza e conformità dei dati.

Cloud Volumes ONTAP è un'appliance di storage solo software che esegue il software di gestione dei dati ONTAP nel cloud. Offre storage di livello Enterprise con le seguenti funzionalità principali:

- Efficienza dello storage

  Sfrutta la deduplica dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi dello storage.

- Alta disponibilità

  Garantisci l'affidabilità aziendale e le operazioni continue in caso di guasti nel tuo ambiente cloud.

- Protezione 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.

  Cloud Volumes ONTAP si integra anche con Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.

- Tiering dei dati

  Passa tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.

- Coerenza applicativa

  Garantire la coerenza delle copie Snapshot di NetApp con NetApp SnapCenter.

- Sicurezza dei dati

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

- Controlli di conformità alla privacy

  L'integrazione con la conformità al cloud ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

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

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

"Scopri di più su Cloud Volumes ONTAP"

Storage

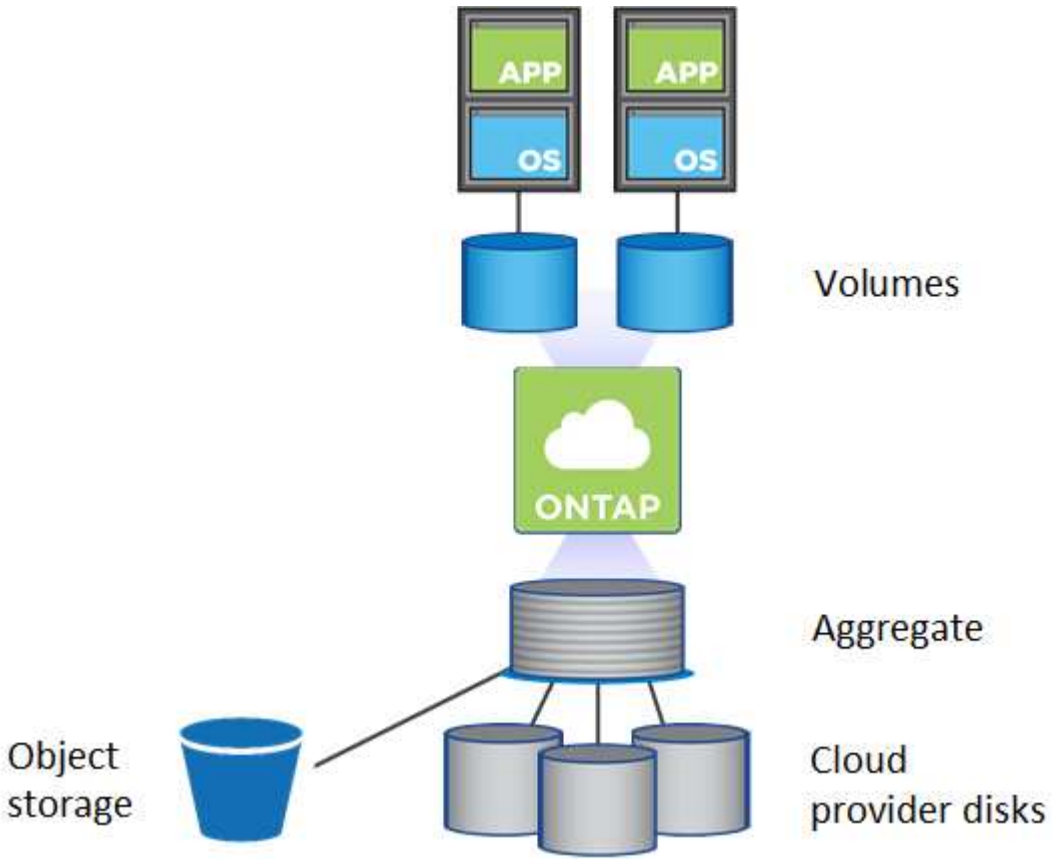
Dischi e aggregati

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

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.

Panoramica

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



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

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

Storage AWS

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

Storage EBS

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

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

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

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

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

Storage NVMe locale

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

Link correlati

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

Storage Azure

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

Sistemi a nodo singolo

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

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.

- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

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

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

Coppie HA

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

Link correlati

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

Storage GCP

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

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

Link correlati

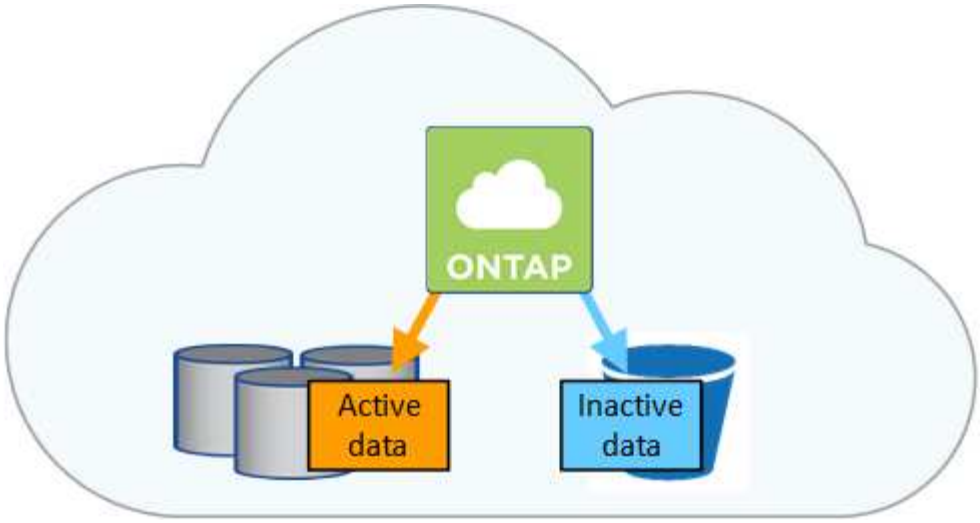
- "Documentazione di Google Cloud Platform: Opzioni di storage"
- "Esaminare i limiti di storage per Cloud Volumes ONTAP in GCP"

Tipo RAID

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

Panoramica sul tiering dei dati

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



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

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

Tiering dei dati in AWS

Quando si abilita il tiering dei dati in AWS, Cloud Volumes ONTAP utilizza EBS come Tier di performance per i dati hot e AWS S3 come Tier di capacità per i dati inattivi.

Tier di performance

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

Tier di capacità

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

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

Classi di storage

La classe di storage predefinita per i dati Tiered in AWS è *Standard*. Se non si prevede di accedere ai dati inattivi, è possibile ridurre i costi di storage cambiando la classe di storage in una delle seguenti opzioni: *Intelligent Tiering*, *One-zone infrequent Access* o *Standard-infrequent Access*. Quando si modifica la classe di storage, i dati inattivi vengono avviati nella classe di storage Standard e vengono passati alla classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi tenere in considerazione questo aspetto prima di modificare la classe di storage. "Scopri di più sulle classi di storage Amazon S3".

È possibile selezionare una classe di storage quando si crea l'ambiente di lavoro e modificarla in qualsiasi momento. Per ulteriori informazioni sulla modifica della classe di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

Tiering dei dati in Azure

Quando abiliti il tiering dei dati in Azure, Cloud Volumes ONTAP utilizza i dischi gestiti da Azure come Tier di performance per i dati hot e lo storage Blob Azure come Tier di capacità per i dati inattivi.

Tier di performance

Il Tier di performance può essere SSD o HDD.

Tier di capacità

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

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

Tier di accesso allo storage

Il Tier di accesso allo storage predefinito per i dati a più livelli in Azure è il *hot* Tier. Se non intendi accedere ai dati inattivi, puoi ridurre i costi di storage passando al Tier di storage *COOL*. Quando si modifica il Tier di storage, i dati inattivi vengono avviati nel Tier di storage hot e vengono passati al Tier di storage cool, se non si accede ai dati dopo 30 giorni.

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

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in qualsiasi momento. Per ulteriori informazioni sulla modifica del Tier di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

Il Tier di accesso allo storage per il tiering dei dati è esteso a tutto il sistema, non per volume.

Tiering dei dati in GCP

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

Tier di performance

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

Tier di capacità

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

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

Classi di storage

La classe di storage predefinita per i dati a più livelli è la classe *Standard Storage*. Se l'accesso ai dati non è frequente, puoi ridurre i costi di storage passando a *Nearline Storage* o *Coldline Storage*. Quando si modifica la classe di storage, i dati inattivi vengono avviati nella classe di storage standard e vengono

passati alla classe di storage selezionata, se non si accede ai dati dopo 30 giorni.

I costi di accesso sono più elevati se si accede ai dati, quindi tenere in considerazione questo aspetto prima di modificare la classe di storage. "Scopri di più sulle classi di storage per Google Cloud Storage".

È possibile selezionare un Tier di storage quando si crea l'ambiente di lavoro e modificarlo in qualsiasi momento. Per ulteriori informazioni sulla modifica della classe di storage, vedere "Tiering dei dati inattivi su storage a oggetti a basso costo".

La classe di storage per il tiering dei dati è estesa a tutto il sistema, non per volume.

Tiering dei dati e limiti di capacità

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

Policy di tiering dei volumi

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

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

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

Solo Snapshot

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

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

Tutto

Tutti i dati (non inclusi i metadati) vengono immediatamente contrassegnati come cold e tiered per lo storage a oggetti il più presto possibile. Non è necessario attendere 48 ore affinché i nuovi blocchi di un volume si raffreddino. Tenere presente che i blocchi situati nel volume prima dell'impostazione del criterio All richiedono 48 ore per diventare freddi.

In caso di lettura, i blocchi di dati cold nel Tier cloud restano freddi e non vengono riscritti nel Tier di performance. Questo criterio è disponibile a partire da ONTAP 9.6.

Automatico

Dopo che un aggregato ha raggiunto la capacità del 50%, Cloud Volumes ONTAP esegue il Tier dei blocchi di dati cold in un volume fino a raggiungere un livello di capacità. I dati cold non includono solo le copie Snapshot, ma anche i dati cold user dal file system attivo. Il periodo di raffreddamento è di circa 31 giorni.

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

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

Nessuno

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

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

La disattivazione di Cloud Volumes ONTAP influisce sul periodo di raffreddamento

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

- Auto: 31 giorni
- Solo snapshot: 2 giorni

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

Impostazione del tiering dei dati

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

Gestione dello storage

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

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

Provisioning dello storage

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

Provisioning semplificato

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

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

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

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

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

Selezione delle dimensioni dei dischi per gli aggregati in AWS

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

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

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

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

Allocazione avanzata

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

Gestione della capacità

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

Gestione automatica della capacità

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

I seguenti esempi illustrano il funzionamento di questa modalità:

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

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

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

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

Gestione delle LUN con gestione automatica della capacità

La gestione automatica della capacità di Cloud Manager non si applica alle LUN. Quando Cloud Manager crea un LUN, disattiva la funzione di crescita automatica.

Gestione degli inode con gestione automatica della capacità

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

Gestione manuale della capacità

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

Flash cache

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

Cos'è Flash cache?

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

Istanze supportate in AWS

Selezionare uno dei seguenti tipi di istanze EC2 con un sistema Cloud Volumes ONTAP Premium o BYOL nuovo o esistente:

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

Tipo di VM supportato in Azure

Selezionare il tipo di macchina virtuale Standard_L8s_v2 con un sistema BYOL Cloud Volumes ONTAP a nodo singolo in Azure.

Limitazioni

- La compressione deve essere disattivata su tutti i volumi per sfruttare i miglioramenti delle prestazioni di Flash cache.

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

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

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.

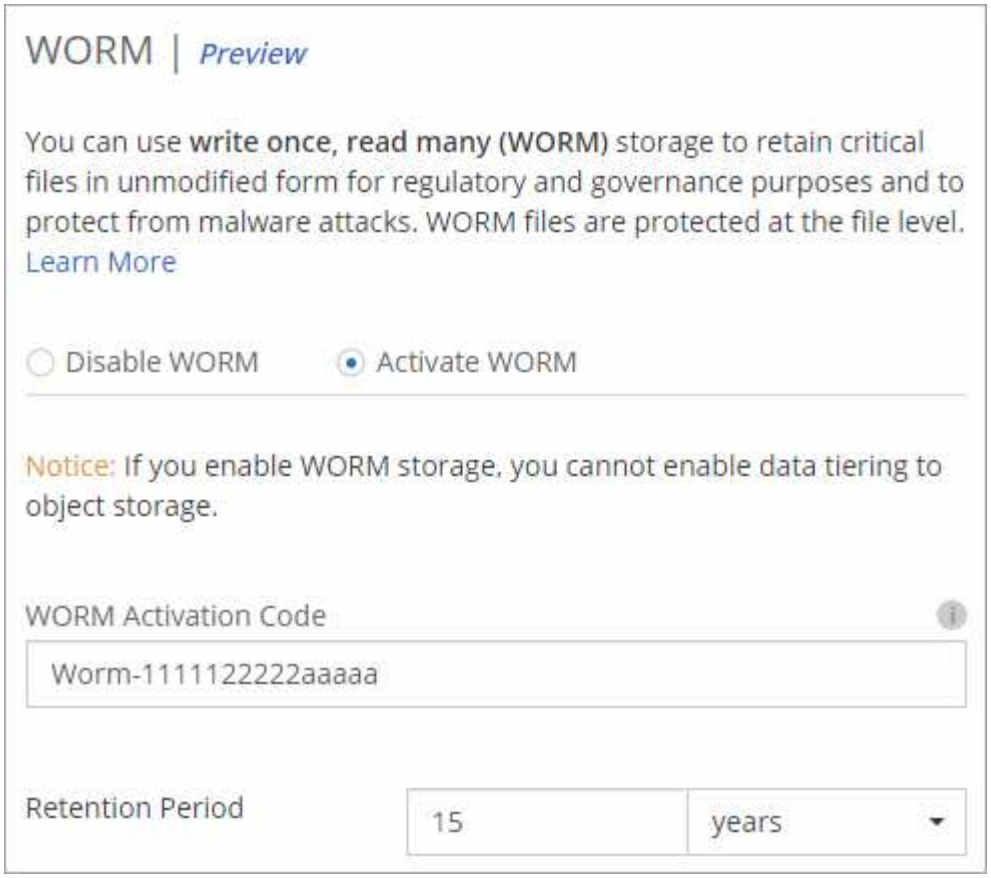
Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari.

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.
- Per abilitare lo storage WORM, è necessario disattivare il backup su cloud.

Coppie ad alta disponibilità

Coppie ad alta disponibilità in AWS

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

sincrono tra i due nodi.

Panoramica

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

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

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

Takeover e giveback dello storage

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

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

RPO e RTO

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

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

Modelli di implementazione HA

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

Cloud Volumes ONTAP ha in più zone di disponibilità

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

Accesso ai dati NFS e CIFS

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

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

Prima di implementare una configurazione ha in più zone di disponibilità, è necessario esaminare i requisiti per gli indirizzi IP mobili e le tabelle di routing. È necessario specificare gli indirizzi IP mobili quando si implementa la configurazione. Gli indirizzi IP privati vengono creati automaticamente da Cloud Manager.

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

Accesso ai dati iSCSI

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

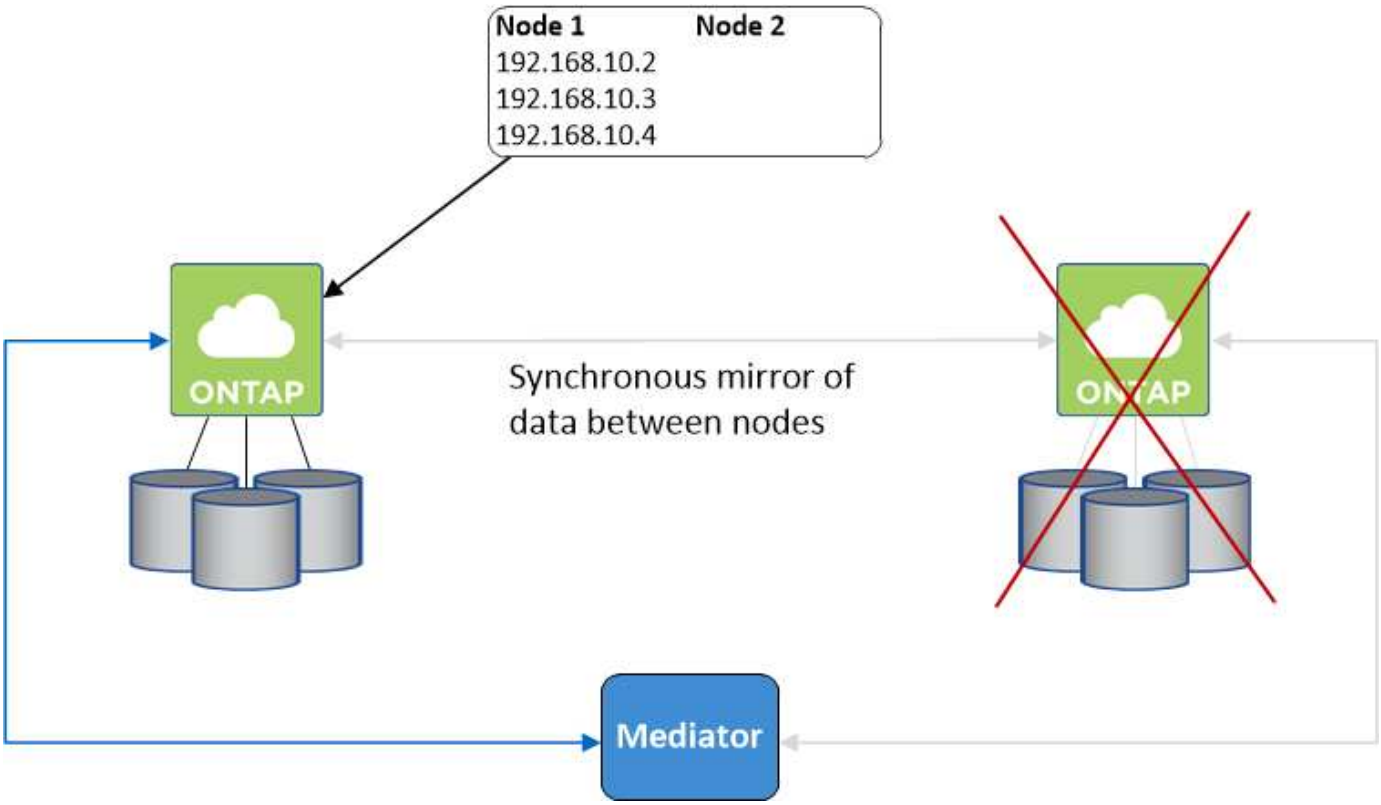
Takeover e giveback dello storage per iSCSI

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

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

Takeover e giveback dello storage per NAS

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



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

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

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

Cloud Volumes ONTAP ha in una singola zona di disponibilità

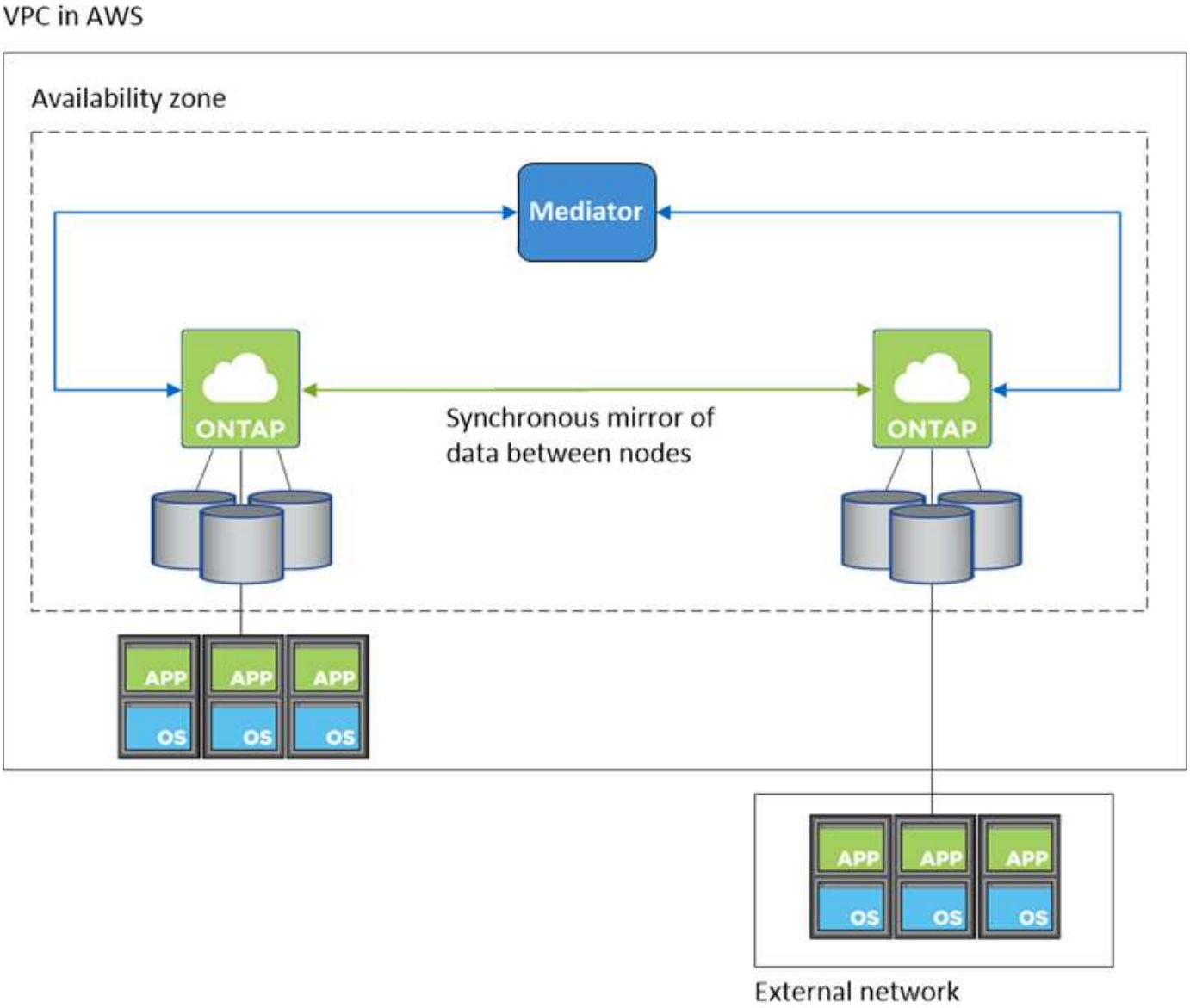
L'implementazione di una configurazione ha in una singola zona di disponibilità (AZ) può garantire un'elevata disponibilità dei dati in caso di guasto di un'istanza che esegue un nodo Cloud Volumes ONTAP. Tutti i dati sono accessibili in modo nativo dall'esterno del VPC.

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

Accesso ai dati

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

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



Takeover e giveback dello storage

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

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

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

Come funziona lo storage in una coppia ha

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

Allocazione dello storage

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

Configurazioni dello storage

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

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

Aspettative di performance per una configurazione ha

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

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

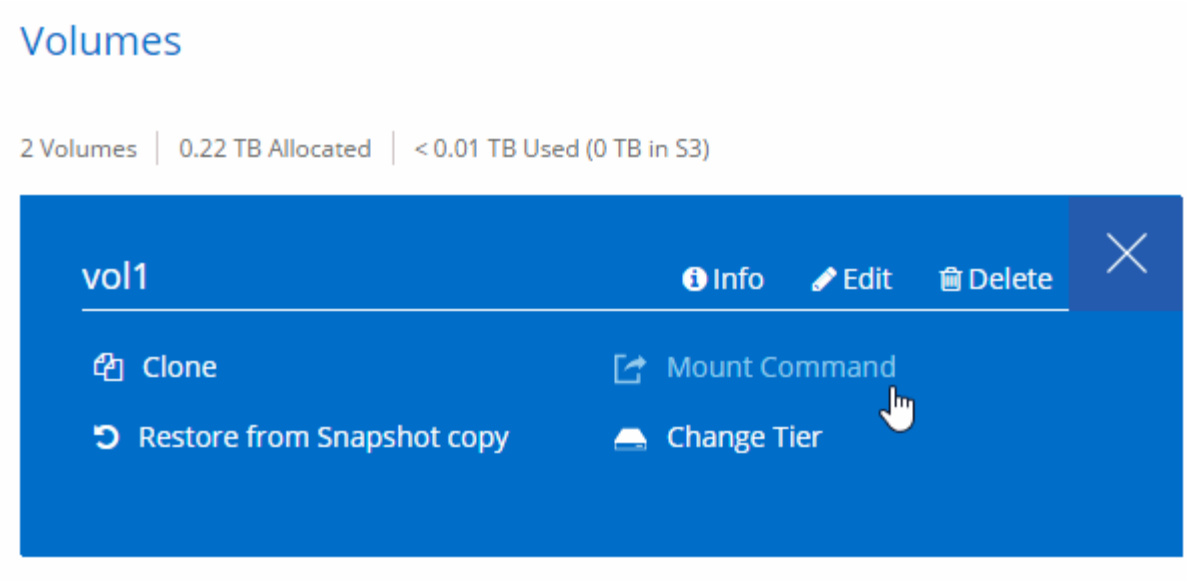
Per ulteriori informazioni sulle prestazioni di Cloud Volumes ONTAP, vedere "Performance".

Accesso client allo storage

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

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

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

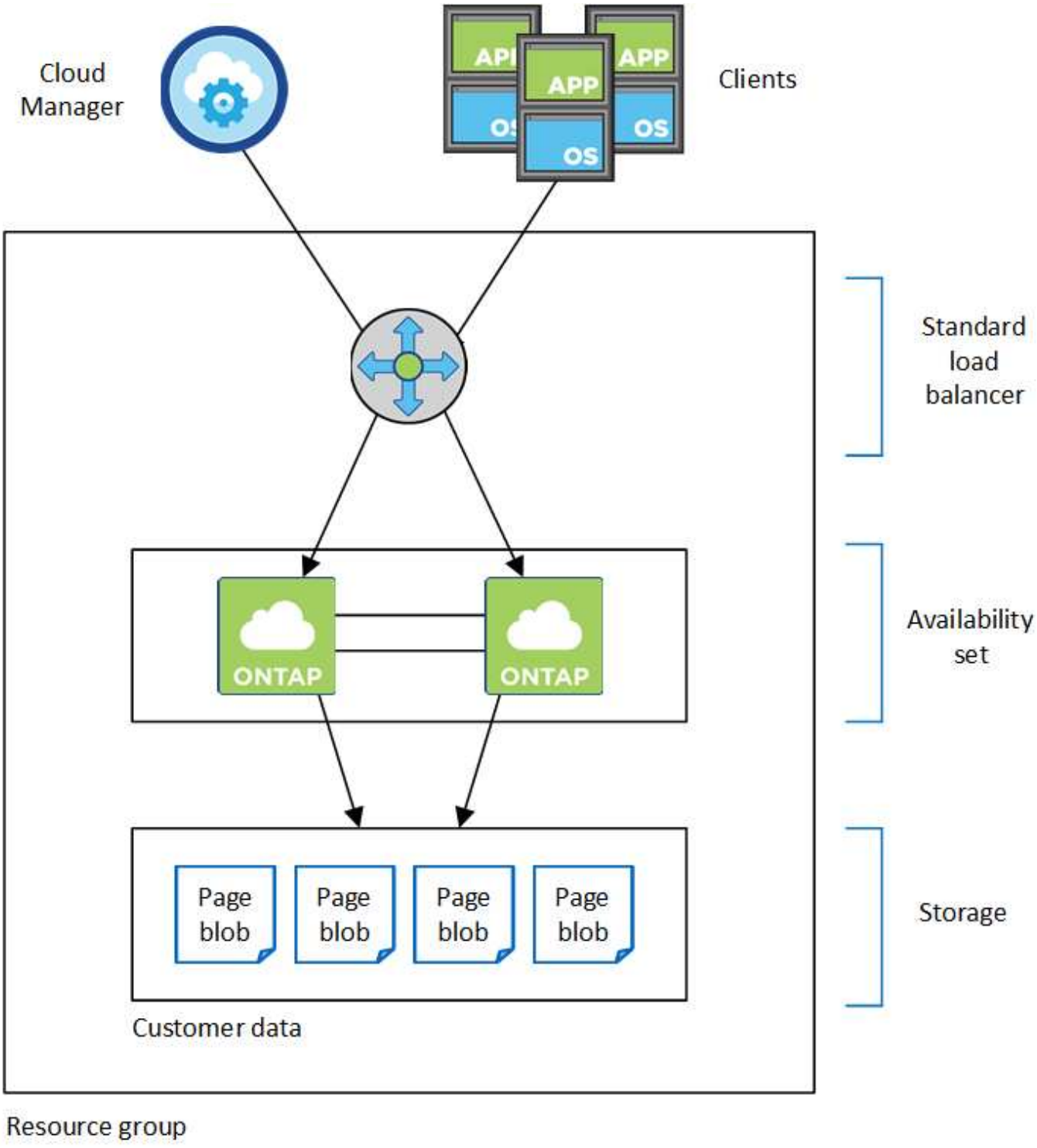


Coppie ad alta disponibilità in Azure

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

Componenti HA

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



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

Bilanciamento del carico standard Azure

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

Set di disponibilità

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

Dischi

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

Account storage

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

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

- Per il tiering dei dati sullo storage Azure Blob è necessario un account storage.
- A partire da Cloud Volumes ONTAP 9.7, gli account storage creati da Cloud Manager per le coppie ha sono account storage v2 generici.
- Durante la creazione di un ambiente di lavoro, è possibile attivare una connessione HTTPS da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage Azure. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

RPO e RTO

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

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

Takeover e giveback dello storage

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

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

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

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

Configurazioni dello storage

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

Limitazioni DI HA

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

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

  "Consulta l'elenco delle aree Azure supportate".

"Scopri come implementare un sistema ha in Azure".

Valutazione

È possibile valutare Cloud Volumes ONTAP prima di pagare il software. Il modo più comune è quello di lanciare LA versione PAYGO del tuo primo sistema Cloud Volumes ONTAP per ottenere una prova gratuita di 30 giorni. Una licenza BYOL di valutazione è anche un'opzione.

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.

30 giorni di prova gratuita per PAYGO

È disponibile una versione di prova gratuita di 30 giorni se si prevede di pagare per Cloud Volumes ONTAP a consumo. Puoi iniziare una prova gratuita di 30 giorni di Cloud Volumes ONTAP da Cloud Manager creando il tuo primo sistema Cloud Volumes ONTAP nell'account del pagante.

Non sono previsti costi di licenza software oraria per l'istanza, ma i costi di infrastruttura del provider cloud continuano a essere applicati.

Una versione di prova gratuita viene convertita automaticamente in un abbonamento oraria a pagamento alla scadenza. Se si termina l'istanza entro il limite di tempo, l'istanza successiva che si implementa non fa parte della versione di prova gratuita (anche se viene implementata entro 30 giorni).

Le versioni di prova pay-as-you-go vengono assegnate tramite un cloud provider e non sono estendibili in alcun modo.

Licenze di valutazione per BYOL

Una licenza BYOL di valutazione è un'opzione per i clienti che prevedono di pagare per Cloud Volumes ONTAP acquistando una licenza denominata da NetApp. Puoi ottenere una licenza di valutazione dal tuo account team, dal tuo Sales Engineer o dal tuo partner.

La chiave di valutazione è valida per 30 giorni e può essere utilizzata più volte, ciascuna per 30 giorni (indipendentemente dal giorno di creazione).

Alla fine di 30 giorni, si verificheranno arresti giornalieri, quindi è meglio pianificare in anticipo. È possibile applicare una nuova licenza BYOL alla licenza di valutazione per un aggiornamento in-place (ciò richiede il riavvio dei sistemi a nodo singolo). I dati ospitati vengono eliminati **non** al termine del periodo di prova.

Non è possibile aggiornare il software Cloud Volumes ONTAP quando si utilizza una licenza di valutazione.

Licensing

Ogni sistema Cloud Volumes ONTAP BYOL deve disporre di una licenza di sistema con un abbonamento attivo. Cloud Manager semplifica il processo gestendo le licenze e avvisandovi prima della scadenza. Le licenze BYOL sono disponibili anche per il backup nel cloud.

Licenze di sistema BYOL

È possibile acquistare più licenze per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TB di capacità. Ad esempio, è possibile acquistare due licenze per allocare fino a 736 TB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare quattro licenze per ottenere fino a 1.4 PB.

Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia ha è illimitato.

Tenere presente che i limiti dei dischi possono impedire di raggiungere il limite di capacità utilizzando solo i dischi. È possibile superare il limite di dischi di "tiering dei dati inattivi sullo storage a oggetti". Per informazioni sui limiti dei dischi, fare riferimento a. "Limiti di storage nelle note di rilascio di Cloud Volumes ONTAP".

Gestione delle licenze per un nuovo sistema

Quando si crea un sistema BYOL, Cloud Manager richiede il numero di serie della licenza e l'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 "Gestione delle licenze BYOL per Cloud Volumes ONTAP".

Avviso di 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 "Gestione delle licenze BYOL per Cloud Volumes ONTAP".

Licenze di backup BYOL

Una licenza di backup BYOL consente di acquistare una licenza da NetApp per utilizzare Backup to Cloud per un determinato periodo di tempo e per una quantità massima di spazio di backup. Una volta raggiunto il limite, è necessario rinnovare la licenza.

"Scopri di più sulla licenza BYOL per il backup nel cloud".

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:

- Soluzioni di crittografia NetApp (NVE e NAE)
- Servizio di gestione delle chiavi AWS
- Azure Storage Service Encryption
- Crittografia predefinita di Google Cloud Platform

È possibile utilizzare le soluzioni di crittografia NetApp con crittografia nativa da AWS, Azure o GCP, che crittografano i dati a livello di hypervisor. In questo modo si fornirebbe una doppia crittografia, che potrebbe essere utile per i dati molto sensibili. Quando si accede ai dati crittografati, questi vengono crittografati due volte, una volta a livello di hypervisor (utilizzando le chiavi del cloud provider) e poi di nuovo utilizzando le soluzioni di crittografia NetApp (utilizzando le chiavi di un gestore di chiavi esterno).

Soluzioni di crittografia NetApp (NVE e NAE)

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp (NVE) e la crittografia aggregata NetApp (NAE) con un gestore di chiavi esterno. NVE e NAE sono soluzioni basate su software che consentono la crittografia dei volumi (data-at-rest) conforme a FIPS 140-2.

- NVE crittografa i dati inattivi un volume alla volta. Ogni volume di dati dispone di una chiave di crittografia univoca.
- NAE è un'estensione di NVE, che crittografa i dati per ogni volume e i volumi condividono una chiave nell'aggregato. NAE consente inoltre di deduplicare i blocchi comuni di tutti i volumi dell'aggregato.

Sia NVE che NAE utilizzano la crittografia AES a 256 bit.

"Scopri di più su NetApp Volume Encryption e NetApp aggregate Encryption".

A partire da Cloud Volumes ONTAP 9.7, i nuovi aggregati avranno la crittografia aggregata NetApp (NAE) attivata per impostazione predefinita dopo aver configurato un gestore di chiavi esterno. I nuovi volumi che non fanno parte di un aggregato NAE avranno NetApp Volume Encryption (NVE) abilitato per impostazione predefinita (ad esempio, se si dispone di aggregati creati prima di impostare un gestore di chiavi esterno).

La configurazione di un gestore di chiavi supportato è l'unica operazione necessaria. Per istruzioni sulla configurazione, vedere "Crittografia dei volumi con le soluzioni di crittografia NetApp".

Servizio di gestione delle chiavi AWS

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

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

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

Azure Storage Service Encryption

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

È possibile crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. Questa funzionalità è supportata tramite le API di Cloud Manager.

È sufficiente aggiungere quanto segue alla richiesta API quando si crea il sistema a nodo singolo:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

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

Crittografia predefinita di Google Cloud Platform

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

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

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".

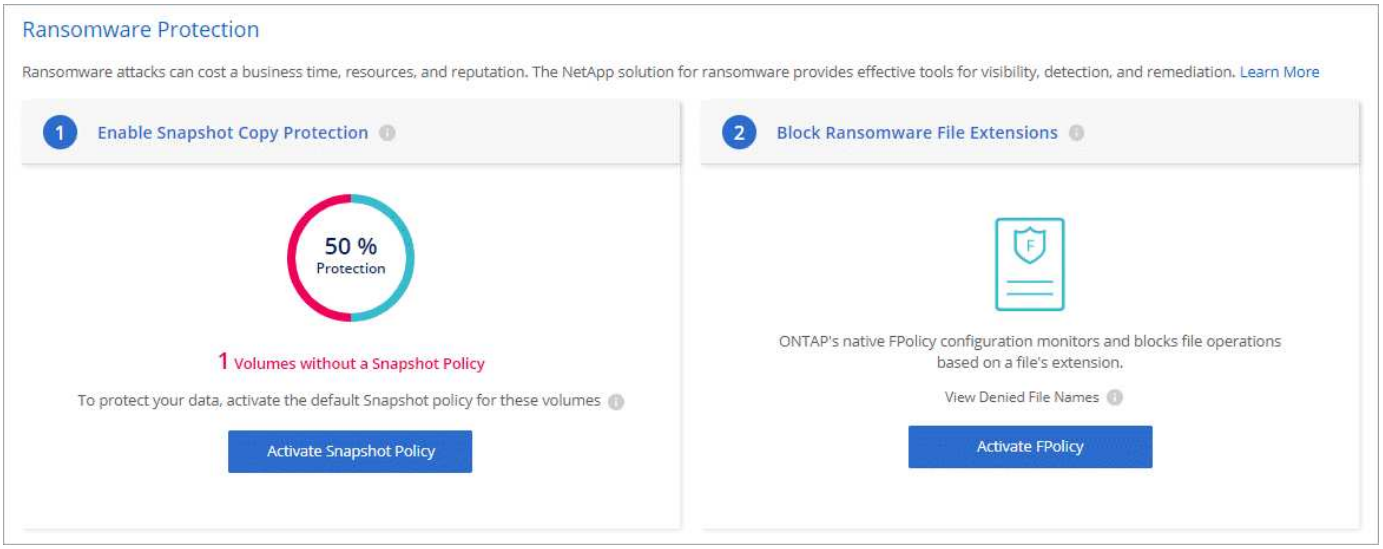
Protezione ransomware

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.

- Cloud Volumes ONTAP per AWS

  "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni".

- Cloud Volumes ONTAP per Microsoft Azure

  "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi".

- Cloud Volumes ONTAP per Google Cloud

  "Report tecnico NetApp 4816: Caratterizzazione delle performance di Cloud Volumes ONTAP per Google Cloud".

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.

Valori predefiniti

- Cloud Volumes ONTAP è disponibile come sistema a nodo singolo in AWS, Azure e GCP e come coppia ha in AWS e Azure.
- Cloud Manager crea una VM di storage per il servizio dei dati quando implementa Cloud Volumes ONTAP. Alcune configurazioni supportano macchine virtuali storage aggiuntive. "Scopri di più sulla gestione delle VM di storage".
- Cloud Manager installa automaticamente le seguenti licenze ONTAP Feature su Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - NetApp Volume Encryption (solo per sistemi BYOL o PAYGO registrati)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Per impostazione predefinita, vengono create diverse interfacce di rete:
  - Una LIF di gestione del cluster
  - Un LIF intercluster
  - LIF di gestione SVM su sistemi ha in Azure, sistemi a nodo singolo in AWS e, facoltativamente, su sistemi ha in più zone di disponibilità AWS
  - Una LIF di gestione dei nodi
  - Una LIF di dati iSCSI

- Una LIF di dati CIFS e NFS

> Il failover LIF è disattivato per impostazione predefinita per Cloud Volumes ONTAP a causa dei requisiti EC2. La migrazione di una LIF a una porta diversa interrompe la mappatura esterna tra gli indirizzi IP e le interfacce di rete sull'istanza, rendendo la LIF inaccessibile.

- Cloud Volumes ONTAP invia i backup della configurazione al connettore utilizzando HTTPS.

  I backup sono accessibili da https://ipaddress/occm/offboxconfig/ Dove *ipaddress* è l'indirizzo IP dell'host del connettore.

- Cloud Manager imposta alcuni attributi di volume in modo diverso rispetto ad altri strumenti di gestione (ad esempio, System Manager o CLI).

  La tabella seguente elenca gli attributi del volume impostati da Cloud Manager in modo diverso dai valori predefiniti:

Attributo	Valore stabilito da Cloud Manager
Modalità di dimensionamento automatico	crescere
Dimensionamento automatico massimo	1,000% L'amministratore dell'account può modificare questo valore dalla pagina Impostazioni.
Stile di sicurezza	NTFS per CIFS Volumes UNIX per NFS Volumes
Stile garanzia di spazio	nessuno
Autorizzazioni UNIX (solo NFS)	777

  Per informazioni su questi attributi, consulta la pagina man *volume create*.

Dati di boot e root per Cloud Volumes ONTAP

Oltre allo storage per i dati degli utenti, Cloud Manager acquista anche lo storage cloud per i dati di boot e root su ogni sistema Cloud Volumes ONTAP.

AWS

- Due dischi per nodo per i dati di boot e root:
  - 9.7: Disco io1 da 160 GB per i dati di avvio e disco gp2 da 220 GB per i dati root
  - 9.6: Disco io1 da 93 GB per i dati di avvio e disco gp2 da 140 GB per i dati root
  - 9.5: Disco io1 da 45 GB per i dati di avvio e disco gp2 da 140 GB per i dati root

- Un'istantanea EBS per ogni disco di boot e disco root
- Per le coppie ha, un volume EBS per l'istanza Mediator, che è di circa 8 GB

Azure (nodo singolo)

- Tre dischi SSD Premium:
  - Un disco da 10 GB per i dati di avvio
  - Un disco da 140 GB per i dati root
  - Un disco da 128 GB per NVRAM

    Se la macchina virtuale scelta per Cloud Volumes ONTAP supporta gli SSD Ultra, il sistema utilizza un SSD Ultra per la NVRAM, anziché un SSD Premium.
- Un disco HDD standard da 1024 GB per il risparmio dei core
- Uno snapshot Azure per ogni disco di boot e disco root

Azure (coppie ha)

- Due dischi SSD Premium da 10 GB per il volume di boot (uno per nodo)
- Due blob di pagina Premium Storage da 140 GB per il volume root (uno per nodo)
- Due dischi HDD standard da 1024 GB per il risparmio di core (uno per nodo)
- Due dischi SSD Premium da 128 GB per NVRAM (uno per nodo)
- Uno snapshot Azure per ogni disco di boot e disco root

GCP

- Un disco persistente standard da 10 GB per i dati di avvio
- Un disco persistente standard da 64 GB per i dati root
- Un disco persistente standard da 500 GB per NVRAM
- Un disco persistente standard da 216 GB per il risparmio dei core
- Uno snapshot GCP per il disco di boot e il disco root

Dove risiedono i dischi

Cloud Manager definisce lo storage come segue:

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

  Questo disco, che contiene l'immagine di avvio, non è disponibile per Cloud Volumes ONTAP.
- I dati root, che contengono la configurazione del sistema e i log, risiedono in aggr0.
- Il volume root della macchina virtuale di storage (SVM) risiede in aggr1.
- I volumi di dati risiedono anche in aggr1.

Crittografia

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

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

Inizia ad utilizzare AWS

Introduzione a Cloud Volumes ONTAP per AWS

Inizia a utilizzare Cloud Volumes ONTAP per AWS in pochi passaggi.

Creare un connettore

Se non si dispone di un "Connettore" Tuttavia, un amministratore dell'account deve crearne uno. "Scopri come creare un connettore in AWS".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

Configurare la rete

1. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Abilitare l'accesso a Internet in uscita dal VPC di destinazione in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

3. 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.

"Scopri di più sui requisiti di rete".

Configurare AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario assicurarsi che esista una chiave master cliente (CMK) attiva. È inoltre necessario modificare il criterio delle chiavi per ogni CMK

aggiungendo il ruolo IAM che fornisce le autorizzazioni al connettore come *utente chiave*. "Scopri di più".

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro), selezionare il tipo di sistema che si desidera implementare e completare la procedura guidata. "Leggi le istruzioni dettagliate".

Link correlati

- "Valutazione"
- "Creazione di un connettore da Cloud Manager"
- "Avvio di un connettore da AWS Marketplace"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa Cloud Manager con le autorizzazioni AWS"

Pianificazione della configurazione Cloud Volumes ONTAP in AWS

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

Scelta di un tipo di licenza

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

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 in AWS"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP 9.7 in AWS"

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*

Scelta di una configurazione che supporti Flash cache

Alcune configurazioni Cloud Volumes ONTAP in AWS includono lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance. "Scopri di più su Flash cache".

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	

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.

Configurare la rete

Requisiti di rete per Cloud Volumes ONTAP in AWS

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

Requisiti generali 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.

"Scopri come configurare AutoSupport".

Accesso a Internet in uscita per il mediatore ha

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

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

Numero di indirizzi IP

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

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

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

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

Gruppi di sicurezza

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

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

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

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

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

Connessioni a sistemi ONTAP in altre reti

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

DNS e Active Directory per CIFS

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

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

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

Requisiti per coppie 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".

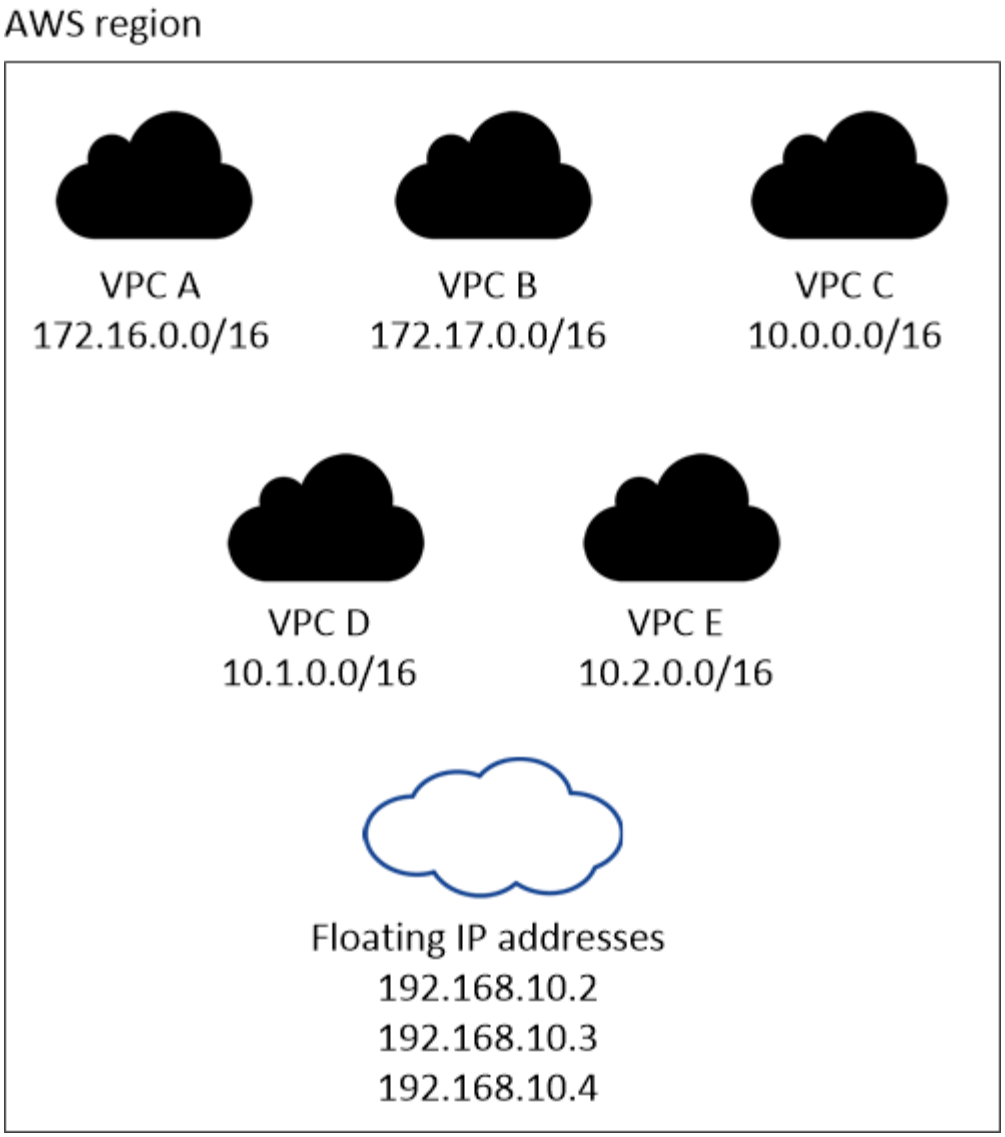
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

> 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".

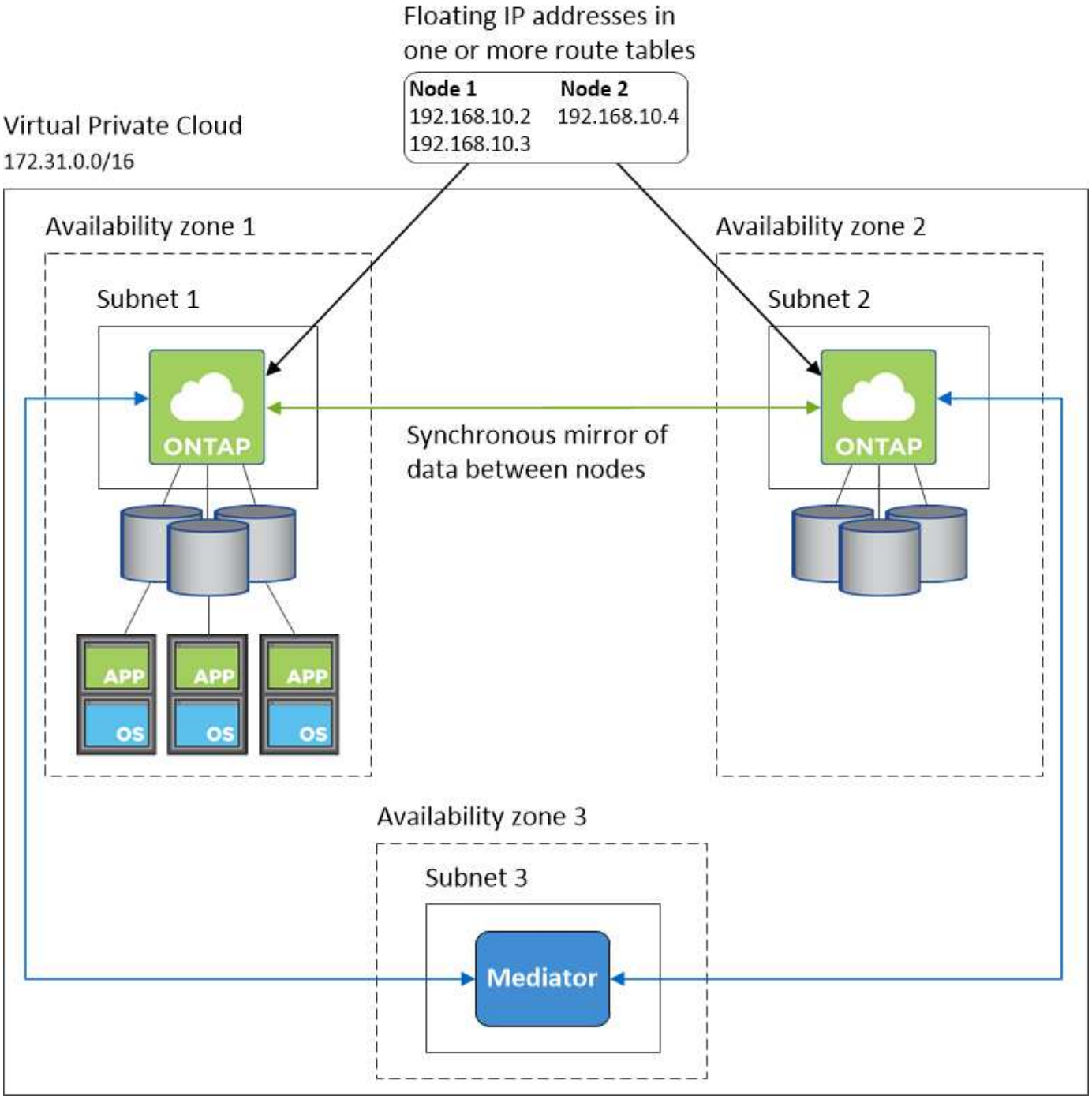
Connessione ai tool di gestione NetApp

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.

Esempio di configurazione ha

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



Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. 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, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

Connessione alle reti di destinazione

Un connettore richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud

Volumes ONTAP.

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

Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse 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.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.

Endpoint	Scopo
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 https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	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.

Endpoint	Scopo
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

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

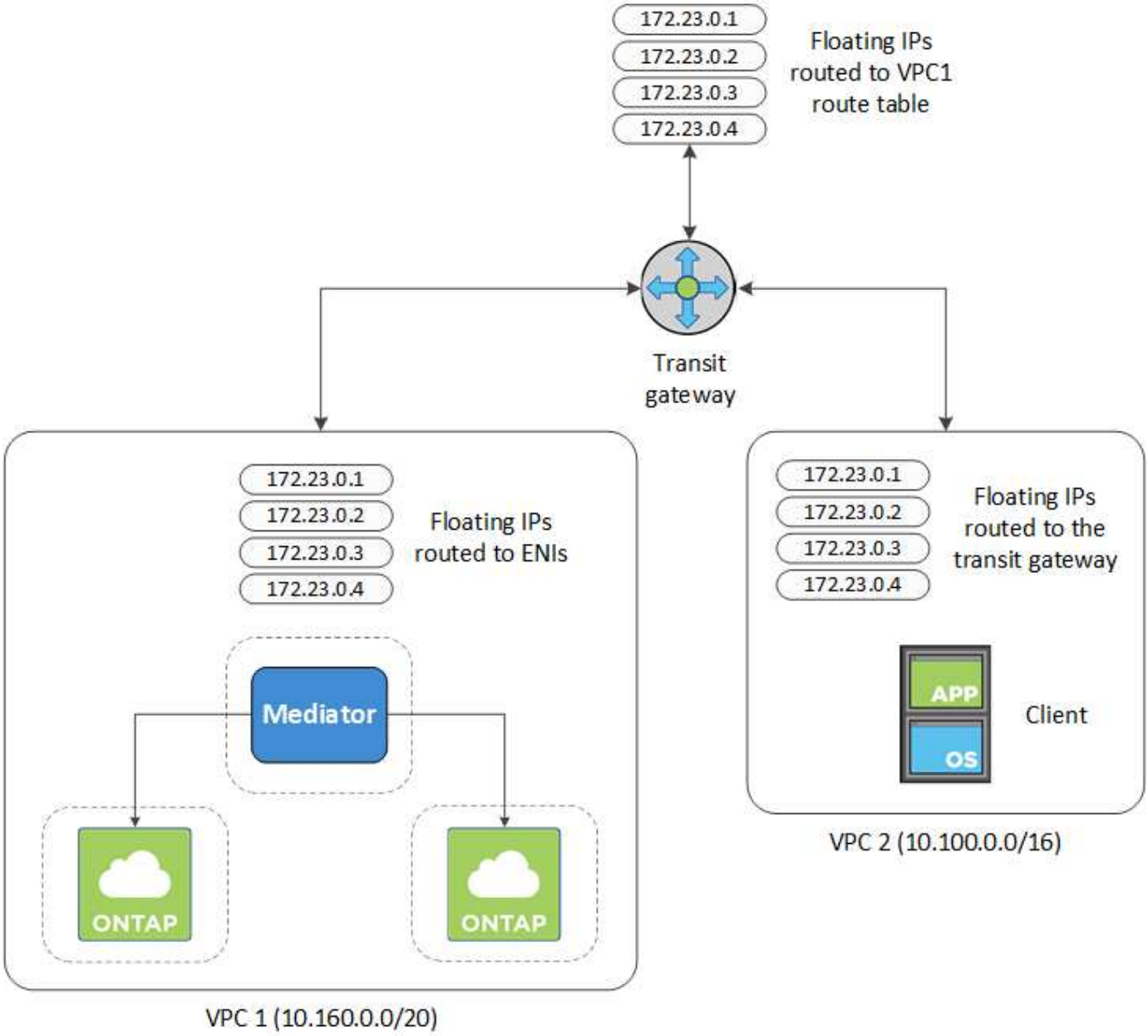
Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

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.

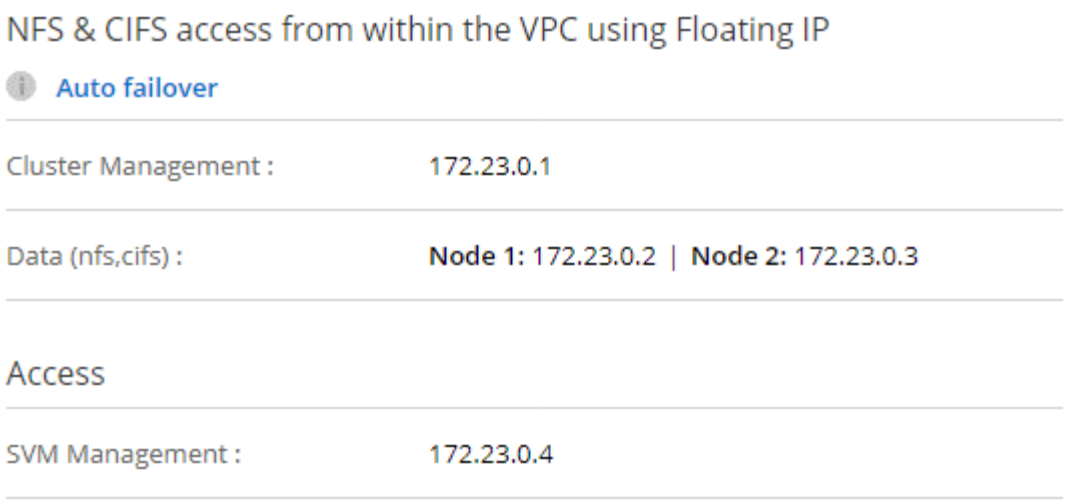


La seguente procedura illustra come configurare una configurazione simile.

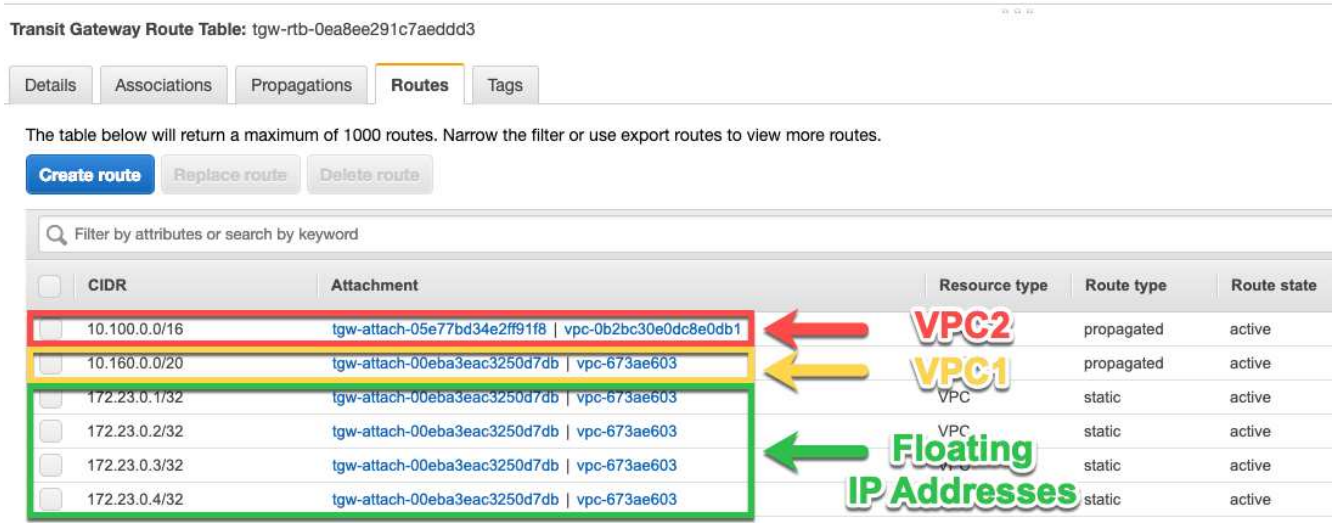
Fasi

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.

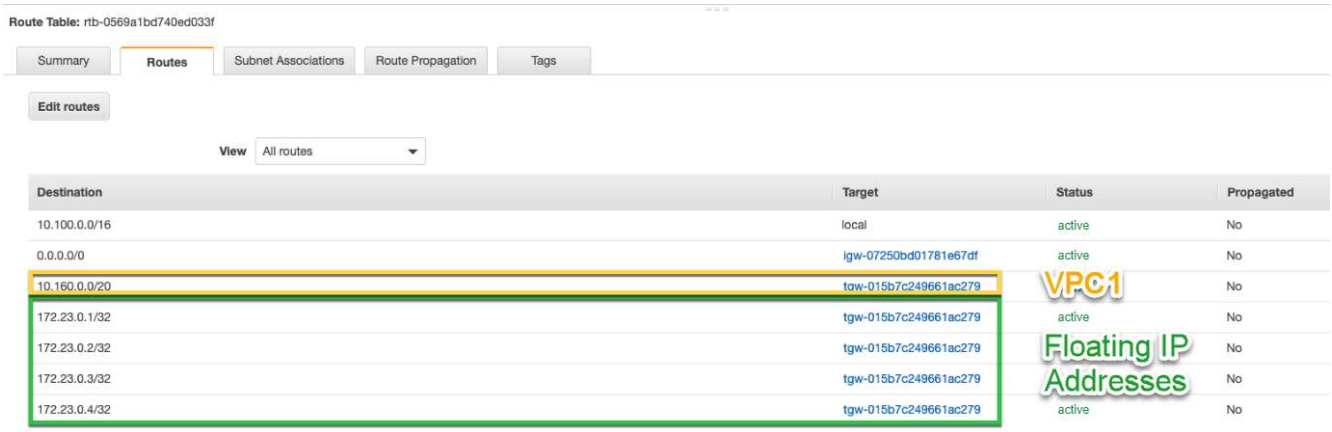


3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

   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.

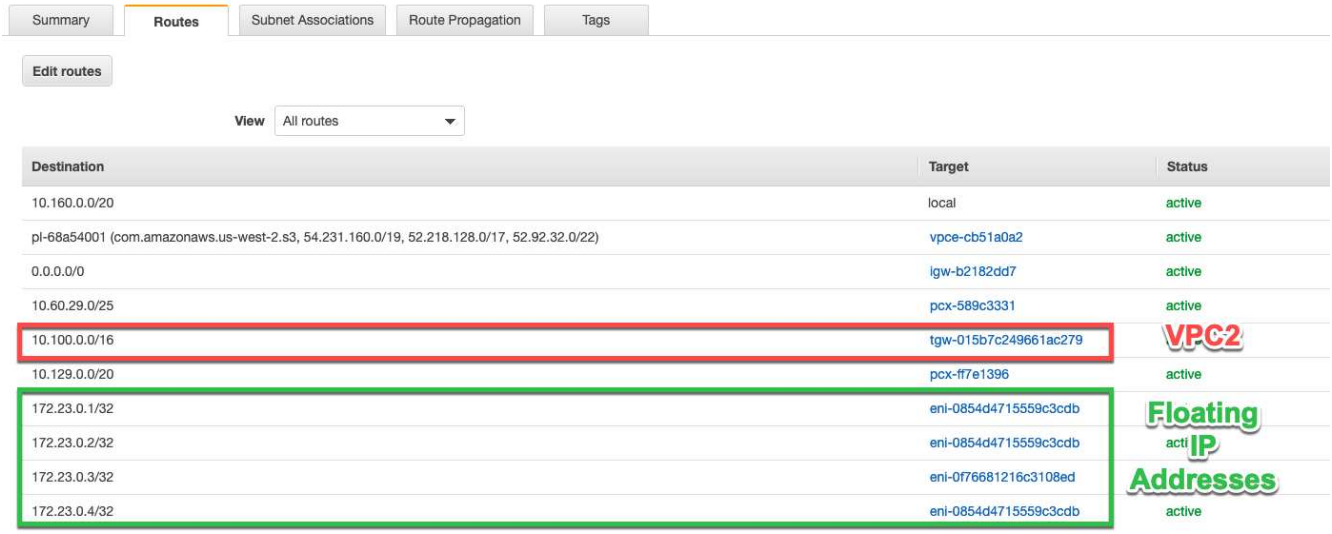
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.

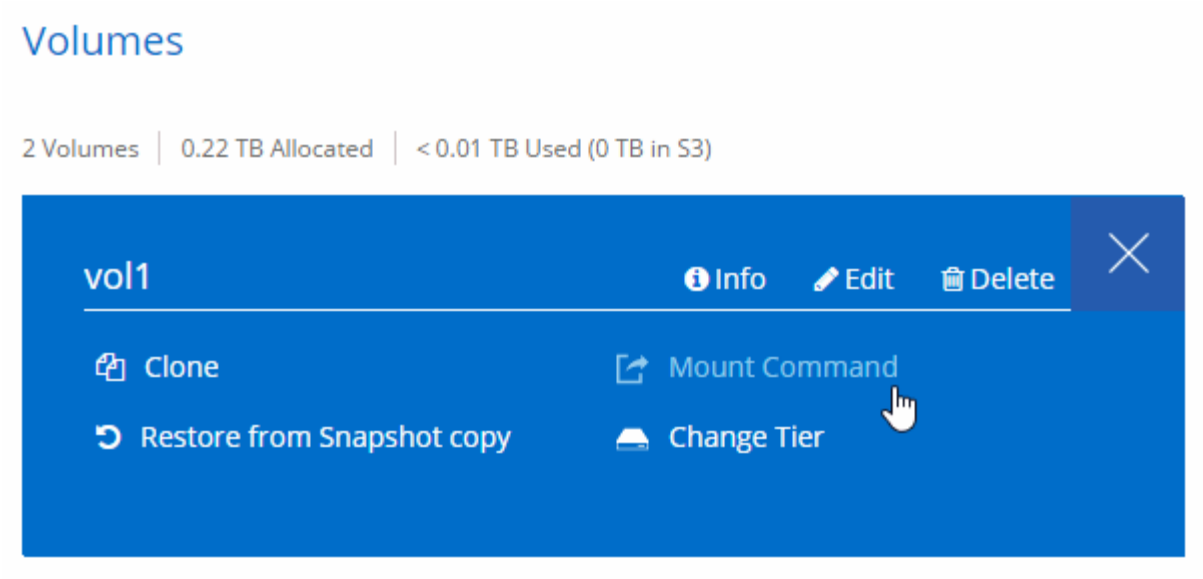
   Questo passaggio è importante perché completa il routing tra i VPC.

   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"

Regole del gruppo di sicurezza per AWS

Cloud Manager crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Connector e Cloud Volumes ONTAP. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata

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

Protocollo	Porta	Scopo
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

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	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	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)

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Backup su S3	TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
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 dal connettore

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 del connettore	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 per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

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 del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale e alle connessioni da Cloud Compliance
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale
TCP	3128	Fornisce all'istanza Cloud Compliance l'accesso a Internet, se la rete AWS non utilizza un NAT o un proxy

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore 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 la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
	TCP	8088	Backup su S3	API chiama il backup in S3
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager
Conformità al cloud	HTTP	80	Istanza di Cloud Compliance	Conformità del cloud per Cloud Volumes ONTAP

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.

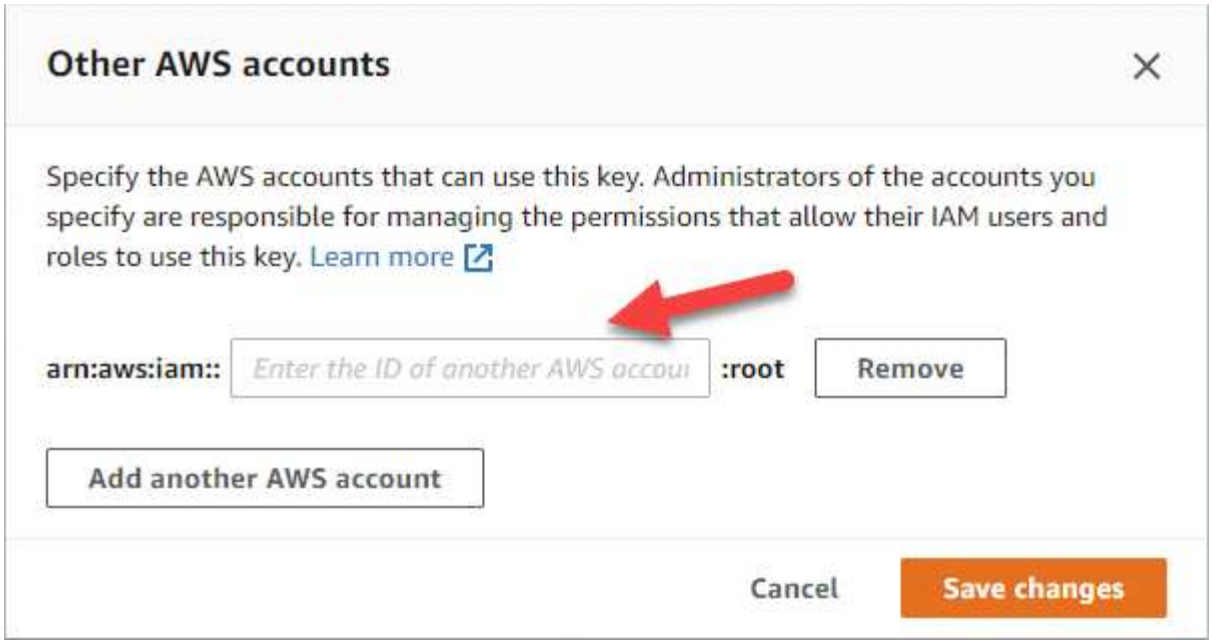
   b. Selezionare la chiave.

   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".

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 sistema Cloud Volumes ONTAP a nodo singolo 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 avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP nodo singolo**.
3. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e l'abbonamento AWS, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

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

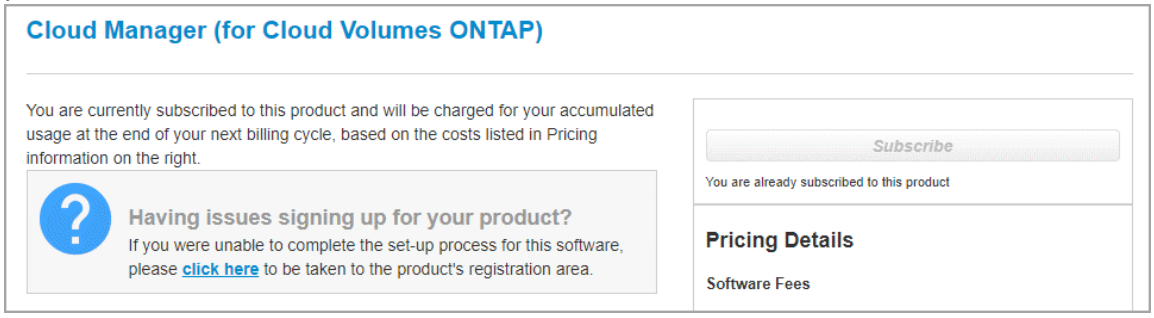
Campo	Descrizione
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.

Campo	Descrizione
Aggiungere tag	I tag AWS sono metadati per le risorse AWS. Cloud Manager aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ogni risorsa AWS associata all'istanza. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione AWS: Contrassegno delle risorse Amazon EC2".
Nome utente e password	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.
Modifica credenziali	Scegli le credenziali AWS e l'abbonamento al marketplace da utilizzare con questo sistema Cloud Volumes ONTAP. Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, selezionare le credenziali AWS associate a un abbonamento a Cloud Volumes ONTAP dal marketplace AWS. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata."Scopri come aggiungere ulteriori credenziali AWS a Cloud Manager".

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go alle tue credenziali AWS:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

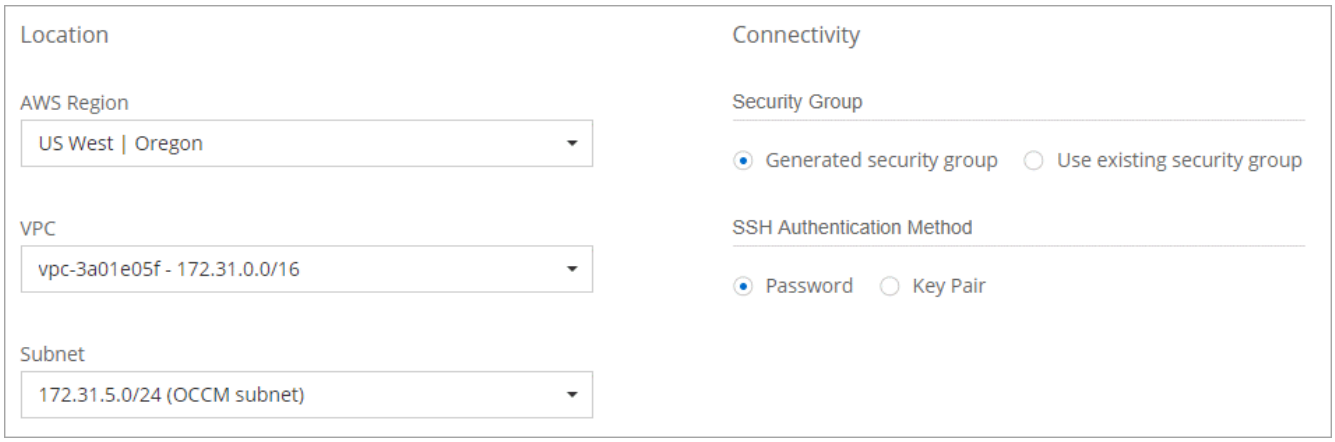
Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi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



4. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
   - "Scopri di più sul monitoraggio".

5. **Location & Connectivity** (posizione e connettività): Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente immagine mostra la pagina compilata:



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

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

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

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

   "Scopri di più sulle tecnologie di crittografia supportate".

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

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

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

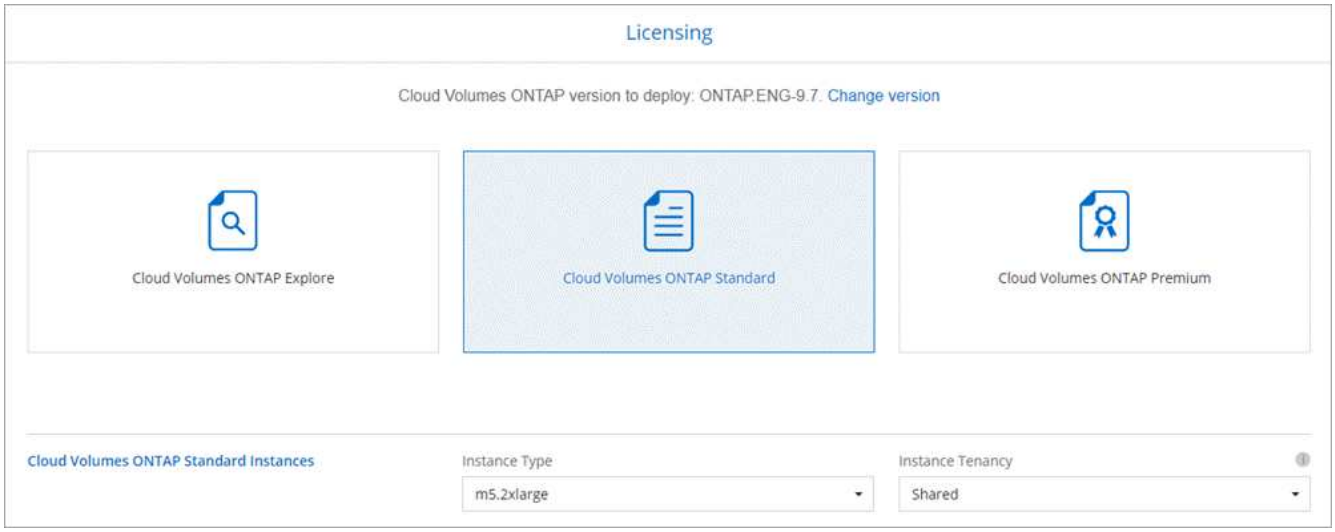
8. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

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

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

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



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

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

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

    Tenere presente quanto segue:

    - 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".

    - Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
    - Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

      "Scopri come funziona il tiering dei dati".

12. **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".

    NON è possibile attivare WORM se è stato attivato il tiering dei dati.

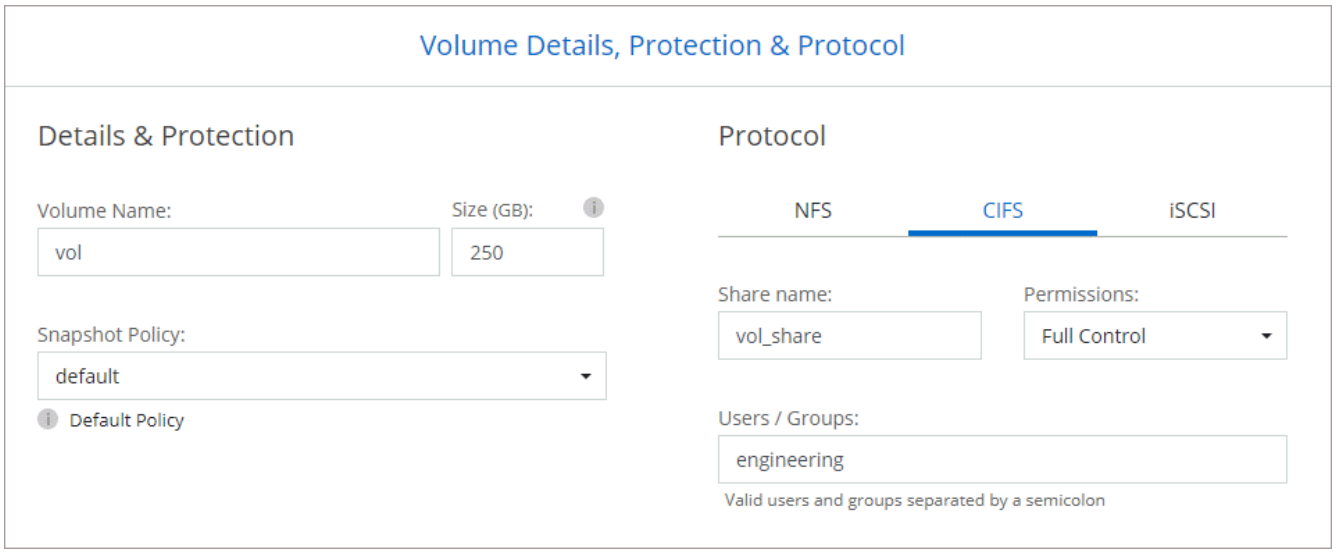
"Scopri di più sullo storage WORM".

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

    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.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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



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

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

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

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

16. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.

a. Esaminare i dettagli della configurazione.

b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

Risultato

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

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

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

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

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

Avvio di una coppia Cloud Volumes ONTAP ha in AWS

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

Prima di iniziare

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

  > Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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".

Limitazione

Al momento, le coppie ha non sono supportate con gli outpost 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** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP nodo singolo**.
3. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e l'abbonamento AWS, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

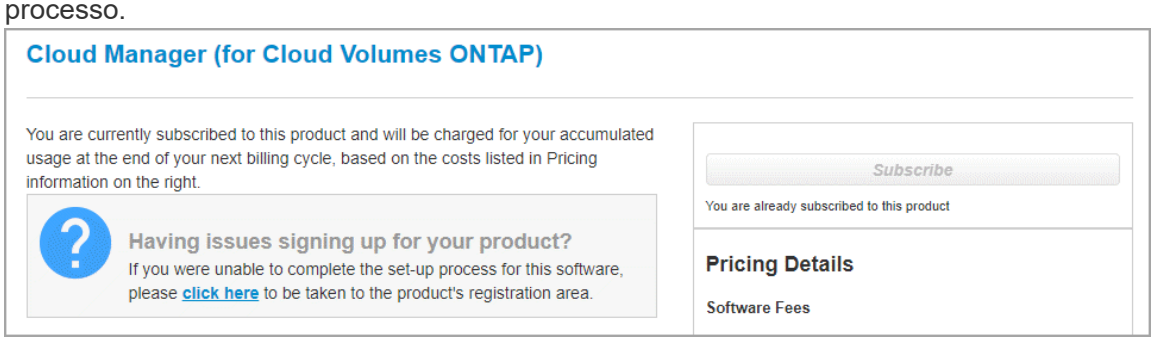
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
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".
Nome utente e password	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.
Modifica credenziali	Scegli le credenziali AWS e l'abbonamento al marketplace da utilizzare con questo sistema Cloud Volumes ONTAP. Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, selezionare le credenziali AWS associate a un abbonamento a Cloud Volumes ONTAP dal marketplace AWS. Da questo abbonamento ti verrà addebitato il costo di ogni sistema PAYGO Cloud Volumes ONTAP 9.6 e versioni successive creato e di ogni funzione aggiuntiva abilitata."Scopri come aggiungere ulteriori credenziali AWS a Cloud Manager".

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go alle tue credenziali AWS:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

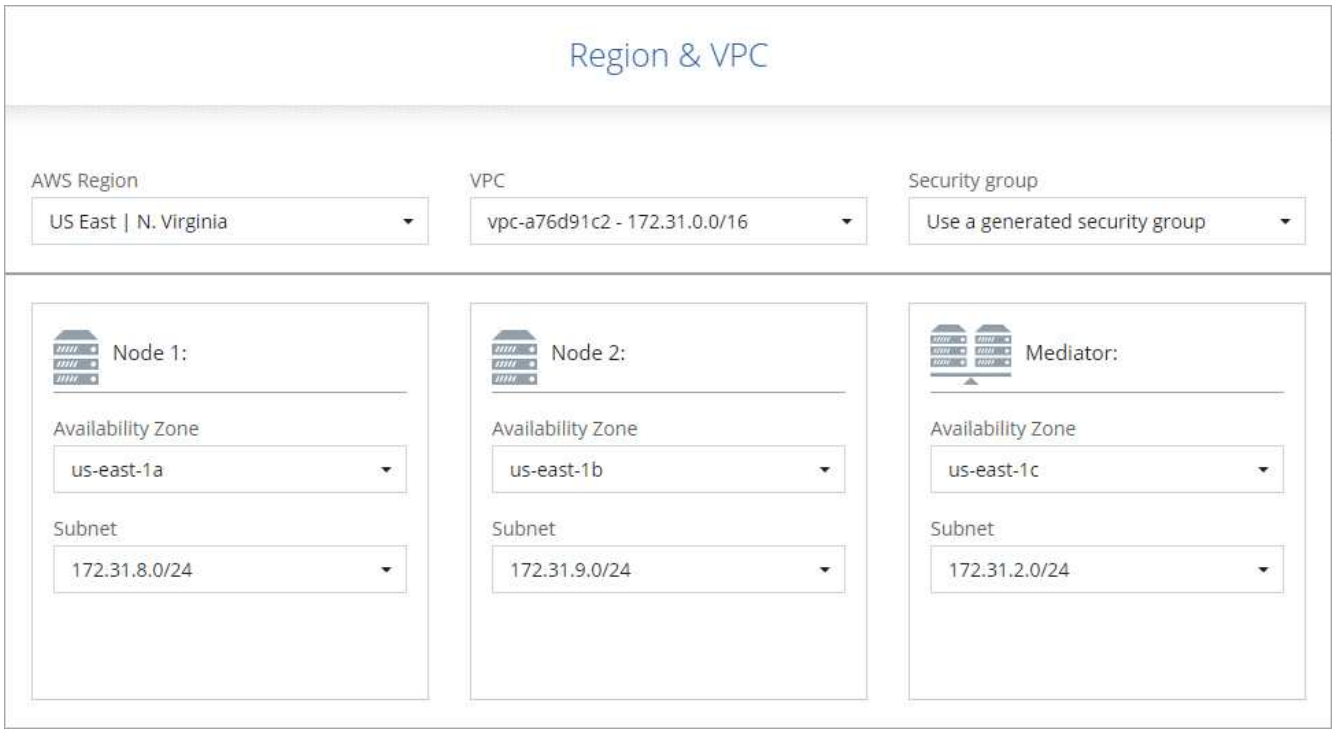
Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi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



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

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

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



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

   Gli indirizzi IP devono essere esterni al blocco CIDR per tutti i VPC della regione. Per ulteriori informazioni, vedere "Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS".

9. **Route Table**: Se si sceglie Multiple AZS, selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili.

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

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

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

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

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

    "Scopri di più sulle tecnologie di crittografia supportate".

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

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

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

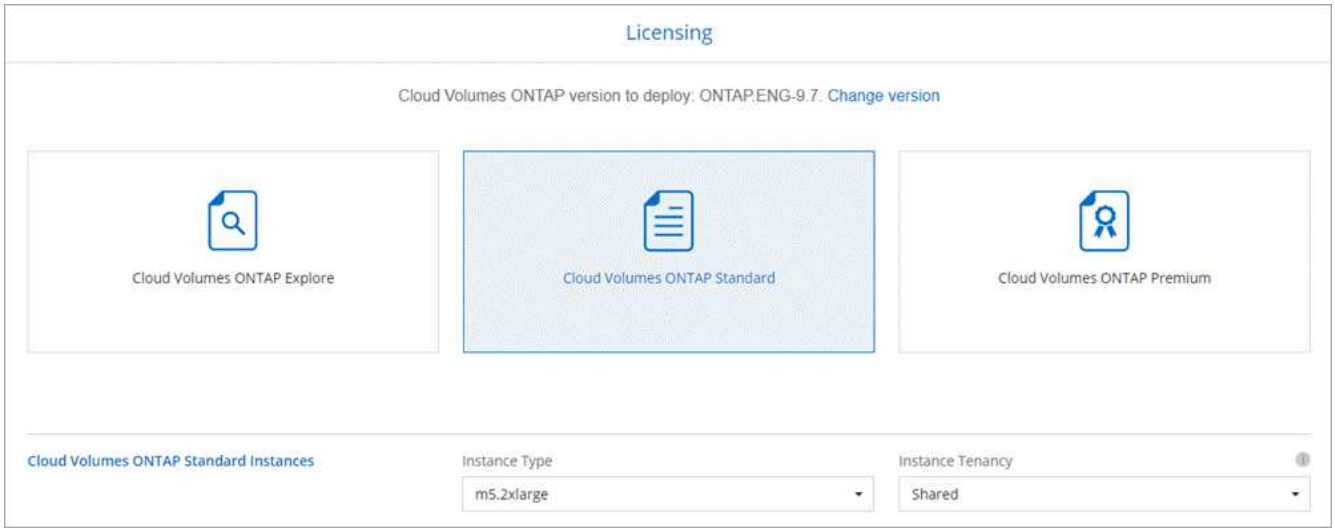
12. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

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

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

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



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

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

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

    Tenere presente quanto segue:

    - 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".

    - Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
    - Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

      "Scopri come funziona il tiering dei dati".

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

    NON è possibile attivare WORM se è stato attivato il tiering dei dati.

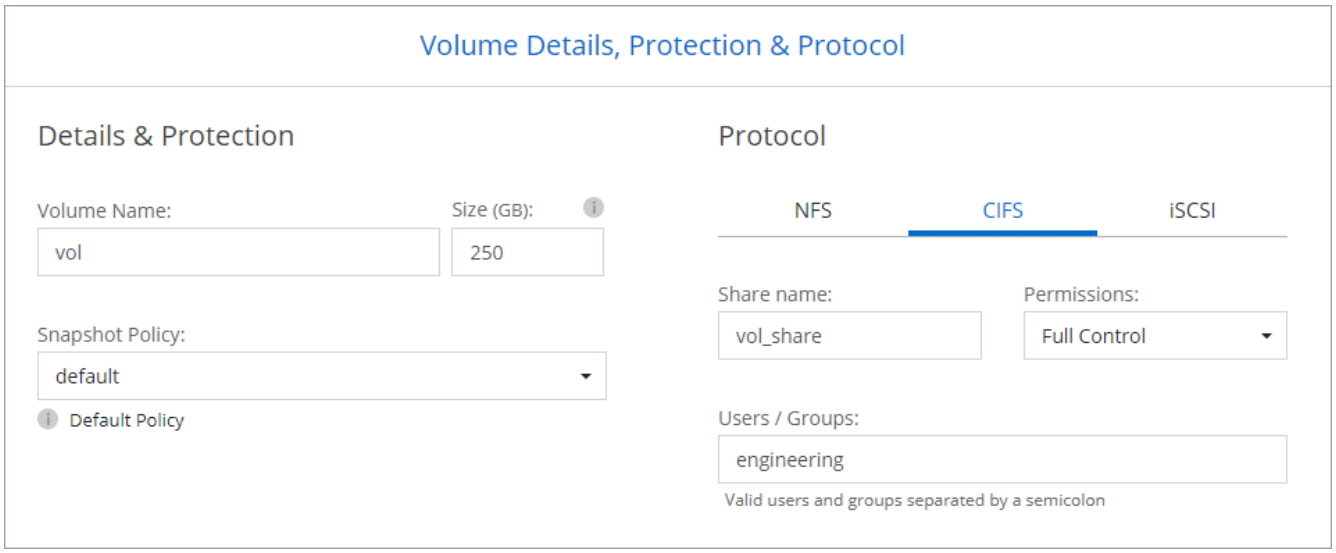
    "Scopri di più sullo storage WORM".

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

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.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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



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

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

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

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

20. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.

a. Esaminare i dettagli della configurazione.

b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse AWS che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

Risultato

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

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

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

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

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

Inizia ad utilizzare Azure

Introduzione a Cloud Volumes ONTAP per Azure

Inizia a utilizzare Cloud Volumes ONTAP per Azure in pochi passaggi.

Creare un connettore

Se non si dispone di un "Connettore" Tuttavia, un amministratore dell'account deve crearne uno. "Scopri come creare un connettore in Azure".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

Configurare la rete

1. Assicurarsi che VNET e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.

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

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

"Scopri di più sui requisiti di rete".

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro), selezionare il tipo di sistema che si desidera implementare e completare la procedura guidata. "Leggi le istruzioni dettagliate".

Link correlati

- "Valutazione"
- "Creazione di un connettore da Cloud Manager"
- "Creazione di un connettore da Azure Marketplace"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa Cloud Manager con le autorizzazioni Azure"

Pianificazione della configurazione di Cloud Volumes ONTAP in Azure

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

Scelta di un tipo di licenza

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

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 in Azure"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP 9.7 in Azure"

Dimensionamento del sistema in Azure

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

Tipo di macchina virtuale

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

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

Tipo di disco Azure

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

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

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

  Per ulteriori informazioni sui casi di utilizzo di questi dischi, vedere "Documentazione di Microsoft Azure: Quali tipi di dischi sono disponibili in 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 di una configurazione che supporti Flash cache

Una configurazione Cloud Volumes ONTAP in Azure include lo storage NVMe locale, che Cloud Volumes ONTAP utilizza come *Flash cache* per migliorare le performance. "Scopri di più su Flash cache".

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)	

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.

Requisiti di rete per implementare e gestire Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente. Ciò include il collegamento in rete per il connettore e Cloud Volumes ONTAP.

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

Accesso a Internet in uscita per Cloud Volumes ONTAP

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

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

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

"Scopri come configurare AutoSupport".

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 alle regole del gruppo di protezione elencate di seguito.

Numero di indirizzi IP

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

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

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

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

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

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

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

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

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

Connessioni a sistemi ONTAP in altre reti

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

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

Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. 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, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

Connessioni alle reti di destinazione

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

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

Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in Azure:

Endpoint	Scopo
https://management.azure.com https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure.

Endpoint	Scopo
https://management.microsoftazure.de https://login.microsoftonline.de	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
*.blob.core.windows.net	Richiesto per coppie ha quando si utilizza un proxy.

Endpoint	Scopo
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.

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	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.

Regole del gruppo di sicurezza per Cloud Volumes ONTAP

Cloud Manager crea gruppi di sicurezza Azure che includono le regole in entrata e in uscita necessarie per il corretto funzionamento di Cloud Volumes ONTAP. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata per sistemi a nodo singolo

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
1001 inbound_http	80 TCP	Qualsiasi a qualsiasi	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1002 inbound_111_tcp	111 TCP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Blocca tutto il traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

Le regole elencate di seguito consentono il traffico, a meno che la descrizione non noti che blocca lo specifico traffico in entrata.

I sistemi HA hanno meno regole in entrata rispetto ai sistemi a nodo singolo perché il traffico dati in entrata passa attraverso il bilanciamento del carico standard di Azure. Per questo motivo, il traffico proveniente dal bilanciamento del carico deve essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

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

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
Active Directory	88	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	137	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	139	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP E UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	445	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	464	UDP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	88	TCP	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	137	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	139	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP E UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	445	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	464	UDP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	749	TCP	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)
DHCP	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione

Servizio	Porta	Protocollo	Origine	Destinazione	Scopo
DHCPS	67	UDP	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	53	UDP	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	25	TCP	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	161	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	161	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	11104	TCP	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	11105	TCP	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	514	UDP	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole del gruppo di sicurezza per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

L'origine delle regole in entrata nel gruppo di sicurezza predefinito è 0.0.0.0/0.

Porta	Protocollo	Scopo
22	SSH	Fornisce l'accesso SSH all'host del connettore
80	HTTP	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
443	HTTPS	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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 connettore include le seguenti regole in uscita.

Porta	Protocollo	Scopo
Tutto	Tutti i TCP	Tutto il traffico in uscita
Tutto	Tutti gli UDP	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

Servizio	Porta	Protocollo	Destinazione	Scopo
Active Directory	88	TCP	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	139	TCP	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	389	TCP	Insieme di strutture di Active Directory	LDAP
	445	TCP	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	464	TCP	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	137	UDP	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	138	UDP	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	464	UDP	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos

Servizio	Porta	Protocollo	Destinazione	Scopo
Chiamate API e AutoSupport	443	HTTPS	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API ad AWS e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	3000	TCP	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	53	UDP	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

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

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- 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.

> **Potenziale perdita di dati**
>
> L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Sebbene il rollback sia attualmente disattivato per impostazione predefinita quando si utilizza l'API per la distribuzione in un gruppo di risorse esistente, l'eliminazione di Cloud Volumes ONTAP potenzialmente eliminerà altre risorse da quel gruppo condiviso.
>
> La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Questa è l'opzione predefinita e consigliata solo quando si implementa Cloud Volumes ONTAP in Azure da Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP** o **alta disponibilità Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e la sottoscrizione di Azure, specificare il nome del cluster e del 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
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	Mantenere il nome predefinito per il nuovo gruppo di risorse o deselezionare **Usa predefinito** e immettere il proprio nome per il nuovo gruppo di risorse. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente utilizzando l'API, non è consigliabile a causa del rischio di perdita di dati. Per ulteriori informazioni, vedere l'avviso riportato sopra.
Tag	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, Cloud Manager li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. 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".
Nome utente e password	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.
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP. Per implementare un sistema Cloud Volumes ONTAP pay-as-you-go, devi associare un abbonamento Azure Marketplace all'abbonamento Azure selezionato. "Scopri come aggiungere le credenziali".

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes ONTAP.
   - "Scopri di più sulla conformità al cloud".
   - "Scopri di più sul backup nel cloud".
5. **Location & Connectivity** (posizione e connettività): Selezionare una posizione e un gruppo di sicurezza e selezionare la casella di controllo per confermare la connettività di rete tra Cloud Manager e la posizione di destinazione.

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

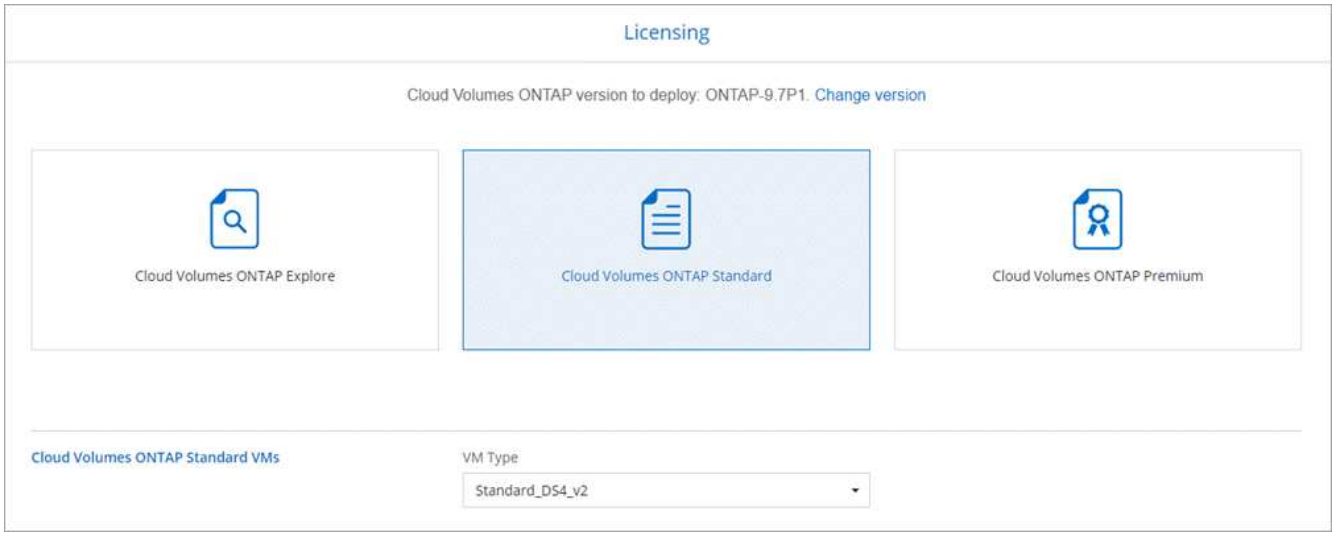
   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

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

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

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

8. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze, selezionare una licenza e selezionare un tipo di macchina virtuale.



   Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

   > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

9. **Iscriviti al marketplace Azure**: Segui la procedura se Cloud Manager non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
10. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

    Tenere presente quanto segue:

    - 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".

- Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
- Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

"Scopri di più sul tiering dei dati".

11. **Write Speed & WORM** (solo sistemi a nodo singolo): Scegliere **normale** o **alta** velocità di scrittura e attivare lo storage WORM (Write Once, Read Many), se desiderato.

    La scelta di una velocità di scrittura è supportata solo nei sistemi a nodo singolo.

    "Scopri di più sulla velocità di scrittura".

    NON è possibile attivare WORM se è stato attivato il tiering dei dati.

    "Scopri di più sullo storage WORM".

12. **Secure Communication to Storage & WORM** (solo ha): Scegliere se abilitare una connessione HTTPS agli account di storage Azure e attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

    La connessione HTTPS proviene da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage Azure. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

    "Scopri di più sullo storage WORM".

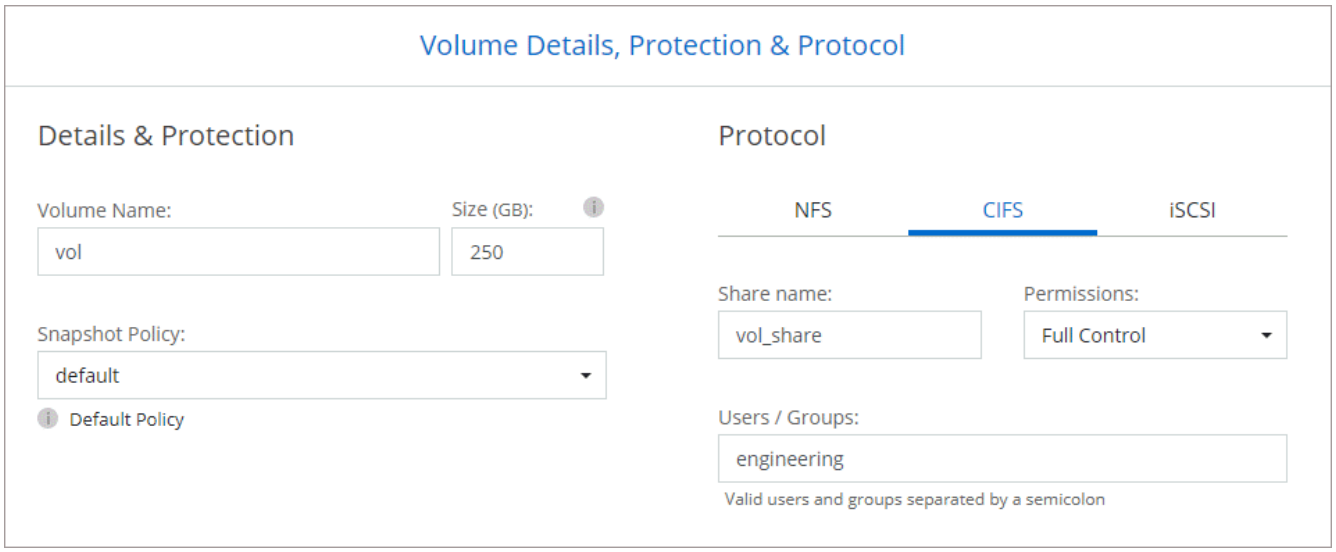
13. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    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.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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



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

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.

Campo	Descrizione
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

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

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

16. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse 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.

Inizia a utilizzare GCP

Introduzione a Cloud Volumes ONTAP per Google Cloud

Inizia a utilizzare Cloud Volumes ONTAP per GCP in pochi passaggi.

Creare un connettore

Se non si dispone di un "Connettore" Tuttavia, un amministratore dell'account deve crearne uno. "Scopri come creare un connettore in GCP".

Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di implementare un connettore se non ne hai ancora uno.

Pianificare la configurazione

Cloud Manager offre pacchetti preconfigurati che soddisfano i tuoi requisiti di carico di lavoro, oppure puoi creare la tua configurazione. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

Configurare la rete

1. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Abilitare l'accesso a Internet in uscita dal VPC di destinazione in modo che il connettore e Cloud Volumes ONTAP possano contattare diversi endpoint.

   Questo passaggio è importante perché il connettore non è in grado di gestire Cloud Volumes ONTAP senza accesso a Internet in uscita. Se è necessario limitare la connettività in uscita, fare riferimento all'elenco degli endpoint per "Il connettore e Cloud Volumes ONTAP".

"Scopri di più sui requisiti di rete".

Configurare GCP per il tiering dei dati

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

1. "Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google".
2. "Impostare un account di servizio per il tiering dei dati":
   - Assegnare il ruolo predefinito *Storage Admin* all'account del servizio di tiering.
   - Aggiungere l'account del servizio Connector come *Service account User* all'account del servizio di tiering.

     È possibile fornire il ruolo dell'utente "nel passaggio 3 della procedura guidata quando si crea l'account

del servizio di tiering", o. "assegnare il ruolo dopo la creazione dell'account di servizio".

Sarà necessario selezionare l'account del servizio di tiering in un secondo momento quando si crea un ambiente di lavoro Cloud Volumes ONTAP.

Se non si attiva il tiering dei dati e si seleziona un account di servizio quando si crea il sistema Cloud Volumes ONTAP, è necessario spegnere il sistema e aggiungere l'account di servizio a Cloud Volumes ONTAP dalla console GCP.

Abilitare le API di Google Cloud

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

- API di Cloud Deployment Manager V2
- API Cloud Logging
- API Cloud Resource Manager
- API di Compute Engine
- API IAM (Identity and Access Management)

Avviare Cloud Volumes ONTAP utilizzando Cloud Manager

Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro), selezionare il tipo di sistema che si desidera implementare e completare la procedura guidata. "Leggi le istruzioni dettagliate".

Link correlati

- "Valutazione"
- "Creazione di un connettore da Cloud Manager"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa Cloud Manager con le autorizzazioni GCP"

Pianificazione della configurazione di Cloud Volumes ONTAP in Google Cloud

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

Scelta di un tipo di licenza

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

"Configurazioni supportate per Cloud Volumes ONTAP 9.7 in GCP"

Comprendere i limiti dello storage

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

"Limiti di storage per Cloud Volumes ONTAP 9.7 in GCP"

Dimensionamento del sistema in GCP

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

Tipo di macchina

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

Per ulteriori informazioni, fare riferimento a quanto segue:

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

Tipo di disco GCP

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

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

Dimensione del disco GCP

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

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

  Per ulteriori informazioni, fare riferimento a quanto segue:

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

Foglio di lavoro delle informazioni di rete GCP

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

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

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.

Requisiti di rete per implementare e gestire Cloud Volumes ONTAP in GCP

Configura la tua rete della piattaforma cloud Google in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente. Ciò include il collegamento in rete per il connettore e Cloud Volumes ONTAP.

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in GCP.

Cloud privato virtuale

Cloud Volumes ONTAP e il connettore sono supportati in un VPC condiviso Google Cloud e anche in VPC non condivisi.

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

L'unico requisito per l'utilizzo di un VPC condiviso è fornire "Ruolo di Compute Network User" All'account del servizio Connector. Cloud Manager necessita di queste autorizzazioni per eseguire query su firewall, VPC e subnet nel progetto host.

Accesso a Internet in uscita per Cloud Volumes ONTAP

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

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

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

  "Scopri come configurare AutoSupport".

Numero di indirizzi IP

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

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

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

Regole del firewall

Non è necessario creare regole firewall perché Cloud Manager fa tutto questo per te. Se è necessario utilizzare il proprio, fare riferimento alle regole del firewall elencate di seguito.

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

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

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

Connessioni a sistemi ONTAP in altre reti

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

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

Requisiti per il connettore

Configura la tua rete in modo che il connettore possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. 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, è possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a. "Configurazione del connettore per l'utilizzo di un server proxy".

Connessione alle reti di destinazione

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

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

Accesso a Internet in uscita

Il connettore richiede l'accesso a Internet in uscita per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Un connettore contatta i seguenti endpoint durante la gestione delle risorse in GCP:

Endpoint	Scopo
https://www.googleapis.com	Consente al connettore di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.

Endpoint	Scopo
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://repo.cloud.support.netapp.com	Utilizzato per scaricare le dipendenze di Cloud Manager.
http://repo.mysql.com/	Utilizzato per scaricare MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Consente al connettore di accedere e scaricare manifesti, modelli e immagini di aggiornamento Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Accesso alle immagini software dei componenti container per un'infrastruttura che esegue Docker e fornisce una soluzione per l'integrazione dei servizi con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
Varie sedi di terze parti, ad esempio: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Le sedi di terze parti sono soggette a modifiche.	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host del connettore	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.

Regole firewall per Cloud Volumes ONTAP

Cloud Manager crea regole firewall GCP che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Le regole del firewall per Cloud Volumes ONTAP richiedono regole sia in entrata che in uscita.

Regole in entrata

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

Protocollo	Porta	Scopo
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

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	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	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)

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
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
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 firewall per il connettore

Le regole firewall per il connettore richiedono regole sia in entrata che in uscita.

Regole in entrata

L'origine delle regole in entrata nelle regole firewall predefinite è 0.0.0.0/0.

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Le regole firewall predefinite per il connettore aprono tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Le regole firewall predefinite per il connettore includono le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti i TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per la comunicazione in uscita dal connettore.

L'indirizzo IP di origine è l'host del connettore.

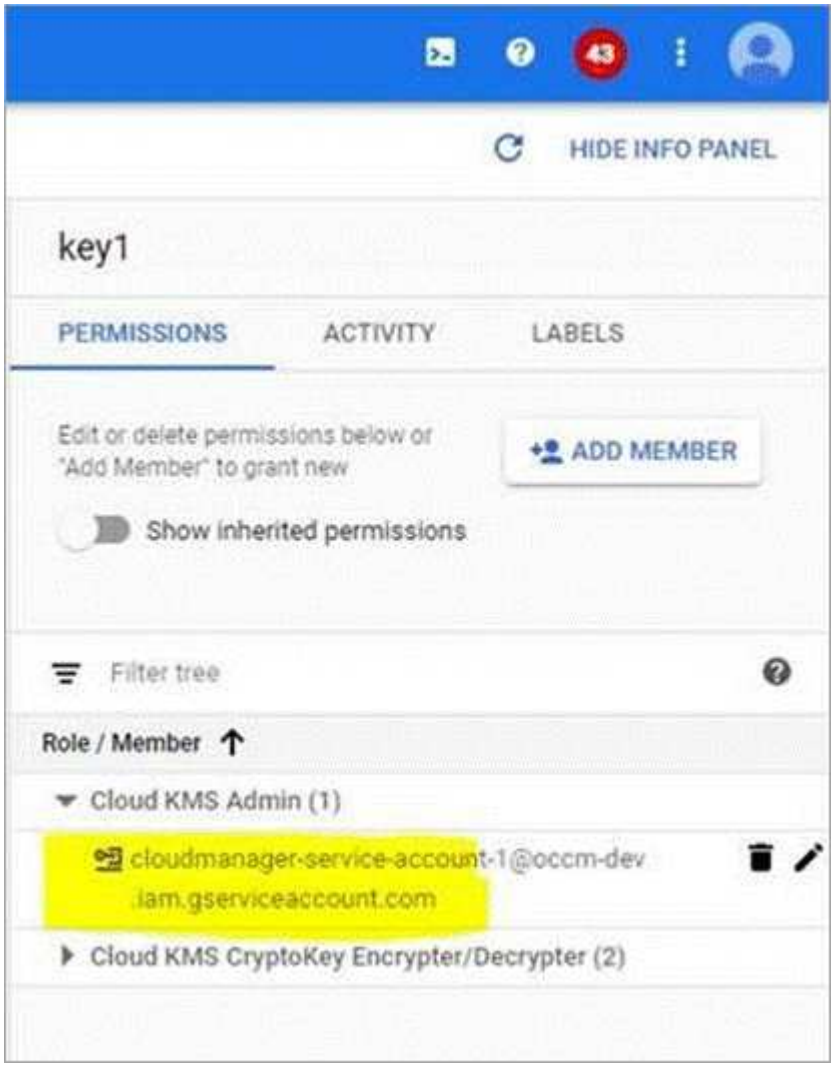
Servizio	Protocollo	Porta	Destinazione	Scopo
Active Directory	TCP	88	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	TCP	139	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP	389	Insieme di strutture di Active Directory	LDAP
	TCP	445	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Insieme di strutture di Active Directory	Modifica e impostazione della password Kerberos V di Active Directory (RPCSEC_GSS)
	UDP	137	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	UDP	464	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
Chiamate API e AutoSupport	HTTPS	443	LIF gestione cluster ONTAP e Internet in uscita	Chiamate API a GCP e ONTAP e invio di messaggi AutoSupport a NetApp
Chiamate API	TCP	3000	LIF gestione cluster ONTAP	Chiamate API a ONTAP
DNS	UDP	53	DNS	Utilizzato per la risoluzione DNS da parte di Cloud Manager

Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP

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

Fasi

1. Assegnare all'account del servizio Connector l'autorizzazione per utilizzare la chiave di crittografia.



2. Ottenere l'id della chiave richiamando il comando get per l'API /gcp/vsa/metadata/gcp-Encryption-keys.
3. Utilizzare il parametro "GcpEncryption" con la richiesta API durante la creazione di un ambiente di lavoro.

Esempio

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

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

Avvio di Cloud Volumes ONTAP in GCP

È possibile avviare un sistema Cloud Volumes ONTAP a nodo singolo in GCP creando un ambiente di lavoro.

Di cosa hai bisogno

- Si dovrebbe avere un "Connettore associato all'area di lavoro".

> Per creare un connettore, è necessario essere un amministratore dell'account. Quando crei il tuo primo ambiente di lavoro Cloud Volumes ONTAP, Cloud Manager ti chiede di creare un connettore se non ne hai ancora uno.

- "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- Si dovrebbe aver scelto una configurazione e ottenuto le informazioni di rete GCP dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".
- Per implementare un sistema BYOL, è necessario il numero seriale a 20 cifre (chiave di licenza) per ciascun nodo.
- Le seguenti API di Google Cloud dovrebbero essere "abilitato nel tuo progetto":
  - API di Cloud Deployment Manager V2
  - API Cloud Logging
  - API Cloud Resource Manager
  - API di Compute Engine
  - API IAM (Identity and Access Management)

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e seguire le istruzioni.
2. **Scegli una località**: Seleziona **Google Cloud** e **Cloud Volumes ONTAP**.
3. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, aggiungere etichette e specificare le credenziali.

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

Campo	Descrizione
Nome ambiente di lavoro	Cloud Manager utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza della VM GCP. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Aggiungi etichette	Le etichette sono metadati per le risorse GCP. Cloud Manager aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse GCP associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a. "Documentazione Google Cloud: Risorse per l'etichettatura".
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema o la relativa CLI.

Campo	Descrizione
Modifica progetto	Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede Cloud Manager. Se non vedi altri progetti nell'elenco a discesa, non hai ancora associato l'account del servizio Cloud Manager ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account di servizio con il ruolo di Cloud Manager a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Questo è l'account di servizio configurato per Cloud Manager, "come descritto nel passo 2b di questa pagina". Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto GCP associato a un abbonamento a Cloud Volumes ONTAP dal mercato GCP.

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go al progetto GCP:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Posizione e connettività**: Selezionare una posizione, scegliere un criterio firewall e selezionare la casella di controllo per confermare la connettività di rete allo storage Google Cloud per il tiering dei dati.

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

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

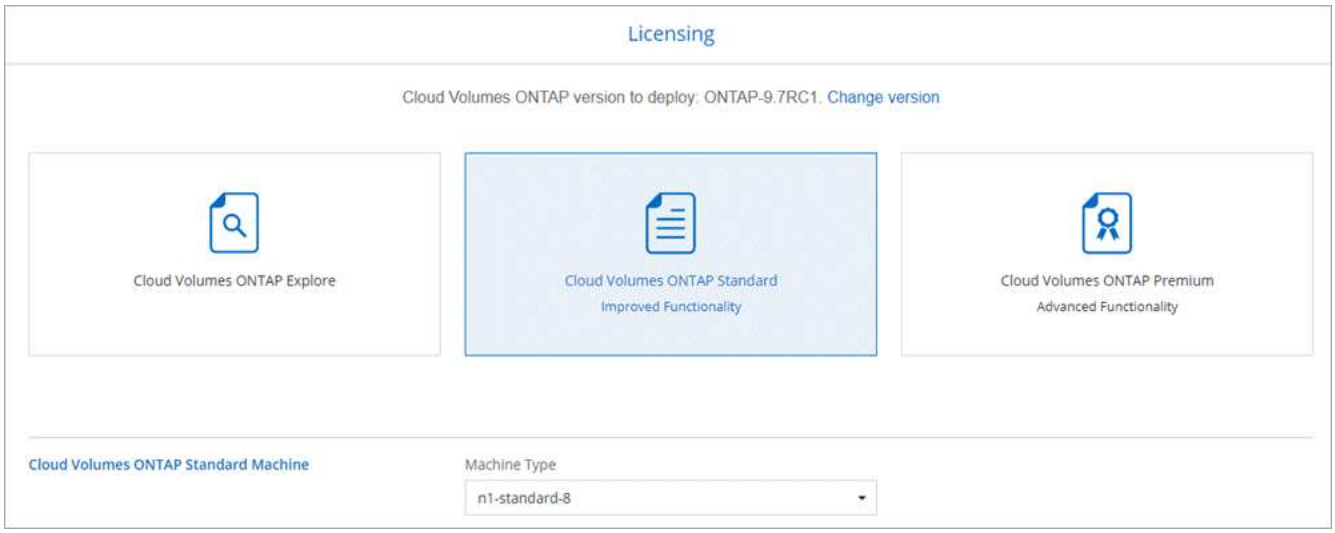
   Per informazioni sul funzionamento delle licenze, vedere "Licensing".

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

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

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

7. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze, selezionare una licenza e selezionare un tipo di macchina virtuale.



Se le esigenze cambiano dopo l'avvio del sistema, è possibile modificare il tipo di licenza o macchina virtuale in un secondo momento.

> Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, Cloud Manager aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.6 RC1 e 9.6 GA è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

8. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

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

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

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

9. **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".

   NON è possibile attivare WORM se è stato attivato il tiering dei dati.

   "Scopri di più sullo storage WORM".

10. **Tiering dei dati nella piattaforma Google Cloud**: Scegliere se attivare il tiering dei dati sull'aggregato iniziale, scegliere una classe di storage per i dati a più livelli, quindi selezionare un account di servizio con il ruolo di amministratore dello storage predefinito (richiesto per Cloud Volumes ONTAP 9.7) oppure selezionare un account GCP (richiesto per Cloud Volumes ONTAP 9.6).

    Tenere presente quanto segue:

- Cloud Manager imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Cloud Manager come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da Cloud Manager.
- Per informazioni sull'aggiunta di un account GCP, vedere "Impostazione e aggiunta di account GCP per il tiering dei dati con 9.6".
- Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
- Se si disattiva il tiering dei dati, è possibile attivarlo su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console GCP.

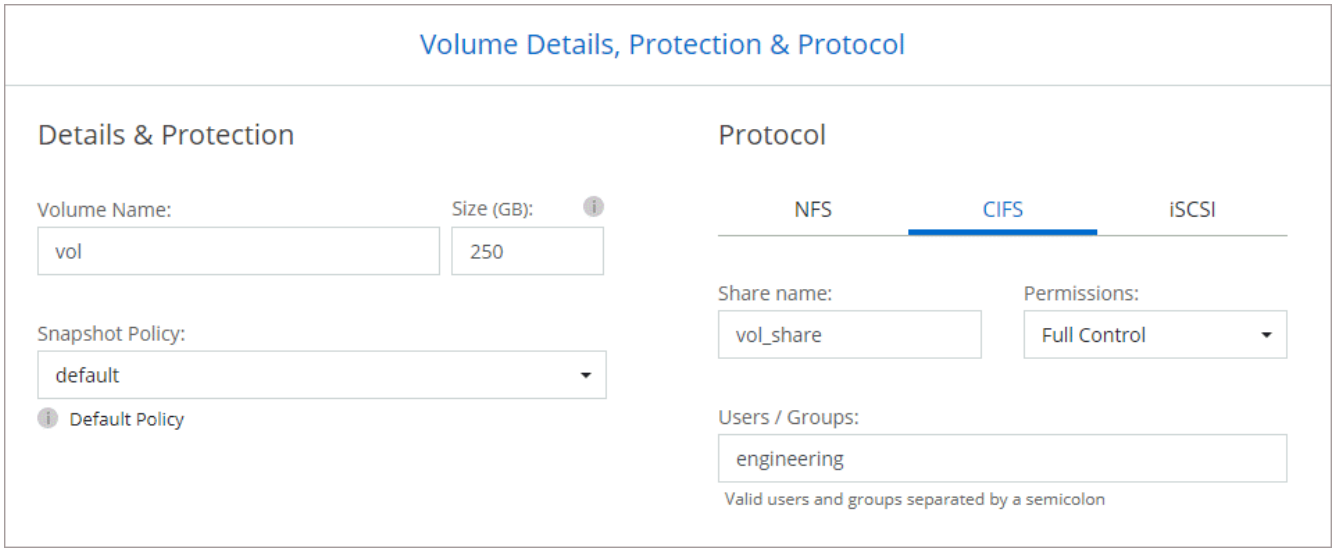
  "Scopri di più sul tiering dei dati".

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

    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.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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



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

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

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

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

14. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.

b. Fare clic su **ulteriori informazioni** per rivedere i dettagli sul supporto e le risorse GCP che Cloud Manager acquisterà.

c. Selezionare le caselle di controllo **ho capito…**.

d. Fare clic su **Go**.

Risultato

Cloud Manager implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare ambiente**.

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

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

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

Provisioning e gestione dello storage

Provisioning dello storage

Puoi eseguire il provisioning di storage aggiuntivo per i tuoi sistemi Cloud Volumes ONTAP da Cloud Manager gestendo volumi e aggregati.

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

Creazione di volumi FlexVol

Se hai bisogno di più storage dopo il lancio di un sistema Cloud Volumes ONTAP, puoi creare nuovi volumi FlexVol per NFS, CIFS o iSCSI da Cloud Manager.

A proposito di questa attività

Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, Utilizzare IQN per connettersi al LUN dagli host.

> È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.

Prima di iniziare

Se si desidera utilizzare CIFS in AWS, è necessario aver configurato DNS e Active Directory. Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP per AWS".

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome del sistema Cloud Volumes ONTAP su cui si desidera eseguire il provisioning dei volumi FlexVol.
2. Creare un nuovo volume su qualsiasi aggregato o su un aggregato specifico:

Azione	Fasi
Crea un nuovo volume e lascia che Cloud Manager scelga l'aggregato contenente	Fare clic su **Add New Volume** (Aggiungi nuovo volume).
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.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.

Campo	Descrizione
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

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.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. • Per configurare AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo. • Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"^]
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.

Campo	Descrizione
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

5. Nella pagina Usage Profile (Profilo di utilizzo), Disk Type (tipo di disco) e Tiering Policy (criterio di tiering), scegliere se attivare le funzionalità di efficienza dello storage, scegliere un tipo di disco e modificare il criterio di tiering, se necessario.

   Per assistenza, fare riferimento a quanto segue:

   - "Comprensione dei profili di utilizzo dei volumi"
   - "Dimensionamento del sistema in AWS"
   - "Dimensionamento del sistema in Azure"
   - "Panoramica sul tiering dei dati"
6. Fare clic su **Go**.

Risultato

Cloud Volumes ONTAP esegue il provisioning del volume.

Al termine

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

Se si desidera applicare le quote ai volumi, è necessario utilizzare System Manager o la CLI. Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Creazione di volumi FlexVol sul secondo nodo in una configurazione ha

Per impostazione predefinita, Cloud Manager crea volumi sul primo nodo in una configurazione ha. Se è necessaria una configurazione Active-Active, in cui entrambi i nodi servono i dati ai client, è necessario creare aggregati e volumi sul secondo nodo.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi creare l'aggregato.
4. Per nodo principale, scegliere il secondo nodo della coppia ha.
5. Dopo che Cloud Manager ha creato l'aggregato, selezionarlo e fare clic su **Create volume** (Crea volume).
6. Inserire i dettagli del nuovo volume, quindi fare clic su **Create** (Crea).

Al termine

Se necessario, è possibile creare volumi aggiuntivi su questo aggregato.

Per le coppie ha implementate in più zone di disponibilità AWS, è necessario montare il volume sui client utilizzando l'indirizzo IP mobile del nodo su cui risiede il volume.

Creazione di aggregati

È possibile creare aggregati o lasciare che Cloud Manager lo faccia per te quando crea volumi. Il vantaggio della creazione di aggregati consiste nella possibilità di scegliere la dimensione del disco sottostante, che consente di dimensionare l'aggregato in base alla capacità o alle performance necessarie.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome dell'istanza di Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
3. Fare clic su **Add aggregate** (Aggiungi aggregato), quindi specificare i dettagli per l'aggregato.

   Per informazioni sul tipo di disco e sulle dimensioni del disco, vedere "Pianificazione della configurazione".

4. Fare clic su **Go**, quindi su **Approve and Purchase** (approva e acquista).

Connessione di un LUN a un host

Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, utilizzare IQN per connettersi al LUN dagli host.

Tenere presente quanto segue:

1. La gestione automatica della capacità di Cloud Manager non si applica alle LUN. Quando Cloud Manager crea un LUN, disattiva la funzione di crescita automatica.
2. È possibile creare ulteriori LUN da System Manager o dall'interfaccia CLI.

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. Selezionare un volume, quindi fare clic su **Target IQN**.
3. Fare clic su **Copy** (Copia) per copiare il nome IQN.
4. Impostare una connessione iSCSI dall'host al LUN.
   - "Configurazione iSCSI Express di ONTAP 9 per Red Hat Enterprise Linux: Avvio delle sessioni iSCSI con la destinazione"
   - "Configurazione iSCSI Express di ONTAP 9 per Windows: Avvio di sessioni iSCSI con la destinazione"

Utilizzo di FlexCache Volumes per accelerare l'accesso ai dati

Un volume FlexCache è un volume di storage che memorizza nella cache i dati di lettura NFS da un volume di origine (o di origine). Le successive letture dei dati memorizzati nella cache consentono un accesso più rapido a tali dati.

È possibile utilizzare i volumi FlexCache per accelerare l'accesso ai dati o per trasferire il traffico dai volumi ad accesso elevato. I volumi FlexCache aiutano a migliorare le performance, soprattutto quando i client devono accedere ripetutamente agli stessi dati, perché i dati possono essere gestiti direttamente senza dover

accedere al volume di origine. I volumi FlexCache funzionano bene per i carichi di lavoro di sistema che richiedono un uso intensivo della lettura.

Cloud Manager non fornisce attualmente la gestione dei volumi FlexCache, ma è possibile utilizzare l'interfaccia CLI di ONTAP o Gestione di sistema di ONTAP per creare e gestire i volumi FlexCache:

- "Guida all'alimentazione di FlexCache Volumes per un accesso più rapido ai dati"
- "Creazione di volumi FlexCache in Gestore di sistema"

A partire dalla versione 3.7.2, Cloud Manager genera una licenza FlexCache per tutti i nuovi sistemi Cloud Volumes ONTAP. La licenza include un limite di utilizzo di 500 GB.

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

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, la versione del protocollo NFS, l'elenco di controllo dell'accesso NFS o le autorizzazioni di condivisione, quindi fare clic su **Update** (Aggiorna). Se sono necessarie policy Snapshot personalizzate, è possibile crearle utilizzando System Manager.
Clonare un volume	a. Selezionare un volume, quindi fare clic su **Clone**. b. Modificare il nome del clone secondo necessità, quindi fare clic su **Clone**. Questo processo crea un volume FlexClone. Un volume FlexClone è una copia point-in-time scrivibile efficiente in termini di spazio, in quanto utilizza una piccola quantità di spazio per i metadati e consuma solo spazio aggiuntivo quando i dati vengono modificati o aggiunti. Per ulteriori informazioni sui volumi FlexClone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
Ripristinare i dati da una copia Snapshot a un nuovo volume	a. Selezionare un volume, quindi fare clic su **Restore from Snapshot copy** (Ripristina da copia Snapshot). b. Selezionare una copia Snapshot, immettere un nome per il nuovo volume, quindi fare clic su **Restore** (Ripristina).
Crea una copia Snapshot on-demand	a. Selezionare un volume, quindi fare clic su **Crea una copia Snapshot**. b. Modificare il nome, se necessario, quindi fare clic su **Crea**.
Scarica il comando NFS mount	a. Selezionare un volume, quindi fare clic su **comando di montaggio**. b. Fare clic su **Copy** (Copia).
Visualizzare l'IQN di destinazione per un volume iSCSI	a. Selezionare un volume, quindi fare clic su **Target IQN**. b. Fare clic su **Copy** (Copia). c. "Utilizzare IQN per connettersi al LUN dagli host".

Attività	Azione
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.
Eliminare un volume	a. Selezionare un volume, quindi fare clic su **Delete** (Elimina). b. Fare nuovamente clic su **Delete** per confermare.

Gestione degli aggregati esistenti

Gestisci gli aggregati aggiungendo dischi, visualizzando informazioni sugli aggregati ed eliminandoli.

Prima di iniziare

Se si desidera eliminare un aggregato, è necessario prima eliminare i volumi nell'aggregato.

A proposito di questa attività

Se un aggregato sta esaurendo lo spazio, è possibile spostare i volumi in un altro aggregato utilizzando Gestione di sistema di OnCommand.

Fasi

1. Nella pagina Working Environments (ambienti di lavoro), fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP su cui si desidera gestire gli aggregati.
2. Fare clic sull'icona del menu, quindi su **Avanzate > allocazione avanzata**.
3. Gestisci i tuoi aggregati:

Attività	Azione
Visualizzare informazioni su un aggregato	Selezionare un aggregato e fare clic su **Info**.
Creare un volume su un aggregato specifico	Selezionare un aggregato e fare clic su **Create volume** (Crea volume).

Attività	Azione
Aggiungere dischi a un aggregato	a. Selezionare un aggregato e fare clic su **Aggiungi dischi AWS** o **Aggiungi dischi Azure**. b. Selezionare il numero di dischi che si desidera aggiungere e fare clic su **Aggiungi**. Tutti i dischi di un aggregato devono avere le stesse dimensioni.
Eliminare un aggregato	a. Selezionare un aggregato che non contiene volumi e fare clic su **Delete** (Elimina). b. Fare nuovamente clic su **Delete** per confermare.

Modifica del server CIFS

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server CIFS in Cloud Volumes ONTAP in modo che possa continuare a fornire storage ai client.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > CIFS setup**.
2. Specificare le impostazioni per il server CIFS:

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

Attività	Azione
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Guida per sviluppatori API di Cloud Manager" per ulteriori informazioni.

3. Fare clic su **Save** (Salva).

Risultato

Cloud Volumes ONTAP aggiorna il server CIFS con le modifiche.

Spostamento di un volume

Spostare i volumi per l'utilizzo della capacità, migliorare le performance e soddisfare i service level agreement.

È possibile spostare un volume in System Manager selezionando un volume e l'aggregato di destinazione, avviando l'operazione di spostamento del volume e monitorando facoltativamente il processo di spostamento del volume. Quando si utilizza System Manager, l'operazione di spostamento del volume termina automaticamente.

Fasi

1. Utilizzare System Manager o CLI per spostare i volumi nell'aggregato.

   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".

Spostamento di un volume quando Cloud Manager visualizza un messaggio Action Required (azione richiesta)

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

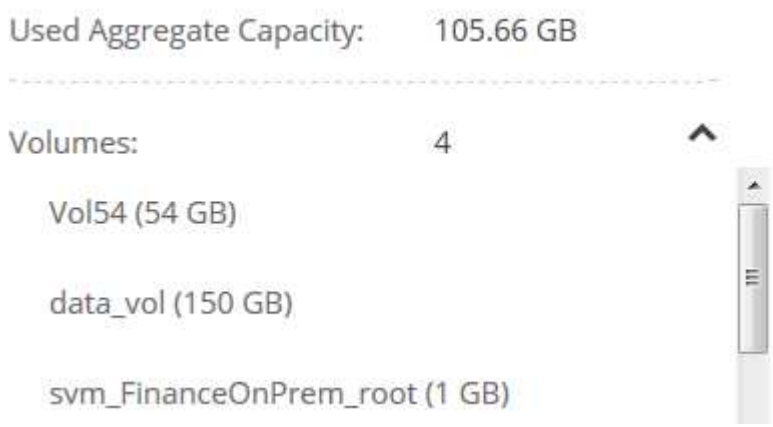
Se Cloud Manager non è in grado di fornire consigli per lo spostamento di un volume per evitare problemi di capacità, è necessario identificare i volumi da spostare e se è necessario spostarli in un altro aggregato sullo stesso sistema o in un altro sistema.

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.

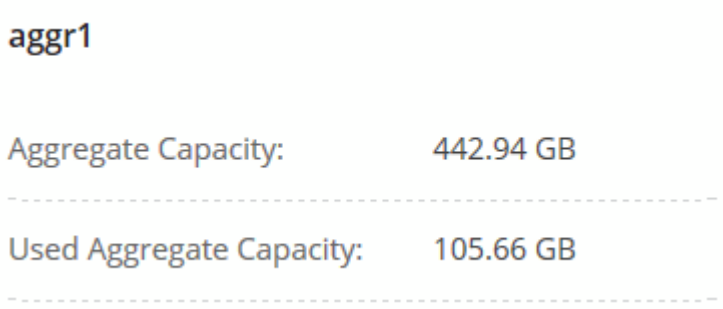
A proposito di questa attività

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".

Motivi per cui lo spostamento di un volume potrebbe risultare lento

Lo spostamento di un volume potrebbe richiedere più tempo del previsto se una delle seguenti condizioni è vera per Cloud Volumes ONTAP:

- Il volume è un clone.
- Il volume è il padre di un clone.
- L'aggregato di origine o di destinazione dispone di un disco HDD (st1) ottimizzato per il throughput singolo.
- Il sistema Cloud Volumes ONTAP è in AWS e un aggregato utilizza uno schema di denominazione precedente per gli oggetti. Entrambi gli aggregati devono utilizzare lo stesso formato dei nomi.

  Viene utilizzato uno schema di denominazione precedente se il tiering dei dati è stato attivato su un aggregato nella versione 9.4 o precedente.
- Le impostazioni di crittografia non corrispondono sugli aggregati di origine e destinazione, oppure è in corso una rekey.
- L'opzione *-tiering-policy* è stata specificata nello spostamento del volume per modificare il criterio di tiering.
- L'opzione *-generate-destination-key* è stata specificata durante lo spostamento del volume.

Tiering dei dati inattivi su storage a oggetti a basso costo

È possibile ridurre i costi di storage per Cloud Volumes ONTAP combinando un Tier di performance SSD o HDD per i dati hot con un Tier di capacità dello storage a oggetti per i dati inattivi. Per una panoramica generale, vedere "Panoramica sul tiering dei dati".

Per impostare il tiering dei dati, è sufficiente eseguire le seguenti operazioni:

Scegliere una configurazione supportata

Sono supportate la maggior parte delle configurazioni. Se si dispone di un sistema Cloud Volumes ONTAP standard, Premium o BYOL con la versione più recente, si consiglia di procedere. "Scopri di più".

Garantire la connettività tra Cloud Volumes ONTAP e lo storage a oggetti

- Per AWS, è necessario un endpoint VPC per S3. Scopri di più.
- Per Azure, non dovrai fare nulla finché Cloud Manager dispone delle autorizzazioni necessarie. Scopri di più.
- Per GCP, è necessario configurare la subnet per Private Google Access e impostare un account di servizio. Scopri di più.

Scegliere un criterio di tiering quando si crea, modifica o replica un volume

Cloud Manager richiede di scegliere una policy di tiering quando si crea, modifica o si replica un volume.

- "Tiering dei dati sui volumi di lettura/scrittura"
- "Tiering dei dati sui volumi di protezione dei dati"

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

- Non è necessario installare una licenza per le funzionalità per abilitare il tiering dei dati.
- Non è necessario creare il Tier di capacità (un bucket S3, un container Azure Blob o un bucket GCP). Cloud Manager fa tutto questo per te.

Configurazioni che supportano il tiering dei dati

È possibile abilitare il tiering dei dati quando si utilizzano configurazioni e funzionalità specifiche:

- Il tiering dei dati è supportato con Cloud Volumes ONTAP standard, Premium e BYOL, a partire dalle seguenti versioni:
  - Versione 9.2 in AWS
  - Versione 9.4 in Azure con sistemi a nodo singolo
  - Versione 9.6 in Azure con coppie ha
  - Versione 9.6 in GCP

  Il tiering dei dati non è supportato in Azure con il tipo di macchina virtuale DS3_v2.
- In AWS, il Tier di performance può essere SSD General Purpose, SSD IOPS con provisioning o HDD ottimizzati per il throughput.
- In Azure, il Tier di performance può essere costituito da dischi gestiti da SSD Premium, dischi gestiti da SSD Standard o dischi gestiti da HDD Standard.
- In GCP, il Tier di performance può essere SSD o HDD (dischi standard).

- Il tiering dei dati è supportato dalle tecnologie di crittografia.
- Il thin provisioning deve essere attivato sui volumi.

Requisiti per il tiering dei dati cold in AWS S3

Assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione consiste nella creazione di un endpoint VPC per il servizio S3. Per istruzioni, vedere "Documentazione AWS: Creazione di un endpoint gateway".

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

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

Requisiti per il tiering dei dati cold nello storage Azure Blob

Non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

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

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

Requisiti per tierare i dati cold in un bucket di storage Google Cloud

- La subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access".
- È necessario disporre di un account di servizio con il ruolo di amministratore dello storage predefinito. Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, è necessario selezionare questo account di servizio.

  "Impostare questo account del servizio di tiering come indicato di seguito":

  a. Assegnare il ruolo predefinito *Storage Admin* all'account del servizio di tiering.
  b. Aggiungere l'account del servizio Connector come *Service account User* all'account del servizio di tiering.

     È possibile fornire il ruolo dell'utente "nel passaggio 3 della procedura guidata quando si crea l'account del servizio di tiering", o. "assegnare il ruolo dopo la creazione dell'account di servizio".

     Sarà necessario selezionare l'account del servizio di tiering in un secondo momento quando si crea un ambiente di lavoro Cloud Volumes ONTAP.

  Se non si attiva il tiering dei dati e si seleziona un account di servizio quando si crea il sistema Cloud Volumes ONTAP, è necessario spegnere il sistema e aggiungere l'account di servizio a Cloud Volumes

ONTAP dalla console GCP.

Tiering dei dati dai volumi di lettura/scrittura

Cloud Volumes ONTAP è in grado di tierare i dati inattivi su volumi di lettura/scrittura per uno storage a oggetti conveniente, liberando il Tier di performance per i dati hot.

Fasi

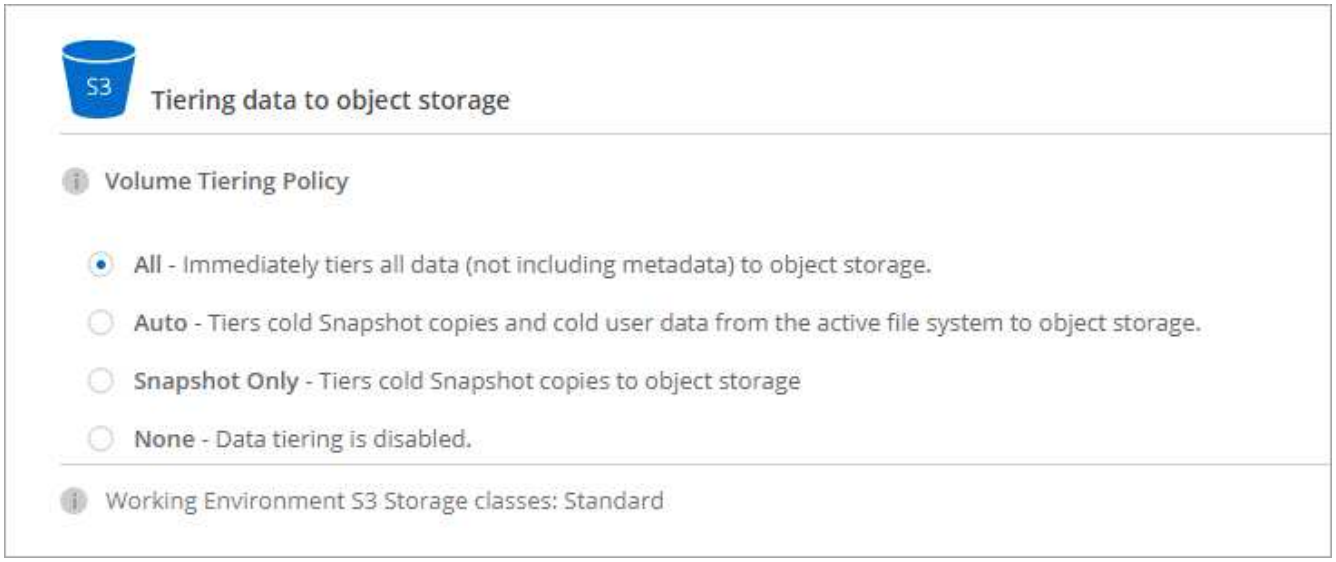
1. Nell'ambiente di lavoro, creare un nuovo volume o modificare il livello di un volume esistente:

Attività	Azione
Creare un nuovo volume	Fare clic su **Add New Volume** (Aggiungi nuovo volume).
Modificare un volume esistente	Selezionare il volume e fare clic su **Change Disk Type & Tiering Policy** (Modifica tipo di disco e policy di tiering).

2. Selezionare una policy di tiering.

   Per una descrizione di questi criteri, vedere "Panoramica sul tiering dei dati".

   Esempio



   Cloud Manager crea un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei dati.

   Se preferisci creare aggregati, puoi abilitare il tiering dei dati sugli aggregati quando li crei.

Tiering dei dati dai volumi di protezione dei dati

Cloud Volumes ONTAP può eseguire il tiering dei dati da un volume di protezione dei dati a un livello di capacità. Se si attiva il volume di destinazione, i dati si spostano gradualmente al livello di performance man mano che vengono letti.

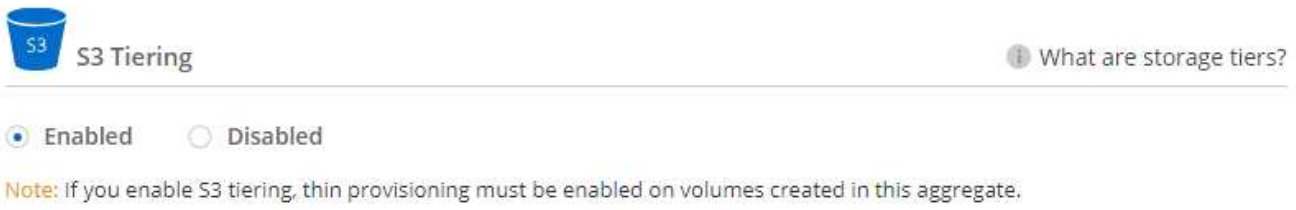
Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi

trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume.

2. Seguire le istruzioni fino a raggiungere la pagina di tiering e abilitare il tiering dei dati allo storage a oggetti.

Esempio



Per assistenza nella replica dei dati, vedere "Replica dei dati da e verso il cloud".

Modifica della classe di storage per i dati a più livelli

Dopo aver implementato Cloud Volumes ONTAP, è possibile ridurre i costi di storage modificando la classe di storage 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, pertanto è necessario prendere in considerazione questo aspetto prima di modificare la classe di storage.

La classe di storage per i dati a più livelli è estesa a tutto il sistema, non a it per volume.

Per informazioni sulle classi di storage supportate, vedere "Panoramica sul tiering dei dati".

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi su **Storage CLASSES** o **Blob Storage Tiering**.
2. Scegliere una classe di storage e fare clic su **Save** (Salva).

È possibile abilitare il tiering dei dati su un aggregato esistente?

No, non è possibile abilitare il tiering dei dati su un aggregato esistente. È possibile attivare il tiering dei dati solo su nuovi aggregati.

È possibile abilitare il tiering dei dati su un nuovo aggregato "creando un aggregato" oppure creando un nuovo volume con il tiering dei dati attivato. Cloud Manager creerebbe quindi un nuovo aggregato per il volume se non esiste già un aggregato abilitato al tiering dei dati.

Gestione delle VM di storage

Una VM di storage è una macchina virtuale in esecuzione in ONTAP che fornisce servizi di storage e dati ai client. Potresti sapere che si tratta di un *SVM* o di un *vserver*. Cloud Volumes ONTAP è configurato con una VM di storage per impostazione predefinita, ma alcune configurazioni supportano altre VM di storage.

Numero di VM storage supportate

Cloud Volumes ONTAP 9.7 supporta più macchine virtuali storage in AWS con determinate configurazioni e una licenza aggiuntiva. "Visualizza il numero di VM di storage supportate in AWS". Contattare il proprio account team per ottenere una licenza add-on SVM.

Tutte le altre configurazioni Cloud Volumes ONTAP supportano una VM di storage per il servizio dati e una VM di storage di destinazione utilizzata per il disaster recovery. È possibile attivare la VM di storage di destinazione per l'accesso ai dati in caso di interruzione della VM di storage di origine.

Una VM di storage copre l'intero sistema Cloud Volumes ONTAP (coppia ha o nodo singolo).

Creazione di VM storage aggiuntive

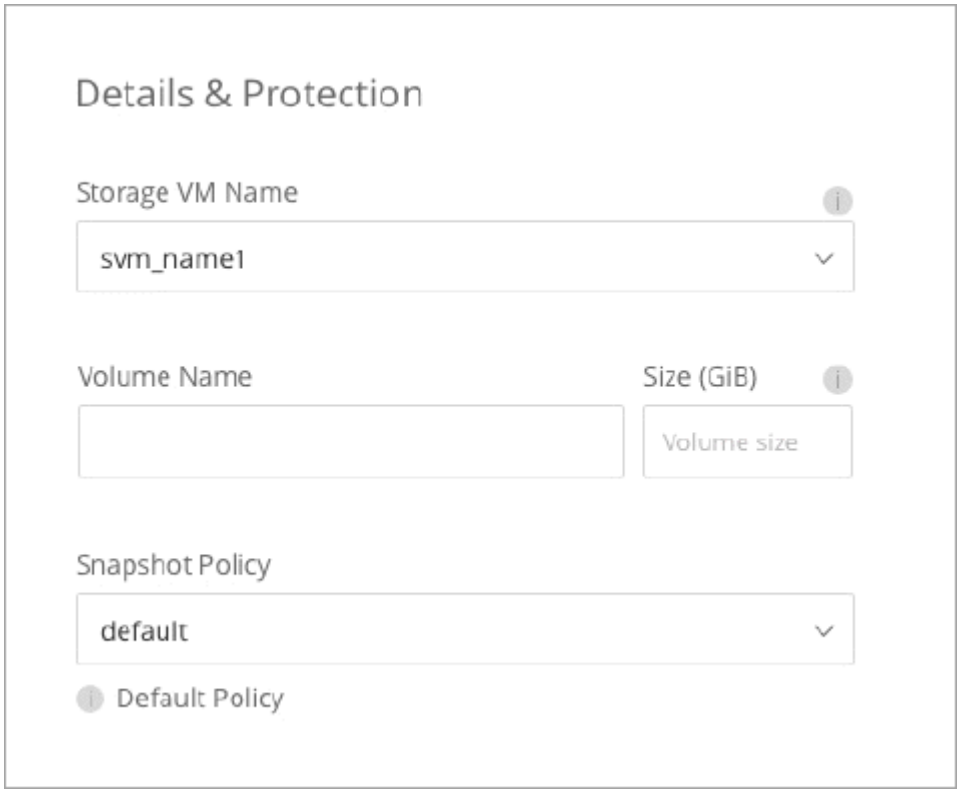
Se supportato dalla configurazione, è possibile creare ulteriori VM di storage utilizzando "System Manager o CLI".

- "Creazione di una SVM per l'accesso SMB"
- "Creazione di una SVM per l'accesso NFS"
- "Creazione di una SVM per l'accesso iSCSI"
- "Creazione di una SVM di destinazione per il disaster recovery"

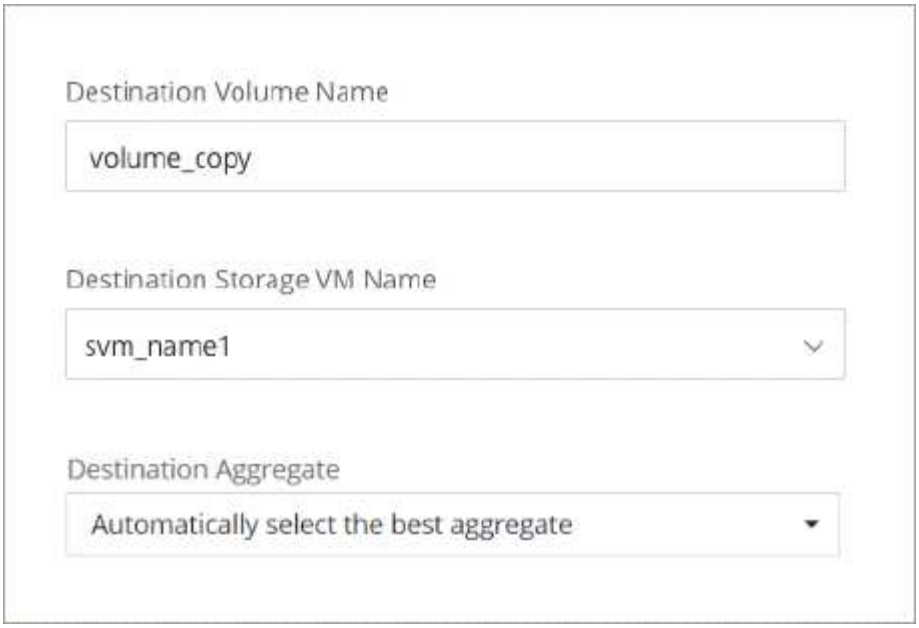
Utilizzo di più macchine virtuali storage in Cloud Manager

Cloud Manager supporta tutte le VM di storage aggiuntive create da System Manager o CLI.

Ad esempio, l'immagine seguente mostra come scegliere una VM di storage quando si crea un volume.



L'immagine seguente mostra come scegliere una VM di storage durante la replica di un volume su un altro sistema.



Gestione del disaster recovery delle macchine virtuali dello storage

Cloud Manager non fornisce alcun supporto di configurazione o orchestrazione per il disaster recovery delle macchine virtuali dello storage. È necessario utilizzare System Manager o la CLI.

- "Guida rapida alla preparazione del disaster recovery per SVM"
- "Guida di SVM Disaster Recovery Express"

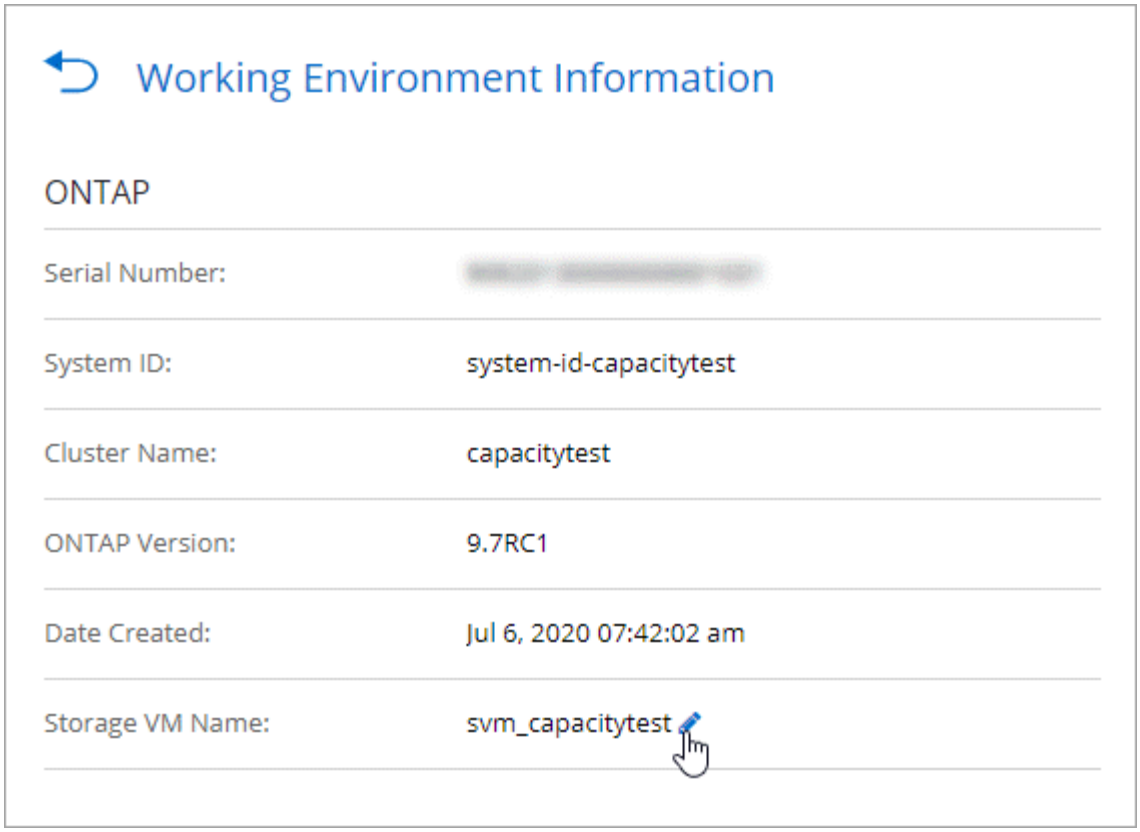
Modifica del nome della VM di storage

Cloud Manager assegna automaticamente un nome alla singola VM di storage creata per Cloud Volumes ONTAP. È possibile modificare il nome della VM di storage se si dispone di standard di denominazione rigorosi. Ad esempio, è possibile che il nome corrisponda a quello delle VM di storage per i cluster ONTAP.

Se hai creato altre VM di storage per Cloud Volumes ONTAP, non puoi rinominare le VM di storage da Cloud Manager. È necessario eseguire questa operazione direttamente da Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI.

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 della VM di storage.



3. Nella finestra di dialogo Modify SVM Name (Modifica nome SVM), modificare il nome, quindi fare clic su **Save** (Salva).

Utilizzo di Cloud Volumes ONTAP come storage persistente per Kubernetes

Cloud Manager può automatizzare l'implementazione di NetApp Trident sui cluster Kubernetes, in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container.

Trident è un progetto open source completamente supportato gestito da NetApp. Trident si integra in modo nativo con Kubernetes e il suo framework per volumi persistenti per eseguire il provisioning e la gestione dei volumi da sistemi che eseguono qualsiasi combinazione delle piattaforme storage NetApp. "Scopri di più su Trident".

La funzionalità Kubernetes non è supportata dai cluster ONTAP on-premise. È supportato solo con Cloud Volumes ONTAP.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti, che includono connettività tra cluster Kubernetes e Cloud Volumes ONTAP, connettività tra cluster Kubernetes e un connettore, una versione minima di Kubernetes 1.14,

almeno un nodo di lavoro in un cluster e molto altro ancora. Consulta l'elenco completo.

Aggiungi i tuoi cluster Kubernetes a Cloud Manager

In Cloud Manager, fai clic su **Kubernetes** e scopri i cluster direttamente dal servizio gestito del tuo provider di cloud oppure importa un cluster fornendo un file kubeconfig.

Connetti i tuoi cluster a Cloud Volumes ONTAP

Dopo aver aggiunto un cluster Kubernetes, fare clic su **connessione all'ambiente di lavoro** per connettere il cluster a uno o più sistemi Cloud Volumes ONTAP.

Avviare il provisioning dei volumi persistenti

Richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi. Cloud Manager crea classi di storage NFS e iSCSI da utilizzare per il provisioning di volumi persistenti.

"Scopri di più sul provisioning del tuo primo volume con Trident for Kubernetes".

Verifica dei prerequisiti

Prima di iniziare, assicurati che i cluster Kubernetes e il connettore soddisfino requisiti specifici.

Requisiti del cluster Kubernetes

- È necessaria la connettività di rete tra un cluster Kubernetes e il connettore e tra un cluster Kubernetes e Cloud Volumes ONTAP.

  Sia il connettore che Cloud Volumes ONTAP necessitano di una connessione all'endpoint API di Kubernetes:

  - Per i cluster gestiti, impostare un percorso tra il VPC di un cluster e il VPC in cui risiedono il connettore e Cloud Volumes ONTAP.
  - Per gli altri cluster, l'indirizzo IP del nodo master o del bilanciamento del carico (come indicato nel file kubeconfig) deve essere raggiungibile dal connettore e da Cloud Volumes ONTAP e deve presentare un certificato TLS valido.
- Un cluster Kubernetes può trovarsi in qualsiasi posizione che disponga della connettività di rete indicata sopra.
- Un cluster Kubernetes deve eseguire almeno la versione 1.14.

  La versione massima supportata è definita da Trident. "Fare clic qui per visualizzare la versione massima supportata di Kubernetes".
- Un cluster Kubernetes deve avere almeno un nodo di lavoro.
- Per i cluster in esecuzione in Amazon Elastic Kubernetes Service (Amazon EKS), ciascun cluster richiede l'aggiunta di un ruolo IAM per risolvere un errore di permessi. Dopo aver aggiunto il cluster, Cloud Manager richiederà l'esatto comando eksctl che risolve l'errore.

"Scopri i limiti delle autorizzazioni IAM".

- Per i cluster in esecuzione in Azure Kubernetes Service (AKS), a tali cluster deve essere assegnato il ruolo *Azure Kubernetes Service RBAC Cluster Admin*. Questo è necessario per consentire a Cloud Manager di installare Trident e configurare le classi di storage sul cluster.
- Per i cluster in esecuzione in Google Kubernetes Engine (GKE), questi cluster non devono utilizzare il sistema operativo predefinito ottimizzato per i container. Si consiglia di passare all'utilizzo di Ubuntu.

  Per impostazione predefinita, GKE utilizza Google "immagine ottimizzata per container", Che non dispone delle utility di cui Trident ha bisogno per montare i volumi.

Requisiti del connettore

Assicurarsi che il connettore disponga delle seguenti autorizzazioni e connessioni di rete.

Networking

- Il connettore necessita di 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.

Autorizzazioni necessarie per rilevare e gestire i cluster EKS

Il connettore necessita delle autorizzazioni di amministratore per rilevare e gestire i cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

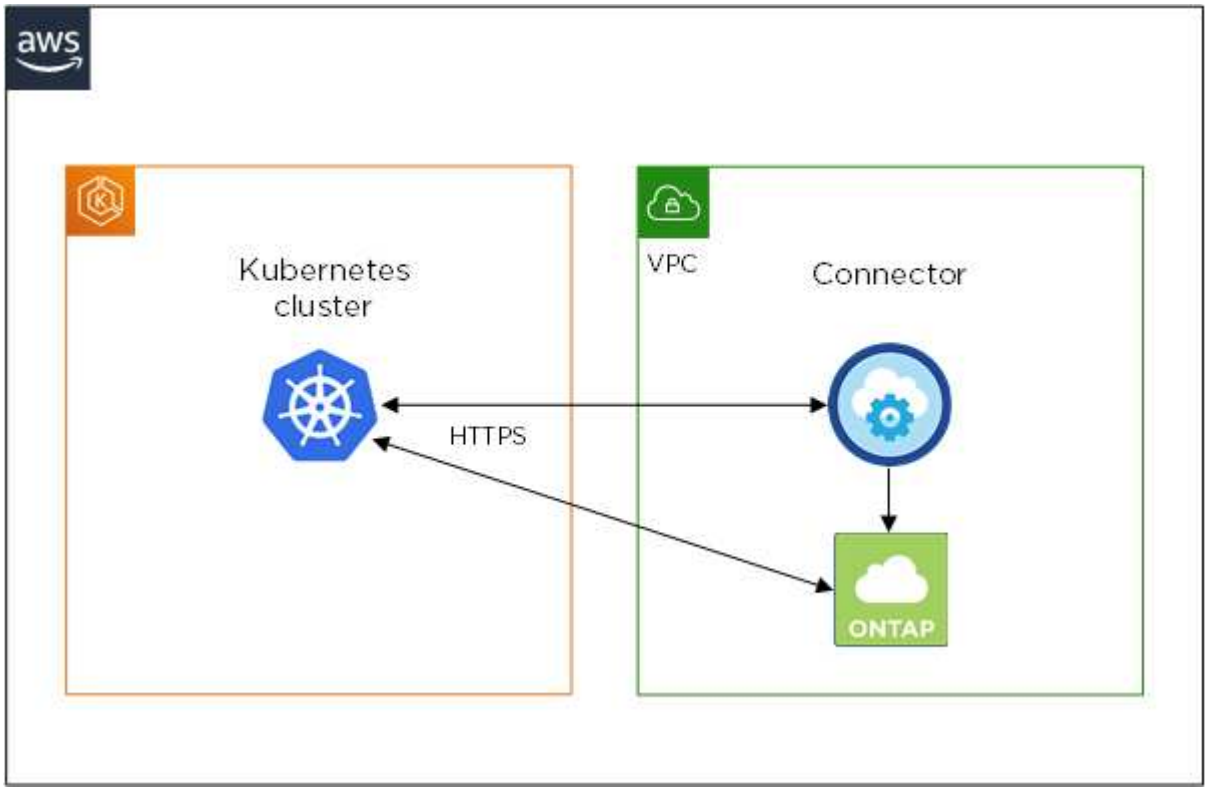
Autorizzazioni necessarie per rilevare e gestire i cluster GKE

Il connettore necessita delle seguenti autorizzazioni per rilevare e gestire i cluster Kubernetes in esecuzione in Google Kubernetes Engine (GKE):

```
container.*
```

Esempio di configurazione

L'immagine seguente mostra un esempio di cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (Amazon EKS) e le relative connessioni a Connector e Cloud Volumes ONTAP.



Aggiunta di cluster Kubernetes

Aggiungi i cluster Kubernetes a Cloud Manager scoprendo i cluster in esecuzione nel servizio Kubernetes gestito dal tuo provider cloud o importando il file kuberconfig di un cluster.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic su **Aggiungi cluster**.
3. Scegliere una delle opzioni disponibili:
   - Fare clic su **Discover Clusters** (Discover Clusters) per scoprire i cluster gestiti a cui Cloud Manager ha accesso in base alle autorizzazioni fornite al connettore.

     Ad esempio, se il connettore è in esecuzione in Google Cloud, Cloud Manager utilizza le autorizzazioni dell'account di servizio del connettore per rilevare i cluster in esecuzione in Google Kubernetes Engine (GKE).

   - Fare clic su **Import Cluster** (Importa cluster) per importare un cluster utilizzando un file kubeconfig.

     Dopo aver caricato il file, Cloud Manager verifica la connettività al cluster e salva una copia crittografata del file kubeconfig.

Risultato

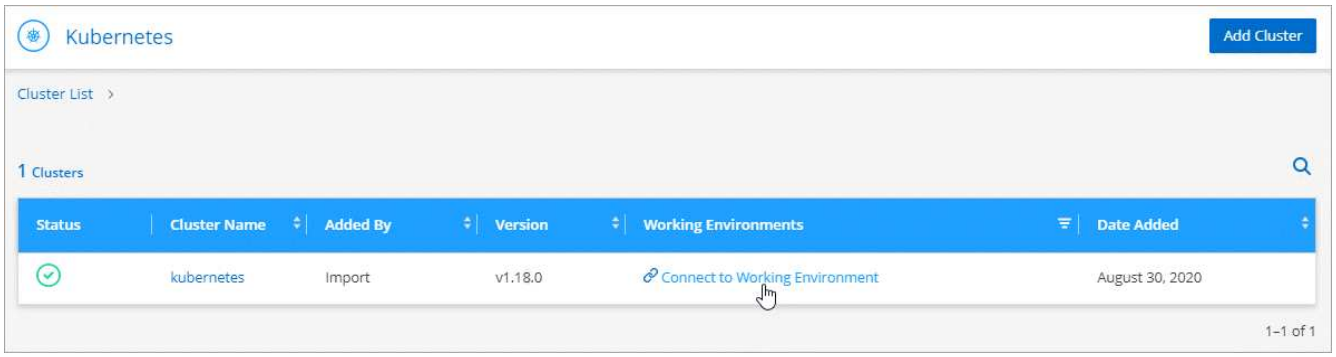
Cloud Manager aggiunge il cluster Kubernetes. È ora possibile collegare il cluster a Cloud Volumes ONTAP.

Connessione di un cluster a Cloud Volumes ONTAP

Collega un cluster Kubernetes a Cloud Volumes ONTAP in modo da poter utilizzare Cloud Volumes ONTAP come storage persistente per i container.

Fasi

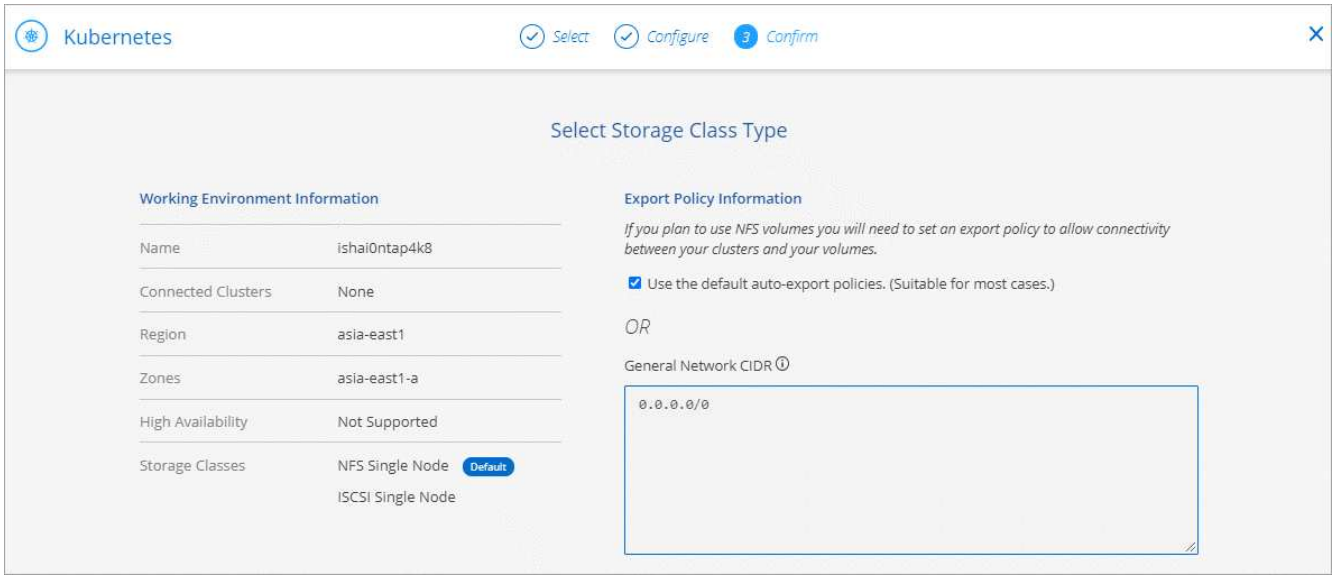
1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic su **Connect to Working Environment** (Connetti all'ambiente di lavoro) per il cluster appena aggiunto.



3. Selezionare un ambiente di lavoro e fare clic su **continua**.
4. Scegliere la classe di storage NetApp da utilizzare come classe di storage predefinita per il cluster Kubernetes e fare clic su **continua**.

   Quando un utente crea un volume persistente, il cluster Kubernetes può utilizzare questa classe di storage come storage back-end per impostazione predefinita.

5. Scegliere se utilizzare i criteri di esportazione automatica predefiniti o se aggiungere un blocco CIDR personalizzato.



6. Fare clic su **Aggiungi ambiente di lavoro**.

Risultato

Cloud Manager connette l'ambiente di lavoro al cluster, che può richiedere fino a 15 minuti.

Gestione dei cluster

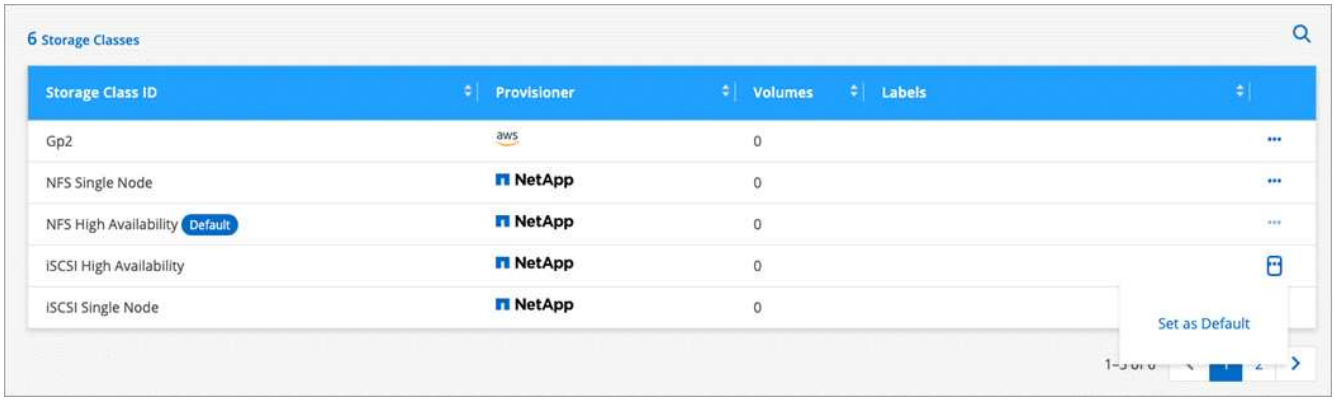
Cloud Manager consente di gestire i cluster Kubernetes modificando la classe di storage predefinita, aggiornando Trident e molto altro ancora.

Modifica della classe di storage predefinita

Assicurarsi di aver impostato una classe di storage Cloud Volumes ONTAP come classe di storage predefinita, in modo che i cluster utilizzino Cloud Volumes ONTAP come storage back-end.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Nella tabella **Storage CLASSES**, fare clic sul menu delle azioni all'estrema destra per la classe di storage che si desidera impostare come predefinita.



4. Fare clic su **Set as Default** (Imposta come predefinito).

Aggiornamento di Trident

Puoi aggiornare Trident da Cloud Manager quando è disponibile una nuova versione di Trident.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Se è disponibile una nuova versione, fare clic su **Upgrade** (Aggiorna) accanto alla versione di Trident.

Aggiornamento del file kubeconfig

Se hai aggiunto il cluster a Cloud Manager importando il file kubeconfig, puoi caricare l'ultimo file kubeconfig su Cloud Manager in qualsiasi momento. Questa operazione può essere eseguita se le credenziali sono state aggiornate, se sono stati modificati utenti o ruoli o se qualcosa è stato modificato in modo da influire sul

cluster, sull'utente, sugli spazi dei nomi o sull'autenticazione.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Fare clic su **Update Kubeconfig** (Aggiorna Kubeconfig*).
4. Quando richiesto dal browser Web, selezionare il file kubeconfig aggiornato e fare clic su **Open** (Apri).

Risultato

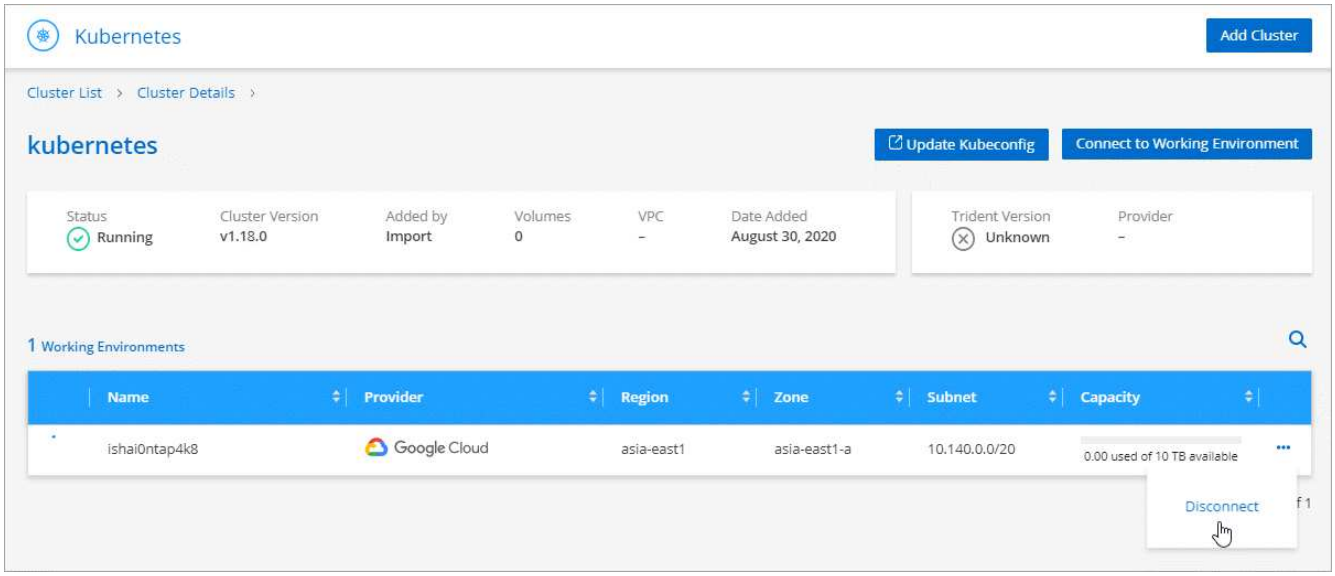
Cloud Manager aggiorna le informazioni sul cluster Kubernetes in base all'ultimo file kubeconfig.

Disconnessione di un cluster

Quando si disconnette un cluster da Cloud Volumes ONTAP, non è più possibile utilizzare tale sistema Cloud Volumes ONTAP come storage persistente per i container. I volumi persistenti esistenti non vengono cancellati.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.
2. Fare clic sul nome del cluster Kubernetes.
3. Nella tabella **ambienti di lavoro**, fare clic sul menu delle azioni a destra dell'ambiente di lavoro che si desidera disconnettere.



4. Fare clic su **Disconnetti**.

Risultato

Cloud Manager disconnette il cluster dal sistema Cloud Volumes ONTAP.

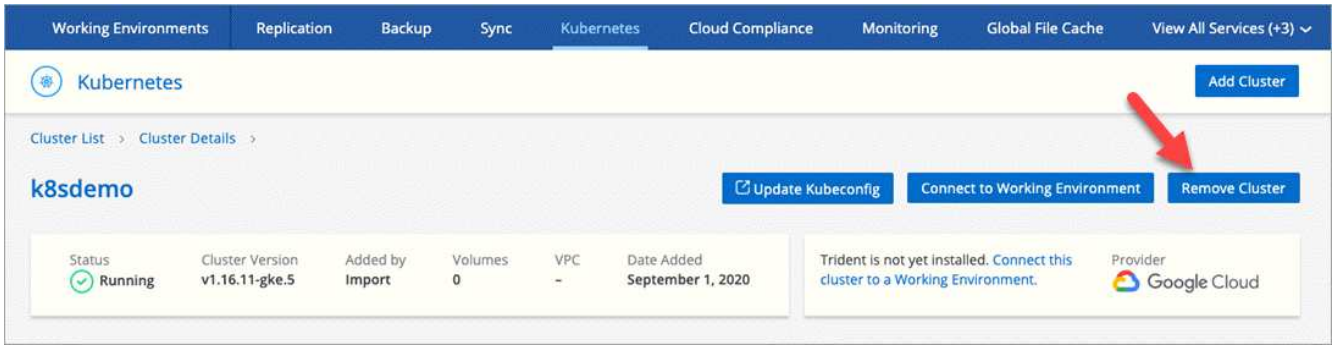
Rimozione di un cluster

Rimuovere i cluster decommissionati da Cloud Manager dopo aver scollegato tutti gli ambienti di lavoro dal cluster.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Kubernetes**.

2. Fare clic sul nome del cluster Kubernetes.
3. Fare clic su **Remove Cluster** (Rimuovi cluster).



Crittografia dei volumi con le soluzioni di crittografia NetApp

Cloud Volumes ONTAP supporta la crittografia dei volumi NetApp (NVE) e la crittografia aggregata NetApp (NAE) con un gestore di chiavi esterno. NVE e NAE sono soluzioni basate su software che consentono la crittografia dei volumi (data-at-rest) conforme a FIPS 140-2. "Scopri di più su queste soluzioni di crittografia".

A partire da Cloud Volumes ONTAP 9.7, i nuovi aggregati avranno attivato NAE per impostazione predefinita dopo aver configurato un gestore di chiavi esterno. I nuovi volumi che non fanno parte di un aggregato NAE avranno NVE abilitato per impostazione predefinita (ad esempio, se si dispone di aggregati già creati prima della configurazione di un gestore di chiavi esterno).

Cloud Volumes ONTAP non supporta la gestione delle chiavi integrata.

Di cosa hai bisogno

Il sistema Cloud Volumes ONTAP deve essere registrato presso il supporto NetApp. A partire da Cloud Manager 3.7.1, una licenza per la crittografia dei volumi NetApp viene installata automaticamente su ogni sistema Cloud Volumes ONTAP registrato presso il supporto NetApp.

- "Aggiunta di account NetApp Support Site a Cloud Manager"
- "Registrazione di sistemi pay-as-you-go"

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

Fasi

1. Esaminare l'elenco dei Key Manager supportati in "Tool di matrice di interoperabilità NetApp".

   Cercare la soluzione **Key Manager**.

2. "Connettersi all'interfaccia utente di Cloud Volumes ONTAP".
3. Installare i certificati SSL e connettersi ai server di gestione delle chiavi esterni.

   "ONTAP 9 Guida all'alimentazione per la crittografia NetApp: Configurazione della gestione esterna delle chiavi"

Replica dei dati tra sistemi

È possibile replicare i dati tra ambienti di lavoro scegliendo una replica dei dati una tantum per il trasferimento dei dati o una pianificazione ricorrente per il disaster recovery o la conservazione a lungo termine. Ad esempio, è possibile configurare la replica dei dati da un sistema ONTAP on-premise a Cloud Volumes ONTAP per il disaster recovery.

Cloud Manager semplifica la replica dei dati tra volumi su sistemi separati utilizzando le tecnologie SnapMirror e SnapVault. È sufficiente identificare il volume di origine e il volume di destinazione, quindi scegliere una policy e una pianificazione di replica. Cloud Manager acquista i dischi richiesti, configura le relazioni, applica la policy di replica e avvia il trasferimento di riferimento tra i volumi.

Il trasferimento di riferimento include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di origine.

Cloud Manager consente la replica dei dati tra i seguenti tipi di ambienti di lavoro:

- Da un sistema Cloud Volumes ONTAP a un altro sistema Cloud Volumes ONTAP
- Tra un sistema Cloud Volumes ONTAP e un cluster ONTAP on-premise
- Da un cluster ONTAP on-premise a un altro cluster ONTAP on-premise

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 sicurezza dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 11104 e 11105.

  Queste regole sono incluse nel gruppo di protezione predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).
- Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e un sistema in Azure, è necessario disporre di una connessione VPN tra AWS VPC e Azure VNET.

Requisiti specifici dei cluster ONTAP

- È necessario installare una licenza SnapMirror attiva.
- Se il cluster si trova all'interno della propria sede, si dovrebbe disporre di una connessione dalla rete aziendale ad AWS o Azure, che in genere è una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Per ulteriori informazioni, consultare la Guida rapida di peering di cluster e SVM per la versione di ONTAP in uso.

Configurazione della replica dei dati tra sistemi

Puoi replicare i dati tra sistemi Cloud Volumes ONTAP e cluster ONTAP scegliendo una replica dei dati una tantum, che può aiutarti a spostare i dati da e verso il cloud, o una pianificazione ricorrente, che può aiutarti con il disaster recovery o la conservazione a lungo termine.

A proposito di questa attività

Cloud Manager supporta configurazioni di protezione dei dati semplici, fanout e a cascata:

- In una configurazione semplice, la replica avviene dal volume A al volume B.
- In una configurazione fanout, la replica avviene dal volume A a più destinazioni.
- In una configurazione a cascata, la replica avviene dal volume A al volume B e dal volume B al volume C.

È possibile configurare configurazioni fanout e a cascata in Cloud Manager impostando più repliche di dati tra sistemi. Ad esempio, replicando un volume dal sistema A al sistema B e replicando lo stesso volume dal sistema B al sistema C.

Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume:

2. Se vengono visualizzate le pagine Source (origine) e Destination peering Setup (Configurazione peering destinazione), selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.

   La rete intercluster deve essere configurata in modo che i peer del cluster dispongano di una *connettività full-mesh a coppie*, il che significa che ogni coppia di cluster in una relazione peer del cluster dispone di connettività tra tutte le proprie LIF intercluster.

   Queste pagine vengono visualizzate se l'origine o la destinazione è un cluster ONTAP con più LIF.

3. Nella pagina Source Volume Selection (selezione volume di origine), selezionare il volume che si desidera replicare.
4. Nella pagina Destination Volume Name and Tiering (Nome volume di destinazione e tiering), specificare il nome del volume di destinazione, scegliere un tipo di disco sottostante, modificare una delle opzioni avanzate e fare clic su **Continue** (continua).

   Se la destinazione è un cluster ONTAP, è necessario specificare anche la SVM di destinazione e l'aggregato.

5. Nella pagina velocità di trasferimento massima, specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.
6. Nella pagina Replication Policy (Criteri di replica), scegliere uno dei criteri predefiniti o fare clic su **Additional Policies** (Criteri aggiuntivi), quindi selezionare uno dei criteri avanzati.

Per ulteriori informazioni, vedere "Scelta di un criterio di replica".

Se si sceglie un criterio di backup personalizzato (SnapVault), le etichette associate al criterio devono corrispondere alle etichette delle copie Snapshot sul volume di origine. Per ulteriori informazioni, vedere "Come funzionano le policy di backup".

7. Nella pagina Pianificazione, scegliere una copia singola o una pianificazione ricorrente.

   Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione nel cluster *destination* utilizzando System Manager.

8. Nella pagina Review (esamina), rivedere le selezioni, quindi fare clic su **Go** (Vai).

Risultato

Cloud Manager avvia il processo di replica dei dati. È possibile visualizzare i dettagli relativi alla replica nella pagina Replication Status (Stato replica).

Gestione delle pianificazioni e delle relazioni di replica dei dati

Dopo aver configurato la replica dei dati tra due sistemi, è possibile gestire la pianificazione e la relazione della replica dei dati da Cloud Manager.

Fasi

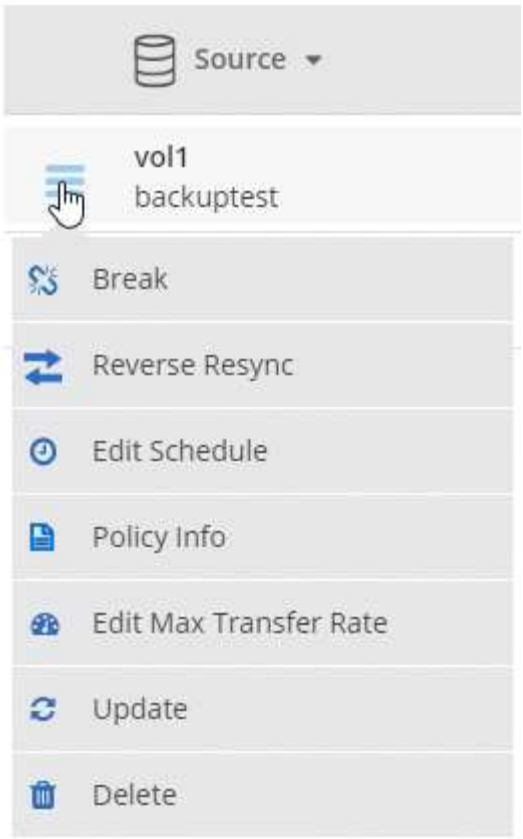
1. Nella pagina ambienti di lavoro, visualizzare lo stato della replica per tutti gli ambienti di lavoro nell'area di lavoro o per un ambiente di lavoro specifico:

Opzione	Azione
Tutti gli ambienti di lavoro nello spazio di lavoro	Nella parte superiore di Cloud Manager, fare clic su **Replication**.
Un ambiente di lavoro specifico	Aprire l'ambiente di lavoro e fare clic su **Replications** (repliche).

2. Esaminare lo stato delle relazioni di replica dei dati per verificare che siano integre.

   Se lo stato di una relazione è inattivo e lo stato di mirroring non è inizializzato, è necessario inizializzare la relazione dal sistema di destinazione per eseguire la replica dei dati in base alla pianificazione definita. È possibile inizializzare la relazione utilizzando System Manager o l'interfaccia della riga di comando (CLI). Questi stati possono essere visualizzati quando il sistema di destinazione non funziona e poi torna in linea.

3. Selezionare l'icona del menu accanto al volume di origine, quindi scegliere una delle azioni disponibili.



La seguente tabella descrive le azioni disponibili:

Azione	Descrizione
Rompere	Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati. Questa opzione viene generalmente utilizzata quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline. Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati e la riattivazione di un volume di origine, consultare la Guida rapida al disaster recovery di ONTAP 9.
Risincronizzare	Consente di ripristinare una relazione interrotta tra i volumi e di riprendere la replica dei dati in base alla pianificazione definita. Quando si risincronizzano i volumi, i contenuti del volume di destinazione vengono sovrascritti dai contenuti del volume di origine. Per eseguire una risincronizzazione inversa, che risincronizza i dati dal volume di destinazione al volume di origine, vedere la "Guida rapida per il disaster recovery dei volumi di ONTAP 9".
Risincronizzazione inversa	Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine originale viene sovrascritto dal contenuto del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline. Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.

Azione	Descrizione
Modifica pianificazione	Consente di scegliere una pianificazione diversa per la replica dei dati.
Info policy	Mostra il criterio di protezione assegnato alla relazione di replica dei dati.
Modifica velocità di trasferimento massima	Consente di modificare la velocità massima (in kilobyte al secondo) alla quale è possibile trasferire i dati.
Aggiornare	Avvia un trasferimento incrementale per aggiornare il volume di destinazione.
Eliminare	Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati. Questa azione elimina anche la relazione peer del cluster e la relazione peer SVM (Storage Virtual Machine), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, Cloud Manager aggiorna la relazione o la pianificazione.

Scelta di un criterio di replica

Quando si imposta la replica dei dati in Cloud Manager, potrebbe essere necessario un aiuto nella scelta di una policy di replica. Un criterio di replica definisce il modo in cui il sistema storage replica i dati da un volume di origine a un volume di destinazione.

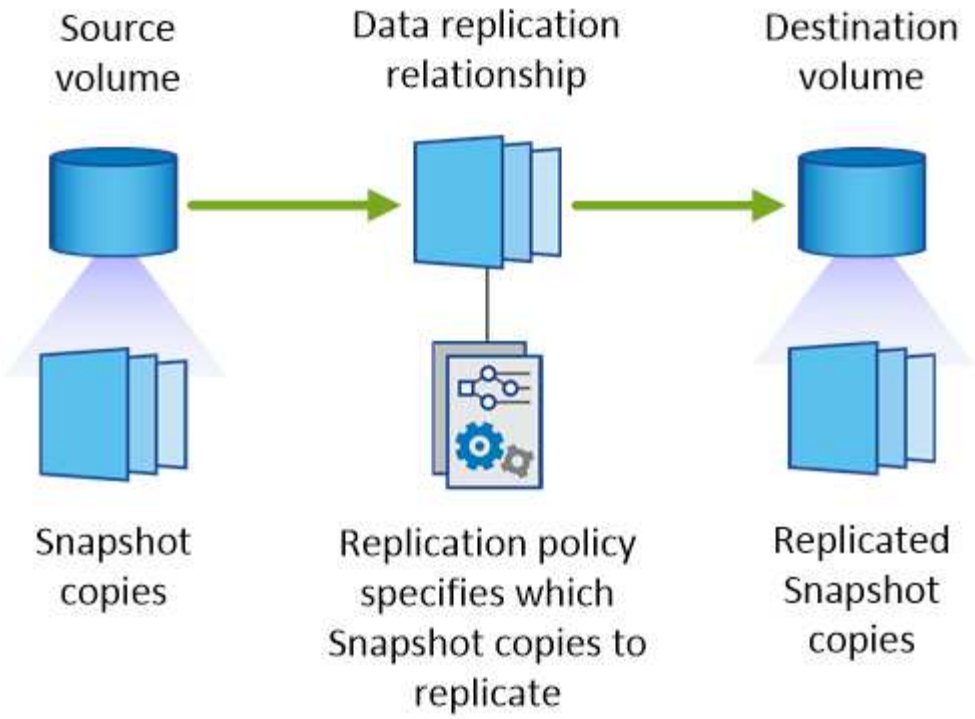
Quali sono le funzioni delle policy di replica

Il sistema operativo ONTAP crea automaticamente i backup denominati copie Snapshot. Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato del file system in un momento specifico.

Quando si replicano i dati tra sistemi, si replicano le copie Snapshot da un volume di origine a un volume di destinazione. Un criterio di replica specifica quali copie Snapshot replicare dal volume di origine al volume di destinazione.

Le policy di replica sono anche denominate policy di *protezione*, in quanto sono basate sulle tecnologie SnapMirror e SnapVault, che forniscono protezione dal disaster recovery e backup e ripristino disk-to-disk.

La seguente immagine mostra la relazione tra le copie Snapshot e i criteri di replica:



Tipi di policy di replica

Esistono tre tipi di policy di replica:

- Un criterio *Mirror* replica le nuove copie Snapshot create in un volume di destinazione.

  È possibile utilizzare queste copie Snapshot per proteggere il volume di origine in preparazione al disaster recovery o alla replica dei dati una tantum. È possibile attivare il volume di destinazione per l'accesso ai dati in qualsiasi momento.

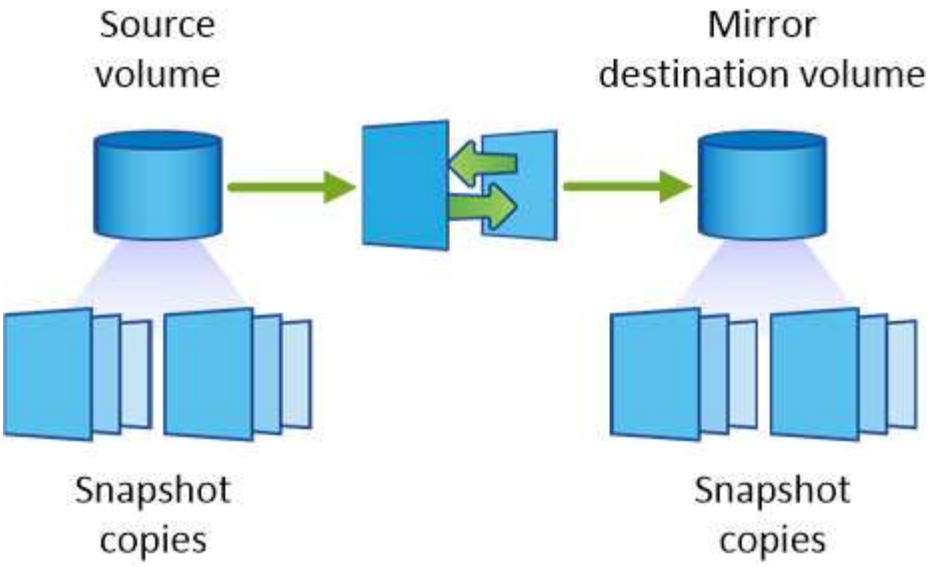
- Un criterio *Backup* replica copie Snapshot specifiche in un volume di destinazione e le conserva per un periodo di tempo più lungo rispetto al volume di origine.

  È possibile ripristinare i dati da queste copie Snapshot quando i dati vengono danneggiati o persi e conservarli per la conformità agli standard e altri scopi correlati alla governance.

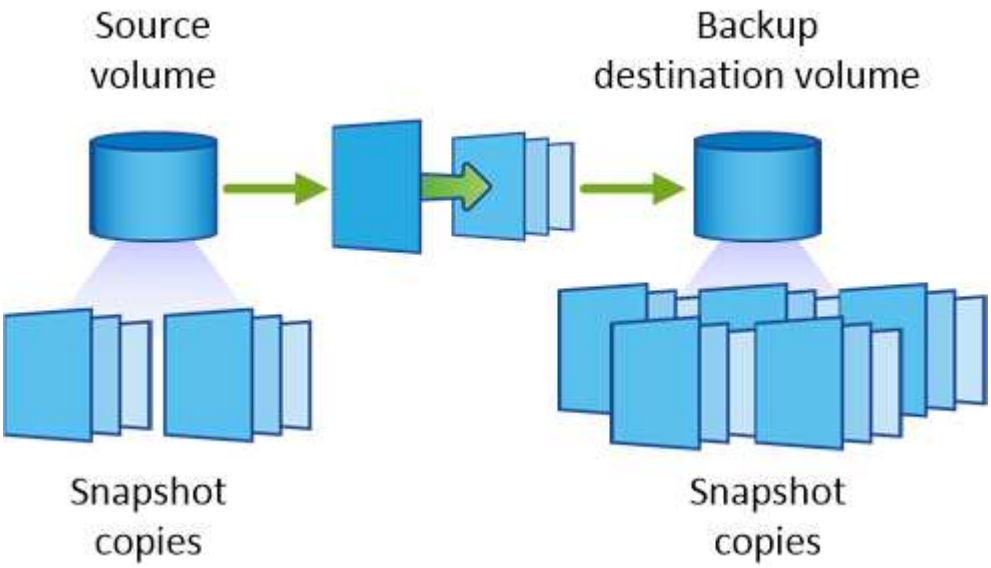
- Una policy di *Mirror e Backup* fornisce sia il disaster recovery che la conservazione a lungo termine.

  Ogni sistema include una policy di backup e mirroring predefinita, che funziona bene per molte situazioni. Se hai bisogno di policy personalizzate, puoi crearle usando System Manager.

Le seguenti immagini mostrano la differenza tra i criteri Mirror e Backup. Un criterio Mirror esegue il mirroring delle copie Snapshot disponibili sul volume di origine.



Una policy di backup conserva in genere le copie Snapshot più a lungo di quanto non vengano conservate nel volume di origine:



Come funzionano le policy di backup

A differenza dei criteri di mirroring, i criteri di backup (SnapVault) replicano copie Snapshot specifiche in un volume di destinazione. È importante comprendere il funzionamento dei criteri di backup se si desidera utilizzare i propri criteri invece dei criteri predefiniti.

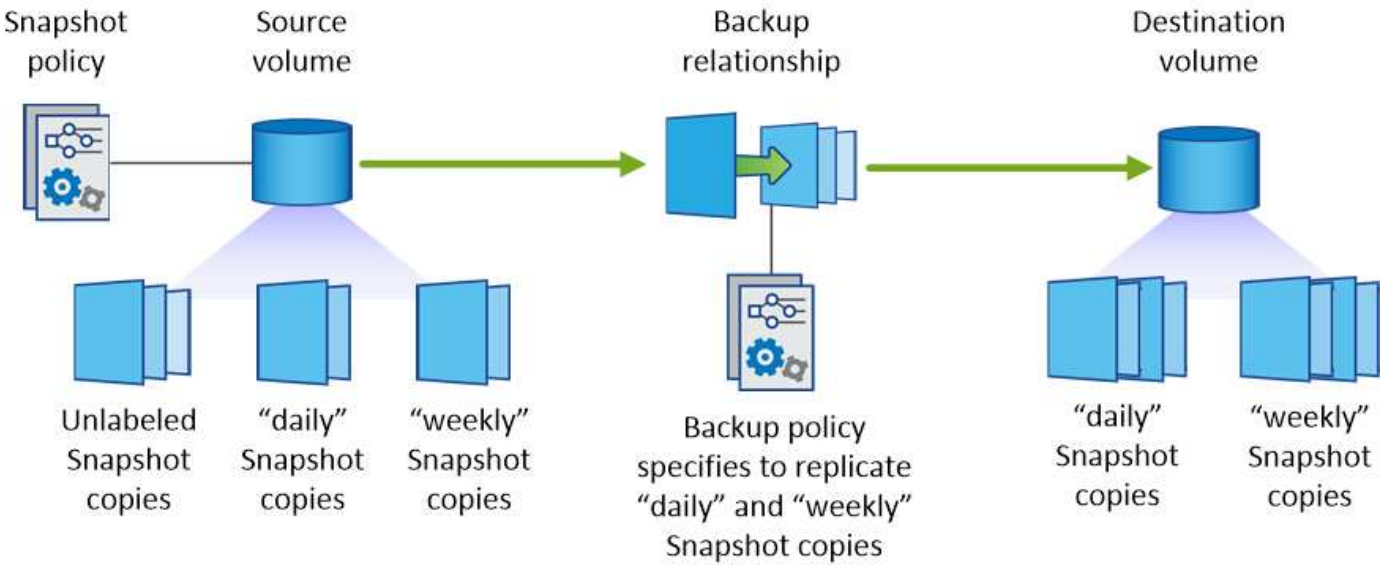
Comprensione della relazione tra le etichette delle copie Snapshot e le policy di backup

Una policy Snapshot definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare e come etichettarle. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti ed etichettarle "ogni giorno".

Un criterio di backup include regole che specificano le copie Snapshot etichettate da replicare in un volume di destinazione e il numero di copie da conservare. Le etichette definite in un criterio di backup devono corrispondere a una o più etichette definite in un criterio Snapshot. In caso contrario, il sistema non può

replicare alcuna copia Snapshot.

Ad esempio, una policy di backup che include le etichette "giornaliere" e "settimanali" produce la replica delle copie Snapshot che includono solo quelle etichette. Non vengono replicate altre copie Snapshot, come mostrato nell'immagine seguente:



Policy predefinite e policy personalizzate

La policy Snapshot predefinita crea copie Snapshot orarie, giornaliere e settimanali, conservando sei copie Snapshot orarie, due giornaliere e due copie Snapshot settimanali.

È possibile utilizzare facilmente un criterio di backup predefinito con il criterio Snapshot predefinito. Le policy di backup predefinite replicano copie Snapshot giornaliere e settimanali, conservando sette copie Snapshot giornaliere e 52 copie Snapshot settimanali.

Se si creano criteri personalizzati, le etichette definite da tali criteri devono corrispondere. È possibile creare policy personalizzate utilizzando System Manager.

Replica dei dati da NetApp HCI a Cloud Volumes ONTAP

Se si tenta di replicare i dati da NetApp HCI a Cloud Volumes ONTAP, è possibile farlo su un sistema NetApp HCI che esegue il software NetApp Element utilizzando SnapMirror. In alternativa, è possibile replicare i dati sui volumi creati su un sistema ONTAP Select in esecuzione come guest virtuale in una soluzione NetApp HCI su Cloud Volumes ONTAP.

Per ulteriori informazioni, fare riferimento ai seguenti report tecnici:

- "Report tecnico 4641: Protezione dei dati NetApp HCI"
- "Report tecnico 4651: Architettura e configurazione di NetApp SolidFire SnapMirror"

Monitorare le performance

Scopri di più sul servizio di monitoraggio

Sfruttando "Servizio NetApp Cloud Insights", Cloud Manager ti offre informazioni sullo

stato di salute e sulle performance delle tue istanze di Cloud Volumes ONTAP e ti aiuta a risolvere i problemi e ottimizzare le performance del tuo ambiente di cloud storage.

Caratteristiche

- Monitorare automaticamente tutti i volumi
- Visualizza i dati sulle performance dei volumi in termini di IOPS, throughput e latenza
- Identifica i problemi di performance per ridurre al minimo l'impatto su utenti e applicazioni

Cloud provider supportati

Il servizio di monitoraggio è supportato con Cloud Volumes ONTAP per AWS.

Costo

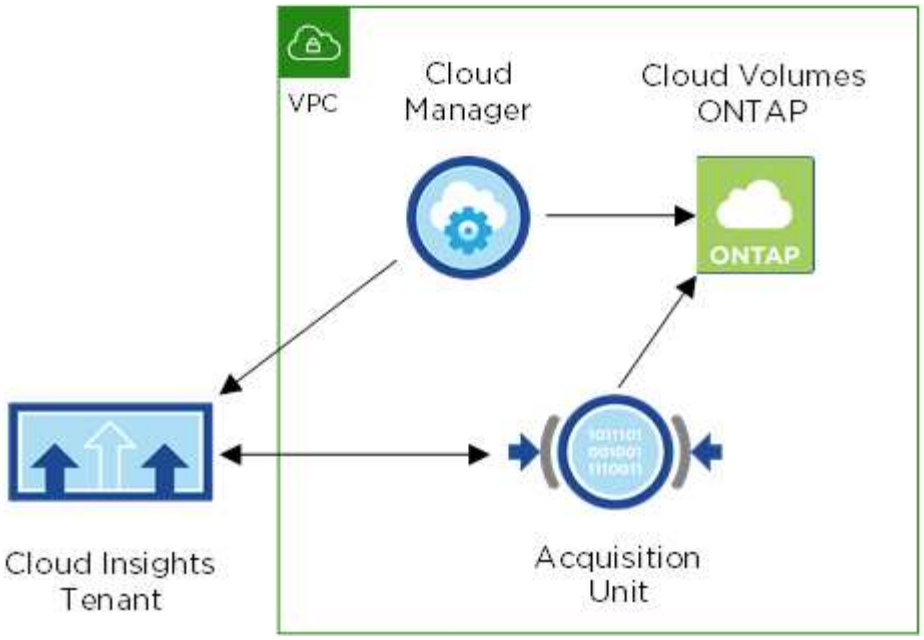
Il monitoraggio è attualmente disponibile come anteprima. L'attivazione è gratuita, ma Cloud Manager lancia una macchina virtuale nel VPC per facilitare il monitoraggio. Questa macchina virtuale comporta costi da parte del tuo cloud provider.

Come funziona Cloud Insights con Cloud Manager

Ad alto livello, l'integrazione di Cloud Insights con Cloud Manager funziona come segue:

1. Il servizio di monitoraggio viene attivato su Cloud Volumes ONTAP.
2. Cloud Manager configura il tuo ambiente. Esegue le seguenti operazioni:
    a. Crea un tenant Cloud Insights (chiamato anche *ambiente*) e associa tutti gli utenti del tuo account Cloud Central al tenant.
    b. Consente una versione di prova gratuita di 30 giorni di Cloud Insights.
    c. Implementa una macchina virtuale nel VPC chiamata unità di acquisizione, che facilita il monitoraggio dei volumi (si tratta della macchina virtuale menzionata nella sezione dei costi sopra).
    d. Collega l'unità di acquisizione a Cloud Volumes ONTAP e al tenant Cloud Insights.
3. In Cloud Manager, fai clic su Monitoring (monitoraggio) e utilizza i dati delle performance per risolvere i problemi e ottimizzare le performance.

La seguente immagine mostra la relazione tra questi componenti:



L'unità di acquisizione

Quando si attiva il monitoraggio, Cloud Manager implementa un'unità di acquisizione nella stessa sottorete del connettore.

Un' *unità di acquisizione* raccoglie i dati delle performance da Cloud Volumes ONTAP e li invia al tenant Cloud Insights. Cloud Manager interroga i dati e li presenta.

Tenere presente quanto segue sull'istanza dell'unità di acquisizione:

- L'unità di acquisizione viene eseguita su un'istanza t3.xlarge con un volume GP2 da 100 GB.
- L'istanza è denominata *AcquisitionUnit* con un hash generato (UUID) concatenato ad essa. Ad esempio: *AcquisitionUnit-FAN7FqeH*
- Per ogni connettore viene implementata una sola unità di acquisizione.
- L'istanza deve essere in esecuzione per accedere alle informazioni sulle prestazioni nella scheda Monitoring (monitoraggio).

Tenant Cloud Insights

Cloud Manager imposta un *tenant* per te quando abiliti il monitoraggio. Un tenant Cloud Insights consente di accedere ai dati sulle prestazioni raccolti dall'unità di acquisizione. Il tenant è una partizione di dati sicura all'interno del servizio NetApp Cloud Insights.

Interfaccia web di Cloud Insights

La scheda Monitoring (monitoraggio) di Cloud Manager fornisce dati di base sulle performance dei volumi. È possibile accedere all'interfaccia Web di Cloud Insights dal browser per eseguire un monitoraggio più approfondito e configurare gli avvisi per i sistemi Cloud Volumes ONTAP.

Prova gratuita e abbonamento

Cloud Manager offre una versione di prova gratuita di 30 giorni di Cloud Insights per fornire dati sulle performance all'interno di Cloud Manager e per consentirti di esplorare le funzionalità offerte dall'edizione standard di Cloud Insights.

Devi iscriverti entro la fine della prova gratuita, altrimenti il tenant Cloud Insights verrà cancellato. Puoi iscriverti all'edizione Basic, Standard o Premium per continuare a utilizzare la funzionalità Monitoring di Cloud Manager.

"Scopri come iscriverti a Cloud Insights".

Monitoraggio di Cloud Volumes ONTAP in AWS

Completa alcuni passaggi per iniziare a monitorare le performance di Cloud Volumes ONTAP.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare il supporto per la configurazione

È necessaria una nuova installazione di Cloud Manager 3.8.4 o successiva in AWS, Cloud Volumes ONTAP in AWS e devi essere un nuovo cliente Cloud Insights.

Abilitare il monitoraggio sul sistema nuovo o esistente

- Nuovi ambienti di lavoro: Assicurarsi di mantenere attivato il monitoraggio quando si crea l'ambiente di lavoro (attivato per impostazione predefinita).
- Ambienti di lavoro esistenti: Selezionare un ambiente di lavoro e fare clic su **Avvia monitoraggio**.

Visualizzare i dati sulle performance

Fare clic su **Monitoring** (monitoraggio) e visualizzare i dati delle performance dei volumi.

Iscriviti a Cloud Insights

Iscriviti prima della fine della prova gratuita di 30 giorni per continuare a visualizzare i dati sulle performance in Cloud Manager e Cloud Insights. "Scopri come iscriverti".

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata.

Versioni supportate di Cloud Manager

È necessaria una nuova installazione di Cloud Manager 3.8.4 o successiva. È necessaria una nuova installazione perché è necessaria una nuova infrastruttura per abilitare il servizio di monitoraggio. Questa infrastruttura è disponibile a partire dalle nuove installazioni di Cloud Manager 3.8.4.

Versioni di Cloud Volumes ONTAP supportate

Qualsiasi versione di Cloud Volumes ONTAP in AWS.

Requisito Cloud Insights

Devi essere un nuovo cliente Cloud Insights. Il monitoraggio non è supportato se si dispone già di un tenant Cloud Insights.

Indirizzo e-mail per Cloud Central

L'indirizzo e-mail dell'account utente Cloud Central deve essere l'indirizzo e-mail aziendale. I domini email gratuiti come gmail e hotmail non sono supportati quando si crea un tenant Cloud Insights.

Collegamento in rete per l'unità di acquisizione

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Cloud Insights. Il certificato client deve essere passato al server Cloud Insights per essere autenticato. A tale scopo, il proxy deve essere impostato per inoltrare la richiesta http al server Cloud Insights senza decifrare i dati.

L'unità di acquisizione utilizza i seguenti due endpoint per comunicare con Cloud Insights. Se si dispone di un firewall tra il server dell'unità di acquisizione e Cloud Insights, sono necessari questi endpoint durante la configurazione delle regole del firewall:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Ad esempio:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contattaci tramite la chat in-product se hai bisogno di aiuto per identificare il tuo dominio Cloud Insights e l'ID tenant.

Collegamento in rete per il connettore

Analogamente all'unità di acquisizione, il connettore deve essere collegato in uscita al tenant Cloud Insights. Tuttavia, l'endpoint a cui il connettore entra in contatto è leggermente diverso. Contatta l'URL host del tenant utilizzando l'ID tenant abbreviato:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Ad esempio:
```

```
 https://abcd12345.c01.cloudinsights.netapp.com
Se hai bisogno di aiuto per identificare l'URL host del tenant, puoi
contattarci tramite la chat del prodotto.
```

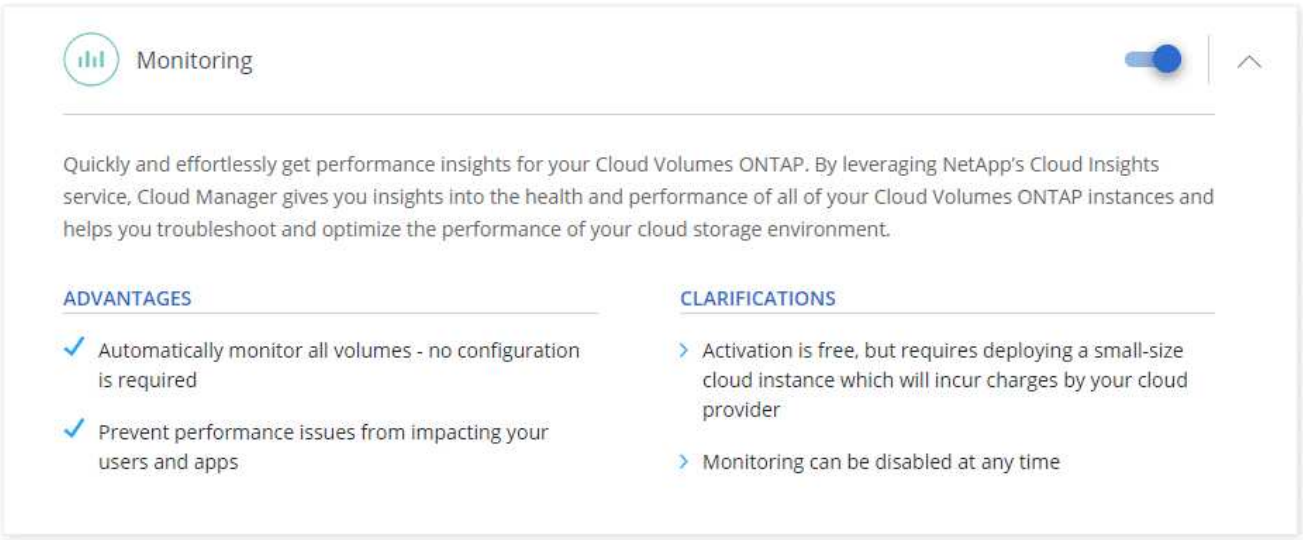
Abilitazione del monitoraggio su un nuovo sistema

Il servizio di monitoraggio viene attivato per impostazione predefinita nella procedura guidata dell'ambiente di

lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare attivato il servizio e fare clic su **continua**.

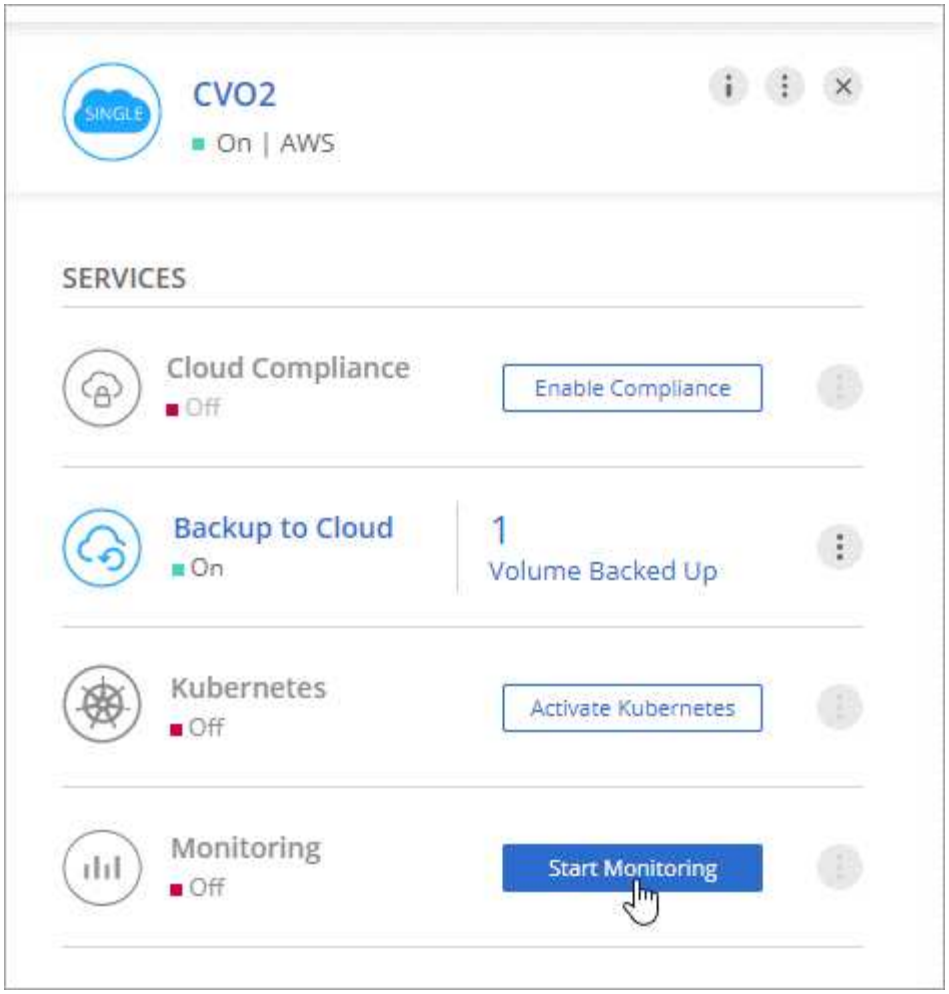


Abilitazione del monitoraggio su un sistema esistente

Consentire il monitoraggio in qualsiasi momento dall'ambiente di lavoro.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.
3. Nel riquadro a destra, fare clic su **Avvia monitoraggio**.



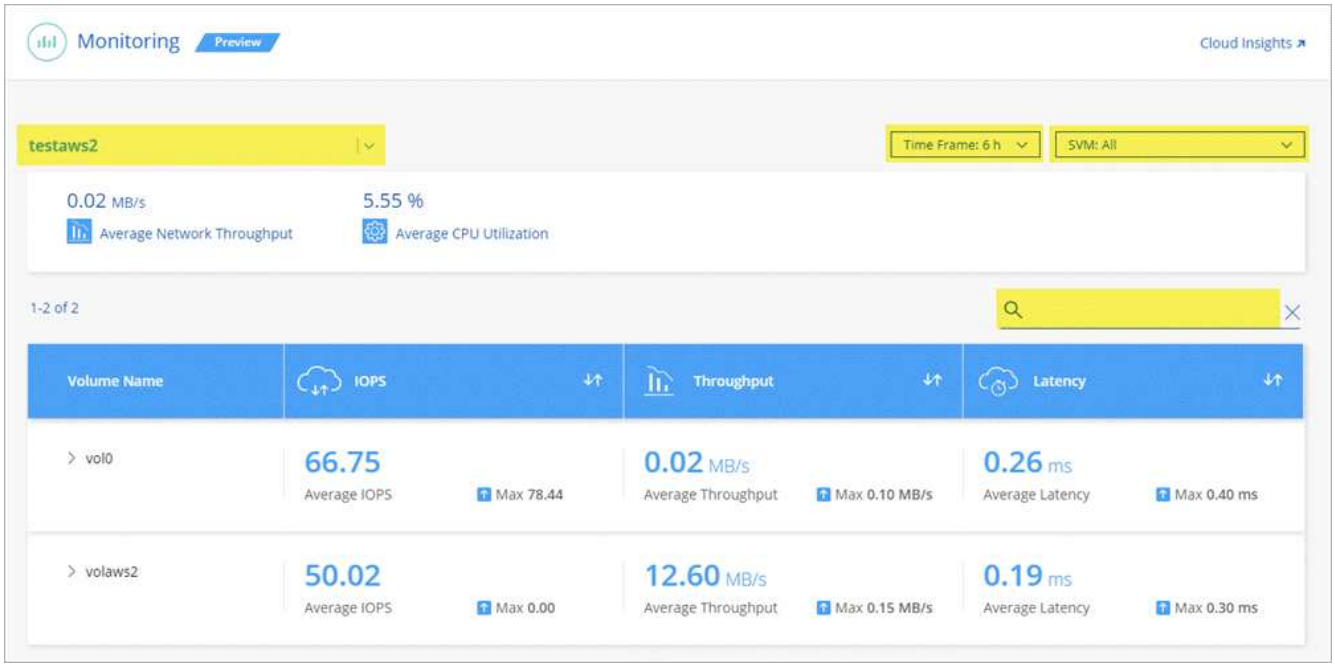
Monitoraggio dei volumi

Monitorate le performance visualizzando IOPS, throughput e latenza per ciascuno dei vostri volumi.

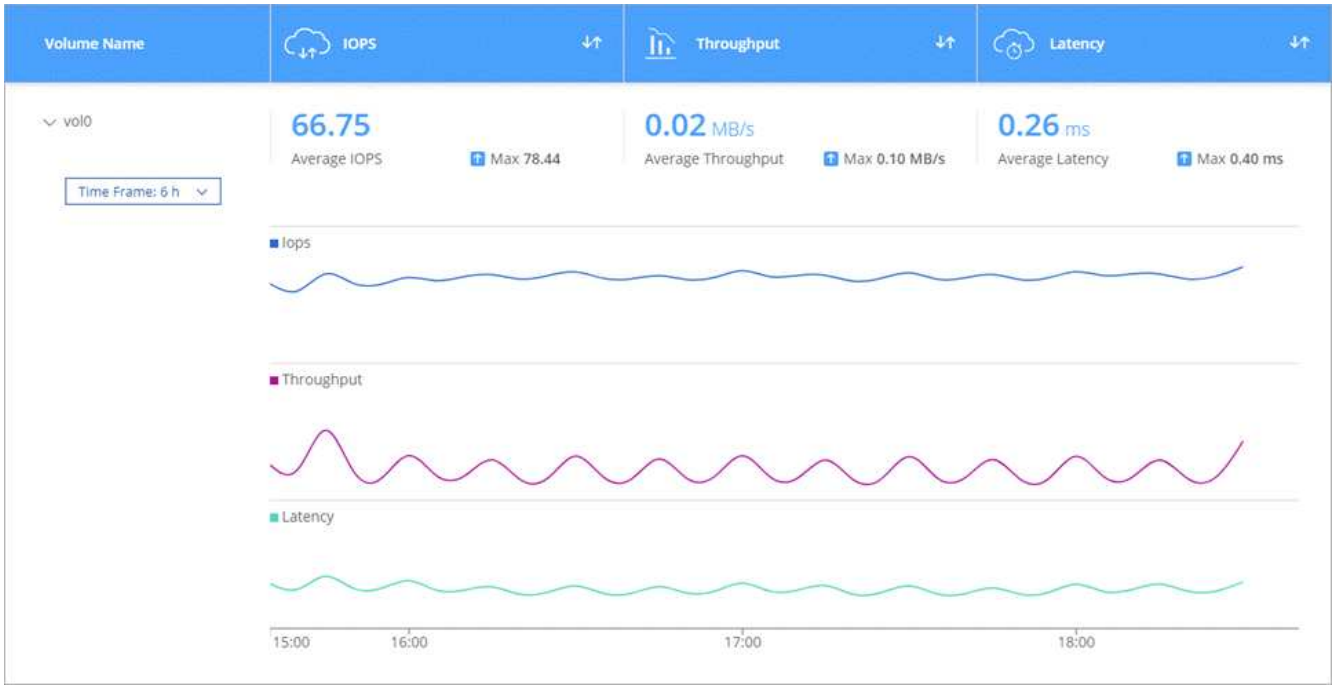
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Monitoring** (monitoraggio).
2. Filtrare il contenuto della dashboard per ottenere le informazioni necessarie.
    - Selezionare un ambiente di lavoro specifico.
    - Selezionare un intervallo di tempo diverso.
    - Selezionare una SVM specifica.
    - Cercare un volume specifico.

      La seguente immagine evidenzia ciascuna di queste opzioni:



3. Fare clic su un volume nella tabella per espandere la riga e visualizzare una timeline per IOPS, throughput e latenza.



4. Utilizza i dati per identificare i problemi di performance e ridurre al minimo l'impatto su utenti e applicazioni.

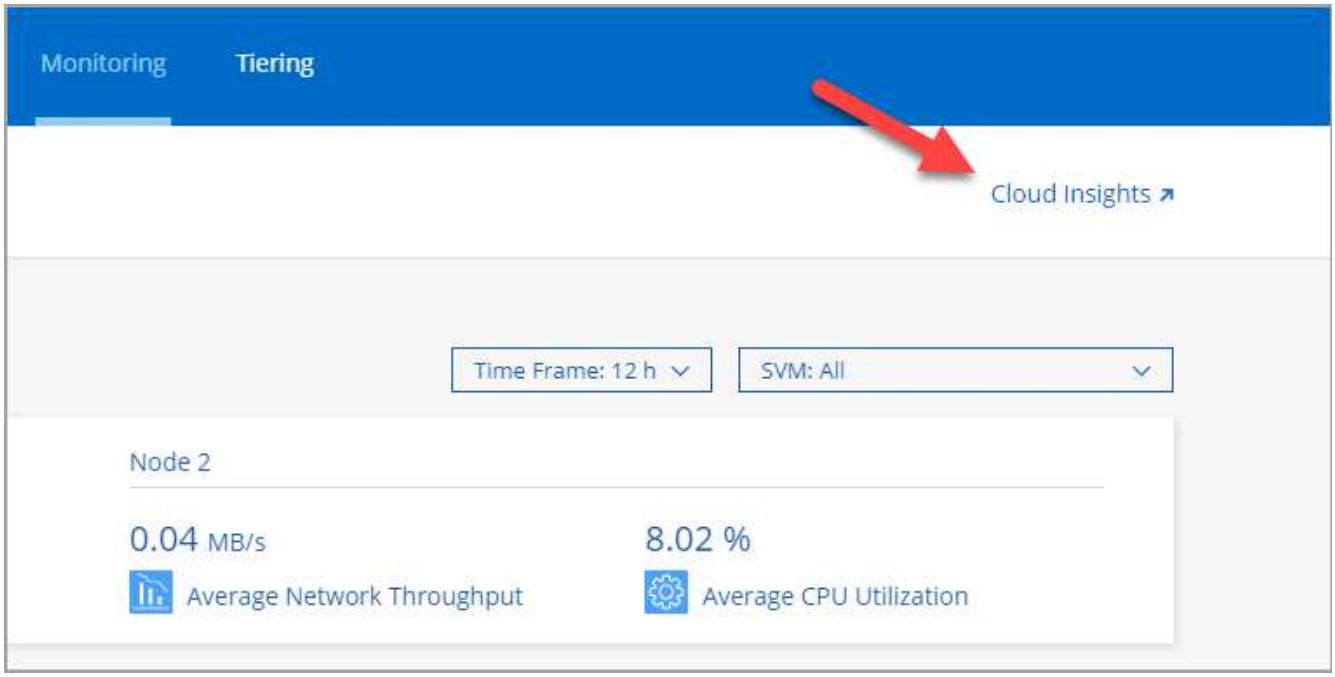
Ottenere ulteriori informazioni da Cloud Insights

La scheda Monitoring (monitoraggio) di Cloud Manager fornisce dati di base sulle performance dei volumi. È possibile accedere all'interfaccia Web di Cloud Insights dal browser per eseguire un monitoraggio più approfondito e configurare gli avvisi per i sistemi Cloud Volumes ONTAP.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Monitoring** (monitoraggio).

2. Fare clic sul collegamento **Cloud Insights**.



Risultato

Cloud Insights si apre in una nuova scheda del browser. Per ulteriori informazioni, consultare la sezione "Documentazione Cloud Insights".

Disattivazione del monitoraggio

Se non si desidera più monitorare Cloud Volumes ONTAP, è possibile disattivare il servizio in qualsiasi momento.

Se si disattiva il monitoraggio da ciascuno degli ambienti di lavoro, sarà necessario eliminare l'istanza EC2 da soli. L'istanza è denominata *AcquisitionUnit* con un hash generato (UUID) concatenato ad essa. Ad esempio: *AcquisitionUnit-FAN7FqeH*

Fasi

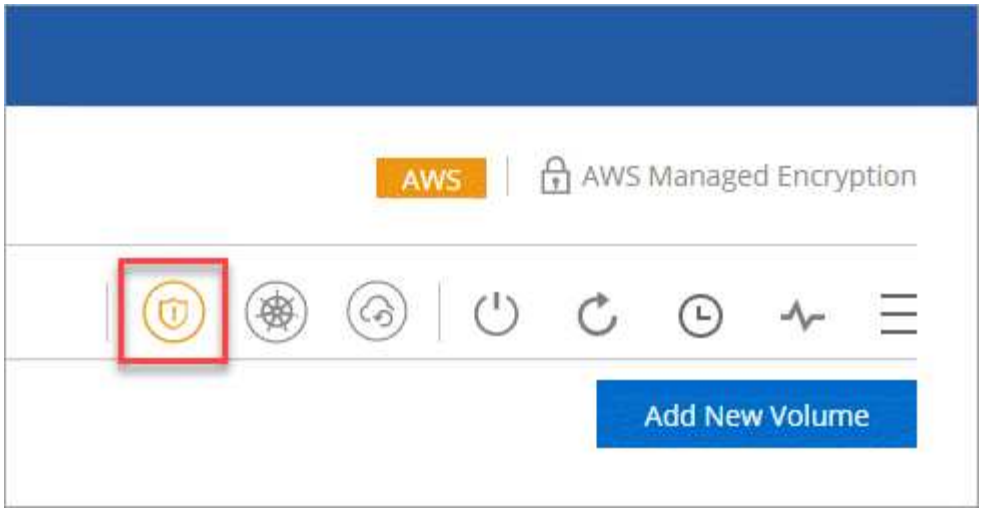
1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare un ambiente di lavoro.
3. Nel riquadro a destra, fare clic su E selezionare **Disattiva scansione**.

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**.

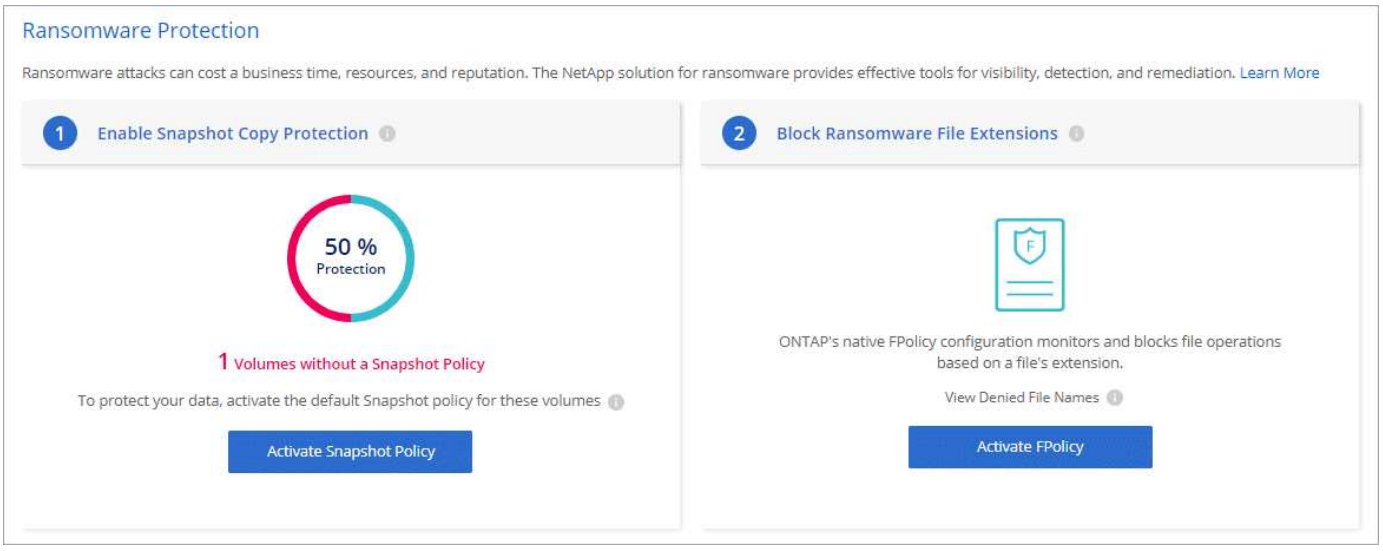


2. Implementare la soluzione NetApp per ransomware:
   a. Fare clic su **Activate Snapshot Policy** (attiva policy Snapshot) se si dispone di volumi che non hanno una policy Snapshot attivata.

      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.



Amministrare

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**:

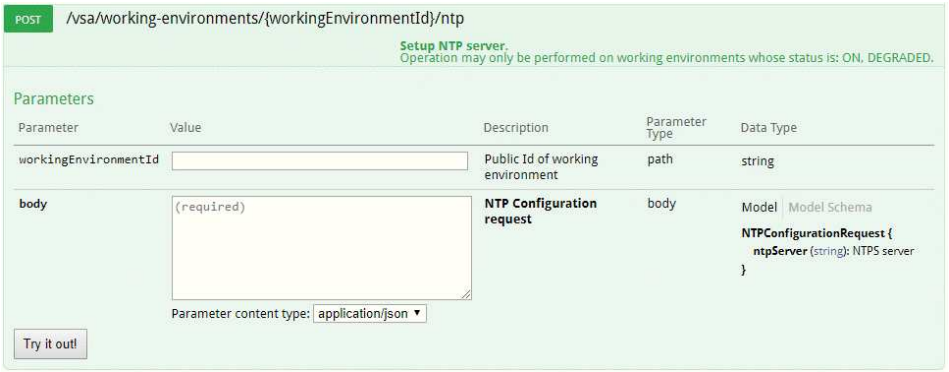
4. Selezionare un account NetApp Support Site e fare clic su **Register**.

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: 
Facoltativo: Configurare AutoSupport	AutoSupport monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp per impostazione predefinita. Se l'amministratore dell'account ha aggiunto un server proxy a Cloud Manager prima di avviare l'istanza, Cloud Volumes ONTAP viene configurato per utilizzare tale server proxy per i messaggi AutoSupport. Verificare che AutoSupport sia in grado di inviare messaggi. Per istruzioni, consultare la Guida in linea di System Manager o il "Guida di riferimento per l'amministrazione del sistema ONTAP 9".
Facoltativo: Configurare Cloud Manager come proxy AutoSupport	Se il tuo ambiente richiede un server proxy per inviare messaggi AutoSupport, puoi configurare Cloud Manager per agire come proxy. Non è richiesta alcuna configurazione per Cloud Manager, ad eccezione dell'accesso a Internet. È sufficiente accedere alla CLI per Cloud Volumes ONTAP ed eseguire il seguente comando: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
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".

Attività	Descrizione
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 sull'host del connettore 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".

Gestione delle licenze BYOL per Cloud Volumes ONTAP

Aggiungere una licenza di sistema Cloud Volumes ONTAP BYOL per aggiungere capacità aggiuntiva, aggiornare una licenza di sistema esistente e gestire le licenze BYOL per il backup nel cloud.

Gestione delle licenze di sistema

È possibile acquistare più licenze per un sistema Cloud Volumes ONTAP BYOL per allocare più di 368 TB di capacità. Ad esempio, è possibile acquistare due licenze per allocare fino a 736 TB di capacità a Cloud Volumes ONTAP. Oppure puoi acquistare quattro licenze per ottenere fino a 1.4 PB.

Il numero di licenze che è possibile acquistare per un sistema a nodo singolo o una coppia ha è illimitato.

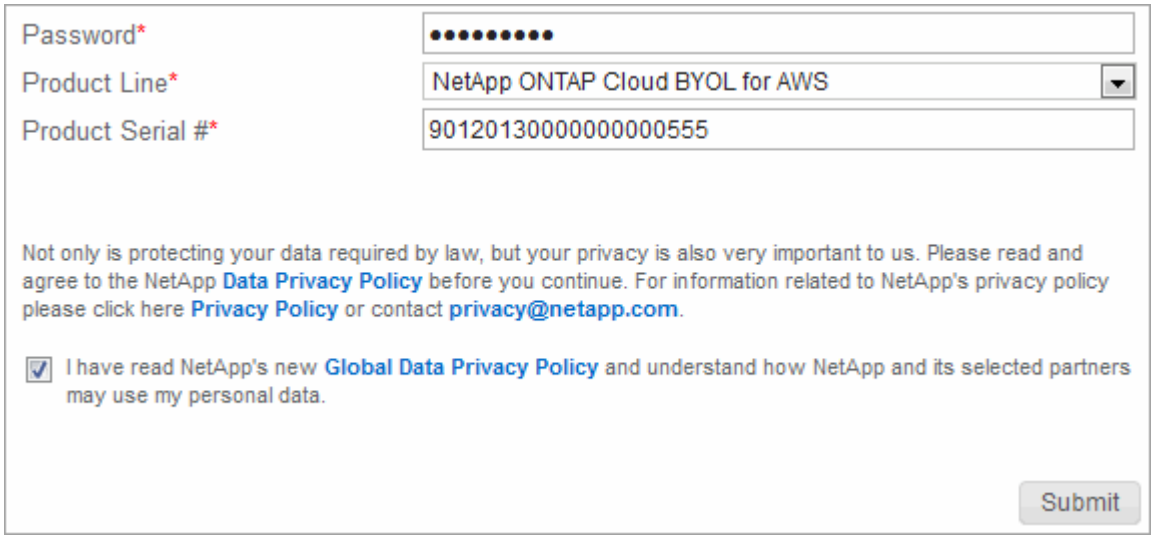
Ottenere un file di licenza di sistema

Nella maggior parte dei casi, Cloud Manager può ottenere automaticamente il file di licenza utilizzando l'account NetApp Support Site. In caso contrario, sarà necessario caricare manualmente il file di licenza. Se non si dispone del file di licenza, è possibile ottenerlo da netapp.com.

Fasi

1. Accedere alla "NetApp License file Generator" Ed effettua l'accesso utilizzando le credenziali del sito di supporto NetApp.
2. Inserire la password, scegliere il prodotto, inserire il numero di serie, confermare di aver letto e accettato l'informativa sulla privacy, quindi fare clic su **Invia**.

   Esempio



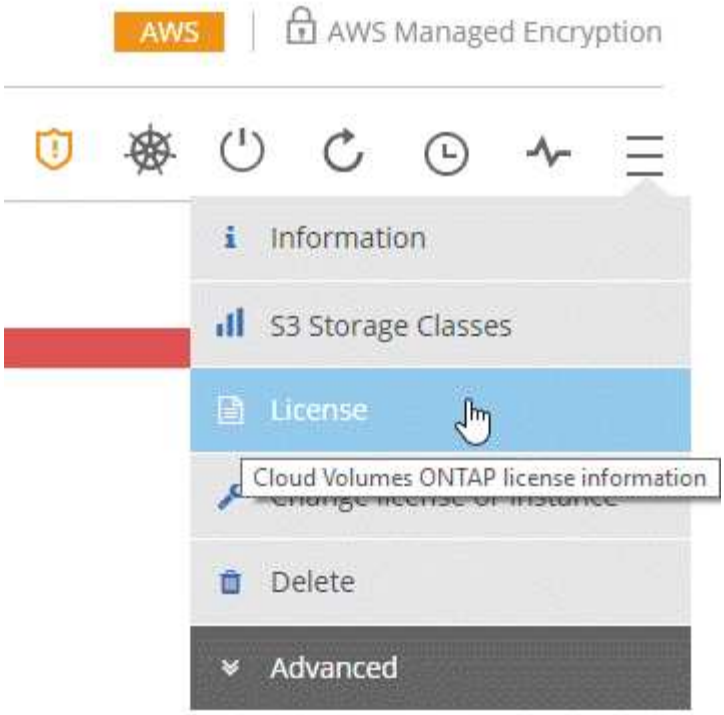
3. Scegliere se si desidera ricevere il file serialnumber.NLF JSON tramite e-mail o download diretto.

Aggiunta di una nuova licenza di sistema

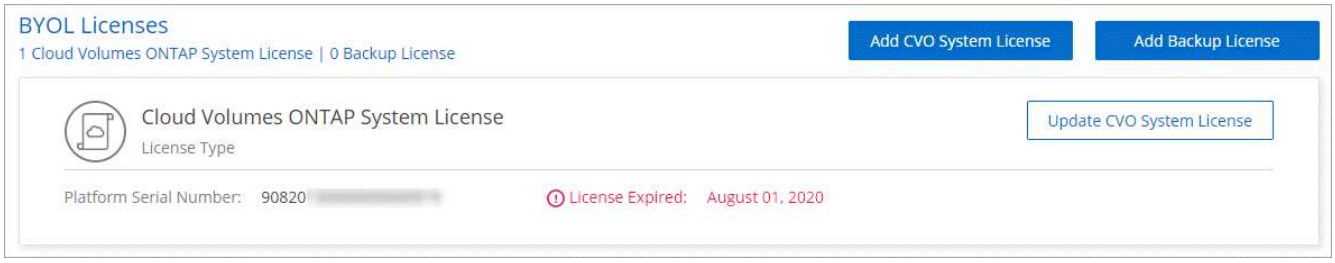
Aggiungi una nuova licenza di sistema BYOL in qualsiasi momento per allocare altri 368 TB di capacità al tuo sistema BYOL Cloud Volumes ONTAP.

Fasi

1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.



3. Fare clic su **Add CVO System License** (Aggiungi licenza di sistema CVO).



4. Scegliere di inserire il numero di serie o di caricare il file di licenza.
5. Fare clic su **Aggiungi licenza**.

Risultato

Cloud Manager installa il nuovo file di licenza sul sistema Cloud Volumes ONTAP.

Aggiornamento di una licenza di sistema

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.

Fasi

1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.
3. Fare clic su **Update CVO System License** (Aggiorna licenza di sistema CVO).

4. Fare clic su **Upload file** (carica file) e selezionare il file di licenza.
5. Fare clic su **Update License** (Aggiorna licenza).

Risultato

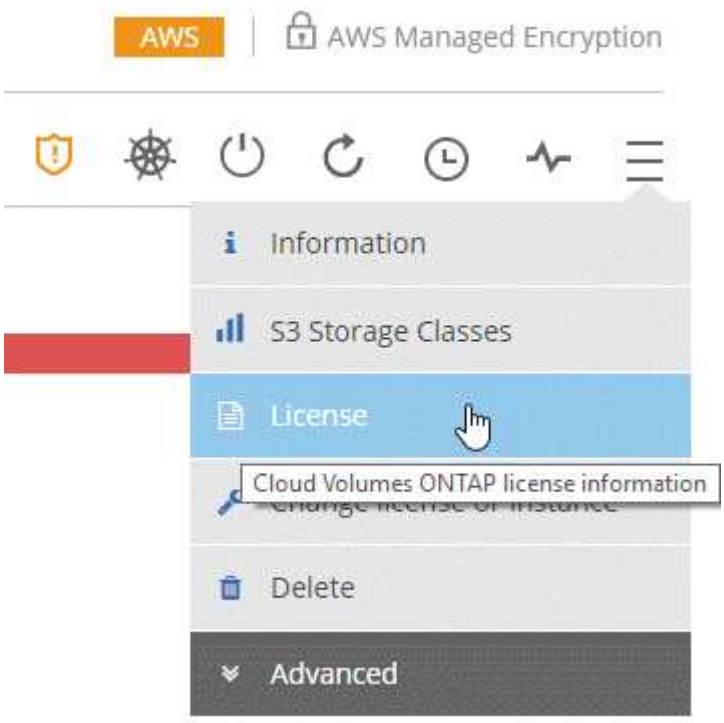
Cloud Manager aggiorna la licenza sul sistema Cloud Volumes ONTAP.

Aggiunta e aggiornamento della licenza BYOL di backup

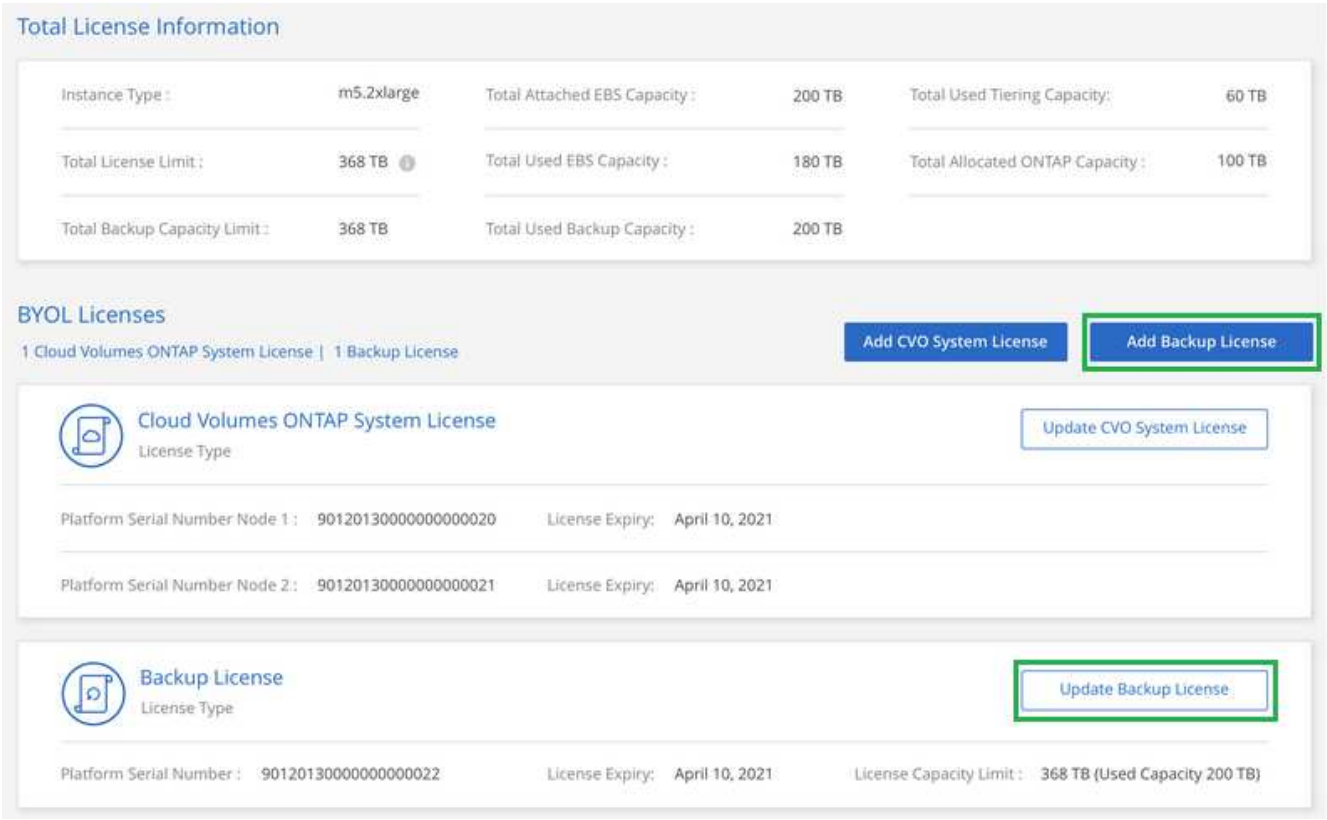
Utilizzare la pagina BYOL Licenses (licenze BYOL) per aggiungere o aggiornare la licenza BYOL di backup.

Fasi

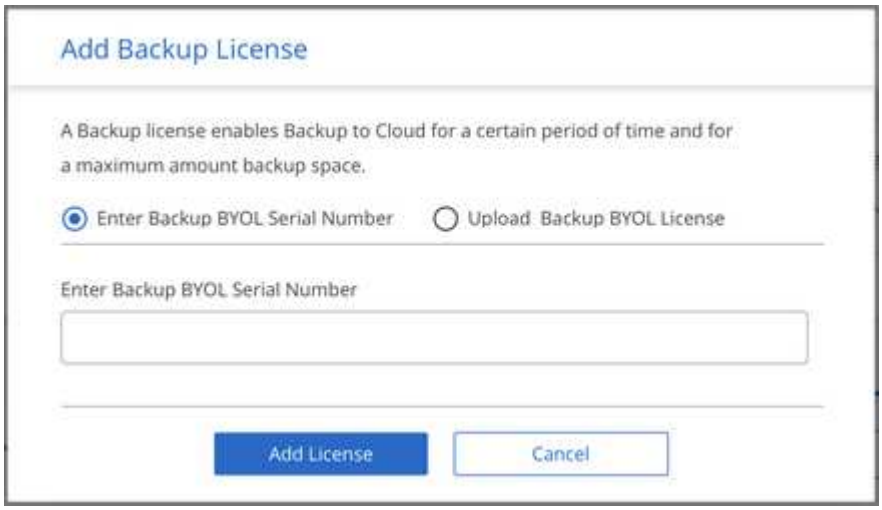
1. In Cloud Manager, aprire l'ambiente di lavoro BYOL di Cloud Volumes ONTAP.
2. Fare clic sull'icona del menu, quindi su **licenza**.



3. Fare clic su **Add Backup License** (Aggiungi licenza di backup) o **Update Backup License** (Aggiorna licenza di backup) a seconda che si stia aggiungendo una nuova licenza o aggiornando una licenza esistente.



4. Inserire le informazioni sulla licenza e fare clic su **Add License** (Aggiungi licenza):
   - Se si dispone del numero di serie, selezionare l'opzione **inserire il numero di serie BYOL di backup** e immettere il numero di serie.
   - Se si dispone del file di licenza di backup, selezionare l'opzione **Upload Backup BYOL License** (carica licenza BYOL di backup) e seguire le istruzioni visualizzate per allegare il file.



Risultato

Cloud Manager aggiunge o aggiorna la licenza in modo che il servizio Backup to Cloud sia attivo.

Aggiornamento del software Cloud Volumes ONTAP

Cloud Manager include diverse opzioni che è possibile utilizzare per eseguire

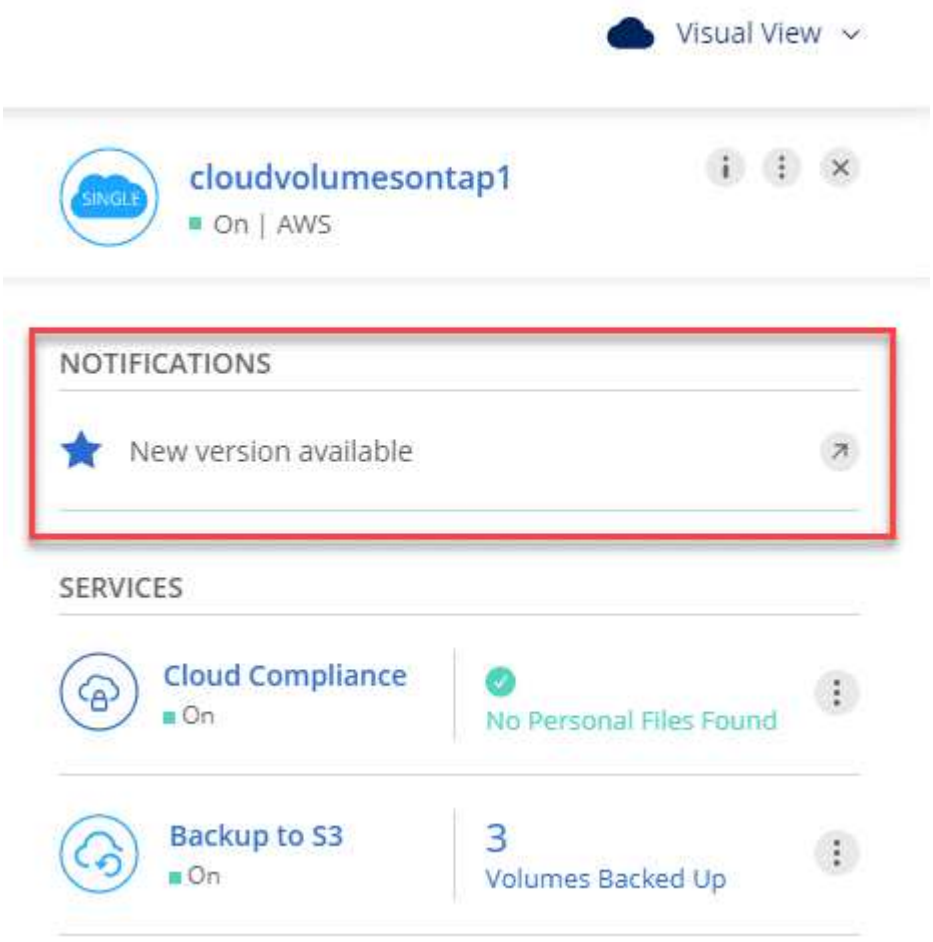
l'aggiornamento alla release corrente di Cloud Volumes ONTAP o per eseguire il downgrade di Cloud Volumes ONTAP a una release precedente. È necessario preparare i sistemi Cloud Volumes ONTAP prima di aggiornare o eseguire il downgrade del software.

Gli aggiornamenti software devono essere completati da Cloud Manager

Gli aggiornamenti di Cloud Volumes ONTAP devono essere completati da Cloud Manager. Non aggiornare Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI. In questo modo si può influire sulla stabilità del sistema.

Metodi per aggiornare Cloud Volumes ONTAP

Cloud Manager visualizza una notifica negli ambienti di lavoro Cloud Volumes ONTAP quando è disponibile una nuova versione di Cloud Volumes ONTAP:



È possibile avviare il processo di aggiornamento da questa notifica, che automatizza il processo ottenendo l'immagine software da un bucket S3, installando l'immagine e riavviando il sistema. Per ulteriori informazioni, vedere Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager.

Per i sistemi ha in AWS, Cloud Manager potrebbe aggiornare il mediatore ha come parte del processo di aggiornamento.

Opzioni avanzate per gli aggiornamenti software

Cloud Manager offre inoltre le seguenti opzioni avanzate per l'aggiornamento del software Cloud Volumes ONTAP:

- Aggiornamenti software utilizzando un'immagine su un URL esterno

  Questa opzione è utile se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software, se è stata fornita una patch o se si desidera eseguire il downgrade del software a una versione specifica.

  Per ulteriori informazioni, vedere Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP.

- Aggiornamenti software utilizzando l'immagine alternativa sul sistema

  È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente, rendendo l'immagine software alternativa l'immagine predefinita. Questa opzione non è disponibile per le coppie ha.

  Per ulteriori informazioni, vedere Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale.

Preparazione all'aggiornamento del software Cloud Volumes ONTAP

Prima di eseguire un upgrade o un downgrade, è necessario verificare che i sistemi siano pronti ed eseguire le modifiche di configurazione richieste.

- Pianificazione del downtime
- Revisione dei requisiti di versione
- Verificare che il giveback automatico sia ancora attivato
- Sospensione dei trasferimenti SnapMirror
- Verificare che gli aggregati siano online

Pianificazione del downtime

Quando si aggiorna un sistema a nodo singolo, il processo di aggiornamento porta il sistema offline per un massimo di 25 minuti, durante i quali l'i/o viene interrotto.

L'aggiornamento di una coppia ha è senza interruzioni e l'i/o è ininterrotto. Durante questo processo di aggiornamento senza interruzioni, ogni nodo viene aggiornato in tandem per continuare a fornire i/o ai client.

Revisione dei requisiti di versione

La versione di ONTAP che è possibile aggiornare o eseguire il downgrade varia in base alla versione di ONTAP attualmente in esecuzione nel sistema.

Per informazioni sui requisiti di versione, fare riferimento a. "Documentazione di ONTAP 9: Requisiti per l'aggiornamento del cluster".

Verificare che il giveback automatico sia ancora attivato

Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

"Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

Sospensione dei trasferimenti SnapMirror

Se un sistema Cloud Volumes ONTAP dispone di relazioni SnapMirror attive, si consiglia di sospendere i trasferimenti prima di aggiornare il software Cloud Volumes ONTAP. La sospensione dei trasferimenti impedisce gli errori di SnapMirror. È necessario sospendere i trasferimenti dal sistema di destinazione.

A proposito di questa attività

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

Fasi

1. "Accedere a System Manager" dal sistema di destinazione.
2. Fare clic su **protezione > Relazioni**.
3. Selezionare la relazione e fare clic su **operazioni > Quiesce**.

Verificare che gli aggregati siano online

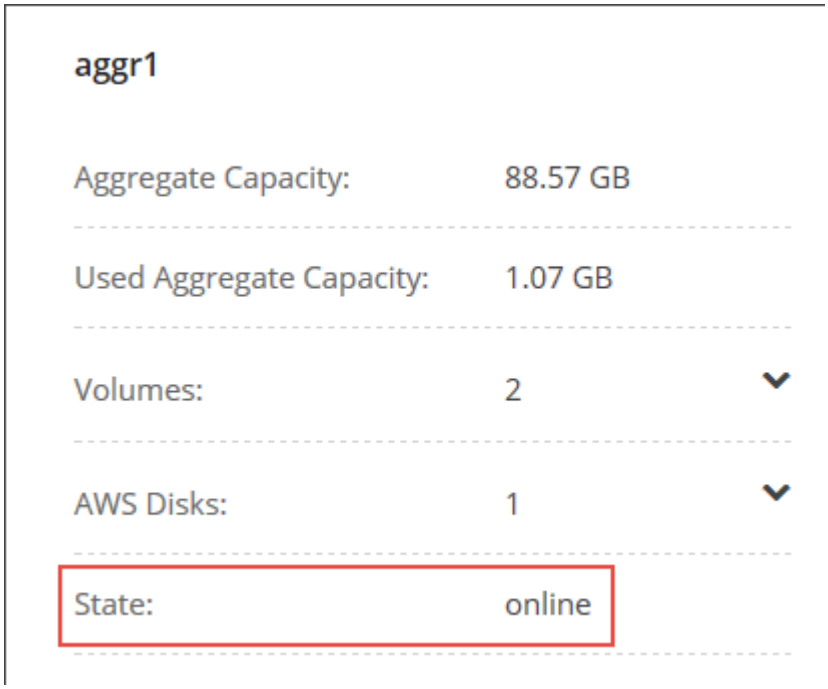
Gli aggregati per Cloud Volumes ONTAP devono essere online prima di aggiornare il software. Gli aggregati devono essere online nella maggior parte delle configurazioni, ma in caso contrario, è necessario portarli online.

A proposito di questa attività

Questa procedura descrive come utilizzare System Manager per la versione 9.3 e successive.

Fasi

1. Nell'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > allocazione avanzata**.
2. Selezionare un aggregato, fare clic su **Info**, quindi verificare che lo stato sia online.



3. Se l'aggregato non è in linea, utilizzare System Manager per portare l'aggregato online:
   a. "Accedere a System Manager".
   b. Fare clic su **Storage > Aggregates & Disks > Aggregates**.

c. Selezionare l'aggregato, quindi fare clic su **altre azioni > Stato > Online**.

Aggiornamento di Cloud Volumes ONTAP dalle notifiche di Cloud Manager

Cloud Manager ti avvisa quando è disponibile una nuova versione di Cloud Volumes ONTAP. Fare clic sulla notifica per avviare il processo di aggiornamento.

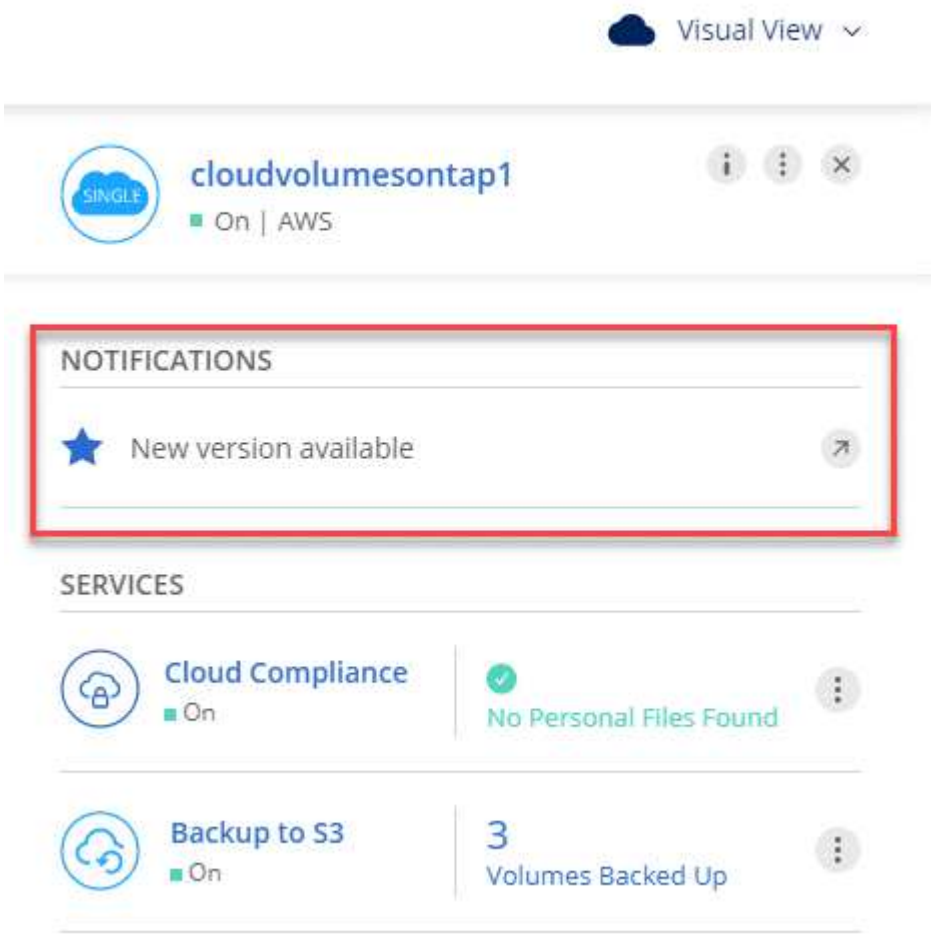
Prima di iniziare

Le operazioni di Cloud Manager, come la creazione di volumi o aggregati, non devono essere in corso per il sistema Cloud Volumes ONTAP.

Fasi

1. Fare clic su **ambienti di lavoro**.
2. Selezionare un ambiente di lavoro.

   Se è disponibile una nuova versione, nel riquadro di destra viene visualizzata una notifica:



3. Se è disponibile una nuova versione, fare clic su **Upgrade** (Aggiorna).
4. Nella pagina Release Information (informazioni sulla release), fare clic sul collegamento per leggere le Note sulla release per la versione specificata, quindi selezionare la casella di controllo **ho letto…**.
5. Nella pagina del Contratto di licenza con l'utente finale (EULA), leggere il Contratto e selezionare **i Read and Approve the EULA** (Leggi e approva il Contratto di licenza con l'utente finale).

6. Nella pagina Review and Approve (esamina e approva), leggere le note importanti, selezionare **i cape…**, quindi fare clic su **Go**.

Risultato

Cloud Manager avvia l'aggiornamento del software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Aggiornamento o downgrade di Cloud Volumes ONTAP utilizzando un server HTTP o FTP

È possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP e avviare l'aggiornamento software da Cloud Manager. È possibile utilizzare questa opzione se Cloud Manager non riesce ad accedere al bucket S3 per aggiornare il software o se si desidera eseguire il downgrade del software.

Fasi

1. Configurare un server HTTP o FTP in grado di ospitare l'immagine del software Cloud Volumes ONTAP.
2. Se si dispone di una connessione VPN alla rete virtuale, è possibile posizionare l'immagine del software Cloud Volumes ONTAP su un server HTTP o FTP nella propria rete. In caso contrario, è necessario posizionare il file su un server HTTP o FTP nel cloud.
3. Se si utilizza il proprio gruppo di protezione per Cloud Volumes ONTAP, assicurarsi che le regole in uscita consentano connessioni HTTP o FTP in modo che Cloud Volumes ONTAP possa accedere all'immagine software.

   Per impostazione predefinita, il gruppo di protezione Cloud Volumes ONTAP predefinito consente le connessioni HTTP e FTP in uscita.

4. Ottenere l'immagine software da "Il sito di supporto NetApp".
5. Copiare l'immagine del software nella directory del server HTTP o FTP da cui verrà servito il file.
6. Dall'ambiente di lavoro in Cloud Manager, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
7. Nella pagina di aggiornamento del software, scegliere **selezionare un'immagine disponibile da un URL**, immettere l'URL, quindi fare clic su **Cambia immagine**.
8. Fare clic su **Procedi** per confermare.

Risultato

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Downgrade di Cloud Volumes ONTAP utilizzando un'immagine locale

La transizione di Cloud Volumes ONTAP a una release precedente nella stessa famiglia di release (ad esempio, da 9.5 a 9.4) viene definita downgrade. È possibile eseguire il downgrade senza assistenza durante il downgrade di cluster nuovi o di test, ma è necessario contattare il supporto tecnico se si desidera eseguire il downgrade di un cluster di produzione.

Ogni sistema Cloud Volumes ONTAP può contenere due immagini software: L'immagine corrente in esecuzione e un'immagine alternativa che è possibile avviare. Cloud Manager può modificare l'immagine alternativa in modo che sia l'immagine predefinita. È possibile utilizzare questa opzione per eseguire il downgrade alla versione precedente di Cloud Volumes ONTAP, in caso di problemi con l'immagine corrente.

A proposito di questa attività

Questo processo di downgrade è disponibile solo per sistemi Cloud Volumes ONTAP singoli. Non è disponibile per le coppie ha.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Avanzate > Aggiorna Cloud Volumes ONTAP**.
2. Nella pagina di aggiornamento del software, selezionare l'immagine alternativa, quindi fare clic su **Cambia immagine**.
3. Fare clic su **Procedi** per confermare.

Risultato

Cloud Manager avvia l'aggiornamento software. Una volta completato l'aggiornamento del software, è possibile eseguire azioni sull'ambiente di lavoro.

Al termine

Se sono state sospese le trasferte SnapMirror, utilizzare System Manager per riprendere le trasferte.

Modifica dei sistemi Cloud Volumes ONTAP

Potrebbe essere necessario modificare la configurazione dei sistemi 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 molto altro ancora.

Modifica dell'istanza o del tipo di macchina per Cloud Volumes ONTAP

Quando si avvia Cloud Volumes ONTAP in AWS, Azure o GCP, è possibile scegliere tra diversi tipi di istanze o computer. È possibile modificare l'istanza o il tipo di macchina in qualsiasi momento se si determina che è sottodimensionato o sovradimensionato per le proprie esigenze.

A proposito di questa attività

- Il giveback automatico deve essere attivato su una coppia Cloud Volumes ONTAP ha (impostazione predefinita). In caso contrario, l'operazione avrà esito negativo.

  "Documentazione di ONTAP 9: Comandi per la configurazione del giveback automatico"

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.
- 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.

Cloud Manager modifica correttamente un nodo alla volta avviando il Takeover e attendendo il give back. Il team di QA di NetApp ha testato sia la scrittura che la lettura dei file durante questo processo e non ha rilevato alcun problema sul lato client. Con la modifica delle connessioni, abbiamo visto tentativi a livello di i/o, ma il livello applicativo ha superato questi brevi "re-wire" delle connessioni NFS/CIFS.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Se si utilizza una configurazione pay-as-you-go, è possibile scegliere una licenza diversa.
3. Selezionare un'istanza o un tipo di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova configurazione.

Passaggio da una configurazione pay-as-you-go all'altra

Dopo aver lanciato i sistemi Cloud Volumes ONTAP pay-as-you-go, è possibile passare da una configurazione Explore a una configurazione standard e a una configurazione Premium in qualsiasi momento modificando la licenza. La modifica della licenza aumenta o diminuisce il limite di capacità raw e consente di scegliere tra diversi tipi di istanze AWS o tipi di macchine virtuali Azure.

In GCP, è disponibile un singolo tipo di macchina per ogni configurazione pay-as-you-go. Non è possibile scegliere tra diversi tipi di computer.

A proposito di questa attività

Tenere presente quanto segue circa il passaggio da una licenza pay-as-you-go all'altra:

- L'operazione riavvia Cloud Volumes ONTAP.

  Per i sistemi a nodo singolo, l'i/o viene interrotto.

  Per le coppie ha, il cambiamento è senza interruzioni. Le coppie HA continuano a servire i dati.

- La modifica dell'istanza o del tipo di macchina influisce sui costi di servizio del provider di cloud.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Change License or instance** for AWS, **Change License or VM** for Azure o **Change License or machine** for GCP.
2. Selezionare un tipo di licenza e un tipo di istanza o di macchina, selezionare la casella di controllo per confermare di aver compreso le implicazioni della modifica, quindi fare clic su **OK**.

Risultato

Cloud Volumes ONTAP si riavvia con la nuova licenza, il tipo di istanza o il tipo di macchina o entrambi.

Passaggio a una configurazione Cloud Volumes ONTAP alternativa

Se si desidera passare da un abbonamento pay-as-you-go a un abbonamento BYOL o tra un singolo sistema Cloud Volumes ONTAP e una coppia ha, è necessario implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

Fasi

1. Creare un nuovo ambiente di lavoro Cloud Volumes ONTAP.

   "Avvio di Cloud Volumes ONTAP in AWS"
   "Lancio di Cloud Volumes ONTAP in Azure"
   "Avvio di Cloud Volumes ONTAP in GCP"

2. "Configurare la replica dei dati una tantum" tra i sistemi per ciascun volume da replicare.
3. Terminare il sistema Cloud Volumes ONTAP di cui non si ha più bisogno "eliminazione dell'ambiente di lavoro originale".

Modifica della velocità di scrittura su normale o alta

Cloud Manager consente di scegliere un'impostazione della velocità di scrittura per i sistemi Cloud Volumes ONTAP a nodo singolo. La velocità di scrittura predefinita è normale. È possibile passare a un'elevata velocità di scrittura se sono richieste prestazioni di scrittura rapide per il carico di lavoro. Prima di modificare la velocità di scrittura, è necessario "comprendere le differenze tra le impostazioni normali e quelle alte".

A proposito di questa attività

- Assicurarsi che operazioni come la creazione di volumi o aggregati non siano in corso.
- Tenere presente che questa modifica riavvia Cloud Volumes ONTAP, il che significa che l'i/o viene interrotto.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Advanced > Writing Speed** (Avanzate > velocità di scrittura).
2. Selezionare **normale** o **alta**.

   Se scegli High, allora devi leggere il messaggio "capisco…" e confermare selezionando la casella.

3. Fare clic su **Save** (Salva), controllare il messaggio di conferma, quindi fare clic su **Proceed** (Procedi).

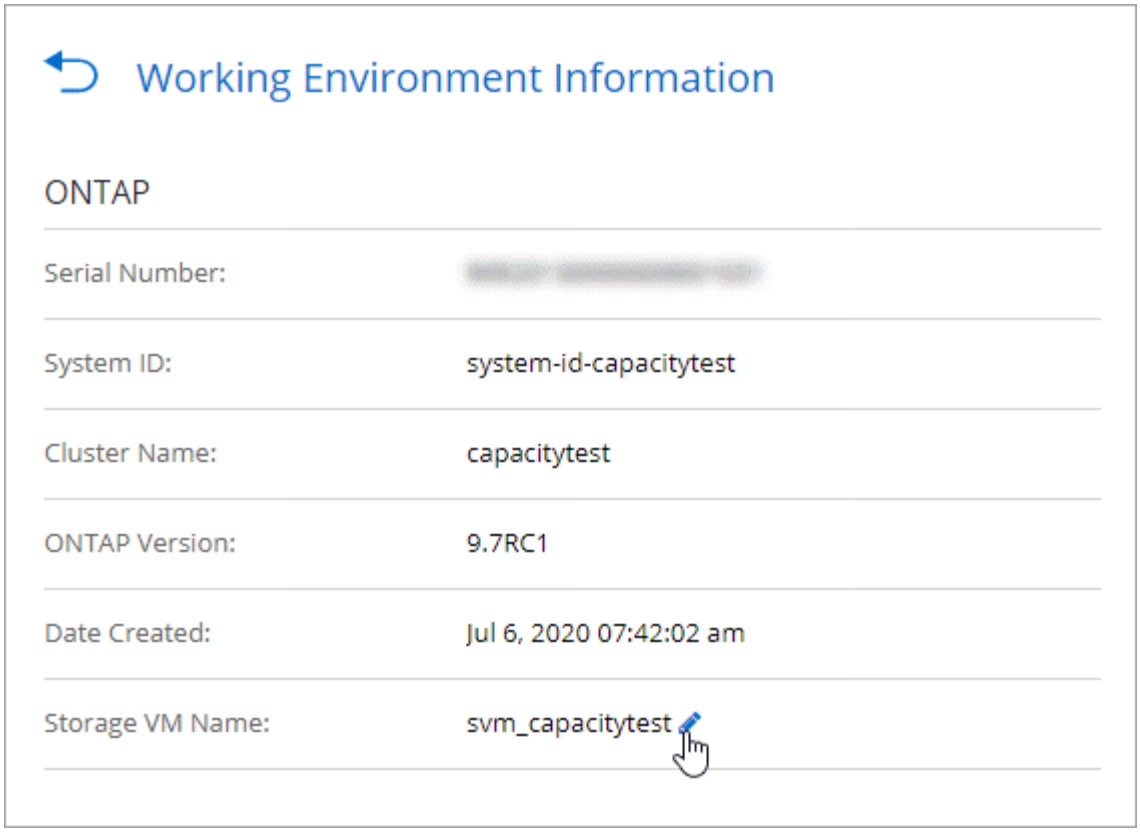
Modifica del nome della VM di storage

Cloud Manager assegna automaticamente un nome alla singola VM di storage creata per Cloud Volumes ONTAP. È possibile modificare il nome della SVM se si dispone di standard di denominazione rigorosi. Ad esempio, è possibile che il nome corrisponda a quello delle SVM per i cluster ONTAP.

Tuttavia, se hai creato altre SVM per Cloud Volumes ONTAP, non puoi rinominare le SVM da Cloud Manager. È necessario eseguire questa operazione direttamente da Cloud Volumes ONTAP utilizzando Gestione di sistema o l'interfaccia CLI.

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 della VM di storage.



3. Nella finestra di dialogo Modify SVM Name (Modifica nome SVM), modificare il nome, 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.

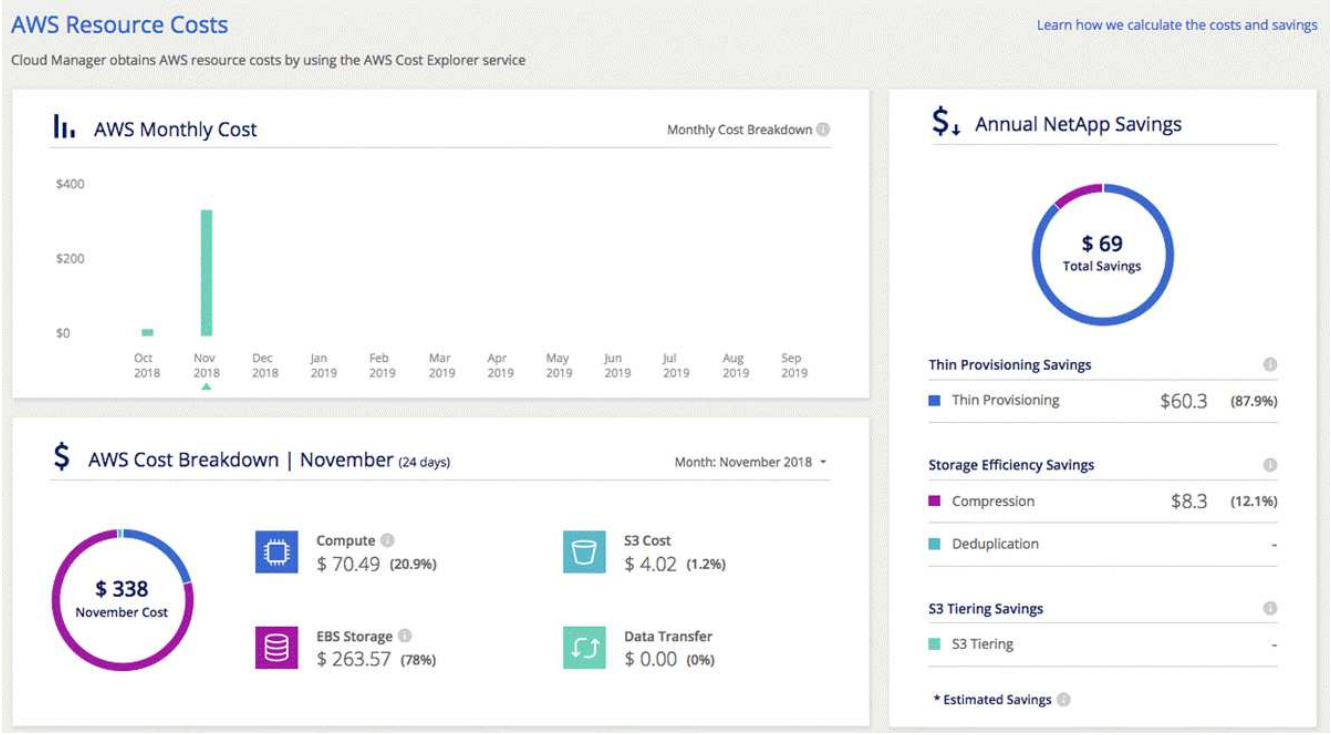
   b. "Attivare il tag **WorkingEnvironmentId**".

      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:



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 System Manager in corso

Potrebbe essere necessario eseguire alcune attività di Cloud Volumes ONTAP da Gestore di sistema, 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.

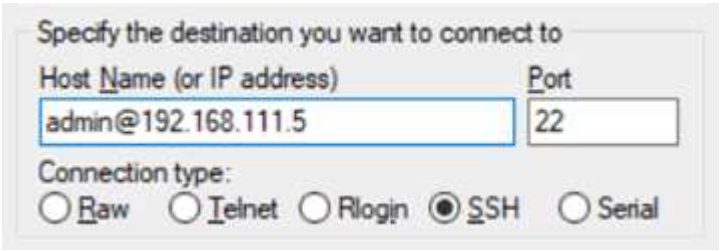
> Quando vengono implementate in più AZS, le configurazioni Cloud Volumes ONTAP ha utilizzano un indirizzo IP mobile per l'interfaccia di gestione del cluster, il che significa che il routing esterno non è disponibile. È necessario connettersi da un host che fa parte dello stesso dominio di routing.

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::>
   ```

Aggiunta di sistemi Cloud Volumes ONTAP esistenti a Cloud Manager

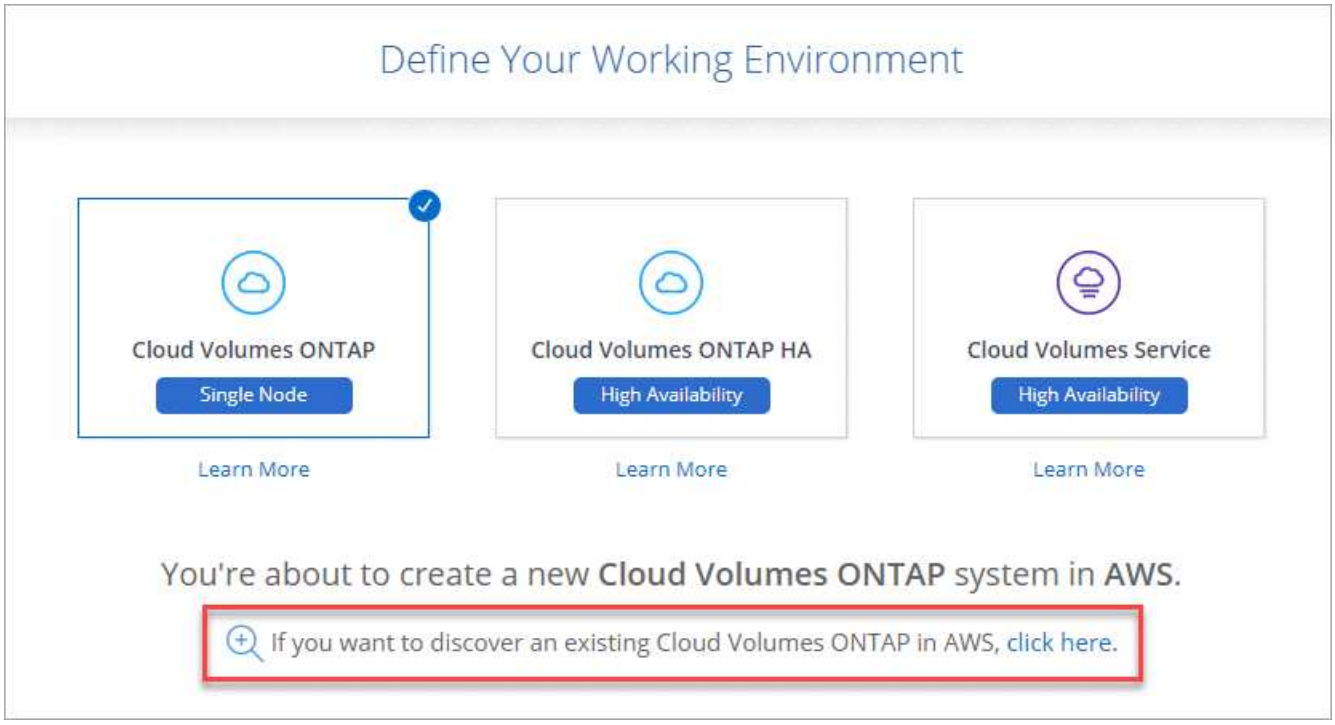
Puoi scoprire e aggiungere sistemi Cloud Volumes ONTAP esistenti a Cloud Manager. Puoi farlo se hai implementato un nuovo sistema Cloud Manager.

Prima di iniziare

È necessario conoscere la password dell'account utente amministratore di Cloud Volumes ONTAP.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. Selezionare il provider cloud in cui risiede il sistema.
3. Scegliere il tipo di sistema Cloud Volumes ONTAP.
4. Fare clic sul collegamento per individuare un sistema esistente.



5. Nella pagina Area, scegliere l'area in cui sono in esecuzione le istanze, quindi selezionare le istanze.
6. Nella pagina credenziali, immettere la password per l'utente amministratore di Cloud Volumes ONTAP, quindi fare clic su **Go**.

Risultato

Cloud Manager aggiunge le istanze di Cloud Volumes ONTAP allo spazio di lavoro.

Eliminazione di un ambiente di lavoro Cloud Volumes ONTAP

Si consiglia di eliminare i sistemi Cloud Volumes ONTAP da Cloud Manager, piuttosto che dalla console del provider di cloud. Ad esempio, se si termina un'istanza di Cloud Volumes ONTAP con licenza da AWS, non è possibile utilizzare la chiave di licenza per un'altra istanza. Per rilasciare la licenza, è necessario eliminare l'ambiente di lavoro da Cloud Manager.

A proposito di questa attività

Quando si elimina un ambiente di lavoro, Cloud Manager termina le istanze, elimina dischi e snapshot.

> Le istanze di Cloud Volumes ONTAP dispongono di una protezione di terminazione abilitata per prevenire la terminazione accidentale da parte di AWS. Tuttavia, se si interrompe un'istanza di Cloud Volumes ONTAP da AWS, è necessario accedere alla console di AWS CloudFormation ed eliminare lo stack dell'istanza. Il nome dello stack è il nome dell'ambiente di lavoro.

Fasi

1. Dall'ambiente di lavoro, fare clic sull'icona del menu, quindi fare clic su **Delete** (Elimina).
2. Digitare il nome dell'ambiente di lavoro, quindi fare clic su **Delete** (Elimina).

   L'eliminazione dell'ambiente di lavoro può richiedere fino a 5 minuti.

Eseguire il provisioning dei volumi utilizzando un file service

Azure NetApp Files

Scopri di più su Azure NetApp Files

Azure NetApp Files consente alle aziende di migrare ed eseguire le proprie applicazioni business-critical ad alta intensità di performance e sensibili alla latenza in Azure senza dover eseguire alcun refactor per il cloud.

Caratteristiche

- Il supporto di più protocolli consente di eseguire senza problemi le applicazioni Linux e Windows in Azure.
- I livelli di performance multipli consentono un allineamento ravvicinato con i requisiti di performance dei carichi di lavoro.
- Le certificazioni leader, tra cui SAP HANA, GDPR e HIPPA, consentono la migrazione dei carichi di lavoro più esigenti in Azure.

Funzionalità aggiuntive in Cloud Manager

- Migrare i dati NFS o SMB su Azure NetApp Files direttamente da Cloud Manager. Le migrazioni dei dati sono basate sul servizio Cloud Sync di NetApp. "Scopri di più".
- Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), la conformità al cloud può aiutarti a comprendere il contesto dei dati e identificare i dati sensibili che risiedono nei tuoi account Azure NetApp Files. "Scopri di più".

Costo

"Visualizza i prezzi Azure NetApp Files".

Tieni presente che l'abbonamento e il costo sono gestiti dal servizio Azure NetApp Files e non da Cloud Manager.

Regioni supportate

"Visualizzare le regioni Azure supportate".

Richiesta di accesso

È necessario concedere l'accesso a Azure NetApp Files da "invio di una richiesta online". Prima di procedere, devi attendere l'approvazione del team Azure NetApp Files.

Assistenza

Per problemi di supporto tecnico associati a Azure NetApp Files, utilizzare il portale Azure per registrare una richiesta di supporto a Microsoft. Selezionare l'abbonamento Microsoft associato e il nome del servizio **Azure NetApp Files** sotto **Storage**. Fornire le informazioni rimanenti necessarie per creare la richiesta di supporto Microsoft.

Per i problemi relativi a Cloud Sync e Azure NetApp Files, puoi iniziare con NetApp utilizzando il tuo numero di serie Cloud Sync direttamente dal servizio Cloud Sync. È necessario accedere al servizio Cloud Sync tramite il collegamento in Gestione cloud. "Visualizza la procedura per abilitare il supporto Cloud Sync".

Link correlati

- "Cloud Central di NetApp: Azure NetApp Files"
- "Documentazione Azure NetApp Files"
- "Documentazione Cloud Sync"

Configurazione di Azure NetApp Files

Creare un ambiente di lavoro Azure NetApp Files in Cloud Manager per creare e gestire account, pool di capacità, volumi e snapshot NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Richiedere l'accesso

"Inviare una richiesta online" Per ottenere l'accesso a Azure NetApp Files.

Configurare un'applicazione Azure ad

Da Azure, concedere le autorizzazioni a un'applicazione Azure ad e copiare l'ID dell'applicazione (client), l'ID della directory (tenant) e il valore di un client secret.

Creare un ambiente di lavoro Azure NetApp Files

In Cloud Manager, fare clic su **Aggiungi ambiente di lavoro** > **Microsoft Azure** > **Azure NetApp Files**, quindi fornire i dettagli sull'applicazione ad.

Richiesta di accesso

È necessario concedere l'accesso a Azure NetApp Files da "invio di una richiesta online". Prima di procedere, devi attendere l'approvazione del team Azure NetApp Files.

Impostazione di un'applicazione Azure ad

Cloud Manager ha bisogno delle autorizzazioni per configurare e gestire Azure NetApp Files. Puoi concedere le autorizzazioni richieste a un account Azure creando e configurando un'applicazione Azure ad e ottenendo le credenziali Azure di cui Cloud Manager ha bisogno.

Creazione dell'applicazione ad

Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per

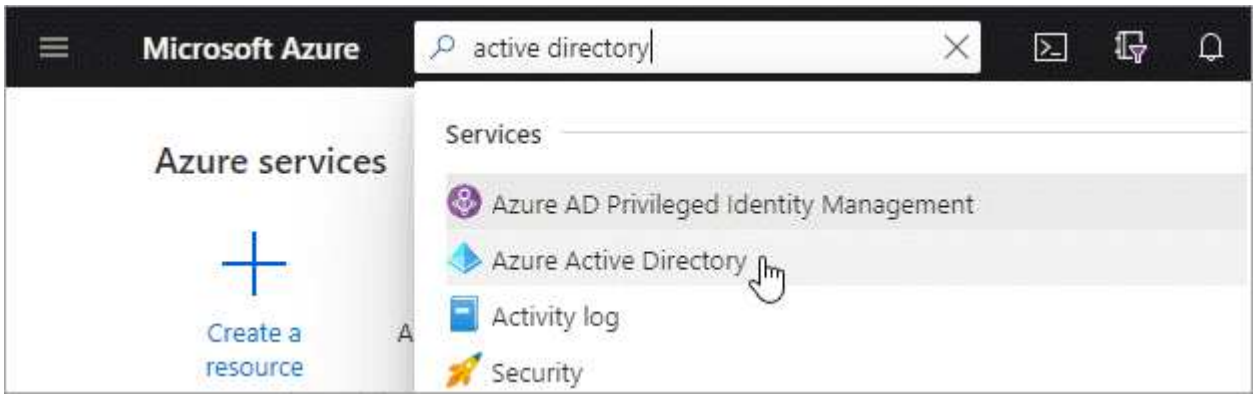
il controllo degli accessi in base al ruolo.

Prima di iniziare

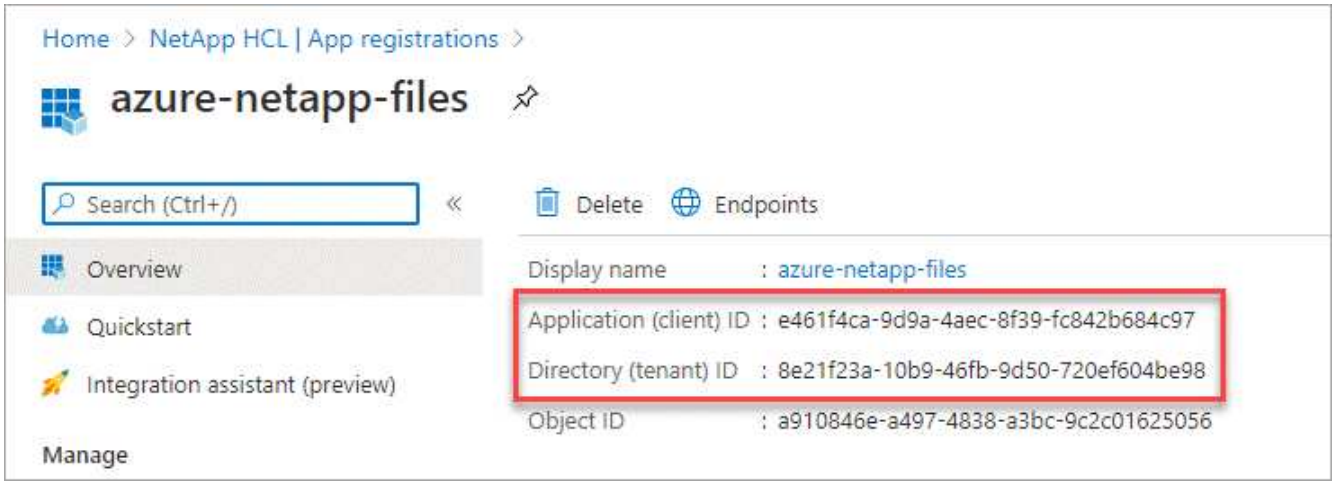
Per creare un'applicazione Active Directory e assegnarla a un ruolo, è necessario disporre delle autorizzazioni appropriate in Azure. Per ulteriori informazioni, fare riferimento a. "Documentazione di Microsoft Azure: Autorizzazioni richieste".

Fasi

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



2. Nel menu, fare clic su **App Registrations**.
3. Creare l'applicazione:
   a. Fare clic su **Nuova registrazione**.
   b. Specificare i dettagli dell'applicazione:
      - **Nome**: Immettere un nome per l'applicazione.
      - **Tipo di account**: Selezionare un tipo di account (qualsiasi verrà utilizzato con Cloud Manager).
      - **Redirect URI**: Lasciare vuoto questo campo.
   c. Fare clic su **Registra**.
4. Copiare **Application (client) ID** e **Directory (tenant) ID**.



Quando si crea l'ambiente di lavoro Azure NetApp Files in Cloud Manager, è necessario fornire l'ID dell'applicazione (client) e l'ID della directory (tenant) per l'applicazione. Cloud Manager utilizza gli ID per effettuare l'accesso a livello di programmazione.

5. Creare un segreto client per l'applicazione in modo che Cloud Manager possa utilizzarlo per l'autenticazione con Azure ad:
   a. Fare clic su **certificati e segreti > nuovo segreto client**.
   b. Fornire una descrizione del segreto e una durata.
   c. Fare clic su **Aggiungi**.
   d. Copiare il valore del client secret.

Risultato

L'applicazione ad è stata configurata e l'ID dell'applicazione (client), l'ID della directory (tenant) e il valore del client secret dovrebbero essere stati copiati. È necessario inserire queste informazioni in Cloud Manager quando si aggiunge un ambiente di lavoro Azure NetApp Files.

Assegnazione dell'applicazione a un ruolo

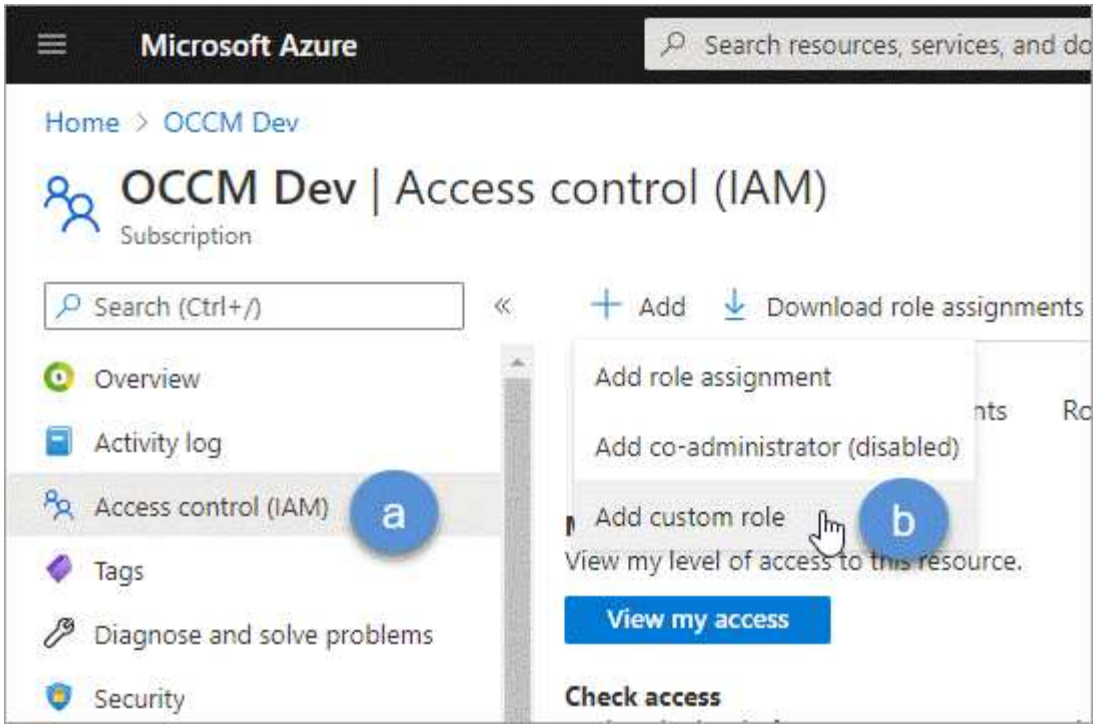
È necessario associare l'entità del servizio all'abbonamento Azure e assegnarle un ruolo personalizzato con le autorizzazioni richieste.

Fasi

1. "Creare un ruolo personalizzato in Azure".

   I passaggi seguenti descrivono come creare il ruolo dal portale Azure.

   a. Aprire l'abbonamento e fare clic su **Access control (IAM)**.
   b. Fare clic su **Aggiungi > Aggiungi ruolo personalizzato**.



c. Nella scheda **Basics**, immettere un nome e una descrizione per il ruolo.

d. Fare clic su **JSON** e fare clic su **Edit** (Modifica) che viene visualizzato in alto a destra del formato JSON.

e. Aggiungere le seguenti autorizzazioni in *azioni*:

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Fare clic su **Salva**, **Avanti**, quindi su **Crea**.

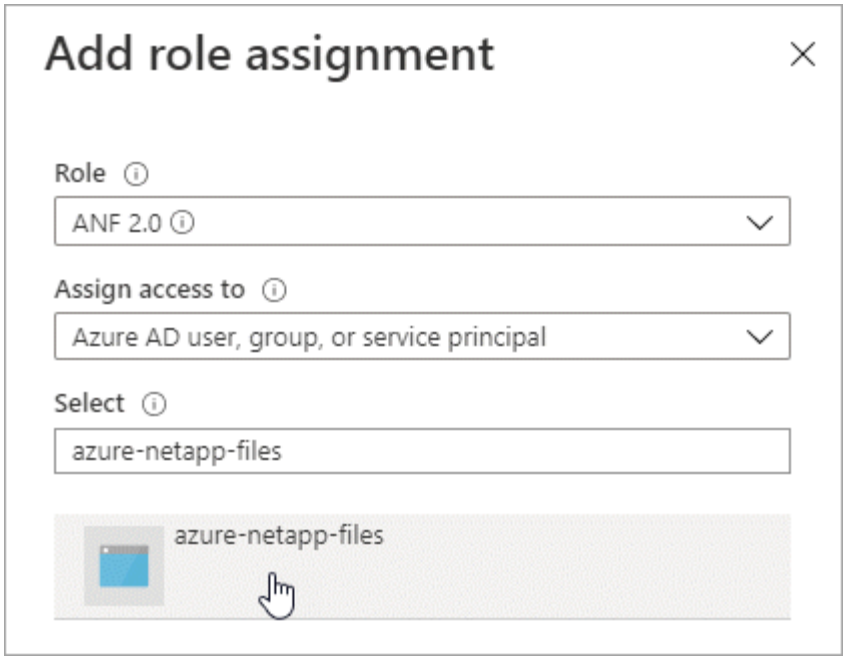
2. Assegnare l'applicazione al ruolo appena creato:

a. Dal portale Azure, aprire l'abbonamento e fare clic su **Access control (IAM) > Add > Add role assignment** (controllo accesso (IAM) > Add > Add role assignment (Aggiungi assegnazione ruolo).

b. Selezionare il ruolo personalizzato creato.

c. Mantieni selezionata l'opzione **Azure ad user, group o service principal**.

d. Cercare il nome dell'applicazione (non è possibile trovarla nell'elenco scorrendo).



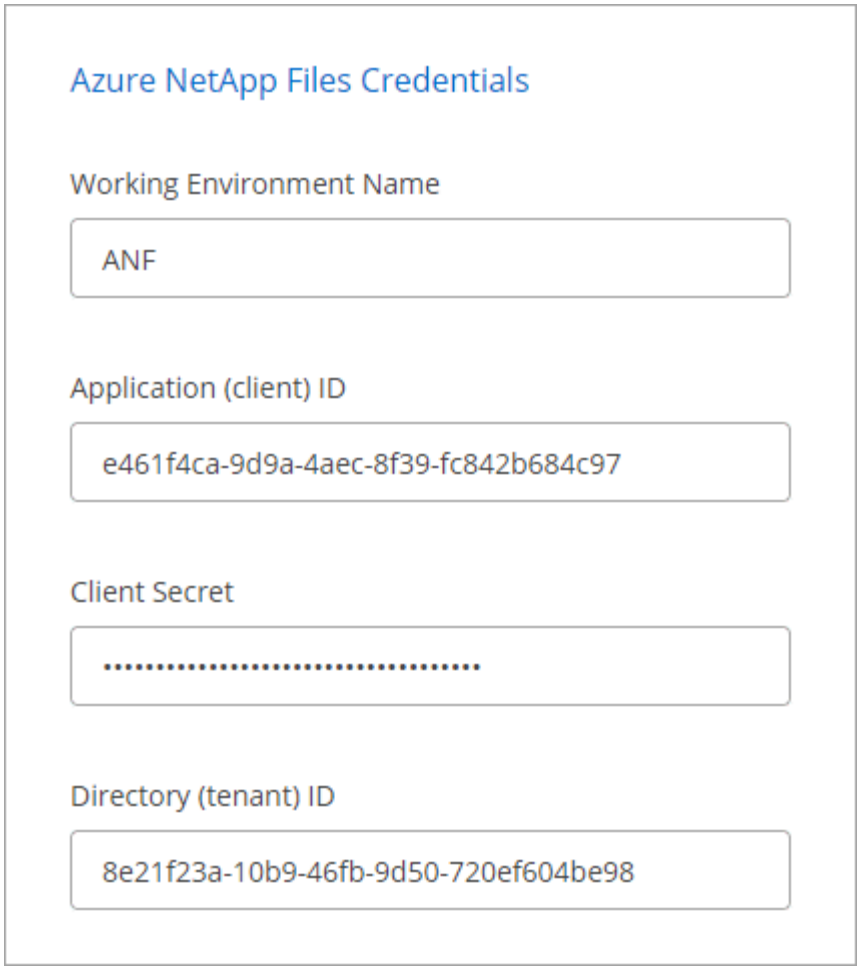
e. Selezionare l'applicazione e fare clic su **Save** (Salva).

   Il service principal per Cloud Manager dispone ora delle autorizzazioni Azure necessarie per tale abbonamento.

Creazione di un ambiente di lavoro Azure NetApp Files

Configura un ambiente di lavoro Azure NetApp Files in Cloud Manager per iniziare a creare volumi.

1. Dalla pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. Selezionare **Microsoft Azure**, quindi **Azure NetApp Files**.
3. Fornire dettagli sull'applicazione ad precedentemente configurata.



4. Fare clic su **Aggiungi**.

Risultato

Ora dovresti disporre di un ambiente di lavoro Azure NetApp Files.

Quali sono le prossime novità?

"Inizia a creare e gestire i volumi".

Creazione e gestione di volumi per Azure NetApp Files

Dopo aver configurato l'ambiente di lavoro, è possibile creare e gestire account Azure NetApp Files, pool di capacità, volumi e snapshot.

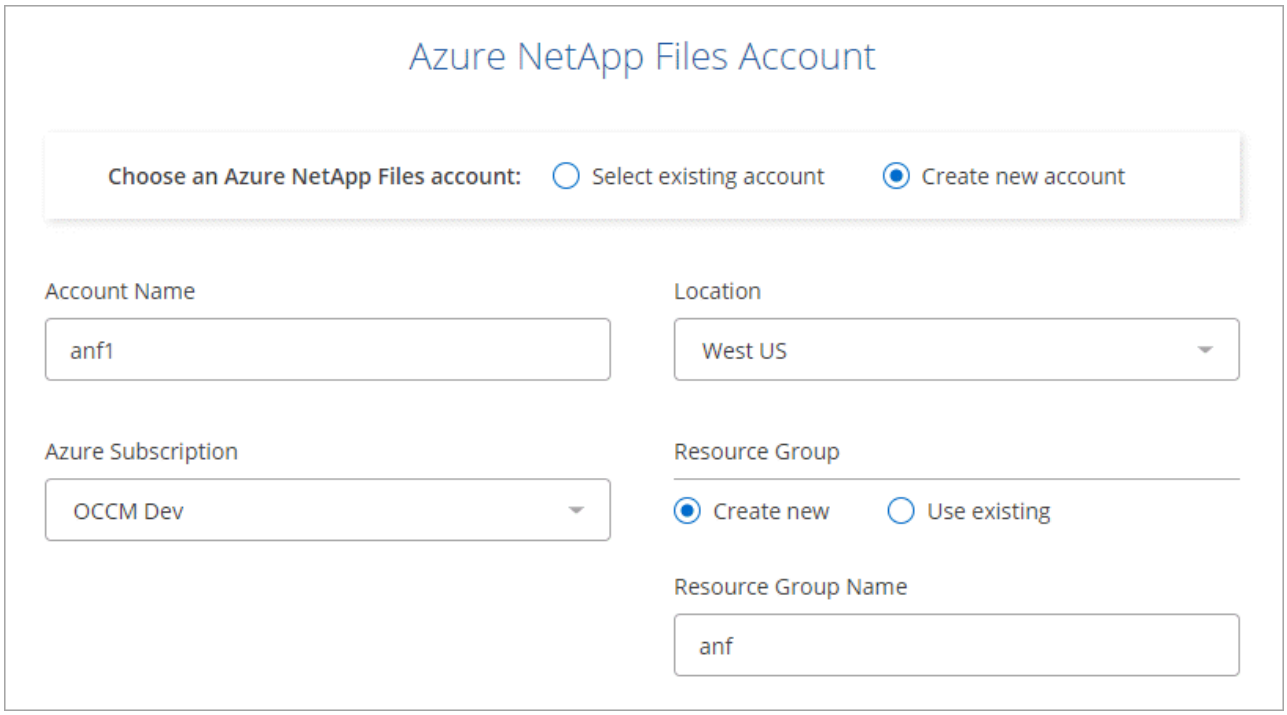
Creazione di volumi

È possibile creare volumi NFS o SMB in un account Azure NetApp Files nuovo o esistente.

Fasi

1. Aprire l'ambiente di lavoro Azure NetApp Files.
2. Fare clic su **Add New Volume** (Aggiungi nuovo volume).
3. Fornire le informazioni richieste in ciascuna pagina:

   - **Azure NetApp Files account**: Scegli un account Azure NetApp Files esistente o crea un nuovo account.



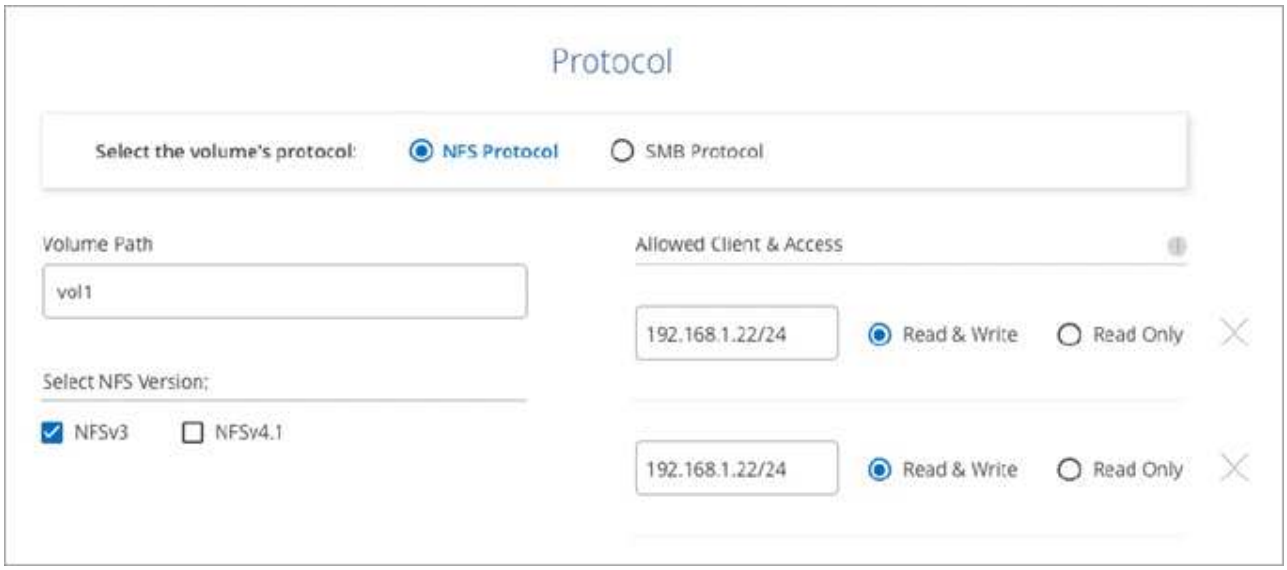
   - **Capacity Pool**: Selezionare un pool di capacità esistente o creare un nuovo pool di capacità.

     Se si crea un nuovo pool di capacità, è necessario specificare una dimensione e selezionare una "livello di servizio".

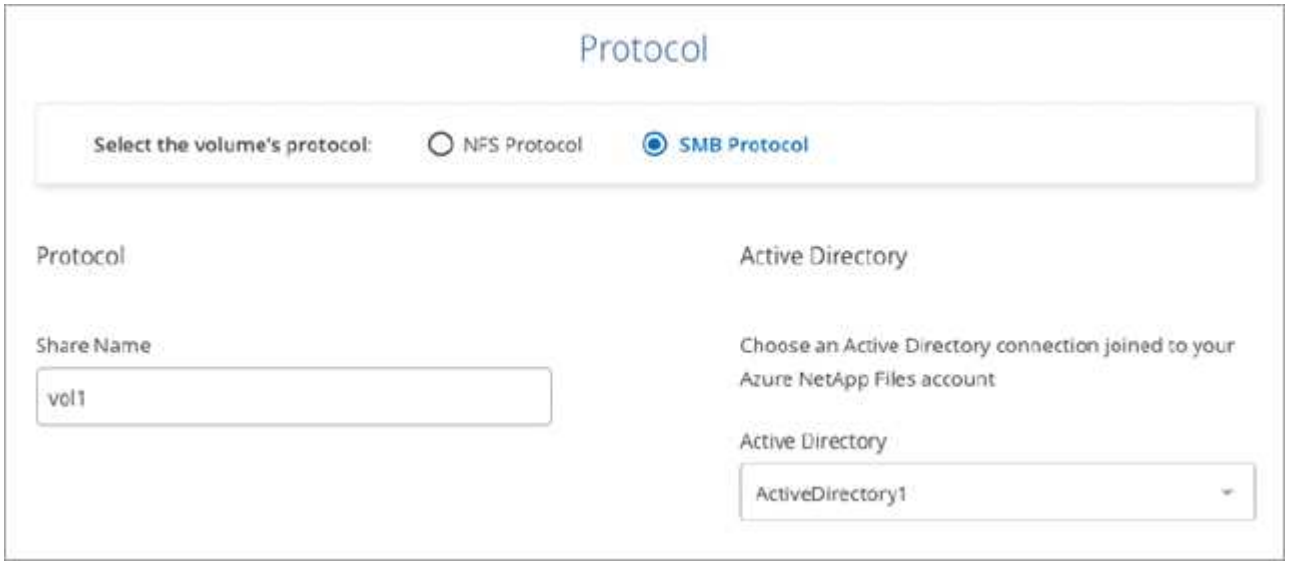
     La dimensione minima per il pool di capacità è di 4 TB. È possibile specificare una dimensione in multipli di 4 TB.

   - **Dettagli e tag**: Inserire il nome e le dimensioni di un volume, il VNET e la subnet in cui deve risiedere il volume e, facoltativamente, specificare i tag per il volume.
   - **Protocol** (protocollo): Scegliere il protocollo NFS o SMB e inserire le informazioni richieste.

     Ecco un esempio di dettagli per NFS.



Ecco un esempio di dettagli per le PMI. Quando si imposta il primo volume SMB, è necessario fornire informazioni su Active Directory.



4. Fare clic su **Add Volume** (Aggiungi volume).

Volumi di montaggio

Accedi alle istruzioni di montaggio da Cloud Manager per montare il volume su un host.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e selezionare **montare il volume**.

3. Seguire le istruzioni per montare il volume.

Modifica delle dimensioni e dei tag di un volume

Dopo aver creato un volume, è possibile modificarne le dimensioni e i tag in qualsiasi momento.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e selezionare **Edit** (Modifica).
3. Modificare le dimensioni e i tag in base alle esigenze.
4. Fare clic su **Apply** (Applica).

Gestione delle copie Snapshot

Le copie Snapshot forniscono una copia point-in-time del volume. Creare copie Snapshot, ripristinare i dati in un nuovo volume ed eliminare le copie Snapshot.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e scegliere una delle opzioni disponibili per gestire le copie Snapshot:
   - **Creare una copia Snapshot**
   - **Ripristinare su un nuovo volume**
   - **Eliminare una copia Snapshot**
3. Seguire le istruzioni per completare l'azione selezionata.

Eliminazione di volumi

Eliminare i volumi non più necessari.

Fasi

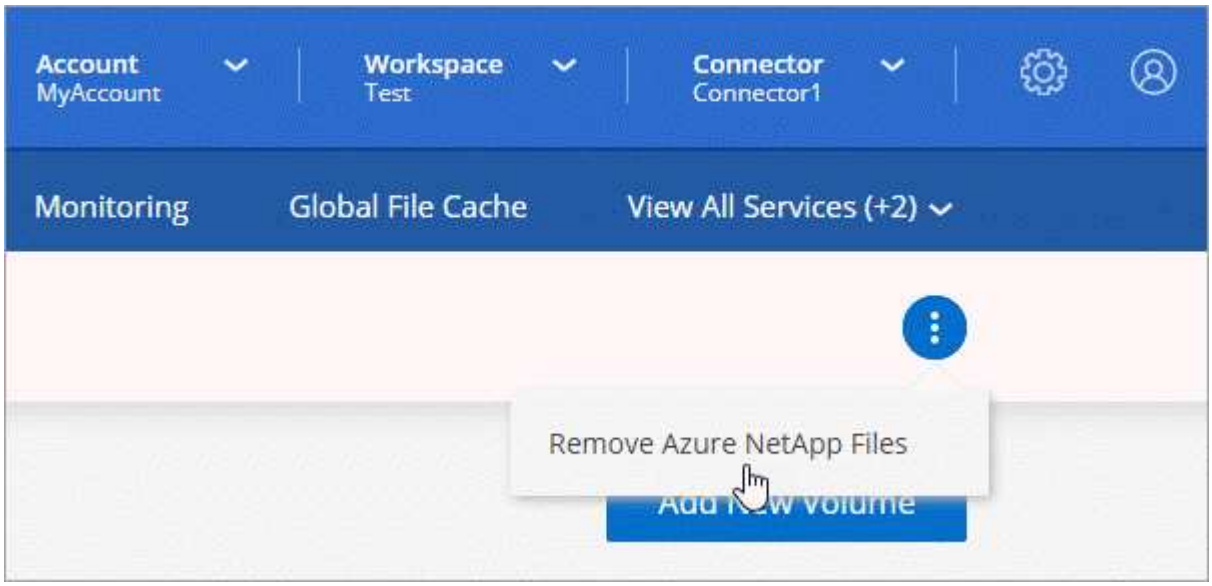
1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Delete** (Elimina).
3. Confermare che si desidera eliminare il volume.

Rimozione di Azure NetApp Files

Questa azione rimuove Azure NetApp Files da Cloud Manager. Non elimina l'account o i volumi Azure NetApp Files. Puoi aggiungere nuovamente Azure NetApp Files a Cloud Manager in qualsiasi momento.

Fasi

1. Aprire l'ambiente di lavoro Azure NetApp Files.
2. Nella parte superiore destra della pagina, selezionare il menu delle azioni e fare clic su **Rimuovi Azure NetApp Files**.



3. Fare clic su **Remove** (Rimuovi) per confermare.

Cloud Volumes Service per AWS

Scopri di più su Cloud Volumes Service per AWS

NetApp Cloud Volumes Service per AWS è un file service nativo nel cloud che offre volumi NAS su NFS e SMB con performance all-flash. Questo servizio consente l'esecuzione di qualsiasi workload, incluse le applicazioni legacy, nel cloud AWS.

Vantaggi dell'utilizzo di Cloud Volumes Service per AWS

Cloud Volumes Service per AWS offre i seguenti vantaggi:

- Servizio completamente gestito, quindi non è necessario configurare o gestire i dispositivi storage
- Supporto per i protocolli NFSv3 e NFSv4.1 e SMB 3.0 e 3.1.1 NAS
- Accesso sicuro alle istanze Linux e Windows Elastic Container Service (ECS), con supporto incluso quanto segue:
  - Amazon Linux 2, Red Hat Enterprise Linux 7.5, SLES 12 SP3 e Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2 e Windows Server 2016
- Scelta di prezzi in bundle e pay-as-you-go

Costo

I volumi creati da Cloud Volumes Service per AWS vengono addebitati in base all'abbonamento al servizio, non tramite Cloud Manager.

Non sono previsti costi per rilevare un volume o una regione Cloud Volumes Service per AWS da Cloud Manager.

Prima di iniziare

- Cloud Manager è in grado di rilevare le sottoscrizioni e i volumi esistenti di Cloud Volumes Service per AWS. Vedere "Guida alla configurazione dell'account NetApp Cloud Volumes Service per AWS" se non hai ancora configurato l'abbonamento. È necessario seguire questa procedura di configurazione per ciascuna regione prima di poter aggiungere gli abbonamenti AWS e i volumi in Cloud Manager.
- È necessario ottenere la chiave API e la chiave segreta Cloud Volumes per poterli fornire a Cloud Manager. "Per istruzioni, consultare la documentazione di Cloud Volumes Service per AWS".

Avvio rapido

Inizia subito seguendo questi passaggi oppure vai alla sezione successiva per i dettagli completi.

Verificare il supporto per la configurazione

È stato configurato AWS per Cloud Volumes Service ed è necessario essere abbonati a uno dei "Offerte NetApp Cloud Volumes Service sul mercato AWS".

Aggiungi il tuo abbonamento a Cloud Volumes Service per AWS

È necessario creare un ambiente di lavoro per i volumi in base all'abbonamento a Cloud Volumes Service per AWS.

Creare volumi cloud

I volumi cloud già esistenti per questo abbonamento vengono visualizzati nel nuovo ambiente di lavoro. In caso contrario, crei nuovi volumi da Cloud Manager.

Montare un volume cloud

Installa nuovi volumi cloud nella tua istanza AWS in modo che gli utenti possano iniziare a utilizzare lo storage.

Assistenza

USA la chat di Cloud Manager per domande generali sull'assistenza.

Per problemi di supporto tecnico associati ai volumi cloud, utilizza il numero di serie a 20 cifre "930" nella scheda "supporto" dell'interfaccia utente di Cloud Volumes Service. Utilizzare questo ID di supporto per aprire un ticket Web o per chiamare il supporto. Assicurarsi di attivare il numero di serie di Cloud Volumes Service per il supporto dall'interfaccia utente di Cloud Volumes Service. "Questi passaggi sono spiegati qui".

Limitazioni

- Cloud Manager non supporta la replica dei dati tra ambienti di lavoro quando si utilizzano volumi Cloud Volumes Service.
- La rimozione dell'abbonamento a Cloud Volumes Service per AWS da Cloud Manager non è supportata. È possibile eseguire questa operazione solo tramite l'interfaccia Cloud Volumes Service per AWS.

Link correlati

- "NetApp Cloud Central: Cloud Volumes Service per AWS"
- "Documentazione di NetApp Cloud Volumes Service per AWS"

Gestione di Cloud Volumes Service per AWS

Cloud Manager ti consente di creare volumi cloud in base al tuo "Cloud Volumes Service per AWS" iscrizione. Puoi anche scoprire i volumi cloud che hai già creato dall'interfaccia Cloud Volumes Service e aggiungerli a un ambiente di lavoro.

Aggiungi il tuo abbonamento a Cloud Volumes Service per AWS

Indipendentemente dal fatto che siano già stati creati volumi dall'interfaccia utente di Cloud Volumes Service o se si è appena iscritti a Cloud Volumes Service per AWS e non si dispone ancora di volumi, il primo passo è creare un ambiente di lavoro per i volumi in base all'abbonamento AWS.

Se per questo abbonamento esistono già volumi cloud, i volumi vengono aggiunti automaticamente al nuovo ambiente di lavoro. Se non hai ancora aggiunto volumi cloud per l'abbonamento AWS, lo fai dopo aver creato il nuovo ambiente di lavoro.

Se si dispone di sottoscrizioni e volumi in più regioni AWS, è necessario eseguire questa attività per ciascuna regione.

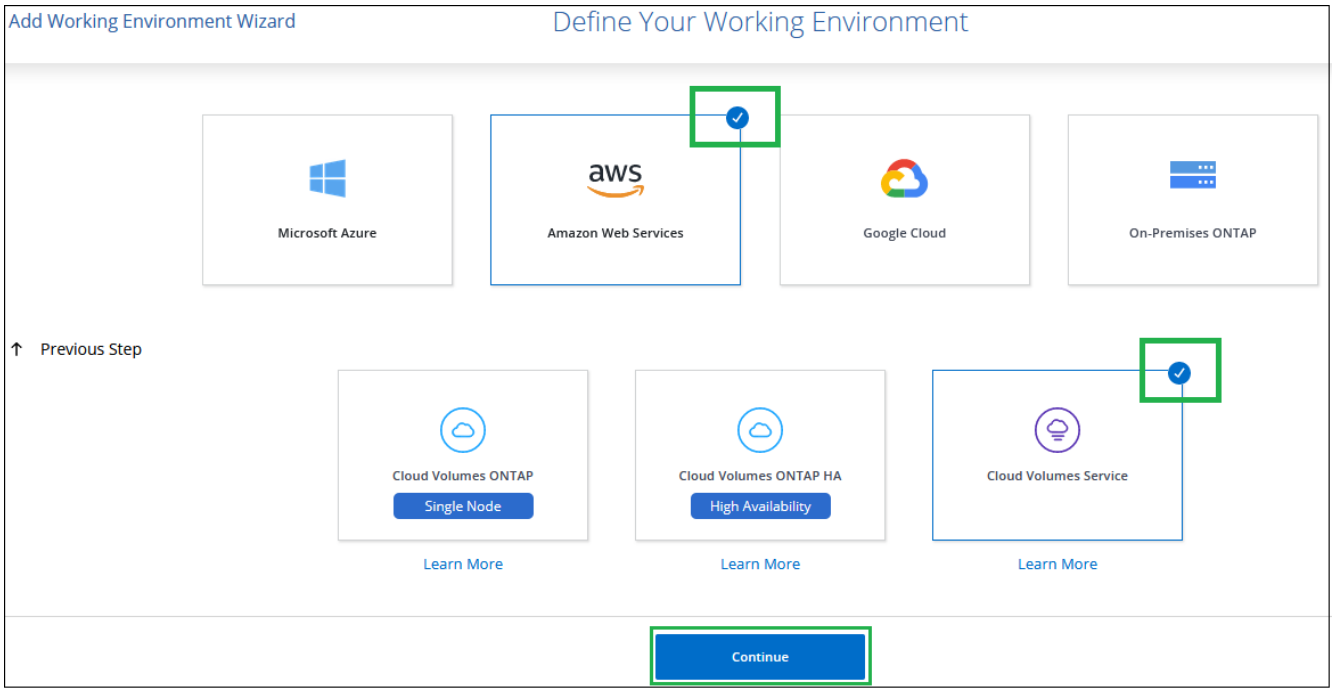
Prima di iniziare

Quando si aggiunge un abbonamento in ciascuna regione, è necessario disporre delle seguenti informazioni:

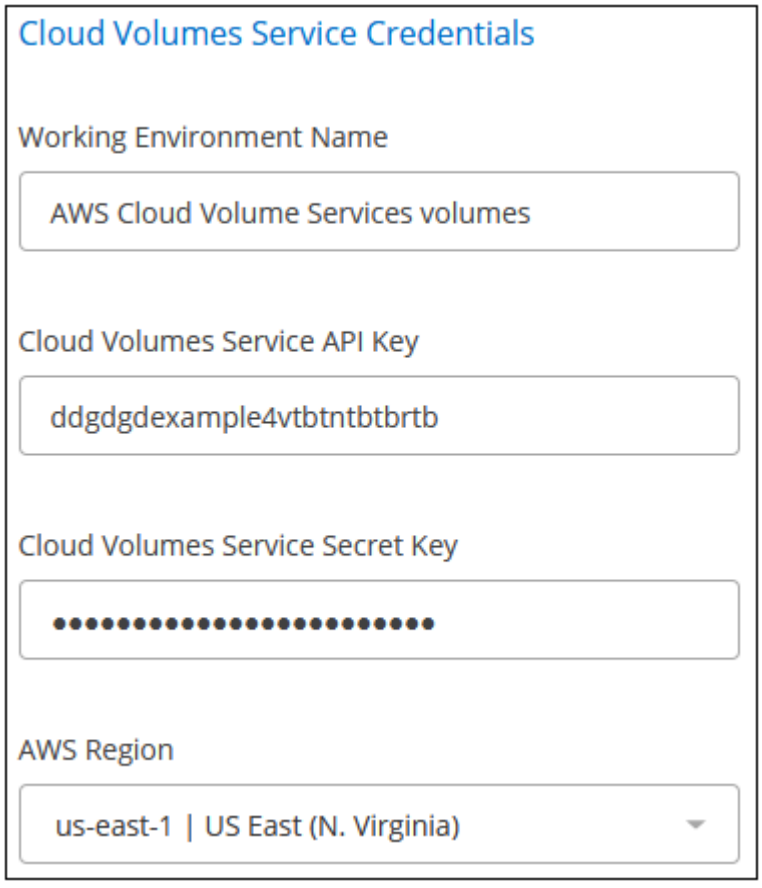
- Chiave API e chiave segreta Cloud Volumes: "Consultare la documentazione di Cloud Volumes Service per AWS per ottenere queste informazioni".
- Regione AWS in cui è stato creato l'abbonamento.

Fasi

1. In Cloud Manager, Aggiungi un nuovo ambiente di lavoro, seleziona la posizione **Amazon Web Services** e fai clic su **continua**.
2. Selezionare **Cloud Volumes Service** e fare clic su **Continue**.



3. Fornisci informazioni sull'abbonamento a Cloud Volumes Service:
   a. Inserire il nome dell'ambiente di lavoro che si desidera utilizzare.
   b. Inserire la chiave API Cloud Volumes Service e la chiave segreta.
   c. Selezionare la regione AWS in cui risiedono i volumi cloud o dove verranno implementati.
   d. Fare clic su **Aggiungi**.



Risultato

Cloud Manager visualizza la configurazione di Cloud Volumes Service per AWS nella pagina Working Environments (ambienti di lavoro).

Se per questo abbonamento esistono già volumi cloud, i volumi vengono aggiunti automaticamente al nuovo ambiente di lavoro, come mostrato nella schermata. Puoi aggiungere altri volumi cloud da Cloud Manager.

Se non esistono volumi cloud per questo abbonamento, puoi crearli ora.

Creare volumi cloud

Per le configurazioni in cui i volumi sono già presenti nell'ambiente di lavoro Cloud Volumes Service, è possibile utilizzare questa procedura per aggiungere nuovi volumi.

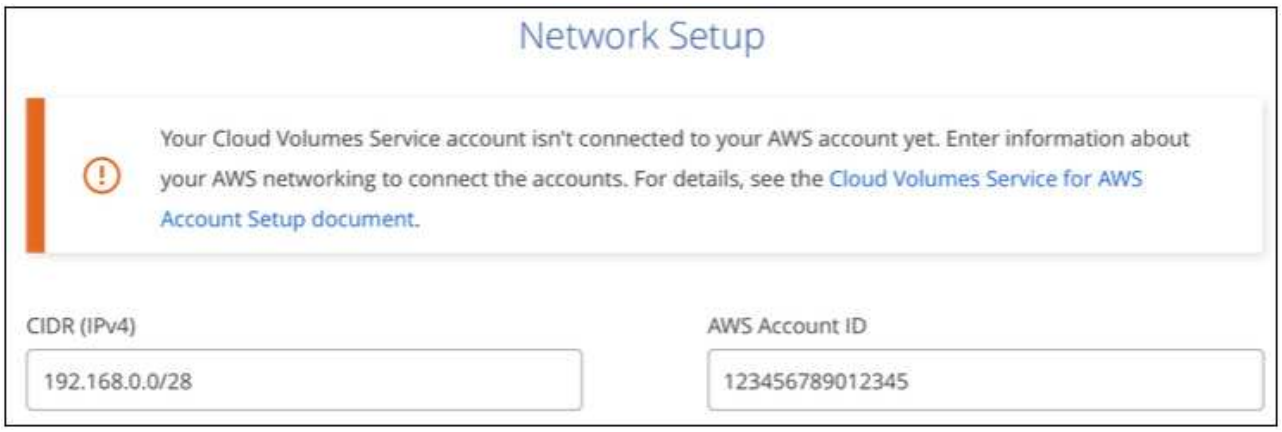
Per le configurazioni in cui non esistono volumi, è possibile creare il primo volume direttamente da Cloud Manager dopo aver configurato l'abbonamento a Cloud Volumes Service per AWS. In passato, il primo volume doveva essere creato direttamente nell'interfaccia utente di Cloud Volumes Service.

Prima di iniziare

- Se si desidera utilizzare SMB in AWS, è necessario aver configurato DNS e Active Directory.
- Quando si intende creare un volume SMB, è necessario disporre di un server Windows Active Directory a cui connettersi. Queste informazioni verranno inserite durante la creazione del volume. Inoltre, assicurarsi che l'utente Admin sia in grado di creare un account macchina nel percorso dell'unità organizzativa (OU) specificato.
- Queste informazioni saranno necessarie quando si crea il primo volume in una nuova regione/ambiente di lavoro:
  - AWS account ID (ID account AWS): Un identificativo di account Amazon a 12 cifre senza trattini. Per trovare l'ID account, fare riferimento a questa sezione "Argomento AWS".
  - Blocco CIDR (Classless Inter-Domain Routing): Un blocco CIDR IPv4 non utilizzato. Il prefisso di rete deve essere compreso tra /16 e /28 e deve rientrare anche negli intervalli riservati alle reti private (RFC 1918). Non scegliere una rete che si sovrapponga alle allocazioni CIDR VPC.

Fasi

1. Selezionare il nuovo ambiente di lavoro e fare clic su **Add New Volume** (Aggiungi nuovo volume).
2. Se si aggiunge il primo volume all'ambiente di lavoro nella regione, è necessario aggiungere informazioni di rete AWS.
   a. Immettere l'intervallo IPv4 (CIDR) per la regione.
   b. Inserisci l'ID dell'account AWS a 12 cifre (senza trattini) per connettere l'account Cloud Volumes al tuo account AWS.
   c. Fare clic su **continua**.



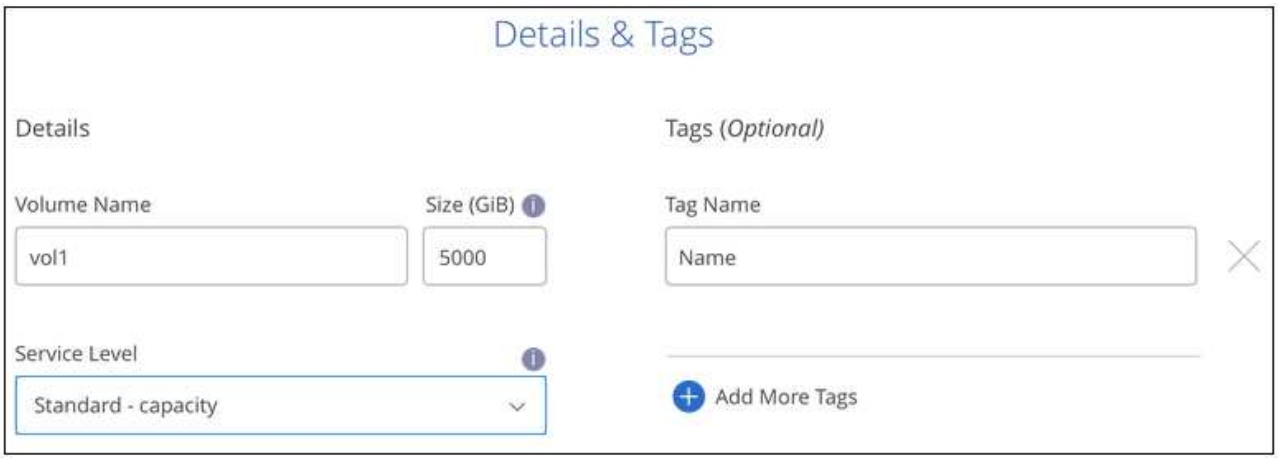
3. La pagina accettazione delle interfacce virtuali descrive alcuni passaggi da eseguire dopo l'aggiunta del volume in modo da essere pronti a completare tale passaggio. Fai clic su **continua** di nuovo.
4. Nella pagina Details & Tags (Dettagli e tag), immettere i dettagli relativi al volume:
   a. Immettere un nome per il volume.
   b. Specificare una dimensione compresa nell'intervallo da 100 GiB a 90,000 GiB (equivalente a 88 Tibs).

      "Scopri di più sulla capacità allocata".

   c. Specificare un livello di servizio: Standard, Premium o Extreme.

      "Scopri di più sui livelli di servizio".

   d. Inserire uno o più nomi di tag per classificare il volume, se si desidera.
   e. Fare clic su **continua**.



5. Nella pagina Protocol (protocollo), selezionare NFS, SMB o Dual Protocol (protocollo doppio), quindi definire i dettagli. Le voci richieste per NFS e SMB sono illustrate in sezioni separate di seguito.
6. Nel campo Volume Path (percorso volume), specificare il nome dell'esportazione del volume che verrà visualizzato quando si monta il volume.
7. Se si seleziona Dual-Protocol, è possibile selezionare lo stile di protezione selezionando NTFS o UNIX. Gli stili di sicurezza influiscono sul tipo di autorizzazione del file utilizzato e sulla modalità di modifica delle autorizzazioni.
   - UNIX utilizza i bit di modalità NFSv3 e solo i client NFS possono modificare le autorizzazioni.

◦ NTFS utilizza ACL NTFS e solo i client SMB possono modificare le autorizzazioni.

8. Per NFS:

   a. Nel campo NFS Version (versione NFS), selezionare NFSv3, NFSv4.1 o entrambi a seconda dei requisiti.

   b. Facoltativamente, è possibile creare una policy di esportazione per identificare i client che possono accedere al volume. Specificare:

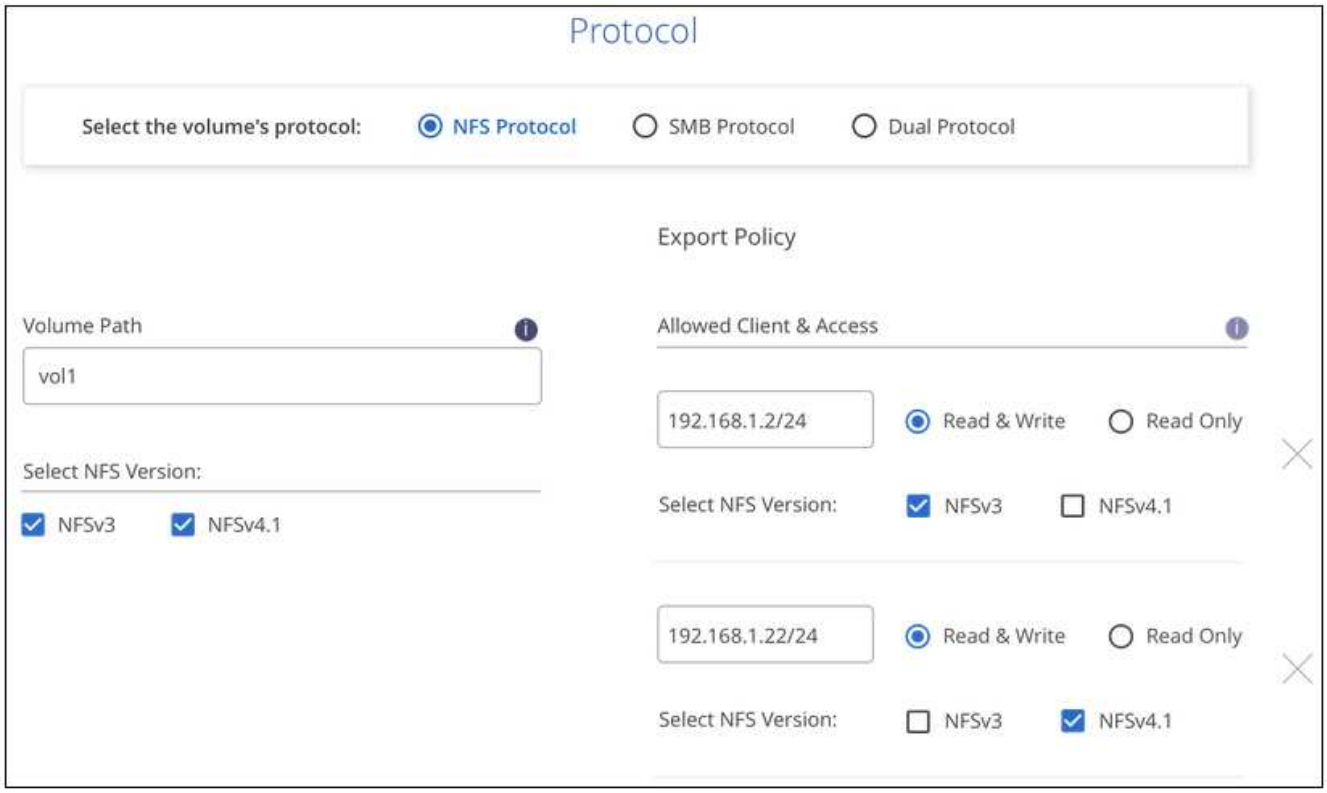
      ▪ Client consentiti utilizzando un indirizzo IP o CIDR (Classless Inter-Domain Routing).

      ▪ Diritti di accesso in lettura e scrittura o in sola lettura.

      ▪ Protocollo di accesso (o protocolli se il volume consente l'accesso NFSv3 e NFSv4.1) utilizzato per gli utenti.

      ▪ Fare clic su **+ Add Export Policy Rule** (Aggiungi regola policy di esportazione) se si desidera definire ulteriori regole dei criteri di esportazione.

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



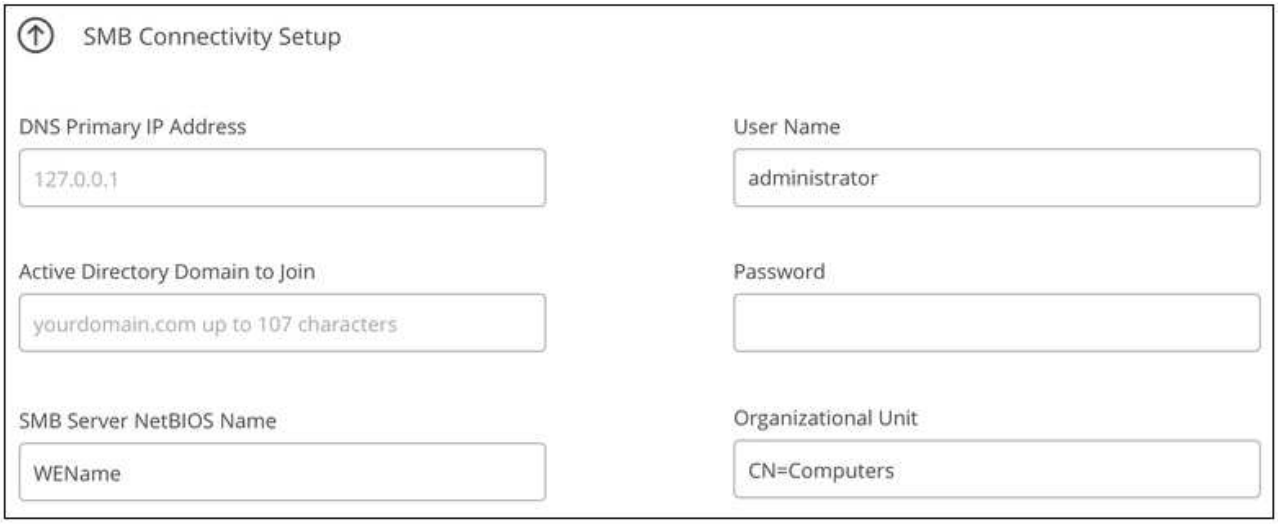
9. Per PMI:

   a. È possibile attivare la crittografia della sessione SMB selezionando la casella di controllo SMB Protocol Encryption (crittografia protocollo SMB).

   b. È possibile integrare il volume con un server Windows Active Directory esistente completando i campi nella sezione Active directory:

Campo	Descrizione
Indirizzo IP primario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server SMB. Utilizzare una virgola per separare gli indirizzi IP quando si fa riferimento a più server, ad esempio 172.31.25.223, 172.31.2.74.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server SMB si unisca. Quando si utilizza AWS Managed Microsoft ad, utilizzare il valore del campo "Directory DNS name" (Nome DNS directory).
Nome NetBIOS del server SMB	Un nome NetBIOS per il server SMB che verrà creato.
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.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server SMB. L'impostazione predefinita è CN=computer per le connessioni al proprio server Windows Active Directory. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes Service, immettere **OU=computer,OU=corp** in questo campo.

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



Seguire le istruzioni relative alle impostazioni del gruppo di sicurezza AWS per consentire ai volumi cloud di integrarsi correttamente con i server Windows Active Directory. Vedere "Impostazioni del gruppo di protezione AWS per i server Windows ad" per ulteriori informazioni.

10. Nella pagina Volume from Snapshot (Volume da snapshot), se si desidera creare questo volume in base a uno snapshot di un volume esistente, selezionare lo snapshot dall'elenco a discesa Snapshot Name (Nome snapshot).
11. Nella pagina Snapshot Policy, è possibile abilitare Cloud Volumes Service per creare copie Snapshot dei volumi in base a una pianificazione. È possibile eseguire questa operazione ora o modificare il volume in un secondo momento per definire il criterio di snapshot.

    Vedere "Creazione di un criterio di snapshot" per ulteriori informazioni sulla funzionalità di snapshot.

12. Fare clic su **Add Volume** (Aggiungi volume).

Il nuovo volume viene aggiunto all'ambiente di lavoro.

Al termine

Se si tratta del primo volume creato in questo abbonamento AWS, è necessario avviare AWS Management Console per accettare le due interfacce virtuali che verranno utilizzate in questa regione AWS per connettere tutti i volumi cloud. Vedere "Guida alla configurazione dell'account NetApp Cloud Volumes Service per AWS" per ulteriori informazioni.

È necessario accettare le interfacce entro 10 minuti dopo aver fatto clic sul pulsante **Add Volume** (Aggiungi volume), altrimenti il sistema potrebbe scadere. In questo caso, inviare un'e-mail all'indirizzo cvs-support@netapp.com con l'ID cliente AWS e il numero di serie NetApp. Il supporto risolverà il problema ed è possibile riavviare il processo di assunzione.

Quindi continuare con "Montaggio del volume cloud".

Montare il volume cloud

È possibile montare un volume cloud sull'istanza di AWS. I volumi cloud attualmente supportano NFSv3 e NFSv4.1 per client Linux e UNIX e SMB 3.0 e 3.1.1 per client Windows.

Nota: utilizzare il protocollo/dialetto evidenziato supportato dal client.

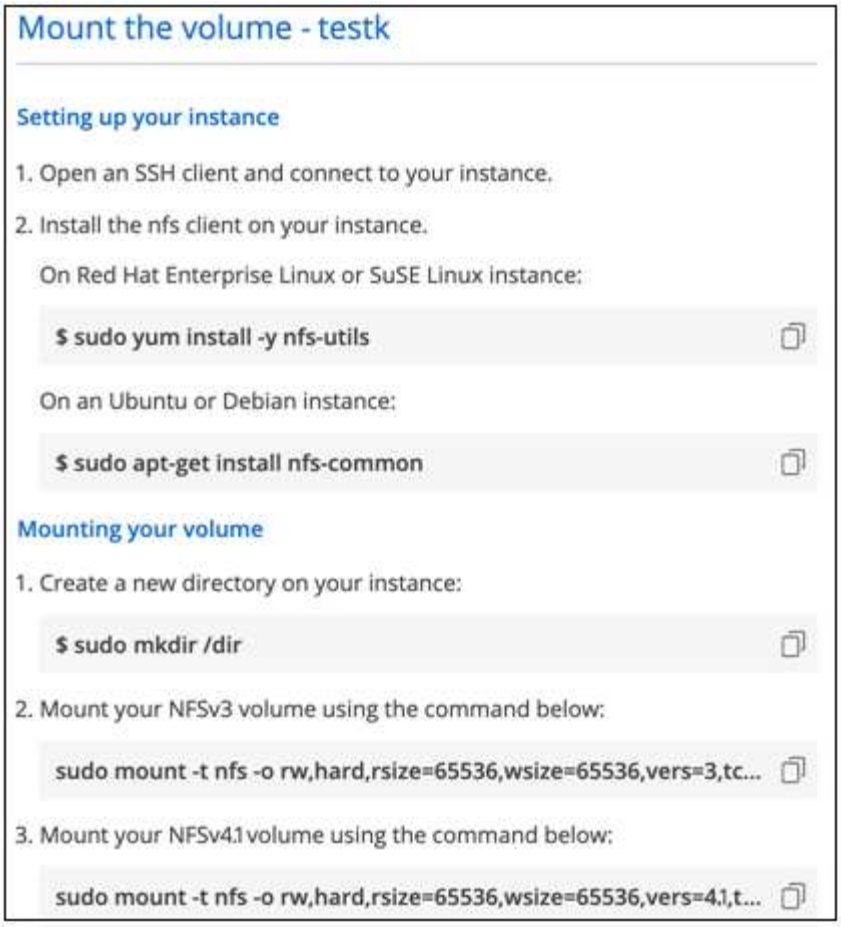
Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **montare il volume**.

   I volumi NFS e SMB visualizzano le istruzioni di montaggio per quel protocollo. I volumi a doppio protocollo forniscono entrambe le serie di istruzioni.

3. Passare il mouse sui comandi e copiarli negli Appunti per semplificare questo processo. Basta aggiungere la directory di destinazione/punto di montaggio alla fine del comando.

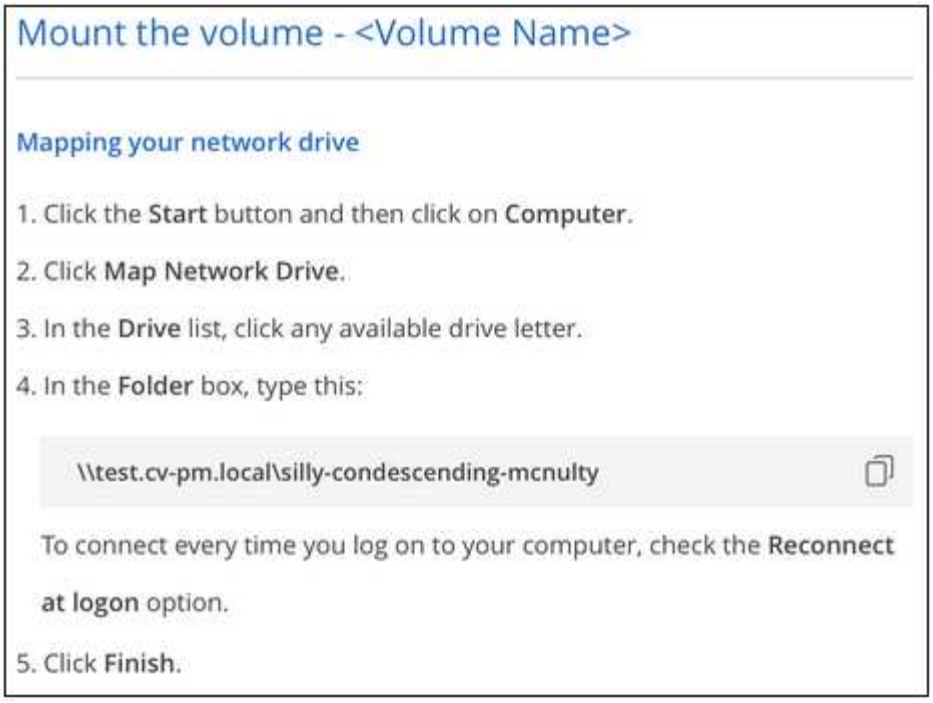
   Esempio NFS:



La dimensione i/o massima definita da `rsize` e. `wsize` options è 1048576, tuttavia 65536 è l'impostazione predefinita consigliata per la maggior parte dei casi di utilizzo.

Si noti che i client Linux imposteranno per impostazione predefinita NFSv4.1, a meno che la versione non sia specificata con `vers=<nfs_version>` opzione.

Esempio SMB:



4. Connettersi all'istanza di Amazon Elastic Compute Cloud (EC2) utilizzando un client SSH o RDP, quindi seguire le istruzioni di montaggio dell'istanza.

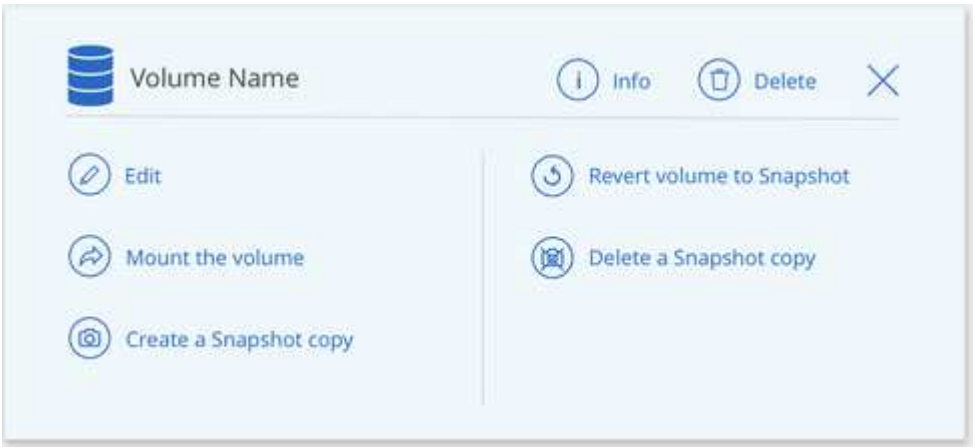
   Dopo aver completato i passaggi nelle istruzioni di montaggio, il volume cloud è stato montato correttamente sull'istanza di AWS.

Gestione dei volumi esistenti

Puoi gestire i volumi esistenti in base alle tue esigenze di storage. È possibile visualizzare, modificare, ripristinare ed eliminare i volumi.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume.



3. Gestisci i tuoi volumi:

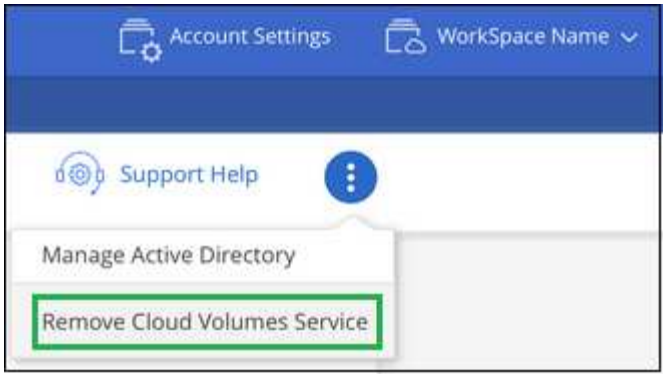
Attività	Azione
Consente di visualizzare informazioni su un volume	Selezionare un volume, quindi fare clic su **Info**.
Modifica di un volume (inclusa la policy di snapshot)	a. Selezionare un volume, quindi fare clic su **Modifica**. b. Modificare le proprietà del volume, quindi fare clic su **Update** (Aggiorna).
Ottieni il comando di montaggio NFS o SMB	a. Selezionare un volume, quindi fare clic su **montare il volume**. b. Fare clic su **Copy** (Copia) per copiare i comandi.
Crea una copia Snapshot on-demand	a. Selezionare un volume, quindi fare clic su **Crea una copia Snapshot**. b. Modificare il nome dello snapshot, se necessario, quindi fare clic su **Create** (Crea).
Sostituire il volume con il contenuto di una copia Snapshot	a. Selezionare un volume, quindi fare clic su **Ripristina volume in Snapshot**. b. Selezionare una copia Snapshot e fare clic su **Ripristina**.
Eliminare una copia Snapshot	a. Selezionare un volume, quindi fare clic su **Delete a Snapshot copy** (Elimina una copia Snapshot). b. Selezionare la copia Snapshot che si desidera eliminare e fare clic su **Delete** (Elimina). c. Fare nuovamente clic su **Delete** per confermare.
Eliminare un volume	a. Smontare il volume da tutti i client: ◦ Sui client Linux, utilizzare `umount` comando. ◦ Sui client Windows, fare clic su **Disconnetti unità di rete**. b. Selezionare un volume, quindi fare clic su **Delete** (Elimina). c. Fare nuovamente clic su **Delete** per confermare.

Rimuovere Cloud Volumes Service da Cloud Manager

Puoi rimuovere un abbonamento a Cloud Volumes Service per AWS e tutti i volumi esistenti da Cloud Manager. I volumi non vengono cancellati, ma vengono semplicemente rimossi dall'interfaccia di Cloud Manager.

Fasi

1. Aprire l'ambiente di lavoro.



2. Fare clic su Nella parte superiore della pagina e fare clic su **Rimuovi Cloud Volumes Service**.
3. Nella finestra di dialogo di conferma, fare clic su **Rimuovi**.

Gestire la configurazione di Active Directory

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server SMB in Cloud Volumes Services in modo che possa continuare a servire lo storage ai client.

È inoltre possibile eliminare il collegamento ad Active Directory se non è più necessario.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic su Nella parte superiore della pagina e fare clic su **Gestisci Active Directory**.
3. Se non è configurata alcuna Active Directory, è possibile aggiungerne una ora. Se ne è stata configurata una, è possibile modificare le impostazioni o eliminarle utilizzando pulsante.
4. Specificare le impostazioni per Active Directory a cui si desidera accedere:

Campo	Descrizione
Indirizzo IP primario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server SMB. Utilizzare una virgola per separare gli indirizzi IP quando si fa riferimento a più server, ad esempio 172.31.25.223, 172.31.2.74.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server SMB si unisca. Quando si utilizza AWS Managed Microsoft ad, utilizzare il valore del campo "Directory DNS name" (Nome DNS directory).
Nome NetBIOS del server SMB	Un nome NetBIOS per il server SMB che verrà creato.
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.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server SMB. L'impostazione predefinita è CN=computer per le connessioni al proprio server Windows Active Directory. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes Service, immettere **OU=computer,OU=corp** in questo campo.

5. Fare clic su **Save** (Salva) per salvare le impostazioni.

Gestire le snapshot dei volumi cloud

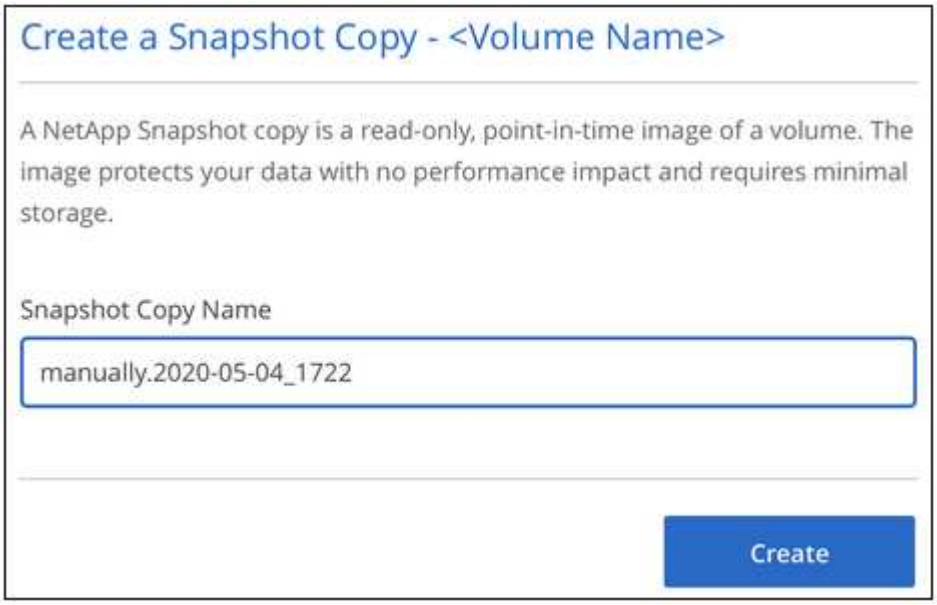
È possibile creare un criterio di snapshot per ciascun volume in modo da poter ripristinare o ripristinare l'intero contenuto di un volume da un momento precedente. È inoltre possibile creare un'istantanea on-demand di un volume cloud quando necessario.

Crea un'istantanea on-demand

È possibile creare uno snapshot on-demand di un volume cloud se si desidera creare uno snapshot con lo stato corrente del volume.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Create a snapshot copy** (Crea una copia snapshot).
3. Immettere un nome per lo snapshot oppure utilizzare il nome generato automaticamente e fare clic su **Create** (Crea).



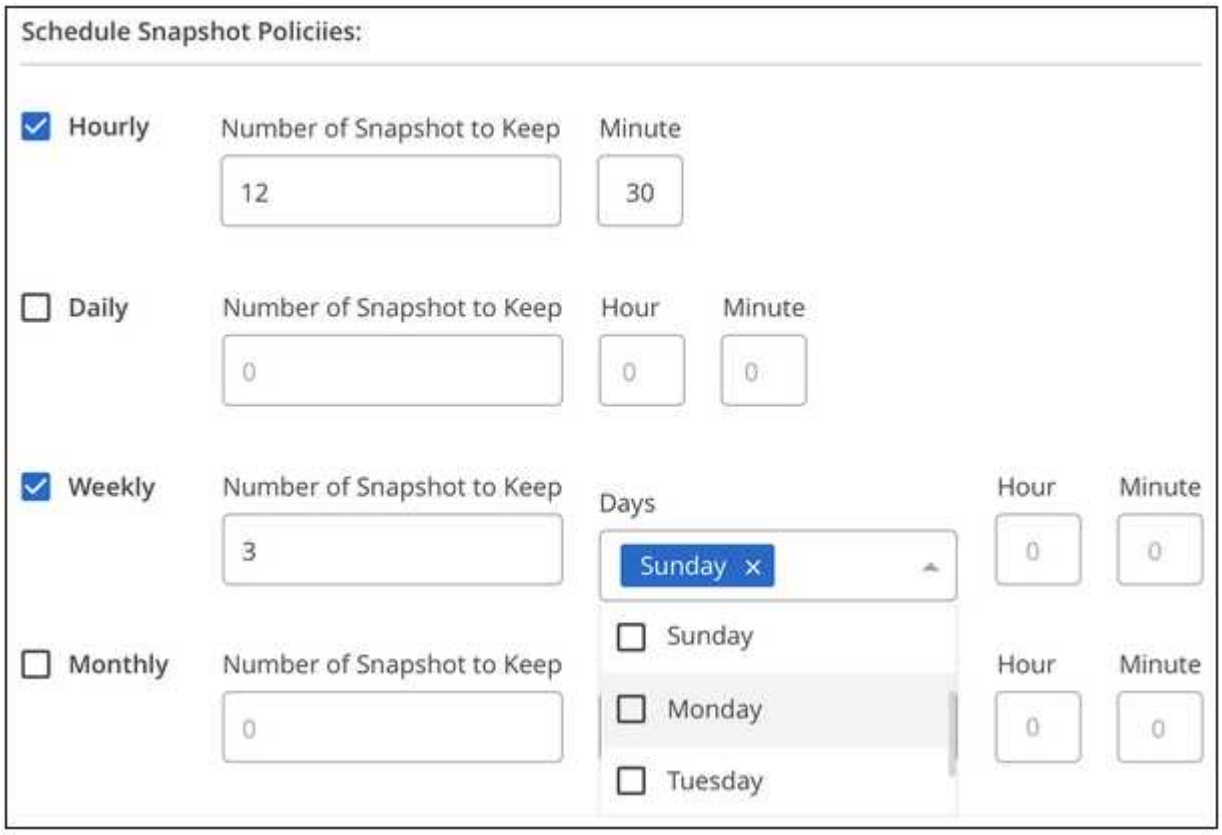
Creare o modificare un criterio di snapshot

È possibile creare o modificare una policy di snapshot in base alle necessità per un volume cloud. La policy di snapshot viene definita dalla scheda *Snapshot Policy* durante la creazione di un volume o la modifica di un volume.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Edit** (Modifica).
3. Dalla scheda *Snapshot Policy*, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso destra.
4. Definire la pianificazione delle snapshot:
   a. Selezionare la frequenza: **Orario**, **giornaliero**, **settimanale** o **mensile**
   b. Selezionare il numero di snapshot che si desidera conservare.

c. Selezionare il giorno, l'ora e il minuto in cui eseguire l'istantanea.



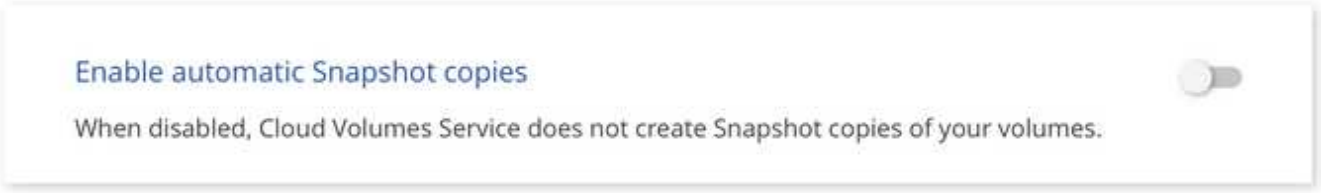
5. Fare clic su **Add volume** (Aggiungi volume) o **Update volume** (Aggiorna volume) per salvare le impostazioni dei criteri.

Disattiva un criterio di snapshot

È possibile disattivare un criterio di snapshot per impedire la creazione di snapshot per un breve periodo di tempo, mantenendo le impostazioni del criterio di snapshot.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Edit** (Modifica).
3. Dalla scheda *Snapshot Policy*, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso sinistra.



4. Fare clic su **Update volume** (Aggiorna volume).

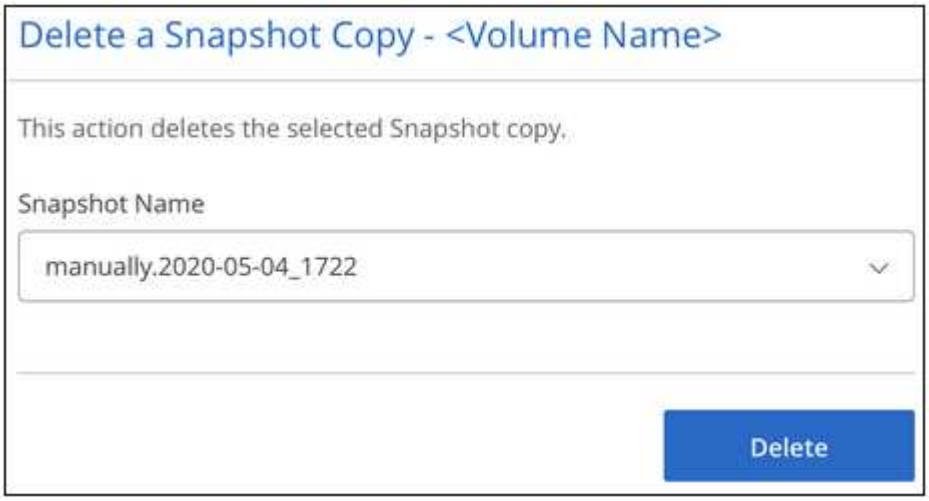
Se si desidera riattivare il criterio di snapshot, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso destra e fare clic su **Update volume** (Aggiorna volume).

Eliminare uno snapshot

È possibile eliminare uno snapshot dalla pagina Volumes (volumi).

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Delete a Snapshot copy** (Elimina una copia Snapshot).
3. Selezionare l'istantanea dall'elenco a discesa e fare clic su **Delete** (Elimina).



4. Nella finestra di dialogo di conferma, fare clic su **Delete** (Elimina).

Ripristinare un volume da uno snapshot

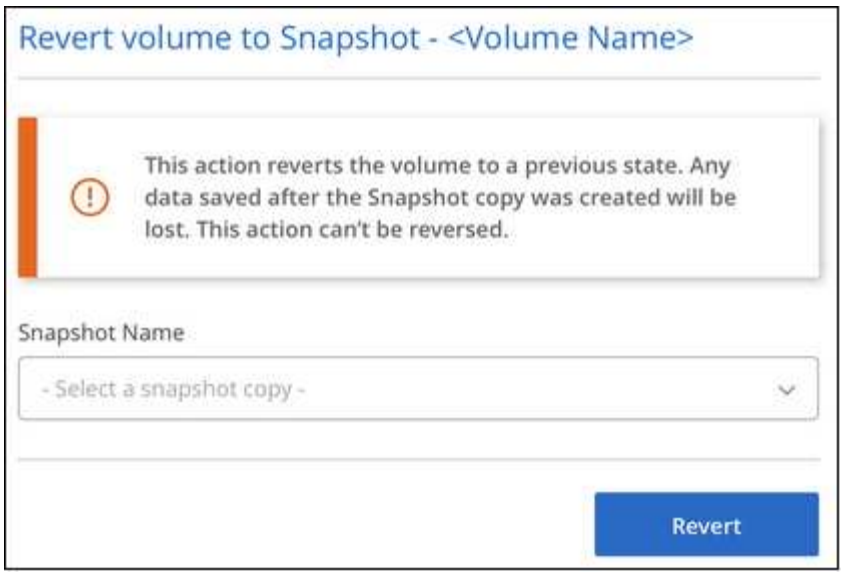
È possibile ripristinare un volume a un momento precedente da uno snapshot esistente.

Quando si ripristina un volume, il contenuto dello snapshot sovrascrive la configurazione del volume esistente. Tutte le modifiche apportate ai dati nel volume dopo la creazione dello snapshot andranno perse.

Tenere presente che i client non devono rimontare il volume dopo l'operazione di revert.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Ripristina volume in Snapshot**.
3. Selezionare l'istantanea che si desidera utilizzare per ripristinare il volume esistente dall'elenco a discesa e fare clic su **Ripristina**.



Riferimento

Livelli di servizio e capacità allocata

Il costo di Cloud Volumes Service per AWS si basa sul *livello di servizio* e sulla *capacità allocata* selezionati. La scelta del livello di servizio e della capacità appropriati ti aiuta a soddisfare le tue esigenze di storage al costo più basso.

Considerazioni

Le esigenze di storage includono due aspetti fondamentali:

- La *capacità* dello storage per la conservazione dei dati
- La *larghezza di banda* dello storage per l'interazione con i dati

Se si consuma più spazio di storage rispetto alla capacità selezionata per il volume, si applicano le seguenti considerazioni:

- La capacità di storage aggiuntiva consumata verrà addebitata al prezzo definito dal livello di servizio.
- La quantità di larghezza di banda dello storage disponibile per il volume non aumenta fino a quando non si aumentano le dimensioni della capacità allocata o si modifica il livello di servizio.

Livelli di servizio

Cloud Volumes Service per AWS supporta tre livelli di servizio. Specificare il livello di servizio quando si crea o si modifica il volume.

I livelli di servizio sono adeguati alle diverse esigenze di capacità dello storage e larghezza di banda dello storage:

- **Standard** (capacità)

  Se si desidera una capacità al costo più basso e le esigenze di larghezza di banda sono limitate, il livello di servizio standard potrebbe essere più adatto alle proprie esigenze. Un esempio è l'utilizzo del volume come destinazione di backup.

    - Larghezza di banda: 16 KB di larghezza di banda per GB di capacità fornita
- **Premium** (equilibrio tra capacità e performance)

  Se l'applicazione ha un'esigenza bilanciata di capacità di storage e larghezza di banda, il livello di servizio Premium potrebbe essere più appropriato. Questo livello è meno costoso per MB/s rispetto al livello di servizio Standard ed è anche meno costoso per GB di capacità di storage rispetto al livello di servizio Extreme.

    - Larghezza di banda: 64 KB di larghezza di banda per GB di capacità fornita
- **Extreme** (prestazioni)

  Il livello di servizio Extreme è meno costoso in termini di larghezza di banda dello storage. Se l'applicazione richiede larghezza di banda dello storage senza la richiesta associata di capacità di storage elevate, il livello di servizio Extreme potrebbe essere più adatto alle tue esigenze.

    - Larghezza di banda: 128 KB di larghezza di banda per GB di capacità fornita

Capacità allocata

Specificare la capacità allocata per il volume quando si crea o si modifica il volume.

Anche se si desidera selezionare il livello di servizio in base alle esigenze aziendali generali di alto livello, è necessario selezionare la dimensione della capacità allocata in base alle esigenze specifiche delle applicazioni, ad esempio:

- Spazio di storage necessario per le applicazioni
- La larghezza di banda dello storage al secondo richiesta dalle applicazioni o dagli utenti

La capacità allocata è specificata in GB. La capacità allocata di un volume può essere impostata nell'intervallo compreso tra 100 GB e 100,000 GB (equivalente a 100 TB).

Numero di inode

Volumi inferiori o uguali a 1 TB possono utilizzare fino a 20 milioni di inode. Il numero di inode aumenta di 20 milioni per ogni TB allocato, fino a un massimo di 100 milioni di inode.

- /1 TB = 20 milioni di inode
- Da >1 TB a 2 TB = 40 milioni di inode
- Da >2 TB a 3 TB = 60 milioni di inode
- Da >3 TB a 4 TB = 80 milioni di inode
- Da >4 TB a 100 TB = 100 milioni di inode

Larghezza di banda

La combinazione del livello di servizio e della capacità allocata selezionata determina la larghezza di banda massima per il volume.

Se le applicazioni o gli utenti necessitano di una larghezza di banda superiore a quella selezionata, è possibile modificare il livello di servizio o aumentare la capacità allocata. Le modifiche non interrompono l'accesso ai dati.

Selezione del livello di servizio e della capacità allocata

Per selezionare il livello di servizio più appropriato e la capacità allocata in base alle proprie esigenze, è necessario conoscere la capacità e la larghezza di banda richieste al picco o all'edge.

Elenco dei livelli di servizio e della capacità allocata

La colonna più a sinistra indica la capacità, mentre le altre colonne definiscono i MB/s disponibili in ciascun punto di capacità in base al livello di servizio.

Vedere "Prezzo dell'abbonamento al contratto" e. "Prezzo di abbonamento misurato" per informazioni complete sui prezzi.

Capacità (TB)	Standard (MB/s)	Premium (MB/s)	Estremo (MB/s)
0.1 (100 GB)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072

Capacità (TB)	Standard (MB/s)	Premium (MB/s)	Estremo (MB/s)
25	400	1,600	3,200
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500

Capacità (TB)	Standard (MB/s)	Premium (MB/s)	Estremo (MB/s)
58	928	3,712	4,500
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500

Capacità (TB)	Standard (MB/s)	Premium (MB/s)	Estremo (MB/s)
91	1,456	4,500	4,500
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

Esempio 1

Ad esempio, l'applicazione richiede 25 TB di capacità e 100 MB/s di larghezza di banda. Con una capacità di 25 TB, il livello di servizio Standard fornirebbe una larghezza di banda di 400 MB/s al costo di 2,500 dollari (stima: Vedi prezzi attuali), rendendo Standard il livello di servizio più adatto in questo caso.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800

Esempio 2

Ad esempio, l'applicazione richiede 12 TB di capacità e 800 MB/s di larghezza di banda di picco. Sebbene il livello di servizio Extreme sia in grado di soddisfare le esigenze dell'applicazione con un livello di 12 TB, è più conveniente (stima: Vedi prezzi attuali) selezionare 13 TB con il livello di servizio Premium.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200

Impostazioni del gruppo di protezione AWS per i server Windows ad

Se si utilizzano server Windows Active Directory (ad) con volumi cloud, è necessario acquisire familiarità con le istruzioni relative alle impostazioni del gruppo di sicurezza AWS. Le impostazioni consentono ai volumi cloud di integrarsi correttamente con ad.

Per impostazione predefinita, il gruppo di protezione AWS applicato a un'istanza di EC2 Windows non contiene regole in entrata per alcun protocollo ad eccezione di RDP. Per abilitare la comunicazione in entrata da Cloud Volumes Service, è necessario aggiungere regole ai gruppi di protezione collegati a ciascuna istanza di Windows ad. Le porte richieste sono le seguenti:

Servizio	Porta	Protocollo
SERVIZI Web AD	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	N/A.	Risposta eco
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
Nome NetBIOS	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
LDAP sicuro	636	TCP
LDAP sicuro	3269	TCP
w32time	123	UDP

Se si distribuiscono e gestiscono i domain controller e i server membri dell'installazione ad in un'istanza di AWS EC2, sono necessarie diverse regole del gruppo di protezione per consentire il traffico per Cloud Volumes Service. Di seguito è riportato un esempio di come implementare queste regole per le applicazioni ad come parte del modello AWS CloudFormation.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
        "Name" :
        {
```

```
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
```

```
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "464",
                        "ToPort" : "464"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "389",
                        "ToPort" : "389"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "53",
                        "ToPort" : "53"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "339",
                        "ToPort" : "339"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "123",
                        "ToPort" : "123"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3389",
                        "ToPort" : "3389"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3268",
                        "ToPort" : "3268"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "88",
```

```
                    "ToPort" : "88"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "636",
                    "ToPort" : "636"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3269",
                    "ToPort" : "3269"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "0",
                    "ToPort" : "65535"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "9389",
                    "ToPort" : "9389"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "445",
                    "ToPort" : "445"
                }
            ]
        }
    }
},
"Outputs" :
{
    "SecurityGroupID" :
    {
```

```
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```

Cloud Volumes Service per GCP

Scopri di più su Cloud Volumes Service per Google Cloud

NetApp Cloud Volumes Service per Google Cloud consente di aggiungere rapidamente carichi di lavoro multiprotocollo, nonché di creare e implementare applicazioni basate su Windows e UNIX.

Caratteristiche principali:

- Migrazione dei dati tra on-premise e Google Cloud.
- Provisioning di volumi da 1 a 100 TIB in pochi secondi.
- Supporto multiprotocollo (è possibile creare un volume NFS o SMB).
- Proteggi i dati con snapshot automatizzate ed efficienti.
- Accelera lo sviluppo delle app con il cloning rapido.

Costo

I volumi creati da Cloud Volumes Service per Google Cloud vengono addebitati al tuo abbonamento al servizio, non tramite Cloud Manager.

"Visualizza i prezzi"

Non sono previsti costi per scoprire un volume o un'area Cloud Volumes Service per Google Cloud da Cloud Manager.

Regioni supportate

"Visualizza le aree di Google Cloud supportate."

Prima di iniziare

Cloud Manager è in grado di rilevare le sottoscrizioni e i volumi Cloud Volumes Service per GCP esistenti. Vedere "Documentazione di NetApp Cloud Volumes Service per Google Cloud" se non hai ancora configurato l'abbonamento.

Assistenza

Utilizza la chat di Cloud Manager per domande generali sul funzionamento di Cloud Volumes Service in Cloud Manager.

Per domande generali su Cloud Volumes Service per Google Cloud, invia un'e-mail al team di Google Cloud di NetApp all'indirizzo gcinfo@netapp.com.

Per problemi tecnici associati ai volumi cloud, puoi creare un caso di supporto tecnico da Google Cloud Console. Vedere "ottenere supporto" per ulteriori informazioni.

Limitazioni

- Cloud Manager non supporta la replica dei dati tra ambienti di lavoro quando si utilizzano volumi Cloud Volumes Service.
- L'eliminazione dell'abbonamento a Cloud Volumes Service per Google Cloud da Cloud Manager non è supportata. Puoi farlo solo attraverso Google Cloud Console.

Link correlati

- "NetApp Cloud Central: Cloud Volumes Service per Google Cloud"
- "Documentazione di NetApp Cloud Volumes Service per Google Cloud"

Configura Cloud Volumes Service per Google Cloud

Creare un ambiente di lavoro Cloud Volumes Service per Google Cloud in Cloud Manager per creare e gestire volumi e snapshot.

Avvio rapido

Inizia subito seguendo questi passaggi oppure vai alla sezione successiva per i dettagli completi.

Attivare l'API Cloud Volumes Service

Da Google, abilita l'API Cloud Volumes Service per GCP in modo che Cloud Manager possa gestire i volumi di abbonamento e cloud.

Creare un account di servizio GCP e scaricare le credenziali

Da Google, crea un account e un ruolo di servizio GCP in modo che Cloud Manager possa accedere al tuo account Cloud Volumes Service per GCP.

Creare un ambiente di lavoro Cloud Volumes Service per GCP

In Cloud Manager, fare clic su **Aggiungi ambiente di lavoro** > **Google Cloud** > **Cloud Volumes Service**, quindi fornire i dettagli sull'account del servizio e sul progetto Google Cloud.

Attivare l'API Cloud Volumes Service

In Google Cloud Shell, eseguire il seguente comando per attivare l'API Cloud Volumes Service:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Offri a Cloud Manager l'accesso all'account Cloud Volumes Service per GCP

Devi completare le seguenti attività in modo che Cloud Manager possa accedere al tuo progetto Google Cloud:

- Creare un nuovo account di servizio
- Aggiungere il nuovo membro dell'account di servizio al progetto e assegnargli ruoli specifici (autorizzazioni)
- Creare e scaricare una coppia di chiavi per l'account di servizio utilizzato per l'autenticazione su Google

Fasi

1. In Google Cloud Console, accedere alla pagina **account di servizio**.
2. Fare clic su **Seleziona un progetto**, scegliere il progetto e fare clic su **Apri**.
3. Fare clic su **Create Service account** (Crea account servizio), immettere il nome dell'account del servizio (nome descrittivo) e la descrizione, quindi fare clic su **Create** (Crea).
4. Dalla *pagina IAM* fare clic su **Add** (Aggiungi) e compilare i campi della pagina *Add Members* (Aggiungi membri):
   a. Nel campo New Members (nuovi membri), immettere l'ID completo dell'account del servizio, ad esempio user1-service-account-cvs@project1.iam.gserviceaccount.com.
   b. Aggiungere i seguenti ruoli:
      - *NetApp Cloud Volumes Admin*
      - *Compute Network Viewer*
      - *Visualizzatore cartelle*
   c. Fare clic su **Save** (Salva).
5. Dalla pagina *Dettagli account servizio*, fare clic su **Aggiungi chiave > Crea nuova chiave**.
6. Selezionare **JSON** come tipo di chiave e fare clic su **Create** (Crea).

   Facendo clic su **Create** (Crea), la nuova coppia di chiavi pubbliche/private viene generata e scaricata nel sistema. Funge da unica copia della chiave privata. Memorizzare questo file in modo sicuro perché può essere utilizzato per l'autenticazione come account di servizio.

Per informazioni dettagliate, consulta gli argomenti di Google Cloud "Creazione e gestione degli account di servizio", "Concessione, modifica e revoca dell'accesso alle risorse", e. "Creazione e gestione delle chiavi dell'account di servizio".

Creare un ambiente di lavoro Cloud Volumes Service per GCP

Configura un ambiente di lavoro Cloud Volumes Service per GCP in Cloud Manager per iniziare a creare volumi.

Indipendentemente dal fatto che siano già stati creati volumi dalla console cloud di Google o se si è appena iscritti a Cloud Volumes Service per GCP e non si dispone ancora di volumi, il primo passo è creare un ambiente di lavoro per i volumi in base al proprio abbonamento GCP.

Se esistono già volumi cloud per questo abbonamento, i volumi verranno visualizzati nel nuovo ambiente di lavoro. Se non hai ancora aggiunto volumi cloud per l'abbonamento GCP, lo fai dopo aver creato il nuovo ambiente di lavoro.

Se si dispone di sottoscrizioni e volumi in più progetti GCP, è necessario eseguire questa attività per ogni progetto.

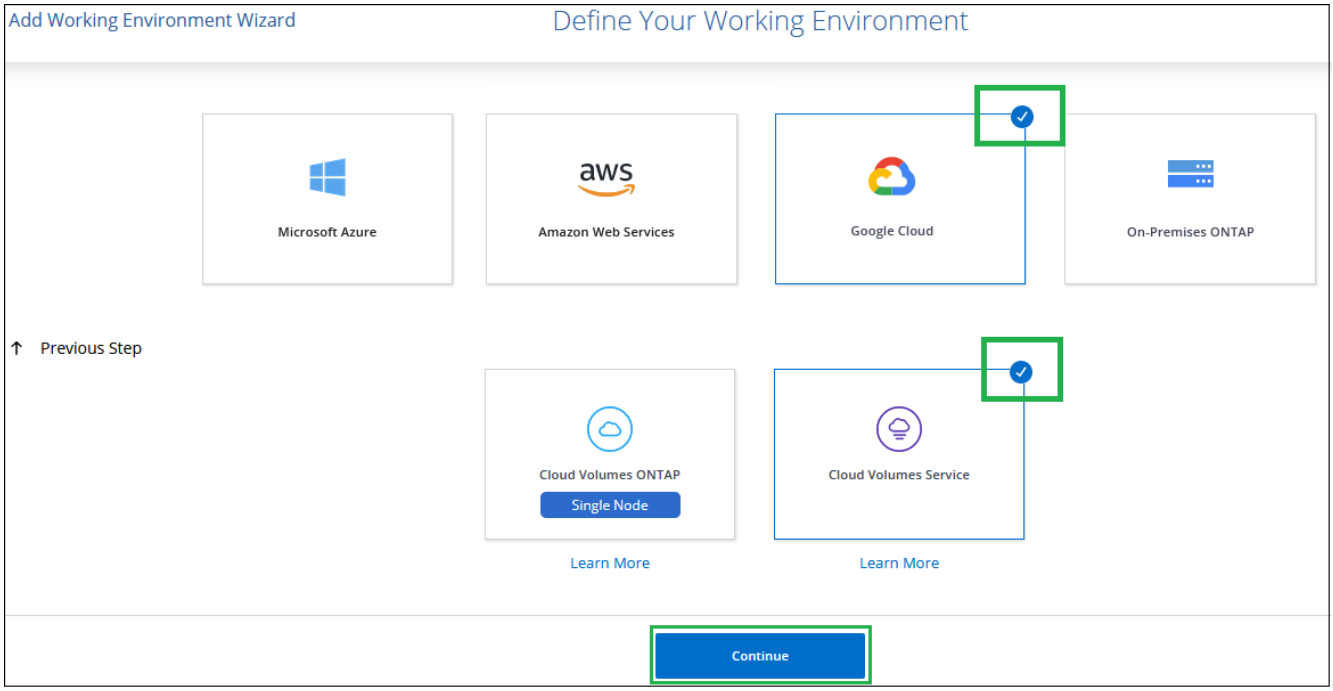
Prima di iniziare

Quando si aggiunge un abbonamento a ciascun progetto, è necessario disporre delle seguenti informazioni:

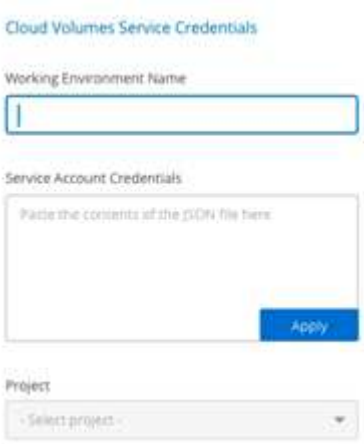
- Credenziali dell'account di servizio (chiave privata JSON scaricata)
- Nome del progetto

Fasi

1. In Cloud Manager, aggiungere un nuovo ambiente di lavoro, selezionare la posizione **Google Cloud** e fare clic su **continua**.
2. Selezionare **Cloud Volumes Service** e fare clic su **Continue**.



3. Fornisci informazioni sull'abbonamento a Cloud Volumes Service:
   a. Inserire il nome dell'ambiente di lavoro che si desidera utilizzare.
   b. Copiare/incollare la chiave privata JSON scaricata nei passaggi precedenti.
   c. Selezionare il nome del progetto Google Cloud.
   d. Fare clic su **Aggiungi**.



Risultato

Cloud Manager visualizza il tuo ambiente di lavoro Cloud Volumes Service per Google Cloud.

Se per questo abbonamento esistono già volumi cloud, i volumi vengono visualizzati nel nuovo ambiente di lavoro, come mostrato nella schermata. Puoi aggiungere altri volumi cloud da Cloud Manager.

Se non esistono volumi cloud per questo abbonamento, creali ora.

Quali sono le prossime novità?

"Inizia a creare e gestire i volumi".

Crea e gestisci volumi per Cloud Volumes Service per Google Cloud

Cloud Manager ti consente di creare volumi cloud in base al tuo "Cloud Volumes Service per Google Cloud" iscrizione. Puoi anche modificare alcuni attributi di un volume, ottenere i relativi comandi di montaggio, creare copie Snapshot ed eliminare volumi cloud.

Creare volumi cloud

È possibile creare volumi NFS o SMB in un account Cloud Volumes Service per Google Cloud nuovo o esistente. I volumi cloud attualmente supportano NFSv3 e NFSv4.1 per client Linux e UNIX e SMB 3.x per client Windows.

Prima di iniziare

- Se si desidera utilizzare SMB in GCP, è necessario aver configurato DNS e Active Directory.
- Quando si intende creare un volume SMB, è necessario disporre di un server Windows Active Directory a cui connettersi. Queste informazioni verranno inserite durante la creazione del volume. Inoltre, assicurarsi che l'utente Admin sia in grado di creare un account macchina nel percorso dell'unità organizzativa (OU) specificato.

Fasi

1. Selezionare l'ambiente di lavoro e fare clic su **Add New Volume** (Aggiungi nuovo volume).
2. Nella pagina Details & Location (Dettagli e posizione), immettere i dettagli relativi al volume:
   a. Immettere un nome per il volume.
   b. Specificare una dimensione compresa tra 1 TIB (1024 GiB) e 100 TIB.

      "Scopri di più sulla capacità allocata".

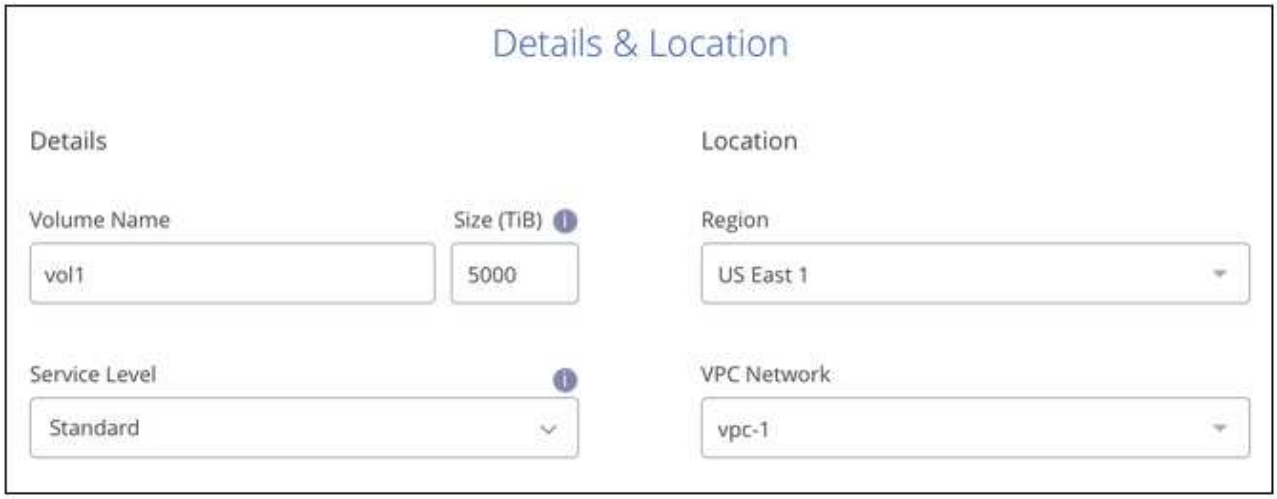
   c. Specificare un livello di servizio: Standard, Premium o Extreme.

      "Scopri di più sui livelli di servizio".

d. Selezionare l'area di Google Cloud.

e. Selezionare la rete VPC da cui sarà possibile accedere al volume. Tenere presente che non è possibile modificare o modificare il VPC dopo la creazione del volume.

f. Fare clic su **continua**.



3. Nella pagina Protocol (protocollo), selezionare NFS o SMB, quindi definire i dettagli. Le voci richieste per NFS e SMB sono illustrate in sezioni separate di seguito.

4. Per NFS:

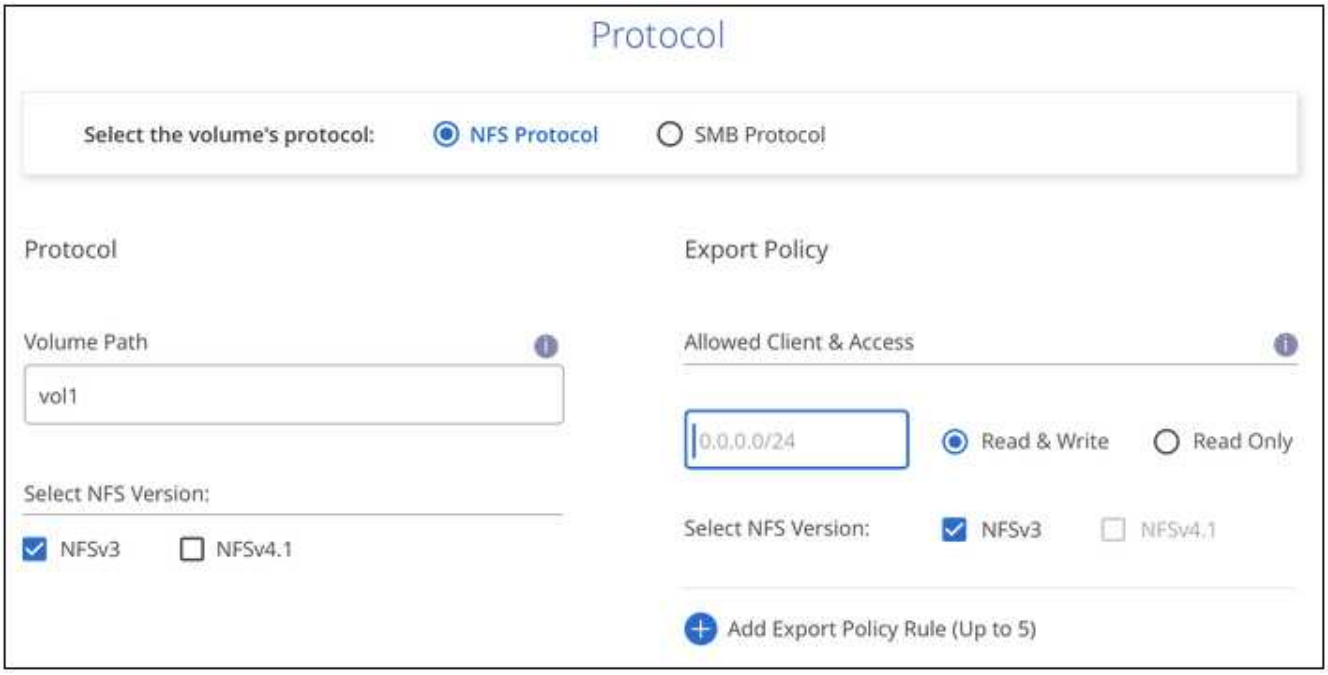
a. Nel campo Volume Path (percorso volume), specificare il nome dell'esportazione del volume che verrà visualizzato quando si monta il volume.

b. Selezionare NFSv3, NFSv4.1 o entrambi a seconda delle proprie esigenze.

c. Facoltativamente, è possibile creare una policy di esportazione per identificare i client che possono accedere al volume. Specificare:

- Client consentiti utilizzando un indirizzo IP o CIDR (Classless Inter-Domain Routing).
- Diritti di accesso in lettura e scrittura o in sola lettura.
- Protocollo di accesso (o protocolli se il volume consente l'accesso NFSv3 e NFSv4.1) utilizzato per gli utenti.
- Fare clic su **+ Add Export Policy Rule** (Aggiungi regola policy di esportazione) se si desidera definire ulteriori regole dei criteri di esportazione.

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



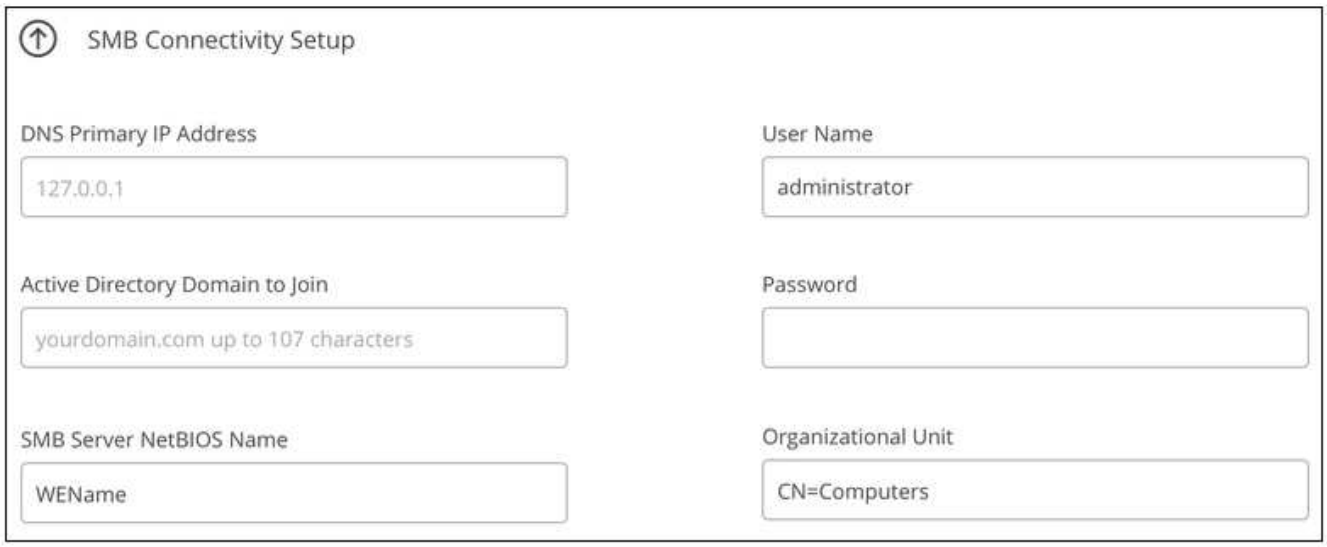
5. Per PMI:

   a. Nel campo Volume Path (percorso volume), specificare il nome dell'esportazione del volume che verrà visualizzato quando si monta il volume e fare clic su **Continue** (continua).

   b. Se Active Directory è stato configurato, viene visualizzata la configurazione. Se si tratta del primo volume da configurare e non è stata configurata alcuna Active Directory, è possibile attivare la crittografia della sessione SMB nella pagina SMB Connectivity Setup:

Campo	Descrizione
Indirizzo IP primario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server SMB. Utilizzare una virgola per separare gli indirizzi IP quando si fa riferimento a più server, ad esempio 172.31.25.223, 172.31.2.74.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server SMB si unisca.
Nome NetBIOS del server SMB	Un nome NetBIOS per il server SMB che verrà creato.
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.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server SMB. L'impostazione predefinita è CN=computer per le connessioni al proprio server Windows Active Directory.

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



6. Fare clic su **continua**.
7. Se si desidera creare il volume in base a uno snapshot di un volume esistente, selezionare lo snapshot dall'elenco a discesa Snapshot Name (Nome snapshot). In caso contrario, fare clic su **continua**.
8. Nella pagina Snapshot Policy, è possibile abilitare Cloud Volumes Service per creare copie Snapshot dei volumi in base a una pianificazione. È possibile eseguire questa operazione spostando il selettore verso destra oppure modificare il volume in un secondo momento per definire il criterio di snapshot.

   Vedere "Creazione di un criterio di snapshot" per ulteriori informazioni sulla funzionalità di snapshot.

9. Fare clic su **Add Volume** (Aggiungi volume).

Il nuovo volume viene aggiunto all'ambiente di lavoro.

Continuare con "Montaggio del volume cloud".

Montare volumi cloud

Accedi alle istruzioni di montaggio da Cloud Manager per montare il volume su un host.

Nota: utilizzare il protocollo/dialetto evidenziato supportato dal client.

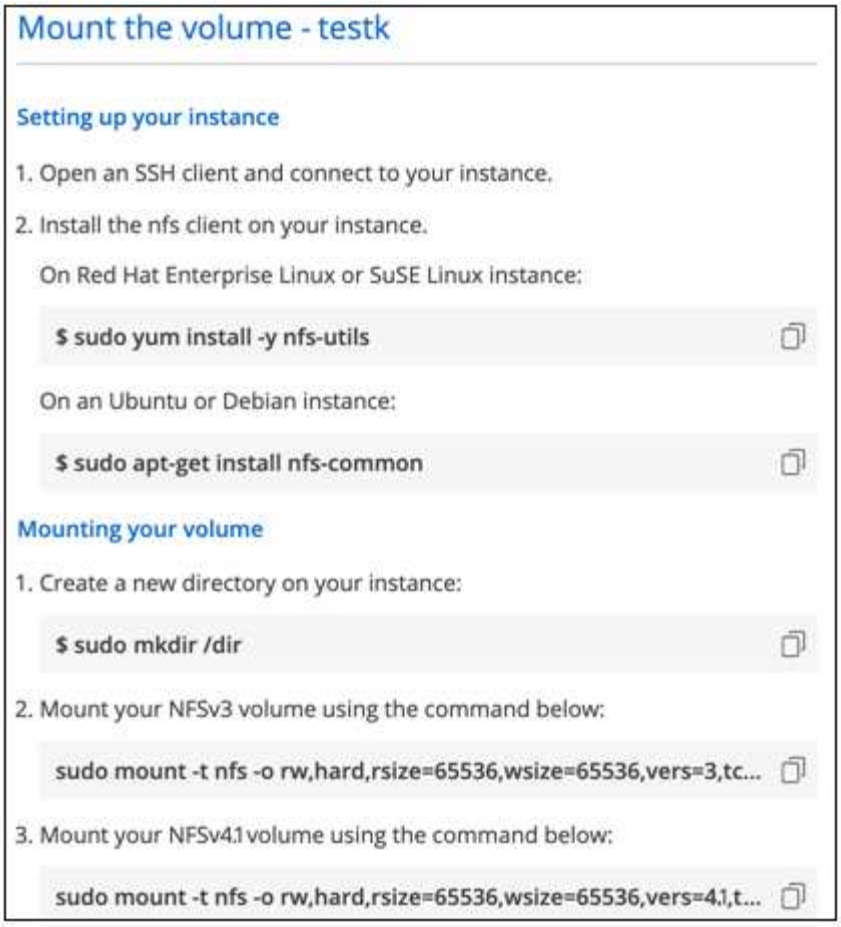
Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **montare il volume**.

   I volumi NFS e SMB visualizzano le istruzioni di montaggio per quel protocollo.

3. Passare il mouse sui comandi e copiarli negli Appunti per semplificare questo processo. Basta aggiungere la directory di destinazione/punto di montaggio alla fine del comando.

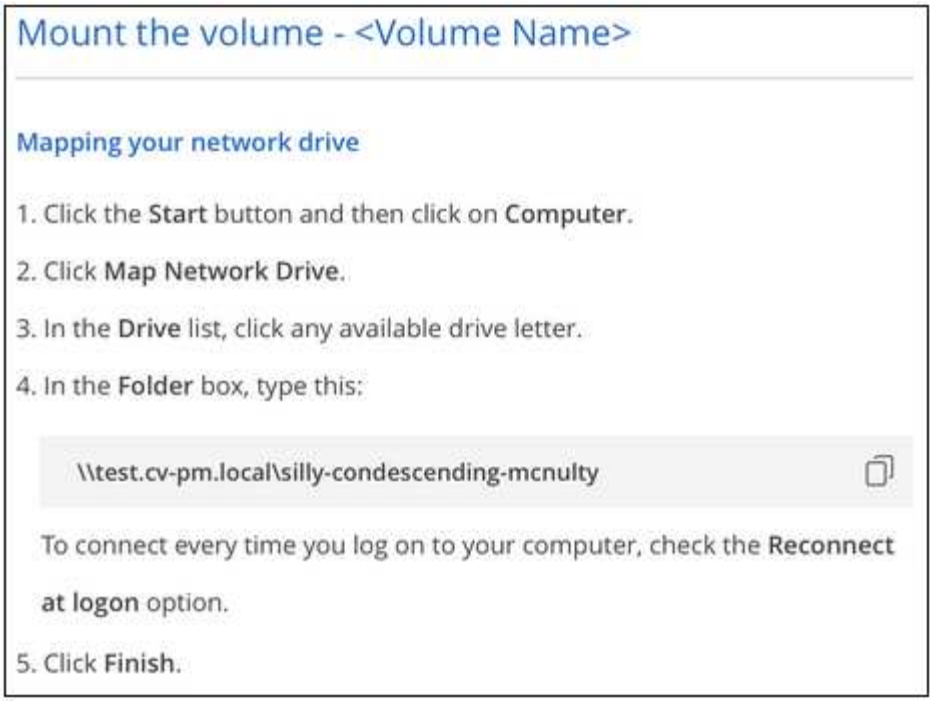
   Esempio NFS:



La dimensione i/o massima definita da `rsize` e. `wsize` options è 1048576, tuttavia 65536 è l'impostazione predefinita consigliata per la maggior parte dei casi di utilizzo.

Si noti che i client Linux imposteranno per impostazione predefinita NFSv4.1, a meno che la versione non sia specificata con `vers=<nfs_version>` opzione.

Esempio SMB:



4. Mappare l'unità di rete seguendo le istruzioni di montaggio dell'istanza.

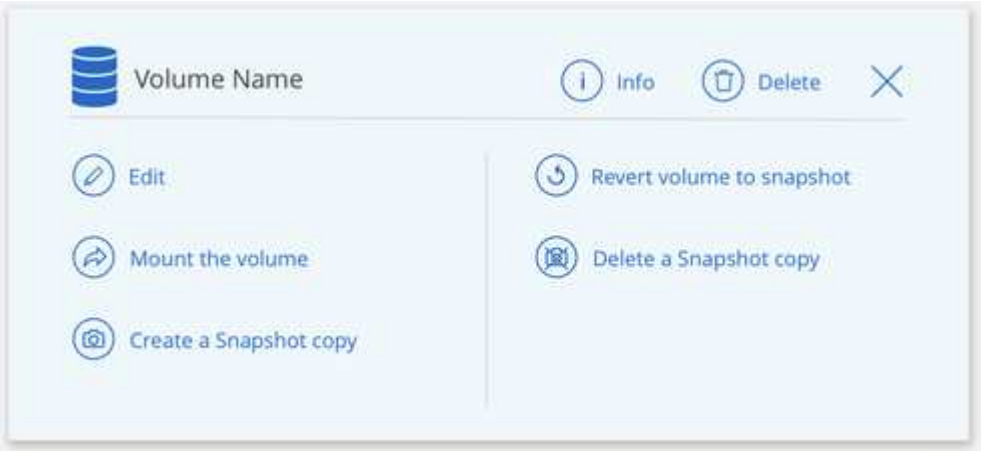
   Dopo aver completato i passaggi delle istruzioni di montaggio, il volume cloud è stato montato correttamente sull'istanza GCP.

Gestire i volumi esistenti

Puoi gestire i volumi esistenti in base alle tue esigenze di storage. È possibile visualizzare, modificare, ripristinare ed eliminare i volumi.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume.



3. Gestisci i tuoi volumi:

Attività	Azione
Consente di visualizzare informazioni su un volume	Fare clic su **Info**.
Modifica di un volume (inclusa la policy di snapshot)	a. Fare clic su **Edit** (Modifica). b. Modificare le proprietà del volume, quindi fare clic su **Update** (Aggiorna).
Ottieni il comando di montaggio NFS o SMB	a. Fare clic su **montare il volume**. b. Fare clic su **Copy** (Copia) per copiare i comandi.
Crea una copia Snapshot on-demand	a. Fare clic su **Crea una copia Snapshot**. b. Modificare il nome, se necessario, quindi fare clic su **Crea**.
Sostituire il volume con il contenuto di una copia Snapshot	a. Fare clic su **Ripristina volume in snapshot**. b. Selezionare una copia Snapshot e fare clic su **Restore** (Ripristina).
Eliminare una copia Snapshot	a. Fare clic su **Elimina una copia Snapshot**. b. Selezionare l'istantanea e fare clic su **Delete** (Elimina). c. Fare nuovamente clic su **Delete** quando viene richiesto di confermare.
Eliminare un volume	a. Smontare il volume da tutti i client: ◦ Sui client Linux, utilizzare `umount` comando. ◦ Sui client Windows, fare clic su **Disconnetti unità di rete**. b. Selezionare un volume, quindi fare clic su **Delete** (Elimina). c. Fare nuovamente clic su **Delete** per confermare.

Rimuovere Cloud Volumes Service da Cloud Manager

Puoi rimuovere un abbonamento a Cloud Volumes Service per Google Cloud e tutti i volumi esistenti da Cloud Manager. I volumi non vengono cancellati, ma vengono semplicemente rimossi dall'interfaccia di Cloud Manager.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic su Nella parte superiore della pagina e fare clic su **Rimuovi Cloud Volumes Service**.
3. Nella finestra di dialogo di conferma, fare clic su **Rimuovi**.

Gestire la configurazione di Active Directory

Se si modificano i server DNS o il dominio Active Directory, è necessario modificare il server SMB in Cloud Volumes Services in modo che possa continuare a servire lo storage ai client.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic su Nella parte superiore della pagina e fare clic su **Gestisci Active Directory**. Se non è configurata alcuna Active Directory, è possibile aggiungerne una ora. Se ne è stata configurata una, è possibile modificare o eliminare le impostazioni utilizzando pulsante.
3. Specificare le impostazioni per il server SMB:

Campo	Descrizione
Indirizzo IP primario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server SMB. Utilizzare una virgola per separare gli indirizzi IP quando si fa riferimento a più server, ad esempio 172.31.25.223, 172.31.2.74.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server SMB si unisca.
Nome NetBIOS del server SMB	Un nome NetBIOS per il server SMB che verrà creato.
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.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server SMB. L'impostazione predefinita è CN=computer per le connessioni al proprio server Windows Active Directory.

4. Fare clic su **Save** (Salva) per salvare le impostazioni.

Gestire le snapshot dei volumi cloud

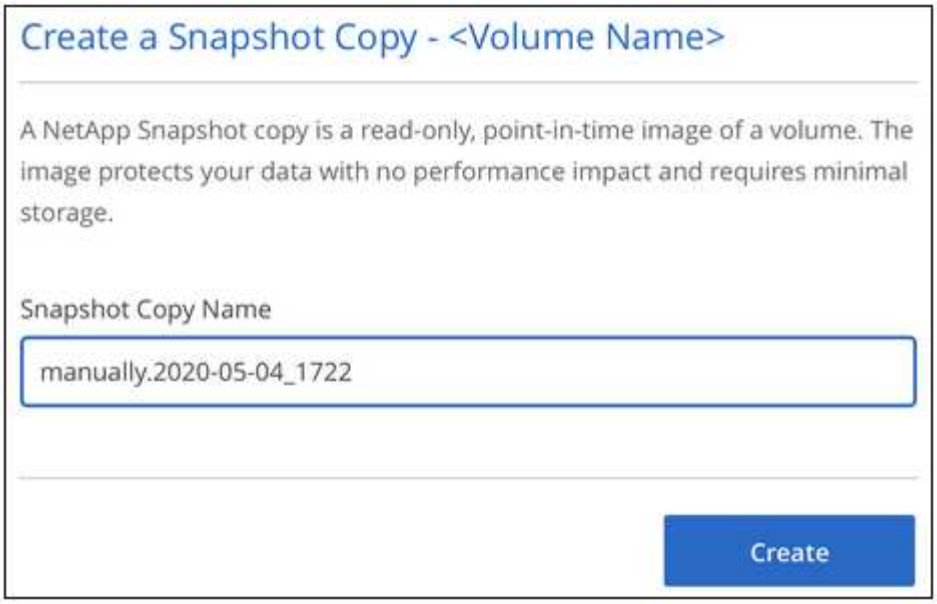
È possibile creare un criterio di snapshot per ciascun volume in modo da poter ripristinare o ripristinare l'intero contenuto di un volume da un momento precedente. È inoltre possibile creare un'istantanea on-demand di un volume cloud quando necessario.

Crea un'istantanea on-demand

È possibile creare uno snapshot on-demand di un volume cloud se si desidera creare uno snapshot con lo stato corrente del volume.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Create a snapshot copy** (Crea una copia snapshot).
3. Immettere un nome per lo snapshot oppure utilizzare il nome generato automaticamente e fare clic su **Create** (Crea).



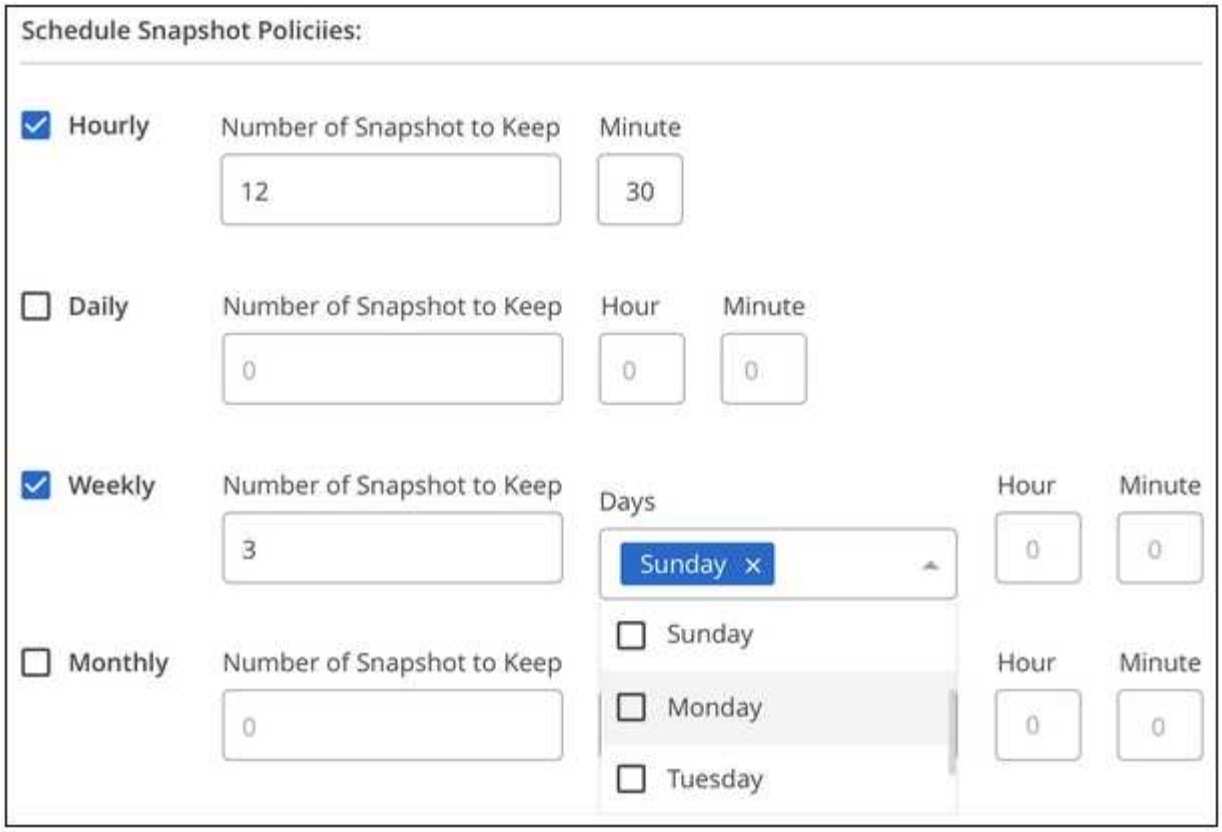
L'istantanea viene creata.

Creare o modificare un criterio di snapshot

È possibile creare o modificare una policy di snapshot in base alle necessità per un volume cloud. La policy di snapshot viene definita dalla scheda *Snapshot Policy* durante la creazione di un volume o la modifica di un volume.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Edit** (Modifica).
3. Dalla scheda *Snapshot Policy*, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso destra.
4. Definire la pianificazione delle snapshot:
   a. Selezionare la frequenza: **Orario**, **giornaliero**, **settimanale** o **mensile**
   b. Selezionare il numero di snapshot che si desidera conservare.
   c. Selezionare il giorno, l'ora e il minuto in cui eseguire l'istantanea.



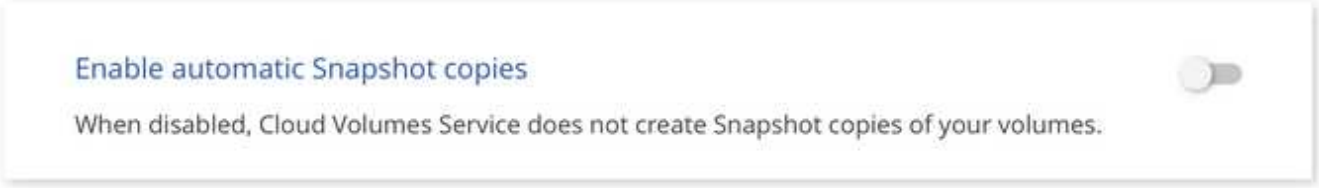
5. Fare clic su **Add volume** (Aggiungi volume) o **Update volume** (Aggiorna volume) per salvare le impostazioni dei criteri.

Disattiva un criterio di snapshot

È possibile disattivare un criterio di snapshot per impedire la creazione di snapshot per un breve periodo di tempo, mantenendo le impostazioni del criterio di snapshot.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Edit** (Modifica).
3. Dalla scheda *Snapshot Policy*, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso sinistra.



4. Fare clic su **Update volume** (Aggiorna volume).

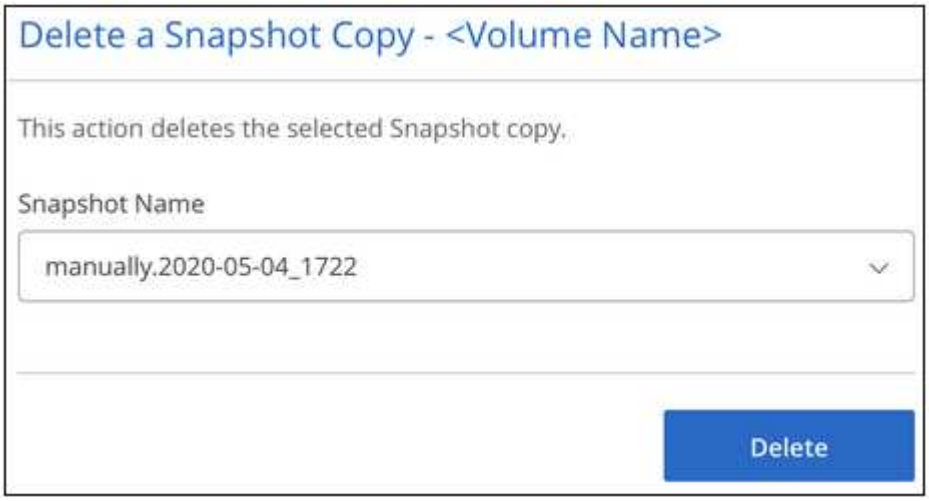
Se si desidera riattivare il criterio di snapshot, spostare il dispositivo di scorrimento Enable Snapshot (attiva snapshot) verso destra e fare clic su **Update volume** (Aggiorna volume).

Eliminare uno snapshot

È possibile eliminare uno snapshot se non è più necessario.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Delete a Snapshot copy** (Elimina una copia Snapshot).
3. Selezionare l'istantanea dall'elenco a discesa e fare clic su **Delete** (Elimina).



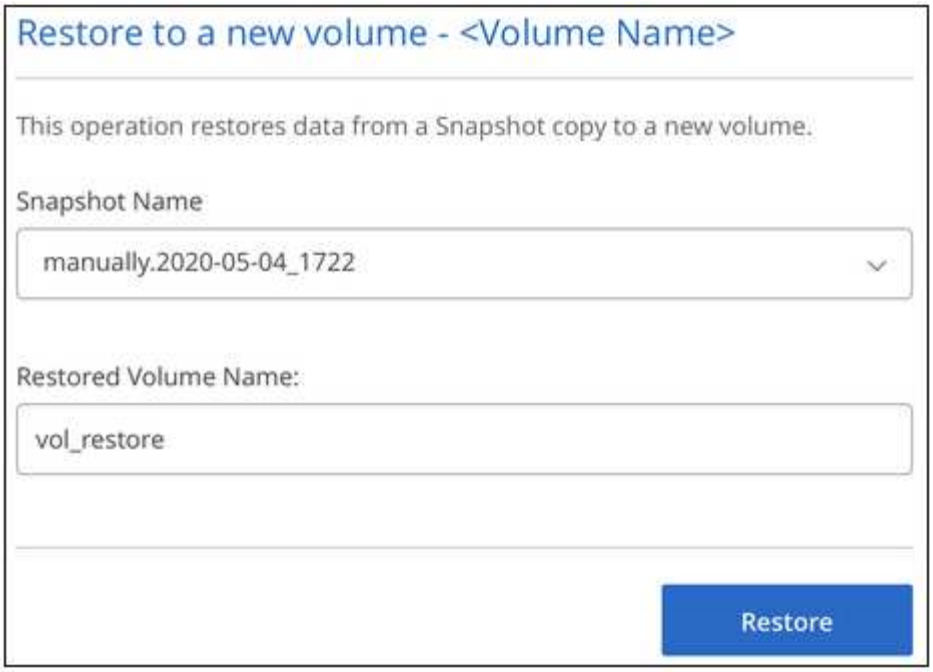
4. Nella finestra di dialogo di conferma, fare clic su **Delete** (Elimina).

Ripristinare uno snapshot in un nuovo volume

Se necessario, è possibile ripristinare uno snapshot in un nuovo volume.

Fasi

1. Aprire l'ambiente di lavoro.
2. Passare il mouse sul volume e fare clic su **Restore to a new volume** (Ripristina un nuovo volume).
3. Selezionare l'istantanea che si desidera utilizzare per creare il nuovo volume dall'elenco a discesa.
4. Immettere un nome per il nuovo volume e fare clic su **Restore** (Ripristina).



Il volume viene creato nell'ambiente di lavoro.

5. Se è necessario modificare uno degli attributi del volume, ad esempio il percorso del volume o il livello di servizio:
   a. Passare il mouse sul volume e fare clic su **Edit** (Modifica).
   b. Apportare le modifiche e fare clic su **Update volume** (Aggiorna volume).

Al termine

Continuare con "Montaggio del volume cloud".

Gestire i cluster ONTAP

Alla scoperta 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. Il rilevamento di un cluster ONTAP consente di eseguire il provisioning dello storage, replicare i dati, eseguire il backup dei dati e tierare i dati cold da un cluster on-premise al cloud.

Di cosa hai bisogno

- Un connettore installato in un cloud provider o on-premise.

  Se si desidera eseguire il tiering dei dati cold nel cloud, è necessario esaminare i requisiti per il connettore in base alla posizione in cui si prevede di eseguire il tiering dei dati cold.

  - "Scopri di più sui connettori"
  - "Passaggio da un connettore all'altro"
  - "Scopri di più sul Cloud Tiering"

- L'indirizzo IP di gestione del cluster e la password dell'account utente amministratore per aggiungere il cluster a Cloud Manager.

  Cloud Manager rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:

  - L'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443.

    Se il connettore si trova nel cloud, 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.

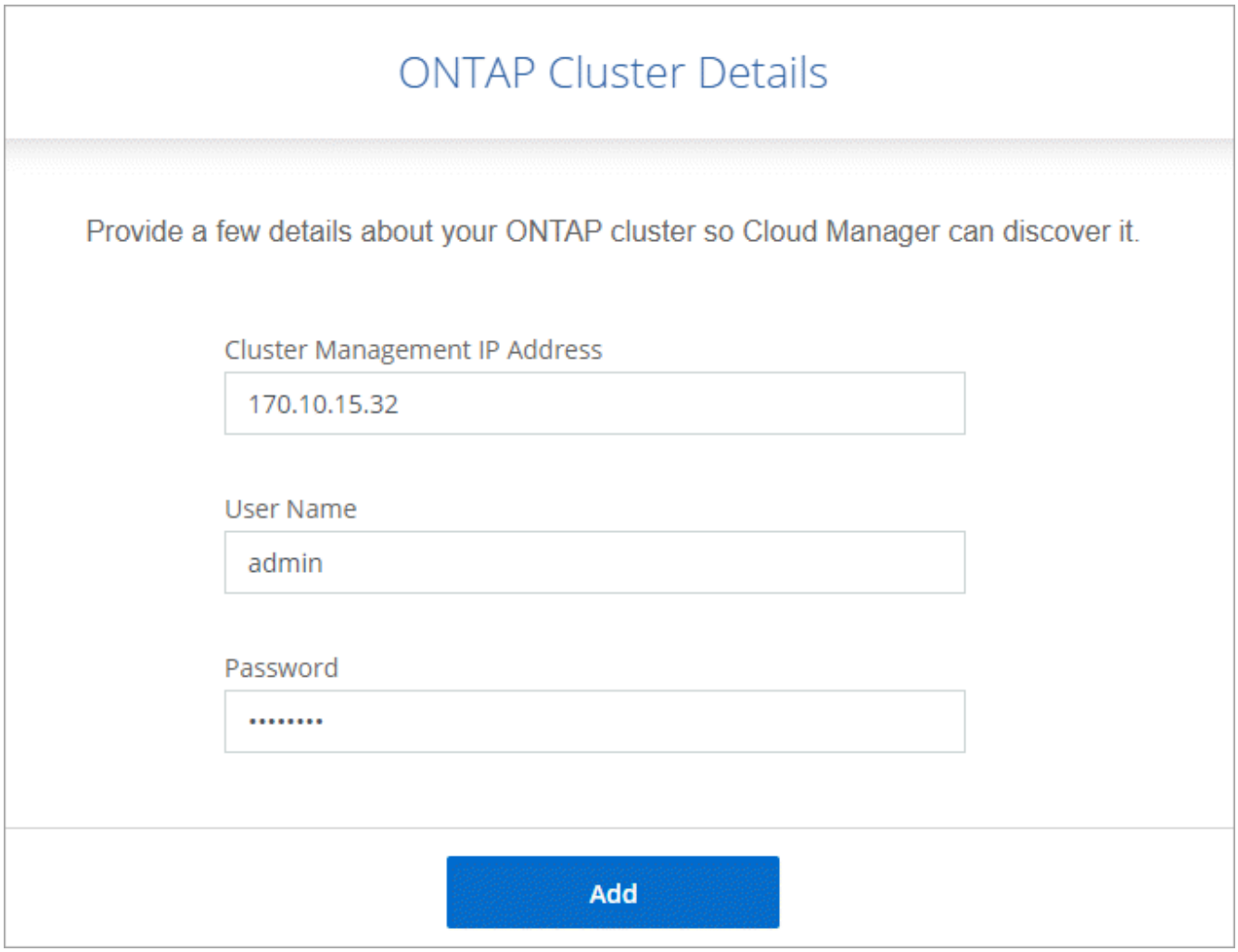
    Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questo criterio predefinito è stato modificato o se è stato creato un criterio firewall personalizzato, è necessario associare il protocollo HTTPS a tale criterio e abilitare l'accesso dall'host del connettore.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro** e selezionare **ONTAP on-premise**.
2. Se richiesto, creare un connettore.

   Per ulteriori informazioni, fare riferimento ai collegamenti riportati sopra.

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



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. Ora puoi creare volumi, replicare i dati da e verso il cluster, configurare il tiering dei dati nel cloud, eseguire il backup dei volumi nel cloud e avviare System Manager per eseguire attività avanzate.

Gestione dello storage per cluster ONTAP

Dopo aver scoperto il cluster ONTAP da Cloud Manager, puoi aprire l'ambiente di lavoro per eseguire il provisioning e la gestione dello storage.

Creazione di volumi per cluster ONTAP

Cloud Manager consente di eseguire il provisioning di volumi NFS, CIFS e iSCSI su cluster ONTAP.

Prima di iniziare

I protocolli dati devono essere impostati sul cluster utilizzando System Manager o CLI.

A proposito di questa attività

È possibile creare volumi su aggregati esistenti. Non puoi 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.
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.
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.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, Cloud Manager crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, selezionarlo, fare clic su Target IQN (IQN di destinazione), quindi utilizzare IQN per connettersi al LUN dagli host.
Profilo di utilizzo	I profili di utilizzo definiscono le funzionalità di efficienza dello storage NetApp abilitate per un volume.

Replica dei dati

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.

"Fai clic qui per ulteriori dettagli".

Backup dei dati

Puoi eseguire il backup dei dati dal tuo sistema ONTAP on-premise allo storage a oggetti a basso costo nel cloud utilizzando il servizio di backup su cloud di Cloud Manager. Questo servizio offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.

"Fai clic qui per ulteriori dettagli".

Tiering dei dati nel cloud

Estendi il tuo data center al cloud attraverso il tiering automatico dei dati inattivi dai cluster ONTAP allo storage a oggetti.

"Fai clic qui per ulteriori dettagli".

Backup nel cloud

Scopri di più sul backup nel cloud

Backup su cloud è un servizio add-on per cluster Cloud Volumes ONTAP e ONTAP on-premise che offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati cloud. I backup vengono memorizzati in un archivio di oggetti nel tuo account cloud, indipendentemente dalle copie Snapshot del volume utilizzate per il ripristino o il cloning a breve termine.

Il backup nel cloud è basato su "Cloud Backup Service".

> È necessario utilizzare Cloud Manager per tutte le operazioni di backup e ripristino. Qualsiasi azione intrapresa direttamente da ONTAP o dal tuo cloud provider comporta una configurazione non supportata.

Caratteristiche

- Backup di copie indipendenti dei volumi di dati su storage a oggetti a basso costo nel cloud.
- I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.
- Backup dal cloud al cloud e dai sistemi ONTAP on-premise al cloud.
- Supporto di un massimo di 1,019 backup di un singolo volume.
- Ripristinare i dati da un momento specifico.
- Ripristinare i dati su un volume del sistema di origine o su un sistema diverso.

Ambienti di lavoro supportati e provider di storage a oggetti

Il backup su cloud è supportato con i seguenti tipi di ambienti di lavoro:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- Cluster ONTAP on-premise

Costo

Backup su cloud è disponibile in due opzioni di prezzo: Bring Your Own License (BYOL) e Pay As You Go (PAYGO).

Per BYOL pagherai NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 6 mesi, e per una capacità di backup massima, ad esempio 10 GB (prima dell'efficienza dello storage), e dovrai pagare al tuo cloud provider per i costi dello storage a oggetti. Riceverai un numero di serie che inserisci nella pagina delle licenze di Cloud Manager per attivare il servizio. Una volta raggiunto il limite, è necessario rinnovare la licenza. Vedere "Aggiunta e aggiornamento della licenza BYOL di backup". La licenza BYOL di backup si applica a tutti i sistemi Cloud Volumes ONTAP associati al "Account Cloud Central".

Per PAYGO dovrai pagare il tuo cloud provider per i costi dello storage a oggetti e NetApp per i costi delle licenze di backup. I costi di licenza si basano sulla capacità utilizzata (prima dell'efficienza dello storage):

- AWS: "Vai all'offerta Cloud Manager Marketplace per i dettagli sui prezzi".
- Azure: "Vai all'offerta Cloud Manager Marketplace per i dettagli sui prezzi".

Versione di prova gratuita

È disponibile una versione di prova gratuita di 30 giorni. Quando utilizzi la versione di prova, ti viene notificato il numero di giorni di prova gratuiti che rimangono. Al termine della prova gratuita, i backup non vengono più creati. Per continuare a utilizzare il servizio, è necessario sottoscrivere il servizio o acquistare una licenza.

I backup non vengono cancellati quando il servizio viene disattivato. Il tuo cloud provider continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup, a meno che non elimini i backup.

Come funziona il backup nel cloud

Quando abiliti il backup nel cloud su un sistema Cloud Volumes ONTAP o ONTAP on-premise, il servizio esegue un backup completo dei tuoi dati. Le snapshot dei volumi non sono incluse nell'immagine di backup. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e dei nuovi blocchi.

Dove risiedono i backup

Le copie di backup vengono memorizzate in un bucket S3 o in un container Azure Blob creato da Cloud Manager nel tuo account cloud. Per i sistemi Cloud Volumes ONTAP, l'archivio di oggetti viene creato nella stessa regione in cui si trova il sistema Cloud Volumes ONTAP. Per i sistemi ONTAP on-premise, l'utente identifica la regione al momento dell'attivazione del servizio.

Esiste un archivio di oggetti per sistema Cloud Volumes ONTAP o ONTAP on-premise. Cloud Manager nomina l'archivio di oggetti come segue: netapp-backup-*clusteruid*

Assicurarsi di non eliminare questo archivio di oggetti.

Note:

- In AWS, Cloud Manager abilita "Funzione di accesso pubblico a blocchi Amazon S3" Sul bucket S3.
- In Azure, Cloud Manager utilizza un gruppo di risorse nuovo o esistente con un account di storage per il container Blob.

Classi di storage S3 supportate

In Amazon S3, i backup iniziano nella classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.

Livelli di accesso supportati da Azure Blob

In Azure, ogni backup è associato al *cold* Tier di accesso.

Le impostazioni di backup sono a livello di sistema

Quando abiliti Backup su cloud, tutti i volumi identificati sul sistema vengono sottoposti a backup nel cloud.

La pianificazione e il numero di backup da conservare sono definiti a livello di sistema. Le impostazioni di backup influiscono su tutti i volumi del sistema.

La pianificazione è giornaliera, settimanale, mensile o combinata

È possibile scegliere backup giornalieri, settimanali o mensili di tutti i volumi. È inoltre possibile selezionare una delle policy definite dal sistema che fornisce backup e conservazione per 3 mesi, 1 anno e 7 anni. Queste policy sono:

Nome policy	Backup per intervallo…			Max. Backup
	Giornaliero	Settimanale	Mensile	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Una volta raggiunto il numero massimo di backup per una categoria o intervallo, i backup meno recenti vengono rimossi in modo da avere sempre i backup più aggiornati.

Si noti che il periodo di conservazione per i backup dei volumi di protezione dei dati è lo stesso definito nella relazione SnapMirror di origine. È possibile modificare questa impostazione utilizzando l'API.

I backup vengono eseguiti a mezzanotte

- I backup giornalieri iniziano ogni giorno dopo la mezzanotte.
- I backup settimanali iniziano subito dopo la mezzanotte di domenica mattina.
- I backup mensili iniziano appena dopo la mezzanotte del primo mese.

Al momento, non è possibile pianificare le operazioni di backup in un orario specificato dall'utente.

Le copie di backup sono associate al tuo account Cloud Central

Le copie di backup sono associate a "Account Cloud Central" In cui risiede Cloud Manager.

Se si dispone di più sistemi Cloud Manager nello stesso account Cloud Central, ciascun sistema Cloud Manager visualizzerà lo stesso elenco di backup. Sono inclusi i backup associati a Cloud Volumes ONTAP e alle istanze di ONTAP on-premise di altri sistemi Cloud Manager.

Considerazioni sulla licenza BYOL

Quando si utilizza una licenza BYOL di Backup su cloud, Cloud Manager avvisa l'utente quando i backup si stanno avvicinando al limite di capacità o si stanno avvicinando alla data di scadenza della licenza. Ricevi queste notifiche:

- quando i backup hanno raggiunto il 80% della capacità concessa in licenza, e ancora una volta quando hai raggiunto il limite
- 30 giorni prima della scadenza di una licenza e di nuovo alla scadenza della stessa

Utilizza l'icona della chat in basso a destra dell'interfaccia di Cloud Manager per rinnovare la licenza quando ricevi queste notifiche.

Due cose possono accadere alla scadenza della licenza:

- Se l'account utilizzato per i sistemi ONTAP dispone di un account Marketplace, il servizio di backup continua a funzionare, ma si passa a un modello di licenza PAYGO. Il tuo cloud provider addebita i costi

dello storage a oggetti e NetApp i costi di licenza per il backup, per la capacità utilizzata dai backup.

- Se l'account utilizzato per i sistemi ONTAP non dispone di un account Marketplace, il servizio di backup continua a essere in esecuzione, ma si continuerà a ricevere il messaggio di scadenza.

Una volta rinnovato l'abbonamento BYOL, Cloud Manager ottiene automaticamente la nuova licenza da NetApp e la installa. 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 "Aggiunta e aggiornamento della licenza BYOL di backup".

I sistemi trasferiti a UNA licenza PAYGO vengono restituiti automaticamente alla licenza BYOL. Inoltre, i sistemi in esecuzione senza licenza non riceveranno più il messaggio di avviso e verranno addebitati i backup eseguiti mentre la licenza è scaduta.

Volumi supportati

Backup su cloud supporta volumi di lettura/scrittura e volumi di protezione dei dati (DP).

I volumi FlexGroup non sono attualmente supportati.

Limitazioni

- Lo storage WORM (SnapLock) non è supportato su un sistema Cloud Volumes ONTAP o on-premise quando è attivato il backup su cloud.
- Restrizioni relative al backup su cloud quando si eseguono backup da sistemi ONTAP on-premise:
  - Il cluster on-premise deve eseguire ONTAP 9.7P5 o versione successiva.
  - Cloud Manager deve essere implementato su Azure. Non è disponibile alcun supporto per le implementazioni di Cloud Manager on-premise.
  - Il percorso di destinazione dei backup è solo lo storage a oggetti su Azure.
  - I backup possono essere ripristinati solo sui sistemi Cloud Volumes ONTAP implementati su Azure. Non è possibile ripristinare un backup su un sistema ONTAP on-premise o su un sistema Cloud Volumes ONTAP che utilizza un provider di cloud diverso.
- Quando si esegue il backup dei volumi di protezione dei dati (DP), la regola definita per il criterio SnapMirror sul volume di origine deve utilizzare un'etichetta che corrisponda ai nomi dei criteri di backup su cloud consentiti di **giornaliero**, **settimanale** o **mensile**. In caso contrario, il backup non verrà eseguito correttamente per quel volume DP.
- In Azure, se abiliti il backup nel cloud quando viene implementato Cloud Volumes ONTAP, il Cloud Manager crea il gruppo di risorse per te e non puoi modificarlo. Se si desidera scegliere il proprio gruppo di risorse quando si attiva il backup nel cloud, **disattivare** il backup nel cloud durante l'implementazione di Cloud Volumes ONTAP, quindi attivare il backup nel cloud e scegliere il gruppo di risorse dalla pagina Backup nelle impostazioni del cloud.
- Quando si esegue il backup dei volumi dai sistemi Cloud Volumes ONTAP, il backup dei volumi creati al di fuori di Cloud Manager non viene eseguito automaticamente.

  Ad esempio, se si crea un volume dall'interfaccia CLI di ONTAP, dall'API di ONTAP o da Gestore di sistema, il backup del volume non verrà eseguito automaticamente.

  Se si desidera eseguire il backup di questi volumi, è necessario disattivare Backup nel cloud e attivarlo nuovamente.

Inizia subito

Backup dei dati su Amazon S3

Completa alcuni passaggi per iniziare a eseguire il backup dei dati da Cloud Volumes ONTAP a Amazon S3.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Verificare il supporto per la configurazione

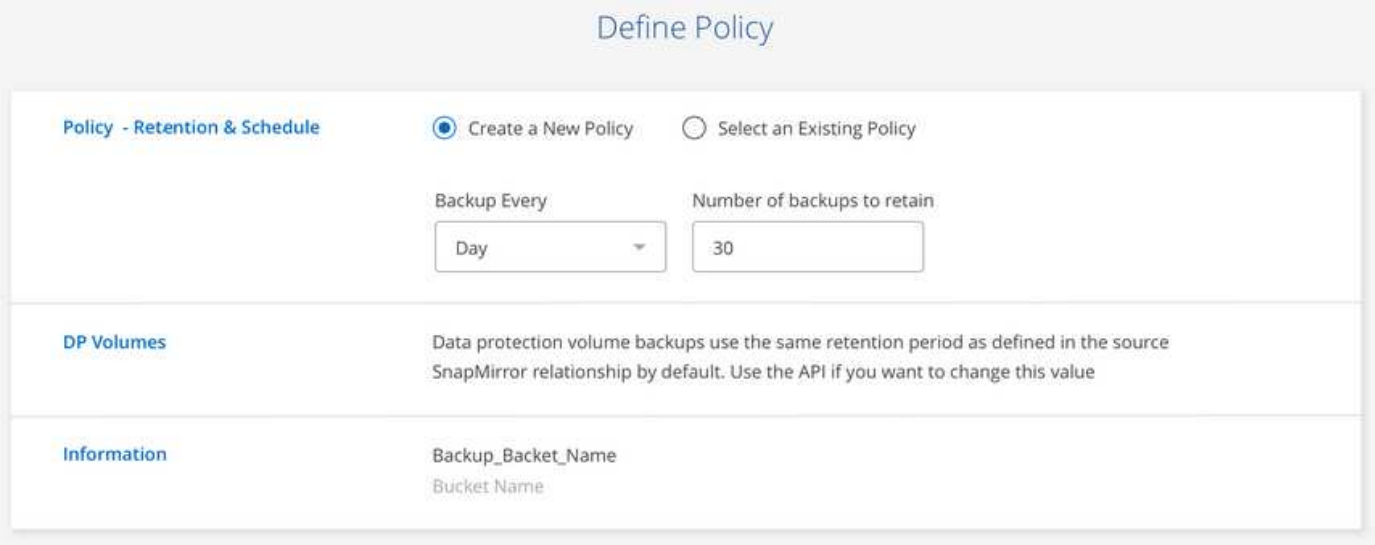
- Cloud Volumes ONTAP 9.6 o versione successiva è in esecuzione in AWS.
- Si è abbonati a. "Offerta di backup Cloud Manager Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup su cloud di NetApp.
- Il ruolo IAM che fornisce le autorizzazioni a Cloud Manager include le autorizzazioni S3 dell'ultima versione "Policy di Cloud Manager".

2 Abilita Backup su cloud sul tuo sistema nuovo o esistente

- Nuovi sistemi: Il backup su cloud è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.
- Sistemi esistenti: Selezionare l'ambiente di lavoro e fare clic su **Activate** (attiva) accanto al servizio Backup to Cloud nel pannello di destra, quindi seguire la procedura di installazione guidata.

3 Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca ulteriori opzioni. È inoltre possibile modificare il numero di copie di backup da conservare.

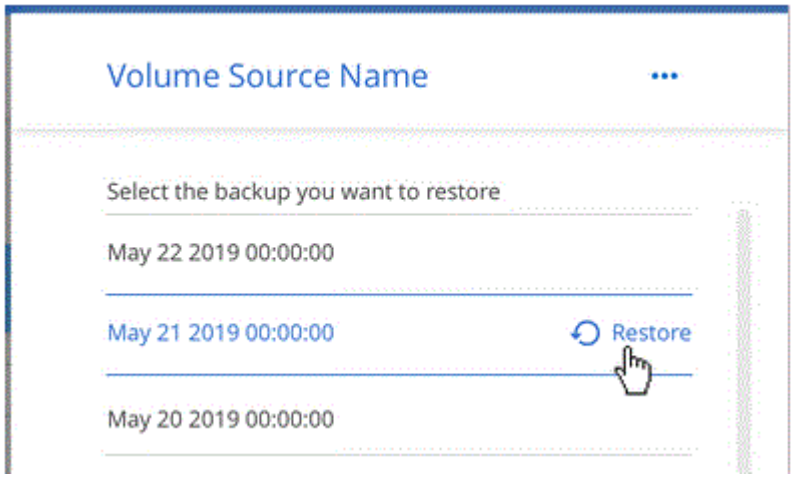


Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi).

Ripristinare i dati, se necessario

Dall'elenco di backup, selezionare un volume, selezionare un backup, quindi ripristinare i dati dal backup a un nuovo volume.



Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi in S3.

Versioni di ONTAP supportate

Cloud Volumes ONTAP 9.6 e versioni successive.

Regioni AWS supportate

Il backup su cloud è supportato in tutte le regioni AWS "Dove è supportato Cloud Volumes ONTAP".

Requisiti di licenza

Per le licenze PAYGO di backup su cloud, è disponibile un abbonamento a Cloud Manager nel marketplace AWS che consente le implementazioni di Cloud Volumes ONTAP 9.6 e versioni successive (PAYGO) e di backup su cloud. È necessario "Iscriviti a questo abbonamento a Cloud Manager" Prima di attivare il backup nel cloud. La fatturazione per il backup su cloud viene effettuata tramite questo abbonamento.

Per le licenze BYOL di Backup to Cloud, non è necessario un abbonamento AWS Backup to Cloud. È necessario il numero di serie di NetApp che consenta di utilizzare il servizio per la durata e la capacità della licenza. Vedere "Aggiunta e aggiornamento della licenza BYOL di backup".

Inoltre, è necessario disporre di un abbonamento AWS per lo spazio di storage in cui verranno collocati i backup.

Autorizzazioni AWS richieste

Il ruolo IAM che fornisce le autorizzazioni a Cloud Manager deve includere le autorizzazioni S3 dell'ultima versione "Policy di Cloud Manager".

Di seguito sono riportate le autorizzazioni specifiche della policy:

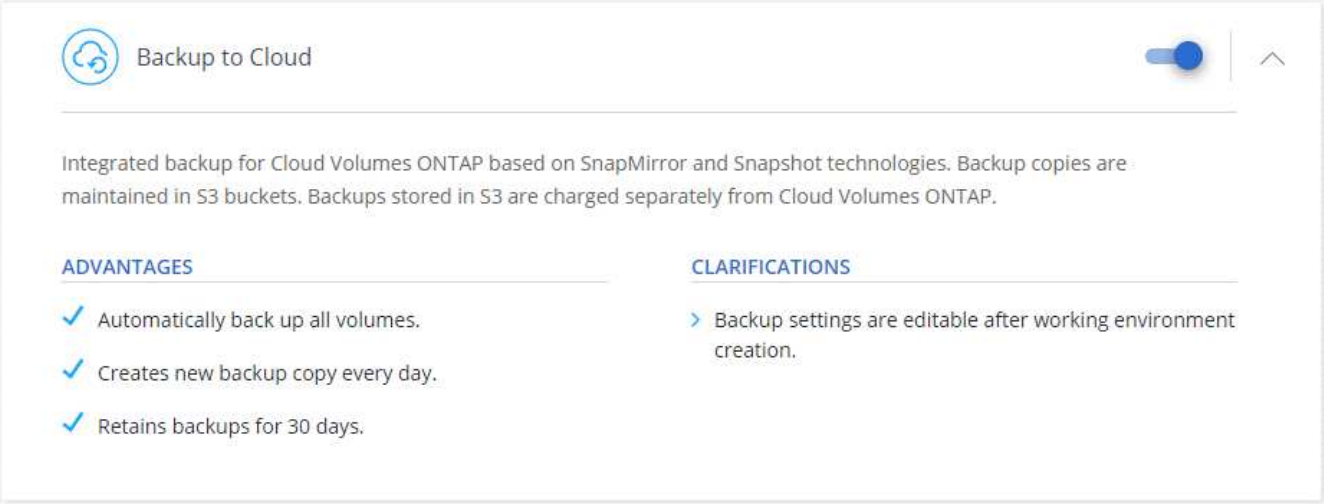
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Attivazione del backup nel cloud su un nuovo sistema

Backup su cloud è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina servizi, lasciare attivato il servizio e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

Il backup su cloud viene attivato sul sistema e consente di eseguire il backup dei volumi ogni giorno, conservando le 30 copie di backup più recenti.

Quali sono le prossime novità?

"È possibile gestire i backup modificando la pianificazione del backup, ripristinando i volumi e molto altro ancora".

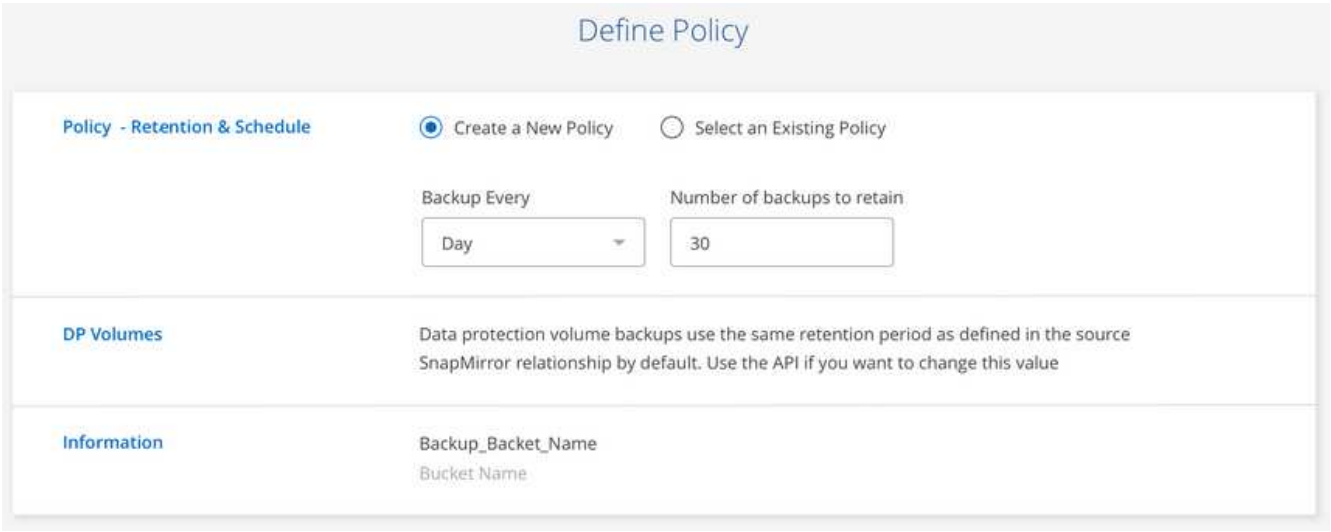
Abilitazione del backup nel cloud su un sistema esistente

Abilita il backup nel cloud in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

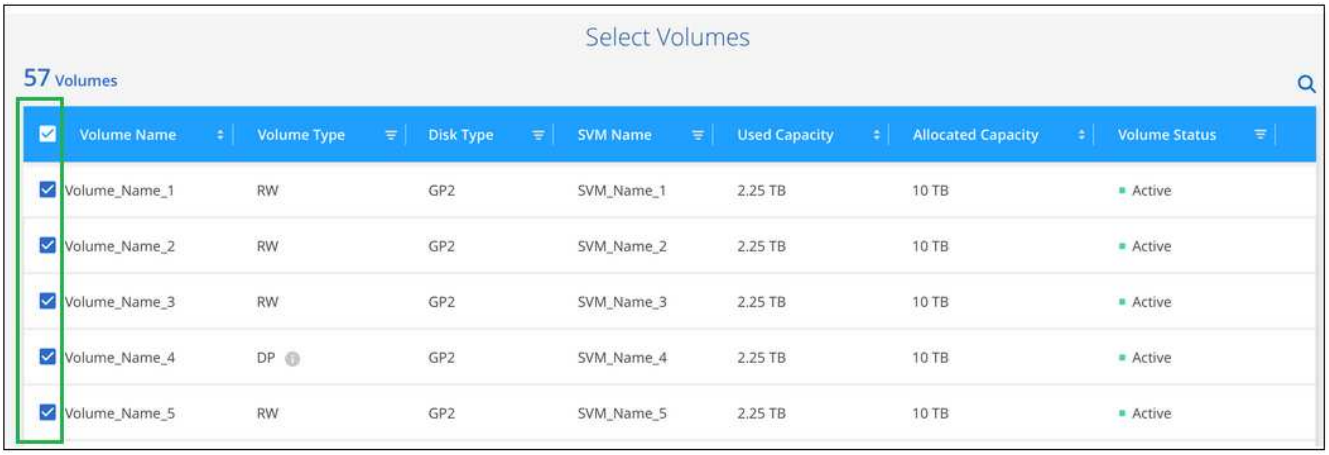
1. Selezionare l'ambiente di lavoro e fare clic su **Activate** accanto al servizio Backup to Cloud nel pannello a destra.

2. Definire la pianificazione del backup e il valore di conservazione e fare clic su **continua**.



Vedere "l'elenco dei criteri esistenti".

3. Selezionare i volumi di cui si desidera eseguire il backup e fare clic su **Activate** (attiva).



Risultato

Backup su cloud inizia a eseguire i backup iniziali di ciascun volume selezionato.

Quali sono le prossime novità?

"È possibile gestire i backup modificando la pianificazione del backup, ripristinando i volumi e molto altro ancora".

Backup dei dati sullo storage Azure Blob

Completa alcuni passaggi per iniziare a eseguire il backup dei dati da Cloud Volumes ONTAP a Azure Blob Storage.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare il supporto per la configurazione

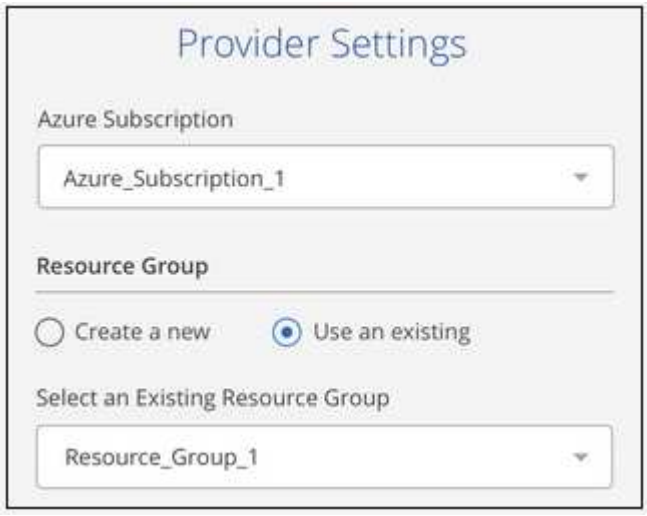
- Stai eseguendo Cloud Volumes ONTAP 9.7 o versione successiva in Azure.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup Cloud Manager Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup su cloud di NetApp.

Abilita Backup su cloud sul tuo sistema nuovo o esistente

- Nuovi sistemi: Il backup su cloud è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.
- Sistemi esistenti: Selezionare l'ambiente di lavoro e fare clic su **Activate** (attiva) accanto al servizio Backup to Cloud nel pannello di destra, quindi seguire la procedura di installazione guidata.

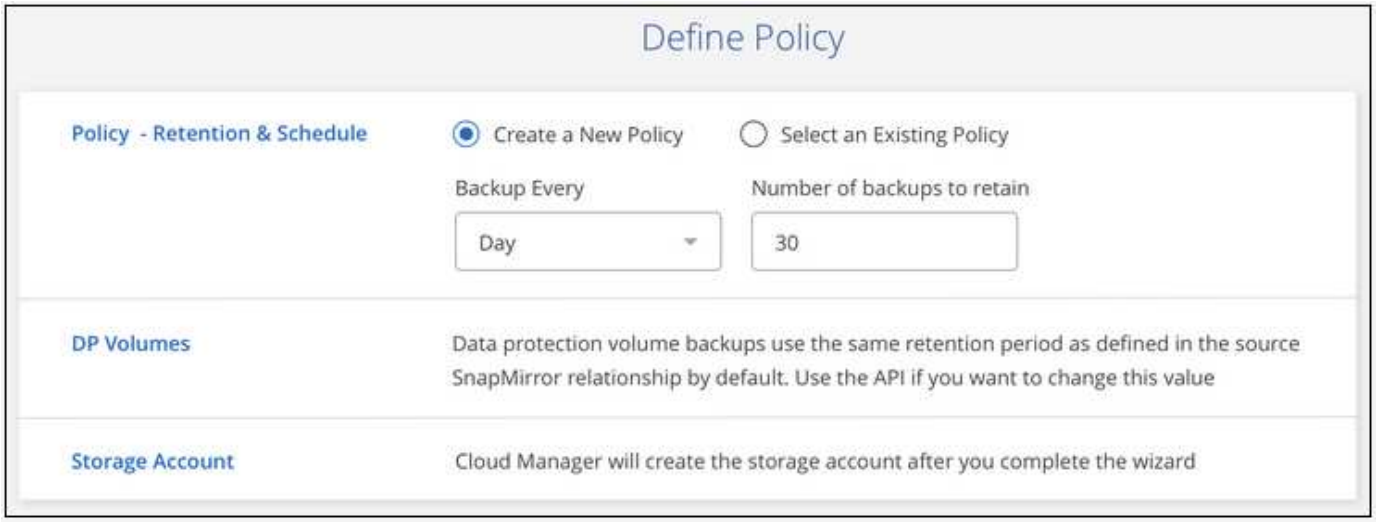
Inserire i dettagli del provider

Selezionare l'abbonamento al provider e scegliere se si desidera creare un nuovo gruppo di risorse o utilizzare un gruppo di risorse già esistente.



Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca ulteriori opzioni.

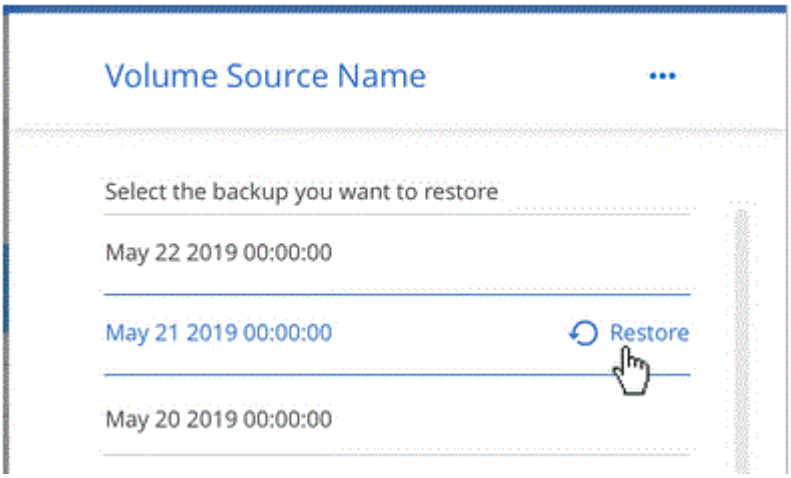


5 Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi).

6 Ripristinare i dati, se necessario

Dall'elenco di backup, selezionare un volume, selezionare un backup, quindi ripristinare i dati dal backup a un nuovo volume.



Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di iniziare il backup dei volumi nello storage Azure Blob.

Versioni di ONTAP supportate

Cloud Volumes ONTAP 9.7 e versioni successive.

Aree Azure supportate

Il backup su cloud è supportato in tutte le regioni di Azure "Dove è supportato Cloud Volumes ONTAP".

Requisiti di licenza

Per le licenze di Backup to Cloud PAYGO, è necessario un abbonamento a Azure Marketplace prima di attivare Backup to Cloud. La fatturazione per il backup su cloud viene effettuata tramite questo abbonamento. "È possibile iscriversi dalla pagina Dettagli credenziali della procedura guidata dell'ambiente di lavoro".

Per le licenze BYOL di Backup su cloud, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. Vedere "Aggiunta e aggiornamento della licenza BYOL di backup".

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di storage in cui verranno collocati i backup.

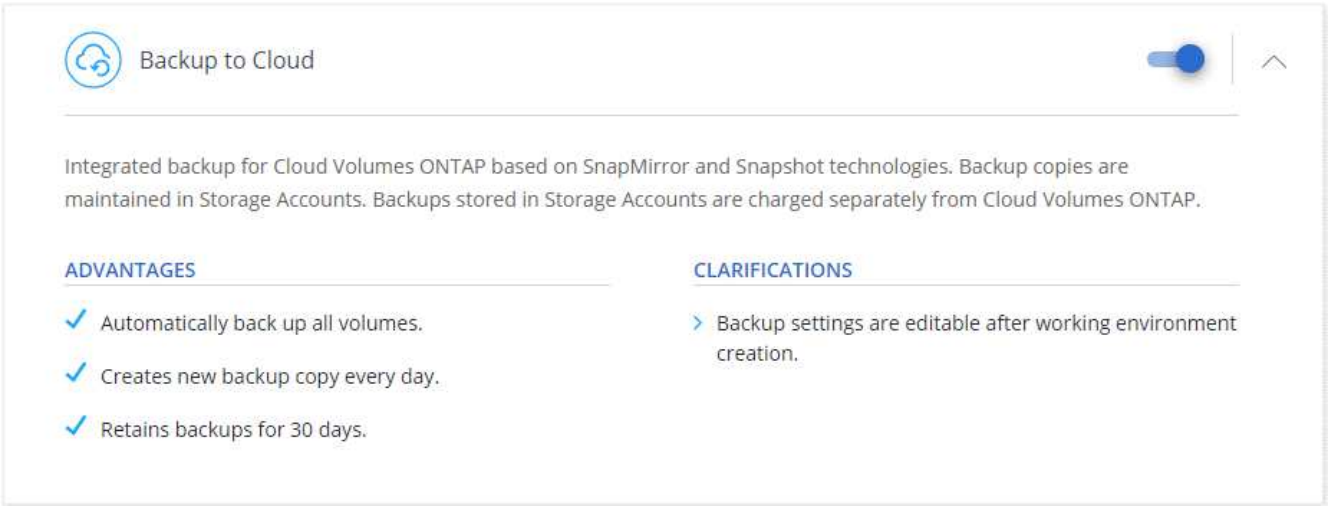
Attivazione del backup nel cloud su un nuovo sistema

Backup su cloud è attivato per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Se si desidera selezionare il nome del gruppo di risorse, **disabilitare** il backup nel cloud durante l'implementazione di Cloud Volumes ONTAP. Seguire la procedura per attivazione del backup nel cloud su un sistema esistente Per attivare il backup nel cloud e scegliere il gruppo di risorse.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Microsoft Azure come cloud provider e scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali e assicurati che sia disponibile un abbonamento a Azure Marketplace.
4. Nella pagina servizi, lasciare attivato il servizio e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

Il backup su cloud viene attivato sul sistema e consente di eseguire il backup dei volumi ogni giorno, conservando le 30 copie di backup più recenti.

Quali sono le prossime novità?

"È possibile gestire i backup modificando la pianificazione del backup, ripristinando i volumi e molto altro ancora".

Abilitazione del backup nel cloud su un sistema esistente

Abilita il backup nel cloud in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

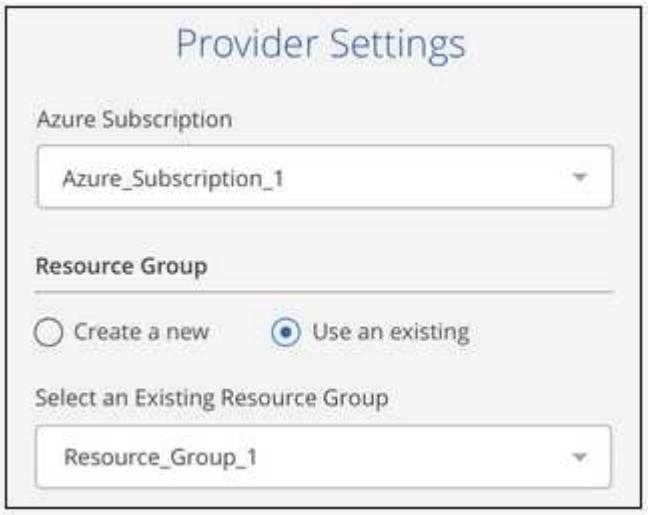
1. Selezionare l'ambiente di lavoro e fare clic su **Activate** accanto al servizio Backup to Cloud nel pannello a destra.

2. Selezionare i dettagli del provider:

   a. L'abbonamento Azure utilizzato per memorizzare i backup.

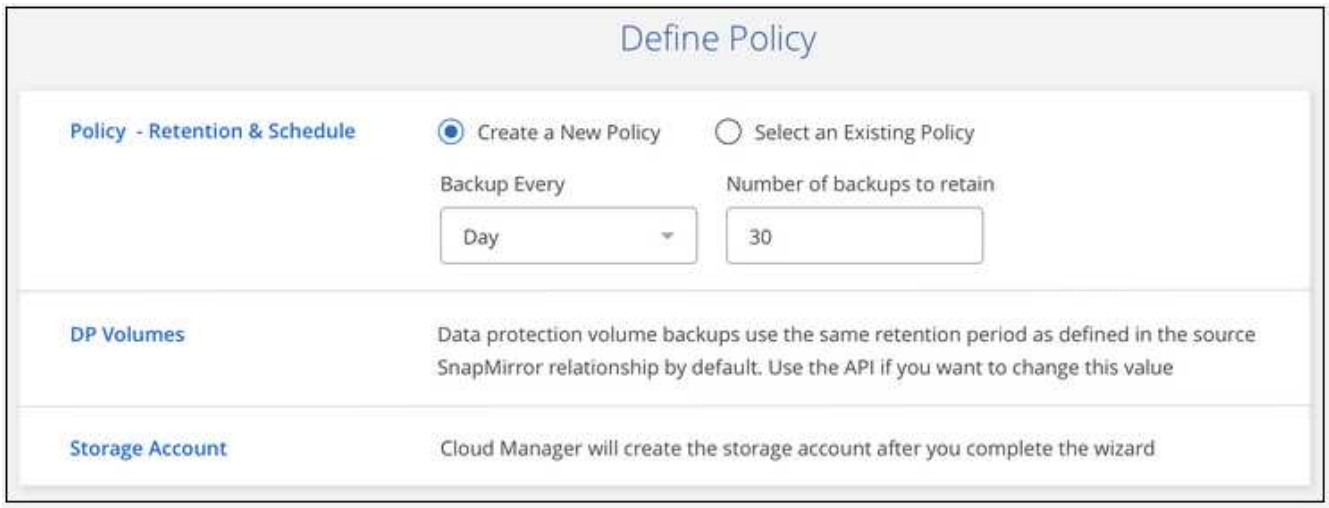
   b. Il gruppo di risorse - è possibile creare un nuovo gruppo di risorse o selezionare un gruppo di risorse esistente.

   c. Quindi fare clic su **continua**.



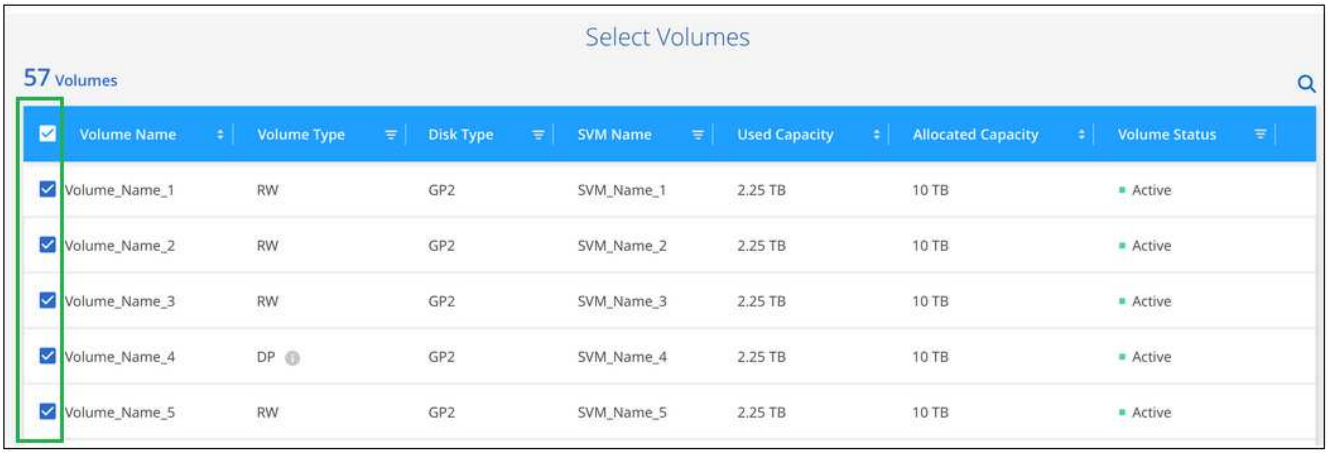
   Tenere presente che non è possibile modificare l'abbonamento o il gruppo di risorse dopo l'avvio dei servizi.

3. Nella pagina *define Policy*, selezionare il valore di pianificazione e conservazione del backup e fare clic su **continua**.



Vedere "l'elenco dei criteri esistenti".

4. Selezionare i volumi di cui si desidera eseguire il backup e fare clic su **Activate** (attiva).



Risultato

Backup su cloud inizia a eseguire i backup iniziali di ciascun volume selezionato.

Quali sono le prossime novità?

"È possibile gestire i backup modificando la pianificazione del backup, ripristinando i volumi e molto altro ancora".

Backup dei dati da un sistema ONTAP on-premise al cloud

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dal tuo sistema ONTAP on-premise allo storage a oggetti a basso costo nel cloud.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare il supporto per la configurazione

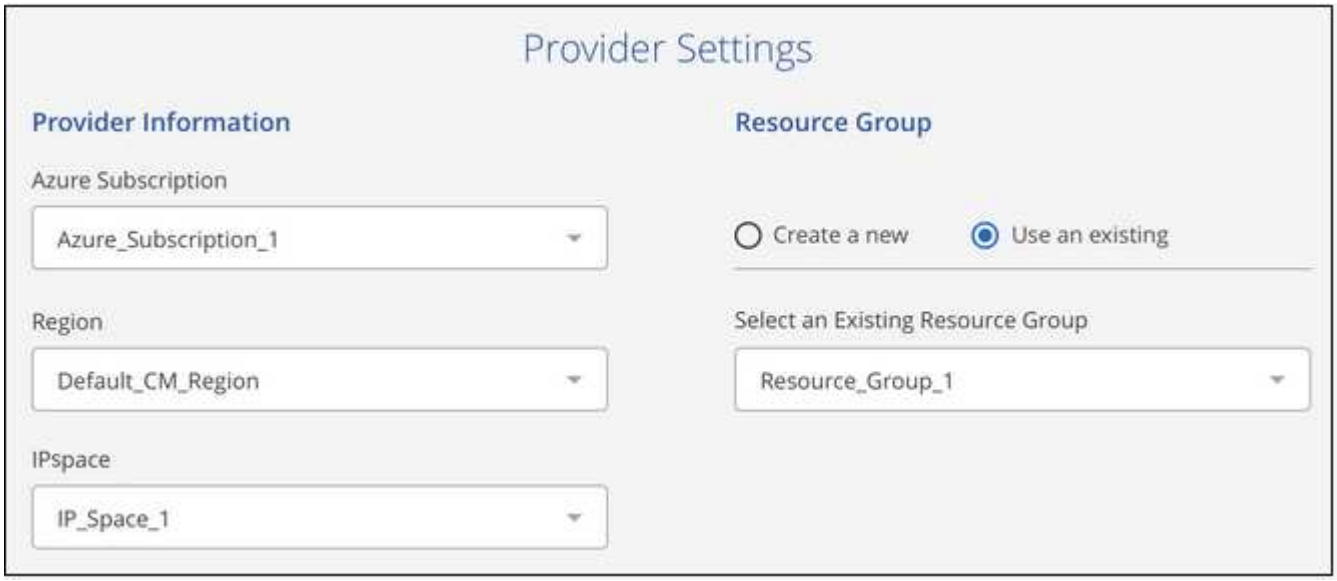
- Hai scoperto il cluster on-premise e lo hai aggiunto a un ambiente di lavoro in Cloud Manager. Vedere "Alla scoperta dei cluster ONTAP" per ulteriori informazioni.
- Sul cluster è in esecuzione ONTAP 9.7P5 o versione successiva.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. "Offerta di backup Cloud Manager Marketplace", oppure è stato acquistato "e attivato" Una licenza BYOL di backup su cloud di NetApp.

Abilitare Backup su cloud nel sistema

Selezionare l'ambiente di lavoro e fare clic su **Activate** accanto al servizio Backup to Cloud nel pannello di destra, quindi seguire la procedura di installazione guidata.

Selezionare il provider cloud e immettere i dettagli del provider

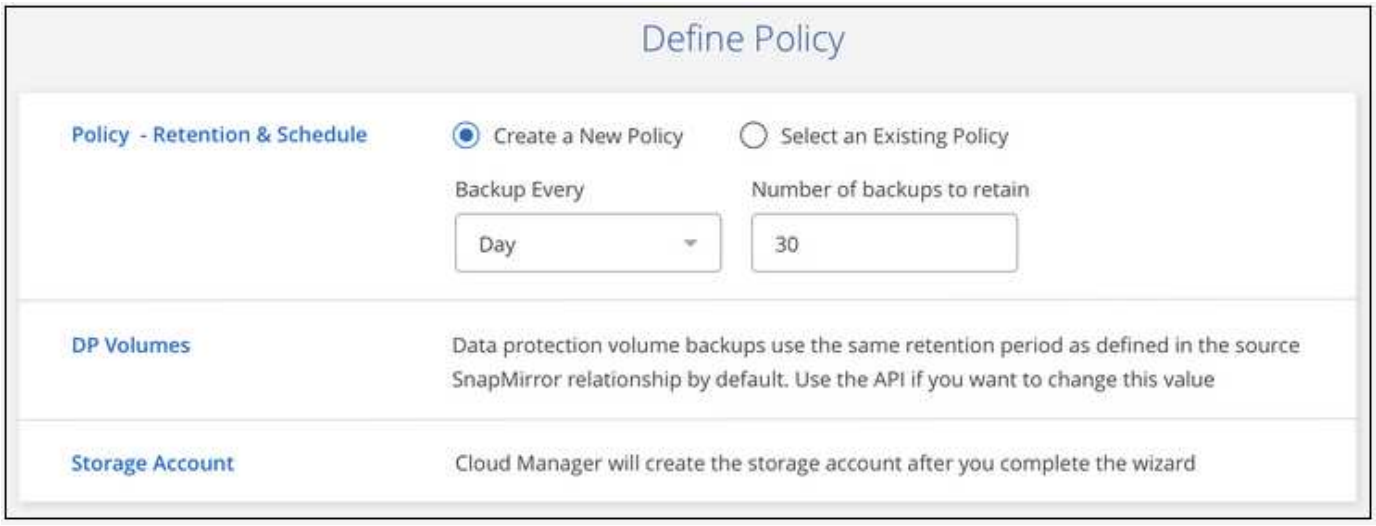
Selezionare il provider, quindi l'abbonamento al provider, la regione e il gruppo di risorse. È inoltre necessario specificare IPSpace nel cluster ONTAP in cui risiedono i volumi.



Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di

ciascun volume. Passare a backup settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca ulteriori opzioni.

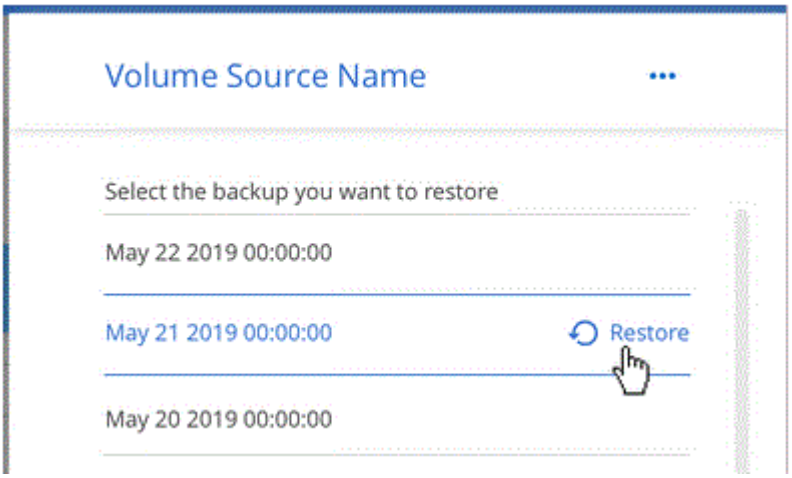


5 Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup dal cluster.

6 Ripristinare i dati, se necessario

Dall'elenco di backup, selezionare un volume, selezionare un backup, quindi ripristinare i dati dal backup a un nuovo volume su un sistema Cloud Volumes ONTAP che utilizza lo stesso provider cloud.



Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi nello storage Azure Blob.

Versioni di ONTAP supportate

ONTAP 9.7P5 e versioni successive.

Requisiti di rete del cluster

Su ogni nodo ONTAP che ospita i volumi di cui si desidera eseguire il backup è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti. La SVM amministrativa deve risiedere su IPSpace. "Scopri di più su IPspaces".

Quando si imposta il backup sul cloud, viene richiesto di utilizzare IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Aree Azure supportate

Il backup su cloud è supportato in tutte le regioni di Azure "dove sono supportati i volumi cloud".

Requisiti di licenza

Per le licenze di Backup to Cloud PAYGO, è necessario sottoscrivere il "Offerta di backup di Azure Marketplace Cloud Manager" È necessario prima di attivare il backup nel cloud. La fatturazione per il backup su cloud viene effettuata tramite questo abbonamento.

Per le licenze BYOL di Backup su cloud, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. Vedere "Aggiunta e aggiornamento della licenza BYOL di backup".

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di storage in cui verranno collocati i backup.

Abilitazione del backup nel cloud

Abilita il backup nel cloud in qualsiasi momento direttamente dall'ambiente di lavoro.

Fasi

1. Selezionare l'ambiente di lavoro e fare clic su **Activate** accanto al servizio Backup to Cloud nel pannello a destra.

2. Selezionare il provider, quindi immettere i dati del provider:

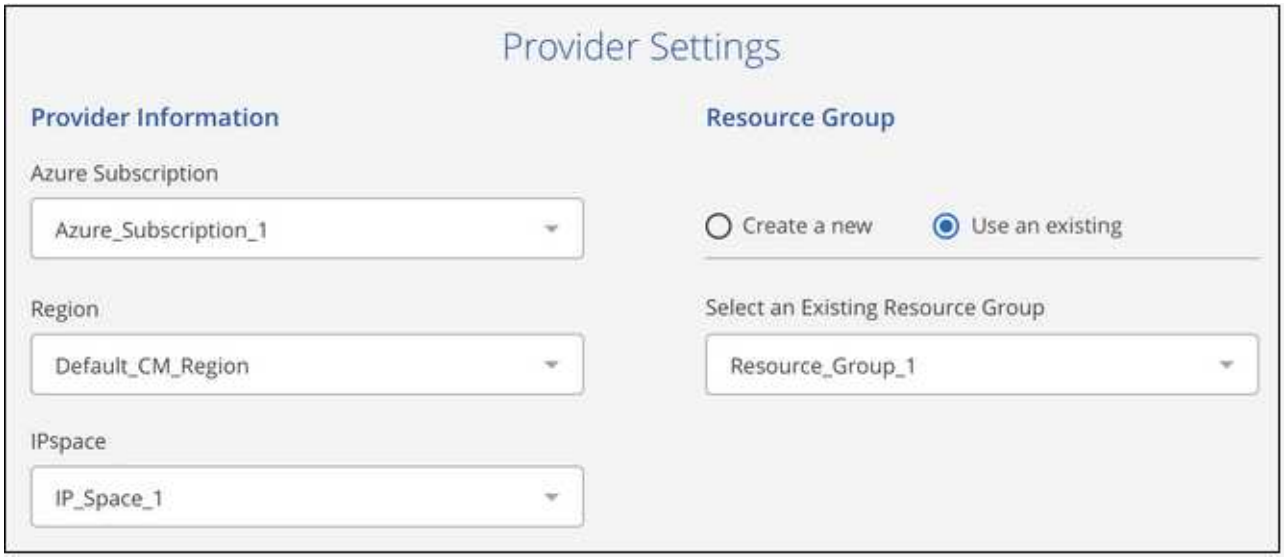
    a. L'abbonamento Azure utilizzato per memorizzare i backup.

    b. La regione di Azure.

    c. Il gruppo di risorse - è possibile creare un nuovo gruppo di risorse o selezionare un gruppo di risorse esistente.

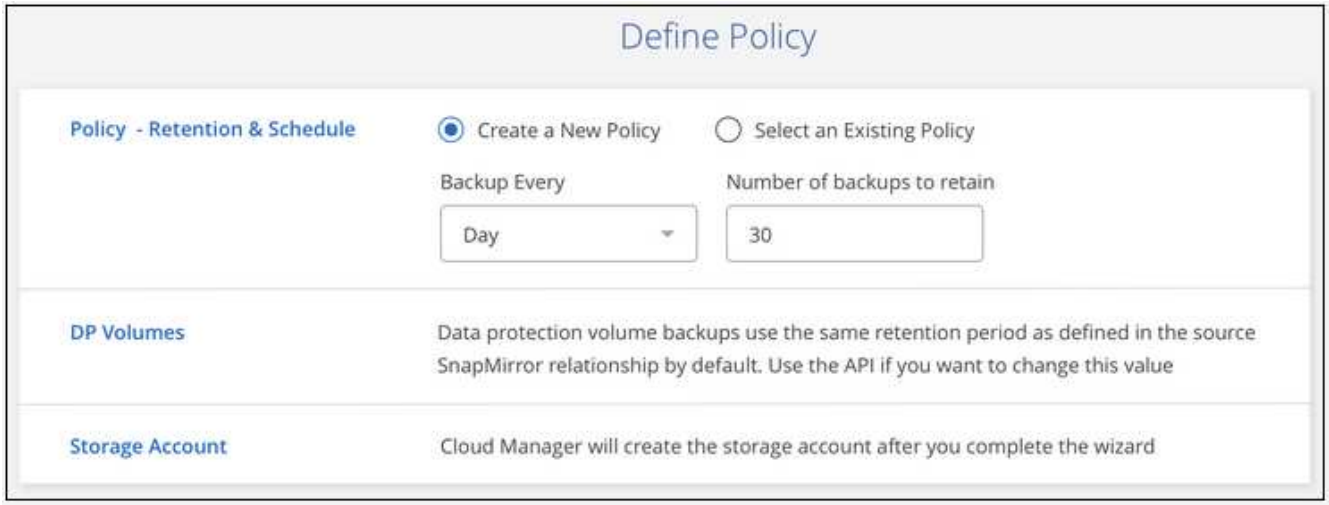
    d. IPSpace nel cluster ONTAP in cui risiedono i volumi di cui si desidera eseguire il backup.

    e. Quindi fare clic su **continua**.



Tenere presente che non è possibile modificare l'abbonamento o il gruppo di risorse dopo l'avvio dei servizi.

3. Nella pagina *define Policy*, selezionare il valore di pianificazione e conservazione del backup e fare clic su **continua**.



Vedere "l'elenco dei criteri esistenti".

4. Selezionare i volumi di cui si desidera eseguire il backup e fare clic su **Activate** (attiva).

Risultato

Backup su cloud inizia a eseguire i backup iniziali di ciascun volume selezionato.

Quali sono le prossime novità?

"È possibile gestire i backup modificando la pianificazione del backup, ripristinando i volumi e molto altro ancora".

Gestione dei backup per sistemi Cloud Volumes ONTAP e ONTAP on-premise

Gestisci i backup per i sistemi Cloud Volumes ONTAP e ONTAP on-premise modificando la pianificazione del backup, ripristinando i volumi, eliminando i backup e molto altro ancora.

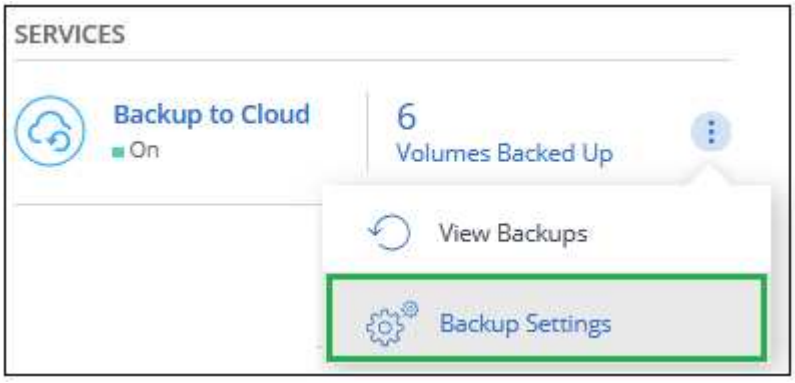
Modifica della pianificazione e della conservazione del backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. È possibile passare a backup settimanali o mensili e modificare il numero di copie di backup da conservare. È inoltre possibile selezionare una delle policy definite dal sistema che fornisce backup pianificati per 3 mesi, 1 anno e 7 anni.

La modifica del criterio di backup influisce solo sui nuovi volumi creati dopo la modifica della pianificazione. Non influisce sulla pianificazione per i volumi esistenti.

Fasi

1. Selezionare l'ambiente di lavoro.
2. Fare clic su E selezionare **Backup Settings**.



3. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Modify Backup Policy** (Modifica policy di backup).

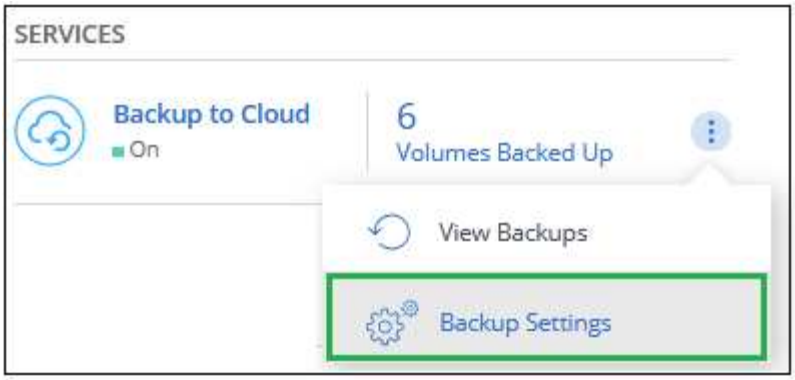
4. Dalla pagina *Modify Backup Policy*, modificare la pianificazione e la conservazione del backup, quindi fare clic su **Save** (Salva).

Avvio e interruzione dei backup dei volumi

È possibile interrompere il backup di un volume se non sono necessarie copie di backup di quel volume e non si desidera pagare il costo di archiviazione dei backup. È inoltre possibile aggiungere un nuovo volume all'elenco di backup, se non viene eseguito il backup.

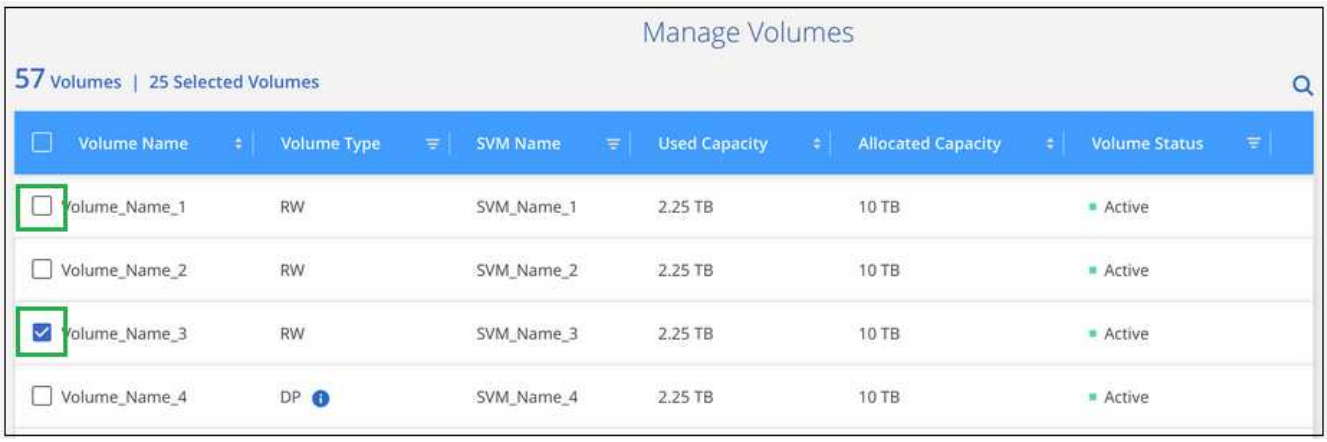
Fasi

1. Selezionare l'ambiente di lavoro.
2. Fare clic su E selezionare **Backup Settings**.



3. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Manage Volumes** (Gestisci volumi).

4. Selezionare la casella di controllo relativa ai volumi che si desidera avviare il backup e deselezionare la casella di controllo relativa ai volumi che si desidera interrompere il backup.



Nota: quando si interrompe il backup di un volume, il provider di cloud continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup a meno che non si utilizzi eliminare i backup.

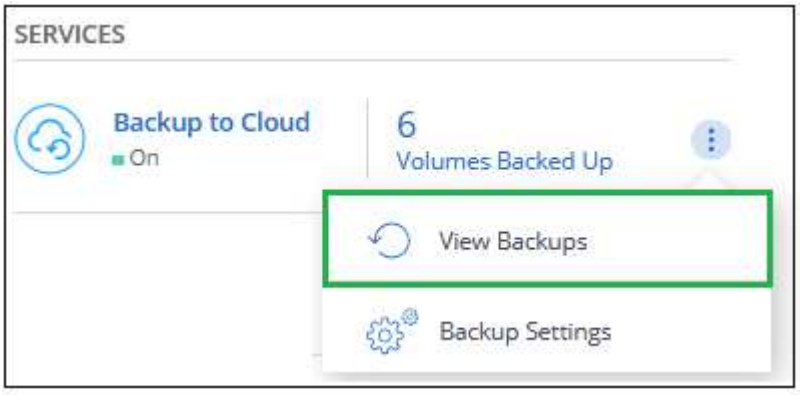
Ripristino di un volume da un backup

Quando ripristini i dati da un backup, Cloud Manager crea un *nuovo* volume utilizzando i dati del backup. È possibile ripristinare i dati in un volume nello stesso ambiente di lavoro o in un ambiente di lavoro diverso che si trova nello stesso account cloud dell'ambiente di lavoro di origine. Poiché il backup non contiene snapshot, anche il volume appena ripristinato non lo è.

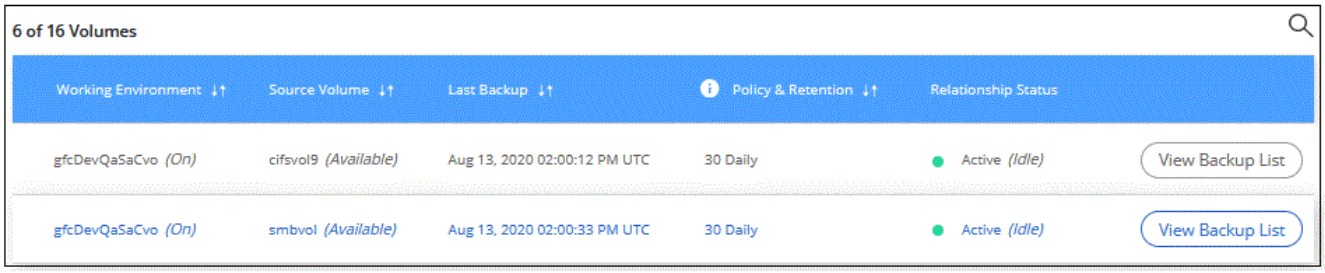
I backup creati da sistemi ONTAP on-premise possono essere ripristinati solo su sistemi Cloud Volumes ONTAP che utilizzano lo stesso cloud provider in cui risiede il backup.

Fasi

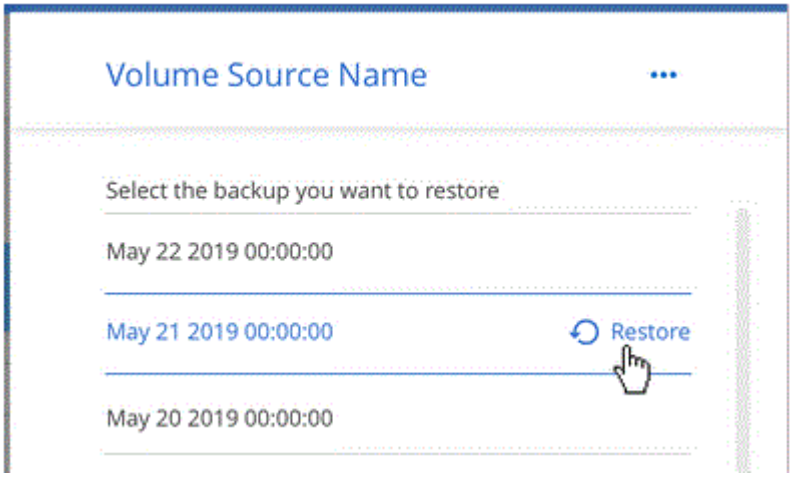
1. Selezionare l'ambiente di lavoro.
2. Fare clic su E selezionare **Visualizza backup**.



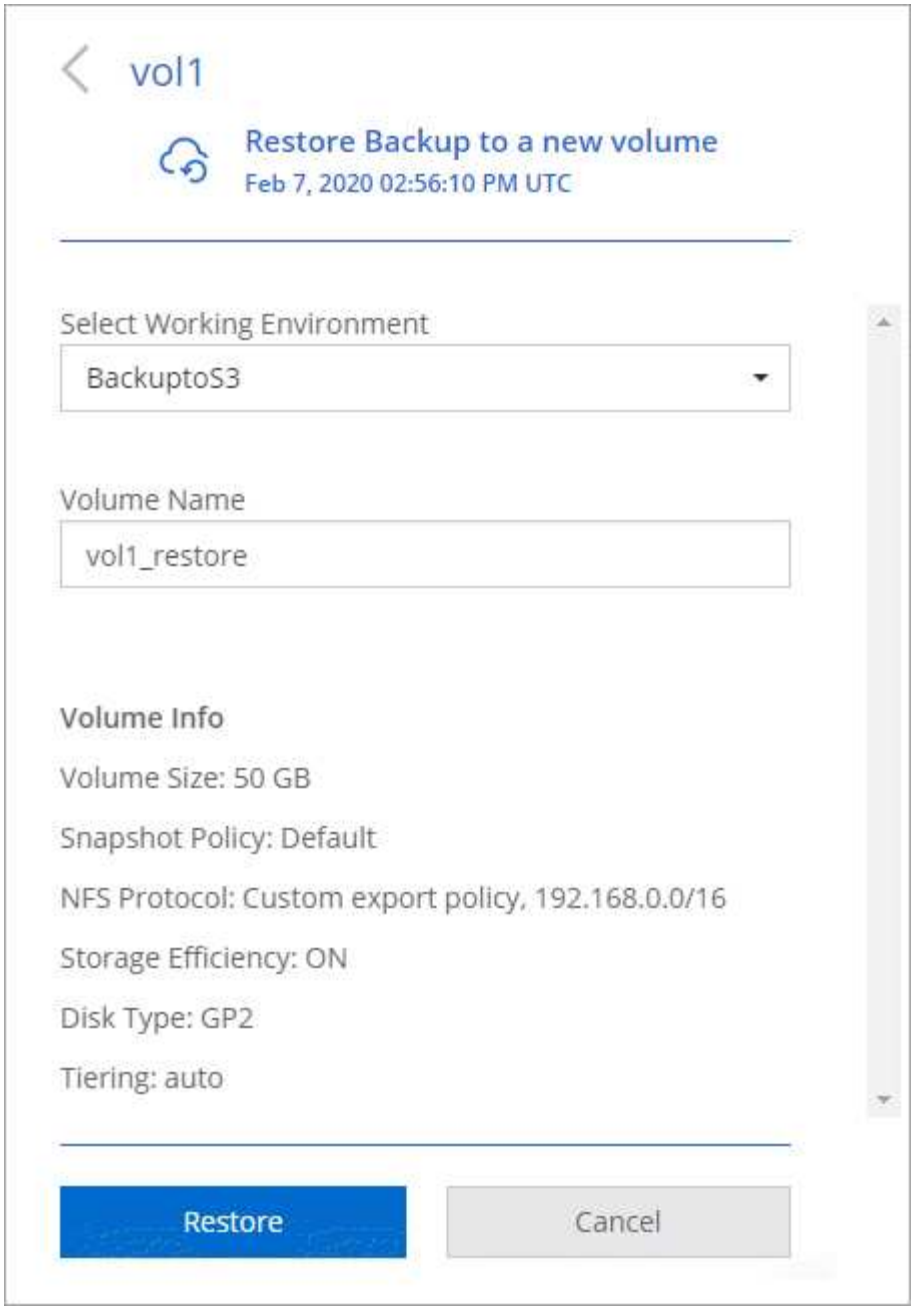
3. Selezionare la riga del volume che si desidera ripristinare e fare clic su **View Backup List** (Visualizza elenco backup).



4. Individuare il backup che si desidera ripristinare e fare clic sull'icona **Restore**.



5. Compilare la pagina *Restore Backup to new volume*:
   a. Selezionare l'ambiente di lavoro in cui si desidera ripristinare il volume.
   b. Immettere un nome per il volume.
   c. Fare clic su **Restore** (Ripristina).



Risultato

Cloud Manager crea un nuovo volume in base al backup selezionato. È possibile "gestire questo nuovo volume" secondo necessità.

Eliminazione dei backup

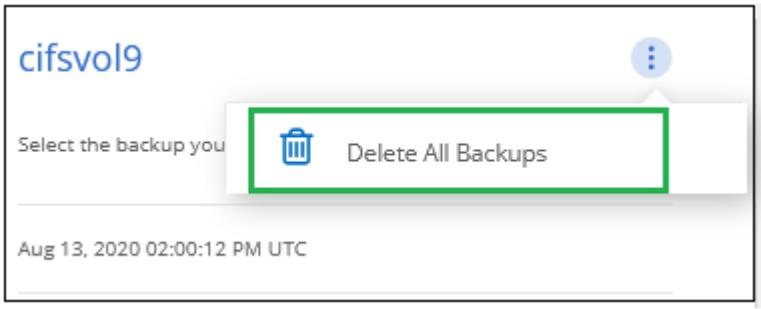
Backup su cloud consente di eliminare *tutti* i backup di un volume specifico. Non puoi eliminare *singoli* backup.

Questa operazione può essere eseguita se non sono più necessari i backup o se è stato eliminato il volume di origine e si desidera rimuovere tutti i backup.

Se si prevede di eliminare un sistema Cloud Volumes ONTAP o ONTAP on-premise con backup, è necessario eliminare i backup **prima** di eliminare il sistema. Backup su cloud non elimina automaticamente i backup quando si elimina un sistema e non esiste attualmente alcun supporto nell'interfaccia utente per eliminare i backup dopo che il sistema è stato eliminato.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Backup**.
2. Dall'elenco dei volumi, individuare il volume e fare clic su **View Backup List** (Visualizza elenco backup).
3. Fare clic su ••• E selezionare **Delete all backups** (Elimina tutti i backup).



4. Nella finestra di dialogo di conferma, fare clic su **Delete** (Elimina).

Disattivazione del backup nel cloud

La disattivazione del backup su cloud per un ambiente di lavoro disattiva i backup di ciascun volume sul sistema e disattiva anche la possibilità di ripristinare un volume. I backup esistenti non verranno eliminati.

Tieni presente che il tuo cloud provider continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup, a meno che non elimini i backup.

Fasi

1. Selezionare l'ambiente di lavoro.
2. Fare clic su ⋮ E selezionare **Backup Settings**.

3. Dalla *pagina Backup Settings*, fare clic su ••• Per l'ambiente di lavoro e selezionare **Disattiva backup su cloud**.

4. Nella finestra di dialogo di conferma, fare clic su **Disattiva**.

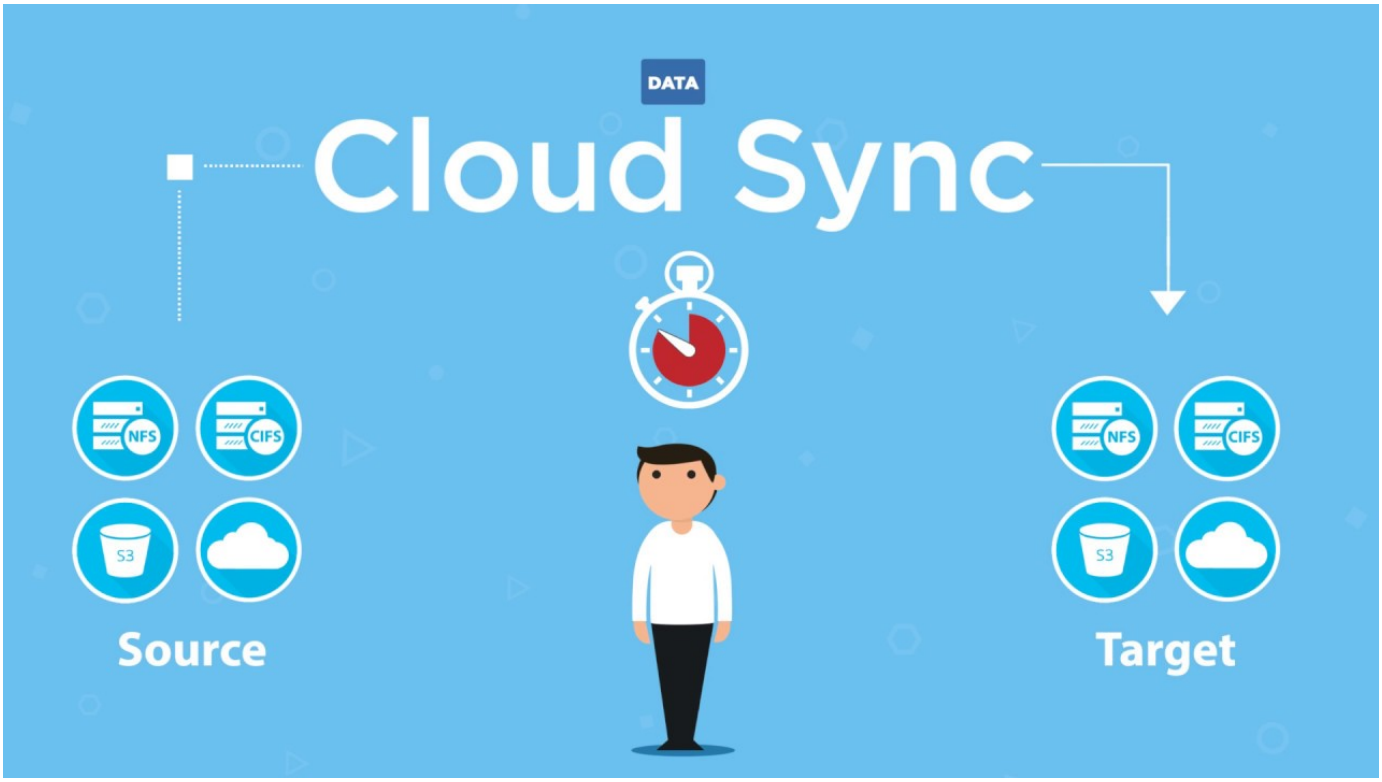
Copiare e sincronizzare i dati

Panoramica di Cloud Sync

Il servizio NetApp Cloud Sync offre un modo semplice, sicuro e automatizzato per migrare i dati a qualsiasi destinazione, nel cloud o on-premise. Sia che si tratti di un set di dati NAS basato su file (NFS o SMB), di un formato di oggetti Amazon Simple Storage Service (S3), di un'appliance NetApp StorageGRID® o di qualsiasi altro archivio di oggetti del provider cloud, Cloud Sync può convertirlo e spostarlo per te.

Caratteristiche

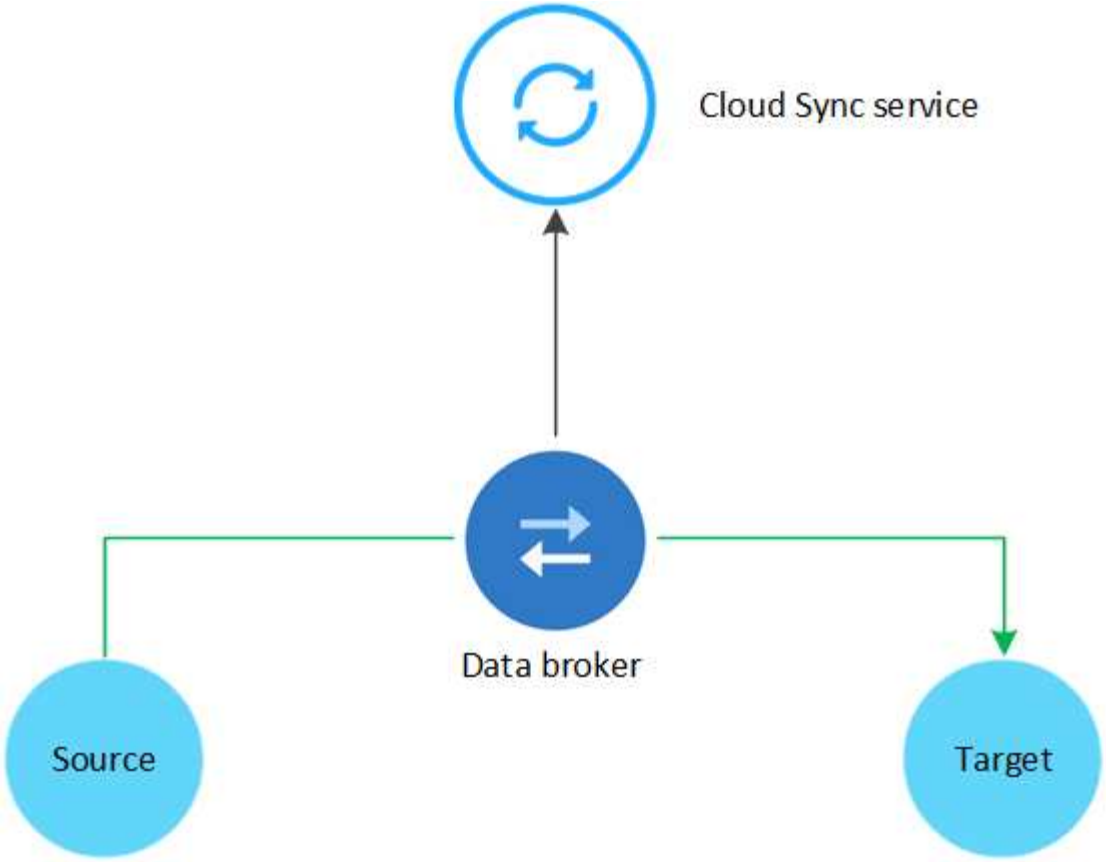
Guarda il seguente video per una panoramica di Cloud Sync:



Come funziona Cloud Sync

Cloud Sync è una piattaforma software-as-a-service (SaaS) che comprende un broker di dati, un'interfaccia basata sul cloud disponibile tramite Cloud Manager e un'origine e un target.

La seguente immagine mostra la relazione tra i componenti di Cloud Sync:



Il software NetApp data broker sincronizza i dati da un'origine a un'area di destinazione (chiamata *relazione di sincronizzazione*). Puoi eseguire il data broker in AWS, Azure, Google Cloud Platform o on-premise. Il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio Cloud Sync e contattare altri servizi e repository. "Visualizzare l'elenco degli endpoint".

Dopo la copia iniziale, il servizio sincronizza i dati modificati in base alla pianificazione impostata.

Tipi di storage supportati

Cloud Sync supporta i seguenti tipi di storage:

- Qualsiasi server NFS
- Qualsiasi server SMB
- EFS AWS
- AWS S3
- Azure Blob
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Storage Google Cloud
- Storage a oggetti IBM Cloud
- Cluster ONTAP on-premise
- Storage ONTAP S3

- StorageGRID

"Esaminare le relazioni di sincronizzazione supportate".

Costo

L'utilizzo di Cloud Sync comporta due tipi di costi: Costi delle risorse e costi del servizio.

Costi delle risorse

I costi delle risorse sono correlati ai costi di calcolo e storage per l'esecuzione del data broker nel cloud.

Costi del servizio

Esistono due modi per pagare le relazioni di sincronizzazione dopo la fine della prova gratuita di 14 giorni. La prima opzione consiste nell'effettuare l'iscrizione da AWS o Azure, che consente di pagare ogni ora o annualmente. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp. Per ulteriori informazioni, leggere le sezioni seguenti.

Iscrizione al Marketplace

La sottoscrizione al servizio Cloud Sync di AWS o Azure consente di pagare a una tariffa oraria o annuale. "Puoi iscriverti tramite AWS o Azure", a seconda del luogo in cui si desidera essere fatturati.

Abbonamenti orari

Con un abbonamento oraria pay-as-you-go, il servizio Cloud Sync addebita ogni ora in base al numero di relazioni di sincronizzazione create.

- "Visualizza i prezzi in Azure"
- "Visualizza i prezzi pay-as-you-go in AWS"

Abbonamenti annuali

Un abbonamento annuale fornisce una licenza per 20 relazioni di sincronizzazione che si paga in anticipo. Se superi le 20 relazioni di sincronizzazione e ti sei iscritto tramite Azure, pagherai per le relazioni aggiuntive entro l'ora.

"Visualizza i prezzi annuali in AWS"

Licenze di NetApp

Un altro modo per pagare anticipatamente le relazioni di sincronizzazione è acquistare le licenze direttamente da NetApp. Ogni licenza consente di creare fino a 20 relazioni di sincronizzazione.

È possibile utilizzare queste licenze con un abbonamento AWS o Azure. Ad esempio, se si dispone di 25 relazioni di sincronizzazione, è possibile pagare le prime 20 relazioni di sincronizzazione utilizzando una licenza e quindi pagare a consumo da AWS o Azure con le restanti 5 relazioni di sincronizzazione.

"Scopri come acquistare le licenze e aggiungerle a Cloud Sync".

Termini di licenza

I clienti che acquistano una licenza Bring Your Own (BYOL) al servizio Cloud Sync devono essere consapevoli delle limitazioni associate al diritto di licenza.

- I clienti hanno il diritto di sfruttare la licenza BYOL per un periodo non superiore a un anno dalla data di

consegna.

- I clienti hanno il diritto di sfruttare la licenza BYOL per stabilire e non superare un totale di 20 singole connessioni tra un'origine e una destinazione (ciascuna una "relazione di sincronizzazione").
- Il diritto di un cliente scade al termine del periodo di validità della licenza di un anno, indipendentemente dal fatto che il cliente abbia raggiunto la limitazione della relazione di sincronizzazione del 20.
- Nel caso in cui il cliente scelga di rinnovare la propria licenza, le relazioni di sincronizzazione inutilizzate associate alla concessione di licenza precedente NON vengono ripristinate al rinnovo della licenza.

Privacy dei dati

NetApp non ha accesso alle credenziali fornite durante l'utilizzo del servizio Cloud Sync. Le credenziali vengono memorizzate direttamente sulla macchina del data broker, che risiede nella rete.

A seconda della configurazione scelta, Cloud Sync potrebbe richiedere le credenziali quando si crea una nuova relazione. Ad esempio, quando si imposta una relazione che include un server SMB o quando si implementa il data broker in AWS.

Queste credenziali vengono sempre salvate direttamente nel data broker stesso. Il data broker risiede su un computer della tua rete, sia esso on-premise che nel tuo account cloud. Le credenziali non vengono mai rese disponibili a NetApp.

Le credenziali vengono crittografate localmente sulla macchina del broker di dati utilizzando HashiCorp Vault.

Limitazioni

- Cloud Sync non è supportato in Cina.
- Oltre alla Cina, il data broker Cloud Sync non è supportato nelle seguenti regioni:
  - AWS GovCloud (USA)
  - Azure US Gov
  - Azure US DOD

Inizia subito

Avvio rapido per Cloud Sync

La guida introduttiva al servizio Cloud Sync include alcuni passaggi.

Preparare l'origine e la destinazione

Verificare che l'origine e la destinazione siano supportate e configurate. Il requisito più importante è verificare la connettività tra il data broker e le posizioni di origine e destinazione. "Scopri di più".

Preparare una posizione per il data broker di NetApp

Il software NetApp data broker sincronizza i dati da un'origine a un'area di destinazione (chiamata *relazione di sincronizzazione*). Puoi eseguire il data broker in AWS, Azure, Google Cloud Platform o on-premise. Il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il

servizio Cloud Sync e contattare altri servizi e repository. "Visualizzare l'elenco degli endpoint".

Cloud Sync ti guida attraverso il processo di installazione quando crei una relazione di sincronizzazione, a questo punto puoi implementare il data broker nel cloud o scaricare uno script di installazione per il tuo host Linux.

- "Esaminare l'installazione di AWS"
- "Esaminare l'installazione di Azure"
- "Esaminare l'installazione di GCP"
- "Esaminare l'installazione dell'host Linux"

Crea la tua prima relazione di sincronizzazione

Accedere a. "Cloud Manager", Fare clic su **Sync**, quindi trascinare le selezioni per l'origine e la destinazione. Seguire le istruzioni per completare la configurazione. "Scopri di più".

Paga le tue relazioni di sincronizzazione al termine della prova gratuita

Iscriviti ad AWS o Azure per pagare a consumo o per pagare annualmente. Oppure acquistare le licenze direttamente da NetApp. Per configurarla, accedere alla pagina Impostazioni di licenza di Cloud Sync. "Scopri di più".

Preparazione dell'origine e della destinazione

Preparare la sincronizzazione dei dati verificando che l'origine e la destinazione siano supportate e configurate.

Relazioni di sincronizzazione supportate

Cloud Sync consente di sincronizzare i dati da un'origine a una destinazione (chiamata *relazione di sincronizzazione*). Prima di iniziare, è necessario comprendere le relazioni supportate.

Posizione di origine	Posizioni di destinazione supportate
EFS AWS	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID
AWS S3	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Azure Blob	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise • Server SMB • StorageGRID
Azure NetApp Files (NFS)	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID
Azure NetApp Files (PMI)	• AWS S3 • Azure Blob • Azure NetApp Files (PMI) • Cloud Volumes ONTAP (PMI) • Cloud Volumes Service (PMI) • Storage Google Cloud • Storage a oggetti IBM Cloud • Cluster ONTAP on-premise • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Cloud Volumes ONTAP (NFS)	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID
Cloud Volumes ONTAP (PMI)	• AWS S3 • Azure Blob • Azure NetApp Files (PMI) • Cloud Volumes ONTAP (PMI) • Cloud Volumes Service (PMI) • Storage Google Cloud • Storage a oggetti IBM Cloud • Cluster ONTAP on-premise • Server SMB • StorageGRID
Cloud Volumes Service (NFS)	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Cloud Volumes Service (PMI)	• AWS S3 • Azure Blob • Azure NetApp Files (PMI) • Cloud Volumes ONTAP (PMI) • Cloud Volumes Service (PMI) • Storage Google Cloud • Storage a oggetti IBM Cloud • Cluster ONTAP on-premise • Server SMB • StorageGRID
Storage Google Cloud	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise • Server SMB • StorageGRID
Storage a oggetti IBM Cloud	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Server NFS	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID
Cluster ONTAP on-premise (NFS)	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • StorageGRID
Cluster ONTAP on-premise (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (PMI) • Cloud Volumes ONTAP (PMI) • Cloud Volumes Service (PMI) • Storage Google Cloud • Storage a oggetti IBM Cloud • Cluster ONTAP on-premise • Server SMB • StorageGRID
Storage ONTAP S3	• StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Server SMB	• AWS S3 • Azure Blob • Azure NetApp Files (PMI) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Storage a oggetti IBM Cloud • Storage Google Cloud • Cluster ONTAP on-premise • Server SMB • StorageGRID
StorageGRID	• EFS AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage a oggetti IBM Cloud • Storage Google Cloud • Server NFS • Cluster ONTAP on-premise • Storage ONTAP S3 • Server SMB • StorageGRID

Note:

1. È possibile scegliere un livello di storage Azure Blob specifico quando un container Blob è la destinazione:
   - Storage a caldo
   - Storage fresco
2. è possibile scegliere una classe di storage S3 specifica quando AWS S3 è la destinazione:
   - Standard (classe predefinita)
   - Tiering intelligente
   - Standard-infrequent Access (accesso standard-non frequente)
   - Accesso non frequente a una sola zona
   - Ghiacciaio
   - Glacier Deep Archive

Networking per l'origine e la destinazione

- L'origine e la destinazione devono disporre di una connessione di rete al data broker.

  Ad esempio, se un server NFS si trova nel data center e il data broker si trova in AWS, è necessaria una connessione di rete (VPN o Direct Connect) dalla rete al VPC.

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Requisiti di origine e destinazione

Verificare che la fonte e le destinazioni soddisfino i seguenti requisiti.

requisiti del bucket AWS S3

Assicurarsi che il bucket AWS S3 soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per AWS S3

Le relazioni di sincronizzazione che includono lo storage S3 richiedono un broker di dati implementato in AWS o on-premise. In entrambi i casi, Cloud Sync richiede di associare il data broker a un account AWS durante l'installazione.

- "Scopri come implementare il data broker AWS"
- "Scopri come installare il data broker su un host Linux"

Regioni AWS supportate

Tutte le regioni sono supportate, ad eccezione di quelle della Cina e di GovCloud (USA).

Autorizzazioni richieste per i bucket S3 in altri account AWS

Quando si imposta una relazione di sincronizzazione, è possibile specificare un bucket S3 che risiede in un account AWS non associato al data broker.

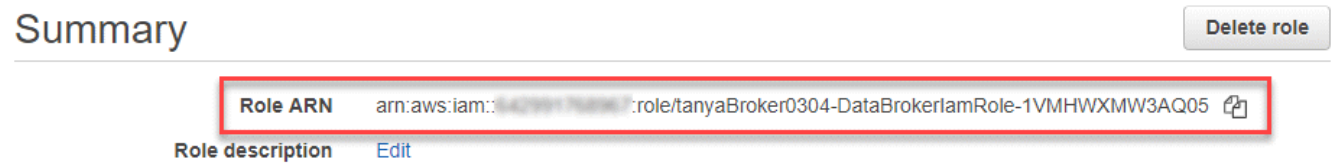
"Le autorizzazioni incluse in questo file JSON" Deve essere applicato al bucket S3 in modo che il data broker possa accedervi. Queste autorizzazioni consentono al broker di dati di copiare i dati da e verso il bucket e di elencare gli oggetti nel bucket.

Tenere presente quanto segue sulle autorizzazioni incluse nel file JSON:

1. *<BucketName>* è il nome del bucket che risiede nell'account AWS non associato al data broker.
2. *<RoleARN>* deve essere sostituito con uno dei seguenti elementi:

   - Se il data broker è stato installato manualmente su un host Linux, *RoleARN* dovrebbe essere l'ARN dell'utente AWS per cui hai fornito le credenziali AWS durante l'implementazione del data broker.
   - Se il data broker è stato implementato in AWS utilizzando il modello CloudFormation, *RoleARN* dovrebbe essere l'ARN del ruolo IAM creato dal modello.

     Per trovare il ruolo ARN, accedere alla console EC2, selezionare l'istanza del broker di dati e fare clic sul ruolo IAM nella scheda Description (Descrizione). Viene visualizzata la pagina Summary (Riepilogo) nella console IAM che contiene il ruolo ARN.



requisiti di storage di Azure Blob

Assicurati che lo storage Azure Blob soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per Azure Blob

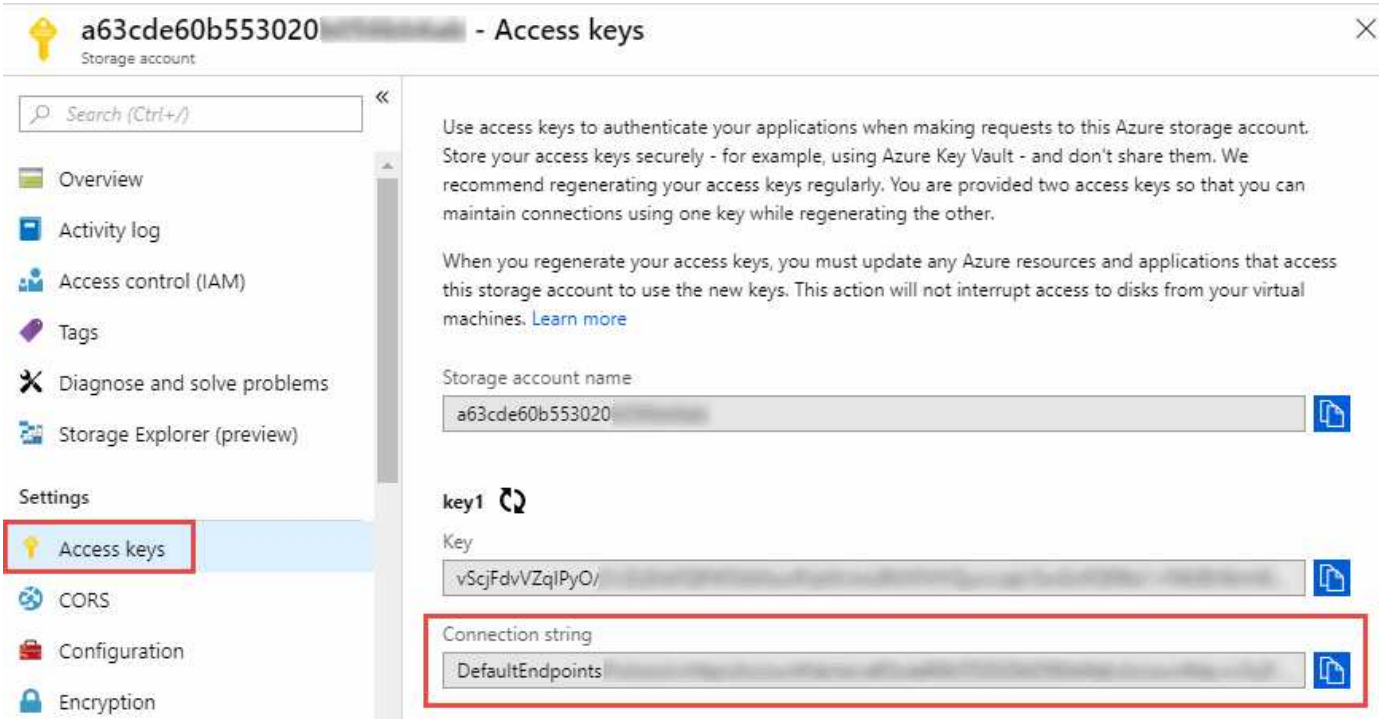
Il data broker può risiedere in qualsiasi posizione quando una relazione di sincronizzazione include lo storage Azure Blob.

Aree Azure supportate

Sono supportate tutte le regioni, ad eccezione di quelle della Cina, degli Stati Uniti e del DOD.

Stringa di connessione richiesta per le relazioni che includono Azure Blob e NFS/SMB

Quando si crea una relazione di sincronizzazione tra un container Azure Blob e un server NFS o SMB, è necessario fornire a Cloud Sync la stringa di connessione dell'account di storage:

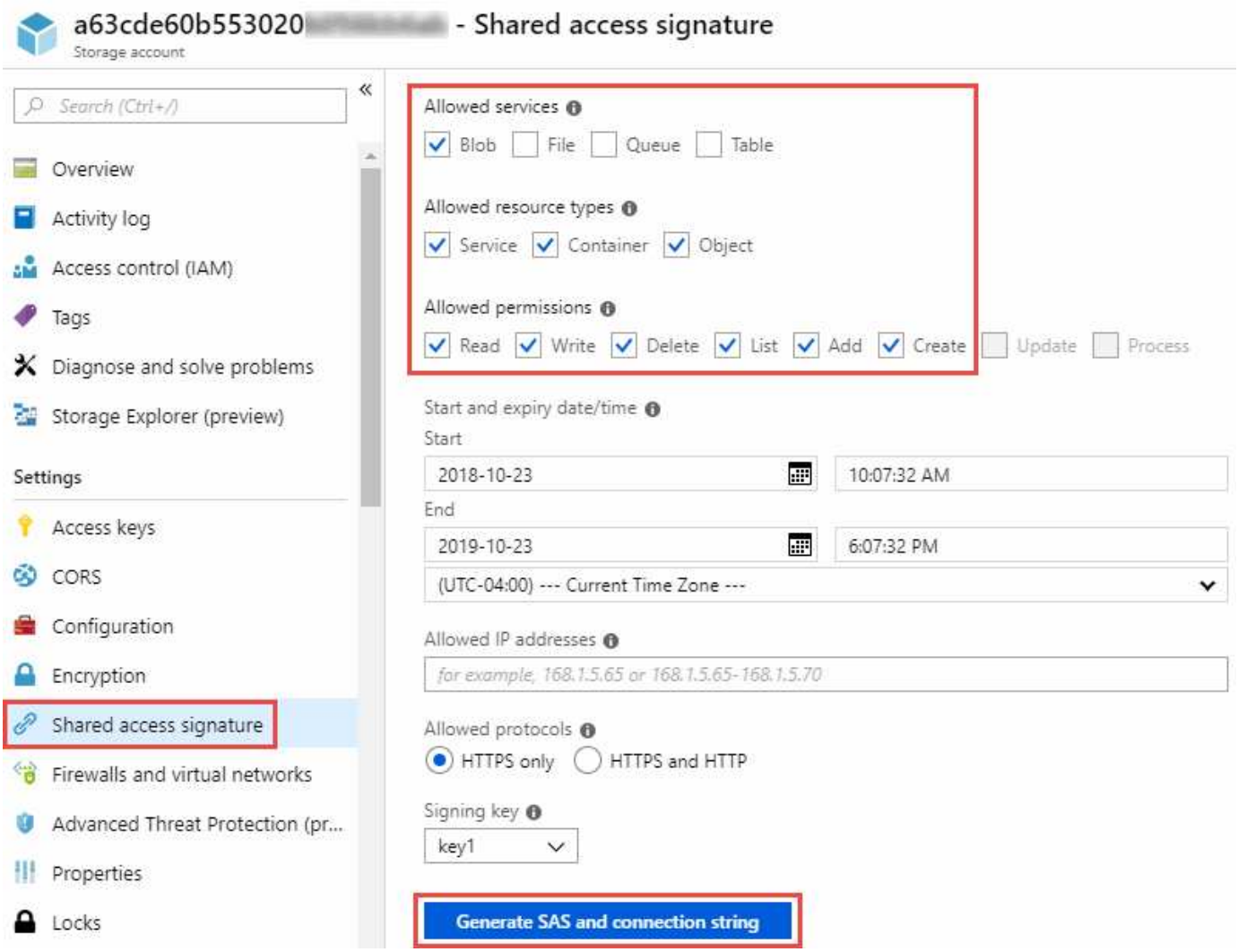


Se si desidera sincronizzare i dati tra due contenitori Azure Blob, la stringa di connessione deve includere un "firma di accesso condivisa" (SAS). È inoltre possibile utilizzare un SAS durante la sincronizzazione tra un container Blob e un server NFS o SMB.

Il SAS deve consentire l'accesso al servizio Blob e a tutti i tipi di risorse (Servizio, container e oggetto). Il SAS deve includere anche le seguenti autorizzazioni:

- Per il contenitore Blob di origine: Read and List (lettura ed elenco)

- Per il contenitore Blob di destinazione: Lettura, scrittura, elenco, Aggiungi e Crea



Requisito Azure NetApp Files

Utilizzare il livello di servizio Premium o Ultra quando si sincronizzano i dati da o verso Azure NetApp Files. Se il livello di servizio del disco è Standard, potrebbero verificarsi errori e problemi di performance.

Se hai bisogno di aiuto per determinare il livello di servizio giusto, consulta un Solutions Architect. Le dimensioni del volume e il Tier del volume determinano il throughput che è possibile ottenere.

"Scopri di più sui livelli di servizio e sul throughput di Azure NetApp Files".

Requisiti del bucket di storage Google Cloud

Assicurati che il tuo bucket di storage Google Cloud soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per Google Cloud Storage

Le relazioni di sincronizzazione che includono Google Cloud Storage richiedono un broker di dati implementato in GCP o on-premise. Cloud Sync ti guida nel processo di installazione del data broker quando crei una relazione di sincronizzazione.

- "Scopri come implementare il data broker GCP"
- "Scopri come installare il data broker su un host Linux"

Regioni GCP supportate

Sono supportate tutte le regioni.

Requisiti del server NFS

- Il server NFS può essere un sistema NetApp o un sistema non NetApp.
- Il file server deve consentire all'host del data broker di accedere alle esportazioni.
- Sono supportate le versioni 3, 4.0, 4.1 e 4.2 di NFS.

  La versione desiderata deve essere abilitata sul server.

- Se si desidera sincronizzare i dati NFS da un sistema ONTAP, assicurarsi che sia abilitato l'accesso all'elenco di esportazione NFS per una SVM (vserver nfs modify -vserver *nome_svm* -showmount abilitato).

  L'impostazione predefinita per showmount è *enabled* a partire da ONTAP 9.2.

Requisiti di storage per ONTAP S3

ONTAP 9.7 supporta Amazon Simple Storage Service (Amazon S3) come anteprima pubblica. "Scopri di più sul supporto ONTAP per Amazon S3".

Quando si imposta una relazione di sincronizzazione che include lo storage ONTAP S3, è necessario fornire quanto segue:

- L'indirizzo IP del LIF connesso a ONTAP S3
- La chiave di accesso e la chiave segreta che ONTAP è configurato per utilizzare

Requisiti dei server SMB

- Il server SMB può essere un sistema NetApp o un sistema non NetApp.
- Il file server deve consentire all'host del data broker di accedere alle esportazioni.
- Sono supportate le versioni SMB 1.0, 2.0, 2.1, 3.0 e 3.11.
- Assegnare al gruppo "Administrators" le autorizzazioni "controllo completo" alle cartelle di origine e di destinazione.

  Se non si concede questa autorizzazione, il broker di dati potrebbe non disporre di autorizzazioni sufficienti per ottenere gli ACL in un file o in una directory. In questo caso, viene visualizzato il seguente errore: "Getxattr error 95"

Limitazione SMB per directory e file nascosti

Una limitazione SMB influisce sulle directory e sui file nascosti durante la sincronizzazione dei dati tra server SMB. Se una delle directory o dei file sul server SMB di origine è stata nascosta tramite Windows, l'attributo nascosto non viene copiato nel server SMB di destinazione.

Comportamento di sincronizzazione SMB dovuto a una limitazione di insensibilità ai casi

Il protocollo SMB non fa distinzione tra maiuscole e minuscole, il che significa che le lettere maiuscole e minuscole sono considerate uguali. Questo comportamento può causare errori di file sovrascritti e copia della directory, se una relazione di sincronizzazione include un server SMB e i dati sono già presenti sulla destinazione.

Ad esempio, supponiamo che vi sia un file denominato "a" sull'origine e un file denominato "A" sull'origine. Quando Cloud Sync copia il file denominato "a" nella destinazione, il file "A" viene sovrascritto dal file "a" proveniente dall'origine.

Nel caso delle directory, supponiamo che sia presente una directory denominata "b" sull'origine e una directory denominata "B" sull'origine. Quando Cloud Sync tenta di copiare la directory denominata "b" nella destinazione, Cloud Sync riceve un errore che indica che la directory esiste già. Di conseguenza, Cloud Sync non riesce sempre a copiare la directory denominata "b."

Il modo migliore per evitare questo limite è quello di garantire la sincronizzazione dei dati in una directory vuota.

Autorizzazioni per una destinazione SnapMirror

Se l'origine di una relazione di sincronizzazione è una destinazione SnapMirror (di sola lettura), le autorizzazioni di "lettura/elenco" sono sufficienti per sincronizzare i dati dall'origine a una destinazione.

Panoramica delle reti per Cloud Sync

Il networking per Cloud Sync include la connettività tra il broker di dati e le posizioni di origine e destinazione e una connessione Internet in uscita dal broker di dati sulla porta 443.

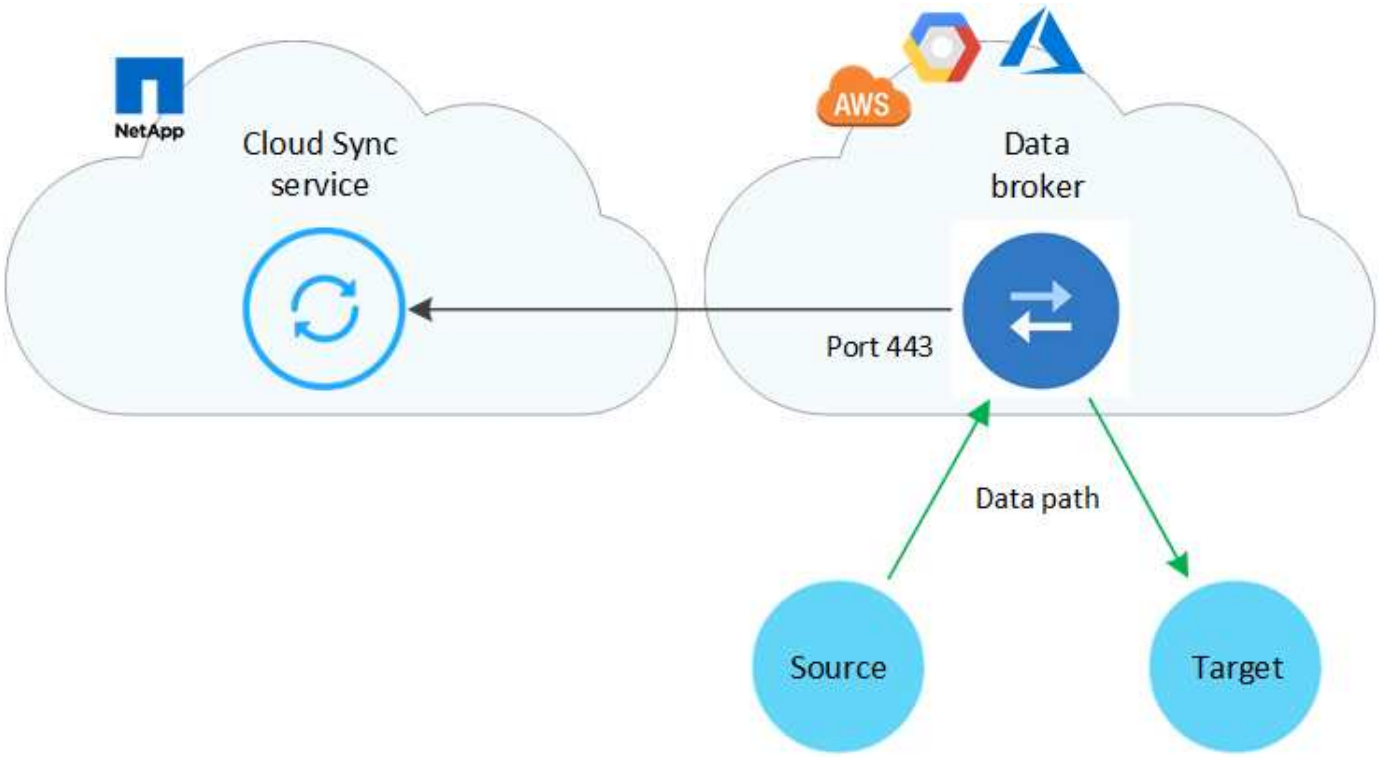
Posizione del data broker

Puoi installare il data broker nel cloud o on-premise.

Broker di dati nel cloud

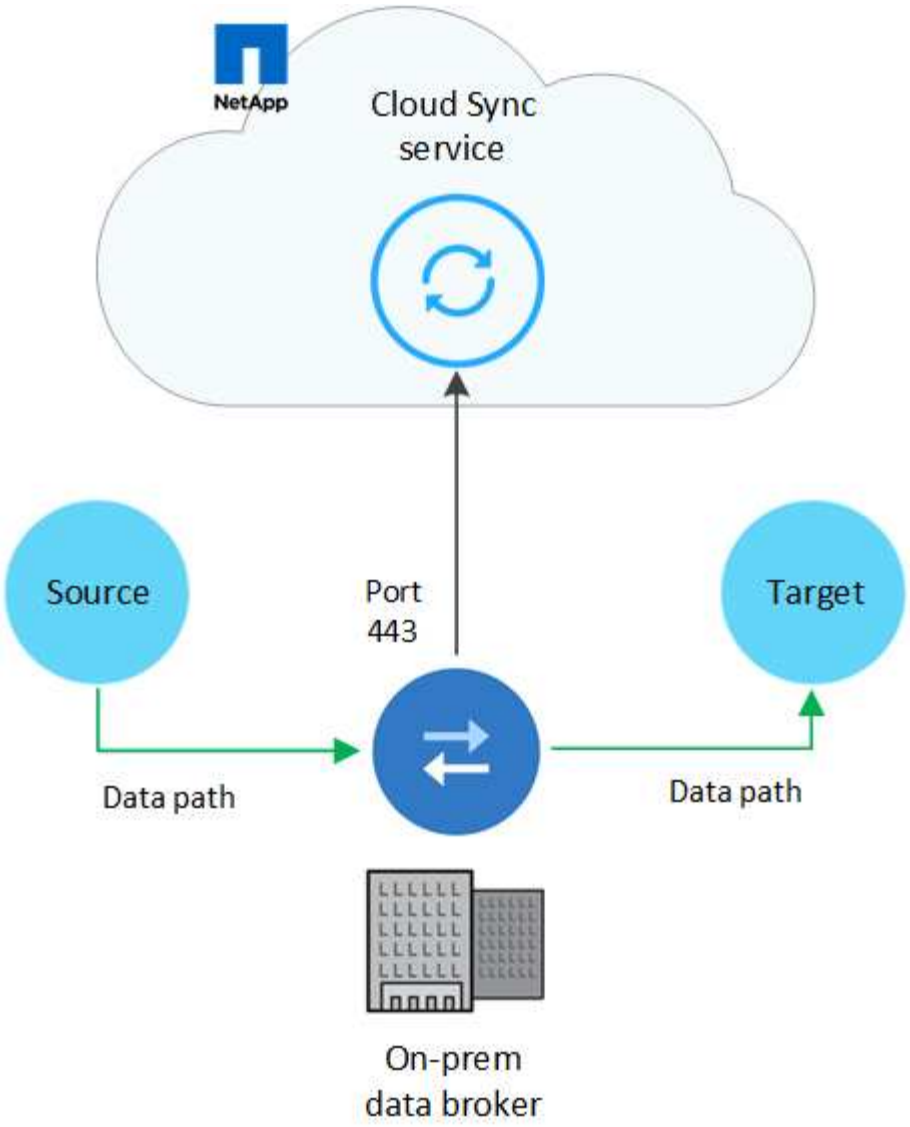
L'immagine seguente mostra il data broker in esecuzione nel cloud, in AWS, GCP o Azure. L'origine e la destinazione possono trovarsi in qualsiasi posizione, a condizione che vi sia una connessione al data broker. Ad esempio, è possibile che si disponga di una connessione VPN dal data center al cloud provider.

Quando Cloud Sync implementa il data broker in AWS, Azure o GCP, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.



Broker di dati on-premise

La seguente immagine mostra il data broker in esecuzione on-premise in un data center. Anche in questo caso, l'origine e la destinazione possono trovarsi in qualsiasi posizione, a condizione che vi sia una connessione al data broker.



Requisiti di rete

- L'origine e la destinazione devono disporre di una connessione di rete al data broker.

  Ad esempio, se un server NFS si trova nel data center e il data broker si trova in AWS, è necessaria una connessione di rete (VPN o Direct Connect) dalla rete al VPC.

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio Cloud Sync per le attività sulla porta 443.
- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Endpoint di rete

Il data broker NetApp richiede l'accesso a Internet in uscita tramite la porta 443 per comunicare con il servizio Cloud Sync e per contattare altri servizi e repository. Il browser Web locale richiede inoltre l'accesso agli endpoint per determinate azioni. Per limitare la connettività in uscita, fare riferimento al seguente elenco di endpoint durante la configurazione del firewall per il traffico in uscita.

Endpoint del data broker

Il data broker contatta i seguenti endpoint:

Endpoint	Scopo
olcentgbl.trafficmanager.net:443	Per contattare un repository per l'aggiornamento dei pacchetti CentOS per l'host del data broker. Questo endpoint viene contattato solo se si installa manualmente il data broker su un host CentOS.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Per contattare i repository per l'aggiornamento di Node.js, npm e altri pacchetti di terze parti utilizzati nello sviluppo.
tgz.pm2.io:443	Per accedere a un repository per l'aggiornamento di PM2, un pacchetto di terze parti utilizzato per monitorare Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Per contattare i servizi AWS utilizzati da Cloud Sync per le operazioni (accodamento di file, registrazione di azioni e invio di aggiornamenti al data broker).
s3.*region*.amazonaws.com:443 ad esempio: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Per un elenco degli endpoint S3, consultare la documentazione di AWS"^]	Per contattare Amazon S3 quando una relazione di sincronizzazione include un bucket S3.
cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Per contattare il servizio Cloud Sync.
support.netapp.com:443	Per contattare il supporto NetApp quando si utilizza una licenza BYOL per le relazioni di sincronizzazione.
fedoraproject.org:443	Per installare 7z sulla macchina virtuale del data broker durante l'installazione e gli aggiornamenti. 7z è necessario per inviare messaggi AutoSupport al supporto tecnico NetApp.

Endpoint del browser Web

Il browser Web deve accedere al seguente endpoint per scaricare i registri a scopo di risoluzione dei problemi:

logs.cloudsync.netapp.com:443

Come installare un data broker

Installazione del data broker in AWS

Quando si crea una relazione di sincronizzazione, scegliere l'opzione AWS Data Broker per implementare il software del data broker su una nuova istanza EC2 in un VPC. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. "Scopri di più".

Regioni AWS supportate

Tutte le regioni sono supportate, ad eccezione di quelle della Cina e di GovCloud (USA).

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio Cloud Sync per le attività sulla porta 443.

  Quando Cloud Sync implementa il data broker in AWS, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta. Nota: È possibile configurare il data broker per l'utilizzo di un server proxy durante il processo di installazione.

  Per limitare la connettività in uscita, vedere "l'elenco degli endpoint a cui il data broker contatta".

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Autorizzazioni necessarie per implementare il data broker in AWS

L'account utente AWS utilizzato per implementare il data broker deve disporre delle autorizzazioni incluse in "Questa policy fornita da NetApp".

requisiti per utilizzare il tuo ruolo IAM con il data broker AWS

Quando Cloud Sync implementa il data broker, crea un ruolo IAM per l'istanza del data broker. Se preferisci, puoi implementare il data broker utilizzando il tuo ruolo IAM. È possibile utilizzare questa opzione se l'organizzazione dispone di policy di sicurezza rigorose.

Il ruolo IAM deve soddisfare i seguenti requisiti:

- Il servizio EC2 deve essere autorizzato ad assumere il ruolo di IAM come entità attendibile.
- "Le autorizzazioni definite in questo file JSON" Deve essere associato al ruolo IAM in modo che il data broker possa funzionare correttamente.

Seguire i passaggi riportati di seguito per specificare il ruolo IAM durante l'implementazione del data broker.

Installazione del data broker

È possibile installare un data broker in AWS quando si crea una relazione di sincronizzazione.

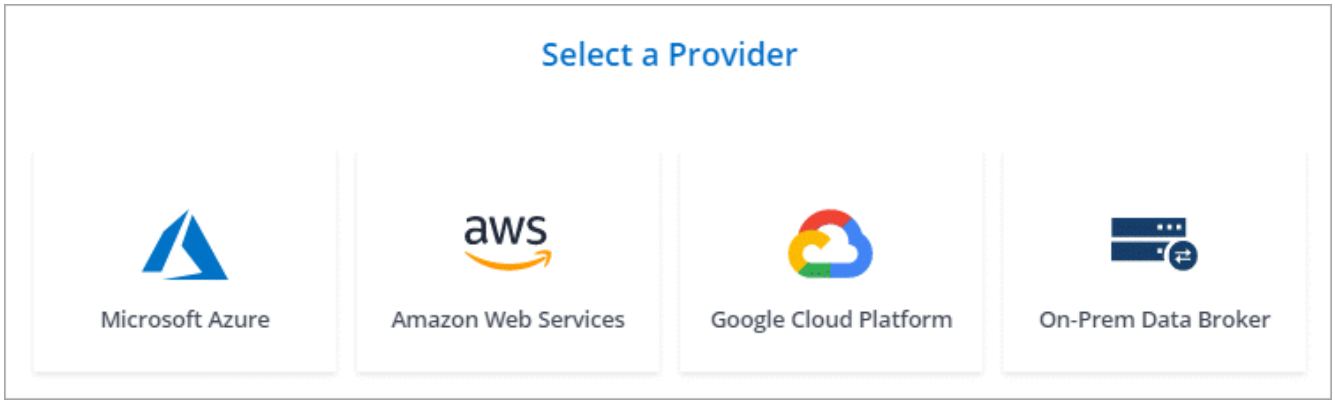
Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

   Completa i passaggi fino a raggiungere la pagina **Data Broker**.

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Amazon Web Services**.

   Se disponi già di un data broker, dovrai fare clic su  prima icona.



4. Immettere un nome per il broker di dati e fare clic su **continua**.
5. Immettere una chiave di accesso AWS in modo che Cloud Sync possa creare il data broker in AWS per conto dell'utente.

   Le chiavi non vengono salvate o utilizzate per altri scopi.

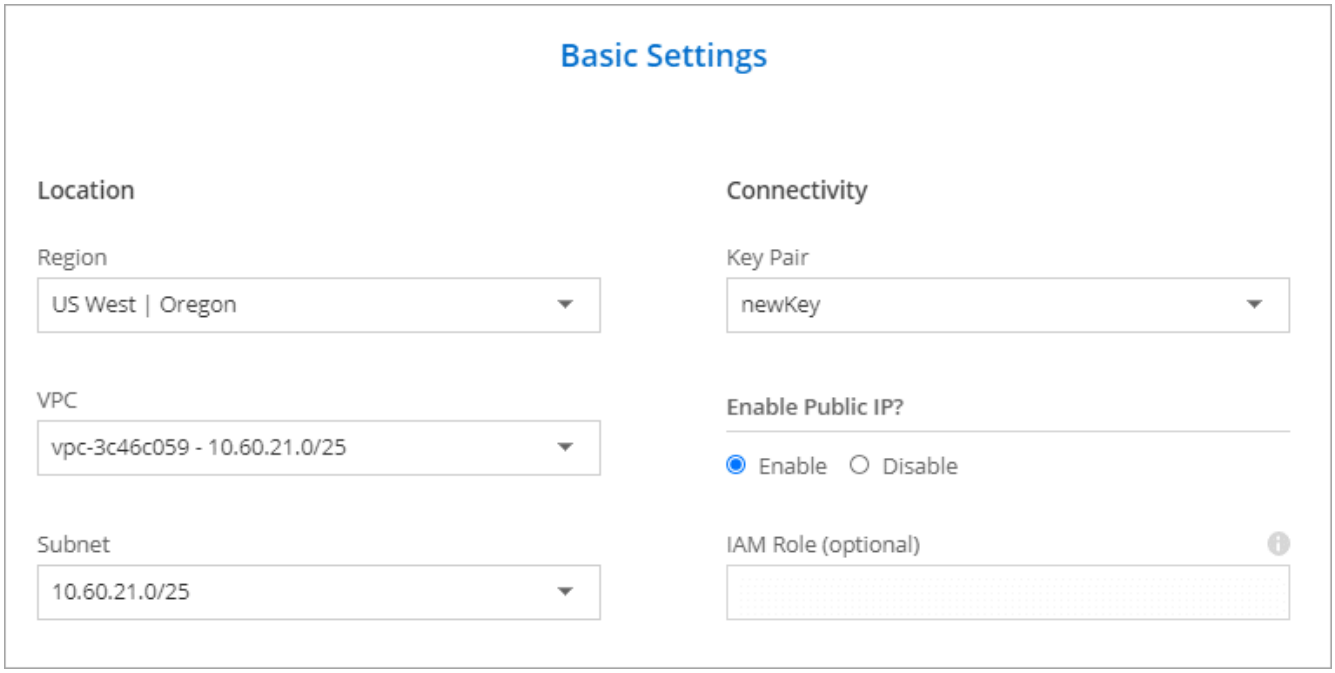
   Se invece non si desidera fornire le chiavi di accesso, fare clic sul collegamento in fondo alla pagina per utilizzare un modello CloudFormation. Quando si utilizza questa opzione, non è necessario fornire le credenziali perché si effettua l'accesso direttamente ad AWS.

   il seguente video mostra come avviare l'istanza del data broker utilizzando un modello CloudFormation:

   ► https://docs.netapp.com/it-it/occm38//media/video_cloud_sync.mp4 *(video)*

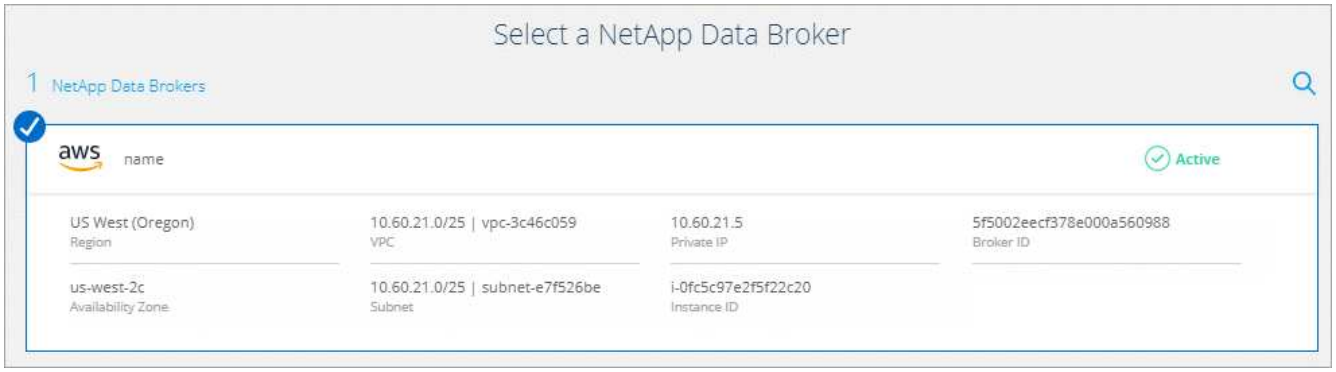
6. Se è stata immessa una chiave di accesso AWS, selezionare una posizione per l'istanza, selezionare una coppia di chiavi, scegliere se attivare un indirizzo IP pubblico, quindi selezionare un ruolo IAM esistente oppure lasciare vuoto il campo in modo che Cloud Sync crei il ruolo.

   Se scegli il tuo ruolo IAM, è necessario fornire le autorizzazioni necessarie.



7. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.

L'immagine seguente mostra un'istanza implementata correttamente in AWS:



8. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

Risultato

Hai implementato un data broker in AWS e creato una nuova relazione di sincronizzazione. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

Installazione del data broker in Azure

Quando si crea una relazione di sincronizzazione, scegliere l'opzione Azure Data Broker per implementare il software del data broker su una nuova macchina virtuale in una VNET. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. "Scopri di più".

Aree Azure supportate

Sono supportate tutte le regioni, ad eccezione di quelle della Cina, degli Stati Uniti e del DOD.

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio Cloud Sync per le attività sulla porta 443.

  Quando Cloud Sync implementa il data broker in Azure, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.

  Per limitare la connettività in uscita, vedere "l'elenco degli endpoint a cui il data broker contatta".

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Metodo di autenticazione

Quando si implementa il data broker, è necessario scegliere un metodo di autenticazione: Una password o una coppia di chiavi SSH pubblico-privato.

Per informazioni sulla creazione di una coppia di chiavi, fare riferimento a. "Documentazione di Azure: Creare e utilizzare una coppia di chiavi SSH pubblico-privato per macchine virtuali Linux in Azure".

Installazione del data broker

È possibile installare un data broker in Azure quando si crea una relazione di sincronizzazione.

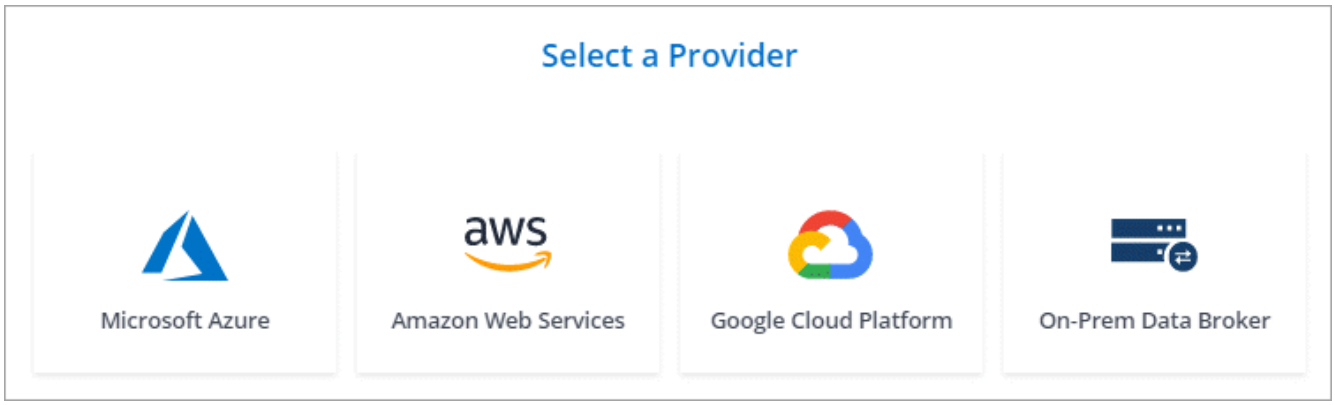
Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

   Completa le pagine fino a raggiungere la pagina **Data Broker**.

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Microsoft Azure**.

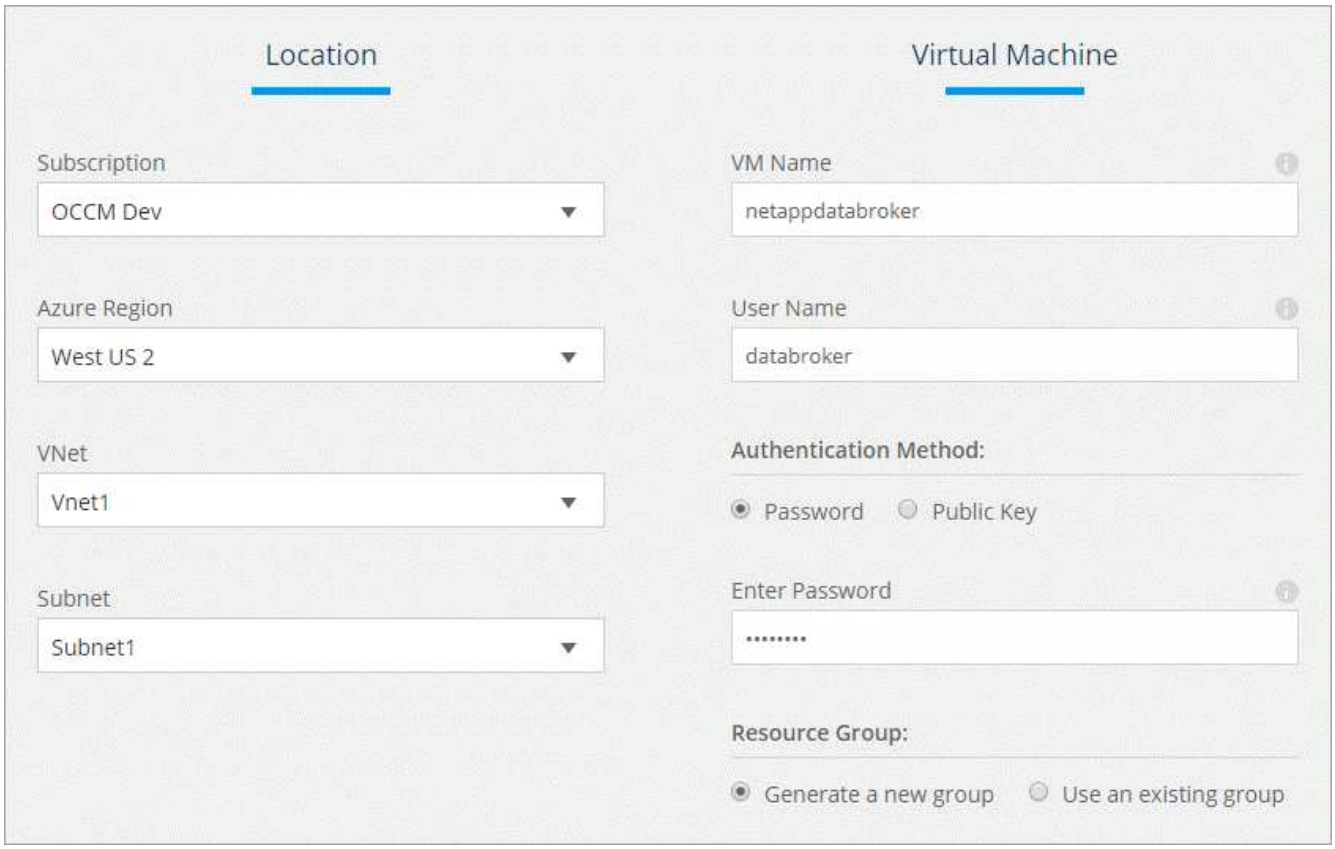
   Se disponi già di un data broker, dovrai fare clic su + prima icona.



4. Immettere un nome per il broker di dati e fare clic su **continua**.
5. Se richiesto, accedere all'account Microsoft. Se non viene richiesto, fare clic su **Accedi ad Azure**.

   Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.

6. Scegliere una posizione per il data broker e inserire i dettagli di base sulla macchina virtuale.



7. Fare clic su **Continue** (continua) e mantenere aperta la pagina fino al completamento dell'implementazione.

   Il processo può richiedere fino a 7 minuti.

8. In Cloud Sync, fare clic su **Continue** una volta che il data broker è disponibile.
9. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

Risultato

Hai implementato un data broker in Azure e creato una nuova relazione di sincronizzazione. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

Viene visualizzato un messaggio che richiede il consenso dell'amministratore?

Se Microsoft notifica che è richiesta l'approvazione dell'amministratore perché Cloud Sync ha bisogno dell'autorizzazione per accedere alle risorse dell'organizzazione per conto dell'utente, sono disponibili due opzioni:

1. Chiedi all'amministratore di ad di fornirti le seguenti autorizzazioni:

   In Azure, accedere a **Admin Center > Azure ad > utenti e gruppi > Impostazioni utente** e abilitare **gli utenti possono autorizzare le applicazioni ad accedere ai dati aziendali per loro conto**.

2. Chiedi al tuo amministratore di ad di acconsentire a **CloudSync-AzureDataBrokerCreator** utilizzando il seguente URL (questo è l'endpoint di consenso dell'amministratore):

   https://login.microsoftonline.com/{FILL QUI IL tuo ID TENANT}/v2.0/adminassenso?client_id=8e4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Come mostrato nell'URL, l'URL dell'applicazione è https://cloudsync.netapp.com e l'ID del client dell'applicazione è 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Installazione del data broker in Google Cloud Platform

Quando si crea una relazione di sincronizzazione, scegliere l'opzione GCP Data Broker per implementare il software del data broker su una nuova istanza di macchina virtuale in un VPC. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. "Scopri di più".

Regioni GCP supportate

Sono supportate tutte le regioni.

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio Cloud Sync per le attività sulla porta 443.

  Quando Cloud Sync implementa il data broker in GCP, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.

  Per limitare la connettività in uscita, vedere "l'elenco degli endpoint a cui il data broker contatta".

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Autorizzazioni necessarie per implementare il data broker in GCP

Assicurarsi che l'utente GCP che implementa il data broker disponga delle seguenti autorizzazioni:

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Autorizzazioni richieste per l'account del servizio

Quando si implementa il data broker, è necessario selezionare un account di servizio che disponga delle seguenti autorizzazioni:

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Installazione del data broker

È possibile installare un data broker in GCP quando si crea una relazione di sincronizzazione.

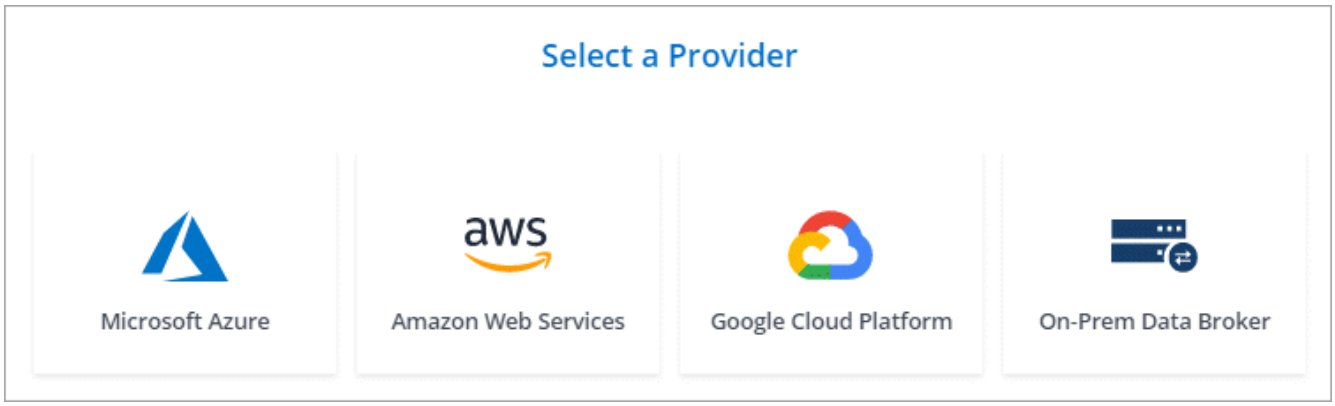
Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

   Completa i passaggi fino a raggiungere la pagina **Data Broker**.

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Google Cloud Platform**.

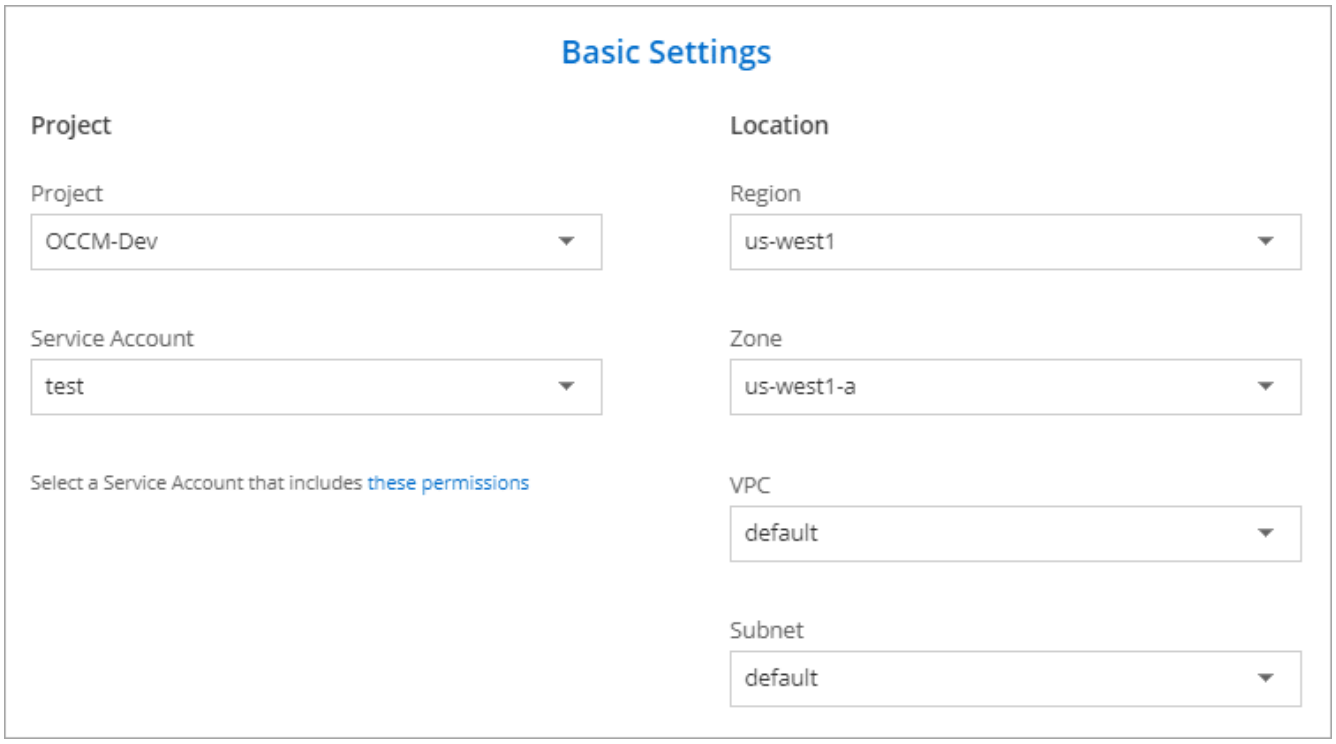
   Se disponi già di un data broker, dovrai fare clic su + prima icona.



4. Immettere un nome per il broker di dati e fare clic su **continua**.
5. Se richiesto, accedere con l'account Google.

   Il modulo è di proprietà e ospitato da Google. Le tue credenziali non vengono fornite a NetApp.

6. Selezionare un account di progetto e servizio, quindi scegliere una posizione per il data broker.



7. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.

   L'implementazione dell'istanza richiede da 5 a 10 minuti circa. È possibile monitorare l'avanzamento del servizio Cloud Sync, che si aggiorna automaticamente quando l'istanza è disponibile.

8. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

Risultato

Hai implementato un data broker in GCP e creato una nuova relazione di sincronizzazione. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

Installazione del data broker su un host Linux

Quando crei una relazione di sincronizzazione, scegli l'opzione on-Prem Data Broker per installare il software data broker su un host Linux on-premise o su un host Linux esistente nel cloud. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

Requisiti degli host Linux

- **Sistema operativo**:

- CentOS 7.0, 7.7 e 8.0
- Red Hat Enterprise Linux 7.7 e 8.0
- Ubuntu Server 18.04 LTS
- SUSE Linux Enterprise Server 15 SP1

  Il comando `yum update all` deve essere eseguito sull'host prima di installare il data broker.

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.

- **RAM**: 16 GB
- **CPU**: 4 core
- **Spazio libero su disco**: 10 GB
- **SELinux**: Si consiglia di disattivarlo "SELinux" sull'host.

  SELinux applica una policy che blocca gli aggiornamenti del software del data broker e impedisce al data broker di contattare gli endpoint necessari per il normale funzionamento.

- **OpenSSL**: OpenSSL deve essere installato sull'host Linux.

Requisiti di rete

- L'host Linux deve disporre di una connessione all'origine e alla destinazione.
- Il file server deve consentire all'host Linux di accedere alle esportazioni.
- La porta 443 deve essere aperta sull'host Linux per il traffico in uscita verso AWS (il data broker comunica costantemente con il servizio Amazon SQS).
- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Abilitazione dell'accesso ad AWS

Se si prevede di utilizzare il data broker con una relazione di sincronizzazione che include un bucket S3, è necessario preparare l'host Linux per l'accesso AWS. Quando si installa il data broker, è necessario fornire le chiavi AWS per un utente AWS che dispone di un accesso programmatico e di autorizzazioni specifiche.

Fasi

1. Creare un criterio IAM utilizzando "Questa policy fornita da NetApp". "Visualizzare le istruzioni AWS".
2. Creare un utente IAM con accesso programmatico. "Visualizzare le istruzioni AWS".

   Assicurarsi di copiare le chiavi AWS perché è necessario specificarle quando si installa il software data broker.

Abilitazione dell'accesso a Google Cloud

Se si prevede di utilizzare il data broker con una relazione di sincronizzazione che include un bucket di storage Google Cloud, è necessario preparare l'host Linux per l'accesso GCP. Quando si installa il data broker, è necessario fornire una chiave per un account di servizio che dispone di autorizzazioni specifiche.

Fasi

1. Creare un account di servizio GCP con autorizzazioni Storage Admin, se non ne hai già uno.
2. Creare una chiave dell'account di servizio salvata in formato JSON. "Visualizzare le istruzioni GCP".

   Il file deve contenere almeno le seguenti proprietà: "Project_id", "private_key" e "client_email"

   Quando si crea una chiave, il file viene generato e scaricato sul computer.

3. Salvare il file JSON nell'host Linux.

Abilitazione dell'accesso a Microsoft Azure

L'accesso ad Azure viene definito in base alla relazione fornendo un account di storage e una stringa di connessione nella procedura guidata delle relazioni di sincronizzazione.

Installazione del data broker

È possibile installare un data broker su un host Linux quando si crea una relazione di sincronizzazione.

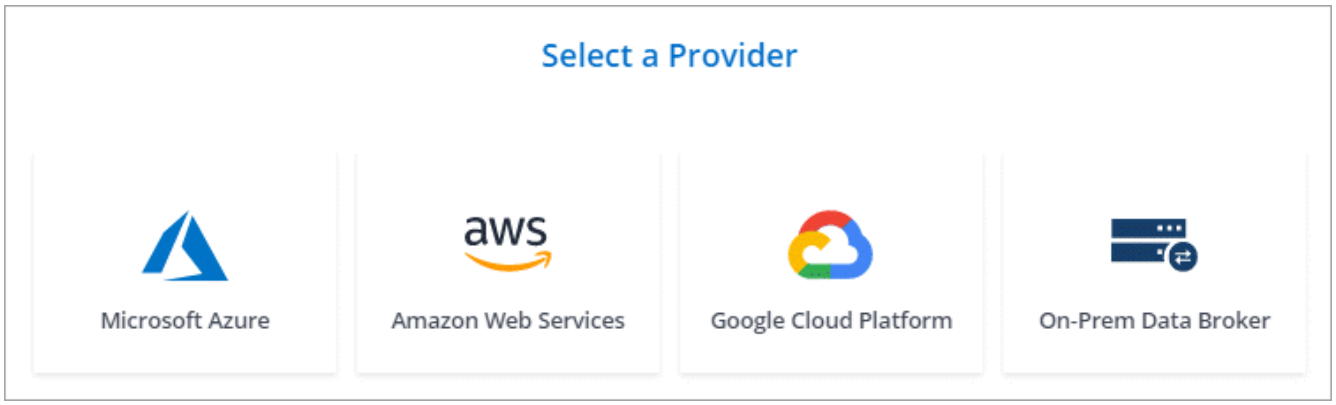
Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

   Completa i passaggi fino a raggiungere la pagina **Data Broker**.

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **on-Prem Data Broker**.

   Se disponi già di un data broker, dovrai fare clic su + prima icona.



   Anche se l'opzione è denominata ***on-Prem*** **Data Broker**, si applica a un host Linux on-premise o nel cloud.

4. Immettere un nome per il broker di dati e fare clic su **continua**.

   La pagina delle istruzioni viene caricata a breve. È necessario seguire queste istruzioni, che includono un link univoco per scaricare il programma di installazione.

5. Nella pagina delle istruzioni:
   a. Selezionare se attivare l'accesso a **AWS**, **Google Cloud** o entrambi.

b. Selezionare un'opzione di installazione: **Nessun proxy**, **Usa server proxy** o **Usa server proxy con autenticazione**.

c. Utilizzare i comandi per scaricare e installare il data broker.

   I seguenti passaggi forniscono dettagli su ciascuna opzione di installazione possibile. Seguire la pagina delle istruzioni per ottenere il comando esatto in base all'opzione di installazione.

d. Scaricare il programma di installazione:

   - Nessun proxy:

     ```
     curl <URI> -o data_broker_installer.sh
     ```

   - USA server proxy:

     ```
     curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
     ```

   - USA server proxy con autenticazione:

     ```
     curl <URI> -o data_broker_installer.sh -x
     <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
     ```

     URI

     Cloud Sync visualizza l'URI del file di installazione nella pagina delle istruzioni, che viene caricato quando si seguono le istruzioni per implementare il Data Broker on-Prem. L'URI non viene ripetuto in questo caso perché il collegamento viene generato dinamicamente e può essere utilizzato una sola volta. Per ottenere l'URI da Cloud Sync, procedere come segue.

e. Passare a superuser, rendere eseguibile il programma di installazione e installare il software:

   Ciascun comando elencato di seguito include i parametri per l'accesso AWS e GCP. Seguire la pagina delle istruzioni per ottenere il comando esatto in base all'opzione di installazione.

   - Nessuna configurazione proxy:

     ```
     sudo -s
     chmod +x data_broker_installer.sh
     ./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
     <absolute_path_to_the_json_file>
     ```

   - Configurazione del proxy:

     ```
     sudo -s
     chmod +x data_broker_installer.sh
     ./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
     <absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
     ```

   - Configurazione del proxy con autenticazione:

     ```
     sudo -s
     chmod +x data_broker_installer.sh
     ./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
     ```

```
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Tasti AWS

Queste sono le chiavi per l'utente che si dovrebbe aver preparato seguire questa procedura. Le chiavi AWS vengono memorizzate nel data broker, che viene eseguito nella rete on-premise o cloud. NetApp non utilizza le chiavi esterne al data broker.

File JSON

Si tratta del file JSON che contiene una chiave dell'account di servizio che si dovrebbe preparare seguire questa procedura.

6. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.
7. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

Creazione di una relazione di sincronizzazione

Quando si crea una relazione di sincronizzazione, il servizio Cloud Sync copia i file dall'origine alla destinazione. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore.

I passaggi riportati di seguito forniscono un esempio che mostra come impostare una relazione di sincronizzazione da un server NFS a un bucket S3.

Fasi

1. In Cloud Manager, fare clic su **Sync**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione.

   I passaggi seguenti forniscono un esempio di come creare una relazione di sincronizzazione da un server NFS a un bucket S3.

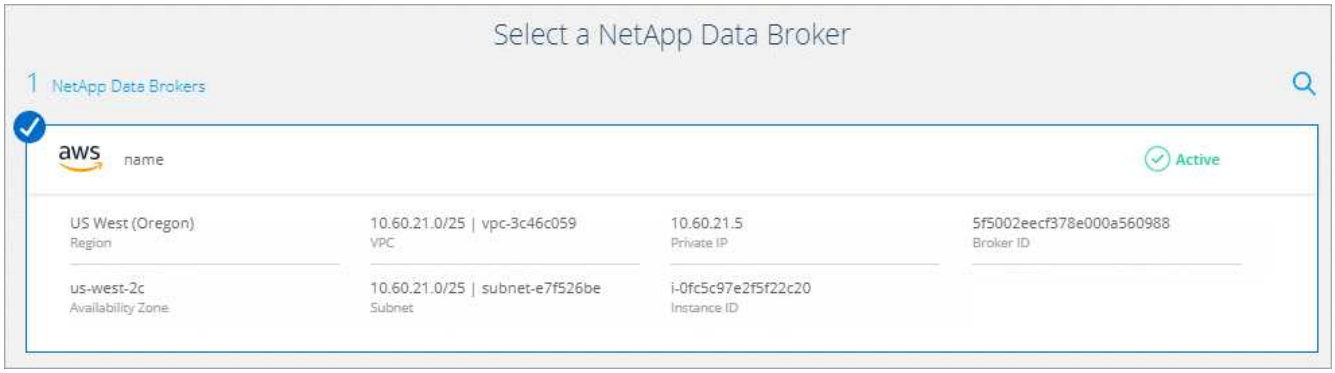
3. Nella pagina **NFS Server**, inserire l'indirizzo IP o il nome di dominio completo del server NFS che si desidera sincronizzare con AWS.
4. Nella pagina **Data Broker**, seguire le istruzioni per creare una macchina virtuale per il data broker in AWS, Azure o Google Cloud Platform, oppure per installare il software per il data broker su un host Linux esistente.

   Per ulteriori informazioni, consultare le seguenti pagine:

- "Installazione del data broker in AWS"
- "Installazione del data broker in Azure"
- "Installazione del data broker in GCP"
- "Installazione del data broker su un host Linux"

5. Dopo aver installato il data broker, fare clic su **Continue** (continua).

   La seguente immagine mostra un data broker implementato correttamente in AWS:

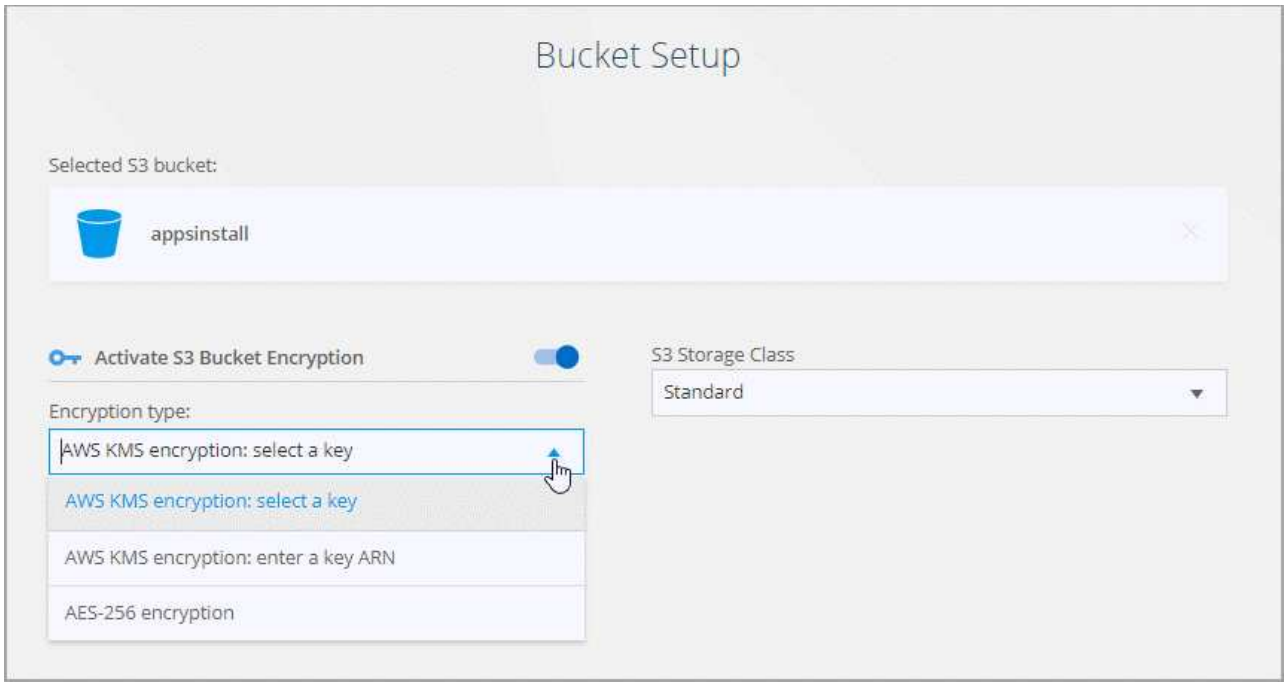


6. nella pagina **Directory**, selezionare una directory o una sottodirectory di livello superiore.

   Se Cloud Sync non riesce a recuperare le esportazioni, fare clic su **Aggiungi esportazione manualmente** e immettere il nome di un'esportazione NFS.

   Se si desidera sincronizzare più di una directory sul server NFS, è necessario creare ulteriori relazioni di sincronizzazione al termine dell'operazione.

7. Nella pagina **bucket AWS S3**, selezionare un bucket:
   - Eseguire il drill-down per selezionare una cartella esistente all'interno del bucket o per selezionare una nuova cartella creata all'interno del bucket.
   - Fare clic su **Aggiungi all'elenco** per selezionare un bucket S3 non associato all'account AWS. "Al bucket S3 devono essere applicate autorizzazioni specifiche".
8. Nella pagina **Bucket Setup**, impostare il bucket:
   - Scegliere se attivare la crittografia del bucket S3, quindi selezionare una chiave AWS KMS, immettere l'ARN di una chiave KMS o selezionare la crittografia AES-256.
   - Selezionare una classe di storage S3. "Visualizzare le classi di storage supportate".



9. Nella pagina **Impostazioni**, definire la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione:

Pianificazione

Scegliere una pianificazione ricorrente per le sincronizzazioni future o disattivare la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

Tentativi

Definire il numero di tentativi di sincronizzazione di un file da parte di Cloud Sync prima di ignorarlo.

File modificati di recente

Scegliere di escludere i file modificati di recente prima della sincronizzazione pianificata.

Elimina file in origine

Scegliere di eliminare i file dalla posizione di origine dopo che Cloud Sync copia i file nella posizione di destinazione. Questa opzione include il rischio di perdita dei dati perché i file di origine vengono cancellati dopo la copia.

Se si attiva questa opzione, è necessario modificare anche un parametro nel file local.json sul data broker. Aprire il file e modificare il parametro denominato *workers.transferrer.delete-on-source* in **true**.

Eliminare i file di destinazione

Scegliere di eliminare i file dalla posizione di destinazione, se sono stati eliminati dall'origine. Per impostazione predefinita, non elimina mai i file dalla posizione di destinazione.

Tagging degli oggetti

Quando AWS S3 è la destinazione in una relazione di sincronizzazione, Cloud Sync contrassegna gli oggetti S3 con metadati rilevanti per l'operazione di sincronizzazione. È possibile disattivare la tagging degli oggetti S3, se non si desidera, nell'ambiente in uso. La disattivazione del tagging non ha alcun impatto su Cloud Sync: Cloud Sync memorizza i metadati di sincronizzazione in un modo diverso.

Tipi di file

Definire i tipi di file da includere in ogni sincronizzazione: File, directory e collegamenti simbolici.

Escludi estensioni file

Specificare le estensioni dei file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file *.log. Non è necessario un separatore per più interni. Il seguente video fornisce una breve demo:

► https://docs.netapp.com/it-it/occm38//media/video_file_extensions.mp4 *(video)*

Dimensione del file

Scegliere di sincronizzare tutti i file indipendentemente dalle dimensioni o solo i file che si trovano in un intervallo di dimensioni specifico.

Data di modifica

Scegliere tutti i file indipendentemente dalla data dell'ultima modifica, i file modificati dopo una data specifica, prima di una data specifica o tra un intervallo di tempo.

10. Nella pagina **Relationship Tags**, inserire fino a 9 tag di relazione, quindi fare clic su **Continue**.

    Il servizio Cloud Sync assegna i tag a ciascun oggetto sincronizzato con il bucket S3.

11. Esaminare i dettagli della relazione di sincronizzazione, quindi fare clic su **Crea relazione**.

Risultato

Cloud Sync avvia la sincronizzazione dei dati tra l'origine e la destinazione.

Pagamento delle relazioni di sincronizzazione al termine della prova gratuita

Esistono due modi per pagare le relazioni di sincronizzazione dopo la fine della prova gratuita di 14 giorni. La prima opzione consiste nell'abbonarsi ad AWS o Azure per il pagamento a consumo o per il pagamento annuale. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp.

È possibile utilizzare le licenze di NetApp con un abbonamento AWS o Azure. Ad esempio, se si dispone di 25 relazioni di sincronizzazione, è possibile pagare le prime 20 relazioni di sincronizzazione utilizzando una licenza e quindi pagare a consumo da AWS o Azure con le restanti 5 relazioni di sincronizzazione.

"Scopri di più sul funzionamento delle licenze".

Cosa succede se non pago 8217 immediatamente dopo la fine della prova gratuita?

Non sarà possibile creare relazioni aggiuntive. Le relazioni esistenti non vengono eliminate, ma non è possibile apportare modifiche fino a quando non si sottoscrive o si inserisce una licenza.

sottoscrizione da AWS

AWS ti consente di pagare a consumo o di pagare annualmente.

Procedura per il pagamento a consumo

1. Fare clic su **Sync > Licensing**.

2. Selezionare **AWS**
3. Fare clic su **Iscriviti**, quindi su **continua**.
4. Iscriviti al marketplace AWS, quindi accedi nuovamente al servizio Cloud Sync per completare la registrazione.

   Il seguente video mostra il processo:

   ► https://docs.netapp.com/it-it/occm38//media/video_cloud_sync_registering.mp4 *(video)*

Passi da pagare annualmente

1. "Accedere alla pagina AWS Marketplace".
2. Fare clic su **continua per iscriversi**.
3. Selezionare le opzioni del contratto e fare clic su **Crea contratto**.

sottoscrizione a Azure

Azure ti consente di pagare in base alle tue esigenze o di pagare ogni anno.

Di cosa hai bisogno

Un account utente Azure che dispone delle autorizzazioni Contributor o Owner nell'abbonamento pertinente.

Fasi

1. Fare clic su **Sync > Licensing**.
2. Selezionare **Azure**.
3. Fare clic su **Iscriviti**, quindi su **continua**.
4. Nel portale Azure, fare clic su **Create**, selezionare le opzioni e fare clic su **Subscribe**.

   Seleziona **mensile** per pagare in base all'ora o **annuale** per pagare in anticipo un anno.

5. Una volta completata l'implementazione, fare clic sul nome della risorsa SaaS nella finestra a comparsa di notifica.
6. Fare clic su **Configura account** per tornare a Cloud Sync.

   Il seguente video mostra il processo:

   ► https://docs.netapp.com/it-it/occm38//media/video_cloud_sync_registering_azure.mp4 *(video)*

Acquisto di licenze NetApp e aggiunta a Cloud Sync

Per pagare anticipatamente le relazioni di sincronizzazione, è necessario acquistare una o più licenze e aggiungerle al servizio Cloud Sync.

Fasi

1. Acquista una licenza inviando un messaggio di posta:ng-cloudsync-contact@netapp.com?subject=Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request[come contattare NetApp].
2. In Cloud Manager, fare clic su **Sync > Licensing**.
3. Fare clic su **Add License** (Aggiungi licenza) e aggiungere la licenza.

Tutorial

Copia degli ACL tra le condivisioni SMB

Cloud Sync può copiare gli elenchi di controllo degli accessi (ACL) tra una condivisione SMB di origine e una condivisione SMB di destinazione. Se necessario, è possibile conservare manualmente gli ACL utilizzando robocopy.

Scelte

- Impostare Cloud Sync per la copia automatica degli ACL
- Copiare manualmente gli ACL

Configurazione di Cloud Sync per copiare gli ACL tra server SMB

Copiare gli ACL tra server SMB attivando un'impostazione quando si crea una relazione o dopo la creazione di una relazione.

Questa funzionalità è disponibile per le nuove relazioni di sincronizzazione create dopo la release 23 febbraio 2020. Se si desidera utilizzare questa funzione con le relazioni esistenti create prima di tale data, sarà necessario ricreare la relazione.

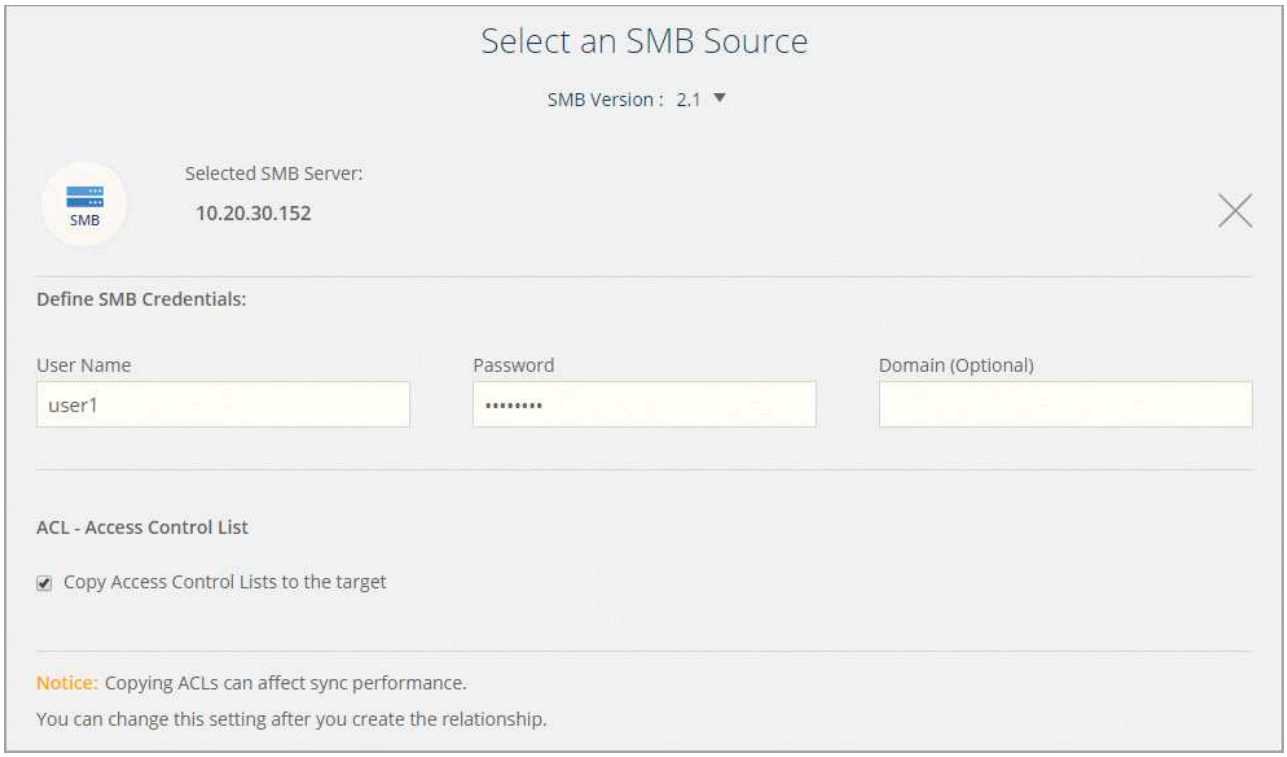
Di cosa hai bisogno

- Una nuova relazione di sincronizzazione o una relazione di sincronizzazione esistente creata dopo la release del 23 febbraio 2020.
- Qualsiasi tipo di broker di dati.

  Questa funzionalità funziona con *qualsiasi* tipo di data broker: AWS, Azure, Google Cloud Platform o data broker on-premise. Il data broker on-premise può essere eseguito "qualsiasi sistema operativo supportato".

Passaggi per una nuova relazione

1. Da Cloud Sync, fare clic su **Crea nuova sincronizzazione**.
2. Trascinare **SMB Server** nell'origine e nella destinazione e fare clic su **Continue** (continua).
3. Nella pagina **SMB Server**:
   a. Immettere un nuovo server SMB o selezionare un server esistente e fare clic su **continua**.
   b. Immettere le credenziali per il server SMB.
   c. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione) e fare clic su **Continue** (continua).



4. Seguire le istruzioni rimanenti per creare la relazione di sincronizzazione.

Passaggi per una relazione esistente

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Impostazioni**.
3. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione).
4. Fare clic su **Save Settings** (Salva impostazioni).

Risultato

Durante la sincronizzazione dei dati, Cloud Sync preserva gli ACL tra le condivisioni SMB di origine e di destinazione.

Copia manuale degli ACL

È possibile conservare manualmente gli ACL tra le condivisioni SMB utilizzando il comando Windows robocopy.

Fasi

1. Identificare un host Windows con accesso completo a entrambe le condivisioni SMB.
2. Se uno degli endpoint richiede l'autenticazione, utilizzare il comando **net use** per connettersi agli endpoint dall'host Windows.

   Eseguire questa procedura prima di utilizzare robocopy.

3. Da Cloud Sync, creare una nuova relazione tra le condivisioni SMB di origine e di destinazione o sincronizzare una relazione esistente.
4. Una volta completata la sincronizzazione dei dati, eseguire il seguente comando dall'host Windows per sincronizzare gli ACL e la proprietà:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:"[logfilepath]
```

È necessario specificare sia *source* che *target* utilizzando il formato UNC. Ad esempio: <server>/<share>/<path>

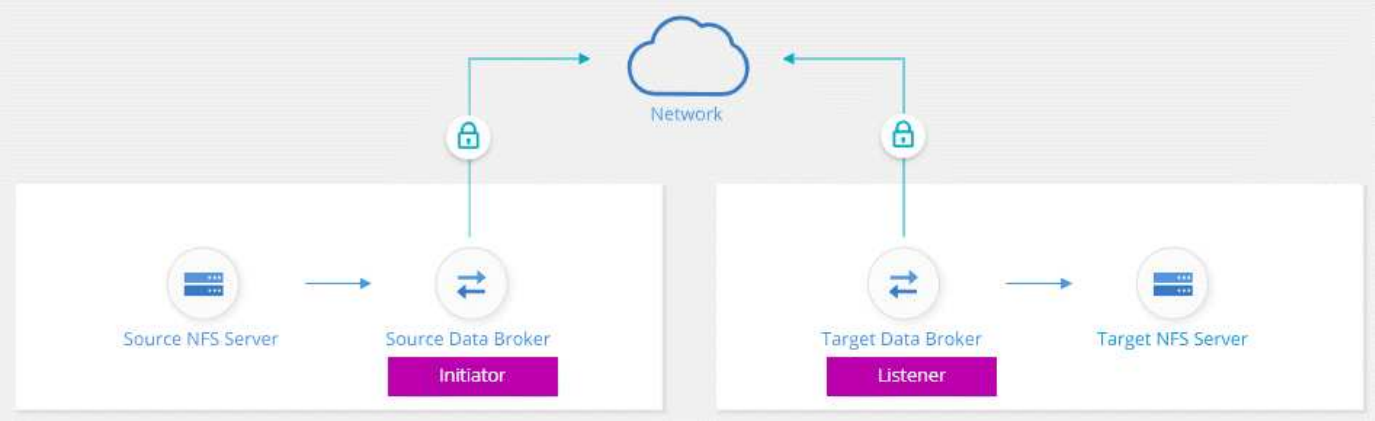
Sincronizzazione dei dati NFS con crittografia data-in-flight

Se la tua azienda ha policy di sicurezza rigorose, puoi sincronizzare i dati NFS utilizzando la crittografia data-in-flight. Questa funzionalità è supportata da un server NFS a un altro server NFS e da Azure NetApp Files a Azure NetApp Files.

Ad esempio, è possibile sincronizzare i dati tra due server NFS che si trovano in reti diverse. In alternativa, potrebbe essere necessario trasferire in modo sicuro i dati su Azure NetApp Files tra sottoreti o regioni.

Come funziona la crittografia dei dati in volo

La crittografia Data-in-flight crittografa i dati NFS quando vengono inviati in rete tra due broker di dati. La seguente immagine mostra una relazione tra due server NFS e due broker di dati:



Un data broker funziona come *initiator*. Quando è il momento di sincronizzare i dati, invia una richiesta di connessione all'altro data broker, che è il *listener*. Il data broker ascolta le richieste sulla porta 443. Se necessario, è possibile utilizzare un'altra porta, ma assicurarsi che la porta non sia utilizzata da un altro servizio.

Ad esempio, se si sincronizzano i dati da un server NFS on-premise a un server NFS basato sul cloud, è possibile scegliere quale broker di dati ascoltare le richieste di connessione e quale inviarle.

Ecco come funziona la crittografia in-flight:

1. Dopo aver creato la relazione di sincronizzazione, l'iniziatore avvia una connessione crittografata con l'altro data broker.
2. Il broker dei dati di origine crittografa i dati dall'origine utilizzando TLS 1.3.
3. Quindi, invia i dati in rete al data broker di destinazione.
4. Il broker di dati di destinazione decrta i dati prima di inviarli alla destinazione.
5. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore. Se sono presenti dati da sincronizzare, il processo inizia con l'iniziatore che apre una connessione crittografata con l'altro data

broker.

Se preferisci sincronizzare i dati più frequentemente, "è possibile modificare la pianificazione dopo aver creato la relazione".

Versioni NFS supportate

- Per i server NFS, la crittografia data-in-flight è supportata con le versioni NFS 3, 4.0, 4.1 e 4.2.
- Per Azure NetApp Files, la crittografia data-in-flight è supportata con NFS versioni 3 e 4.1.

Cosa ti serve per iniziare

Assicurarsi di disporre di quanto segue:

- Due server NFS che si incontrano "requisiti di origine e destinazione" O Azure NetApp Files in due sottoreti o regioni.
- Gli indirizzi IP o i nomi di dominio completi dei server.
- Posizioni di rete per due broker di dati.

  È possibile selezionare un data broker esistente, ma deve funzionare come iniziatore. Il data broker listener deve essere un *new* data broker.

  Se non hai ancora implementato un data broker, esamina i requisiti del data broker. Poiché si dispone di policy di sicurezza rigorose, assicurarsi di esaminare i requisiti di rete, che includono il traffico in uscita dalla porta 443 e da "endpoint internet" che il data broker contatta.

  - "Esaminare l'installazione di AWS"
  - "Esaminare l'installazione di Azure"
  - "Esaminare l'installazione di GCP"
  - "Esaminare l'installazione dell'host Linux"

Sincronizzazione dei dati NFS con crittografia data-in-flight

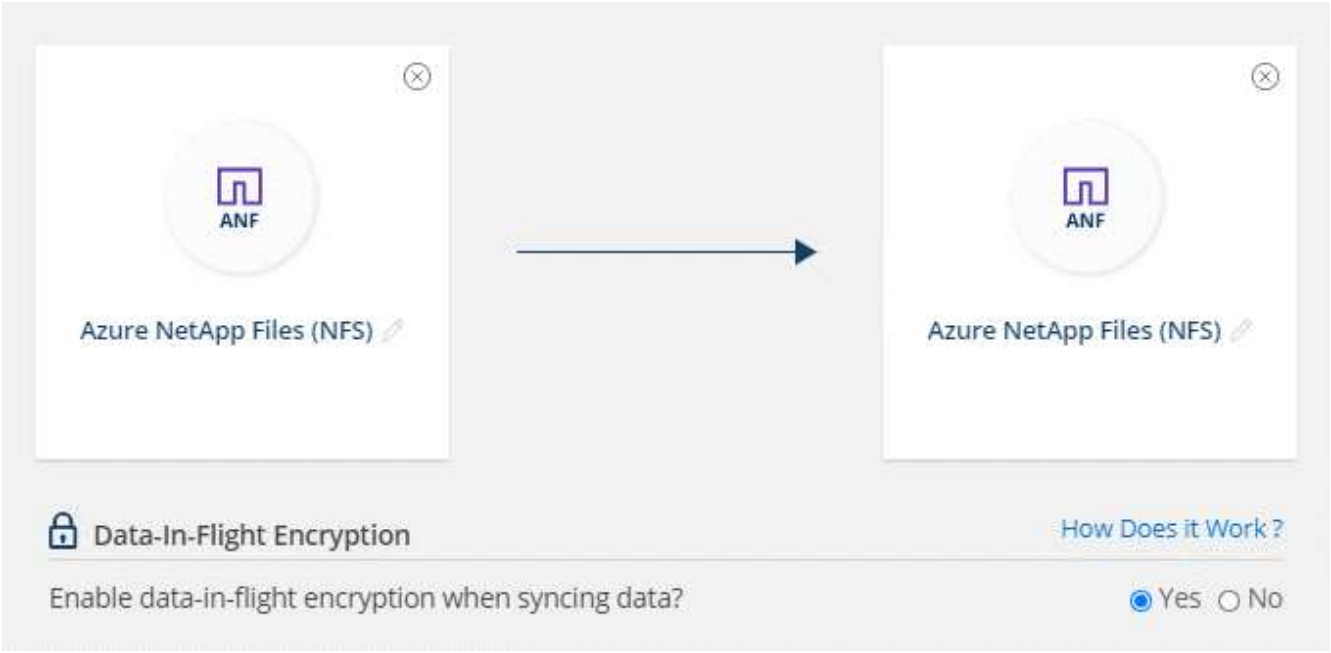
Creare una nuova relazione di sincronizzazione tra due server NFS o tra Azure NetApp Files, attivare l'opzione di crittografia in-flight e seguire le istruzioni.

Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Trascinare **server NFS** nelle posizioni di origine e destinazione o **Azure NetApp Files** nelle posizioni di origine e destinazione e selezionare **Sì** per attivare la crittografia dei dati in volo.

   La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra due server NFS:

La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra Azure NetApp Files:



3. Seguire le istruzioni per creare la relazione:

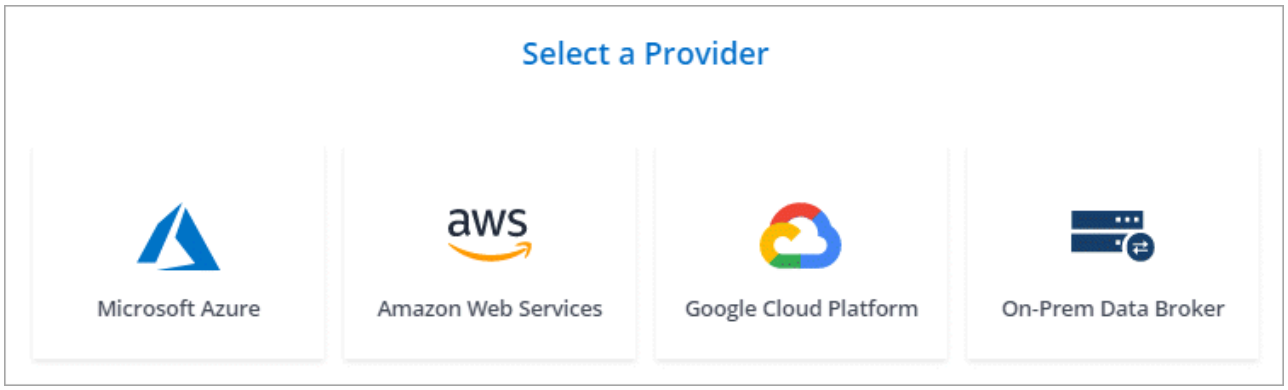
   a. **Server NFS/Azure NetApp Files**: Scegliere la versione di NFS e specificare una nuova origine NFS oppure selezionare un server esistente.

   b. **Definisci funzionalità Data Broker**: Definire quale broker di dati *ascolta* per le richieste di connessione su una porta e quale *avvia* la connessione. Scegli la tua scelta in base ai tuoi requisiti di rete.

   c. **Data Broker**: Seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionare un data broker esistente.

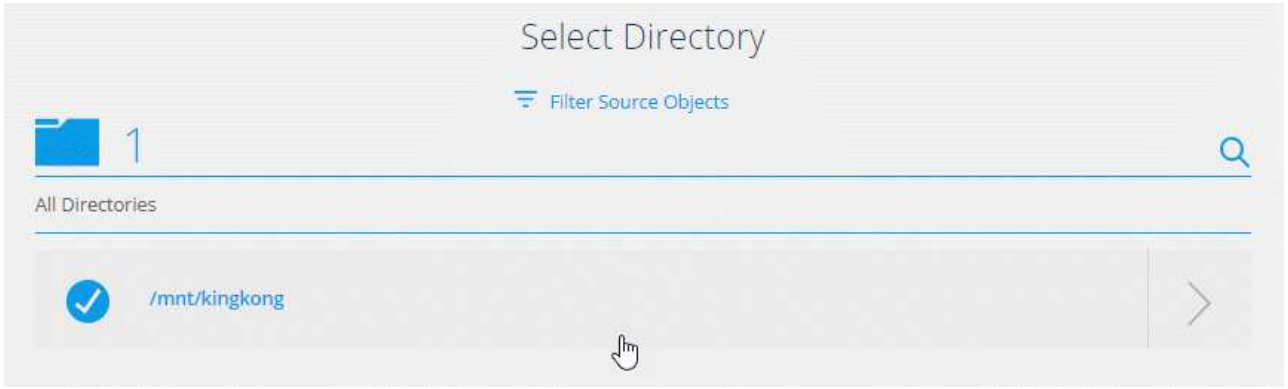
      Se il broker di dati di origine agisce come listener, deve essere un nuovo broker di dati.

Se è necessario un nuovo data broker, Cloud Sync richiede le istruzioni per l'installazione. Puoi implementare il data broker nel cloud o scaricare uno script di installazione per il tuo host Linux.



d. **Directory**: Scegliere le directory che si desidera sincronizzare selezionando tutte le directory oppure eseguendo il drill-down e selezionando una sottodirectory.

   Fare clic su **Filter Source Objects** (Filtra oggetti origine) per modificare le impostazioni che definiscono la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

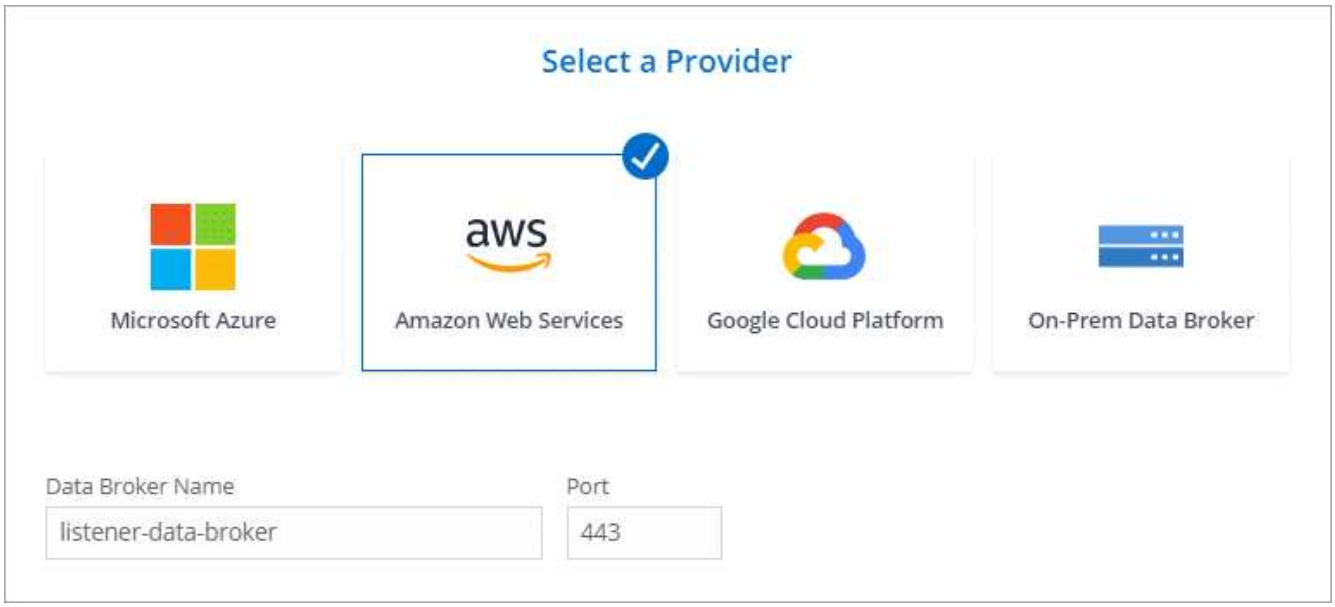


e. **Server NFS di destinazione/Azure NetApp Files di destinazione**: Scegliere la versione di NFS, quindi inserire una nuova destinazione NFS o selezionare un server esistente.

f. **Target Data Broker**: Seguire le istruzioni per aggiungere un nuovo broker di dati di origine o selezionare un broker di dati esistente.

   Se il data broker di destinazione agisce come listener, deve essere un nuovo data broker.

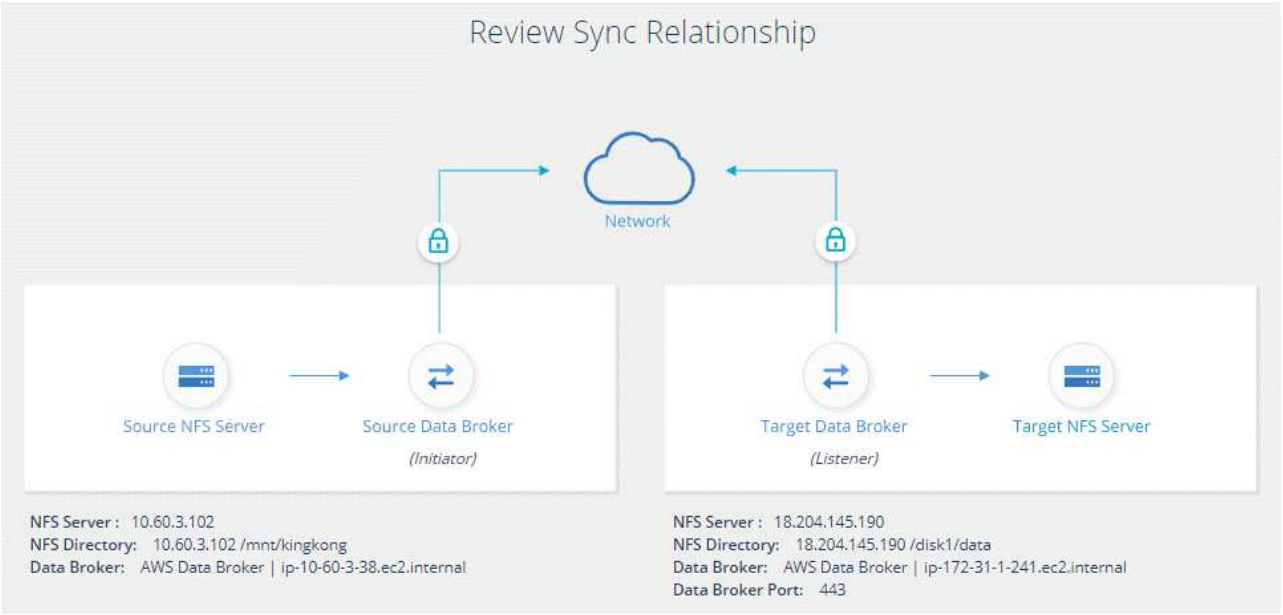
   Ecco un esempio del prompt quando il broker di dati di destinazione funziona come listener. Notare l'opzione per specificare la porta.



a. **Directory di destinazione**: Selezionare una directory di primo livello oppure eseguire il drill-down per selezionare una sottodirectory esistente o per creare una nuova cartella all'interno di un'esportazione.

b. **Impostazioni**: Consente di definire la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

c. **Revisione**: Esaminare i dettagli della relazione di sincronizzazione, quindi fare clic su **Crea relazione**.



Risultato

Cloud Sync inizia a creare la nuova relazione di sincronizzazione. Al termine, fare clic su **View in Dashboard** (Visualizza in Dashboard) per visualizzare i dettagli sulla nuova relazione.

Gestione delle relazioni di sincronizzazione

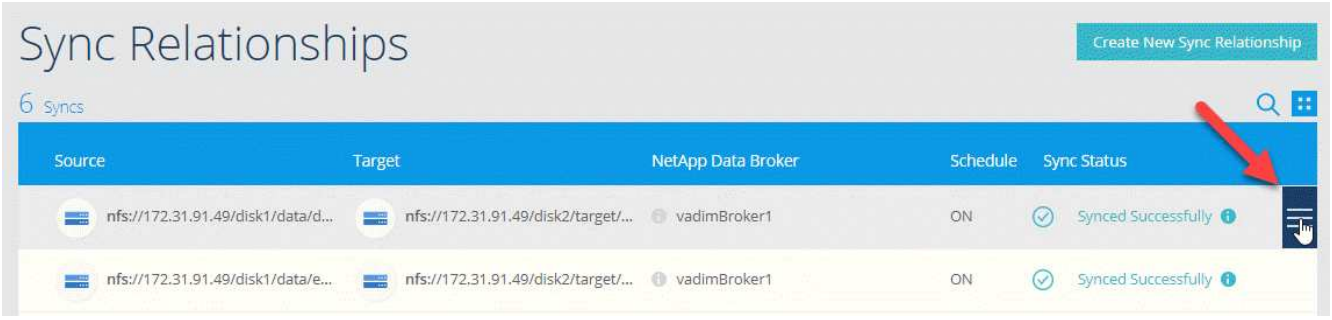
Puoi gestire le relazioni di sincronizzazione in qualsiasi momento sincronizzando immediatamente i dati, modificando le pianificazioni e molto altro ancora.

Esecuzione di una sincronizzazione dei dati immediata

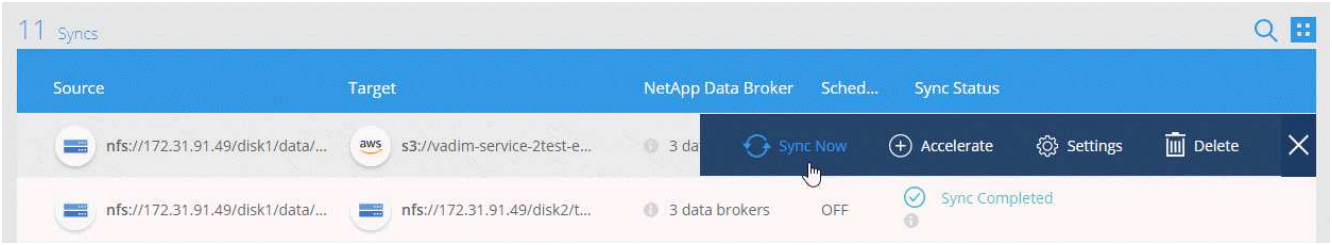
Invece di attendere la successiva sincronizzazione pianificata, è possibile premere un pulsante per sincronizzare immediatamente i dati tra l'origine e la destinazione.

Fasi

1. Dalla dashboard di sincronizzazione, passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.



2. Fare clic su **Sincronizza ora**, quindi su **Sincronizza** per confermare.



Risultato

Cloud Sync avvia il processo di sincronizzazione dei dati per la relazione.

Accelerazione delle performance di sincronizzazione

Accelera le performance di una relazione di sincronizzazione aggiungendo un broker di dati aggiuntivo alla relazione. Il data broker aggiuntivo deve essere un *new* data broker.

Come funziona

Se i data broker esistenti nella relazione vengono utilizzati in altre relazioni di sincronizzazione, Cloud Sync aggiunge automaticamente anche il nuovo data broker a tali relazioni.

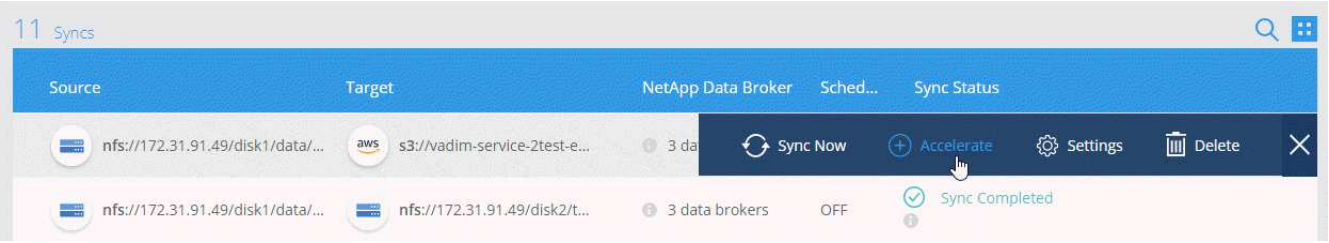
Ad esempio, supponiamo di avere tre relazioni:

- La relazione 1 utilizza il broker di dati A.
- La relazione 2 utilizza il data broker B.
- La relazione 3 utilizza il data broker A.

Si desidera accelerare le performance della relazione 1 in modo da aggiungere un nuovo data broker a tale relazione (data broker C). Poiché il broker di dati A viene utilizzato anche nella relazione 3, anche il nuovo broker di dati viene aggiunto automaticamente alla relazione 3.

Fasi

1. Assicurarsi che almeno uno dei broker di dati esistenti nella relazione sia online.
2. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
3. Fare clic su **Accelerate** (accelera).



4. Seguire le istruzioni per creare un nuovo data broker.

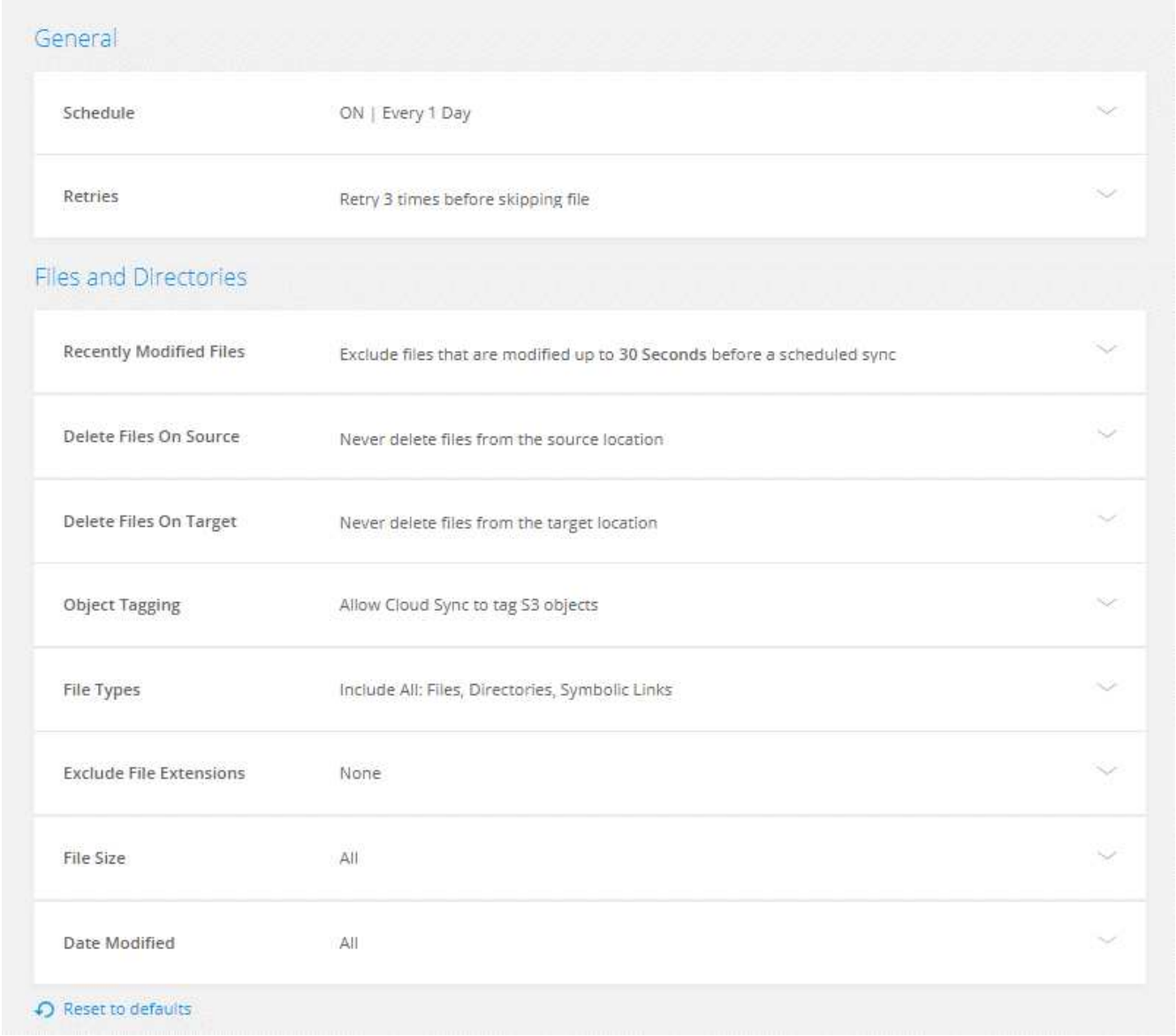
Risultato

Cloud Sync aggiunge il nuovo data broker alle relazioni di sincronizzazione. Le performance della successiva sincronizzazione dei dati dovrebbero essere accelerate.

Modifica delle impostazioni per una relazione di sincronizzazione

Modificare le impostazioni che definiscono la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Impostazioni**.
3. Modificare le impostazioni.



Ecco una breve descrizione di ciascuna impostazione:

Pianificazione

Scegliere una pianificazione ricorrente per le sincronizzazioni future o disattivare la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

Tentativi

Definire il numero di tentativi di sincronizzazione di un file da parte di Cloud Sync prima di ignorarlo.

File modificati di recente

Scegliere di escludere i file modificati di recente prima della sincronizzazione pianificata.

Elimina file in origine

Scegliere di eliminare i file dalla posizione di origine dopo che Cloud Sync copia i file nella posizione di destinazione. Questa opzione include il rischio di perdita dei dati perché i file di origine vengono cancellati dopo la copia.

Se si attiva questa opzione, è necessario modificare anche un parametro nel file local.json sul data broker. Aprire il file e modificare il parametro denominato *workers.transferrer.delete-on-source* in **true**.

Eliminare i file di destinazione

Scegliere di eliminare i file dalla posizione di destinazione, se sono stati eliminati dall'origine. Per impostazione predefinita, non elimina mai i file dalla posizione di destinazione.

Tagging degli oggetti

Quando AWS S3 è la destinazione in una relazione di sincronizzazione, Cloud Sync contrassegna gli oggetti S3 con metadati rilevanti per l'operazione di sincronizzazione. È possibile disattivare la tagging degli oggetti S3, se non si desidera, nell'ambiente in uso. La disattivazione del tagging non ha alcun impatto su Cloud Sync: Cloud Sync memorizza i metadati di sincronizzazione in un modo diverso.

Tipi di file

Definire i tipi di file da includere in ogni sincronizzazione: File, directory e collegamenti simbolici.

Escludi estensioni file

Specificare le estensioni dei file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file *.log. Non è necessario un separatore per più interni. Il seguente video fornisce una breve demo:

► https://docs.netapp.com/it-it/occm38//media/video_file_extensions.mp4 *(video)*

Dimensione del file

Scegliere di sincronizzare tutti i file indipendentemente dalle dimensioni o solo i file che si trovano in un intervallo di dimensioni specifico.

Data di modifica

Scegliere tutti i file indipendentemente dalla data dell'ultima modifica, i file modificati dopo una data specifica, prima di una data specifica o tra un intervallo di tempo.

Copia gli elenchi di controllo degli accessi nella destinazione

Scegliere di copiare gli elenchi di controllo degli accessi (ACL) tra le condivisioni SMB di origine e le condivisioni SMB di destinazione. Si noti che questa opzione è disponibile solo per le relazioni di sincronizzazione create dopo la release del 23 febbraio 2020.

4. Fare clic su **Save Settings** (Salva impostazioni).

Risultato

Cloud Sync modifica la relazione di sincronizzazione con le nuove impostazioni.

Eliminazione delle relazioni

È possibile eliminare una relazione di sincronizzazione, se non è più necessario sincronizzare i dati tra l'origine e la destinazione. Questa azione non elimina l'istanza del broker di dati e non elimina i dati dalla destinazione.

Fasi

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Delete** (Elimina), quindi fare nuovamente clic su **Delete** (Elimina) per confermare.

Risultato

Cloud Sync elimina la relazione di sincronizzazione.

API Cloud Sync

Le funzionalità di Cloud Sync disponibili tramite l'interfaccia utente Web sono disponibili anche tramite le API RESTful.

Per iniziare

Per iniziare a utilizzare le API di Cloud Sync, è necessario ottenere un token utente e l'ID account di Cloud Central. Quando si effettua una chiamata API, è necessario aggiungere il token e l'ID dell'account all'intestazione Authorization (autorizzazione).

Fasi

1. Ottieni un token utente da NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Ottieni il tuo ID account Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Questa API restituirà una risposta come la seguente:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Aggiungere il token utente e l'ID account nell'intestazione Authorization di ogni chiamata API.

Esempio

Nell'esempio seguente viene illustrata una chiamata API per creare un data broker in Microsoft Azure. È sufficiente sostituire <user_token> e <accountId> con il token e l'ID ottenuti nei passaggi precedenti.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

Cosa devo fare quando il token scade?

Il token utente di NetApp Cloud Central ha una data di scadenza. Per aggiornare il token, è necessario richiamare nuovamente l'API dal passaggio 1.

La risposta API include un campo "expires_in" che indica la scadenza del token.

Riferimento API

La documentazione per ogni API Cloud Sync è disponibile all'indirizzo "NetApp Cloud Central".

Utilizzo delle API di elenco

Le API di elenco sono API asincrone, pertanto il risultato non viene restituito immediatamente (ad esempio: `GET /data-brokers/{id}/list-nfs-export-folders` e. `GET /data-brokers/{id}/list-s3-buckets`). L'unica risposta dal server è lo stato HTTP 202. Per ottenere il risultato effettivo, è necessario utilizzare `GET /messages/client` API.

Fasi

1. Chiamare l'API dell'elenco che si desidera utilizzare.
2. Utilizzare `GET /messages/client` API per visualizzare il risultato dell'operazione.
3. Utilizzare la stessa API aggiungendo l'ID appena ricevuto: `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Tenere presente che l'ID cambia ogni volta che si chiama `GET /messages/client` API.

Esempio

Quando si chiama `list-s3-buckets` API, un risultato non viene restituito immediatamente:

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è il codice di stato HTTP 202, che significa che il messaggio è stato accettato, ma non è stato ancora elaborato.

Per ottenere il risultato dell'operazione, è necessario utilizzare la seguente API:

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è una matrice con un oggetto che include un campo ID. Il campo ID rappresenta l'ultimo messaggio inviato dal server. Ad esempio:

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

A questo punto, effettuare la seguente chiamata API utilizzando l'ID appena ricevuto:

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è una serie di messaggi. All'interno di ogni messaggio è presente un oggetto payload, che consiste nel nome dell'operazione (come chiave) e nel relativo risultato (come valore). Ad esempio:

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


Domande tecniche frequenti su Cloud Sync

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Per iniziare

Le seguenti domande si riferiscono alla guida introduttiva di Cloud Sync.

Come funziona Cloud Sync?

Cloud Sync utilizza il software per il broker dei dati NetApp per sincronizzare i dati da un'origine a una destinazione (questa è denominata *relazione di sincronizzazione*).

Il data broker controlla le relazioni di sincronizzazione tra le origini e le destinazioni. Dopo aver impostato una relazione di sincronizzazione, Cloud Sync analizza il sistema di origine e lo suddivide in più flussi di replica per eseguire il push sui dati di destinazione selezionati.

Dopo la copia iniziale, il servizio sincronizza i dati modificati in base alla pianificazione impostata.

Come funziona la prova gratuita di 14 giorni?

La prova gratuita di 14 giorni inizia quando ti iscrivi al servizio Cloud Sync. Non sei soggetto ai costi di NetApp per le relazioni Cloud Sync che crei per 14 giorni. Tuttavia, tutti i costi relativi alle risorse per qualsiasi broker di dati implementato sono ancora validi.

Quanto costa Cloud Sync?

L'utilizzo di Cloud Sync comporta due tipi di costi: Costi di servizio e costi delle risorse.

Costi di servizio

Per i prezzi pay-as-you-go, i costi del servizio Cloud Sync sono orari, in base al numero di relazioni di sincronizzazione create.

- "Visualizza i prezzi pay-as-you-go in AWS"
- "Visualizza i prezzi annuali in AWS"
- "Visualizza i prezzi in Azure"

Le licenze Cloud Sync sono disponibili anche presso il vostro rappresentante NetApp. Ogni licenza consente 20 relazioni di sincronizzazione per 12 mesi.

"Scopri di più sulle licenze".

Costi delle risorse

I costi delle risorse sono correlati ai costi di calcolo e storage per l'esecuzione del data broker nel cloud.

Come viene fatturato Cloud Sync?

Esistono due modi per pagare le relazioni di sincronizzazione dopo la fine della prova gratuita di 14 giorni. La prima opzione consiste nell'abbonarsi ad AWS o Azure, che consente di pagare a consumo o di pagare annualmente. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp.

Posso utilizzare Cloud Sync al di fuori del cloud?

Sì, puoi utilizzare Cloud Sync in un'architettura non cloud. L'origine e la destinazione possono risiedere on-premise e così anche il broker di dati.

Nota i seguenti punti chiave sull'utilizzo di Cloud Sync al di fuori del cloud:

- Per la sincronizzazione on-premise, NetApp StorageGRID mette a disposizione un bucket Amazon S3 privato.
- Il data broker ha bisogno di una connessione a Internet per comunicare con il servizio Cloud Sync.
- Se non acquisti una licenza direttamente da NetApp, dovrai disporre di un account AWS o Azure per la fatturazione del servizio PAYGO Cloud Sync.

Come si accede a Cloud Sync?

Cloud Sync è disponibile in Gestione cloud nella scheda **sincronizzazione**.

Fonti e destinazioni supportate

Le seguenti domande relative all'origine e alle destinazioni supportate in una relazione di sincronizzazione.

Quali fonti e destinazioni supporta Cloud Sync?

Cloud Sync supporta diversi tipi di relazioni di sincronizzazione. "Visualizzare l'intero elenco".

Quali versioni di NFS e SMB sono supportate da Cloud Sync?

Cloud Sync supporta NFS versione 3 e successive e SMB versione 1 e successive.

"Scopri di più sui requisiti di sincronizzazione".

Quando Amazon S3 è la destinazione, è possibile eseguire il tiering dei dati in base a una classe di storage S3 specifica?

Sì, è possibile scegliere una classe di storage S3 specifica quando AWS S3 è la destinazione:

- Standard (classe predefinita)
- Tiering intelligente
- Standard-infrequent Access (accesso standard-non frequente)
- Accesso non frequente a una sola zona
- Ghiacciaio
- Glacier Deep Archive

E i Tier di storage per lo storage Azure Blob?

È possibile scegliere un livello di storage Azure Blob specifico quando un container Blob è la destinazione:

- Storage a caldo
- Storage fresco

Networking

Le seguenti domande si riferiscono ai requisiti di rete per Cloud Sync.

Quali sono i requisiti di rete per Cloud Sync?

L'ambiente Cloud Sync richiede che il data broker sia connesso all'origine e alla destinazione attraverso il protocollo selezionato (NFS, SMB, EFS) o l'API dello storage a oggetti (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Inoltre, il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio Cloud Sync e contattare altri servizi e repository.

Per ulteriori informazioni, "esaminare i requisiti di rete".

Esistono limitazioni di rete relative alla connettività del data broker?

I broker di dati richiedono l'accesso a Internet. Non supportiamo un server proxy durante l'implementazione del data broker in Azure o in Google Cloud Platform.

Sincronizzazione dei dati

Le seguenti domande si riferiscono al funzionamento della sincronizzazione dei dati.

Con quale frequenza si verifica la sincronizzazione?

La pianificazione predefinita è impostata per la sincronizzazione giornaliera. Dopo la sincronizzazione iniziale, è possibile:

- Modificare la pianificazione di sincronizzazione in base al numero di giorni, ore o minuti desiderato
- Disattivare la pianificazione della sincronizzazione
- Eliminare la pianificazione di sincronizzazione (nessun dato andrà perso; verrà rimossa solo la relazione di sincronizzazione)

Qual è la pianificazione minima di sincronizzazione?

È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

Il broker di dati riprova quando un file non riesce a sincronizzarsi? O il timeout?

Il data broker non esegue il timeout quando un singolo file non riesce a trasferire. Invece, il data broker tenta di nuovo 3 volte prima di saltare il file. Il valore di RETRY è configurabile nelle impostazioni per una relazione di sincronizzazione.

"Scopri come modificare le impostazioni per una relazione di sincronizzazione".

E se si dispone di un set di dati molto grande?

Se una singola directory contiene almeno 600,000 file, contattaci per aiutarti a configurare il data broker in modo da gestire il payload. Potrebbe essere necessario aggiungere ulteriore memoria alla macchina del broker di dati.

Sicurezza

Le seguenti domande relative alla sicurezza.

Cloud Sync è sicuro?

Sì. Tutta la connettività di rete del servizio Cloud Sync viene eseguita utilizzando "Amazon Simple Queue Service (SQS)".

Tutte le comunicazioni tra il data broker e Amazon S3, Azure Blob, Google Cloud Storage e IBM Cloud Object Storage vengono effettuate tramite il protocollo HTTPS.

Se utilizzi Cloud Sync con sistemi on-premise (di origine o di destinazione), ecco alcune opzioni di connettività consigliate:

- Una connessione AWS Direct Connect, Azure ExpressRoute o Google Cloud Interconnect, non instradata su Internet (e in grado di comunicare solo con le reti cloud specificate)
- Una connessione VPN tra il dispositivo gateway on-premise e le reti cloud
- Per un trasferimento dei dati estremamente sicuro con i bucket S3, lo storage Azure Blob o Google Cloud Storage, è possibile stabilire un endpoint Amazon Private S3 Endpoint, un endpoint del servizio Azure Virtual Network o un accesso privato a Google.

Uno qualsiasi di questi metodi stabilisce una connessione sicura tra i server NAS on-premise e un data broker Cloud Sync.

I dati sono crittografati da Cloud Sync?

- Cloud Sync supporta la crittografia data-in-flight tra server NFS di origine e di destinazione. "Scopri di più".
- La crittografia non è supportata con SMB.
- Quando un bucket Amazon S3 è la destinazione di una relazione di sincronizzazione, puoi scegliere se attivare la crittografia dei dati utilizzando la crittografia AWS KMS o AES-256.

Permessi

Le seguenti domande si riferiscono alle autorizzazioni per i dati.

Le autorizzazioni dei dati SMB sono sincronizzate con la posizione di destinazione?

È possibile impostare Cloud Sync in modo da conservare gli elenchi di controllo degli accessi (ACL) tra una condivisione SMB di origine e una condivisione SMB di destinazione. In alternativa, è possibile copiare manualmente gli ACL. "Scopri come copiare gli ACL tra le condivisioni SMB".

Le autorizzazioni dei dati NFS sono sincronizzate con la posizione di destinazione?

Cloud Sync copia automaticamente le autorizzazioni NFS tra i server NFS come segue:

- NFS versione 3: Cloud Sync copia i permessi e il proprietario del gruppo di utenti.
- NFS versione 4: Cloud Sync copia gli ACL.

Performance

Le seguenti domande si riferiscono alle performance di Cloud Sync.

Cosa rappresenta l'indicatore di avanzamento di una relazione di sincronizzazione?

La relazione di sincronizzazione mostra il throughput della scheda di rete del data broker. Se le prestazioni di sincronizzazione sono state accelerate utilizzando più broker di dati, il throughput è la somma di tutto il traffico. Questo throughput viene aggiornato ogni 20 secondi.

Sto riscontrando problemi di performance. Possiamo limitare il numero di trasferimenti simultanei?

Il data broker può sincronizzare 4 file alla volta. Se si dispone di file di grandi dimensioni (più TB ciascuno), il completamento del processo di trasferimento può richiedere molto tempo e le prestazioni potrebbero risentirne.

Limitare il numero di trasferimenti simultanei può essere di aiuto. Mailto:ng-cloudsync-support@netapp.com[Contattaci per ricevere assistenza].

Perché si riscontrano prestazioni ridotte con Azure NetApp Files?

Quando si sincronizzano i dati con o da Azure NetApp Files, potrebbero verificarsi errori e problemi di performance se il livello di servizio del disco è standard.

Impostare il livello di servizio su Premium o Ultra per migliorare le prestazioni di sincronizzazione.

"Scopri di più sui livelli di servizio e sul throughput di Azure NetApp Files".

Perché si riscontrano prestazioni ridotte con Cloud Volumes Service per AWS?

Quando sincronizzi i dati da o verso un volume cloud, potresti riscontrare guasti e problemi di performance se il livello di performance per il volume cloud è Standard.

Impostare il livello di servizio su Premium o Extreme per migliorare le prestazioni di sincronizzazione.

Quanti broker di dati sono richiesti?

Quando si crea una nuova relazione, si inizia con un singolo data broker (a meno che non sia stato selezionato un data broker esistente che appartiene a una relazione di sincronizzazione accelerata). In molti casi, un singolo data broker può soddisfare i requisiti di performance per una relazione di sincronizzazione. In caso contrario, puoi accelerare le performance di sincronizzazione aggiungendo ulteriori broker di dati. Tuttavia, è necessario prima controllare altri fattori che possono influire sulle prestazioni di sincronizzazione.

Diversi fattori possono influire sulle performance di trasferimento dei dati. Le performance di sincronizzazione complessive potrebbero risentire della larghezza di banda, della latenza e della topologia di rete, delle specifiche delle macchine virtuali del data broker e delle performance del sistema storage. Ad esempio, un singolo broker di dati in una relazione di sincronizzazione può raggiungere 100 MB/s, mentre il throughput del disco sulla destinazione potrebbe consentire solo 64 MB/s. Di conseguenza, il data broker continua a cercare di copiare i dati, ma la destinazione non può soddisfare le performance del data broker.

Pertanto, verificare le prestazioni della rete e il throughput del disco sulla destinazione.

Quindi, puoi prendere in considerazione l'accelerazione delle performance di sincronizzazione aggiungendo un ulteriore broker di dati per condividere il carico di tale relazione. "Scopri come accelerare le performance di sincronizzazione".

Eliminare le cose

Le seguenti domande si riferiscono all'eliminazione di relazioni di sincronizzazione e dati da origini e destinazioni.

Cosa succede se si elimina la relazione Cloud Sync?

L'eliminazione di una relazione interrompe tutte le future sincronizzazioni dei dati e termina il pagamento. Tutti i dati sincronizzati con la destinazione rimangono invariato.

Cosa succede se si elimina qualcosa dal server di origine? Viene rimosso anche dalla destinazione?

Per impostazione predefinita, se si dispone di una relazione di sincronizzazione attiva, l'elemento eliminato sul server di origine non viene eliminato dalla destinazione durante la sincronizzazione successiva. Tuttavia, nelle impostazioni di sincronizzazione per ciascuna relazione è disponibile un'opzione in cui è possibile definire che Cloud Sync elimini i file nella posizione di destinazione se sono stati eliminati dall'origine.

"Scopri come modificare le impostazioni per una relazione di sincronizzazione".

Cosa succede se si elimina qualcosa dalla destinazione? Viene rimosso anche dalla fonte?

Se un elemento viene eliminato dalla destinazione, non verrà rimosso dall'origine. La relazione è unidirezionale, dall'origine alla destinazione. Al successivo ciclo di sincronizzazione, Cloud Sync confronta l'origine con la destinazione, identifica l'elemento mancante e Cloud Sync lo copia di nuovo dall'origine alla destinazione.

Risoluzione dei problemi

"Knowledge base di NetApp: Domande frequenti su Cloud Sync: Supporto e risoluzione dei problemi"

Analisi approfondita del data broker

La seguente domanda si riferisce al data broker.

Puoi spiegare l'architettura del data broker?

Certo. Ecco i punti più importanti:

- Il data broker è un'applicazione node.js in esecuzione su un host Linux.
- Cloud Sync implementa il data broker come segue:
  - AWS: Da un modello AWS CloudFormation
  - Azure: Da Azure Resource Manager
  - Google: Da Google Cloud Deployment Manager
  - Se si utilizza il proprio host Linux, è necessario installare manualmente il software
- Il software data broker si aggiorna automaticamente alla versione più recente.
- Il data broker utilizza AWS SQS come canale di comunicazione affidabile e sicuro e per il controllo e il monitoraggio. SQS fornisce anche un layer di persistenza.
- È possibile aggiungere ulteriori broker di dati a una relazione per aumentare la velocità di trasferimento e aggiungere alta disponibilità. In caso di guasto di un broker di dati, esiste una resilienza del servizio.

Approfondimenti sulla privacy dei dati

Scopri di più sulla conformità al cloud

Cloud Compliance è un servizio di privacy e conformità dei dati per Cloud Manager che esegue la scansione di volumi, bucket Amazon S3 e database per identificare i dati personali e sensibili presenti in tali file. Utilizzando la tecnologia basata sull'intelligenza artificiale (ai), Cloud Compliance aiuta le organizzazioni a comprendere il contesto dei dati e a identificare i dati sensibili.

"Scopri i casi di utilizzo per la conformità al cloud".

Caratteristiche

Cloud Compliance offre diversi strumenti che possono aiutarti con le tue attività di compliance. Puoi utilizzare la conformità al cloud per:

- Identificare le informazioni personali identificabili (PII)
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR, CCPA, PCI e HIPAA
- Rispondere alle richieste di accesso dei soggetti a dati (DSAR)

Ambienti di lavoro e origini dati supportati

Cloud Compliance può eseguire la scansione dei dati dai seguenti tipi di origini dati:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- Azure NetApp Files
- Amazon S3
- Database che risiedono ovunque (non è necessario che il database risieda in un ambiente di lavoro)

Nota: per Azure NetApp Files, la conformità del cloud può eseguire la scansione di tutti i volumi che si trovano nella stessa regione di Cloud Manager.

Costo

- Il costo per l'utilizzo della conformità cloud dipende dalla quantità di dati che si sta scansionando. A partire dal 7 ottobre 2020, i primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Sono inclusi i dati provenienti da volumi Cloud Volumes ONTAP, volumi Azure NetApp Files, bucket Amazon S3 e schemi di database. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace. Vedere "prezzi" per ulteriori informazioni.

  "Scopri come iscriverti".

- L'installazione di Cloud Compliance richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del cloud provider in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider

- La conformità al cloud richiede l'implementazione di un connettore. In molti casi hai già un connettore a causa di altri servizi e storage utilizzati in Cloud Manager. L'istanza del connettore comporta addebiti da parte del cloud provider in cui viene implementata. Vedere "tipo di istanza implementata per ciascun cloud provider".

Costi di trasferimento dei dati

I costi di trasferimento dei dati dipendono dalla configurazione. Se l'istanza di Cloud Compliance e l'origine dati si trovano nella stessa zona di disponibilità e nella stessa regione, non ci sono costi di trasferimento dei dati. Tuttavia, se l'origine dati, come un cluster Cloud Volumes ONTAP o un bucket S3, si trova in una _area o regione di disponibilità diversa, il tuo cloud provider addebiterà i costi di trasferimento dei dati. Per ulteriori informazioni, consulta i seguenti xref:./* "AWS: Prezzi Amazon EC2"
* "Microsoft Azure: Dettagli sui prezzi della larghezza di banda"

Come funziona Cloud Compliance

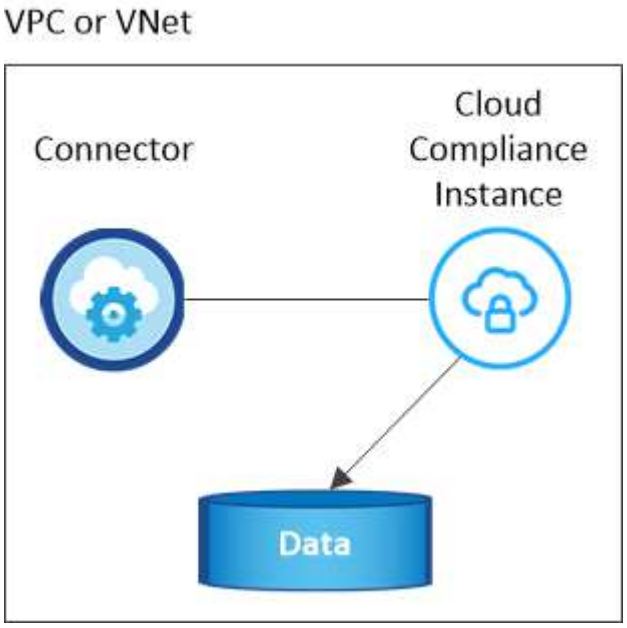
Ad alto livello, la conformità al cloud funziona come segue:

1. Implementa un'istanza di Cloud Compliance in Cloud Manager.
2. È possibile attivarlo su uno o più ambienti di lavoro o sui database.
3. Cloud Compliance esegue la scansione dei dati utilizzando un processo di apprendimento ai.
4. In Cloud Manager, fai clic su **Compliance** e utilizza la dashboard e gli strumenti di reporting forniti per aiutarti nelle tue attività di compliance.

L'istanza di Cloud Compliance

Quando si attiva Cloud Compliance, Cloud Manager implementa un'istanza di Cloud Compliance nella stessa sottorete del connettore. "Scopri di più sui connettori."

Se il connettore è installato on-premise, implementa l'istanza di conformità cloud nello stesso VPC o VNET del primo sistema Cloud Volumes ONTAP nella richiesta.



Tenere presente quanto segue a proposito dell'istanza:

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco GP2 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

> La modifica o il ridimensionamento del tipo di istanza/VM non è supportato. È necessario utilizzare le dimensioni fornite.

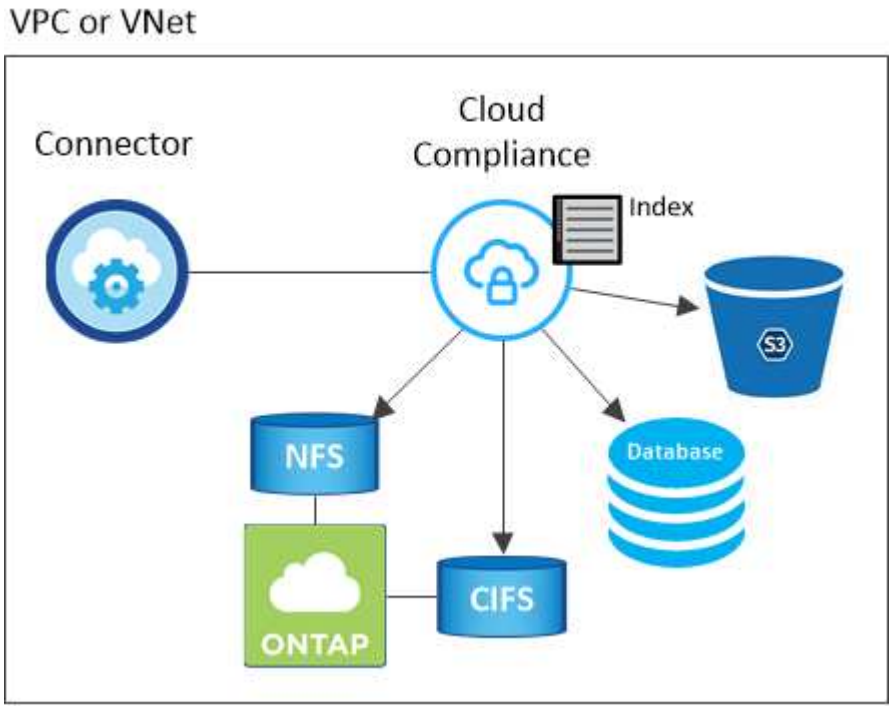
- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Viene implementata una sola istanza di Cloud Compliance per connettore.
- Gli aggiornamenti del software Cloud Compliance sono automatizzati e non dovrai preoccuparti di questo.

> L'istanza deve rimanere sempre in esecuzione perché Cloud Compliance esegue continuamente la scansione dei dati.

Come funzionano le scansioni

Dopo aver attivato Cloud Compliance e selezionato i volumi, i bucket o gli schemi di database da sottoporre a scansione, inizia immediatamente la scansione dei dati per identificare i dati personali e sensibili. Mappa i dati dell'organizzazione, classifica ciascun file e identifica ed estrae entità e modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili e categorie di dati.

Cloud Compliance si connette ai dati come qualsiasi altro client montando volumi NFS e CIFS. Ai volumi NFS viene automaticamente eseguito l'accesso in sola lettura, mentre è necessario fornire le credenziali Active Directory per eseguire la scansione dei volumi CIFS.



Dopo la scansione iniziale, Cloud Compliance esegue una scansione continua di ciascun volume per rilevare

le modifiche incrementali (per questo motivo è importante mantenere l'istanza in esecuzione).

È possibile attivare e disattivare le scansioni in "livello del volume"in corrispondenza di "livello della benna"e in "livello di schema del database".

Informazioni indicizzati dalla Cloud Compliance

Cloud Compliance raccoglie, indicizza e assegna le categorie ai dati non strutturati (file). I dati indicizzati dalla Cloud Compliance includono:

Metadati standard

Cloud Compliance raccoglie i metadati standard relativi ai file: Il tipo, le dimensioni, le date di creazione e modifica e così via.

Dati personali

Informazioni personali come indirizzi e-mail, numeri di identificazione o numeri di carta di credito. "Scopri di più sui dati personali".

Dati personali sensibili

Tipi speciali di informazioni sensibili, come dati sanitari, origine etnica o opinioni politiche, come definito dal GDPR e da altre normative sulla privacy. "Scopri di più sui dati personali sensibili".

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Scopri di più sulle categorie".

Riconoscimento entità nome

Cloud Compliance utilizza l'ai per estrarre i nomi delle persone fisiche dai documenti. "Scopri come rispondere alle richieste di accesso ai soggetti dati".

Panoramica delle reti

Cloud Manager implementa l'istanza Cloud Compliance con un gruppo di sicurezza che abilita le connessioni HTTP in entrata dall'istanza del connettore.

Quando si utilizza Cloud Manager in modalità SaaS, la connessione a Cloud Manager viene servita su HTTPS e i dati privati inviati tra il browser e l'istanza di conformità cloud sono protetti con crittografia end-to-end, il che significa che NetApp e terze parti non possono leggerli.

Se per qualsiasi motivo è necessario utilizzare l'interfaccia utente locale invece dell'interfaccia utente SaaS, è comunque possibile "Accedere all'interfaccia utente locale".

Le regole in uscita sono completamente aperte. L'accesso a Internet è necessario per installare e aggiornare il software Cloud Compliance e per inviare metriche di utilizzo.

Se hai requisiti di rete rigorosi, "Scopri gli endpoint che la Cloud Compliance contatta".

Accesso dell'utente alle informazioni di conformità

Il ruolo assegnato a ciascun utente offre diverse funzionalità all'interno di Cloud Manager e nell'ambito della Cloud Compliance:

- **Gli account Admins** possono gestire le impostazioni di conformità e visualizzare le informazioni di conformità per tutti gli ambienti di lavoro.
- **Workspace Admins** è in grado di gestire le impostazioni di conformità e visualizzare le informazioni di conformità solo per i sistemi ai quali sono autorizzati ad accedere. Se un amministratore dell'area di lavoro non riesce ad accedere a un ambiente di lavoro in Cloud Manager, non può visualizzare alcuna informazione di conformità per l'ambiente di lavoro nella scheda Compliance.
- Gli utenti con il ruolo **Cloud Compliance Viewer** possono solo visualizzare le informazioni di conformità e generare report per i sistemi ai quali sono autorizzati ad accedere. Questi utenti non possono attivare/disattivare la scansione di volumi, bucket o schemi di database.

"Scopri di più sui ruoli di Cloud Manager" e come fare "aggiungere utenti con ruoli specifici".

Inizia subito

Implementazione della conformità al cloud

Completa alcuni passaggi per implementare l'istanza Cloud Compliance nel tuo spazio di lavoro Cloud Manager.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Creare un connettore

Se non si dispone già di un connettore, creare un connettore in Azure o AWS. Vedere "Creazione di un connettore in AWS" oppure "Creazione di un connettore in Azure".

Esaminare i prerequisiti

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i prerequisiti, che includono 16 vCPU per l'istanza Cloud Compliance, accesso a Internet in uscita per l'istanza, connettività tra il connettore e Cloud Compliance tramite la porta 80 e altro ancora. Consulta l'elenco completo.

Implementazione della conformità al cloud

Avviare l'installazione guidata per implementare l'istanza Cloud Compliance in Cloud Manager.

Iscriviti al servizio Cloud Compliance

I primi 1 TB di dati che Cloud Compliance analizza in Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace.

Creazione di un connettore

Se non si dispone già di un connettore, creare un connettore in Azure o AWS. Vedere "Creazione di un connettore in AWS" oppure "Creazione di un connettore in Azure". Nella maggior parte dei casi, è probabile che sia stato configurato un connettore prima di tentare di attivare la conformità cloud, perché la maggior parte di essi "Le funzionalità di Cloud Manager richiedono un connettore", ma in alcuni casi è necessario impostarne uno ora.

Esistono alcuni scenari in cui è necessario utilizzare un connettore in AWS o Azure per la conformità al cloud.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP nei bucket AWS o AWS S3, si utilizza un connettore in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un connettore in Azure.
- È possibile eseguire la scansione dei database utilizzando uno dei due connettori.

Come puoi vedere, potrebbero esserci alcune situazioni in cui devi utilizzare "Connettori multipli".

> Se si intende eseguire la scansione di Azure NetApp Files, è necessario assicurarsi che l'implementazione venga eseguita nella stessa regione dei volumi che si desidera sottoporre a scansione.

Verifica dei prerequisiti

Prima di implementare Cloud Compliance, esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata.

Abilitare l'accesso a Internet in uscita

La conformità al cloud richiede l'accesso a Internet in uscita. Se la rete virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza Cloud Compliance disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint. Si noti che Cloud Manager implementa l'istanza Cloud Compliance nella stessa subnet del connettore.

Endpoint	Scopo
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce l'accesso a immagini, manifesti e modelli software.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Consente alla conformità del cloud di accedere e scaricare manifesti e modelli e di inviare registri e metriche.

Assicurarsi che Cloud Manager disponga delle autorizzazioni necessarie

Assicurarsi che Cloud Manager disponga delle autorizzazioni per implementare le risorse e creare gruppi di sicurezza per l'istanza di conformità cloud. Le autorizzazioni più recenti di Cloud Manager sono disponibili in "Le policy fornite da NetApp".

Controllare i limiti della vCPU

Assicurati che il limite vCPU del tuo provider cloud consenta l'implementazione di un'istanza con 16 core. È necessario verificare il limite vCPU per la famiglia di istanze pertinente nella regione in cui è in esecuzione Cloud Manager.

In AWS, la famiglia di istanze è *istanze standard on-Demand*. In Azure, la famiglia di istanze è *Standard DSv3 Family*.

Per ulteriori informazioni sui limiti delle vCPU, consulta la seguente pagina:

- "Documentazione AWS: Limiti di servizio Amazon EC2"
- "Documentazione di Azure: Quote vCPU delle macchine virtuali"

Assicurati che Cloud Manager possa accedere alla conformità al cloud

Garantire la connettività tra il connettore e l'istanza Cloud Compliance. Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulla porta 80 da e verso l'istanza Cloud Compliance.

Questa connessione consente l'implementazione dell'istanza Cloud Compliance e consente di visualizzare le informazioni nella scheda Compliance.

Impostare il rilevamento di Azure NetApp Files

Prima di eseguire la scansione dei volumi per Azure NetApp Files, "Cloud Manager deve essere configurato per rilevare la configurazione".

Assicurati di mantenere la conformità al cloud in esecuzione

L'istanza di Cloud Compliance deve continuare a eseguire la scansione dei dati.

Garantire la connettività del browser Web alla conformità al cloud

Dopo aver attivato Cloud Compliance, assicurarsi che gli utenti accedano all'interfaccia di Cloud Manager da un host che dispone di una connessione all'istanza di Cloud Compliance.

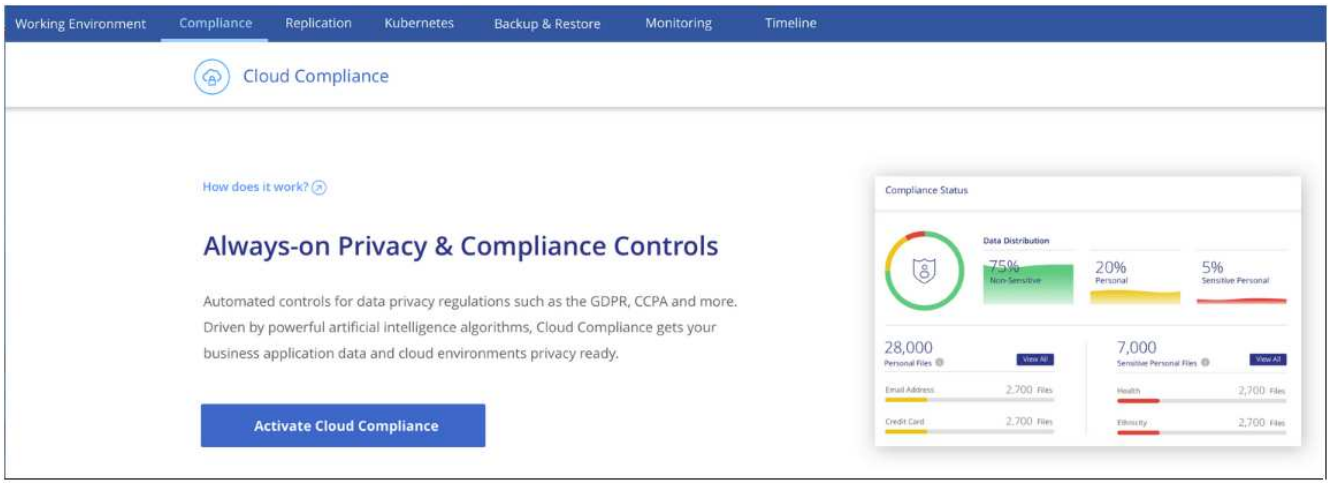
L'istanza Cloud Compliance utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili a Internet. Di conseguenza, il browser Web utilizzato per accedere a Cloud Manager deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta ad AWS o Azure (ad esempio, una VPN) o da un host che si trova all'interno della stessa rete dell'istanza Cloud Compliance.

Implementazione dell'istanza Cloud Compliance

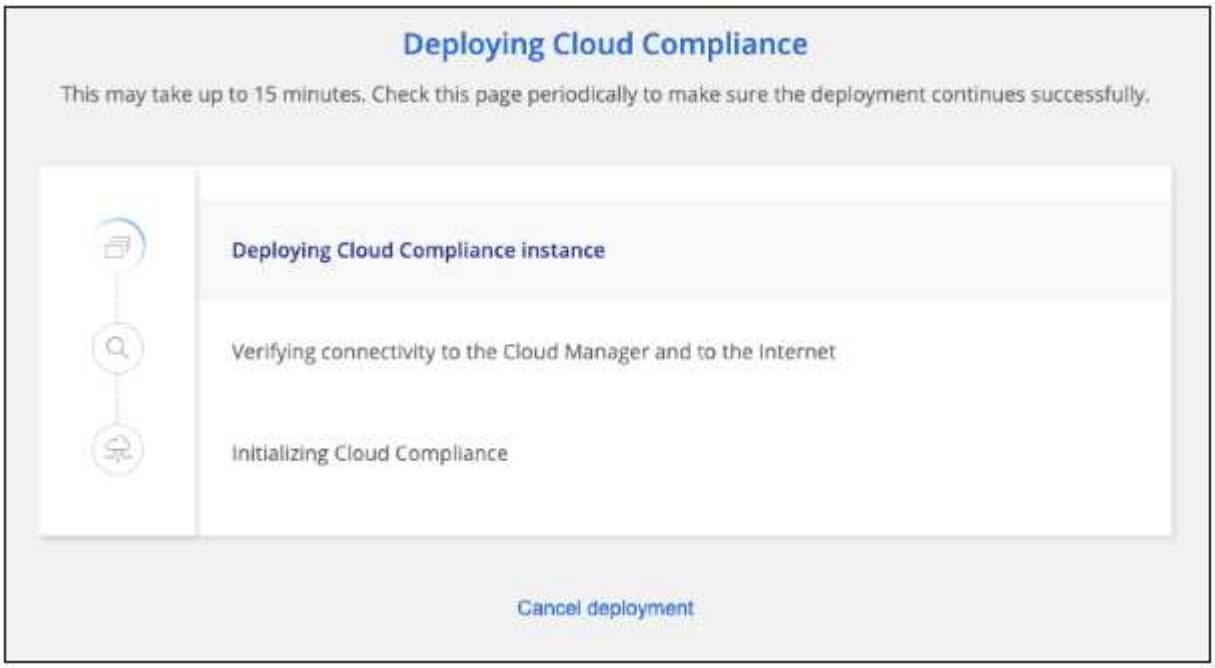
Implementa un'istanza di Cloud Compliance per ogni istanza di Cloud Manager.

Fasi

1. In Cloud Manager, fare clic su **Cloud Compliance**.
2. Fare clic su **Activate Cloud Compliance** (attiva conformità cloud) per avviare la procedura guidata di implementazione.



3. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si interrompe e richiede un input.



4. Una volta implementata l'istanza, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Scan Configuration* (Configurazione scansione).

Risultato

Cloud Manager implementa l'istanza Cloud Compliance nel tuo cloud provider.

Cosa c'è di nuovo

Dalla pagina Scan Configuration (Configurazione scansione) è possibile selezionare gli ambienti di lavoro, i volumi e i bucket che si desidera sottoporre a scansione per verificare la conformità. È inoltre possibile connettersi a un server di database per eseguire la scansione di schemi di database specifici. Attivare la conformità del cloud su una qualsiasi di queste origini dati.

Iscrizione al servizio Cloud Compliance

I primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure

Marketplace.

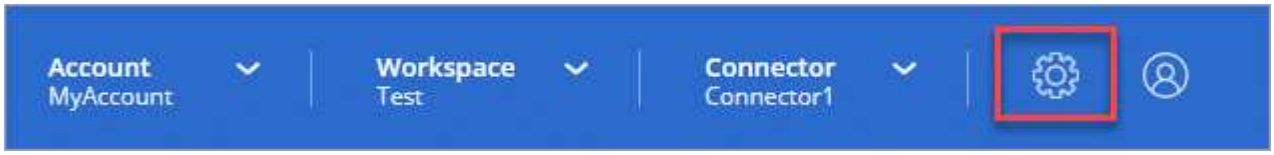
Puoi iscriverti in qualsiasi momento e non ti verrà addebitato alcun costo fino a quando la quantità di dati non supera 1 TB. Puoi sempre visualizzare la quantità totale di dati sottoposti a scansione dal Cloud Compliance Dashboard. Inoltre, il pulsante *Iscriviti ora* semplifica l'iscrizione quando sei pronto.

Nota: se la Cloud Compliance ti chiede di iscriverti, ma hai già un abbonamento Azure, probabilmente stai utilizzando il vecchio abbonamento **Cloud Manager** e devi passare al nuovo abbonamento **NetApp Cloud Manager**. VederePassaggio al nuovo piano NetApp Cloud Manager in Azure per ulteriori informazioni.

Fasi

Questi passaggi devono essere completati da un utente che ha il ruolo di *account Admin*.

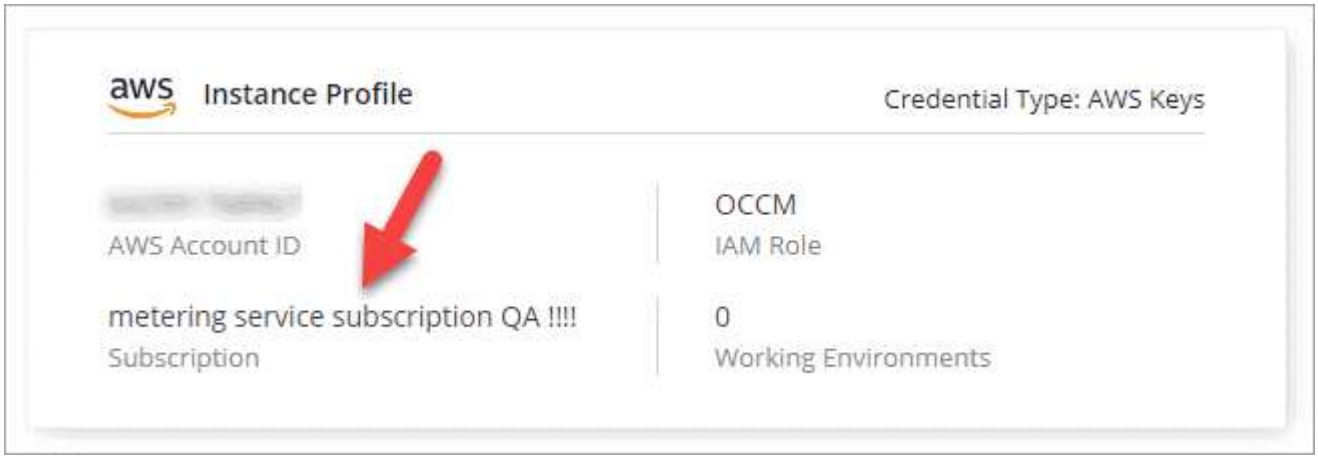
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



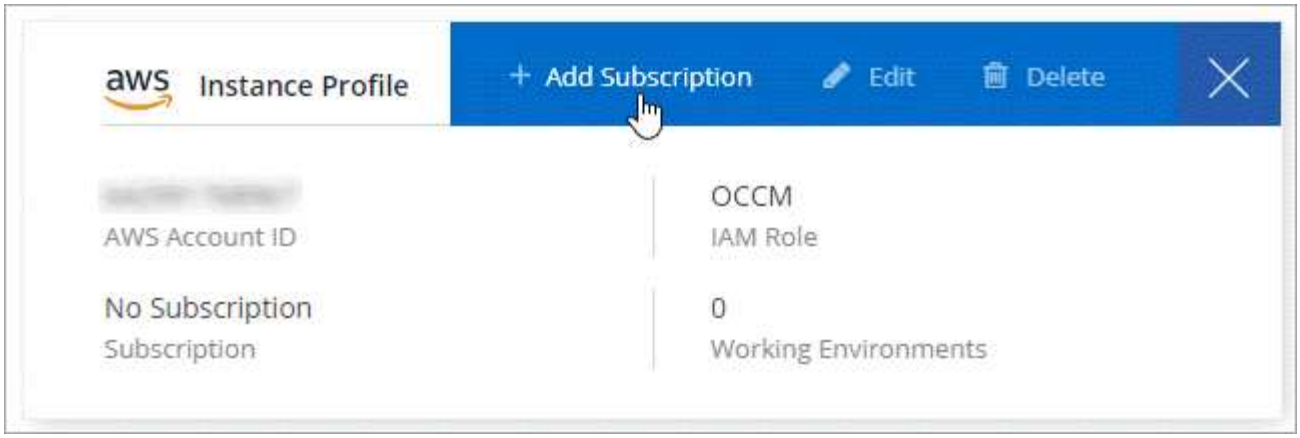
2. Trova le credenziali per AWS Instance Profile o Azure Managed Service Identity.

   L'abbonamento deve essere aggiunto al profilo istanza o all'identità del servizio gestito. La ricarica non funziona altrimenti.

   Se hai già un abbonamento, sei tutto impostato, non c'è altro da fare.



3. Se non disponi ancora di un abbonamento, passa il mouse sulle credenziali e fai clic sul menu delle azioni.
4. Fare clic su **Aggiungi abbonamento**.



5. Fare clic su **Add Subscription** (Aggiungi abbonamento), fare clic su **Continue** (continua) e seguire la procedura.

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento AWS:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

   Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

Passaggio al nuovo piano Cloud Manager in Azure

Cloud Compliance è stata aggiunta all'abbonamento ad Azure Marketplace denominato **NetApp Cloud Manager** al 7 ottobre 2020. Se disponi già dell'abbonamento originale a Azure **Cloud Manager**, non potrai utilizzare Cloud Compliance.

Seguire questi passaggi e selezionare il nuovo abbonamento **NetApp Cloud Manager**, quindi rimuovere il vecchio abbonamento **Cloud Manager**.

Se il tuo abbonamento esistente è stato emesso con un'offerta privata speciale, devi contattare NetApp in modo da poter emettere una nuova offerta privata speciale con conformità inclusa.

Fasi

Questi passaggi sono simili all'aggiunta di un nuovo abbonamento come descritto in precedenza, ma variano in alcuni punti.

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Individuare le credenziali per Azure Managed Service Identity per cui si desidera modificare l'abbonamento e passare il mouse sulle credenziali e fare clic su **Associa abbonamento**.

   Vengono visualizzati i dettagli dell'attuale abbonamento Marketplace.

3. Fare clic su **Add Subscription** (Aggiungi abbonamento), fare clic su **Continue** (continua) e seguire la procedura. Verrai reindirizzato al portale Azure per creare il nuovo abbonamento.
4. Assicurati di selezionare il piano **NetApp Cloud Manager** che fornisce l'accesso alla conformità del cloud e non **Cloud Manager**.
5. Seguire i passaggi del video per associare un abbonamento Marketplace a un abbonamento Azure:

► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

6. Torna a Cloud Manager, seleziona il nuovo abbonamento e fai clic su **associate**.
7. Per verificare che l'abbonamento sia stato modificato, passare il mouse sopra la "i" nella scheda credenziali.

   Ora puoi annullare la tua vecchia iscrizione dal portale Azure.

8. Nel portale Azure, accedere a Software as a Service (SaaS), selezionare l'abbonamento e fare clic su **Annulla iscrizione**.

Attivare la scansione sulle origini dati

Introduzione alla conformità del cloud per Cloud Volumes ONTAP e Azure NetApp Files

Completa alcuni passaggi per iniziare a utilizzare la conformità cloud per Cloud Volumes ONTAP o Azure NetApp Files.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Implementare l'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Abilita la conformità al cloud nei tuoi ambienti di lavoro

Fare clic su **Cloud Compliance**, selezionare la scheda **Configuration** e attivare le scansioni di compliance per ambienti di lavoro specifici.

Garantire l'accesso ai volumi

Ora che la conformità al cloud è abilitata, assicurati che l'IT possa accedere ai volumi.

- L'istanza di conformità cloud richiede una connessione di rete a ciascuna subnet Cloud Volumes ONTAP o subnet Azure NetApp Files.
- I gruppi di sicurezza per Cloud Volumes ONTAP devono consentire connessioni in entrata dall'istanza di conformità cloud.
- Le policy di esportazione dei volumi NFS devono consentire l'accesso dall'istanza Cloud Compliance.
- Cloud Compliance necessita delle credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** e fornire le credenziali. Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere i dati che richiedono autorizzazioni elevate.

Configurare i volumi da sottoporre a scansione

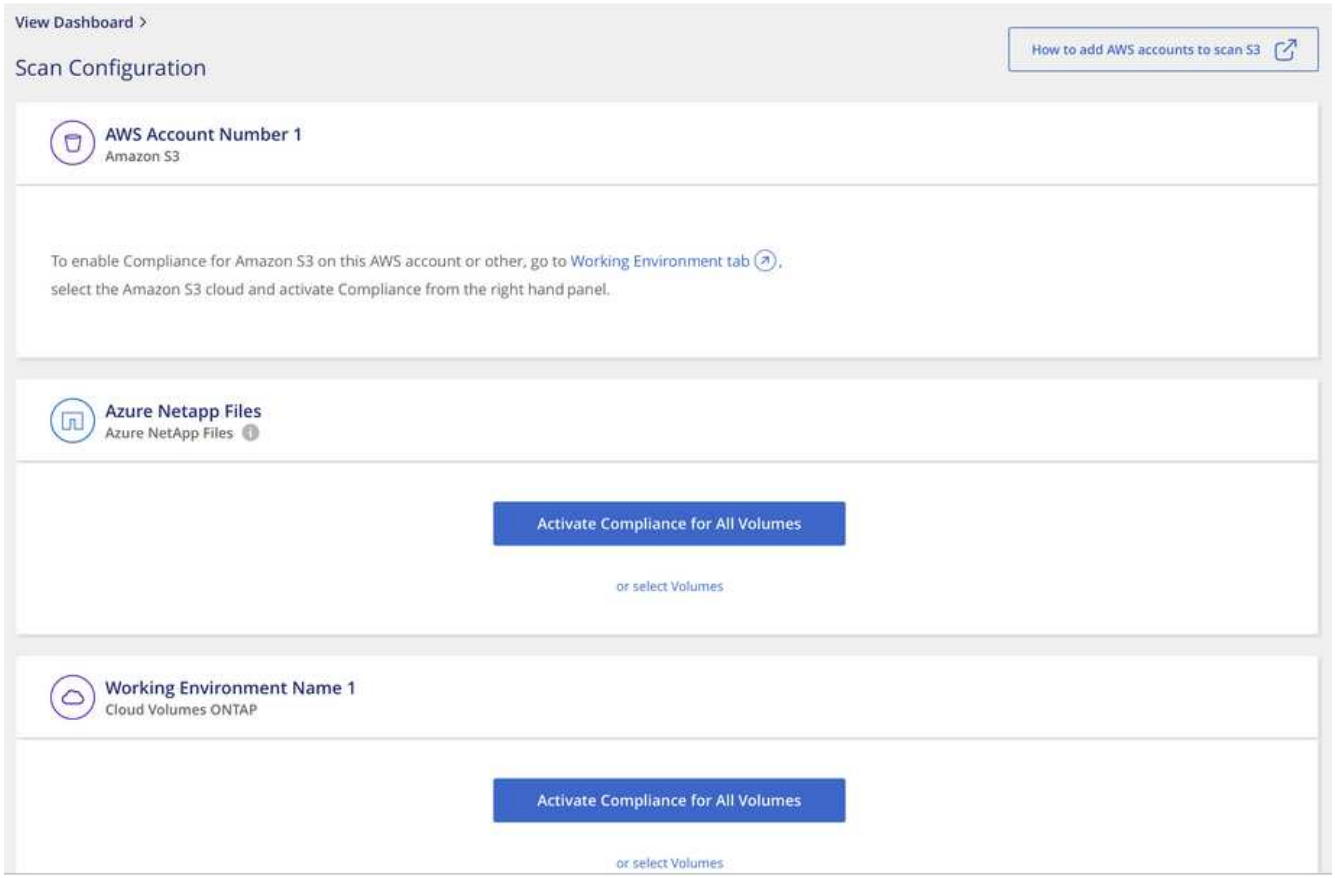
Seleziona i volumi che desideri sottoporre a scansione e la Cloud Compliance inizierà a eseguirne la scansione.

Implementazione dell'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Abilitare la conformità al cloud nei tuoi ambienti di lavoro

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**, quindi selezionare la scheda **Configuration**.



2. Per eseguire la scansione di tutti i volumi in un ambiente di lavoro, fare clic su **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi).

   Per eseguire la scansione solo di determinati volumi in un ambiente di lavoro, fare clic su **o selezionare Volumes** (volumi), quindi scegliere i volumi da sottoporre a scansione.

Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

Risultato

Cloud Compliance inizia la scansione dei dati in ogni ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la Cloud Compliance terminerà le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore.

Verificare che la conformità del cloud abbia accesso ai volumi

Assicurati che Cloud Compliance possa accedere ai volumi controllando il networking, i gruppi di sicurezza e le policy di esportazione. È necessario fornire le credenziali CIFS per la conformità al cloud in modo che possa accedere ai volumi CIFS.

Fasi

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di conformità cloud e ogni rete che include volumi per Cloud Volumes ONTAP o Azure NetApp Files.

   Per Azure NetApp Files, la conformità del cloud può eseguire la scansione solo dei volumi che si trovano nella stessa regione di Cloud Manager.

2. Assicurarsi che il gruppo di sicurezza per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di conformità cloud.

   È possibile aprire il gruppo di sicurezza per il traffico dall'indirizzo IP dell'istanza Cloud Compliance oppure aprire il gruppo di sicurezza per tutto il traffico dall'interno della rete virtuale.

3. Assicurarsi che le policy di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza Cloud Compliance in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la conformità cloud con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

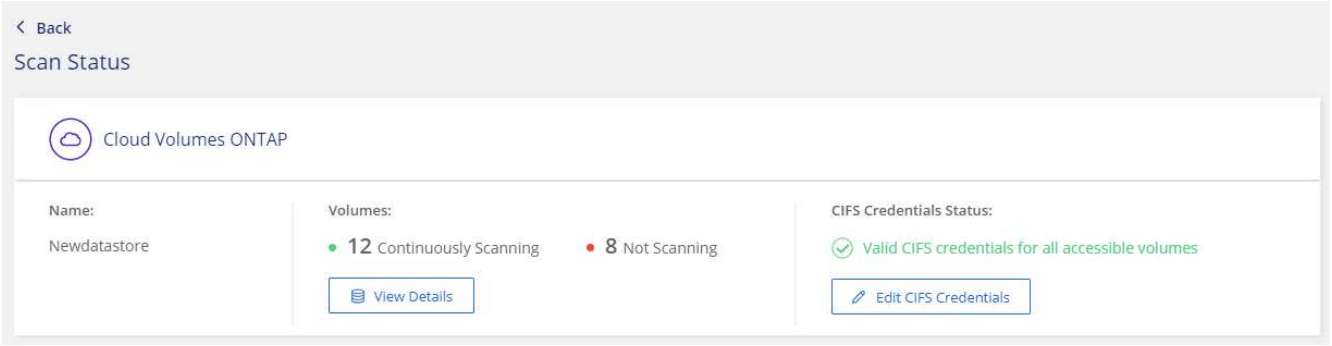
   a. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.

   b. Fare clic sulla scheda **Configurazione**.

   c. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per l'accesso ai volumi CIFS nel sistema.

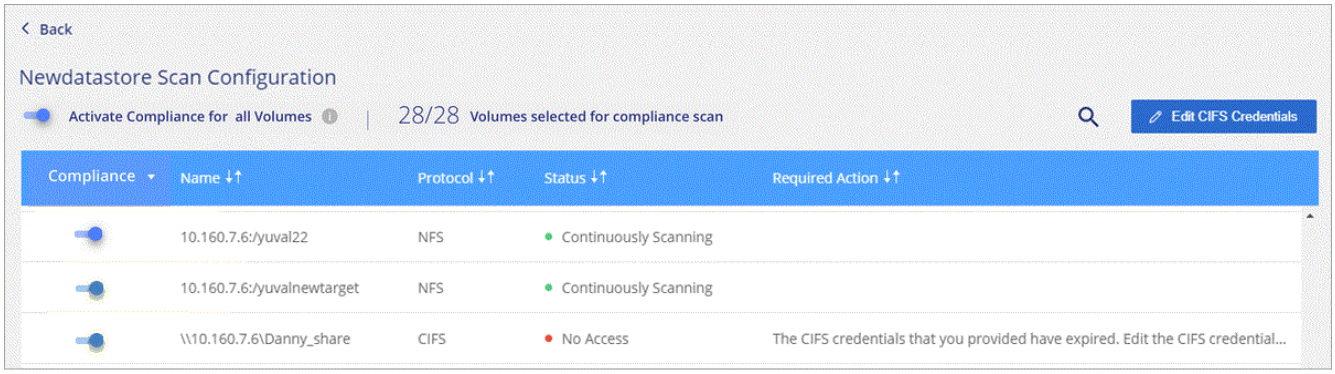
      Le credenziali possono essere di sola lettura, ma fornire credenziali di amministratore garantisce che Cloud Compliance possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza Cloud Compliance.

      Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.



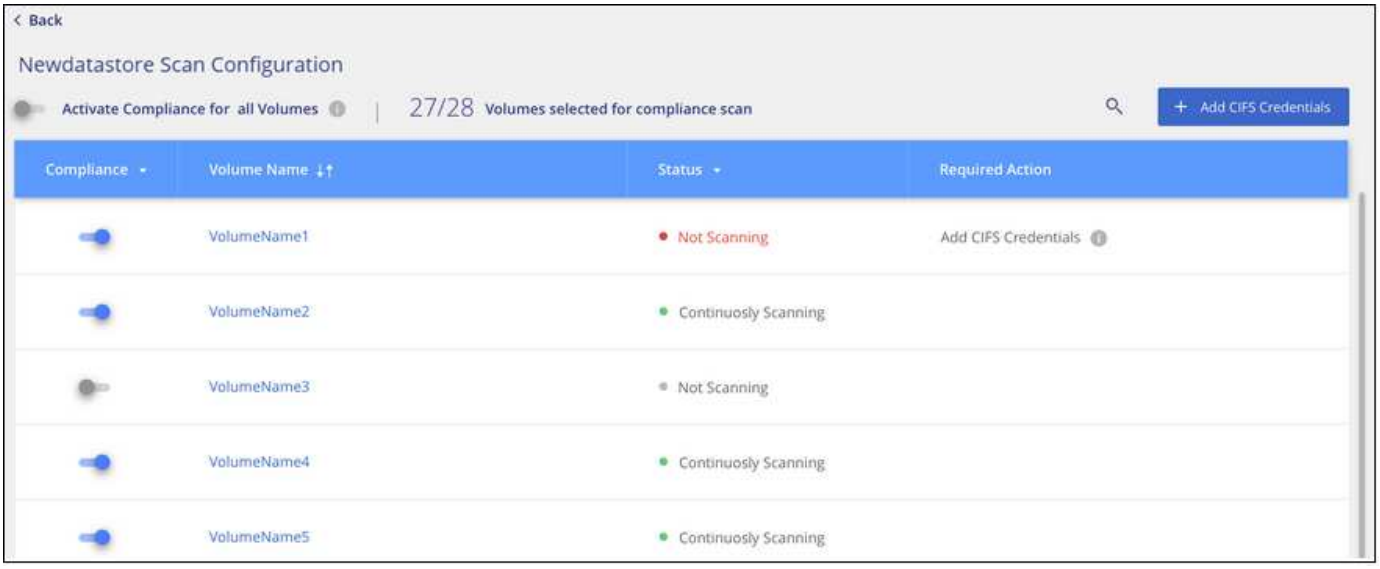
5. Nella pagina *Scan Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

   Ad esempio, l'immagine seguente mostra tre volumi, uno dei quali non è in grado di eseguire la scansione di Cloud Compliance a causa di problemi di connettività di rete tra l'istanza di Cloud Compliance e il volume.



Attivazione e disattivazione delle scansioni di compliance sui volumi

È possibile interrompere o avviare la scansione dei volumi in un ambiente di lavoro in qualsiasi momento dalla pagina Scan Configuration (Configurazione scansione). Si consiglia di eseguire la scansione di tutti i volumi.



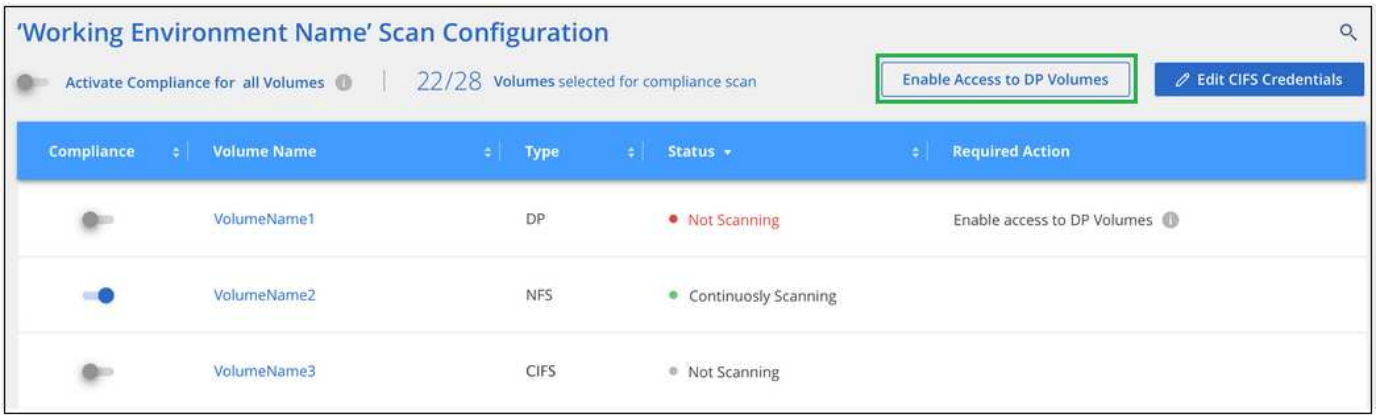
A:	Eseguire questa operazione:
Disattivare la scansione di un volume	Spostare il dispositivo di scorrimento del volume verso sinistra
Disattivare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento **Activate Compliance for all Volumes** (attiva compliance per tutti i volumi) verso sinistra
Abilitare la scansione per un volume	Spostare il dispositivo di scorrimento del volume verso destra
Abilitare la scansione per tutti i volumi	Spostare il dispositivo di scorrimento **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) verso destra

I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo quando è attivata l'impostazione **attiva conformità per tutti i volumi**. Quando questa impostazione è disattivata, è necessario attivare la scansione su ogni nuovo volume creato nell'ambiente di lavoro.

Scansione dei volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dei dati (DP) non vengono sottoposti a scansione perché non sono esposti esternamente e la Cloud Compliance non può accedervi. Questi volumi sono in genere i volumi di destinazione per le operazioni SnapMirror da un cluster ONTAP on-premise.

Inizialmente, l'elenco dei volumi Cloud Compliance identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.



Fasi

Se si desidera eseguire la scansione di questi volumi di protezione dei dati:

1. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina.
2. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Una volta attivata, Cloud Compliance crea una condivisione NFS da ogni volume DP attivato per la conformità, in modo che possa essere scansionato. Le policy di esportazione delle condivisioni consentono l'accesso solo

dall'istanza Cloud Compliance.

> Solo i volumi creati inizialmente come volumi NFS nel sistema ONTAP di origine vengono visualizzati nell'elenco dei volumi. I volumi di origine creati inizialmente come CIFS non vengono attualmente visualizzati in Cloud Compliance.

Introduzione alla conformità cloud per Amazon S3

Cloud Compliance può eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili che risiedono nello storage a oggetti S3. Cloud Compliance può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.

Imposta i requisiti S3 nel tuo ambiente cloud

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i requisiti per la conformità al cloud, tra cui la preparazione di un ruolo IAM e la configurazione della connettività da Cloud Compliance a S3. Consulta l'elenco completo.

Implementare l'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

Attivare la conformità sull'ambiente di lavoro S3

Selezionare l'ambiente di lavoro Amazon S3, fare clic su **Enable Compliance** (attiva conformità) e selezionare un ruolo IAM che includa le autorizzazioni richieste.

Selezionare i bucket da sottoporre a scansione

Seleziona i bucket che desideri sottoporre a scansione e Cloud Compliance inizierà a eseguirne la scansione.

Verifica dei prerequisiti di S3

I seguenti requisiti sono specifici per la scansione dei bucket S3.

Impostare un ruolo IAM per l'istanza Cloud Compliance

Cloud Compliance ha bisogno di autorizzazioni per connettersi ai bucket S3 del tuo account e per eseguirne la scansione. Impostare un ruolo IAM che includa le autorizzazioni elencate di seguito. Cloud Manager ti chiede di selezionare un ruolo IAM quando abiliti Cloud Compliance sull'ambiente di lavoro Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Connettività da Cloud Compliance ad Amazon S3

Cloud Compliance richiede una connessione ad Amazon S3. Il modo migliore per fornire tale connessione è tramite un endpoint VPC al 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 Compliance. 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 Compliance 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?"

In alternativa, è possibile stabilire la connessione utilizzando un gateway NAT.

Non puoi utilizzare un proxy per accedere a S3 tramite Internet.

Implementazione dell'istanza Cloud Compliance

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

È necessario implementare l'istanza in un connettore AWS in modo che Cloud Manager scopra automaticamente i bucket S3 in questo account AWS e li visualizzi in un ambiente di lavoro Amazon S3.

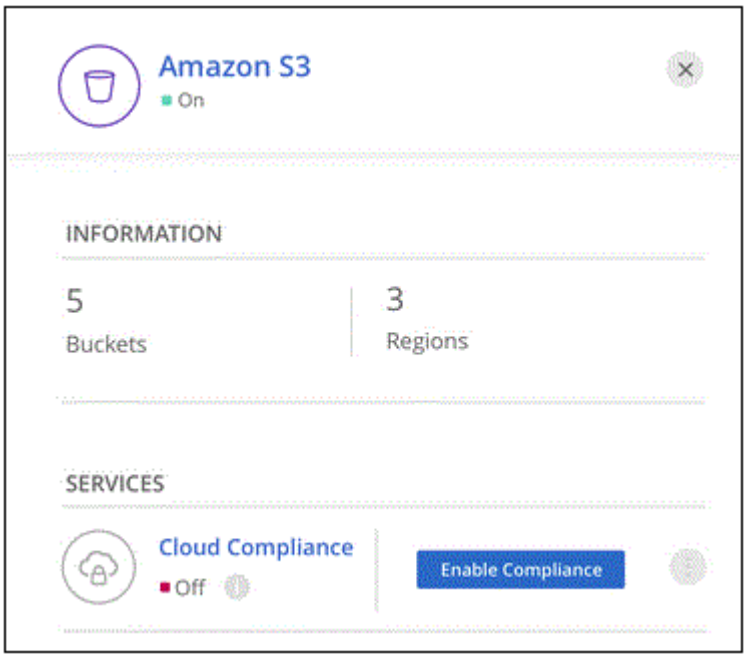
Attivazione della conformità nell'ambiente di lavoro S3

Attiva Cloud Compliance su Amazon S3 dopo aver verificato i prerequisiti.

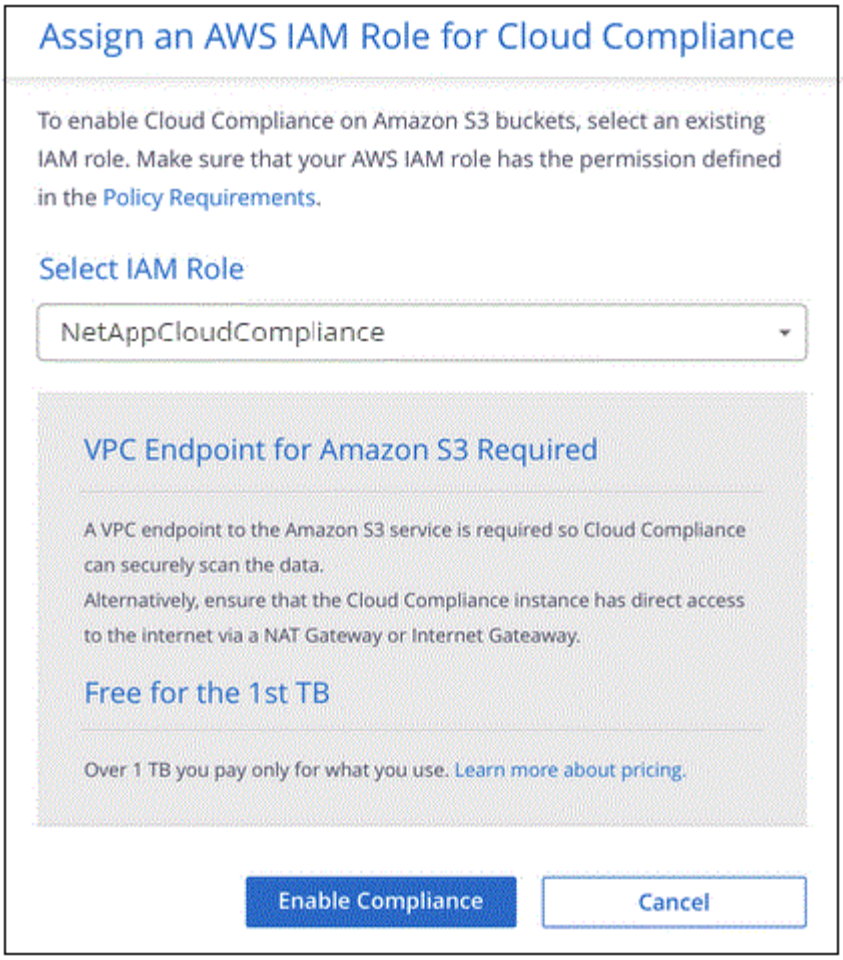
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Working Environments** (ambienti di lavoro).
2. Selezionare l'ambiente di lavoro Amazon S3.

3. Nel riquadro a destra, fare clic su **Enable Compliance** (attiva conformità).



4. Quando richiesto, assegnare un ruolo IAM all'istanza di Cloud Compliance che ha le autorizzazioni richieste.



5. Fare clic su **Enable Compliance** (attiva conformità)

È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina Scan Configuration (Configurazione scansione) facendo clic su E selezionando **Activate Compliance**.

Risultato

Cloud Manager assegna il ruolo IAM all'istanza.

Attivazione e disattivazione delle scansioni di compliance sui bucket S3

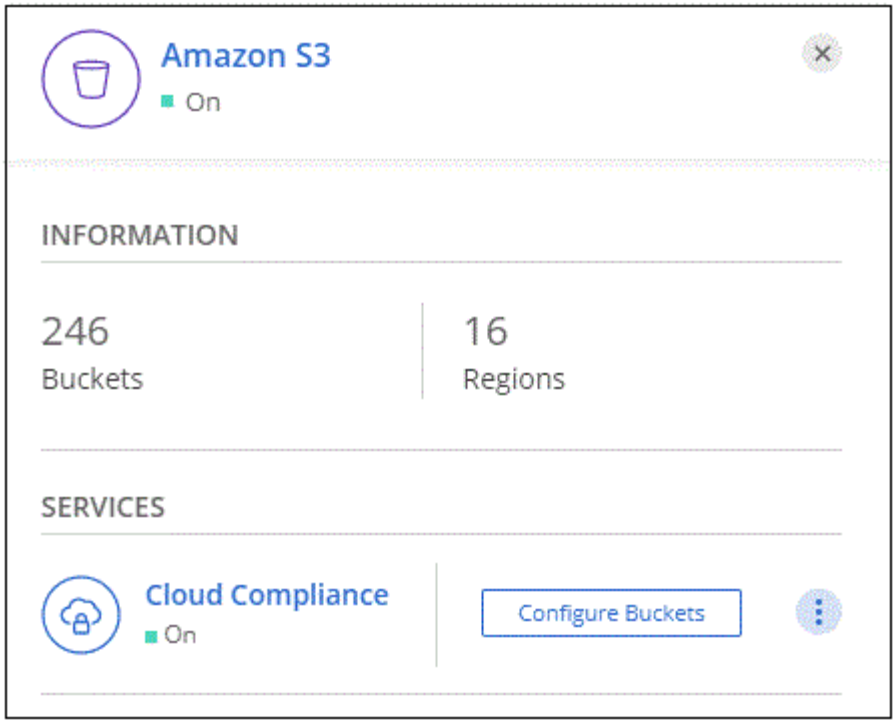
Dopo che Cloud Manager ha attivato Cloud Compliance su Amazon S3, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione.

Quando Cloud Manager viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

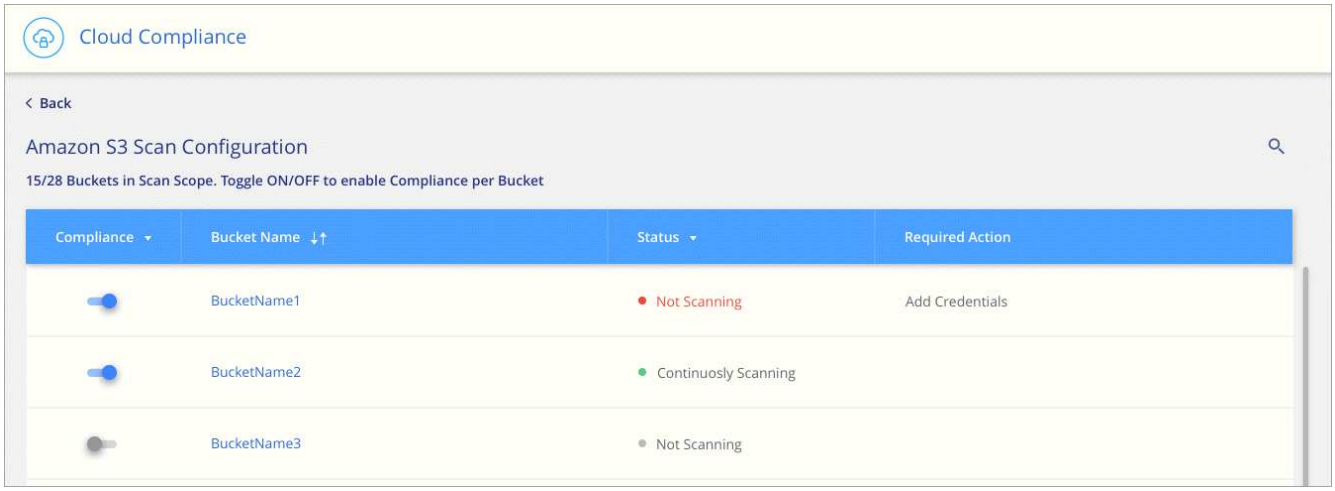
Anche la conformità al cloud può farlo Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS.

Fasi

1. Selezionare l'ambiente di lavoro Amazon S3.
2. Nel riquadro a destra, fare clic su **Configure Bucket** (Configura bucket).



3. Consentire la conformità sui bucket che si desidera sottoporre a scansione.



Risultato

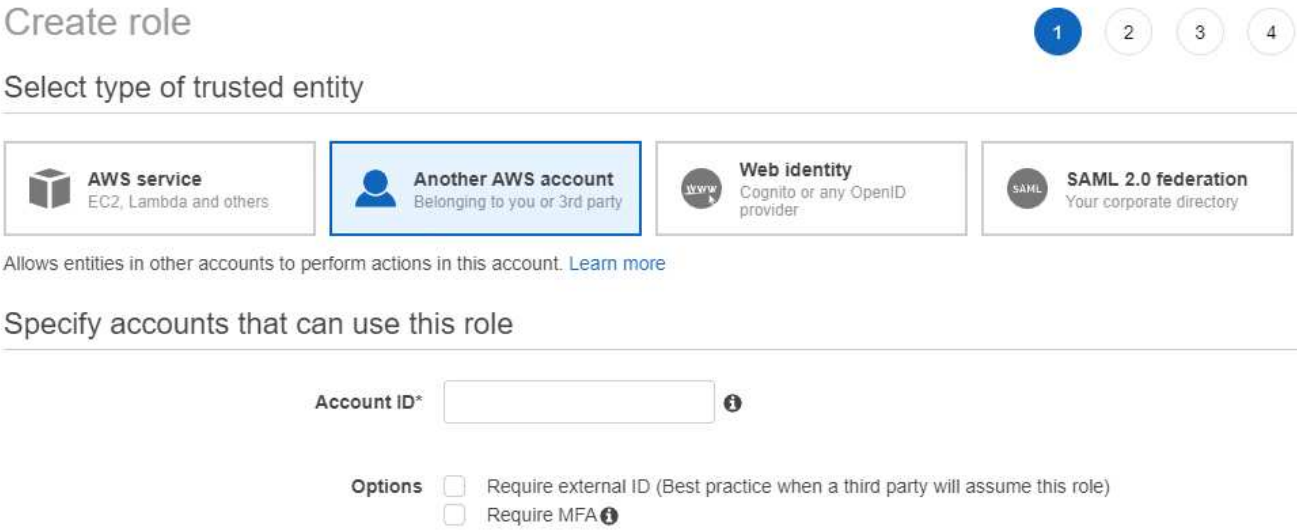
Cloud Compliance inizia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Scansione dei bucket da account AWS aggiuntivi

È possibile eseguire la scansione dei bucket S3 che si trovano sotto un account AWS diverso assegnando un ruolo da tale account per accedere all'istanza esistente di Cloud Compliance.

Fasi

1. Accedere all'account AWS di destinazione in cui si desidera eseguire la scansione dei bucket S3 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 Compliance.
- Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
- Allega la policy IAM sulla conformità al cloud. Assicurarsi che disponga delle autorizzazioni necessarie.

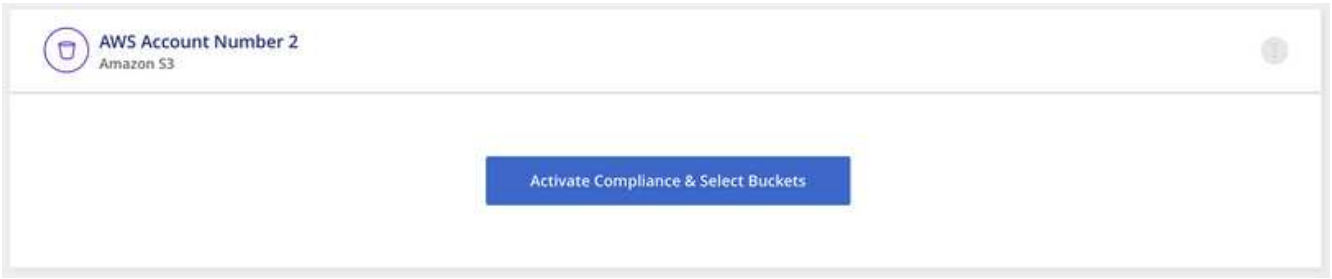
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Accedere all'account AWS di origine in cui risiede l'istanza Cloud Compliance e selezionare il ruolo IAM associato all'istanza.
   a. Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
   b. Fare clic su **Allega policy**, quindi su **Crea policy**.
   c. Creare una policy che includa l'azione "sts:AssumeRole" e l'ARN del ruolo creato nell'account di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

L'account del profilo dell'istanza Cloud Compliance ora ha accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Scan Configuration** (Configurazione scansione Amazon S3) per visualizzare il nuovo account AWS. Nota: La sincronizzazione dell'ambiente di lavoro del nuovo account e la visualizzazione di queste informazioni possono richiedere alcuni minuti per la conformità cloud.



4. Fare clic su **Activate Compliance & Select Bucket** (attiva Compliance e seleziona bucket) e selezionare i bucket da sottoporre a scansione.

Risultato

Cloud Compliance inizia la scansione dei nuovi bucket S3 che hai attivato.

Scansione degli schemi del database

Completa alcuni passaggi per iniziare la scansione degli schemi di database con Cloud

Compliance.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

 **Esaminare i prerequisiti del database**

Assicurarsi che il database sia supportato e di disporre delle informazioni necessarie per la connessione al database.

 **Implementare l'istanza Cloud Compliance**

"Implementazione della conformità al cloud in Cloud Manager" se non è già stata implementata un'istanza.

 **Aggiungere il server database**

Aggiungere il server database a cui si desidera accedere.

 **Selezionare gli schemi**

Selezionare gli schemi da sottoporre a scansione.

Verifica dei prerequisiti

Prima di attivare la conformità al cloud, verificare di disporre di una configurazione supportata.

Database supportati

Cloud Compliance può eseguire la scansione degli schemi dai seguenti database:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

La funzione di raccolta delle statistiche **deve essere abilitata** nel database.

Requisiti del database

È possibile eseguire la scansione di qualsiasi database con connettività all'istanza Cloud Compliance, indipendentemente da dove è ospitato. Per connettersi al database sono necessarie solo le seguenti informazioni:

- Indirizzo IP o nome host
- Porta
- Nome del servizio (solo per l'accesso ai database Oracle)
- Credenziali che consentono l'accesso in lettura agli schemi

  Quando si sceglie un nome utente e una password, è importante sceglierne uno che disponga delle autorizzazioni di lettura complete per tutti gli schemi e le tabelle che si desidera sottoporre a scansione. Si consiglia di creare un utente dedicato per il sistema Cloud Compliance con tutte le autorizzazioni necessarie.

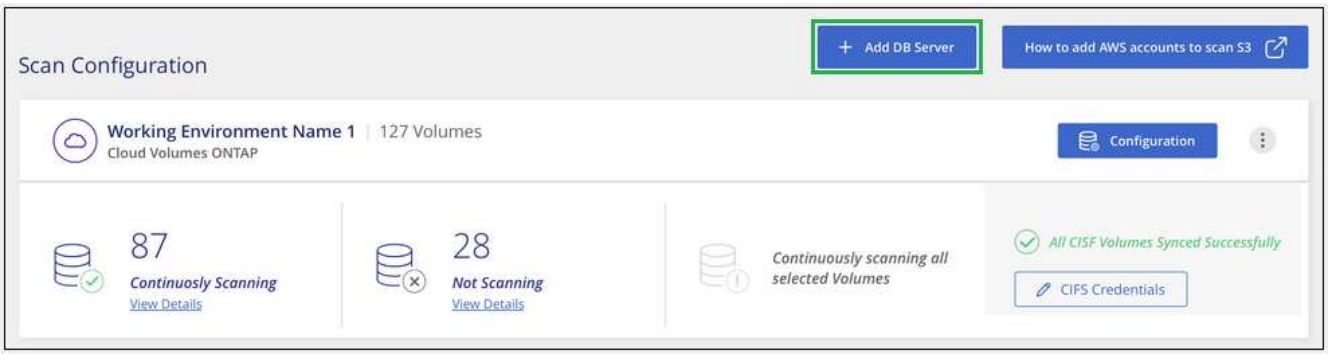
Nota: per MongoDB, è necessario un ruolo Admin di sola lettura.

Aggiunta del server database

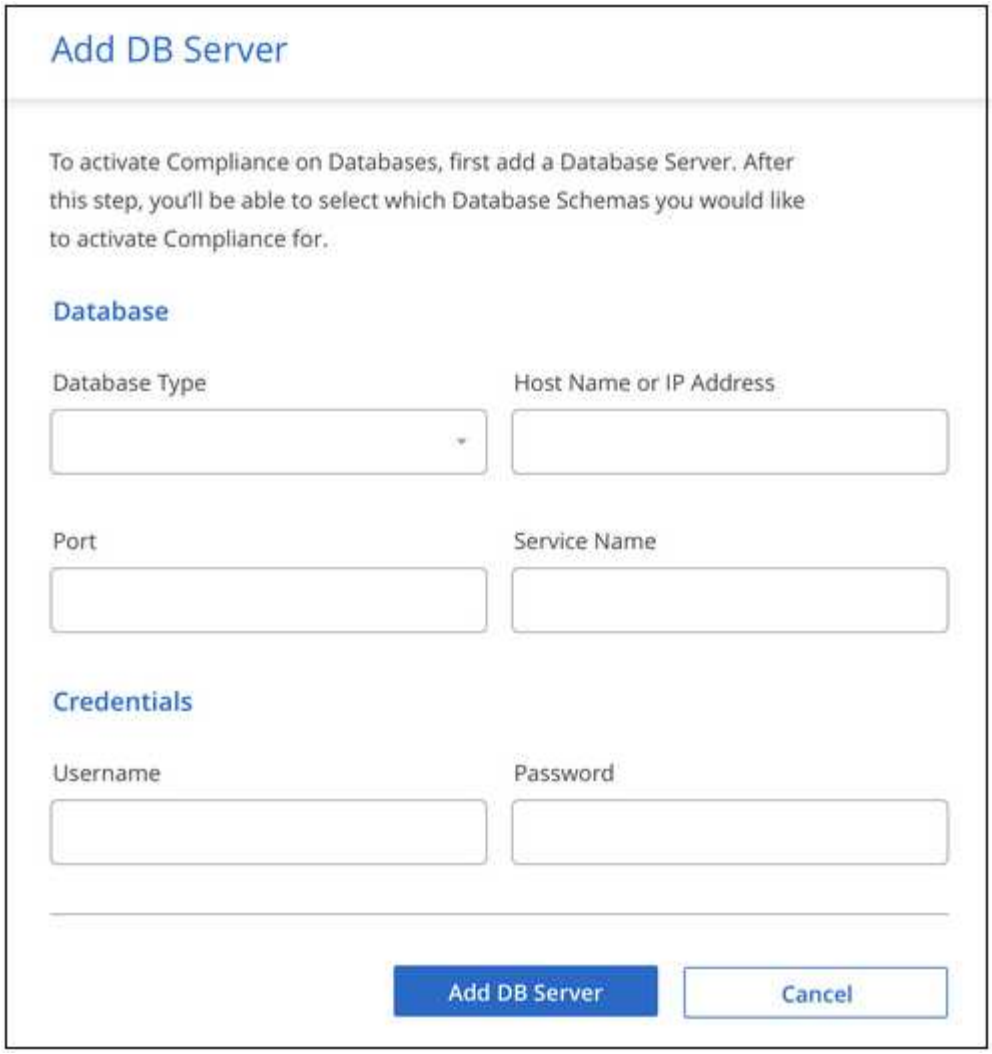
Devi avere "Ha già implementato un'istanza di Cloud Compliance in Cloud Manager".

Aggiungere il server di database in cui risiedono gli schemi.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Add DB Server** (Aggiungi server DB).



2. Inserire le informazioni richieste per identificare il server di database.
   a. Selezionare il tipo di database.
   b. Immettere la porta e il nome host o l'indirizzo IP per la connessione al database.
   c. Per i database Oracle, immettere il nome del servizio.
   d. Inserire le credenziali in modo che Cloud Compliance possa accedere al server.
   e. Fare clic su **Add DB Server** (Aggiungi server DB).



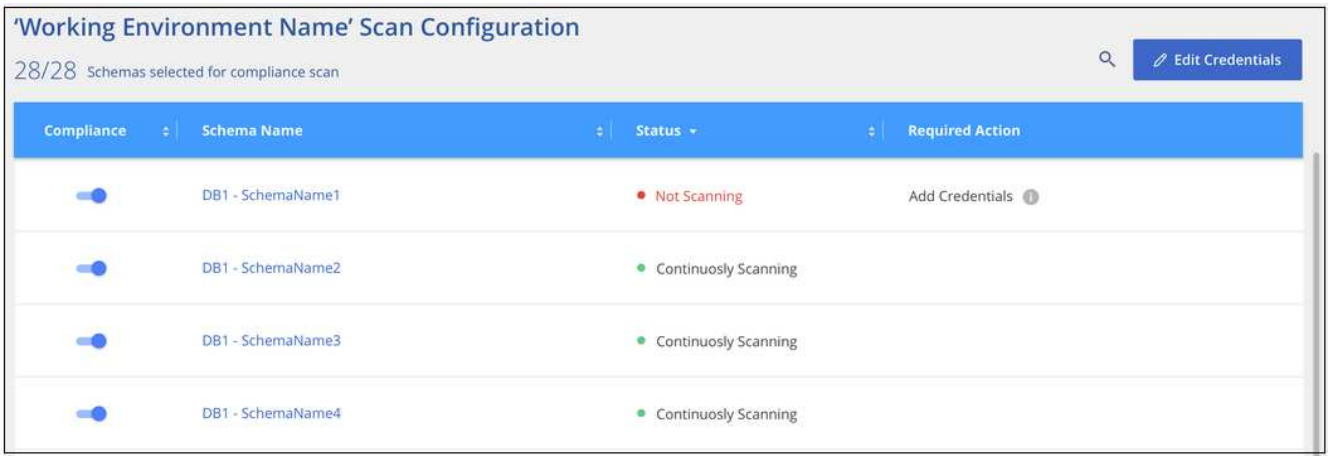
Il database viene aggiunto all'elenco delle directory di lavoro.

Attivazione e disattivazione delle scansioni di compliance sugli schemi di database

È possibile interrompere o avviare la scansione degli schemi in qualsiasi momento.

1. Dalla pagina *Scan Configuration*, fare clic sul pulsante **Configuration** relativo al database che si desidera configurare.

2. Selezionare gli schemi da sottoporre a scansione spostando il dispositivo di scorrimento verso destra.



Risultato

Cloud Compliance inizia la scansione degli schemi di database abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Rimozione di un database da Cloud Manager

Se non si desidera più eseguire la scansione di un determinato database, è possibile eliminarlo dall'interfaccia di Cloud Manager e interrompere tutte le scansioni.

Dalla pagina *Scan Configuration*, fare clic su Nella riga del database, quindi fare clic su **Remove DB Server** (Rimuovi server DB).

Scansione on-premise dei dati ONTAP con conformità al cloud utilizzando SnapMirror

È possibile eseguire la scansione dei dati ONTAP on-premise con la conformità al cloud replicando i dati NFS o CIFS on-premise in un ambiente di lavoro Cloud Volumes ONTAP e abilitando quindi la conformità. La scansione dei dati direttamente da un ambiente di lavoro ONTAP on-premise non è supportata.

Devi avere "Ha già implementato un'istanza di Cloud Compliance in Cloud Manager".

Fasi

1. Da Cloud Manager, creare una relazione SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP.
   a. "Scopri il cluster on-premise in Cloud Manager".
   b. "Creare una replica SnapMirror tra il cluster ONTAP on-premise e Cloud Volumes ONTAP da Cloud

Manager".

2. Per i volumi DP creati dai volumi di origine SMB, dalla CLI ONTAP, configurare i volumi di destinazione SMB per l'accesso ai dati. (Non è necessario per i volumi NFS perché l'accesso ai dati viene attivato automaticamente tramite Cloud Compliance).
   a. "Creare una condivisione SMB sul volume di destinazione".
   b. "Applicare gli ACL appropriati alla condivisione SMB nel volume di destinazione".
3. Da Cloud Manager, attivare la conformità cloud nell'ambiente di lavoro Cloud Volumes ONTAP che contiene i dati SnapMirror:
   a. Fare clic su **ambienti di lavoro**.
   b. Selezionare l'ambiente di lavoro che contiene i dati SnapMirror e fare clic su **Enable Compliance** (attiva conformità).

      "Fai clic qui per ricevere assistenza per abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP".

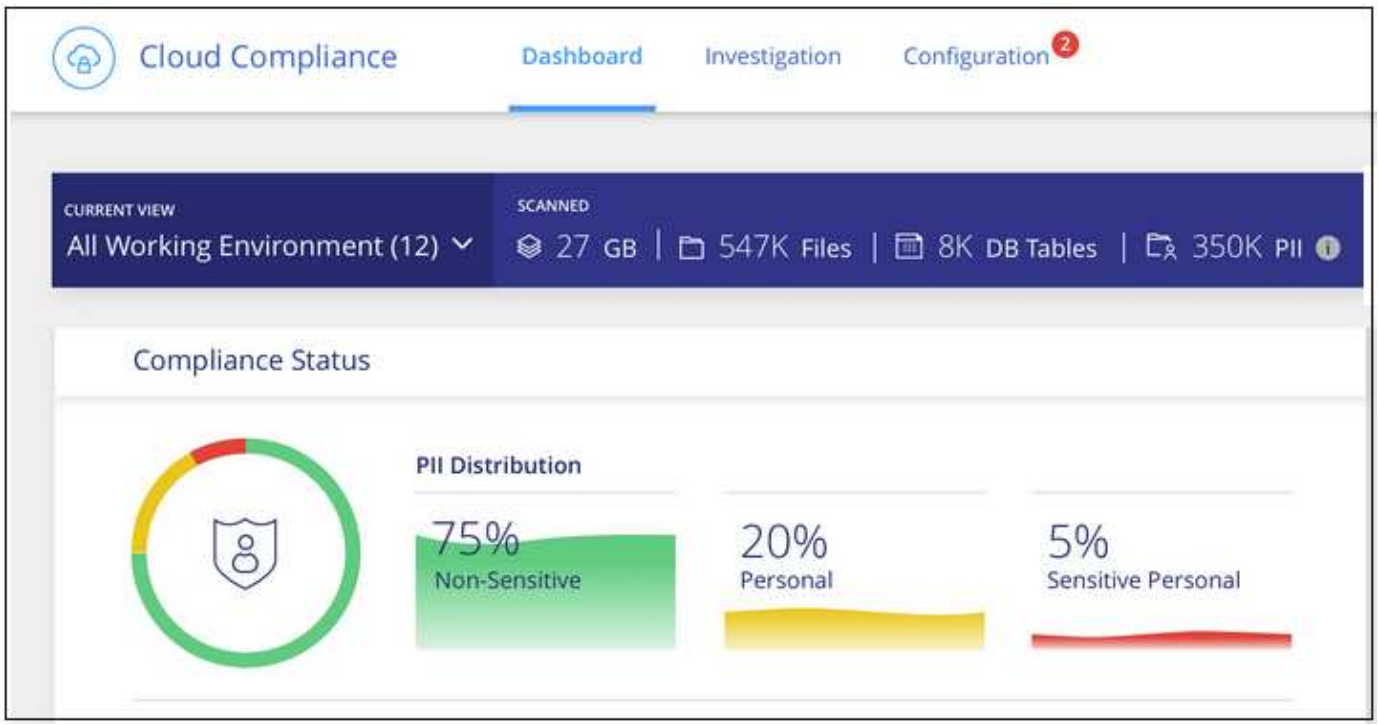
   c. Fare clic sul pulsante **Enable Access to DP Volumes** (Abilita accesso ai volumi DP) nella parte superiore della pagina *Scan Configuration* (Configurazione scansione).
   d. Attivare ciascun volume DP che si desidera sottoporre a scansione oppure utilizzare il controllo **Activate Compliance for All Volumes** (attiva conformità per tutti i volumi) per abilitare tutti i volumi, inclusi tutti i volumi DP.

Vedere "Scansione dei volumi di protezione dei dati" Per ulteriori informazioni sulla scansione di volumi DP.

Ottenere visibilità e controllo sui dati privati

Ottieni il controllo dei tuoi dati privati visualizzando i dettagli relativi ai dati personali e ai dati personali sensibili della tua organizzazione. Puoi anche ottenere visibilità esaminando le categorie e i tipi di file che Cloud Compliance ha trovato nei tuoi dati.

Per impostazione predefinita, il dashboard Cloud Compliance visualizza i dati di conformità per tutti gli ambienti di lavoro e i database.



Se si desidera visualizzare i dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

Dati personali

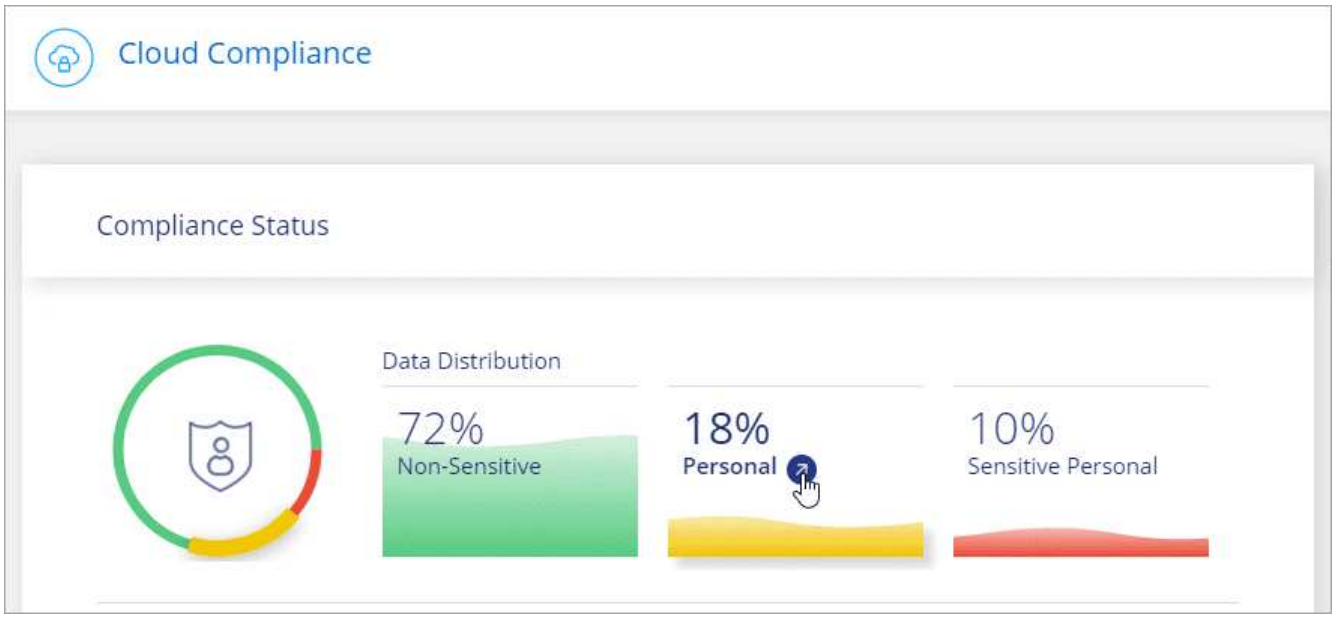
Cloud Compliance identifica automaticamente parole, stringhe e modelli specifici (Regex) all'interno dei dati. Ad esempio, informazioni di identificazione personale (PII), numeri di carta di credito, numeri di previdenza sociale, numeri di conto bancario e altro ancora. Consulta l'elenco completo.

Per alcuni tipi di dati personali, Cloud Compliance utilizza *Proximity Validation* per validarne i risultati. La convalida avviene cercando una o più parole chiave predefinite in prossimità dei dati personali trovati. Ad esempio, Cloud Compliance identifica un Numero di previdenza sociale (SSN) come SSN se viene visualizzato un termine di prossimità, ad esempio *SSN* o *social Security*. L'elenco seguente Mostra quando Cloud Compliance utilizza la convalida di prossimità.

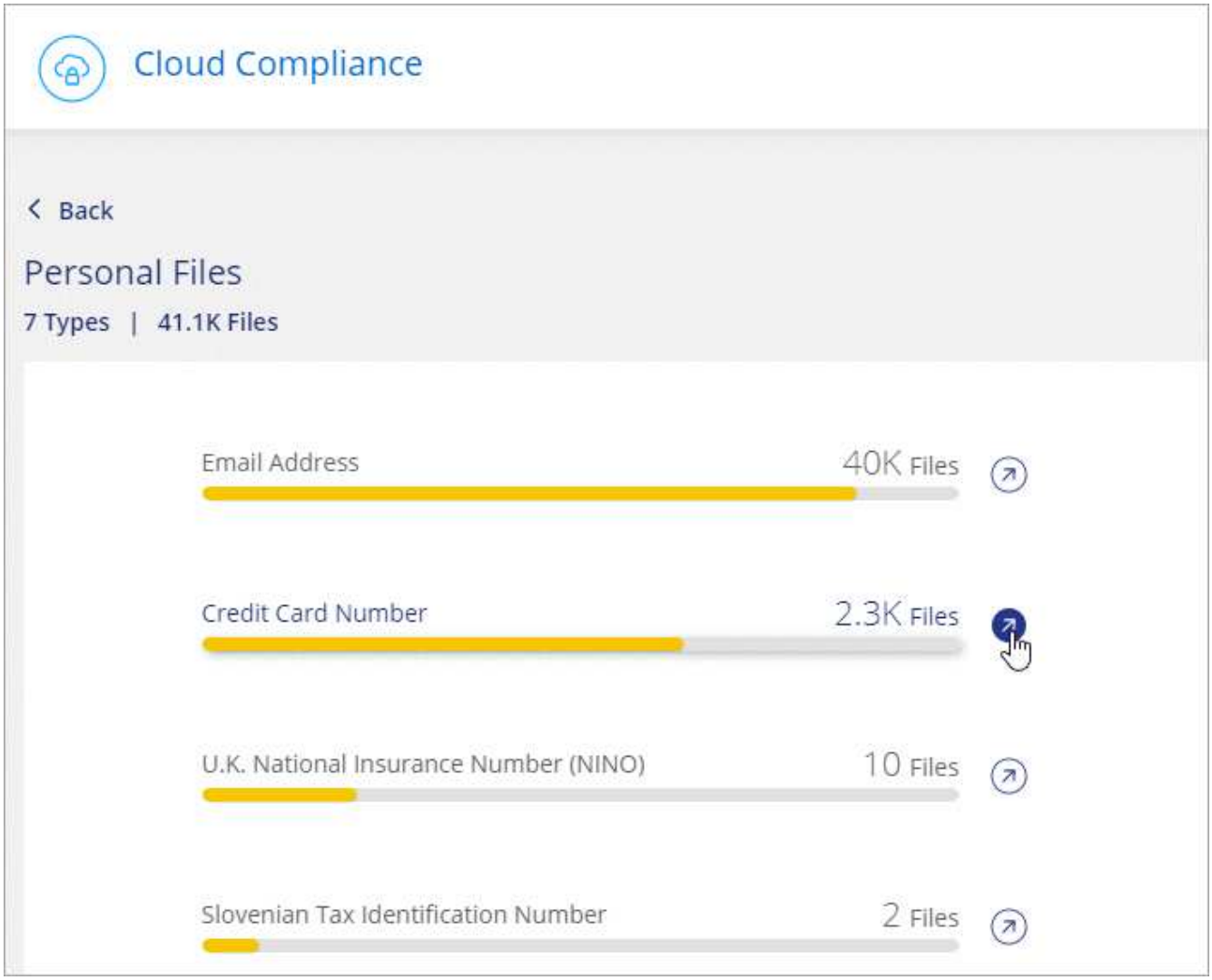
Visualizzazione di file contenenti dati personali

Fasi

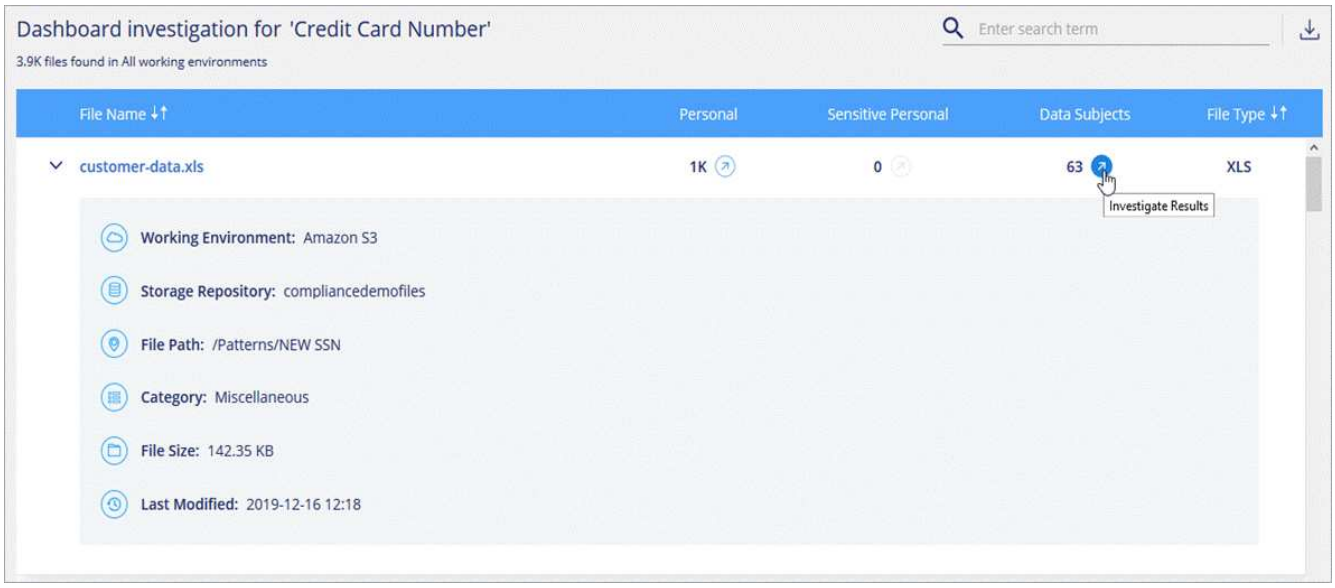
1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance** e fare clic sulla scheda **Dashboard**.
2. Per esaminare i dettagli di tutti i dati personali, fare clic sull'icona accanto alla percentuale dei dati personali.



3. Per esaminare i dettagli di un tipo specifico di dati personali, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali.

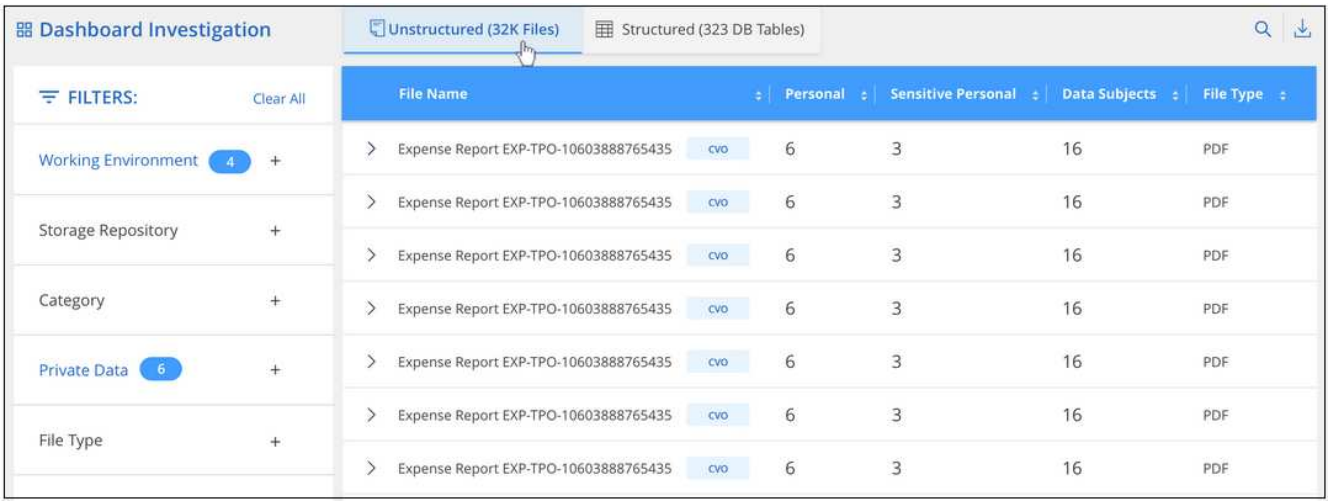


4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.



5. È inoltre possibile filtrare il contenuto della pagina di analisi per visualizzare solo i risultati desiderati. Le schede di primo livello consentono di visualizzare i dati dai file (dati non strutturati) o dai database (dati strutturati).

   Sono disponibili filtri per ambiente di lavoro, repository di storage, categoria, dati privati, tipo di file, Data dell'ultima modifica e se le autorizzazioni dell'oggetto S3 sono aperte all'accesso pubblico.



Tipi di dati personali

I dati personali contenuti nei file possono essere dati personali di carattere generale o identificativi nazionali. La terza colonna indica se la conformità al cloud utilizza convalida della prossimità per convalidare i risultati per l'identificatore.

Tipo	Identificatore	Convalida della prossimità?
Generale	Indirizzo e-mail	No
	Numero della carta di credito	No
	Numero IBAN (International Bank account Number)	No

Tipo	Identificatore	Convalida della prossimità?
Identificatori nazionali	ID belga (numero nazionale)	Sì
	ID brasiliano (CPF)	Sì
	ID bulgaro (UCN)	Sì
	California driver’s License	Sì
	ID croato (OIB)	Sì
	Codice fiscale di Cipro (TIC)	Sì
	Documento d’identità ceco/slovacco	Sì
	ID danese (CPR)	Sì
	Olandese ID (BSN)	Sì
	ID estone	Sì
	ID finlandese (HETU)	Sì
	Francese Tax Identification Number (SPI)	Sì
	Codice fiscale tedesco (Steuerliche Identifikationsnummer)	Sì
	ID greco	Sì
	Codice fiscale ungherese	Sì
	Irish ID (PPS) (ID irlandese)	Sì
	ID Israeliano	Sì
	Codice fiscale italiano	Sì
	Documento d’identità lettone	Sì
	ID lituano	Sì
	Lussemburgo ID	Sì
	ID maltese	Sì
	ID polacco (PESEL)	Sì
	Portoghese Tax Identification Number (NIF)	Sì
	ID rumeno (CNP)	Sì
	ID sloveno (EMSO)	Sì
	ID sudafricano	Sì
	Codice fiscale spagnolo	Sì
	ID svedese	Sì
	REGNO UNITO ID (NINO)	Sì
	Numero di previdenza sociale (SSN) USA	Sì

Dati personali sensibili

Cloud Compliance identifica automaticamente tipi speciali di informazioni personali sensibili, come definito dalle normative sulla privacy, ad esempio "articoli 9 e 10 del GDPR". Ad esempio, informazioni relative alla salute, all'origine etnica o all'orientamento sessuale di una persona. Consulta l'elenco completo.

Cloud Compliance utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP), l'apprendimento automatico (ML) e il calcolo cognitivo (CC) per comprendere il significato dei contenuti che scansiona al fine di estrarre le entità e classificarle di conseguenza.

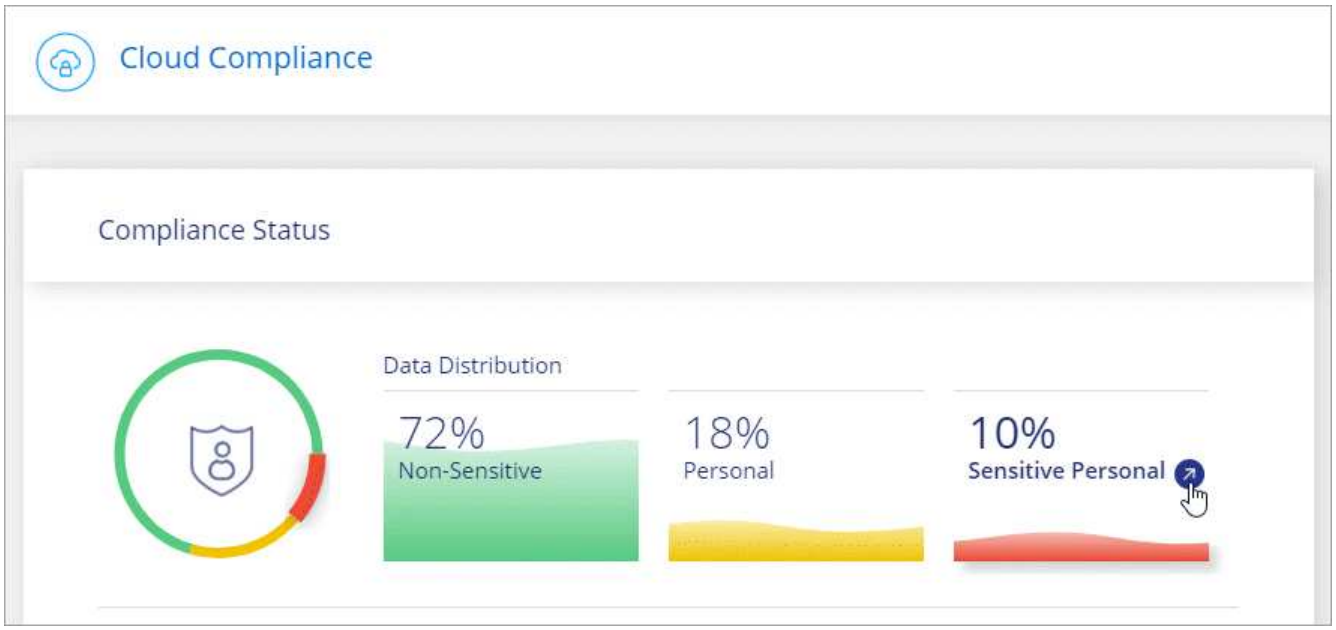
Ad esempio, una categoria di dati GDPR sensibili è l'origine etnica. Grazie alle sue capacità di NLP, Cloud Compliance è in grado di distinguere la differenza tra una frase con la dicitura "George is Mexican" (che indica i dati sensibili come specificato nell'articolo 9 del GDPR) e "George is Eating Mexican Food" (George is Eating Mexican Food).

Quando si esegue la scansione di dati personali sensibili, è supportata solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

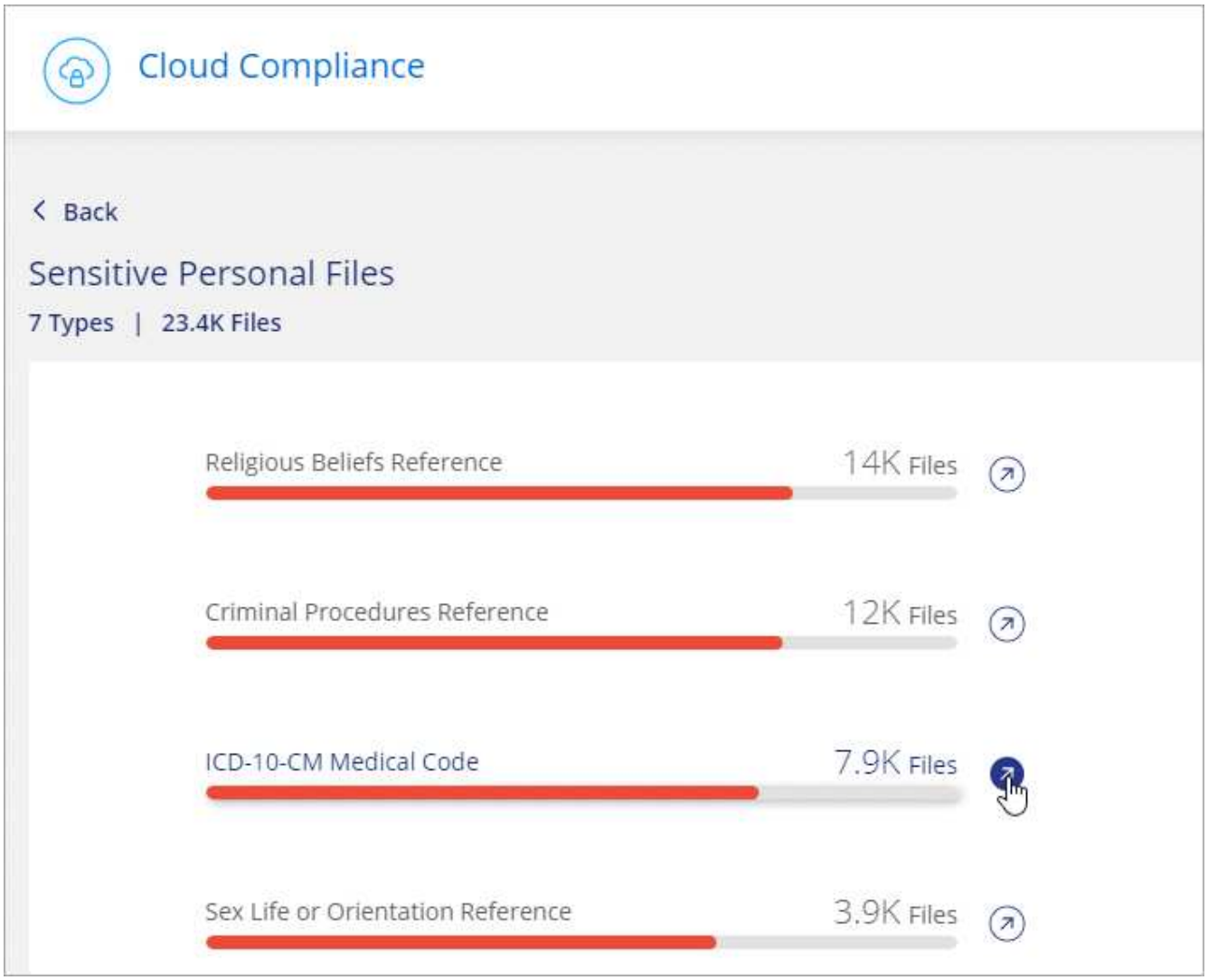
Visualizzazione di file contenenti dati personali sensibili

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. Per esaminare i dettagli di tutti i dati personali sensibili, fare clic sull'icona accanto alla percentuale dei dati personali sensibili.



3. Per esaminare i dettagli di un tipo specifico di dati personali sensibili, fare clic su **Visualizza tutto**, quindi fare clic sull'icona **esamina risultati** per un tipo specifico di dati personali sensibili.



4. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Tipi di dati personali sensibili

I dati personali sensibili che Cloud Compliance può trovare nei file includono:

Riferimento alle procedure penali
Dati relativi alle condanne e ai reati penali di una persona fisica.

Riferimento di etnia
Dati relativi alla razza o all'origine etnica di una persona fisica.

Riferimento di salute
Dati relativi alla salute di una persona fisica.

Codici medici ICD-9-CM
Codici utilizzati nel settore medico e sanitario.

Codici medici ICD-10-CM
Codici utilizzati nel settore medico e sanitario.

Riferimento alle credenze filosofiche

Dati relativi alle convinzioni filosofiche di una persona naturale.

Riferimenti alle credenze religiose

Dati relativi alle convinzioni religiose di una persona fisica.

Sex Life o orientamento di riferimento

Dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Categorie

Cloud Compliance prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. Vedere l'elenco delle categorie.

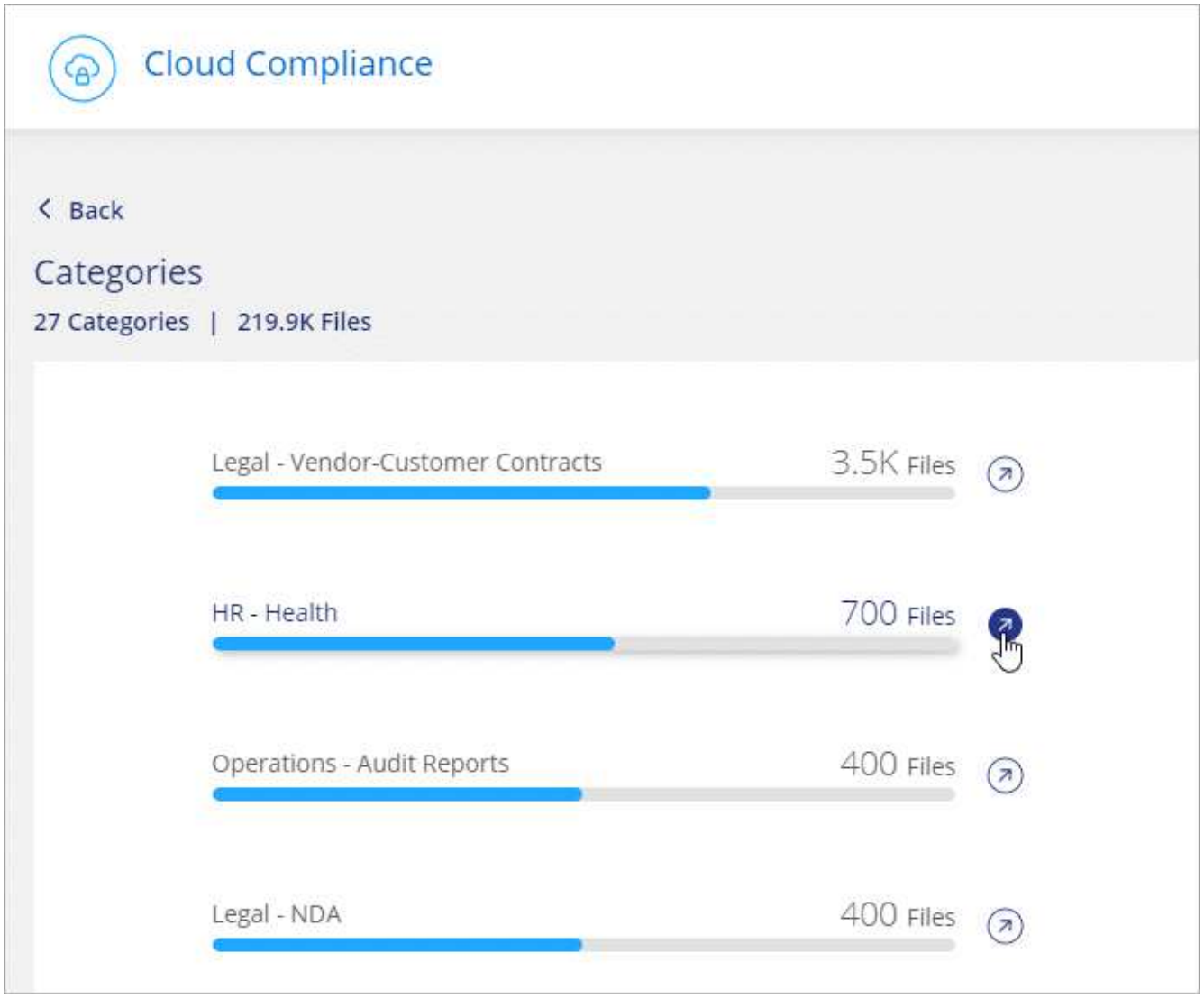
Le categorie possono aiutarti a capire cosa accade con i tuoi dati mostrando i tipi di informazioni di cui disponi. Ad esempio, una categoria come i curriculum o i contratti dei dipendenti può includere dati sensibili. Quando si analizzano i risultati, è possibile che i contratti dei dipendenti siano memorizzati in una posizione non sicura. A questo punto, è possibile correggere il problema.

Per le categorie è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

Visualizzazione dei file in base alle categorie

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. Fare clic sull'icona **esamina risultati** di una delle 4 categorie principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto** e quindi sull'icona corrispondente a una delle categorie.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Tipi di categorie

La conformità al cloud classifica i tuoi dati nel modo seguente:

Finanza

- Bilanci
- Ordini di acquisto
- Fatture
- Report trimestrali

FC

- Controlli in background
- Piani di compensazione
- Contratti con i dipendenti
- Recensioni dei dipendenti

- Salute
- Riprende

Legale

- NDA
- Contratti fornitore-cliente

Marketing

- Campagne
- Conferenze

Operazioni

- Report di audit

Vendite

- Ordini di vendita

Servizi

- RFI
- RFP
- SOW
- Formazione

Supporto

- Reclami e biglietti

Categorie di metadati

- Dati dell'applicazione
- Archiviare i file
- Audio
- Dati delle applicazioni di business
- File CAD
- Codice
- Database e file di indice
- File di progettazione
- Email Application Data (dati applicazione email)
- Eseguibili
- Dati delle applicazioni finanziarie
- Health Application Data
- Immagini
- Registri
- Documenti vari
- Presentazioni varie

- Fogli di calcolo vari
- Video

Tipi di file

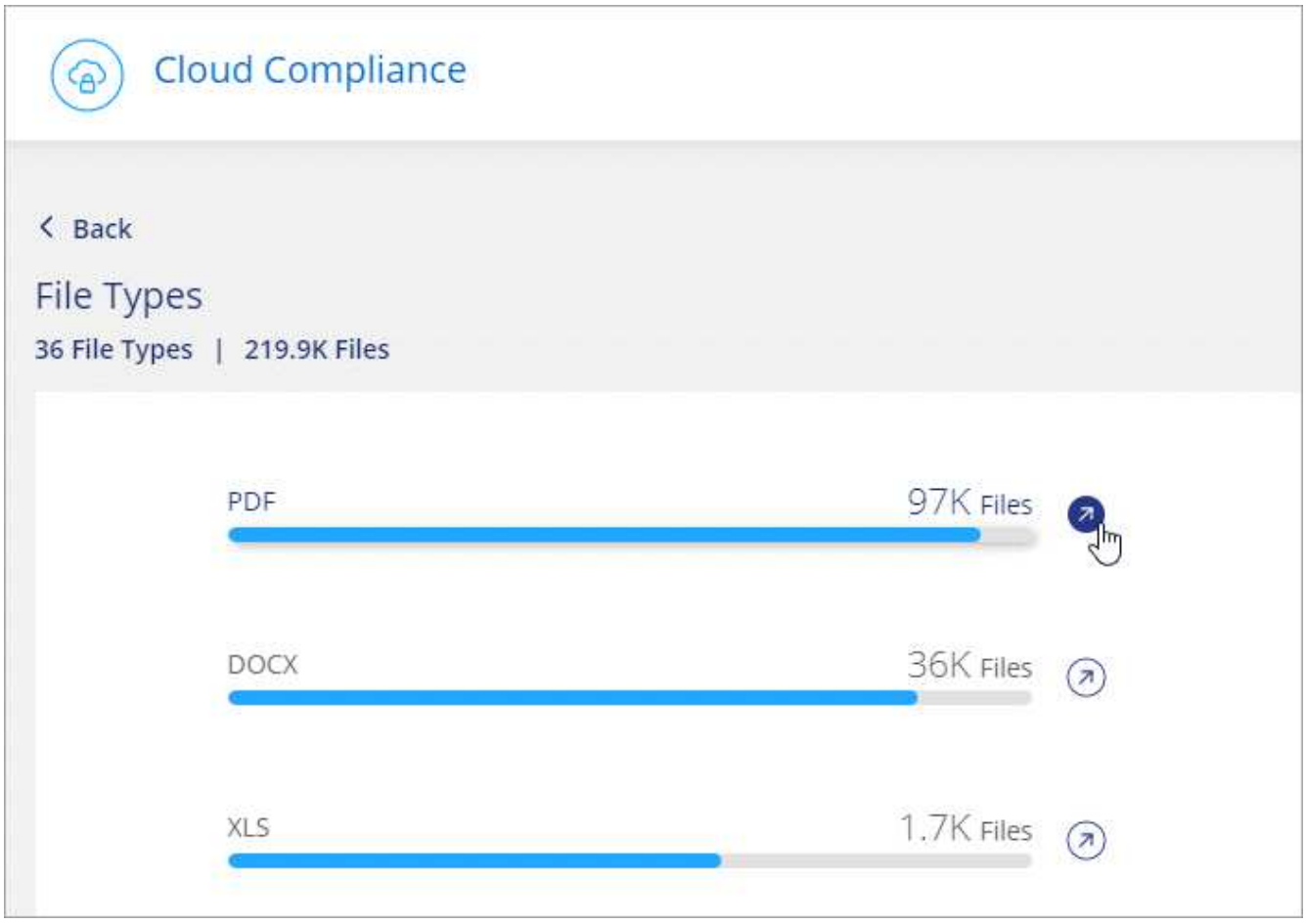
Cloud Compliance prende i dati sottoposti a scansione e li suddivide in base al tipo di file. La revisione dei tipi di file consente di controllare i dati sensibili, poiché alcuni tipi di file potrebbero non essere memorizzati correttamente. Vedere l'elenco dei tipi di file.

Ad esempio, è possibile memorizzare file CAD che includono informazioni molto sensibili sull'organizzazione. Se non sono protetti, è possibile assumere il controllo dei dati sensibili limitando le autorizzazioni o spostando i file in un'altra posizione.

Visualizzazione dei tipi di file

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. Fare clic sull'icona **esamina risultati** per uno dei 4 tipi di file principali direttamente dalla schermata principale oppure fare clic su **Visualizza tutto**, quindi fare clic sull'icona corrispondente a uno qualsiasi dei tipi di file.



3. Esaminare i dati ricercando, ordinando, espandendo i dettagli di un file specifico, facendo clic su **esamina risultati** per visualizzare le informazioni mascherate o scaricando l'elenco dei file.

Tipi di file

Cloud Compliance esegue la scansione di tutti i file per individuare informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Tuttavia, quando Cloud Compliance rileva le informazioni personali identificabili (PII) o esegue una ricerca DSAR, sono supportati solo i seguenti formati di file: .PDF, .DOCX, .DOC, .PPTX, .XLS, XLSX, .CSV, .TXT, .RTF E .JSON.

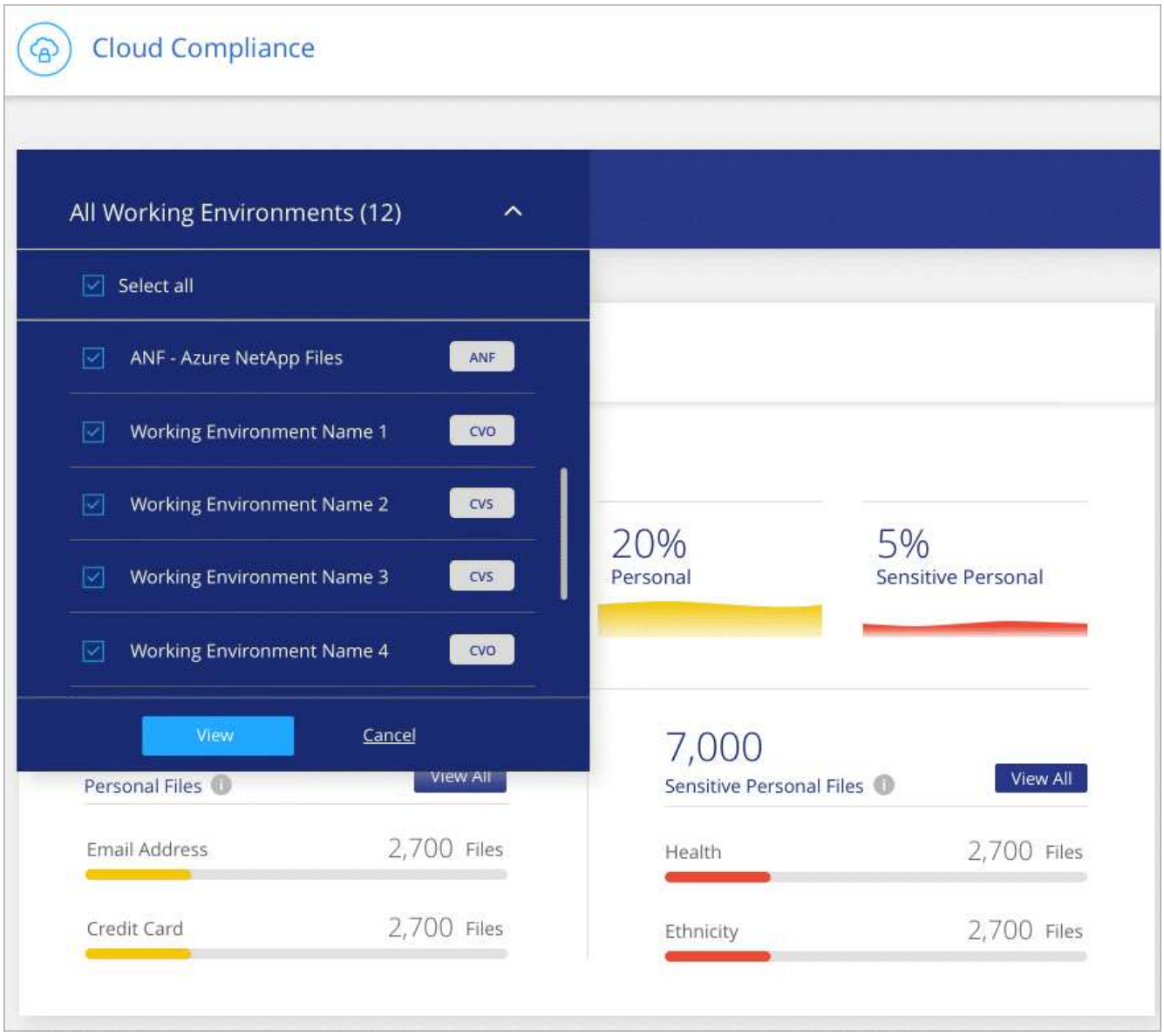
Visualizzazione dei dati da ambienti di lavoro specifici

Puoi filtrare i contenuti della dashboard Cloud Compliance per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando filtri la dashboard, Cloud Compliance regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



Accuratezza delle informazioni rilevate

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

In base ai nostri test, la tabella seguente mostra l'accuratezza delle informazioni rilevate dalla Cloud Compliance. Lo suddivideremo per *precisione* e *richiamo*:

Precisione

La probabilità che ciò che trova Cloud Compliance sia stata identificata correttamente. Ad esempio, un tasso di precisione del 90% per i dati personali significa che 9 file su 10 identificati come contenenti informazioni personali contengono effettivamente informazioni personali. 1 file su 10 sarebbe un falso positivo.

Ricorda

La probabilità che la conformità cloud trovi ciò che dovrebbe. Ad esempio, un tasso di richiamo del 70% per i dati personali significa che Cloud Compliance è in grado di identificare 7 file su 10 che contengono effettivamente informazioni personali nella tua organizzazione. La conformità al cloud perderebbe il 30% dei

dati e non verrà visualizzata nella dashboard.

Cloud Compliance è in una release di disponibilità controllata e stiamo costantemente migliorando la precisione dei nostri risultati. Tali miglioramenti saranno automaticamente disponibili nelle future release di Cloud Compliance.

Tipo	Precisione	Ricorda
Dati personali - Generale	90%-95%	60%-80%
Dati personali - identificatori del Paese	30%-60%	40%-60%
Dati personali sensibili	80%-95%	20%-30%
Categorie	90%-97%	60%-80%

Contenuto di ciascun report elenco file (file CSV)

Da ogni pagina di analisi è possibile scaricare elenchi di file (in formato CSV) che includono dettagli sui file identificati. Se sono presenti più di 10,000 risultati, nell'elenco vengono visualizzati solo i primi 10,000 risultati.

Ciascun elenco di file include le seguenti informazioni:

- Nome del file
- Tipo di ubicazione
- Ambiente di lavoro
- Repository di storage
- Protocollo
- Percorso del file
- Tipo di file
- Categoria
- Informazioni personali
- Informazioni personali sensibili
- Data di rilevamento dell'eliminazione

  Una data di rilevamento dell'eliminazione identifica la data in cui il file è stato cancellato o spostato. In questo modo è possibile identificare quando sono stati spostati file sensibili. I file cancellati non fanno parte del numero di file visualizzato nella dashboard o nella pagina di analisi. I file vengono visualizzati solo nei report CSV.

Visualizzazione dei report di conformità

Cloud Compliance fornisce report che puoi utilizzare per comprendere meglio lo stato del programma per la privacy dei dati della tua organizzazione.

Per impostazione predefinita, il dashboard Cloud Compliance visualizza i dati di conformità per tutti gli ambienti di lavoro e i database. Se si desidera visualizzare report contenenti dati solo per alcuni ambienti di lavoro, selezionare gli ambienti di lavoro.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Report sulla valutazione dei rischi per la privacy

Il report sulla valutazione dei rischi per la privacy fornisce una panoramica dello stato di rischio per la privacy della tua organizzazione, come richiesto dalle normative sulla privacy come GDPR e CCPA. Il report contiene le seguenti informazioni:

Stato di compliance

R punteggio di severità e la distribuzione dei dati, sia che si tratti di dati personali, non sensibili o sensibili.

Panoramica della valutazione

Analisi dei tipi di dati personali rilevati, nonché delle categorie di dati.

Argomenti trattati in questa valutazione

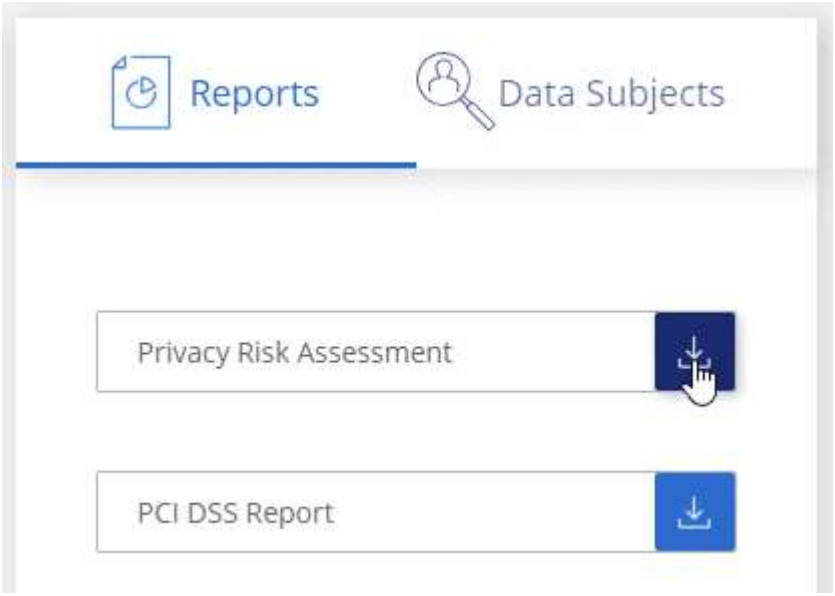
Il numero di persone, per località, per le quali sono stati trovati identificatori nazionali.

Generazione del report sulla valutazione dei rischi per la privacy

Accedere alla scheda Compliance per generare il report.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. In **Report**, fare clic sull'icona di download accanto a **Privacy Risk Assessment**.



Risultato

Cloud Compliance genera un report PDF che puoi rivedere e inviare ad altri gruppi in base alle esigenze.

Punteggio di severità

Cloud Compliance calcola il punteggio di severità per il report di valutazione dei rischi per la privacy sulla base

di tre variabili:

- La percentuale di dati personali su tutti i dati.
- La percentuale di dati personali sensibili rispetto a tutti i dati.
- La percentuale di file che includono soggetti dati, determinata da identificatori nazionali come ID nazionali, numeri di previdenza sociale e numeri di identificazione fiscale.

La logica utilizzata per determinare il punteggio è la seguente:

Punteggio di severità	Logica
0	Tutte e tre le variabili sono esattamente 0%
1	Una delle variabili è maggiore dello 0%
2	Una delle variabili è maggiore del 3%
3	Due delle variabili sono maggiori del 3%
4	Tre delle variabili sono maggiori del 3%
5	Una delle variabili è maggiore del 6%
6	Due delle variabili sono maggiori del 6%
7	Tre delle variabili sono maggiori del 6%
8	Una delle variabili è maggiore del 15%
9	Due delle variabili sono maggiori del 15%
10	Tre delle variabili sono maggiori del 15%

Report PCI DSS

Il report PCI DSS (Payment Card Industry Data Security Standard) consente di identificare la distribuzione delle informazioni sulle carte di credito nei file. Il report contiene le seguenti informazioni:

Panoramica
: Quanti file contengono informazioni sulla carta di credito e in quali ambienti di lavoro.

Crittografia
: La percentuale di file contenenti informazioni sulla carta di credito presenti in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware
: La percentuale di file contenenti informazioni sulla carta di credito che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione
: Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni della carta di credito per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sulla carta di credito

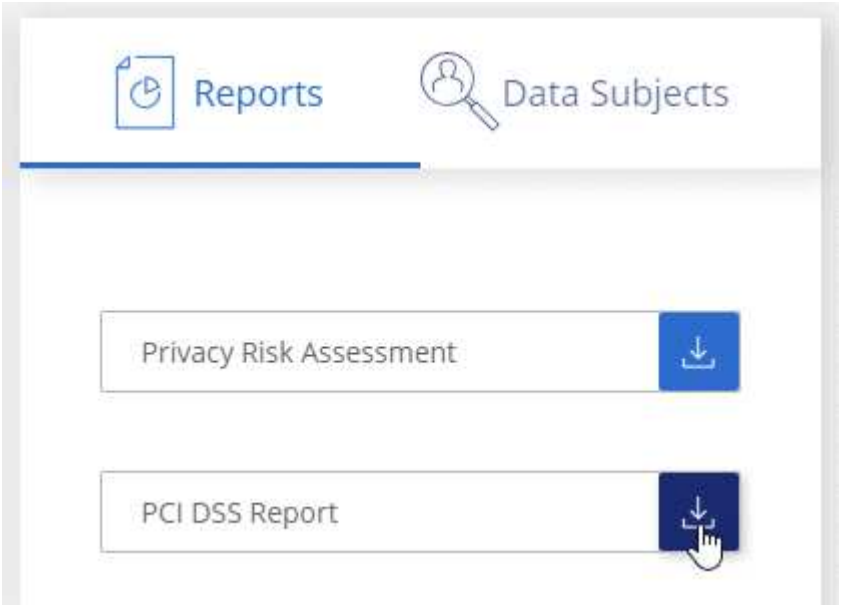
Gli ambienti di lavoro in cui sono state rilevate le informazioni sulla carta di credito e se sono attivate la crittografia e la protezione ransomware.

Generazione del rapporto PCI DSS

Accedere alla scheda Compliance per generare il report.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. In **Report**, fare clic sull'icona di download accanto a **PCI DSS Report**.



Risultato

Cloud Compliance genera un report PDF che puoi rivedere e inviare ad altri gruppi in base alle esigenze.

Report HIPAA

Il report HIPAA (Health Insurance Portability and Accountability Act) consente di identificare i file contenenti informazioni sulla salute. È progettato per soddisfare i requisiti della tua organizzazione in materia di privacy dei dati HIPAA. Le informazioni che la Cloud Compliance cerca includono:

- Schema di riferimento per lo stato di salute
- ICD-10-CM Codice medico
- Codice medico ICD-9-CM
- HR – Categoria di salute
- Categoria Health Application Data

Il report contiene le seguenti informazioni:

Panoramica

Quanti file contengono informazioni sullo stato di salute e in quali ambienti di lavoro.

Crittografia

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro crittografati o non crittografati. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Protezione ransomware

La percentuale di file contenenti informazioni sullo stato di salute che si trovano in ambienti di lavoro in cui la protezione ransomware è attivata o meno. Queste informazioni sono specifiche di Cloud Volumes ONTAP.

Conservazione

Il periodo di tempo in cui i file sono stati modificati per l'ultima volta. Ciò è utile perché non è necessario conservare le informazioni sulla salute per un periodo di tempo superiore a quello necessario per elaborarle.

Distribuzione delle informazioni sanitarie

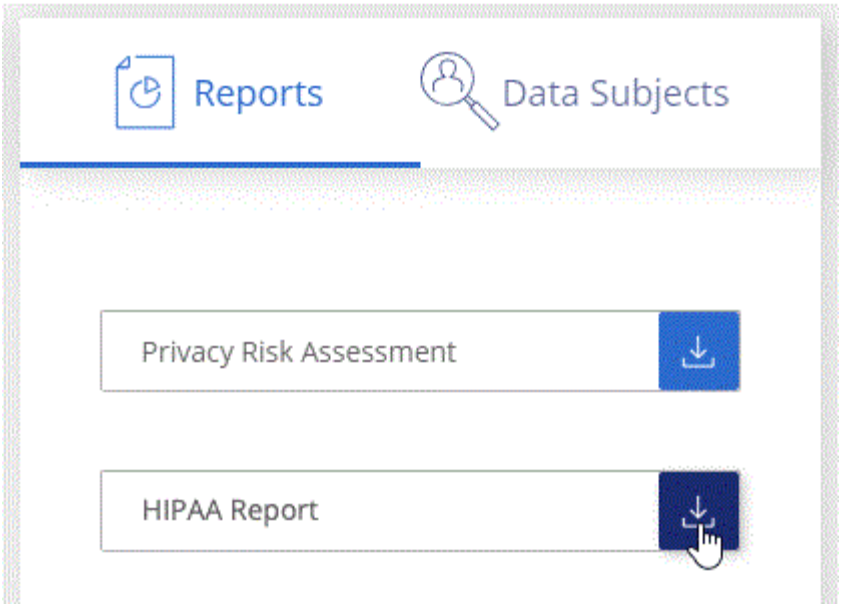
Gli ambienti di lavoro in cui sono state trovate le informazioni di salute e se sono attivate la crittografia e la protezione ransomware.

Generazione del report HIPAA

Accedere alla scheda Compliance per generare il report.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. In **Report**, fare clic sull'icona di download accanto a **Report HIPAA**.



Risultato

Cloud Compliance genera un report PDF che puoi rivedere e inviare ad altri gruppi in base alle esigenze.

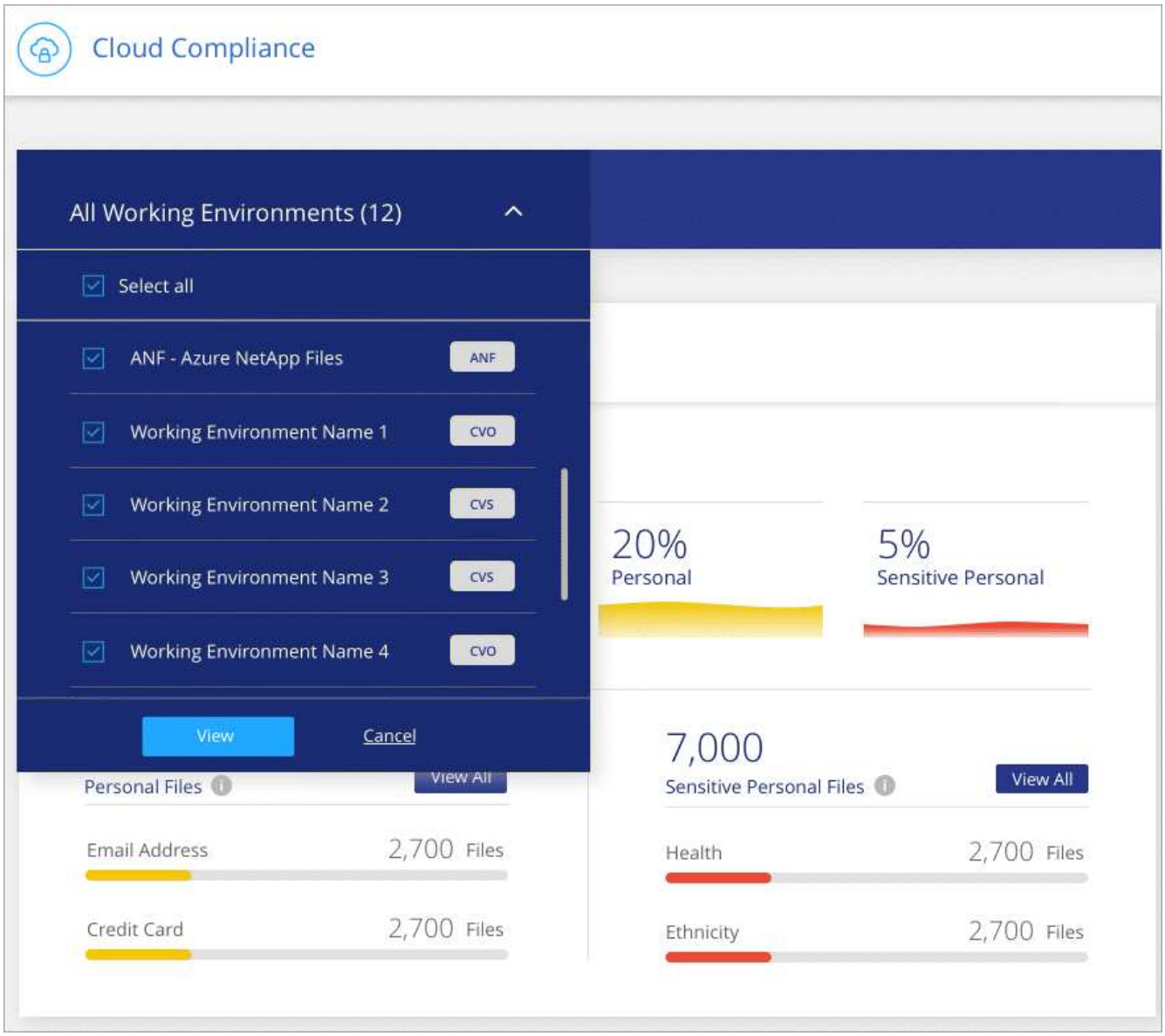
Selezione degli ambienti di lavoro per i report

Puoi filtrare i contenuti della dashboard Cloud Compliance per visualizzare i dati di conformità per tutti gli ambienti di lavoro e i database o solo per ambienti di lavoro specifici.

Quando filtri la dashboard, Cloud Compliance regola i dati di conformità e invia report solo agli ambienti di lavoro selezionati.

Fasi

1. Fare clic sul menu a discesa del filtro, selezionare gli ambienti di lavoro per i quali si desidera visualizzare i dati e fare clic su **View** (Visualizza).



Risposta a una richiesta di accesso soggetto a dati

Rispondere a una richiesta di accesso soggetto a dati (DSAR) cercando il nome completo o l'identificatore noto di un soggetto (ad esempio un indirizzo e-mail) e scaricando un report. Il report è stato progettato per aiutare l'organizzazione a rispettare il GDPR o leggi simili sulla privacy dei dati.

NetApp non può garantire una precisione del 100% dei dati personali e dei dati personali sensibili identificati dalla Cloud Compliance. È sempre necessario convalidare le informazioni esaminando i dati.

Che cos'è una richiesta di accesso ai dati?

Le normative sulla privacy, come il GDPR europeo, concedono ai soggetti interessati (come clienti o dipendenti) il diritto di accedere ai propri dati personali. Quando un soggetto interessato richiede queste informazioni, queste vengono denominate DSAR (data subject access request). Le organizzazioni devono rispondere a queste richieste "senza ritardi indebito" e al più tardi entro un mese dalla ricezione.

In che modo la Cloud Compliance può aiutarti a rispondere a una DSAR?

Quando esegui una ricerca dell'oggetto dati, Cloud Compliance trova tutti i file che contengono il nome o l'identificatore della persona. Cloud Compliance verifica i dati pre-indicizzati più recenti per il nome o l'identificatore. Non avvia una nuova scansione.

Una volta completata la ricerca, è possibile scaricare l'elenco di file per un report Data Subject Access Request. Il report aggrega le informazioni dei dati e le inserisce in termini legali che è possibile inviare alla persona.

Ricerca di dati e download di report

Cercare il nome completo o l'identificatore noto del soggetto interessato, quindi scaricare un report elenco file o un report DSAR. È possibile eseguire la ricerca in base a. "qualsiasi tipo di informazione personale".

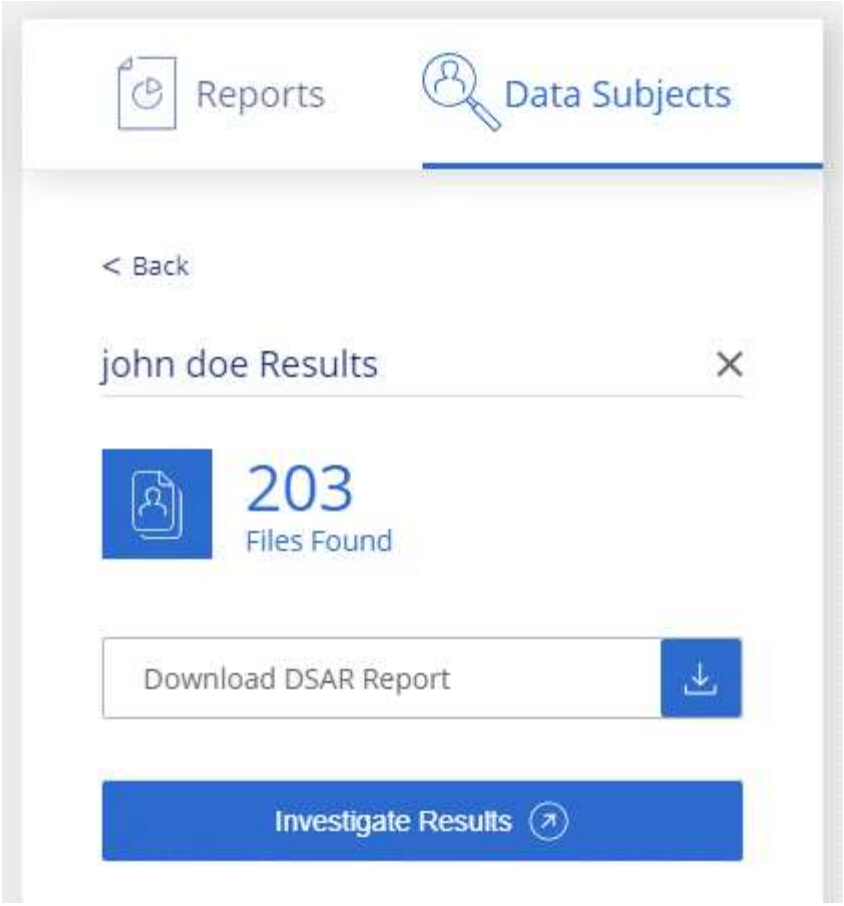
Quando si ricercano i nomi dei soggetti dati, è supportato solo l'inglese. Il supporto per altre lingue verrà aggiunto in un secondo momento.

La ricerca dei dati non è attualmente supportata nei database.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Cloud Compliance**.
2. Fare clic su **Data subjects**.
3. Cercare il nome completo o l'identificativo noto dell'interessato.

   Ecco un esempio che mostra una ricerca per il nome *john Doe*:



4. Scegliere una delle opzioni disponibili:
   - **Download del report DSAR**: Una risposta formale alla richiesta di accesso che è possibile inviare al soggetto interessato. Questo report contiene informazioni generate automaticamente in base ai dati rilevati dalla Cloud Compliance nell'oggetto dei dati ed è progettato per essere utilizzato come modello. Completare il modulo e esaminarlo internamente prima di inviarlo al soggetto interessato.
   - **Investigate Results**: Pagina che consente di analizzare i dati ricercando, ordinando, espandendo i dettagli di un file specifico e scaricando l'elenco dei file.

     Se sono presenti più di 10,000 risultati, nell'elenco dei file vengono visualizzati solo i primi 10,000 risultati.

Disattivazione della conformità al cloud

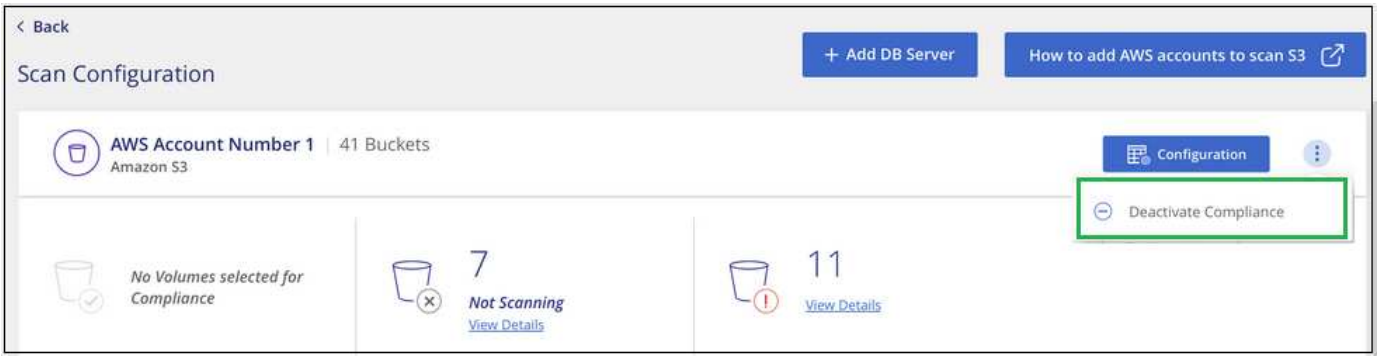
Se necessario, puoi impedire alla conformità cloud di eseguire la scansione di uno o più ambienti di lavoro o database. Puoi anche eliminare l'istanza Cloud Compliance se non desideri più utilizzare Cloud Compliance con i tuoi ambienti di lavoro.

Disattivazione delle scansioni di compliance per un ambiente di lavoro

Quando si disattivano le scansioni, Cloud Compliance non esegue più la scansione dei dati sul sistema e rimuove le informazioni indicizzate sulla conformità dall'istanza Cloud Compliance (i dati dell'ambiente di lavoro o del database stesso non vengono cancellati).

Fasi

Dalla pagina *Scan Configuration*, fare clic su Nella riga dell'ambiente di lavoro, quindi fare clic su **Disattiva conformità**.



È inoltre possibile disattivare le scansioni di conformità per un ambiente di lavoro dal pannello servizi quando si seleziona l'ambiente di lavoro.

Eliminazione dell'istanza di Cloud Compliance

Se non si desidera più utilizzare Cloud Compliance, è possibile eliminare l'istanza di Cloud Compliance. L'eliminazione dell'istanza comporta anche l'eliminazione dei dischi associati in cui risiedono i dati indicizzati.

Fase

1. Accedere alla console del provider di servizi cloud ed eliminare l'istanza Cloud Compliance.

   L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

Domande frequenti sulla conformità al cloud

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Che cos'è la conformità al cloud?

La conformità al cloud è un'offerta cloud che utilizza la tecnologia basata sull'intelligenza artificiale (ai) per aiutare le organizzazioni a comprendere il contesto dei dati e identificare i dati sensibili nelle configurazioni Azure NetApp Files, nei sistemi Cloud Volumes ONTAP ospitati in AWS o Azure, nei bucket Amazon S3 e nei database.

Cloud Compliance offre parametri predefiniti (ad esempio tipi e categorie di informazioni sensibili) per soddisfare le nuove normative sulla conformità dei dati per la privacy e la sensibilità dei dati, come GDPR, CCPA, HIPAA e altro ancora.

Perché dovrei utilizzare Cloud Compliance?

La conformità al cloud può aiutarti con i dati per aiutarti a:

- Rispettare le normative sulla privacy e sulla conformità dei dati.
- Rispettare le policy di conservazione dei dati.

- Individuare e creare report su dati specifici in risposta a soggetti interessati, come richiesto da GDPR, CCPA, HIPAA e altre normative sulla privacy dei dati.

Quali sono i casi di utilizzo più comuni per la conformità al cloud?

- Identificare le informazioni personali identificabili (PII).
- Identificare un ampio ambito di informazioni sensibili come richiesto dalle normative sulla privacy GDPR e CCPA.
- Rispettare le nuove e future normative sulla privacy dei dati.

"Scopri di più sui casi di utilizzo per la conformità al cloud".

Quali tipi di dati è possibile sottoporre a scansione con la conformità al cloud?

Cloud Compliance supporta la scansione di dati non strutturati su protocolli NFS e CIFS gestiti da Cloud Volumes ONTAP e Azure NetApp Files. Cloud Compliance può anche eseguire la scansione dei dati memorizzati nei bucket Amazon S3.

Inoltre, Cloud Compliance è in grado di eseguire la scansione di database che si trovano ovunque, non devono essere gestiti da Cloud Manager.

"Scopri come funzionano le scansioni".

Quali cloud provider sono supportati?

Cloud Compliance opera come parte di Cloud Manager e attualmente supporta AWS e Azure. In questo modo, la tua organizzazione potrà ottenere una visibilità unificata della privacy tra diversi cloud provider. Il supporto per Google Cloud Platform (GCP) verrà aggiunto a breve.

Come posso accedere alla conformità cloud?

La conformità al cloud viene gestita e gestita tramite Cloud Manager. Puoi accedere alle funzionalità Cloud Compliance dalla scheda **Compliance** di Cloud Manager.

Come funziona Cloud Compliance?

Cloud Compliance implementa un altro livello di intelligenza artificiale insieme al sistema Cloud Manager e ai sistemi storage. Esegue quindi la scansione dei dati su volumi, bucket e database e indicizza le informazioni sui dati trovate.

"Scopri di più sul funzionamento della conformità al cloud".

Quanto costa la Cloud Compliance?

Il costo per l'utilizzo della conformità cloud dipende dalla quantità di dati che si sta scansionando. I primi 1 TB di dati che Cloud Compliance analizza in uno spazio di lavoro di Cloud Manager sono gratuiti. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento ad AWS o Azure Marketplace. Vedere "prezzi" per ulteriori informazioni.

Con quale frequenza la Cloud Compliance esegue la scansione dei miei dati?

I dati cambiano di frequente, pertanto la conformità del cloud esegue una scansione continua dei dati senza

alcun impatto sui dati. Anche se la scansione iniziale dei dati potrebbe richiedere più tempo, le scansioni successive eseguono solo la scansione delle modifiche incrementali, riducendo i tempi di scansione del sistema.

"Scopri come funzionano le scansioni".

Cloud Compliance offre report?

Sì. Le informazioni offerte dalla Cloud Compliance possono essere rilevanti per gli altri stakeholder delle tue organizzazioni, pertanto ti consentiamo di generare report per condividere le informazioni.

Per la conformità al cloud sono disponibili i seguenti report:

Report sulla valutazione dei rischi per la privacy
: Fornisce informazioni sulla privacy dai dati e un punteggio di rischio per la privacy. "Scopri di più".

Report Data Subject Access Request
: Consente di estrarre un report di tutti i file che contengono informazioni relative al nome specifico o all'identificativo personale di un soggetto. "Scopri di più".

Report PCI DSS
: Consente di identificare la distribuzione delle informazioni sulla carta di credito nei file. "Scopri di più".

Report HIPAA
: Consente di identificare la distribuzione delle informazioni sanitarie tra i file. "Scopri di più".

Report su un tipo di informazioni specifico
: Sono disponibili report che includono dettagli sui file identificati che contengono dati personali e dati personali sensibili. È inoltre possibile visualizzare i file suddivisi per categoria e tipo di file. "Scopri di più".

Quale tipo di istanza o macchina virtuale è richiesto per la conformità al cloud?

- In Azure, Cloud Compliance viene eseguito su una macchina virtuale Standard_D16s_v3 con un disco da 512 GB.
- In AWS, Cloud Compliance viene eseguito su un'istanza m5.4xLarge con un disco GP2 da 500 GB.

  Nelle regioni in cui m5.4xlarge non è disponibile, Cloud Compliance viene eseguito su un'istanza m4.4xlarge.

> La modifica o il ridimensionamento del tipo di istanza/VM non è supportato. È necessario utilizzare le dimensioni predefinite fornite.

"Scopri di più sul funzionamento della conformità al cloud".

Le prestazioni di scansione variano?

Le performance di scansione possono variare in base alla larghezza di banda della rete e alle dimensioni medie dei file nel tuo ambiente cloud.

Quali tipi di file sono supportati?

Cloud Compliance esegue la scansione di tutti i file per individuare informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Quando Cloud Compliance rileva le informazioni personali identificabili (PII) o esegue una ricerca DSAR, sono supportati solo i seguenti formati di file: .PDF, .DOCX, .DOC, .PPTX, .XLS, XLSX, .CSV, .TXT, .RTF E .JSON.

Come posso abilitare la conformità al cloud?

Innanzitutto, devi implementare un'istanza di Cloud Compliance in Cloud Manager. Una volta eseguita l'istanza, è possibile abilitarla negli ambienti di lavoro e nei database esistenti dalla scheda **Compliance** o selezionando un ambiente di lavoro specifico.

"Scopri come iniziare".

L'attivazione della conformità cloud comporta una scansione iniziale immediata. I risultati della compliance vengono visualizzati poco dopo.

Come si disattiva la conformità al cloud?

Dopo aver selezionato un singolo ambiente di lavoro, è possibile disattivare Cloud Compliance dalla pagina Working Environments (ambienti di lavoro).

"Scopri di più".

Per rimuovere completamente l'istanza di Cloud Compliance, puoi rimuovere manualmente l'istanza di Cloud Compliance dal portale del tuo cloud provider.

Cosa succede se il tiering dei dati è attivato su Cloud Volumes ONTAP?

Potresti voler abilitare la conformità al cloud su un sistema Cloud Volumes ONTAP che esegue il Tier dei dati cold sullo storage a oggetti. Se il tiering dei dati è attivato, Cloud Compliance esegue la scansione di tutti i dati presenti sui dischi e cold data tiered in storage a oggetti.

La scansione di compliance non riscalda i dati cold, ma rimane fredda e viene tierata per lo storage a oggetti.

Posso utilizzare la conformità al cloud per eseguire la scansione dello storage ONTAP on-premise?

La scansione dei dati direttamente da un ambiente di lavoro ONTAP on-premise non è supportata. Tuttavia, è possibile eseguire la scansione dei dati ONTAP on-premise replicando i dati NFS o CIFS on-premise in un ambiente di lavoro Cloud Volumes ONTAP e attivando la conformità su tali volumi. Stiamo pianificando di supportare la conformità al cloud con offerte cloud aggiuntive come Cloud Volumes Service.

"Scopri di più".

Cloud Compliance può inviare notifiche alla mia organizzazione?

No, ma è possibile scaricare i report di stato che è possibile condividere internamente all'organizzazione.

Posso personalizzare il servizio in base alle esigenze della mia organizzazione?

La conformità al cloud offre informazioni pronte all'uso ai tuoi dati. Queste informazioni possono essere estratte e utilizzate per le esigenze della tua organizzazione.

Posso limitare le informazioni sulla conformità al cloud a utenti specifici?

Sì, la conformità del cloud è completamente integrata con Cloud Manager. Gli utenti di Cloud Manager possono visualizzare le informazioni solo per gli ambienti di lavoro che possono visualizzare in base ai privilegi dell'area di lavoro.

Inoltre, se si desidera consentire a determinati utenti di visualizzare solo i risultati della scansione Cloud Compliance senza avere la possibilità di gestire le impostazioni Cloud Compliance, è possibile assegnare a tali utenti il ruolo *Cloud Compliance Viewer*.

"Scopri di più".

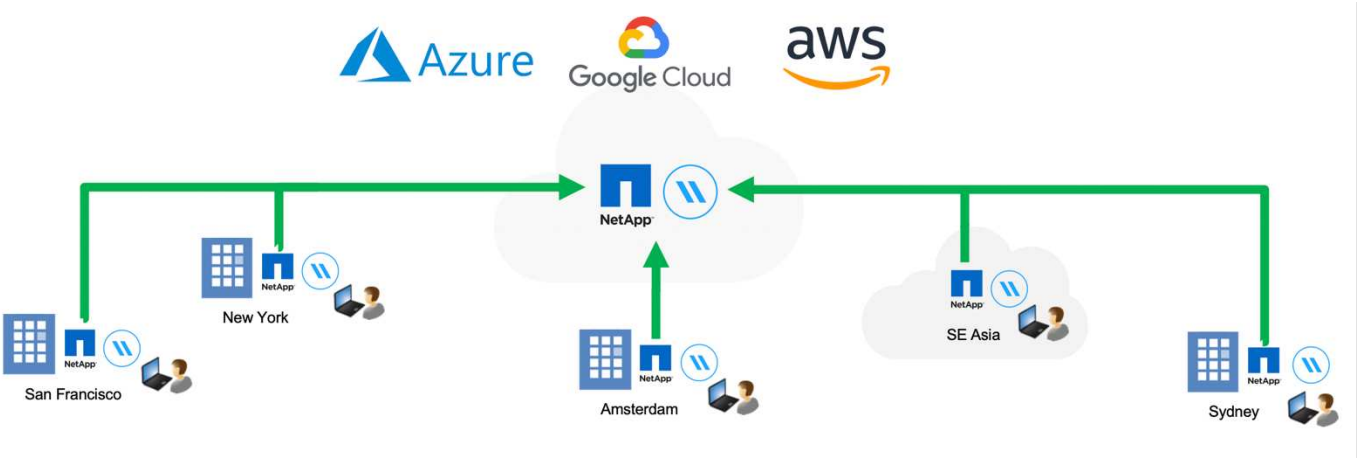
Condivisione globale dei file in tempo reale

Scopri la Global file cache

NetApp Global file cache consente di consolidare silos di file server distribuiti in un unico footprint di storage globale e coerente nel cloud pubblico. In questo modo si crea un file system accessibile a livello globale nel cloud che tutte le ubicazioni remote possono utilizzare come se fossero locali.

Panoramica

L'implementazione di Global file cache consente di ottenere un unico footprint dello storage centralizzato rispetto a un'architettura di storage distribuita che richiede gestione dei dati locale, backup, gestione della sicurezza, storage e impatto dell'infrastruttura in ciascuna posizione.



Caratteristiche

Global file cache offre le seguenti funzionalità:

- Consolida e centralizza i tuoi dati nel cloud pubblico e sfrutta la scalabilità e le performance delle soluzioni storage di livello Enterprise
- Crea un singolo set di dati per gli utenti a livello globale e sfrutta il caching intelligente dei file per migliorare l'accesso ai dati globali, la collaborazione e le performance
- Affidati a una cache autogestita e a gestione automatica ed elimina copie e backup completi dei dati. Utilizza il caching dei file locali per i dati attivi e taglia i costi dello storage
- Accesso trasparente dalle filiali attraverso uno spazio dei nomi globale con blocco dei file centralizzato in tempo reale

Scopri di più sulle funzionalità e sui casi d'utilizzo di Global file cache "qui".

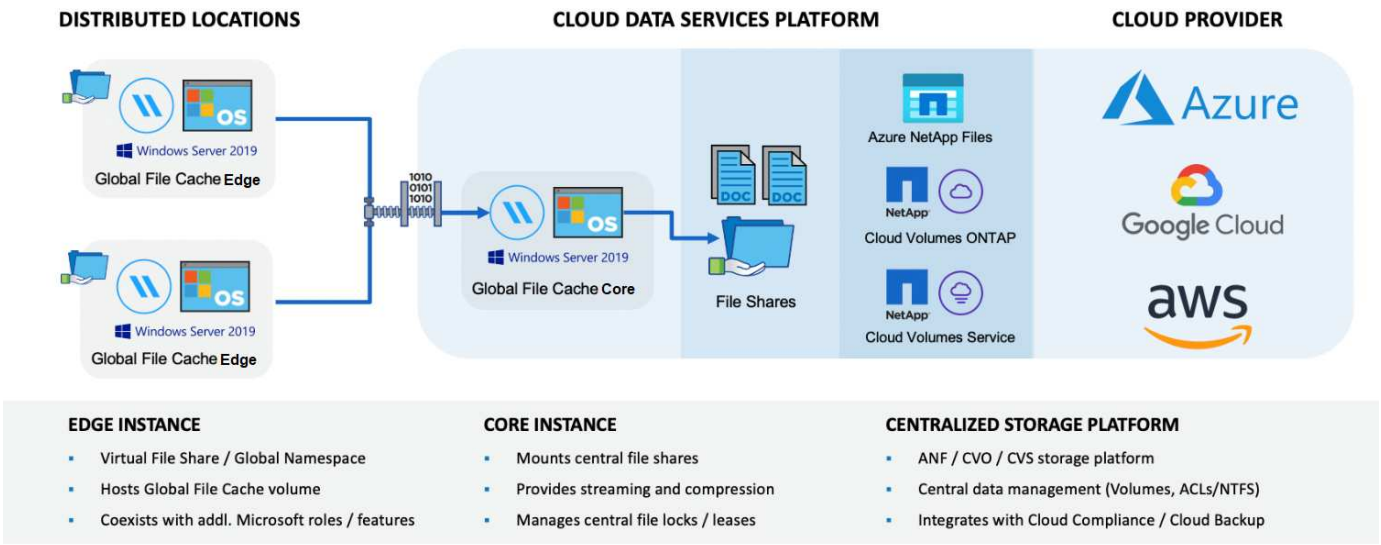
Componenti Global file cache

Global file cache è costituito dai seguenti componenti:

- Global file cache Management Server

- Core Global file cache
- Global file cache Edge (distribuito nelle sedi remote)

L'istanza di base Global file cache viene montata sulle condivisioni di file aziendali ospitate sulla piattaforma di storage di back-end scelta (ad esempio Cloud Volumes ONTAP, Cloud Volumes Service, E Azure NetApp Files) e crea il fabric Global file cache che offre la possibilità di centralizzare e consolidare i dati non strutturati in un singolo set di dati, che si trovino su una o più piattaforme di storage nel cloud pubblico.



Piattaforme di storage supportate

Le piattaforme di storage supportate per Global file cache variano a seconda dell'opzione di implementazione selezionata.

Opzioni di implementazione automatizzate

Global file cache è supportato con i seguenti tipi di ambienti di lavoro quando implementato con Cloud Manager:

- Cloud Volumes ONTAP in Azure
- Cloud Volumes ONTAP in AWS

Questa configurazione consente di implementare e gestire l'intera implementazione lato server di Global file cache, inclusi Global file cache Management Server e Global file cache Core, da Cloud Manager.

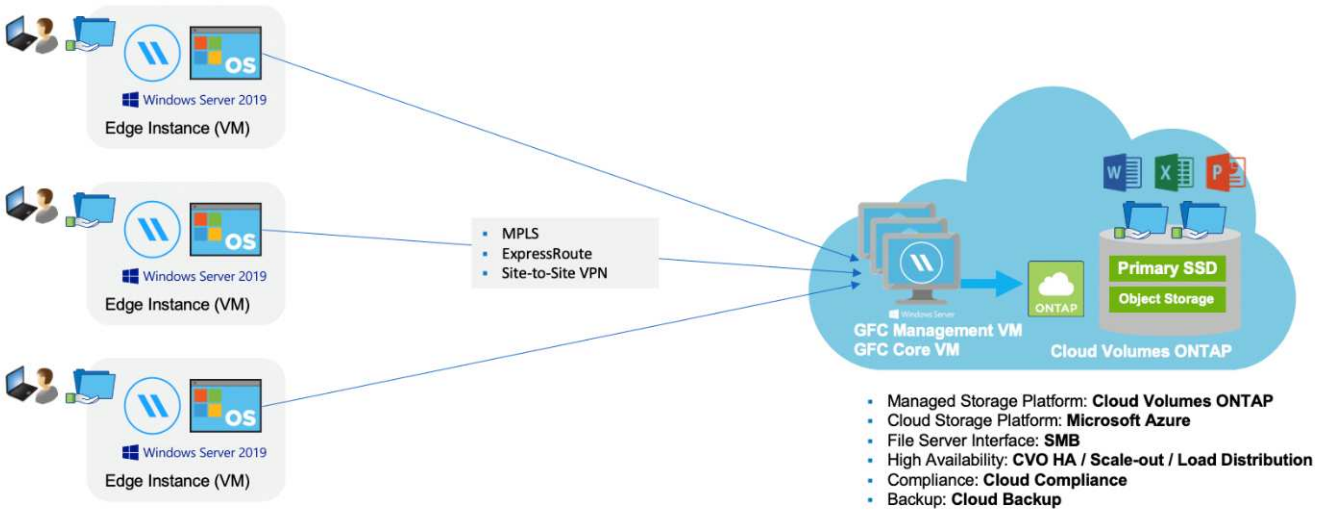
Opzioni di implementazione manuale

Le configurazioni della Global file cache sono supportate anche con Cloud Volumes ONTAP, Cloud Volumes Service o Azure NetApp Files installati su Microsoft Azure, sulla piattaforma cloud di Google o sull'infrastruttura di cloud storage pubblico di Amazon Web Services. Le soluzioni on-premise sono disponibili anche sulle piattaforme NetApp AFF e FAS. In queste installazioni, i componenti lato server Global file cache devono essere configurati e implementati manualmente, non utilizzando Cloud Manager.

Vedere "Guida utente di NetApp Global file cache" per ulteriori informazioni.

Come funziona Global file cache

Global file cache crea un fabric software che memorizza nella cache i set di dati attivi negli uffici remoti a livello globale. Di conseguenza, agli utenti aziendali viene garantito un accesso trasparente ai dati e performance ottimali su scala globale.



La topologia a cui si fa riferimento in questo esempio è un modello hub e spoke, per cui la rete di uffici/sedi remote sta accedendo a un insieme comune di dati nel cloud. I punti chiave di questo esempio sono:

- Data store centralizzato:
  - Piattaforma di cloud storage pubblico aziendale, come Cloud Volumes ONTAP
- Fabric Global file cache:
  - Estensione dell'archivio dati centrale alle postazioni remote
  - Istanza Global file cache Core, montaggio su condivisioni file aziendali (SMB).
  - Istanze di Global file cache Edge in esecuzione in ogni posizione remota.
  - Presenta una condivisione di file virtuale in ogni posizione remota che fornisce l'accesso ai dati centrali.
  - Ospita Intelligent file cache su un volume NTFS di dimensioni personalizzate (`D:\`).
- Configurazione di rete:
  - Connettività MPLS (MultiProtocol Label Switching), ExpressRoute o VPN
- Integrazione con i servizi di dominio Active Directory del cliente.
- Spazio dei nomi DFS per l'utilizzo di uno spazio dei nomi globale (consigliato).

Costo

Il costo per l'utilizzo di Global file cache dipende dal tipo di installazione scelta.

- Tutte le installazioni richiedono l'implementazione di uno o più volumi nel cloud (Cloud Volumes ONTAP, Cloud Volumes Service o Azure NetApp Files). Ciò comporta addebiti da parte del cloud provider selezionato.
- Tutte le installazioni richiedono inoltre l'implementazione di due o più macchine virtuali (VM) nel cloud. Ciò

comporta addebiti da parte del cloud provider selezionato.

- Global file cache Management Server:

  In Azure, viene eseguito su una macchina virtuale D2s_V3 o equivalente (2 vCPU/8 GB di RAM) con SSD premium da 127 GB

  In AWS, viene eseguito su un'istanza m4.Large o equivalente (2 vCPU/8 GB di RAM) con 127 GB di SSD General Purpose

- Core Global file cache:

  In Azure, viene eseguito su una macchina virtuale D4S_V3 o equivalente (4 vCPU/16 GB di RAM) con SSD premium da 127 GB

  In AWS, viene eseguito su un'istanza m4.xlarge o equivalente (4 vCPU/16 GB di RAM) con 127 GB di SSD General Purpose

- Quando viene installato con Cloud Volumes ONTAP in Azure o AWS (le configurazioni supportate sono implementate completamente tramite Cloud Manager), viene addebitato un costo annuo di 3,000 dollari per sito (per ogni istanza Global file cache Edge).
- Se installato utilizzando le opzioni di implementazione manuale, il prezzo è diverso. Per una stima dei costi di alto livello, vedere "Calcola il tuo potenziale di risparmio" In alternativa, rivolgiti al tuo Global file cache Solutions Engineer per discutere delle opzioni migliori per l'implementazione aziendale.

Licensing

Global file cache include un License Management Server (LMS) basato su software, che consente di consolidare la gestione delle licenze e distribuire le licenze a tutte le istanze di Core ed Edge utilizzando un meccanismo automatizzato.

Quando si implementa la prima istanza Core nel data center o nel cloud, è possibile scegliere di designare tale istanza come LMS per la propria organizzazione. Questa istanza di LMS viene configurata una volta, si connette al servizio di abbonamento (su HTTPS) e convalida l'abbonamento utilizzando l'ID cliente fornito dal nostro reparto di assistenza/operazioni al momento dell'abilitazione dell'abbonamento. Una volta effettuata questa designazione, associare le istanze di Edge a LMS fornendo l'ID cliente e l'indirizzo IP dell'istanza di LMS.

Quando acquisti licenze Edge aggiuntive o rinnovi l'abbonamento, il nostro reparto assistenza/operazioni aggiorna i dettagli della licenza, ad esempio il numero di siti o la data di scadenza dell'abbonamento. Dopo che l'LMS ha richiesto il servizio di abbonamento, i dettagli della licenza vengono aggiornati automaticamente sull'istanza di LMS e verranno applicati alle istanze di GFC Core ed Edge.

Vedere "Guida utente di NetApp Global file cache" per ulteriori dettagli sulle licenze.

Limitazioni

- La versione di Global file cache supportata in Cloud Manager richiede che la piattaforma di storage back-end utilizzata come storage centrale sia un ambiente di lavoro in cui è stato implementato un nodo singolo o una coppia ha Cloud Volumes ONTAP in Azure o AWS.

  Altre piattaforme storage e altri cloud provider non sono attualmente supportati con Cloud Manager, ma possono essere implementati utilizzando procedure di implementazione legacy.

Queste altre configurazioni, ad esempio Global file cache con Cloud Volumes ONTAP, Cloud Volumes Service e Azure NetApp Files su Microsoft Azure, Google Cloud e AWS, continuano ad essere supportate utilizzando le procedure legacy. Vedere "Panoramica e inserimento della Global file cache" per ulteriori informazioni.

Prima di iniziare a implementare Global file cache

Prima di iniziare a implementare Global file cache nel cloud e nelle sedi remote, è necessario conoscere molti requisiti.

Considerazioni sulla progettazione di Global file cache Core

A seconda dei requisiti, potrebbe essere necessario implementare una o più istanze Global file cache Core per creare il fabric Global file cache. L'istanza Core è progettata per fungere da cooperativa di traffico tra le istanze di Global file cache Edge distribuite e le risorse del file server del data center, ad esempio condivisioni di file, cartelle e file.

Durante la progettazione dell'implementazione di Global file cache, è necessario determinare le caratteristiche più adatte al proprio ambiente in termini di scalabilità, disponibilità delle risorse e ridondanza. Global file cache Core può essere implementato nei seguenti modi:

- Istanza standalone di GFC Core
- GFC Core Load Distributed Design (Cold Standby)

Vedere Linee guida per il dimensionamento Per comprendere il numero massimo di istanze Edge e utenti totali che ciascuna configurazione può supportare:

Rivolgiti al tuo Global file cache Solutions Engineer per discutere delle opzioni migliori per l'implementazione aziendale.

Linee guida per il dimensionamento

Sono disponibili alcuni rapporti di dimensionamento delle linee guida che è necessario tenere a mente durante la configurazione del sistema iniziale. È necessario rivedere questi rapporti dopo aver accumulato una certa cronologia di utilizzo per assicurarsi di utilizzare il sistema in modo ottimale. Questi includono:

- Rapporto Global file cache Edges/Core
- Rapporto utenti distribuiti/edge Global file cache
- Rapporto core utenti distribuiti/Global file cache

Numero di istanze Edge per istanza principale

Le nostre linee guida consigliano fino a 10 istanze Edge per istanza Global file cache Core, con un massimo di 20 edge per istanza Global file cache Core. Ciò dipende in misura significativa dal tipo e dalla dimensione media del file del carico di lavoro più comune. In alcuni casi, con carichi di lavoro più comuni è possibile aggiungere più istanze Edge per core, ma in questi casi è necessario contattare il supporto NetApp per dimensionare correttamente il numero di istanze Edge e Core in base al tipo e alle dimensioni dei set di file.

Puoi sfruttare più istanze Global file cache Edge e Core contemporaneamente per scalare l'infrastruttura in base ai requisiti.

Numero di utenti simultanei per istanza Edge

Global file cache Edge gestisce l'elevato carico di lavoro in termini di algoritmi di caching e differenze a livello di file. Una singola istanza Global file cache Edge può servire fino a 400 utenti per istanza fisica Edge dedicata e fino a 200 utenti per implementazioni virtuali dedicate. Ciò dipende in misura significativa dal tipo e dalla dimensione media del file del carico di lavoro più comune. Per tipi di file collaborativi più grandi, guidare verso il 50% del numero massimo di utenti per limite inferiore Global file cache Edge (a seconda dell'implementazione fisica o virtuale). Per gli elementi Office più comuni con dimensioni medie dei file <1 MB, guida verso il 100% di utenti per limite superiore Global file cache Edge (a seconda dell'implementazione fisica o virtuale).

> Global file cache Edge rileva se è in esecuzione su un'istanza virtuale o fisica e limita il numero di connessioni SMB alla condivisione di file virtuale locale al massimo di 200 o 400 connessioni simultanee.

Numero di utenti simultanei per istanza Core

L'istanza Global file cache Core è estremamente scalabile, con un numero di utenti simultanei consigliato di 3,000 utenti per core. Ciò dipende in misura significativa dal tipo e dalla dimensione media del file del carico di lavoro più comune.

Rivolgiti al tuo Global file cache Solutions Engineer per discutere delle opzioni migliori per l'implementazione aziendale.

Prerequisiti

I prerequisiti descritti in questa sezione si riferiscono ai componenti installati nel cloud: Global file cache Management Server e Global file cache Core.

Vengono descritti i prerequisiti di Global file cache Edge "qui".

Istanza di Cloud Manager

Quando utilizzi Cloud Volumes ONTAP per Azure come piattaforma di storage, assicurati che Cloud Manager disponga delle autorizzazioni come mostrato nella più recente "Policy di Cloud Manager per Azure".

Per impostazione predefinita, le istanze create di recente dispongono di tutte le autorizzazioni necessarie. Se l'istanza è stata distribuita prima della versione 3.8.7 (3 agosto 2020), sarà necessario aggiungere questi elementi.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Piattaforma di storage (volumi)

La piattaforma di storage back-end, in questo caso l'istanza di Cloud Volumes ONTAP implementata, dovrebbe presentare le condivisioni di file SMB. Tutte le condivisioni che verranno esposte tramite Global file cache devono consentire al gruppo Everyone il controllo completo a livello di condivisione, limitando al contempo le autorizzazioni attraverso le autorizzazioni NTFS.

Se non è stata impostata almeno una condivisione file SMB sull'istanza di Cloud Volumes ONTAP, è necessario disporre delle seguenti informazioni per poter configurare queste informazioni durante l'installazione:

- Nome di dominio di Active Directory, indirizzo IP del server dei nomi, credenziali di amministratore di Active Directory.
- Il nome e le dimensioni del volume che si desidera creare, il nome dell'aggregato su cui verrà creato il volume e il nome della condivisione.

Si consiglia di utilizzare un volume sufficientemente grande per ospitare il set di dati totale dell'applicazione, oltre alla possibilità di scalare di conseguenza in base alla crescita del set di dati. Se nell'ambiente di lavoro sono presenti più aggregati, vedere "Gestione degli aggregati esistenti" per determinare quale aggregato dispone dello spazio più disponibile per il nuovo volume.

Global file cache Management Server

Questo Global file cache Management Server richiede l'accesso esterno su HTTPS (porta TCP 443) per connettersi al servizio di abbonamento del provider cloud e per accedere ai seguenti URL:

- "https://talonazuremicroservices.azurewebsites.net"
- "https://talonlicensing.table.core.windows.net"

Questa porta deve essere esclusa da qualsiasi dispositivo di ottimizzazione WAN o policy di restrizione firewall affinché il software Global file cache funzioni correttamente.

Global file cache Management Server richiede anche un nome NetBIOS univoco (geografico) per l'istanza (ad esempio GFC-MS1).

> Un server di gestione può supportare più istanze Global file cache Core distribuite in diversi ambienti di lavoro. Se implementato da Cloud Manager, ogni ambiente di lavoro dispone di un proprio storage back-end separato e non contiene gli stessi dati.

Core Global file cache

Questo core Global file cache è in attesa sull'intervallo di porte TCP 6618-6630. A seconda della configurazione del firewall o del Network Security Group (NSG), potrebbe essere necessario consentire esplicitamente l'accesso a queste porte tramite le regole delle porte in entrata. Inoltre, queste porte devono essere escluse da qualsiasi dispositivo di ottimizzazione WAN o policy di restrizione firewall affinché il software Global file cache funzioni correttamente.

I requisiti di base della Global file cache sono:

- Un nome NetBIOS univoco (geografico) per l'istanza (ad esempio GFC-CORE1)
- Nome di dominio di Active Directory
  - Le istanze Global file cache devono essere unite al dominio Active Directory.

    - Le istanze di Global file cache devono essere gestite in un'unità organizzativa (OU) specifica di Global file cache ed escluse dagli oggetti Criteri di gruppo aziendali ereditati.
- Account di servizio. I servizi su questo Global file cache Core vengono eseguiti come account utente di dominio specifico. Questo account, noto anche come account di servizio, deve disporre dei seguenti privilegi su ciascuno dei server SMB che saranno associati all'istanza Global file cache Core:
    - L'account di servizio fornito deve essere un utente di dominio.

A seconda del livello di restrizioni e GPO nell'ambiente di rete, questo account potrebbe richiedere privilegi di amministratore di dominio.

- Deve disporre dei privilegi di "Esegui come servizio".
- La password deve essere impostata su "non scade mai".
- L'opzione dell'account "l'utente deve modificare la password all'accesso successivo" deve essere DISATTIVATA (deselezionata).
- Deve essere membro del gruppo Built-in Backup Operators del file server back-end (attivato automaticamente quando implementato tramite Cloud Manager).

Server di gestione delle licenze

- Global file cache License Management Server (LMS) deve essere configurato su Microsoft Windows Server 2016 Standard o Datacenter Edition o Windows Server 2019 Standard o Datacenter Edition, preferibilmente sull'istanza Global file cache Core nel data center o nel cloud.
- Se si richiede un'istanza separata di Global file cache LMS, è necessario installare il pacchetto di installazione del software Global file cache più recente su un'istanza di Microsoft Windows Server non aggiornata.
- L'istanza di LMS deve essere in grado di connettersi al servizio di abbonamento (servizi Azure / Internet pubblico) utilizzando HTTPS (porta TCP 443).
- Le istanze Core ed Edge devono connettersi all'istanza LMS utilizzando HTTPS (porta TCP 443).

Networking

- Firewall: Le porte TCP devono essere consentite tra le istanze Global file cache Edge e Core.
- Porte TCP Global file cache: 443 (HTTPS), 6618–6630.
- I dispositivi di ottimizzazione di rete (come Riverbed Steelhead) devono essere configurati per passare attraverso porte specifiche Global file cache (TCP 6618-6630).

Per iniziare

Si utilizza Cloud Manager per implementare il software Global file cache Management Server e Global file cache Core nell'ambiente di lavoro.

Attiva Global file cache utilizzando Cloud Manager

In questa configurazione implementerai il server di gestione della cache dei file globali e il core della cache dei file globali nello stesso ambiente di lavoro in cui hai creato il tuo sistema Cloud Volumes ONTAP utilizzando Cloud Manager.

Guarda "questo video" per visualizzare i passaggi dall'inizio alla fine.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere informazioni complete:

Implementare Cloud Volumes ONTAP

Implementare Cloud Volumes ONTAP in Azure o AWS e configurare le condivisioni di file SMB. Per ulteriori informazioni, vedere "Lancio di Cloud Volumes ONTAP in Azure" oppure "Avvio di Cloud Volumes ONTAP in AWS".

Implementare Global file cache Management Server

Implementare un'istanza del server di gestione della cache dei file globale nello stesso ambiente di lavoro dell'istanza di Cloud Volumes ONTAP.

Implementare il core Global file cache

Distribuire una o più istanze del core Global file cache nello stesso ambiente di lavoro dell'istanza di Cloud Volumes ONTAP e unirsi al dominio Active Directory.

Cache file globale licenza

Configurare il servizio Global file cache License Management Server (LMS) su un'istanza Global file cache Core. Per attivare l'abbonamento, è necessario disporre delle credenziali NSS o di un ID cliente fornito da NetApp.

Implementare le istanze Global file cache Edge

Vedere "Implementazione di istanze Global file cache Edge" Per implementare le istanze Global file cache Edge in ogni posizione remota. Questo passaggio non viene eseguito con Cloud Manager.

Implementa Cloud Volumes ONTAP come piattaforma di storage

Nella versione corrente, Global file cache supporta Cloud Volumes ONTAP implementato in Azure o AWS. Per informazioni dettagliate su prerequisiti, requisiti e istruzioni di implementazione, vedere "Lancio di Cloud Volumes ONTAP in Azure" oppure "Avvio di Cloud Volumes ONTAP in AWS".

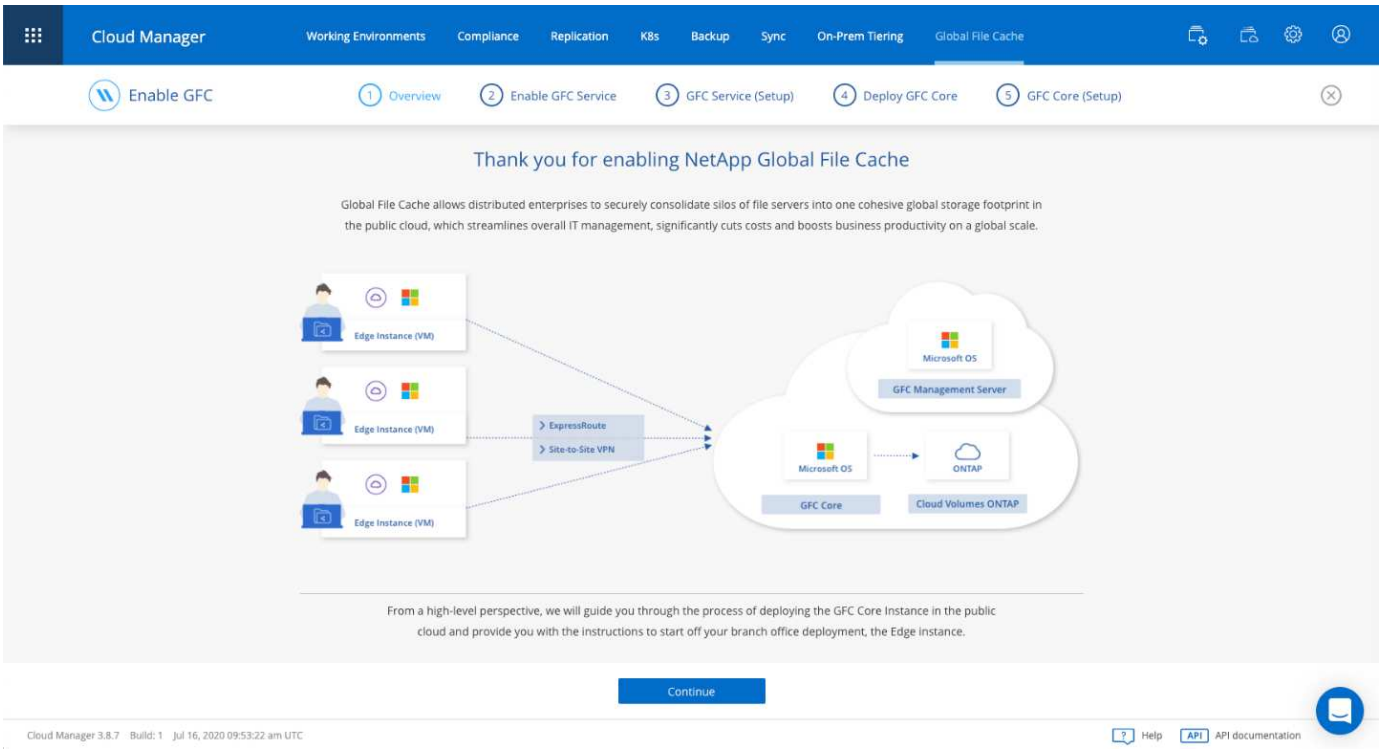
Tenere presente il seguente requisito aggiuntivo Global file cache:

- È necessario configurare le condivisioni di file SMB sull'istanza di Cloud Volumes ONTAP.

  Se non sono state impostate condivisioni di file SMB nell'istanza, viene richiesto di configurare le condivisioni SMB durante l'installazione dei componenti Global file cache.

Attiva Global file cache nel tuo ambiente di lavoro

La procedura guidata Global file cache guida l'utente attraverso i passaggi per implementare l'istanza di Global file cache Management Server e l'istanza Global file cache Core, come evidenziato di seguito.



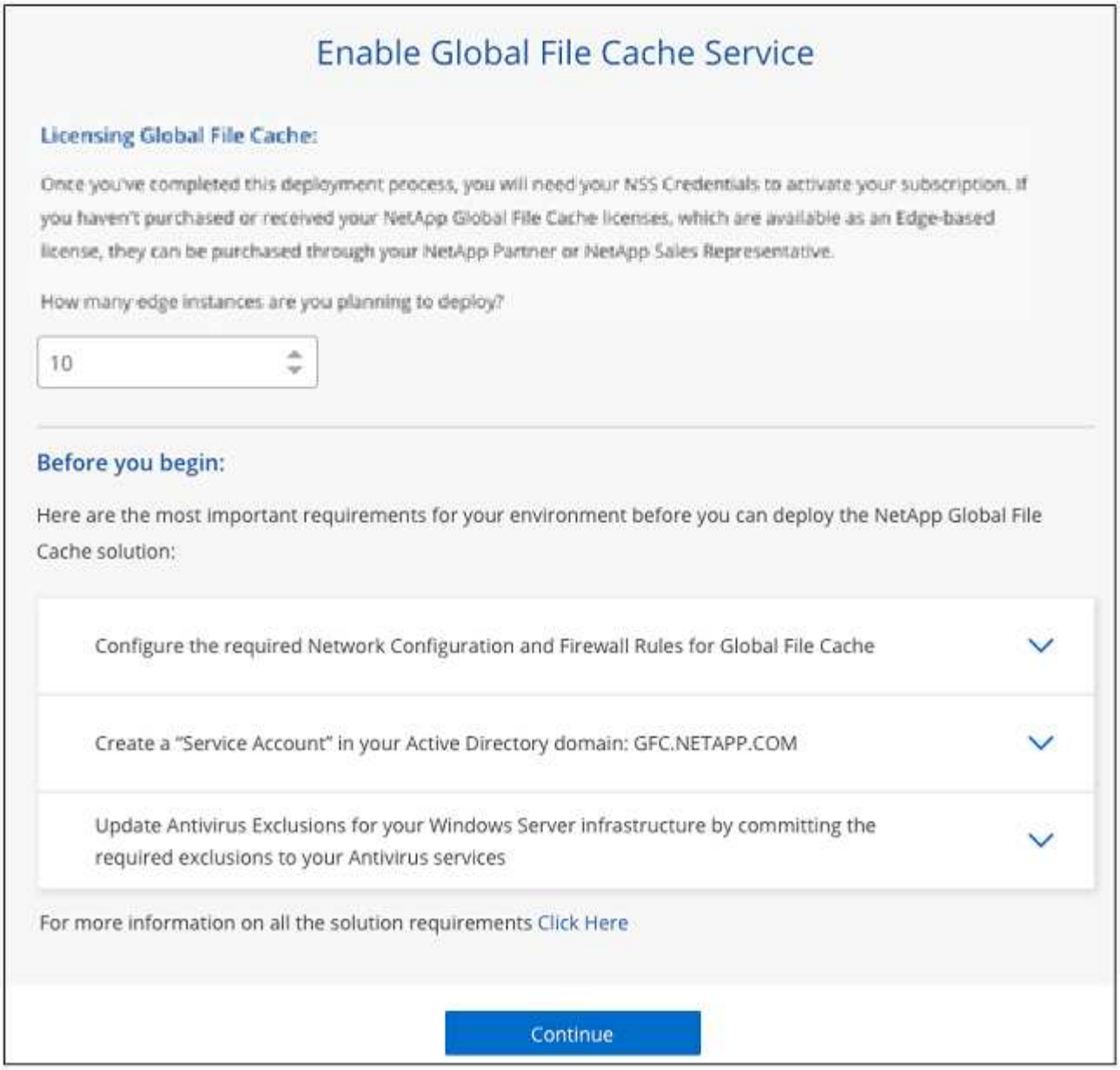
Fasi

1. Selezionare l'ambiente di lavoro in cui è stato implementato Cloud Volumes ONTAP.
2. Nel pannello servizi, fare clic su **Enable GFC** (attiva GFC).

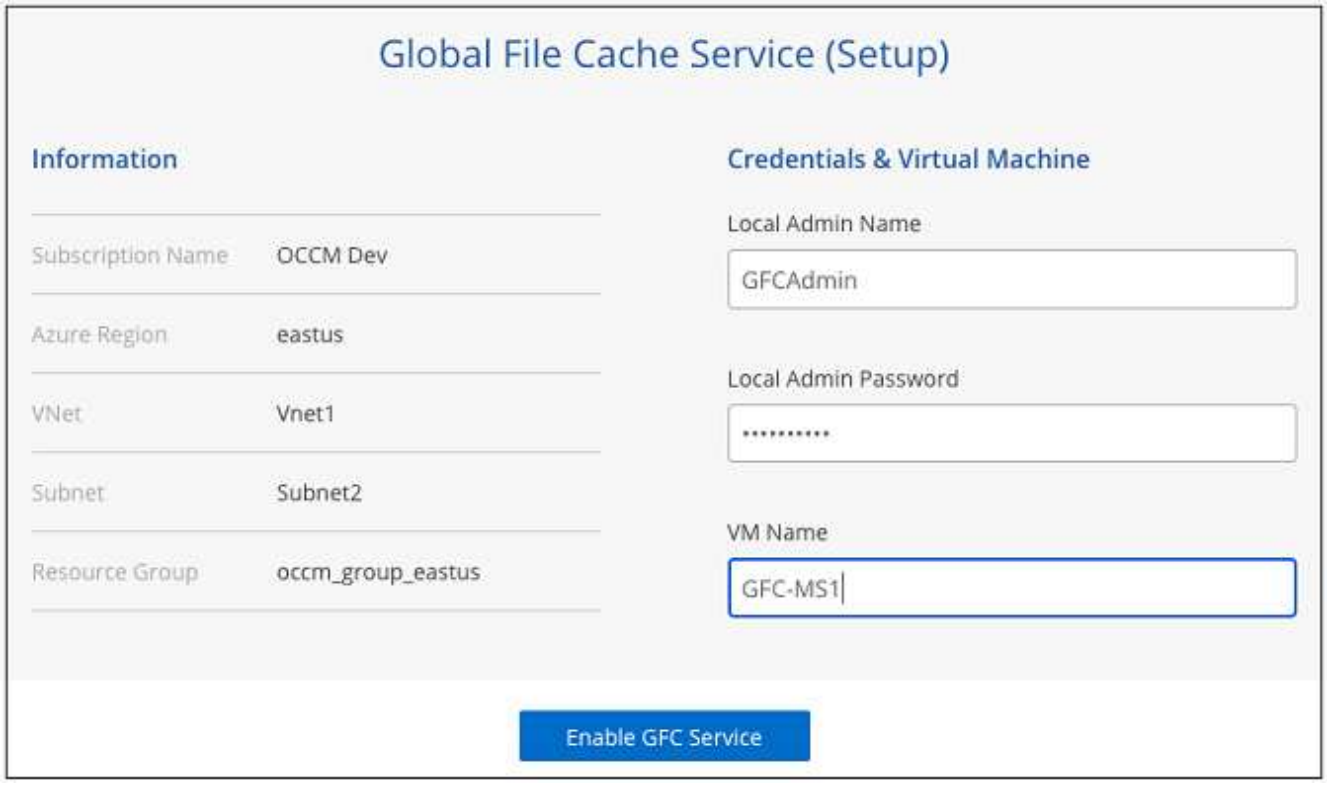
3. Leggi la pagina Panoramica e fai clic su **continua**.
4. Se non sono disponibili condivisioni SMB nell'istanza di Cloud Volumes ONTAP, viene richiesto di inserire i dettagli relativi al server SMB e alla condivisione SMB per creare la condivisione. Per ulteriori informazioni sulla configurazione SMB, vedere "Piattaforma di storage".

   Al termine, fare clic su **continua** per creare la condivisione SMB.

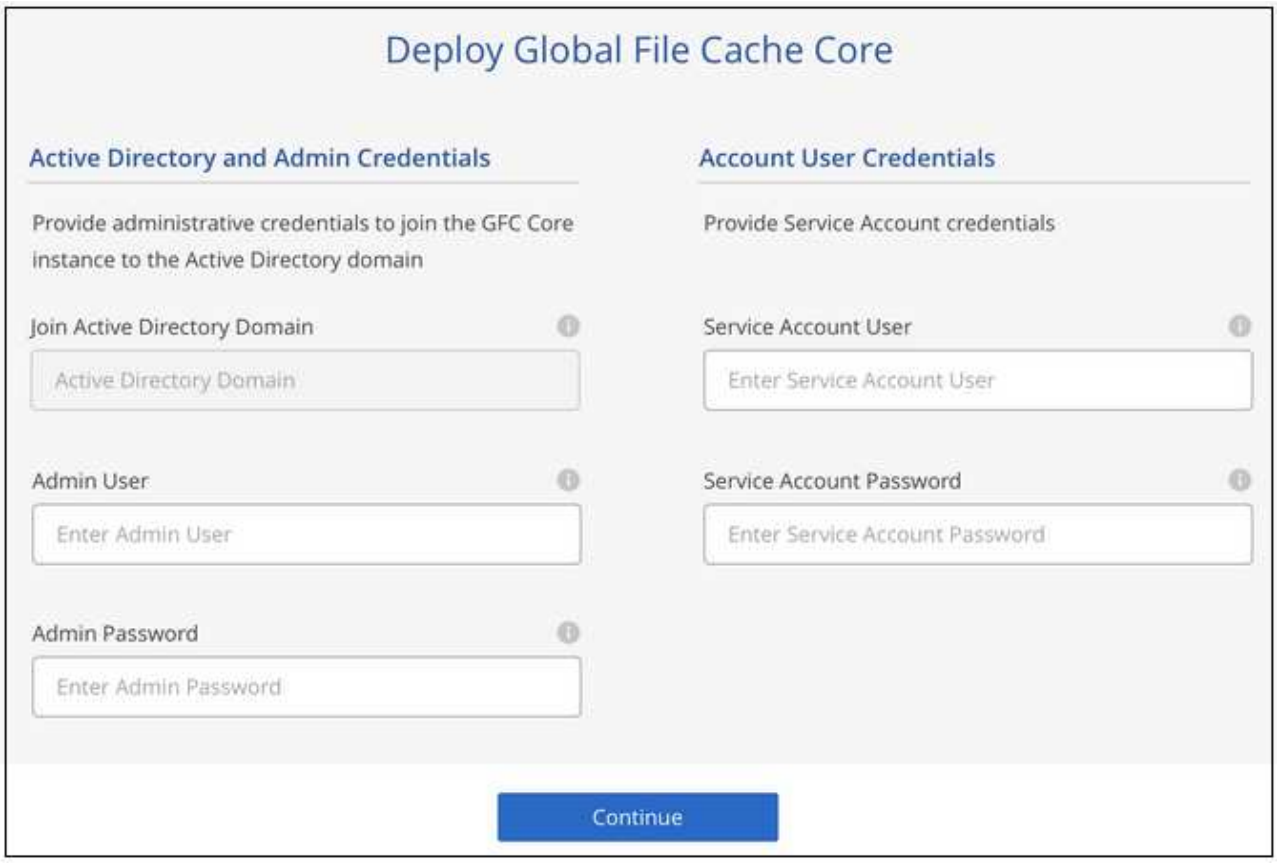
5. Nella pagina Global file cache Service, immettere il numero di istanze Global file cache Edge che si desidera implementare, quindi assicurarsi che il sistema soddisfi i requisiti per le regole di configurazione di rete e firewall, le impostazioni di Active Directory e le esclusioni antivirus. Vedere "Prerequisiti" per ulteriori dettagli.



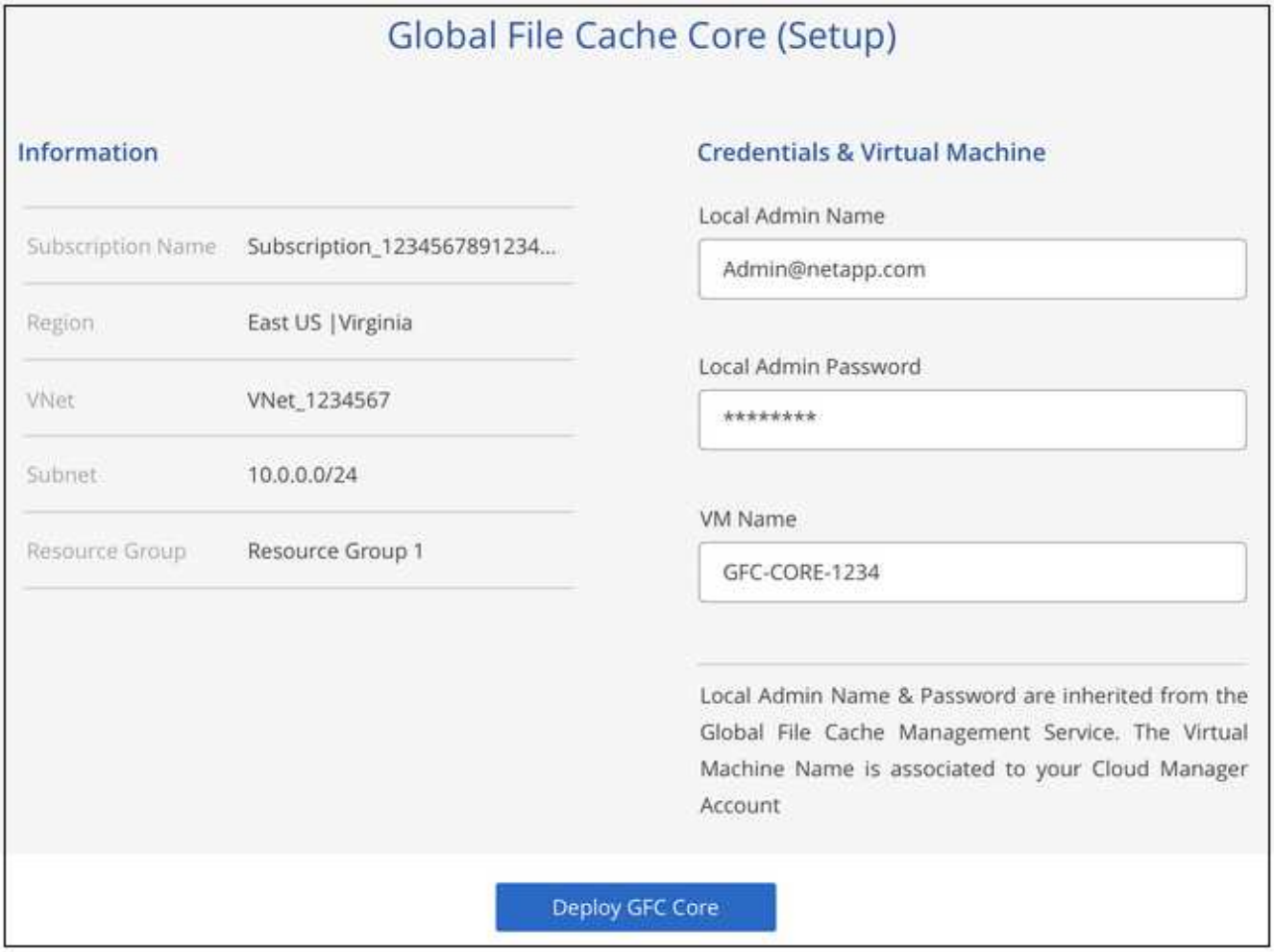
6. Dopo aver verificato che i requisiti sono stati soddisfatti o che si dispone delle informazioni necessarie per soddisfare tali requisiti, fare clic su **continua**.
7. Immettere le credenziali di amministratore da utilizzare per accedere alla macchina virtuale Global file cache Management Server e fare clic su **Enable GFC Service** (attiva servizio GFC). Per Azure, immettere le credenziali come nome utente e password; per AWS selezionare la coppia di chiavi appropriata. Se si desidera, è possibile modificare il nome della macchina virtuale/istanza.



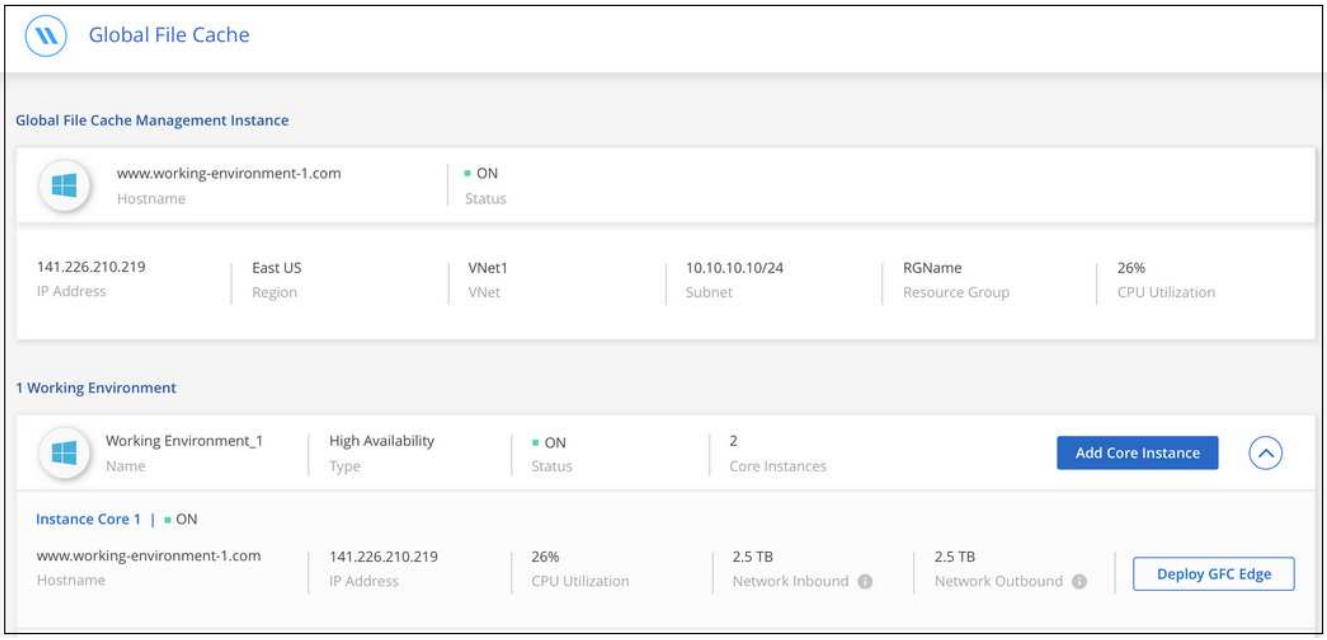
8. Una volta implementato correttamente il servizio di gestione della cache dei file globali, fare clic su **continua**.
9. Per Global file cache Core, immettere le credenziali dell'utente admin per accedere al dominio Active Directory e le credenziali dell'utente dell'account di servizio. Quindi fare clic su **continua**.
   - L'istanza principale Global file cache deve essere implementata nello stesso dominio Active Directory dell'istanza di Cloud Volumes ONTAP.
   - L'account di servizio è un utente di dominio e fa parte del gruppo BUILTIN/Backup Operators sull'istanza di Cloud Volumes ONTAP.



10. Immettere le credenziali di amministratore da utilizzare per accedere alla Global file cache Core VM e fare clic su **Deploy GFC Core**. Per Azure, immettere le credenziali come nome utente e password; per AWS selezionare la coppia di chiavi appropriata. Se si desidera, è possibile modificare il nome della macchina virtuale/istanza.



11. Una volta implementato il core Global file cache, fare clic su **Vai alla dashboard**.



La dashboard mostra che l'istanza di Management Server e l'istanza di Core sono entrambe **ON** e funzionanti.

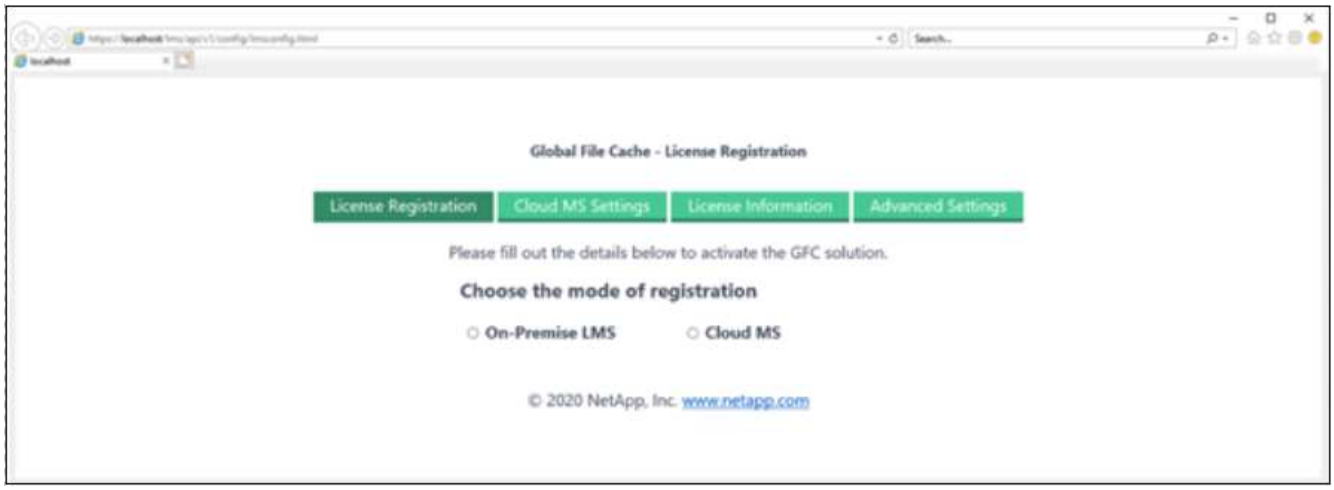
Concedere in licenza l'installazione di Global file cache

Prima di poter utilizzare Global file cache, è necessario configurare il servizio Global file cache License Management Server (LMS) su un'istanza Global file cache Core. Per attivare l'abbonamento, è necessario disporre delle credenziali NSS o di un ID cliente fornito da NetApp.

In questo esempio, configureremo il servizio LMS su un'istanza Core appena implementata nel cloud pubblico. Si tratta di un processo unico che consente di configurare il servizio LMS.

Fasi

1. Aprire la pagina Global file cache License Registration (registrazione licenza cache globale) nel Global file cache Core (il core che si sta designando come servizio LMS) utilizzando il seguente URL. Sostituire *<ip_address>* con l'indirizzo IP del core Global file cache:https://<ip_address>/lms/api/v1/config/lmsconfig.html[]
2. Fare clic su "continua con questo sito Web (scelta non consigliata)" per continuare. Viene visualizzata una pagina che consente di configurare l'LMS o di controllare le informazioni di licenza esistenti.



3. Scegliere la modalità di registrazione selezionando "LMS on-premise" o "Cloud MS".
   - "LMS on-premise" viene utilizzato per i clienti esistenti o in prova che hanno ricevuto un ID cliente tramite il supporto NetApp.
   - "Cloud MS" viene utilizzato per i clienti che hanno acquistato licenze NetApp Global file cache Edge da NetApp o dai suoi partner certificati e dispongono delle credenziali NetApp.
4. Per Cloud MS, fare clic su **Cloud MS**, inserire le credenziali NSS e fare clic su **Invia**.

5. Per LMS on-premise, fare clic su **LMS on-premise**, inserire l'ID cliente e fare clic su **Registra LMS**.

Quali sono le prossime novità?

Se si è stabilito che è necessario implementare più core Global file cache per supportare la configurazione, fare clic su **Add Core Instance** (Aggiungi istanza principale) dal dashboard e seguire la procedura guidata di implementazione.

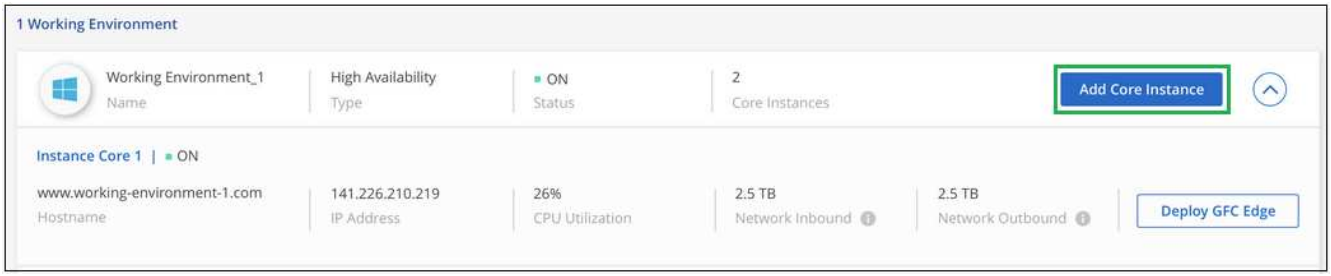
Una volta completata l'implementazione Core, è necessario "Implementare le istanze Global file cache Edge" in ogni sede remota.

Implementare istanze core aggiuntive

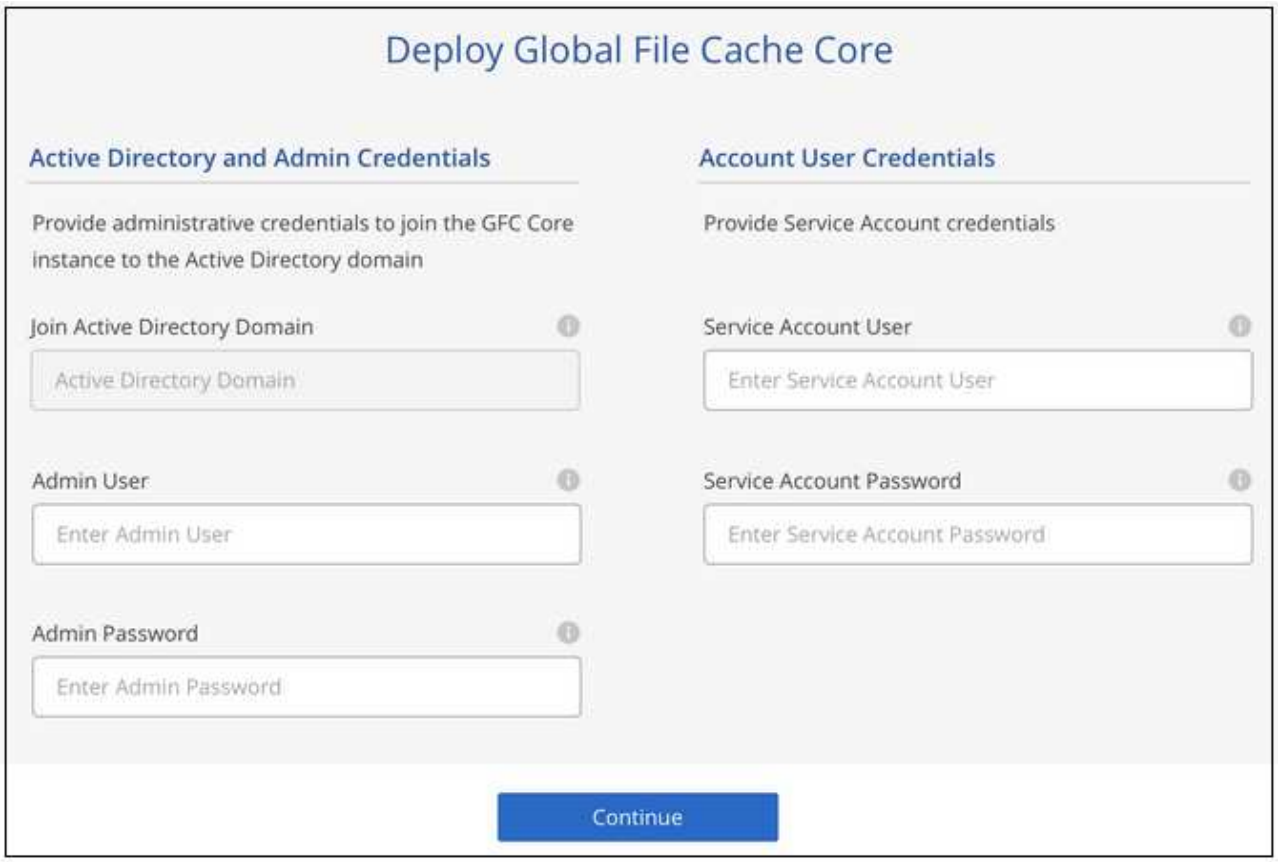
Se la configurazione richiede l'installazione di più Global file cache Core a causa di un elevato numero di istanze Edge, è possibile aggiungere un altro core all'ambiente di lavoro.

Durante l'implementazione delle istanze Edge, alcune verranno configurate per la connessione al primo core e altre al secondo core. Entrambe le istanze principali accedono allo stesso storage back-end (l'istanza di Cloud Volumes ONTAP) nell'ambiente di lavoro.

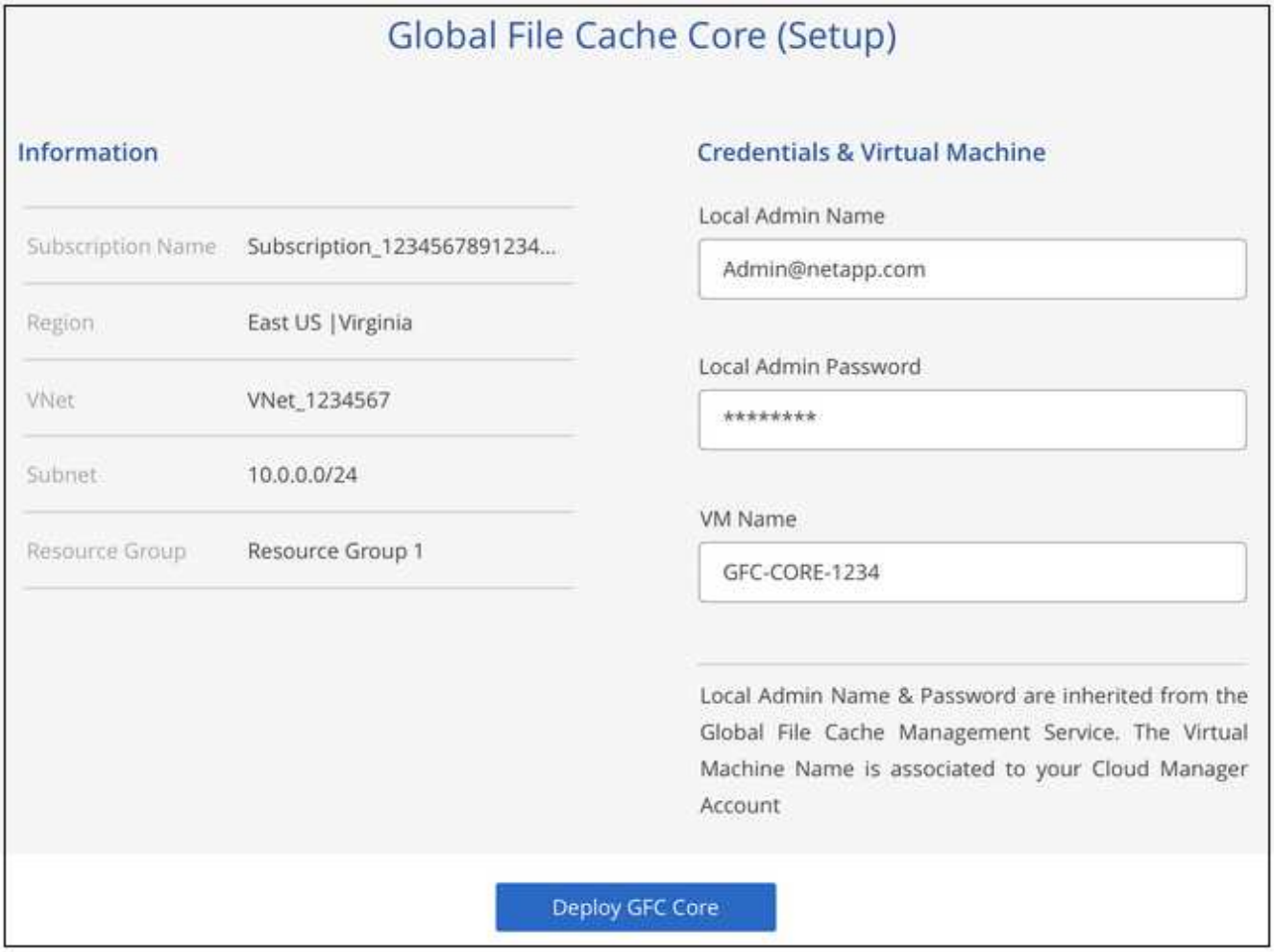
1. Dalla dashboard Global file cache, fare clic su **Add Core Instance** (Aggiungi istanza principale).



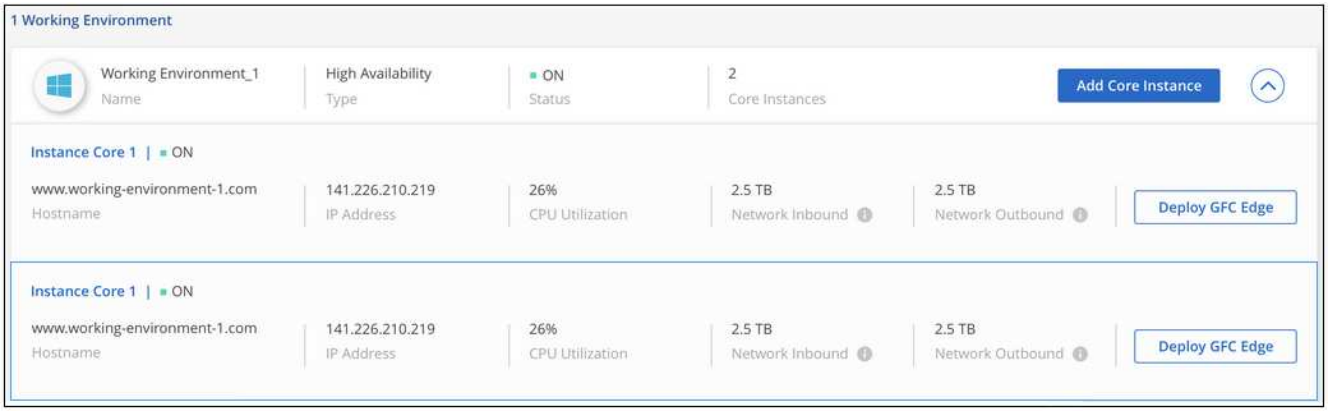
2. Immettere le credenziali dell'utente amministratore per accedere al dominio Active Directory e le credenziali dell'utente dell'account di servizio. Quindi fare clic su **continua**.
   - L'istanza principale Global file cache deve trovarsi nello stesso dominio Active Directory dell'istanza di Cloud Volumes ONTAP.
   - L'account di servizio è un utente di dominio e fa parte del gruppo BUILTIN/Backup Operators sull'istanza di Cloud Volumes ONTAP.



3. Immettere le credenziali di amministratore da utilizzare per accedere alla Global file cache Core VM e fare clic su **Deploy GFC Core**. Per Azure, immettere le credenziali come nome utente e password; per AWS selezionare la coppia di chiavi appropriata. Se si desidera, è possibile modificare il nome della macchina virtuale.



4. Una volta implementato il core Global file cache, fare clic su **Vai alla dashboard**.



La dashboard riflette la seconda istanza Core per l'ambiente di lavoro.

Prima di iniziare a implementare istanze Global file cache Edge

Prima di iniziare a installare il software Global file cache Edge nelle sedi remote, è necessario conoscere molti requisiti.

Scaricare le risorse richieste

Scarica i modelli virtuali Global file cache che intendi utilizzare nelle filiali, il pacchetto di installazione del software e la documentazione di riferimento aggiuntiva:

- Modello virtuale di Windows Server 2016:

  "Windows Server 2016 .OVA con NetApp GFC (VMware vSphere 6.5+)"
  "Windows Server 2016 .VHDX con NetApp GFC (Microsoft Hyper-v)"

- Modello virtuale di Windows Server 2019:

  "Windows Server 2019 .OVA con NetApp GFC (VMware vSphere 6.5+)"
  "Windows Server 2019 .VHDX con NetApp GFC (Microsoft Hyper-v)"

- Software Global file cache Edge:

  "Software NetApp GFC (.EXE)"

- Documentazione Global file cache:

  "Guida utente di NetApp Global file cache"

Progettazione e implementazione di Global file cache Edge

A seconda dei requisiti, potrebbe essere necessario implementare una o più istanze Global file cache Edge in base alle sessioni utente simultanee in una filiale. L'istanza di Edge presenta la condivisione di file virtuale agli utenti finali all'interno della filiale, che è stata estesa in modo trasparente dall'istanza di Global file cache Core associata. Global file cache Edge deve contenere un `D:\` Volume NTFS, che contiene i file memorizzati nella cache all'interno della filiale.

> Per Global file cache Edge, è importante comprendere "linee guida per il dimensionamento". In questo modo sarà possibile creare la progettazione corretta per l'implementazione di Global file cache. Inoltre, è necessario determinare le caratteristiche più adatte al proprio ambiente in termini di scalabilità, disponibilità delle risorse e ridondanza.

Istanza Global file cache Edge

Quando si implementa un'istanza Global file cache Edge, è necessario eseguire il provisioning di una singola macchina virtuale, implementando Windows Server 2016 Standard o Datacenter Edition, Windows Server 2019 Standard o Datacenter Edition, oppure utilizzando Global file cache `.OVA` oppure `.VHD` Modello, che include il sistema operativo Windows Server scelto e il software Global file cache.

Passaggi rapidi

1. Implementare il modello virtuale Global file cache, Windows Server 2016 VM o Windows Server 2019 Standard o Datacenter Edition.
2. Assicurarsi che la macchina virtuale sia connessa alla rete, collegata al dominio e accessibile tramite RDP.
3. Installare il software Global file cache Edge più recente.
4. Identificare Global file cache Management Server e l'istanza Core.
5. Configurare l'istanza Global file cache Edge.

Requisiti Global file cache Edge

Global file cache Edge è progettato per funzionare su tutte le piattaforme che supportano Windows Server 2016 e 2019, offrendo UN IT semplificato alle sedi remote aziendali e oltre. In modo critico, Global file cache può essere implementata nell'infrastruttura hardware esistente, nella virtualizzazione o negli ambienti di cloud ibrido/pubblico in quasi tutti i casi, se soddisfano alcuni requisiti di livello base.

Global file cache Edge richiede le seguenti risorse hardware e software per funzionare in modo ottimale. Per ulteriori informazioni sulle linee guida generali sul dimensionamento, vedere "Linee guida per il dimensionamento".

Appliance server rinforzata

Il pacchetto di installazione Global file cache crea un'appliance software avanzata su qualsiasi istanza di Microsoft Windows Server. *Non disinstallare* il pacchetto Global file cache. La disinstallazione di Global file cache avrà un impatto sulla funzionalità dell'istanza del server e potrebbe richiedere una ricostruzione completa dell'istanza del server.

Requisiti hardware fisici

- Minimo 4 core CPU
- Minimo 16 GB di RAM
- NIC dedicata singola o ridondante a 1 Gbps
- Disco rigido SAS o SSD da 10.000 rpm (preferibile)
- Controller RAID con funzionalità di caching write-back attivata

Requisiti di implementazione virtuale

È noto che le piattaforme hypervisor sono soggette a peggioramento delle performance dal punto di vista di un sottosistema di storage (ad esempio, latenza). Per ottenere performance ottimali con Global file cache, si consiglia di utilizzare un'istanza di server fisica con SSD.

Per ottenere le migliori performance negli ambienti virtuali, oltre ai requisiti degli host fisici, è necessario soddisfare i seguenti requisiti e riserve di risorse:

Microsoft Hyper-V 2012 R2 e versioni successive:

- Processore (CPU): Le CPU devono essere impostate su **statico**: Minimo: 4 core vCPU.
- Memoria (RAM): Minimo: 16 GB impostato come **statico**.
- Provisioning del disco rigido: I dischi rigidi devono essere configurati come **disco fisso**.

VMware vSphere 6.x e versioni successive:

- Processor (CPU): È necessario impostare la riserva dei cicli CPU. Minimo: 4 core vCPU @ 10000 MHz.
- Memoria (RAM): Minimo: 16 GB di spazio disponibile.
- Provisioning del disco rigido:
  - Il provisioning dei dischi deve essere impostato su **thick provisioning ansioso azzerato**.
  - Le condivisioni hard disk devono essere impostate su **High**.
  - Devices.hotplug deve essere impostato su **False** utilizzando il client vSphere per impedire a Microsoft Windows di presentare le unità Global file cache come rimovibili.

- Rete: L'interfaccia di rete deve essere impostata su **VMXNET3** (richiede VM Tools).

Global file cache viene eseguito su Windows Server 2016 e 2019, pertanto la piattaforma di virtualizzazione deve supportare il sistema operativo, oltre all'integrazione con utility che migliorano le performance del sistema operativo guest della macchina virtuale e la gestione della macchina virtuale, come VM Tools.

Requisiti di dimensionamento delle partizioni

- C: - Minimo 250 GB (volume di sistema/boot)
- D: Minimo 1 TB (volume di dati separato per Global file cache Intelligent file cache*)

*La dimensione minima è il doppio del set di dati attivo. Il volume cache (D:) può essere esteso ed è limitato solo dalle limitazioni del file system NTFS di Microsoft Windows.

Requisiti del disco Global file cache Intelligent file cache

La latenza del disco sul disco Global file cache Intelligent file cache (D:) deve garantire una latenza media dei dischi i/o inferiore a 0,5 ms e un throughput di 1 MiBps per utente simultaneo.

Per ulteriori informazioni, consultare "Guida utente di NetApp Global file cache".

Networking

- Firewall: Le porte TCP devono essere consentite tra Global file cache Edge e le istanze di Management Server e Core.

  Porte TCP Global file cache: 443 (HTTPS - LMS), 6618 – 6630.

- I dispositivi di ottimizzazione di rete (come Riverbed Steelhead) devono essere configurati per passare attraverso porte specifiche Global file cache (TCP 6618-6630).

Best practice per workstation client e applicazioni

Global file cache si integra in modo trasparente negli ambienti dei clienti, consentendo agli utenti di accedere ai dati centralizzati utilizzando le workstation client e le applicazioni aziendali. Utilizzando Global file cache, è possibile accedere ai dati attraverso una mappatura diretta del disco o uno spazio dei nomi DFS. Per ulteriori informazioni su Global file cache Fabric, Intelligent file Caching e sugli aspetti chiave del software, consultare "Prima di iniziare a implementare Global file cache" sezione.

Per garantire un'esperienza e performance ottimali, è importante rispettare i requisiti e le Best practice del client Microsoft Windows, come descritto nella Global file cache User Guide. Questo vale per tutte le versioni di Microsoft Windows.

Per ulteriori informazioni, consultare "Guida utente di NetApp Global file cache".

Best practice per firewall e antivirus

Sebbene Global file cache faccia un ragionevole sforzo per verificare che le suite di applicazioni antivirus più comuni siano compatibili con Global file cache, NetApp non può garantire e non è responsabile di eventuali incompatibilità o problemi di performance causati da questi programmi o dai relativi aggiornamenti, service pack o modifiche.

Global file cache sconsiglia l'installazione o l'applicazione di soluzioni antivirus o di monitoraggio su qualsiasi istanza abilitata per Global file cache (Core o Edge). Nel caso in cui una soluzione venga installata, a scelta o

in base a policy, è necessario applicare le seguenti Best practice e raccomandazioni. Per le suite antivirus più comuni, consultare l'Appendice A nella "Guida utente di NetApp Global file cache".

Impostazioni del firewall

- Firewall Microsoft:
  - Mantenere le impostazioni predefinite del firewall.
  - Consiglio: Lasciare le impostazioni e i servizi firewall Microsoft all'impostazione predefinita OFF e non avviarlo per le istanze standard di Global file cache Edge.
  - Consiglio: Lasciare I servizi e le impostazioni firewall Microsoft impostate su ON e avviarle per le istanze di Edge che eseguono anche il ruolo di controller di dominio.
- Firewall aziendale:
  - L'istanza Global file cache Core è in attesa sulle porte TCP 6618-6630, assicurarsi che le istanze Global file cache Edge possano connettersi a queste porte TCP.
  - Le istanze di Global file cache richiedono comunicazioni con il server di gestione della cache dei file globale sulla porta TCP 443 (HTTPS).
- Le soluzioni/i dispositivi di ottimizzazione di rete devono essere configurati per passare attraverso porte specifiche Global file cache.

Best practice antivirus

Questa sezione consente di comprendere i requisiti per l'esecuzione di software antivirus su un'istanza di Windows Server che esegue Global file cache. Global file cache ha testato i prodotti antivirus più comunemente utilizzati, tra cui Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky e Windows Defender per l'utilizzo con Global file cache.

> L'aggiunta di un antivirus a un'appliance Edge può introdurre un impatto del 10-20% sulle performance degli utenti.

Per ulteriori informazioni, consultare "Guida utente di NetApp Global file cache".

Configurare le esclusioni

Il software antivirus o altre utilità di indicizzazione o scansione di terze parti non devono mai eseguire la scansione del disco D: Sull'istanza di Edge. Queste scansioni dell'unità edge server D: Comportano numerose richieste di apertura dei file per l'intero namespace della cache. In questo modo, i file fetch sulla WAN su tutti i file server vengono ottimizzati nel data center. Si verificherà un flooding della connessione WAN e un carico non necessario sull'istanza di Edge, con conseguente peggioramento delle performance.

Oltre al disco D:, la seguente directory e i seguenti processi Global file cache dovrebbero essere generalmente esclusi da tutte le applicazioni antivirus:

- `C:\Program Files\TalonFAST\`
- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`
- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`
- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`

- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\tfs.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\ or \\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

Policy di supporto NetApp

Le istanze Global file cache sono progettate appositamente per Global file cache come applicazione principale in esecuzione su una piattaforma Windows Server 2016 e 2019. Global file cache richiede un accesso prioritario alle risorse della piattaforma, ad esempio disco, memoria, interfacce di rete, e può porre richieste elevate su queste risorse. Le implementazioni virtuali richiedono riserve di memoria/CPU e dischi dalle performance elevate.

- Per le implementazioni di Global file cache nelle filiali, i servizi e le applicazioni supportati sul server che esegue Global file cache sono limitati a:
  - DNS/DHCP
  - Controller di dominio Active Directory (Global file cache deve trovarsi su un volume separato)
  - Servizi di stampa
  - Microsoft System Center Configuration Manager (SCCM)
  - Global file cache ha approvato agenti di sistema lato client e applicazioni antivirus
- Il supporto e la manutenzione NetApp si applicano solo alla Global file cache.
- Software per la produttività delle linee di business, che in genere richiedono un uso intensivo delle risorse, ad esempio server di database, server di posta e così via, non sono supportati.
- Il cliente è responsabile di qualsiasi software non Global file cache che possa essere installato sul server che esegue Global file cache:
  - Se un pacchetto software di terze parti causa conflitti di software o risorse con Global file cache o se le prestazioni sono compromesse, l'organizzazione di supporto di Global file cache potrebbe richiedere al cliente di disattivare o rimuovere il software dal server che esegue Global file cache.
  - È responsabilità del cliente per l'installazione, l'integrazione, il supporto e l'aggiornamento di qualsiasi software aggiunto al server che esegue l'applicazione Global file cache.
- Le utility e gli agenti di gestione dei sistemi, come gli strumenti antivirus e gli agenti di licenza, potrebbero coesistere. Tuttavia, ad eccezione dei servizi e delle applicazioni supportati elencati in precedenza, queste applicazioni non sono supportate da Global file cache e devono comunque essere seguite le stesse linee guida riportate in precedenza:
  - È responsabilità del cliente per l'installazione, l'integrazione, il supporto e l'aggiornamento di qualsiasi software aggiunto.

- Se un cliente installa un pacchetto software di terze parti che causa, o si sospetta, conflitti di software o risorse con Global file cache o se le prestazioni sono compromesse, l'organizzazione di supporto di Global file cache potrebbe richiedere di disattivare/rimuovere il software.

Implementare istanze Global file cache Edge

Dopo aver verificato che l'ambiente soddisfa tutti i requisiti, installare il software Global file cache Edge in ogni sede remota.

Prima di iniziare

Per completare le attività di configurazione di Global file cache Edge, sono necessarie le seguenti informazioni:

- Indirizzi IP statici per ogni istanza di Global file cache
- Subnet mask
- Indirizzo IP del gateway
- Il nome FQDN che si desidera assegnare a ciascun server Global file cache
- Il suffisso DNS (opzionale)
- Il nome utente e la password di un utente amministrativo nel dominio
- L'FQDN e/o l'indirizzo IP dei server Core associati
- Volume da utilizzare come Intelligent file cache. Si consiglia di raddoppiare la dimensione del dataset attivo. Deve essere formattato come NTFS e assegnato come `D:\`.

Porte TCP comunemente utilizzate

I servizi Global file cache utilizzano diverse porte TCP. È obbligatorio che i dispositivi possano comunicare su queste porte ed essere esclusi da qualsiasi dispositivo di ottimizzazione WAN o policy di restrizione firewall:

- Global file cache Licensing TCP Port: 443
- Porte TCP Global file cache: 6618-6630

Implementare il modello virtuale Global file cache

Il modello virtuale `.OVA` e. `.VHD`) Le immagini contengono l'ultima versione del software Global file cache. Se si sta implementando Global file cache utilizzando `.OVA` oppure `.VHD` Modello di macchina virtuale (VM), seguire i passaggi descritti in questa sezione. Si presuppone che si comprenda come implementare `.OVA` oppure `.VHD` modello sulla piattaforma hypervisor designata.

Assicurarsi che le preferenze delle macchine virtuali, incluse le prenotazioni delle risorse, siano in linea con i requisiti descritti nella "Requisiti di implementazione virtuale".

Fasi

1. Estrarre il pacchetto dal modello scaricato.
2. Implementare il modello virtuale. Fare riferimento ai seguenti video prima di iniziare l'implementazione:
   - "Implementare il modello virtuale su VMware"
   - "Implementare il modello virtuale su Hyper-V."
3. Dopo aver implementato il modello virtuale e aver configurato le impostazioni della macchina virtuale,

avviare la macchina virtuale.

4. Durante l'avvio iniziale, quando il sistema operativo Windows Server 2016 o 2019 si prepara per il primo utilizzo, completare l'esperienza pronta all'uso installando i driver corretti e installando i componenti necessari per il rispettivo hardware.
5. Una volta completata l'installazione di base dell'istanza Global file cache Edge, il sistema operativo Windows Server 2016 o 2019 guida l'utente attraverso una configurazione guidata iniziale per configurare le specifiche del sistema operativo, come la localizzazione e il codice "Product Key".
6. Una volta completata la configurazione guidata iniziale, accedere localmente al sistema operativo Windows Server 2016 o 2019 con le seguenti credenziali:
   - Nome utente: **FASTAdmin**
   - Password: **Tal0nFAST!**
7. Configurare la macchina virtuale Windows Server, accedere al dominio Active Directory dell'organizzazione e passare alla sezione di configurazione Global file cache Edge.

Configurare l'istanza Global file cache Edge

L'istanza Global file cache Edge si connette a un core Global file cache per fornire agli utenti della filiale l'accesso alle risorse del file server del data center.

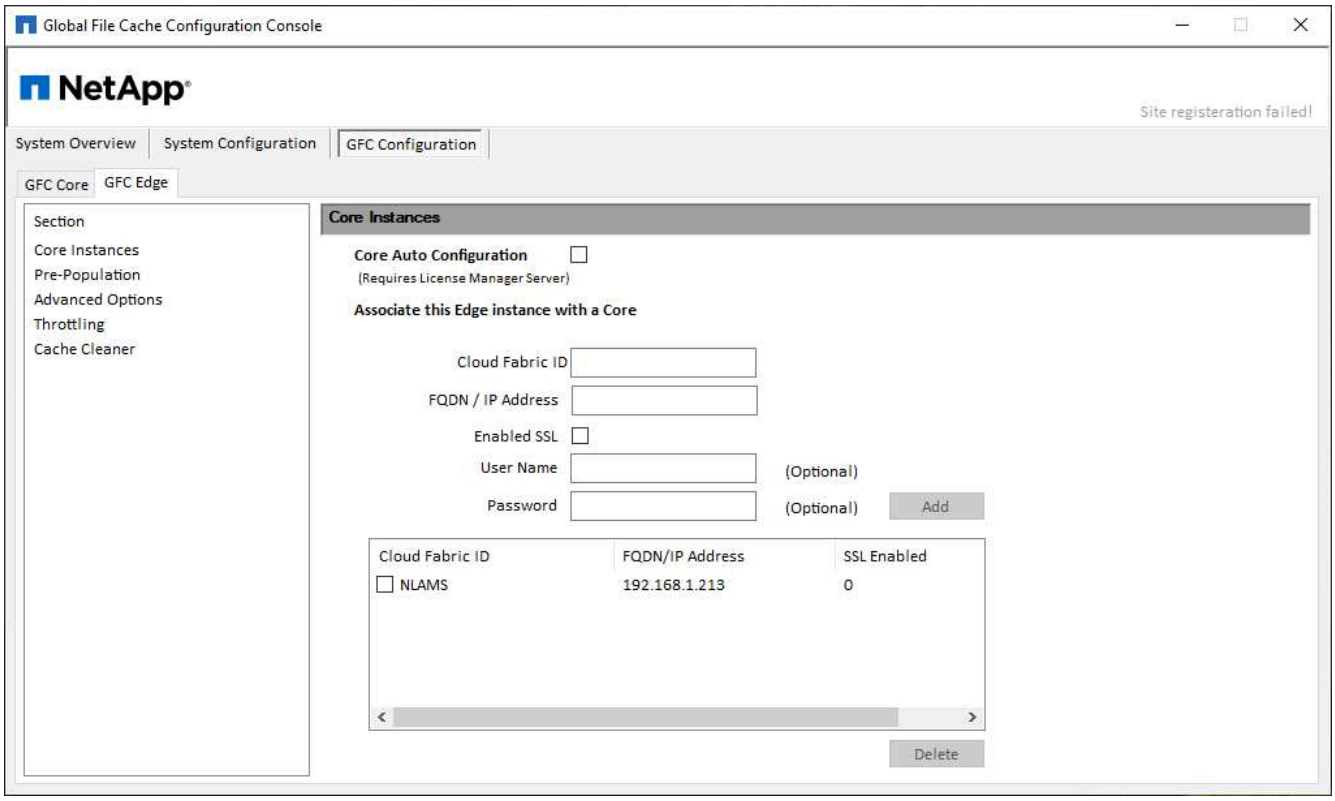
Prima di iniziare la configurazione, l'istanza di Edge deve essere concessa in licenza come parte della distribuzione di Cloud Volumes ONTAP. Vedere "Licensing" per ulteriori informazioni sulle licenze.

Se la configurazione richiede l'installazione di più di un Global file cache Core a causa di un elevato numero di istanze Edge, verranno configurate alcune istanze Edge per la connessione al primo core e altre per la connessione al secondo core. Assicurarsi di disporre dell'FQDN o dell'indirizzo IP e di altre informazioni necessarie per l'istanza Core corretta.

Per configurare l'istanza di Edge, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Perform** (Esegui) accanto alla fase Core Configuration (Configurazione principale) non selezionata, elencata nella sezione "Edge Configuration Steps" (fasi di configurazione edge) dell'assistente di configurazione iniziale. Viene visualizzata una nuova scheda, GFC Edge, che mostra la sezione *istanze core*.
2. Fornire l'ID **Cloud Fabric** del server Global file cache Core. L'ID Cloud Fabric è generalmente il nome NetBIOS o la posizione geografica del file server back-end.
3. Fornire l'indirizzo **FQDN/IP** del server Global file cache Core:
   a. (Facoltativo) selezionare la casella **SSL** per abilitare il supporto SSL per la crittografia avanzata dall'edge al core.
   b. Inserire il nome utente e la password, ovvero le credenziali dell'account di servizio utilizzato nel Core.
4. Fare clic su **Add** (Aggiungi) per confermare l'aggiunta dell'appliance Global file cache Core. Viene visualizzata una finestra di conferma. Fare clic su **OK** per chiudere l'operazione.



Aggiornare il software Global file cache Edge

Global file cache rilascia frequentemente aggiornamenti al software, patch, miglioramenti o nuove funzionalità. Anche se il modello virtuale (`.OVA` e. `.VHD`) Le immagini contengono l'ultima release del software Global file cache, è possibile che una versione più recente sia disponibile sul portale NetApp Support Download.

Assicurarsi che le istanze Global file cache siano aggiornate con la versione più recente.

> Questo pacchetto software può essere utilizzato anche per installazioni incontaminate su Microsoft Windows Server 2016 Standard o Datacenter Edition, Windows Server 2019 Standard o Datacenter Edition, oppure come parte della strategia di upgrade.

Di seguito sono riportati i passaggi necessari per aggiornare il pacchetto di installazione Global file cache:

Fasi

1. Dopo aver salvato l'ultimo pacchetto di installazione nell'istanza di Windows Server desiderata, fare doppio clic su di esso per eseguire l'eseguibile di installazione.
2. Fare clic su **Avanti** per continuare il processo.
3. Fare clic su **Avanti** per continuare.
4. Accettare il Contratto di licenza e fare clic su **Avanti**.
5. Selezionare la posizione di destinazione dell'installazione desiderata.

   NetApp consiglia di utilizzare la posizione di installazione predefinita.

6. Fare clic su **Avanti** per continuare.
7. Selezionare la cartella del menu Start.

8. Fare clic su **Avanti** per continuare.
9. Verificare i parametri di installazione desiderati e fare clic su **Install** (Installa) per avviare l'installazione.

   Il processo di installazione viene eseguito.

10. Al termine dell'installazione, riavviare il server quando richiesto.

Quali sono le prossime novità?

Per ulteriori informazioni sulla configurazione avanzata di Global file cache Edge, consultare "Guida utente di NetApp Global file cache".

Formazione per l'utente finale

Si desidera formare gli utenti sulle Best practice per l'accesso ai file condivisi tramite Global file cache.

Questa è la fase finale dell'implementazione della Global file cache, ovvero la fase di implementazione dell'utente finale.

Per preparare e ottimizzare il processo di assunzione dell'utente finale, utilizza il modello di e-mail riportato di seguito che ti aiuterà a informare gli utenti finali su cosa significa lavorare in un ambiente "dati centrali". In questo modo, gli utenti potranno sfruttare tutti i vantaggi della soluzione Global file cache. Abbiamo anche pubblicato un video che può essere condiviso per "formare" gli utenti dove necessario.

Personalizzare e inoltrare le seguenti risorse agli utenti finali per prepararle all'implementazione:

- Video di training per l'utente"Video di training per l'utente finale"
- Modello e-mail"Modello e-mail Mac (.emltpl)"

  "Modello e-mail Windows (.msg)"

- Comunicazioni di assunzione"Documento Word (.docx)"

Vedere il capitolo 12 della "Guida utente di NetApp Global file cache" per materiale aggiuntivo.

Ulteriori informazioni

Utilizza i seguenti link per saperne di più su Global file cache e altri prodotti NetApp:

- Domande frequenti su Global file cache
  - Consulta un elenco di domande e risposte frequenti "qui"
- "Guida utente di NetApp Global file cache"
- Documentazione sui prodotti NetApp
  - Consultare la documentazione aggiuntiva per i prodotti cloud NetApp "qui"
  - Consultare la documentazione aggiuntiva per tutti i prodotti NetApp "qui"
- Il supporto clienti per gli utenti di Global file cache con Cloud Volumes ONTAP è disponibile attraverso i seguenti canali:
  - Risoluzione guidata dei problemi, Gestione dei casi, Knowledge base, Download, Strumenti, e molto altro ancora "qui"

    - Accedere al supporto NetApp all'indirizzo https://mysupport.netapp.com Con le tue credenziali NSS
    - Per assistenza immediata per un problema P1, chiamare il numero: +1 856.481.3990 (opzione 2)
- Il supporto clienti per gli utenti di Global file cache che utilizzano Cloud Volumes Services e Azure NetApp Files è disponibile attraverso il supporto standard del tuo provider. Contattare rispettivamente il supporto clienti Google o il supporto clienti Microsoft.

Ottimizza i costi di calcolo del cloud

Scopri di più sul servizio di calcolo

Sfruttando "Servizio Cloud Analyzer di Spot", Cloud Manager può fornire un'analisi dei costi di alto livello delle spese di calcolo del cloud e identificare i potenziali risparmi.

Cloud Analyzer è una soluzione per la gestione dell'infrastruttura cloud che utilizza analytics avanzati per fornire visibilità e informazioni sui costi del cloud. Ti mostra dove puoi ottimizzare questi costi e ti consente di implementare l'ottimizzazione utilizzando il portfolio di prodotti di ottimizzazione continua di Spot in pochi clic.

Caratteristiche

- Un'analisi dei costi che mostra il costo corrente del mese, i costi mensili previsti e i risparmi persi
- Una vista dell'efficienza della spesa per account, inclusi i risparmi aggiuntivi stimati
- Un link a Spot's Cloud Analyzer per ulteriori dettagli sulla spesa per tutti gli account

Cloud provider supportati

Questo servizio è supportato da AWS.

Costo

L'utilizzo di questo servizio tramite Cloud Manager è gratuito.

Come funziona Cloud Analyzer con Cloud Manager

Ad alto livello, l'integrazione di Cloud Analyzer con Cloud Manager funziona come segue:

1. Fai clic su **Compute** (Calcola) e connetti il tuo account master payer AWS.
2. NetApp configura il tuo ambiente come segue:
   a. Crea un'organizzazione nella piattaforma Spot.
   b. Invia un'e-mail di benvenuto a Spot.

      Puoi accedere al servizio Spot utilizzando le stesse credenziali di single-sign-on utilizzate con Cloud Central e Cloud Manager.

   c. Cloud Analyzer avvia l'elaborazione dei dati dell'account AWS.
3. In Cloud Manager, la pagina di calcolo viene aggiornata e le informazioni vengono utilizzate per ottenere informazioni sui costi del cloud passati, attuali e futuri.
4. Fai clic su **Ottieni analisi completa** in qualsiasi momento per accedere a Spot's Cloud Analyzer, che offre un'analisi completa della spesa nel cloud e delle opportunità di risparmio.

Sicurezza dei dati

I dati Cloud Analyzer vengono crittografati a riposo e non vengono memorizzate credenziali per alcun account.

Inizia a ottimizzare i costi di calcolo del cloud

Connetti il tuo account AWS e visualizza l'analisi per iniziare a ottimizzare i costi di calcolo del cloud.

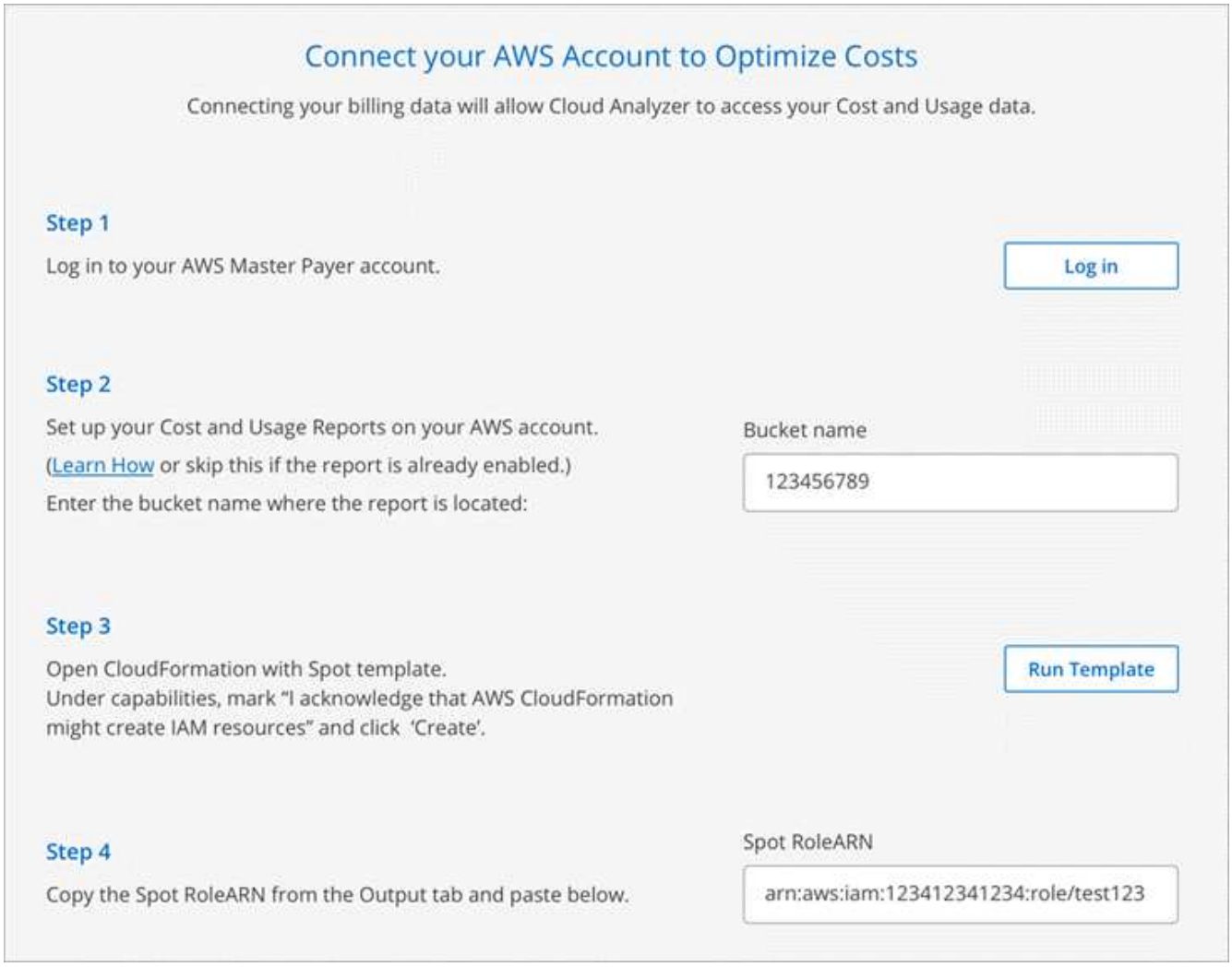
Connetti Cloud Analyzer al tuo account AWS

Fare clic su **Compute** (Calcola) e collegare l'account AWS payer.

Fasi

1. Fare clic su **Compute** (Calcola).
2. Fare clic su **Add AWS Credentials to Start** (Aggiungi credenziali AWS a Start).
3. Seguire la procedura riportata nella pagina per collegare l'account AWS:
    a. Accedi al tuo account master payer di AWS.
    b. Impostare i report sui costi e sull'utilizzo sull'account AWS.
    c. Eseguire il modello CloudFormation.
    d. Incollare il RoleARN di Spot.

    "Visualizza ulteriori dettagli su questi passaggi".

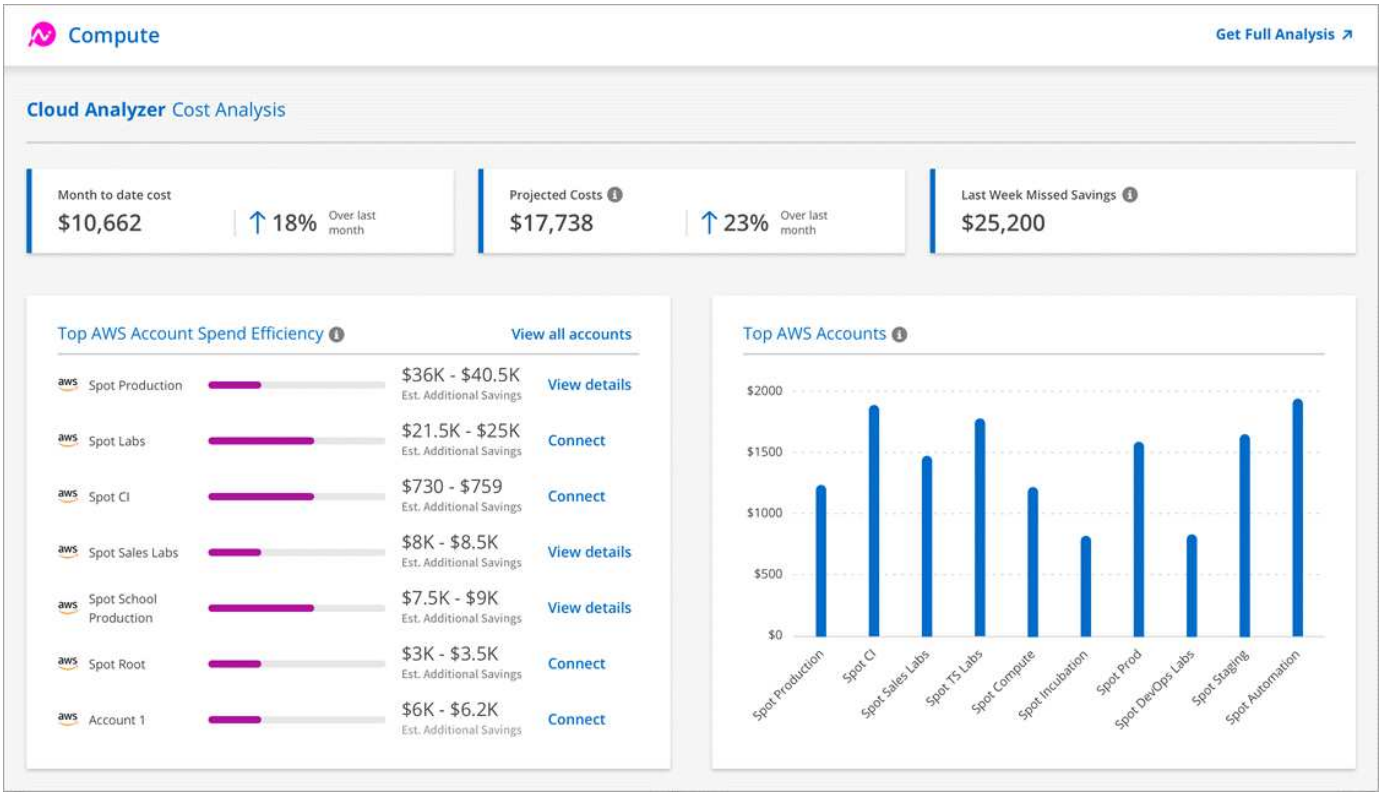


Risultato

Cloud Analyzer avvia l'elaborazione dei dati dell'account AWS. Se disponi di più account, Cloud Analyzer inizia con funzionalità di sola lettura per tutti gli account collegati nell'account master pager. Se desideri ottenere ulteriori informazioni sui potenziali risparmi per questi account, dovrai collegarli. Per ulteriori informazioni su tale processo, consultare la sezione seguente.

Analizza i costi di calcolo

Dopo che Cloud Analyzer elabora i dati del tuo account, la scheda calcolo mostra informazioni sui costi del cloud passati, attuali e futuri.



Costo mensile

Il costo totale dei carichi di lavoro dall'inizio del mese corrente fino al momento attuale.

Costi previsti

Il costo previsto alla fine del mese in base all'analisi del tuo modello di utilizzo.

Risparmi mancati la scorsa settimana

Risparmi che avrebbero potuto essere ottenuti nei sette giorni precedenti utilizzando l'ottimizzazione delle istanze e delle prenotazioni spot.

Massima efficienza di spesa degli account AWS

I primi 10 conti in base alla maggiore quantità di risparmi aggiuntivi stimati.

A ciascun account viene assegnato un punteggio di efficienza basato sui potenziali risparmi attuali e aggiuntivi. I risparmi aggiuntivi stimati indicano quanto può essere ulteriormente risparmiato sfruttando l'utilizzo di istanze spot e riservate.

Per ottimizzare ulteriormente i tuoi account, puoi eseguire le seguenti azioni:

- **Visualizza i dettagli**: Visualizza le tue opportunità di ottimizzazione dei costi visitando Spot's Cloud Analyzer.
- **Connect**: Consente di connettere un account non ancora gestito. Viene visualizzata la procedura guidata che connette l'account.

Principali account AWS

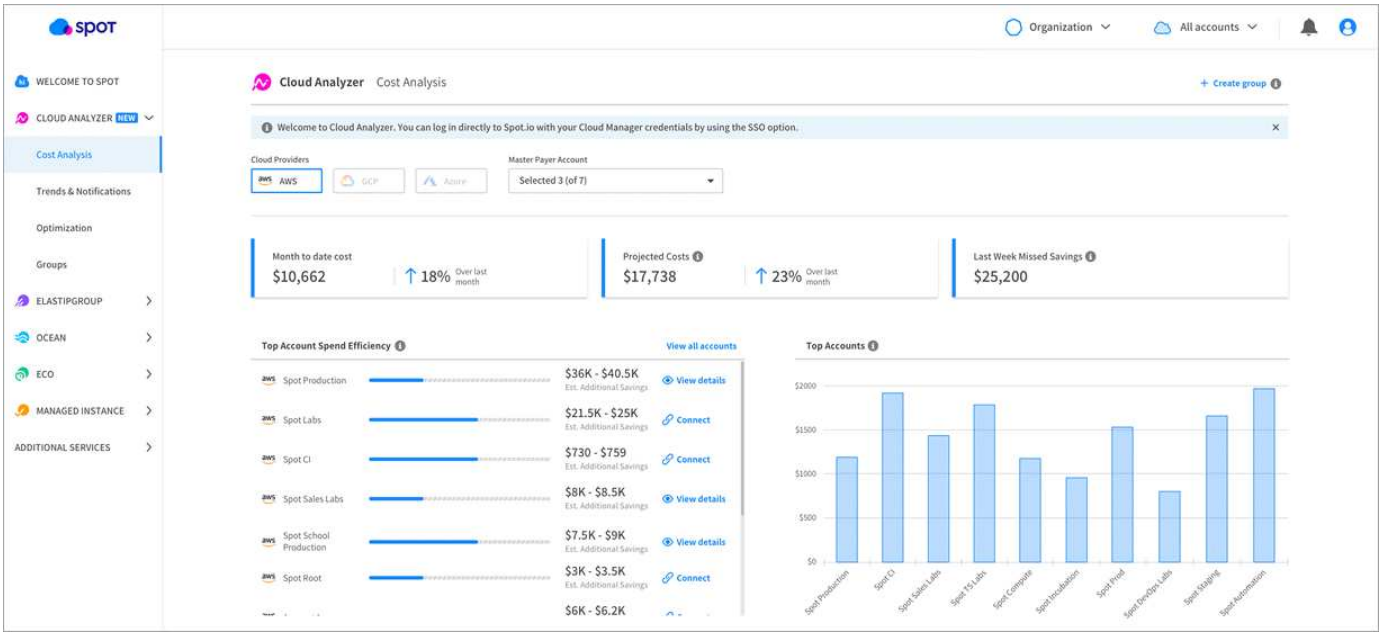
Questo è un grafico a barre che mostra i primi dieci account in base al costo. Il grafico si basa sugli ultimi 30 giorni di attività di spesa.

"Scopri di più sulla pagina analisi dei costi disponibile in Spot's Cloud Analyzer".

Vai a Cloud Analyzer per ulteriori analisi e consigli

Fai clic su **Ottieni analisi completa** in qualsiasi momento per accedere a più grafici e analisi, consigli approfonditi, analisi per l'ottimizzazione dei casi d'utilizzo (container, ElasticApps e prenotazioni) e molto altro ancora.

Ecco un esempio di ciò che vedrai in Cloud Analyzer:



- "Consulta la pagina del prodotto di Cloud Analyzer per saperne di più sulle sue funzionalità".
- "Consulta la documentazione di Spot per ottenere assistenza con Cloud Analyzer".

Tiering dei dati nel cloud

Scopri di più sul Cloud Tiering

Il servizio di tiering cloud di NetApp estende il tuo data center al cloud attraverso il tiering automatico dei dati inattivi dai cluster ONTAP on-premise allo storage a oggetti. In questo modo si libera spazio prezioso sul cluster per più carichi di lavoro, senza apportare modifiche al livello applicativo. Il cloud tiering può ridurre i costi nel tuo data center e consente di passare da un modello CAPEX a un modello OPEX.

Il servizio di tiering cloud sfrutta le funzionalità di *FabricPool*. FabricPool è una tecnologia NetApp Data Fabric che consente il tiering automatizzato dei dati verso uno storage a oggetti a basso costo. I dati attivi rimangono su SSD dalle performance elevate, mentre i dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo, preservando al contempo l'efficienza dei dati ONTAP.

Caratteristiche

Cloud Tiering offre automazione, monitoraggio, report e un'interfaccia di gestione comune:

- L'automazione semplifica la configurazione e la gestione del tiering dei dati dai cluster ONTAP on-premise al cloud
- Un singolo pannello di controllo elimina la necessità di gestire in modo indipendente FabricPool in diversi cluster
- I report mostrano la quantità di dati attivi e inattivi su ciascun cluster
- Uno stato di salute tiering ti aiuta a identificare e correggere i problemi man mano che si verificano
- Se disponi di sistemi Cloud Volumes ONTAP, puoi trovarli nella dashboard dei cluster per ottenere una vista completa del tiering dei dati nella tua infrastruttura di cloud ibrido

I sistemi Cloud Volumes ONTAP sono di sola lettura dal cloud tiering. "Hai impostato il tiering per Cloud Volumes ONTAP dall'ambiente di lavoro in Cloud Manager".

Per ulteriori informazioni sul valore offerto dal Cloud Tiering, "Consulta la pagina Cloud Tiering su NetApp Cloud Central".

Anche se il Cloud Tiering può ridurre significativamente l'ingombro dello storage, non è una soluzione di backup.

Provider di storage a oggetti supportati

È possibile raggruppare i dati inattivi da un cluster ONTAP in Amazon S3, storage Blob Microsoft Azure, storage cloud Google o StorageGRID (cloud privato).

Prezzi e licenze

Paga il tiering cloud con un abbonamento pay-as-you-go, una licenza di tiering ONTAP chiamata *FabricPool* o una combinazione di entrambi. Se non si dispone di una licenza, è disponibile una versione di prova gratuita di 30 giorni per il primo cluster.

Non sono previsti costi per il tiering dei dati su StorageGRID. Non è richiesta alcuna licenza BYOL o registrazione PAYGO.

"Visualizza i dettagli dei prezzi".

30 giorni di prova gratuita

Se non disponi di una licenza FabricPool, inizia una prova gratuita di 30 giorni del Cloud Tiering quando configuri il tiering sul primo cluster. Al termine della prova gratuita di 30 giorni, dovrai pagare il Tier cloud tramite un abbonamento pay-as-you-go, una licenza FabricPool o una combinazione di entrambi.

Se la versione di prova gratuita termina e non hai sottoscritto o aggiunto una licenza, ONTAP non esegue più il Tier dei dati cold sullo storage a oggetti, ma i dati esistenti sono ancora disponibili per l'accesso.

Abbonamento pay-as-you-go

Cloud Tiering offre licenze basate sui consumi in un modello pay-as-you-go. Dopo aver effettuato l'iscrizione attraverso il marketplace del tuo cloud provider, paghi per GB i dati a più livelli, senza alcun pagamento anticipato. Il tuo cloud provider ti addebita la fattura mensile.

È necessario iscriversi anche se si dispone di una versione di prova gratuita o se si porta la propria licenza (BYOL):

- L'iscrizione garantisce che non vi siano interruzioni del servizio al termine della prova gratuita.

  Al termine del periodo di prova, ti verrà addebitato ogni ora in base alla quantità di dati che hai effettuato il tiering.

- Se si dispone di un numero di dati superiore a quello consentito dalla licenza FabricPool, il tiering dei dati continua con l'abbonamento pay-as-you-go.

  Ad esempio, se si dispone di una licenza da 10 TB, tutta la capacità oltre i 10 TB viene addebitata tramite l'abbonamento pay-as-you-go.

Durante la prova gratuita o se non hai superato la licenza di FabricPool, non ti verrà addebitato alcun costo dal tuo abbonamento pay-as-you-go.

"Scopri come impostare un abbonamento pay-as-you-go".

Porta la tua licenza

Porta la tua licenza acquistando una licenza ONTAP FabricPool da NetApp. È possibile acquistare licenze a termine o perpetue.

Dopo aver acquistato una licenza FabricPool, sarà necessario aggiungerla al cluster, "Che puoi fare direttamente da Cloud Tiering".

Dopo aver attivato la licenza tramite Cloud Tiering, se si acquista ulteriore capacità aggiuntiva in un secondo momento, la licenza sul cluster viene aggiornata automaticamente con la nuova capacità. Non è necessario applicare un nuovo file di licenza NetApp (NLF) al cluster.

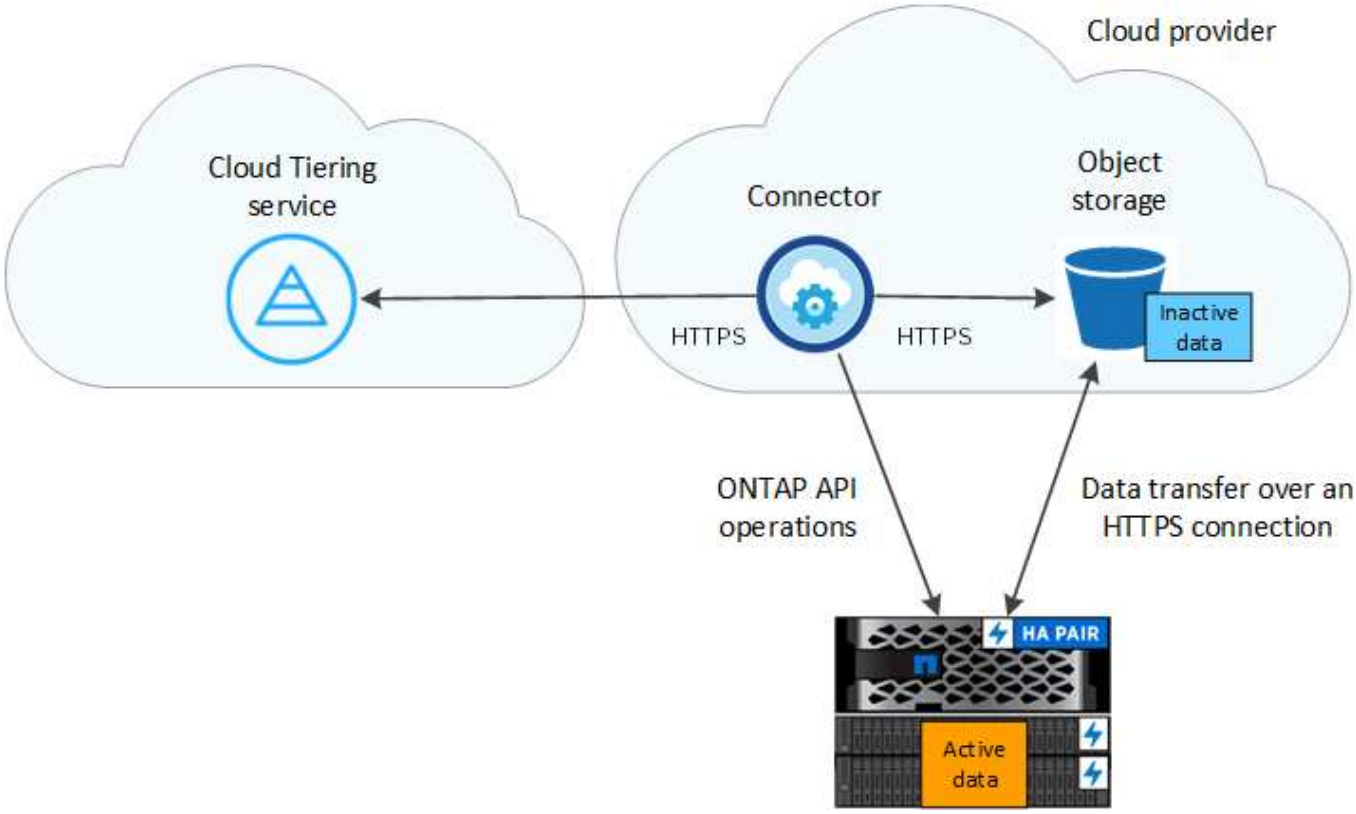
Come indicato in precedenza, si consiglia di impostare un abbonamento pay-as-you-go, anche se il cluster dispone di una licenza BYOL.

Mailto:ng-cloud-tiering@netapp.com?subject=Licensing[Contattaci per acquistare una licenza].

Come funziona il Cloud Tiering

Cloud Tiering è un servizio gestito da NetApp che utilizza la tecnologia FabricPool per tierare automaticamente i dati inattivi (cold) dai cluster ONTAP on-premise allo storage a oggetti nel cloud pubblico o privato. Le connessioni a ONTAP avvengono da un connettore.

La seguente immagine mostra la relazione tra ciascun componente:



A un livello elevato, il Cloud Tiering funziona come segue:

1. Scopri il tuo cluster on-premise da Cloud Manager.
2. È possibile impostare il tiering fornendo dettagli sullo storage a oggetti, tra cui bucket/container e una classe di storage o un Tier di accesso.
3. Cloud Manager configura ONTAP per l'utilizzo del provider di storage a oggetti e rileva la quantità di dati attivi e inattivi nel cluster.
4. È possibile scegliere i volumi da tiering e il criterio di tiering da applicare a tali volumi.
5. ONTAP avvia il tiering dei dati inattivi nell'archivio di oggetti, non appena i dati raggiungono le soglie da considerare inattivi (vedere Policy di tiering dei volumi).

Storage a oggetti

Ogni cluster ONTAP esegue il Tier dei dati inattivi in un singolo archivio di oggetti. Quando si imposta il tiering dei dati, è possibile aggiungere un nuovo bucket/container o selezionare un bucket/container esistente, insieme a una classe di storage o a un Tier di accesso.

- "Scopri le classi di storage S3 supportate"
- "Scopri i Tier di accesso supportati da Azure Blob"

- "Scopri le classi di storage supportate da Google Cloud"

Policy di tiering dei volumi

Quando si selezionano i volumi che si desidera applicare il Tier, si sceglie una *policy di tiering dei volumi* da applicare a ciascun volume. Una policy di tiering determina quando o se i blocchi di dati utente di un volume vengono spostati nel cloud.

Nessuna policy di tiering
: Mantiene i dati su un volume nel Tier di performance, impedendo che vengano spostati nel cloud.

Snapshot a freddo (solo Snapshot)
: ONTAP esegue il tiering dei blocchi snapshot cold nel volume che non sono condivisi con il file system attivo sullo storage a oggetti. Se letti, i blocchi di dati cold nel Tier cloud diventano hot e vengono spostati nel Tier di performance.

  I dati vengono suddivisi in livelli solo dopo che un aggregato ha raggiunto la capacità del 50% e quando i dati hanno raggiunto il periodo di raffreddamento. Il numero predefinito di giorni di raffreddamento è 2, ma è possibile regolare il numero di giorni.

  > Le scritture dal Tier cloud al Tier performance sono disattivate se la capacità del Tier performance è superiore al 70%. In questo caso, si accede ai blocchi direttamente dal livello cloud.

Cold User Data (Auto) (dati utente cold)
: ONTAP esegue il tiering di tutti i cold block del volume (esclusi i metadati) nello storage a oggetti. I dati cold non includono solo le copie Snapshot, ma anche i dati cold user dal file system attivo.

  Se letti in lettura casuale, i blocchi di dati cold nel Tier cloud diventano hot e vengono spostati nel Tier di performance. Se letti in base a letture sequenziali, come quelle associate a scansioni di indice e antivirus, i blocchi di dati cold sul livello cloud rimangono freddi e non vengono scritti sul livello di performance.

  I dati vengono suddivisi in livelli solo dopo che un aggregato ha raggiunto la capacità del 50% e quando i dati hanno raggiunto il periodo di raffreddamento. Il periodo di raffreddamento è il tempo in cui i dati dell'utente in un volume devono rimanere inattivi per essere considerati "freddi" e spostati nell'archivio di oggetti. Il numero predefinito di giorni di raffreddamento è 31, ma è possibile regolare il numero di giorni.

  > Le scritture dal Tier cloud al Tier performance sono disattivate se la capacità del Tier performance è superiore al 70%. In questo caso, si accede ai blocchi direttamente dal livello cloud.

Tutti i dati utente (tutti)
: Tutti i dati (non inclusi i metadati) vengono immediatamente contrassegnati come cold e tiered per lo storage a oggetti il più presto possibile. Non è necessario attendere 48 ore affinché i nuovi blocchi di un volume si raffreddino. Tenere presente che i blocchi situati nel volume prima dell'impostazione del criterio All richiedono 48 ore per diventare freddi.

  In caso di lettura, i blocchi di dati cold nel Tier cloud restano freddi e non vengono riscritti nel Tier di performance. Questo criterio è disponibile a partire da ONTAP 9.6.

  Prima di scegliere questa policy di tiering, prendere in considerazione quanto segue:

  - Il tiering dei dati riduce immediatamente l'efficienza dello storage (solo inline).

- Utilizzare questa policy solo se si è sicuri che i dati cold sul volume non cambiano.
- Lo storage a oggetti non è transazionale e si tradurrà in una frammentazione significativa se soggetto a modifiche.
- Considerare l'impatto dei trasferimenti SnapMirror prima di assegnare la policy di tiering a volumi di origine nelle relazioni di protezione dei dati.

  Poiché i dati vengono immediatamente suddivisi in Tier, SnapMirror legge i dati dal Tier cloud piuttosto che dal Tier di performance. Ciò rallenterà le operazioni di SnapMirror, probabilmente rallentando altre operazioni di SnapMirror in un secondo momento in coda, anche se utilizzano policy di tiering diverse.

Tutti i dati utente DP (backup)

Tutti i dati presenti in un volume di protezione dei dati (esclusi i metadati) vengono immediatamente spostati nel Tier cloud. In caso di lettura, i blocchi di dati cold nel livello cloud rimangono freddi e non vengono riscritti nel Tier di performance (a partire da ONTAP 9.4).

Questo criterio è disponibile per ONTAP 9.5 o versioni precedenti. È stato sostituito con la policy di tiering **all** a partire da ONTAP 9.6.

Inizia subito

Tiering dei dati dai cluster ONTAP on-premise ad Amazon S3

Liberare spazio sui cluster ONTAP on-premise mediante il tiering dei dati su Amazon S3. Il tiering dei dati è basato sul servizio Cloud Tiering di NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Preparatevi a eseguire il tiering dei dati su Amazon S3

Sono necessari i seguenti elementi:

- Un sistema AFF o FAS con aggregati all-SSD che esegue ONTAP 9.2 o versione successiva e dispone di una connessione HTTPS ad Amazon S3.
- Un account AWS che dispone di una chiave di accesso e. le autorizzazioni richieste In questo modo, il cluster ONTAP può eseguire il tiering dei dati inattivi in e fuori da S3.
- Un connettore installato in un VPC AWS o on-premise.
- Rete per il connettore che abilita una connessione HTTPS in uscita al cluster ONTAP, allo storage S3 e al servizio di tiering cloud.

Impostare il tiering

In Cloud Manager, selezionare un ambiente di lavoro on-premise, fare clic su **Setup Tiering** e seguire le istruzioni per assegnare i dati ad Amazon S3.

Impostare la licenza

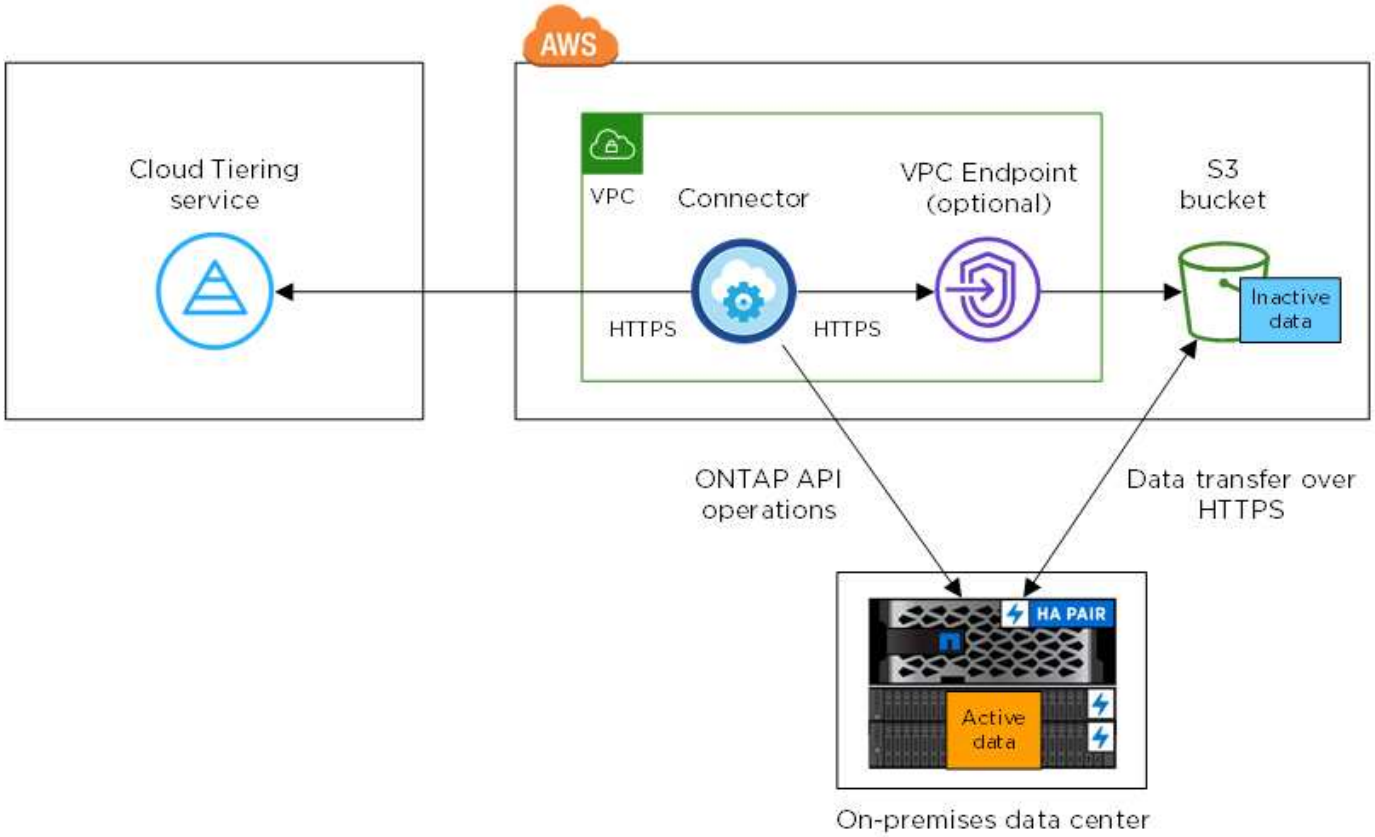
Al termine della prova gratuita, paga il Tier cloud con un abbonamento pay-as-you-go, una licenza di tiering ONTAP o una combinazione di entrambi:

- Per iscriversi a AWS Marketplace, fare clic su **Tiering > Licensing**, fare clic su **Subscribe**, quindi seguire le istruzioni.
- Per pagare utilizzando una licenza di tiering, contattaci se devi acquistarne una, quindi "Aggiungilo al tuo cluster da Cloud Tiering".

Requisiti

Verificare il supporto per il cluster ONTAP, configurare la rete e preparare lo storage a oggetti.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



La comunicazione tra un connettore e S3 è solo per la configurazione dello storage a oggetti. Il connettore può risiedere in sede, invece che nel cloud.

Preparazione dei cluster ONTAP

I cluster ONTAP devono soddisfare i seguenti requisiti quando si esegue il tiering dei dati su Amazon S3.

Piattaforme ONTAP supportate

Cloud Tiering supporta sistemi AFF e aggregati all-SSD su sistemi FAS.

Versione di ONTAP supportata

ONTAP 9.2 o versione successiva

Requisiti di rete del cluster

- Il cluster ONTAP avvia una connessione HTTPS tramite la porta 443 ad Amazon S3.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

  Sebbene AWS Direct Connect offra performance migliori e costi di trasferimento dei dati inferiori, non è necessario tra il cluster ONTAP e S3. Poiché le performance sono significativamente migliori quando si utilizza AWS Direct Connect, si consiglia di farlo.

- È necessaria una connessione in entrata dal connettore, che può risiedere in un VPC AWS o in sede.

  Non è richiesta una connessione tra il cluster e il servizio Cloud Tiering.

- Su ogni nodo ONTAP che ospita volumi a più livelli è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti.

  Gli IPspaces consentono la segregazione del traffico di rete, consentendo la separazione del traffico client per la privacy e la sicurezza. "Scopri di più su IPspaces".

  Quando si imposta il tiering dei dati, Cloud Tiering richiede l'utilizzo di IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Volumi e aggregati supportati

Il numero totale di volumi che il cloud tiering può tierare potrebbe essere inferiore al numero di volumi sul sistema ONTAP. Questo perché i volumi non possono essere suddivisi in livelli da alcuni aggregati. Ad esempio, non è possibile eseguire il tiering dei dati dai volumi SnapLock o dalle configurazioni MetroCluster. Consultare la documentazione ONTAP per "Funzionalità o funzionalità non supportate da FabricPool".

Cloud Tiering supporta FlexGroup Volumes, a partire da ONTAP 9.5. Il programma di installazione funziona come qualsiasi altro volume.

Creazione o commutazione di connettori

Per eseguire il Tier dei dati nel cloud è necessario un connettore. Quando si esegue il tiering dei dati in AWS S3, è possibile utilizzare un connettore che si trova in un VPC AWS o on-premise. Sarà necessario creare un nuovo connettore o assicurarsi che il connettore attualmente selezionato si trovi in AWS o on-premise.

- "Scopri di più sui connettori"
- "Creazione di un connettore in AWS"
- "Requisiti host del connettore"
- "Installazione del connettore su un host Linux esistente"
- "Passaggio da un connettore all'altro"

Preparazione del collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste. Un connettore può essere installato on-premise o in AWS.

Fasi

1. Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:
   - Una connessione Internet in uscita al servizio Cloud Tiering sulla porta 443 (HTTPS)
   - Una connessione HTTPS sulla porta 443 a S3
   - Una connessione HTTPS tramite la porta 443 ai cluster ONTAP
2. Se necessario, abilitare un endpoint VPC su S3.

   Si consiglia di utilizzare un endpoint VPC su S3 se si dispone di una connessione diretta o VPN dal cluster ONTAP al VPC e si desidera che la comunicazione tra il connettore e S3 rimanga nella rete interna AWS.

Preparazione di Amazon S3

Quando si imposta il tiering dei dati su un nuovo cluster, viene richiesto di creare un bucket S3 o di selezionare un bucket S3 esistente nell'account AWS in cui è configurato il connettore.

L'account AWS deve disporre di autorizzazioni e di una chiave di accesso che è possibile inserire in Cloud Tiering. Il cluster ONTAP utilizza la chiave di accesso per raggruppare i dati in S3 e in S3.

Fasi

1. Fornire le seguenti autorizzazioni all'utente IAM:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

   "Documentazione AWS: Creazione di un ruolo per delegare le autorizzazioni a un utente IAM"

2. Creare o individuare una chiave di accesso.

   Cloud Tiering passa la chiave di accesso al cluster ONTAP. Le credenziali non vengono memorizzate nel servizio Cloud Tiering.

   "Documentazione AWS: Gestione delle chiavi di accesso per gli utenti IAM"

Tiering dei dati inattivi dal primo cluster ad Amazon S3

Dopo aver preparato l'ambiente AWS, iniziare a tiering dei dati inattivi dal primo cluster.

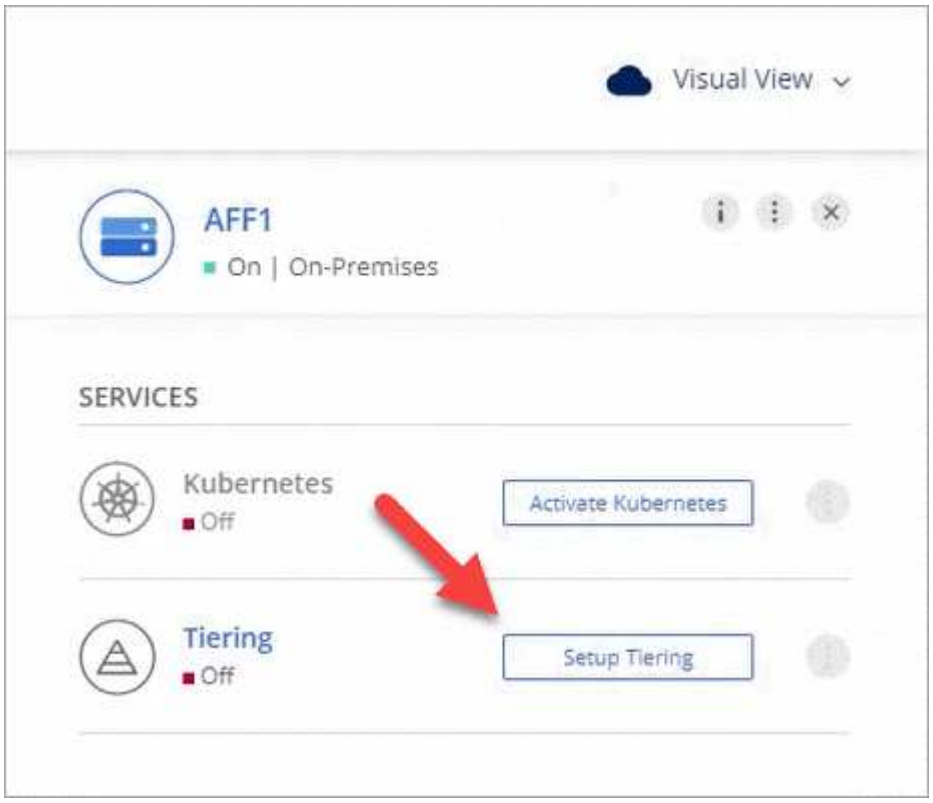
Di cosa hai bisogno

- "Un ambiente di lavoro on-premise".

- Chiave di accesso AWS per un utente IAM che dispone delle autorizzazioni S3 richieste.

Fasi

1. Selezionare un cluster on-premise.
2. Fare clic su **Setup Tiering**.



Ora ti trovi nella dashboard di Tiering.

3. Fare clic su **Set up Tiering** (Configura tiering) accanto al cluster.
4. Completare la procedura riportata nella pagina **Tiering Setup**:

   a. **S3 bucket**: Aggiungi un nuovo bucket S3 o seleziona un bucket S3 esistente che inizia con il prefisso *fabric-pool* e fai clic su **continua**.

      Il prefisso *fabric-pool* è necessario perché il criterio IAM per il connettore consente all'istanza di eseguire azioni S3 sui bucket denominati con quel prefisso esatto.

   Ad esempio, è possibile chiamare il bucket fabric-pool-AFF1 S3, dove AFF1 è il nome del cluster.

   a. **Storage Class** (Classe di storage): Selezionare la classe di storage S3 a cui si desidera trasferire i dati dopo 30 giorni e fare clic su **Continue** (continua).

      Se si sceglie Standard, i dati rimangono in quella classe di storage.

   b. **Credenziali**: Inserire l'ID della chiave di accesso e la chiave segreta per un utente IAM che dispone delle autorizzazioni S3 richieste.

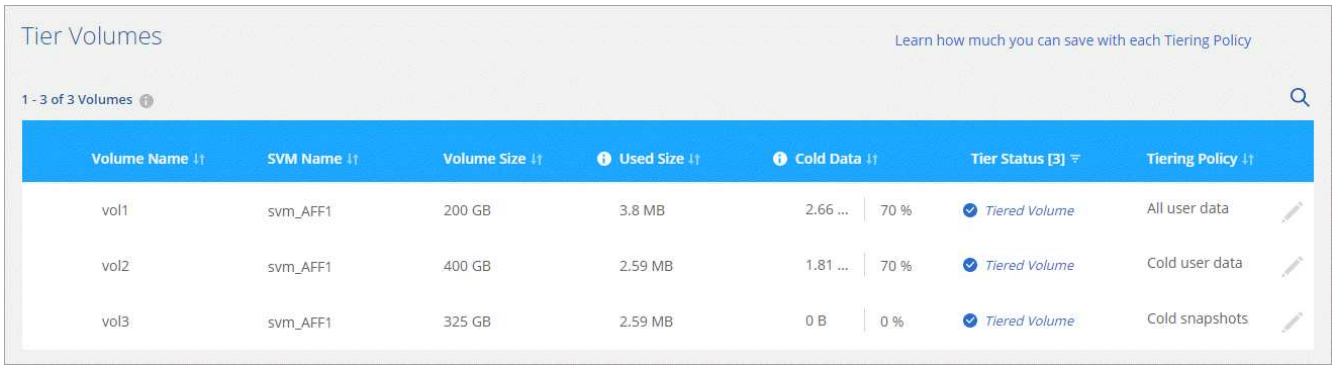
      L'utente IAM deve trovarsi nello stesso account AWS del bucket selezionato o creato nella pagina **S3 bucket**.

c. **Rete cluster**: Selezionare l'IPSpace che ONTAP deve utilizzare per connettersi allo storage a oggetti e fare clic su **continua**.

   La scelta dell'IPSpace corretto garantisce che il Cloud Tiering possa configurare una connessione da ONTAP allo storage a oggetti del tuo provider di cloud.

5. Fare clic su **Continue** (continua) per selezionare i volumi a cui si desidera assegnare il Tier.
6. Nella pagina **Tier Volumes**, impostare il tiering per ciascun volume. Fare clic su  Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".



Risultato

Il tiering dei dati è stato configurato correttamente dai volumi del cluster allo storage a oggetti S3.

Quali sono le prossime novità?

"Assicurati di iscriverti al servizio Cloud Tiering".

È inoltre possibile aggiungere cluster aggiuntivi o rivedere le informazioni sui dati attivi e inattivi sul cluster. Per ulteriori informazioni, vedere "Gestione del tiering dei dati dai cluster".

Tiering dei dati dai cluster ONTAP on-premise allo storage Azure Blob

Liberare spazio sui cluster ONTAP on-premise eseguendo il tiering dei dati sullo storage Azure Blob. Il tiering dei dati è basato sul servizio Cloud Tiering di NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

 **Preparatevi a eseguire il tiering dei dati sullo storage Azure Blob**

Sono necessari i seguenti elementi:

- Un sistema AFF o FAS con aggregati all-SSD che eseguono ONTAP 9.4 o versione successiva e dispone di una connessione HTTPS allo storage Azure Blob.
- Un connettore installato in Azure VNET.

- Rete per un connettore che abilita una connessione HTTPS in uscita al cluster ONTAP nel data center, allo storage Azure Blob e al servizio di tiering cloud.

2 Impostare il tiering

In Cloud Manager, selezionare un ambiente di lavoro on-premise, fare clic su **Setup Tiering** e seguire le istruzioni per assegnare i dati allo storage Azure Blob.

3 Impostare la licenza

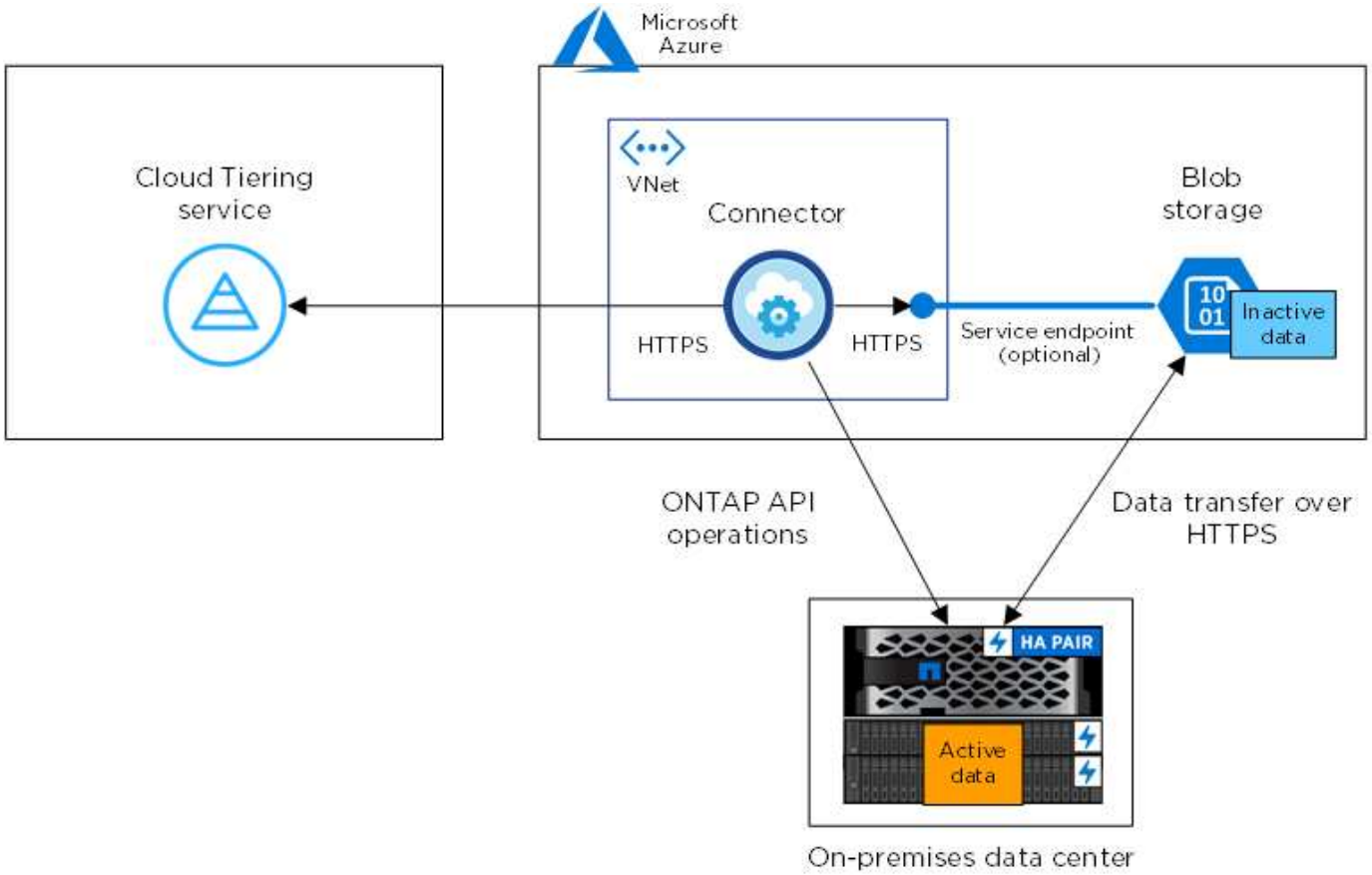
Al termine della prova gratuita, paga il Tier cloud con un abbonamento pay-as-you-go, una licenza di tiering ONTAP o una combinazione di entrambi:

- Per iscriversi a Azure Marketplace, fare clic su **Tiering > Licensing**, fare clic su **Subscribe**, quindi seguire le istruzioni.
- Per aggiungere una licenza di tiering, contattaci se devi acquistarne una, quindi "Aggiungilo al tuo cluster da Cloud Tiering".

Requisiti

Verificare il supporto per il cluster ONTAP, configurare la rete e preparare lo storage a oggetti.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



La comunicazione tra il connettore e lo storage BLOB è solo per la configurazione dello storage a oggetti.

Preparazione dei cluster ONTAP

I cluster ONTAP devono soddisfare i seguenti requisiti quando si esegue il tiering dei dati sullo storage Azure Blob.

Piattaforme ONTAP supportate

Cloud Tiering supporta sistemi AFF e aggregati all-SSD su sistemi FAS.

Versione di ONTAP supportata

ONTAP 9.4 o versione successiva

Requisiti di rete del cluster

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 allo storage Azure Blob.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

  Sebbene ExpressRoute offra performance migliori e costi di trasferimento dei dati inferiori, non è necessario tra il cluster ONTAP e lo storage Azure Blob. Poiché le prestazioni sono notevolmente migliori quando si utilizza ExpressRoute, si consiglia di farlo.

- È necessaria una connessione in entrata da NetApp Service Connector, che risiede in Azure VNET.

  Non è richiesta una connessione tra il cluster e il servizio Cloud Tiering.

- Su ogni nodo ONTAP che ospita volumi a più livelli è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti.

  Gli IPspaces consentono la segregazione del traffico di rete, consentendo la separazione del traffico client per la privacy e la sicurezza. "Scopri di più su IPspaces".

  Quando si imposta il tiering dei dati, Cloud Tiering richiede l'utilizzo di IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Volumi e aggregati supportati

Il numero totale di volumi che il cloud tiering può tierare potrebbe essere inferiore al numero di volumi sul sistema ONTAP. Questo perché i volumi non possono essere suddivisi in livelli da alcuni aggregati. Ad esempio, non è possibile eseguire il tiering dei dati dai volumi SnapLock o dalle configurazioni MetroCluster. Consultare la documentazione ONTAP per "Funzionalità o funzionalità non supportate da FabricPool".

Cloud Tiering supporta FlexGroup Volumes, a partire da ONTAP 9.5. Il programma di installazione funziona come qualsiasi altro volume.

Creazione o commutazione di connettori

Per eseguire il Tier dei dati nel cloud è necessario un connettore. Quando si esegue il tiering dei dati nello storage Azure Blob, un connettore deve essere disponibile in Azure VNET. Sarà necessario creare un nuovo connettore o assicurarsi che il connettore attualmente selezionato risieda in Azure.

- "Scopri di più sui connettori"
- "Creazione di un connettore in Azure"
- "Passaggio da un connettore all'altro"

Preparazione del collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste.

Fasi

1. Assicurarsi che il VNET su cui è installato il connettore abiliti le seguenti connessioni:
   - Una connessione Internet in uscita al servizio Cloud Tiering sulla porta 443 (HTTPS)
   - Una connessione HTTPS tramite la porta 443 allo storage Azure Blob
   - Una connessione HTTPS tramite la porta 443 ai cluster ONTAP
2. Se necessario, abilitare un endpoint del servizio VNET allo storage Azure.

   Si consiglia di utilizzare un endpoint del servizio VNET per lo storage Azure se si dispone di una connessione ExpressRoute o VPN dal cluster ONTAP a VNET e si desidera che la comunicazione tra il connettore e lo storage Blob rimanga nella rete privata virtuale.

Tiering dei dati inattivi dal primo cluster allo storage Azure Blob

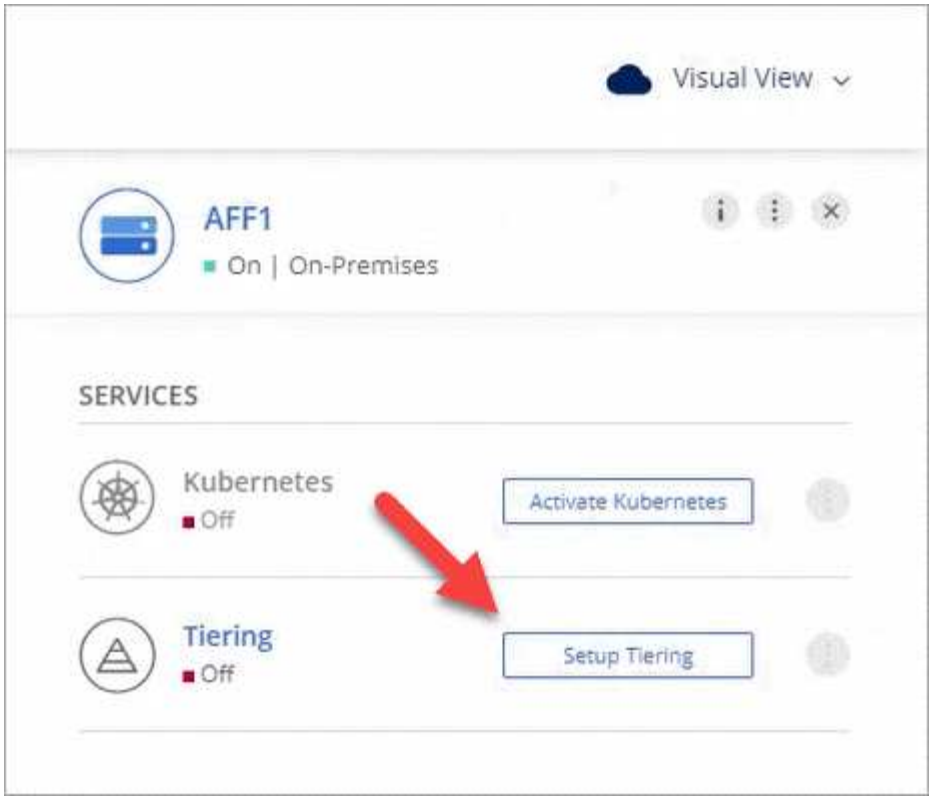
Dopo aver preparato l'ambiente Azure, inizia a tiering dei dati inattivi dal primo cluster.

Di cosa hai bisogno

"Un ambiente di lavoro on-premise".

Fasi

1. Selezionare un cluster on-premise.
2. Fare clic su **Setup Tiering**.



Ora ti trovi nella dashboard di Tiering.

3. Fare clic su **Set up Tiering** (Configura tiering) accanto al cluster.
4. Completare la procedura riportata nella pagina **Tiering Setup**:
   a. **Resource Group**: Selezionare un gruppo di risorse in cui viene gestito un container esistente o in cui si desidera creare un nuovo container per i dati a più livelli.
   b. **Azure Container**: Aggiungere un nuovo container Blob a un account storage o selezionare un container esistente e fare clic su **Continue** (continua).

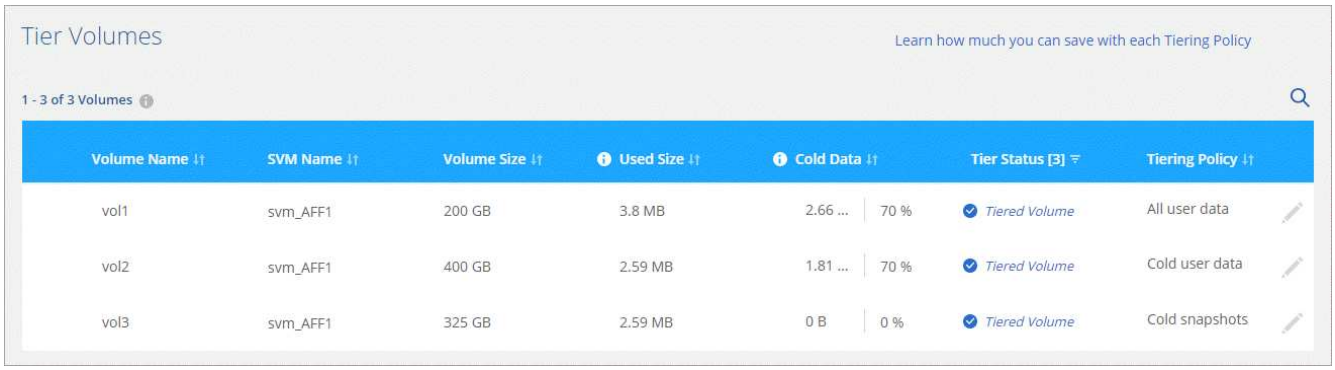
      L'account di storage e i contenitori visualizzati in questa fase appartengono al gruppo di risorse selezionato nella fase precedente.

   c. **Access Tier**: Selezionare il livello di accesso che si desidera utilizzare per i dati a più livelli e fare clic su **Continue** (continua).
   d. **Rete cluster**: Selezionare l'IPSpace che ONTAP deve utilizzare per connettersi allo storage a oggetti e fare clic su **continua**.

      La scelta dell'IPSpace corretto garantisce che il Cloud Tiering possa configurare una connessione da ONTAP allo storage a oggetti del tuo provider di cloud.

5. Fare clic su **Continue** (continua) per selezionare i volumi a cui si desidera assegnare il Tier.
6. Nella pagina **Tier Volumes**, impostare il tiering per ciascun volume. Fare clic su  Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".



Risultato

Hai configurato correttamente il tiering dei dati dai volumi del cluster allo storage a oggetti Azure Blob.

Quali sono le prossime novità?

"Assicurati di iscriverti al servizio Cloud Tiering".

È inoltre possibile aggiungere cluster aggiuntivi o rivedere le informazioni sui dati attivi e inattivi sul cluster. Per ulteriori informazioni, vedere "Gestione del tiering dei dati dai cluster".

Tiering dei dati dai cluster ONTAP on-premise allo storage cloud Google

Liberare spazio sui cluster ONTAP on-premise mediante il tiering dei dati su Google Cloud Storage. Il tiering dei dati è basato sul servizio Cloud Tiering di NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Preparatevi a eseguire il tiering dei dati su Google Cloud Storage

Sono necessari i seguenti elementi:

- Un sistema AFF o FAS con aggregati all-SSD che esegue ONTAP 9.6 o versione successiva e dispone di una connessione HTTPS allo storage cloud di Google.
- Account di servizio con il ruolo Storage Admin predefinito e le chiavi di accesso allo storage.
- Un connettore installato in un VPC della piattaforma Google Cloud.
- Rete per il connettore che abilita una connessione HTTPS in uscita al cluster ONTAP nel data center, allo storage cloud Google e al servizio di tiering cloud.

2 Impostare il tiering

In Cloud Manager, selezionare un ambiente di lavoro on-premise, fare clic su **Setup Tiering** e seguire le istruzioni per assegnare i dati a Google Cloud Storage.

Impostare la licenza

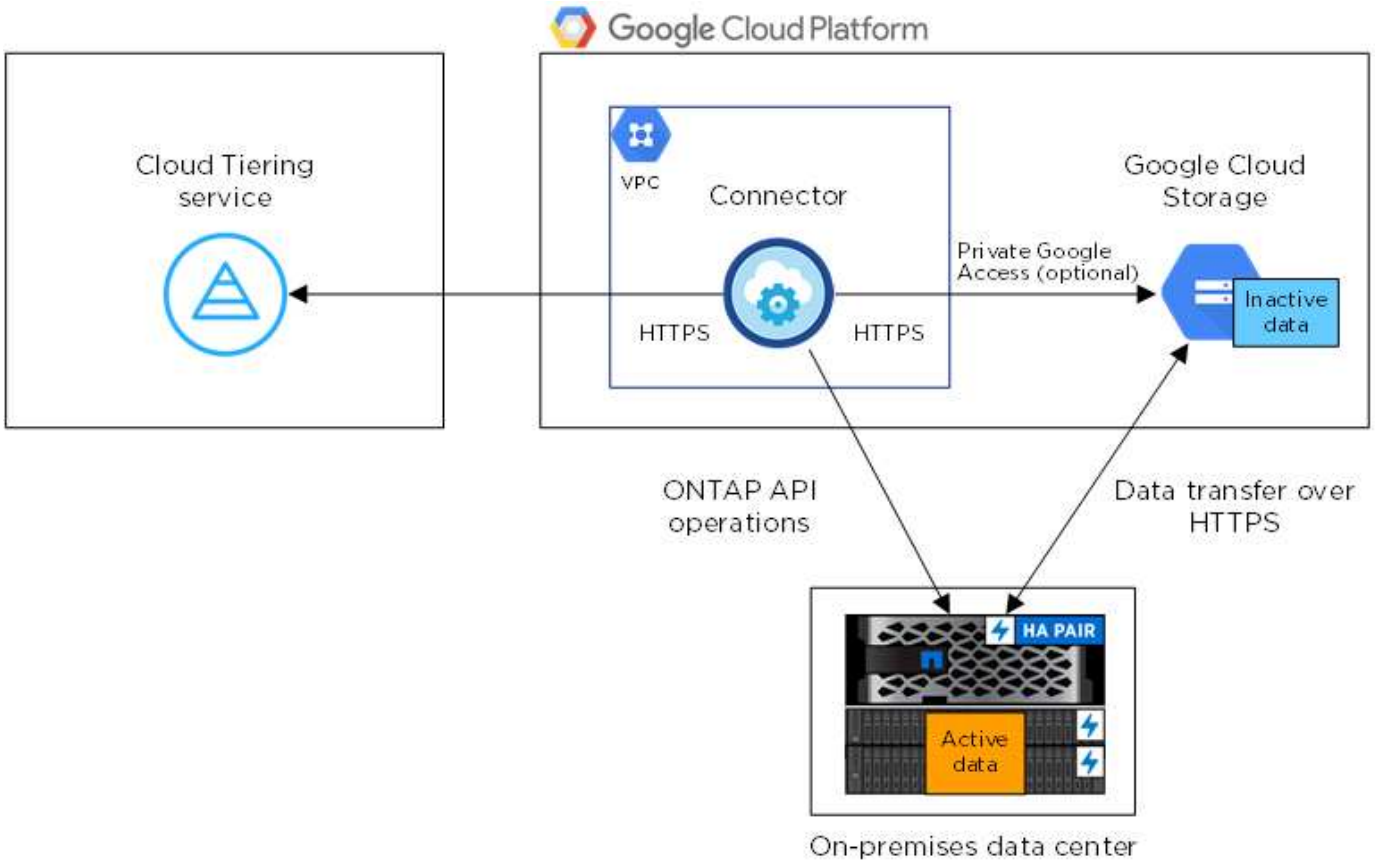
Al termine della prova gratuita, paga il Tier cloud con un abbonamento pay-as-you-go, una licenza di tiering ONTAP o una combinazione di entrambi:

- Per iscriversi a GCP Marketplace, fare clic su **Tiering > Licensing**, fare clic su **Subscribe**, quindi seguire le istruzioni.
- Per aggiungere una licenza di tiering, contattaci se devi acquistarne una, quindi "Aggiungilo al tuo cluster da Cloud Tiering".

Requisiti

Verificare il supporto per il cluster ONTAP, configurare la rete e preparare lo storage a oggetti.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



La comunicazione tra il connettore e Google Cloud Storage è solo per la configurazione dello storage a oggetti.

Preparazione dei cluster ONTAP

I cluster ONTAP devono soddisfare i seguenti requisiti quando si esegue il tiering dei dati su Google Cloud Storage.

Piattaforme ONTAP supportate

Cloud Tiering supporta sistemi AFF e aggregati all-SSD su sistemi FAS.

Versioni di ONTAP supportate

ONTAP 9.6 o versione successiva

Requisiti di rete del cluster

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 allo storage cloud Google.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

  Sebbene un'interconnessione cloud di Google offra performance migliori e costi di trasferimento dei dati inferiori, non è necessaria tra il cluster ONTAP e lo storage cloud di Google. Poiché le performance sono significativamente migliori quando si utilizza Google Cloud Interconnect, si consiglia di farlo.

- È necessaria una connessione in entrata da NetApp Service Connector, che risiede in un VPC della piattaforma Google Cloud.

  Non è richiesta una connessione tra il cluster e il servizio Cloud Tiering.

- Su ogni nodo ONTAP che ospita volumi a più livelli è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti.

  Gli IPspaces consentono la segregazione del traffico di rete, consentendo la separazione del traffico client per la privacy e la sicurezza. "Scopri di più su IPspaces".

  Quando si imposta il tiering dei dati, Cloud Tiering richiede l'utilizzo di IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Volumi e aggregati supportati

Il numero totale di volumi che il cloud tiering può tierare potrebbe essere inferiore al numero di volumi sul sistema ONTAP. Questo perché i volumi non possono essere suddivisi in livelli da alcuni aggregati. Ad esempio, non è possibile eseguire il tiering dei dati dai volumi SnapLock o dalle configurazioni MetroCluster. Consultare la documentazione ONTAP per "Funzionalità o funzionalità non supportate da FabricPool".

Il tiering cloud supporta i volumi FlexGroup. Il programma di installazione funziona come qualsiasi altro volume.

Creazione o commutazione di connettori

Per eseguire il Tier dei dati nel cloud è necessario un connettore. Quando si esegue il tiering dei dati su Google Cloud Storage, un connettore deve essere disponibile in un VPC Google Cloud Platform. Sarà necessario creare un nuovo connettore o assicurarsi che il connettore attualmente selezionato risieda in GCP.

- "Scopri di più sui connettori"
- "Creazione di un connettore in GCP"
- "Passaggio da un connettore all'altro"

Preparazione del collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste.

Fasi

1. Assicurarsi che il VPC su cui è installato il connettore consenta i seguenti collegamenti:
   - Una connessione Internet in uscita al servizio Cloud Tiering sulla porta 443 (HTTPS)
   - Una connessione HTTPS tramite la porta 443 a Google Cloud Storage
   - Una connessione HTTPS tramite la porta 443 ai cluster ONTAP
2. Facoltativo: Attivare l'accesso privato a Google nella subnet in cui si intende implementare Service Connector.

   "Accesso privato a Google" È consigliabile se si dispone di una connessione diretta dal cluster ONTAP al VPC e si desidera che la comunicazione tra il connettore e lo storage cloud di Google rimanga nella rete privata virtuale. Si noti che Private Google Access funziona con istanze di macchine virtuali che hanno solo indirizzi IP interni (privati) (non indirizzi IP esterni).

Preparazione di Google Cloud Storage per il tiering dei dati

Quando si imposta il tiering, è necessario fornire le chiavi di accesso allo storage per un account di servizio che dispone delle autorizzazioni Storage Admin. Un account di servizio consente al Cloud Tiering di autenticare e accedere ai bucket di Cloud Storage utilizzati per il tiering dei dati. Le chiavi sono necessarie in modo che Google Cloud Storage sappia chi sta effettuando la richiesta.

Fasi

1. "Creare un account di servizio con il ruolo di amministratore dello storage predefinito".
2. Passare a. "Impostazioni storage GCP" e creare le chiavi di accesso per l'account di servizio:
   a. Selezionare un progetto e fare clic su **interoperabilità**. Se non è già stato fatto, fare clic su **Enable Interoperability access** (attiva accesso all'interoperabilità).
   b. In **chiavi di accesso per gli account di servizio**, fare clic su **Crea una chiave per un account di servizio**, selezionare l'account di servizio appena creato e fare clic su **Crea chiave**.

      È necessario "Immettere le chiavi in Cloud Tiering" successivamente, quando si imposta il tiering.

Tiering dei dati inattivi dal primo cluster a Google Cloud Storage

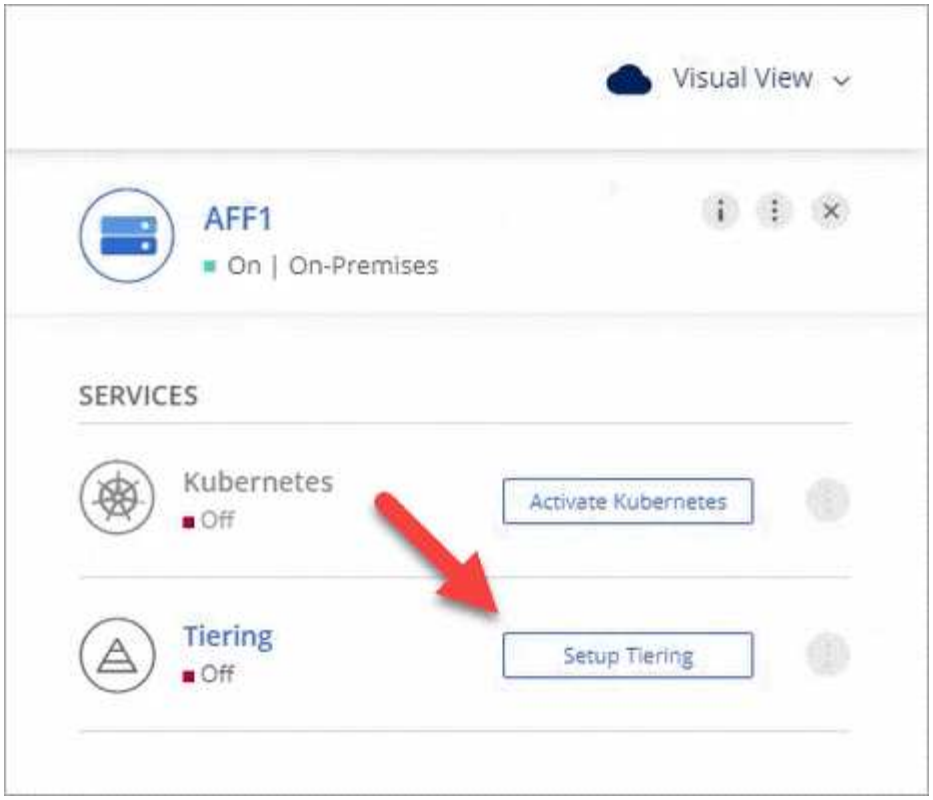
Dopo aver preparato l'ambiente Google Cloud, inizia a tiering dei dati inattivi dal primo cluster.

Di cosa hai bisogno

- "Un ambiente di lavoro on-premise".
- Chiavi di accesso allo storage per un account di servizio che ha il ruolo di amministratore dello storage.

Fasi

1. Selezionare un cluster on-premise.
2. Fare clic su **Setup Tiering**.

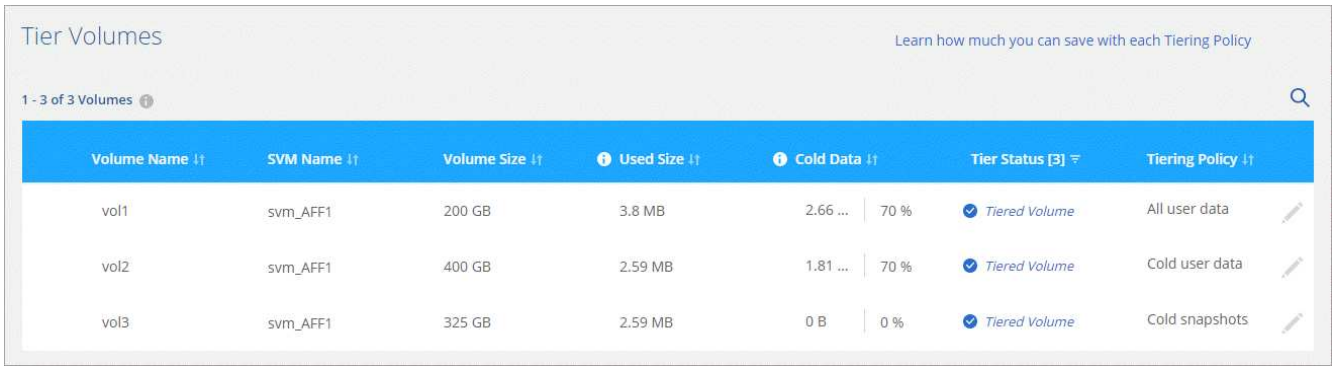


Ora ti trovi nella dashboard di Tiering.

3. Fare clic su **Set up Tiering** (Configura tiering) accanto al cluster.
4. Completare la procedura riportata nella pagina **Tiering Setup**:
   a. **Bucket**: Aggiungi un nuovo bucket di storage Google Cloud o seleziona un bucket esistente e fai clic su **continua**.
   b. **Storage Class** (Classe di storage): Selezionare la classe di storage che si desidera utilizzare per i dati a più livelli e fare clic su **Continue** (continua).
   c. **Credenziali**: Inserire la chiave di accesso allo storage e la chiave segreta per un account di servizio che ha il ruolo di amministratore dello storage.
   d. **Rete cluster**: Selezionare l'IPSpace che ONTAP deve utilizzare per connettersi allo storage a oggetti e fare clic su **continua**.

      La scelta dell'IPSpace corretto garantisce che il Cloud Tiering possa configurare una connessione da ONTAP allo storage a oggetti del tuo provider di cloud.
5. Fare clic su **Continue** (continua) per selezionare i volumi a cui si desidera assegnare il Tier.
6. Nella pagina **Tier Volumes**, impostare il tiering per ciascun volume. Fare clic su Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".



Risultato

Hai configurato correttamente il tiering dei dati dai volumi del cluster allo storage a oggetti Google Cloud.

Quali sono le prossime novità?

"Assicurati di iscriverti al servizio Cloud Tiering".

È inoltre possibile aggiungere cluster aggiuntivi o rivedere le informazioni sui dati attivi e inattivi sul cluster. Per ulteriori informazioni, vedere "Gestione del tiering dei dati dai cluster".

Tiering dei dati dai cluster ONTAP on-premise a StorageGRID

Liberare spazio sui cluster ONTAP on-premise eseguendo il tiering dei dati su StorageGRID. Il tiering dei dati è basato sul servizio Cloud Tiering di NetApp.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1 Preparatevi a eseguire il tiering dei dati su StorageGRID

Sono necessari i seguenti elementi:

- Un sistema AFF o FAS con aggregati all-SSD che eseguono ONTAP 9.4 o versione successiva e una connessione a StorageGRID tramite una porta specificata dall'utente.
- StorageGRID 10.3 o versione successiva con chiavi di accesso AWS che dispongono delle autorizzazioni S3.
- Un connettore installato in sede.
- Rete per il connettore che abilita una connessione HTTPS in uscita al cluster ONTAP, a StorageGRID e al servizio di tiering cloud.

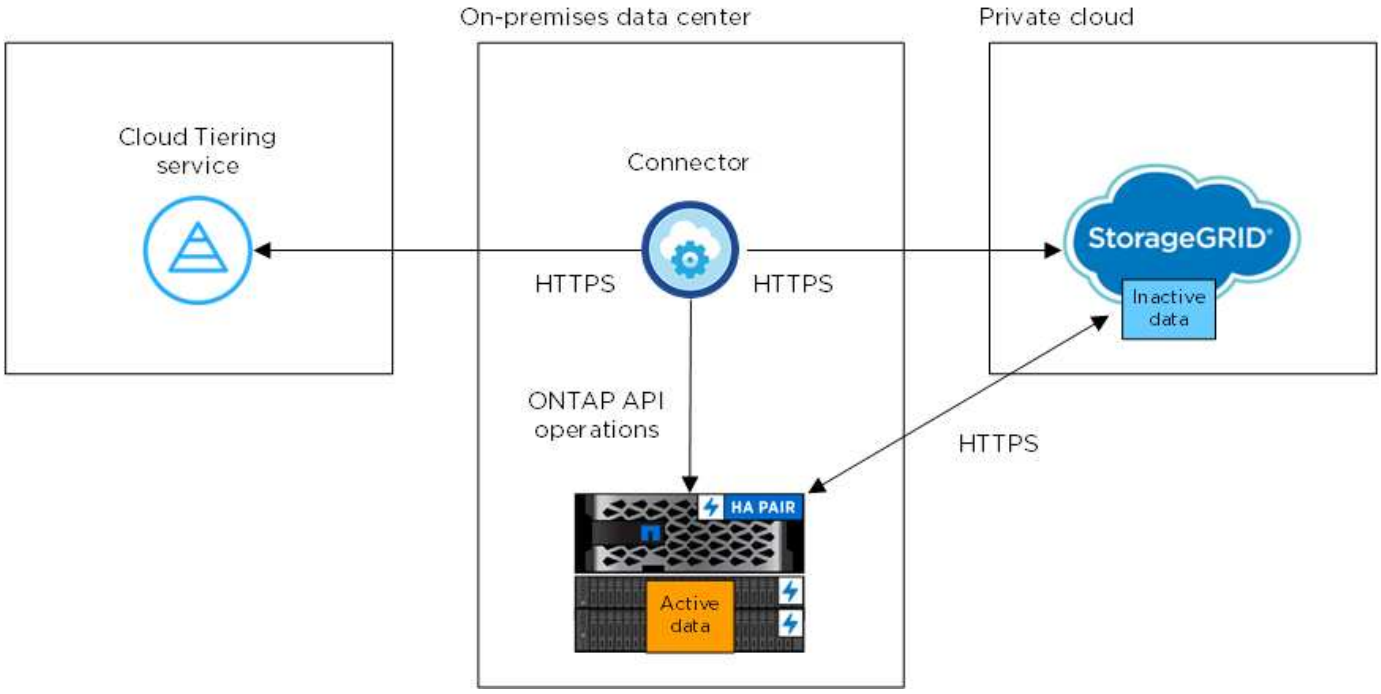
2 Impostare il tiering

Selezionare un ambiente di lavoro on-premise, fare clic su **Setup Tiering** e seguire le istruzioni per assegnare i dati a StorageGRID.

Requisiti

Verificare il supporto per il cluster ONTAP, configurare la rete e preparare lo storage a oggetti.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



La comunicazione tra il connettore e StorageGRID è solo per la configurazione dello storage a oggetti.

Preparazione dei cluster ONTAP

I cluster ONTAP devono soddisfare i seguenti requisiti quando si esegue il tiering dei dati in StorageGRID.

Piattaforme ONTAP supportate

Cloud Tiering supporta sistemi AFF e aggregati all-SSD su sistemi FAS.

Versione di ONTAP supportata

ONTAP 9.4 o versione successiva

Licensing

Non è richiesta una licenza FabricPool sul cluster ONTAP quando si esegue il tiering dei dati su StorageGRID.

Requisiti di rete del cluster

- Il cluster ONTAP avvia una connessione HTTPS a StorageGRID tramite una porta specificata dall'utente (la porta è configurabile durante la configurazione del tiering).

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- È necessaria una connessione in entrata dal connettore, che deve risiedere in sede.

  Non è richiesta una connessione tra il cluster e il servizio Cloud Tiering.

- Su ogni nodo ONTAP che ospita volumi a più livelli è richiesta una LIF intercluster. La LIF deve essere associata a *IPSpace* che ONTAP deve utilizzare per connettersi allo storage a oggetti.

  Gli IPspaces consentono la segregazione del traffico di rete, consentendo la separazione del traffico client per la privacy e la sicurezza. "Scopri di più su IPspaces".

  Quando si imposta il tiering dei dati, Cloud Tiering richiede l'utilizzo di IPSpace. È necessario scegliere l'IPSpace a cui ciascun LIF è associato. Potrebbe trattarsi dell'IPSpace "predefinito" o di un IPSpace personalizzato creato.

Volumi e aggregati supportati

Il numero totale di volumi che il cloud tiering può tierare potrebbe essere inferiore al numero di volumi sul sistema ONTAP. Questo perché i volumi non possono essere suddivisi in livelli da alcuni aggregati. Ad esempio, non è possibile eseguire il tiering dei dati dai volumi SnapLock o dalle configurazioni MetroCluster. Consultare la documentazione ONTAP per "Funzionalità o funzionalità non supportate da FabricPool".

Cloud Tiering supporta FlexGroup Volumes, a partire da ONTAP 9.5. Il programma di installazione funziona come qualsiasi altro volume.

Preparazione di StorageGRID

StorageGRID deve soddisfare i seguenti requisiti.

Versioni di StorageGRID supportate

Sono supportati StorageGRID 10.3 e versioni successive.

Credenziali S3

Quando si imposta il tiering su StorageGRID, è necessario fornire il tiering cloud con una chiave di accesso S3 e una chiave segreta. Cloud Tiering utilizza le chiavi per accedere ai bucket.

Queste chiavi di accesso devono essere associate a un utente che dispone delle seguenti autorizzazioni:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Versione degli oggetti

Non è necessario attivare la versione degli oggetti StorageGRID nel bucket dell'archivio di oggetti.

Creazione o commutazione di connettori

Per eseguire il Tier dei dati nel cloud è necessario un connettore. Quando si esegue il tiering dei dati su StorageGRID, è necessario che un connettore sia disponibile on-premise. È necessario installare un nuovo connettore o assicurarsi che il connettore attualmente selezionato risieda on-premise.

- "Scopri di più sui connettori"

- "Requisiti host del connettore"
- "Installazione del connettore su un host Linux esistente"
- "Passaggio da un connettore all'altro"

Preparazione del collegamento in rete per il connettore

Assicurarsi che il connettore disponga delle connessioni di rete richieste.

Fasi

1. Assicurarsi che la rete in cui è installato il connettore abiliti le seguenti connessioni:
   - Una connessione Internet in uscita al servizio Cloud Tiering sulla porta 443 (HTTPS)
   - Una connessione HTTPS tramite la porta 443 a StorageGRID
   - Una connessione HTTPS tramite la porta 443 ai cluster ONTAP

Tiering dei dati inattivi dal primo cluster a StorageGRID

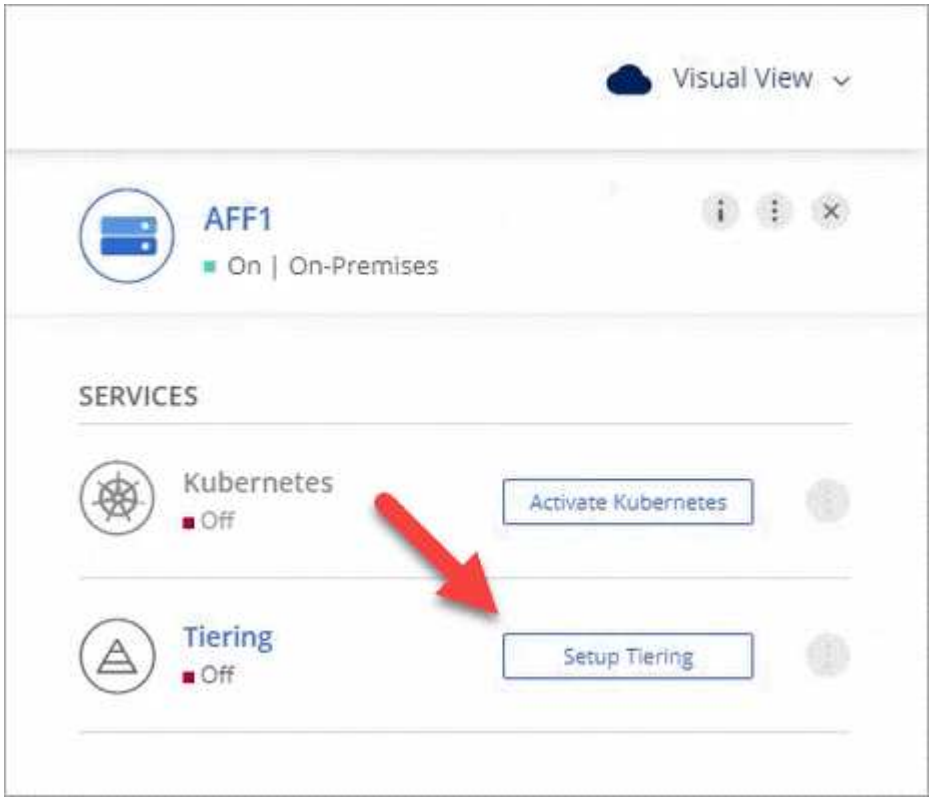
Dopo aver preparato l'ambiente, iniziare a tiering dei dati inattivi dal primo cluster.

Di cosa hai bisogno

- "Un ambiente di lavoro on-premise".
- Chiave di accesso AWS con le autorizzazioni S3 richieste.

Fasi

1. Selezionare un cluster on-premise.
2. Fare clic su **Setup Tiering**.

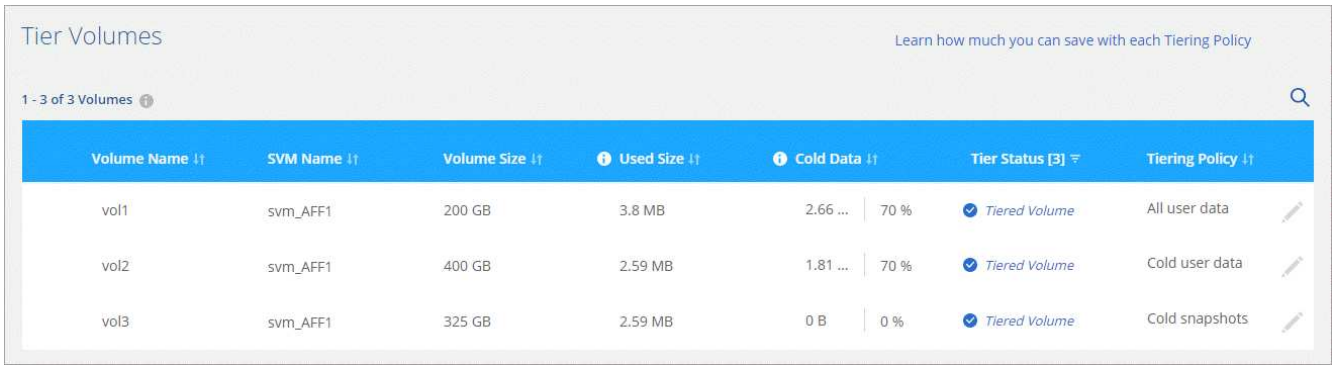


Ora ti trovi nella dashboard di Tiering.

3. Fare clic su **Set up Tiering** (Configura tiering) accanto al cluster.
4. Completare la procedura riportata nella pagina **Tiering Setup**:
   a. **Scegli il tuo provider**: Seleziona StorageGRID.
   b. **Server**: Immettere l'FQDN del server StorageGRID, la porta che ONTAP deve utilizzare per la comunicazione HTTPS con StorageGRID e immettere la chiave di accesso e la chiave segreta per un account AWS che dispone delle autorizzazioni S3 richieste.
   c. **Bucket**: Aggiungi un nuovo bucket o seleziona un bucket esistente per i dati su più livelli.
   d. **Rete cluster**: Selezionare l'IPSpace che ONTAP deve utilizzare per connettersi allo storage a oggetti e fare clic su **continua**.

      La scelta dell'IPSpace corretto garantisce che il Cloud Tiering possa configurare una connessione da ONTAP allo storage a oggetti del tuo provider di cloud.
5. Fare clic su **Continue** (continua) per selezionare i volumi a cui si desidera assegnare il Tier.
6. Nella pagina **Tier Volumes**, impostare il tiering per ciascun volume. Fare clic su  Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".



Risultato

Il tiering dei dati è stato configurato correttamente dai volumi del cluster a StorageGRID.

Quali sono le prossime novità?

È possibile aggiungere cluster aggiuntivi o rivedere le informazioni sui dati attivi e inattivi sul cluster. Per ulteriori informazioni, vedere "Gestione del tiering dei dati dai cluster".

Impostare le licenze per il Cloud Tiering

Paga il tiering cloud con un abbonamento pay-as-you-go, una licenza di tiering ONTAP chiamata *FabricPool* o una combinazione di entrambi. Se desideri pagare a consumo, devi iscriverti al marketplace per il cloud provider a cui vuoi mettere a livello i dati cold. Non c'è bisogno di iscriversi da ogni mercato.

Alcune note prima di leggere ulteriori informazioni:

- Se nel cluster è già installata una licenza FabricPool, non è necessario eseguire altre operazioni.

- Se hai già sottoscritto l'abbonamento a Cloud Manager nel marketplace del tuo cloud provider, sarai automaticamente iscritto anche a Cloud Tiering. Verrà visualizzato un abbonamento attivo nella scheda Cloud Tiering **Licensing**. Non dovrai più iscriverti.
- Non sono previsti costi per il tiering dei dati su StorageGRID. Non è richiesta alcuna licenza BYOL o registrazione PAYGO.

"Scopri di più sul funzionamento delle licenze per il Cloud Tiering".

Iscrizione a AWS Marketplace

Iscriviti al Cloud Tiering dal marketplace AWS per impostare un abbonamento pay-as-you-go per il tiering dei dati dai cluster ONTAP ad AWS S3.

Fasi

1. In Cloud Manager, fare clic su **Tiering > Licensing**.
2. Fare clic su **Subscribe** sotto AWS Marketplace, quindi fare clic su **Continue** (continua).
3. Iscriviti a AWS Marketplace, quindi accedi nuovamente a Cloud Central per completare la registrazione.

   Il seguente video mostra il processo:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws_tiering.mp4 *(video)*

Iscrizione a Azure Marketplace

Iscriviti a Cloud Tiering dal marketplace Azure per impostare un abbonamento pay-as-you-go per il tiering dei dati dai cluster ONTAP allo storage Blob Azure.

Fasi

1. In Cloud Manager, fare clic su **Tiering > Licensing**.
2. Fare clic su **Subscribe** sotto Azure Marketplace, quindi fare clic su **Continue**.
3. Iscriviti a Azure Marketplace, quindi accedi nuovamente a Cloud Central per completare la registrazione.

   Il seguente video mostra il processo:

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure_tiering.mp4 *(video)*

Iscrizione al GCP Marketplace

Iscriviti al Cloud Tiering dal GCP Marketplace per impostare un abbonamento pay-as-you-go per il tiering dei dati dai cluster ONTAP allo storage Google Cloud.

Fasi

1. In Cloud Manager, fare clic su **Tiering > Licensing**.
2. Fare clic su **Subscribe** sotto GCP Marketplace, quindi fare clic su **Continue** (continua).
3. Iscriviti al GCP Marketplace, quindi accedi nuovamente a Cloud Central per completare la registrazione.

   il seguente video mostra il processo:

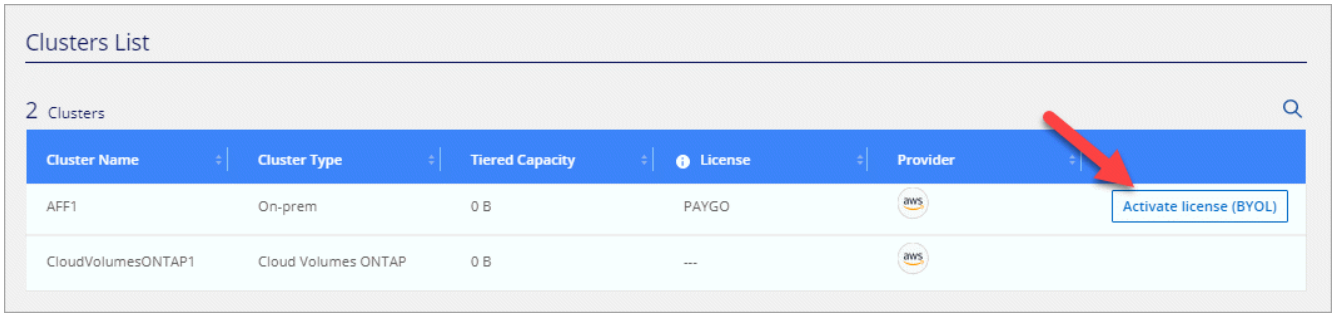
   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_gcp_tiering.mp4 *(video)*

Aggiunta di una licenza di tiering a ONTAP

Porta la tua licenza acquistando una licenza ONTAP FabricPool da NetApp.

Fasi

1. Se non disponi di una licenza FabricPool, contattaci per acquistarne una.
2. In Cloud Manager, fare clic su **Tiering > Licensing**.
3. Nella tabella elenco cluster, fare clic su **Activate License (BYOL)** per un cluster ONTAP on-premise.



4. Inserire il numero di serie della licenza, quindi l'account NetApp Support Site associato al numero di serie.
5. Fare clic su **Activate License** (attiva licenza).

Risultato

Cloud Tiering registra la licenza e la installa sul cluster.

Al termine

Se si acquista ulteriore capacità aggiuntiva in un secondo momento, la licenza sul cluster viene aggiornata automaticamente con la nuova capacità. Non è necessario applicare un nuovo file di licenza NetApp (NLF) al cluster.

Gestione del tiering dei dati dai cluster

Ora che hai impostato il tiering dei dati dai cluster ONTAP, puoi tierare i dati da volumi aggiuntivi, modificare la policy di tiering di un volume e molto altro ancora.

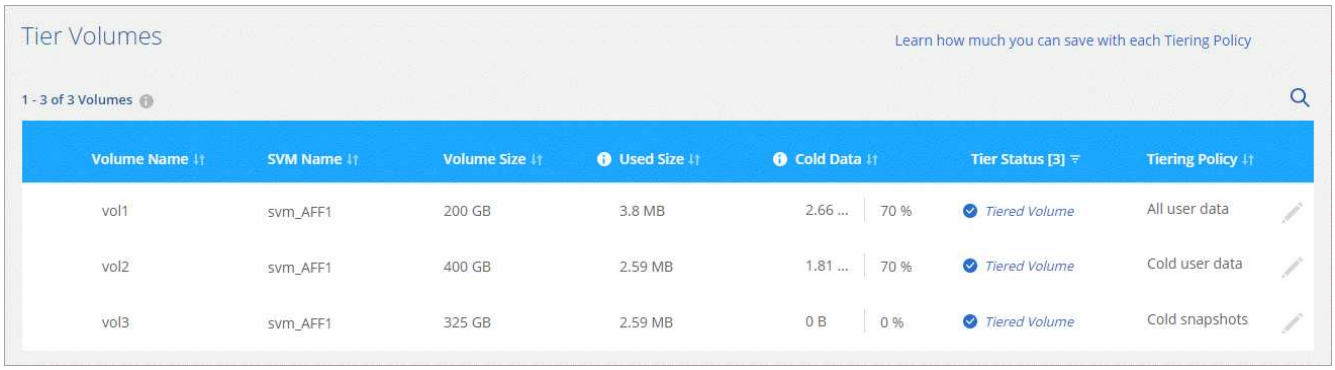
Tiering dei dati da volumi aggiuntivi

Impostare il tiering dei dati per volumi aggiuntivi in qualsiasi momento, ad esempio dopo la creazione di un nuovo volume.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Tiering**.
2. Dal pannello di controllo del cluster, fare clic su **Tier Volumes** per il cluster.
3. Per ciascun volume, fare clic su  Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".



Non è necessario configurare lo storage a oggetti perché è già stato configurato durante la configurazione iniziale del tiering per il cluster. ONTAP eseguirà il tiering dei dati inattivi da questi volumi nello stesso archivio di oggetti.

4. Al termine, fare clic su **Chiudi**.

Modifica della policy di tiering di un volume

La modifica del criterio di tiering per un volume modifica il modo in cui ONTAP esegue il tiering dei dati cold in storage a oggetti. La modifica ha inizio dal momento in cui si modifica la policy, ovvero solo il successivo comportamento di tiering per il volume.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Tiering**.
2. Dal pannello di controllo del cluster, fare clic su **Tier Volumes** per il cluster.
3. Fare clic su Selezionare una policy di tiering, regolare i giorni di raffreddamento e fare clic su **Apply** (Applica).

   "Scopri di più sulle policy di tiering dei volumi".

Gestione delle impostazioni di tiering sugli aggregati

Ogni aggregato dispone di due impostazioni che è possibile regolare: La soglia di fullness del tiering e se è attivata la funzione di reporting dei dati inattivi.

Soglia di fullness tiering

Impostando la soglia su un numero inferiore, si riduce la quantità di dati da memorizzare nel Tier di performance prima di eseguire il tiering. Questo potrebbe essere utile per grandi aggregati che contengono pochi dati attivi.

Impostando la soglia su un numero più elevato, si aumenta la quantità di dati da memorizzare nel Tier di performance prima di eseguire il tiering. Questo potrebbe essere utile per le soluzioni progettate per il Tier solo quando gli aggregati sono quasi alla capacità massima.

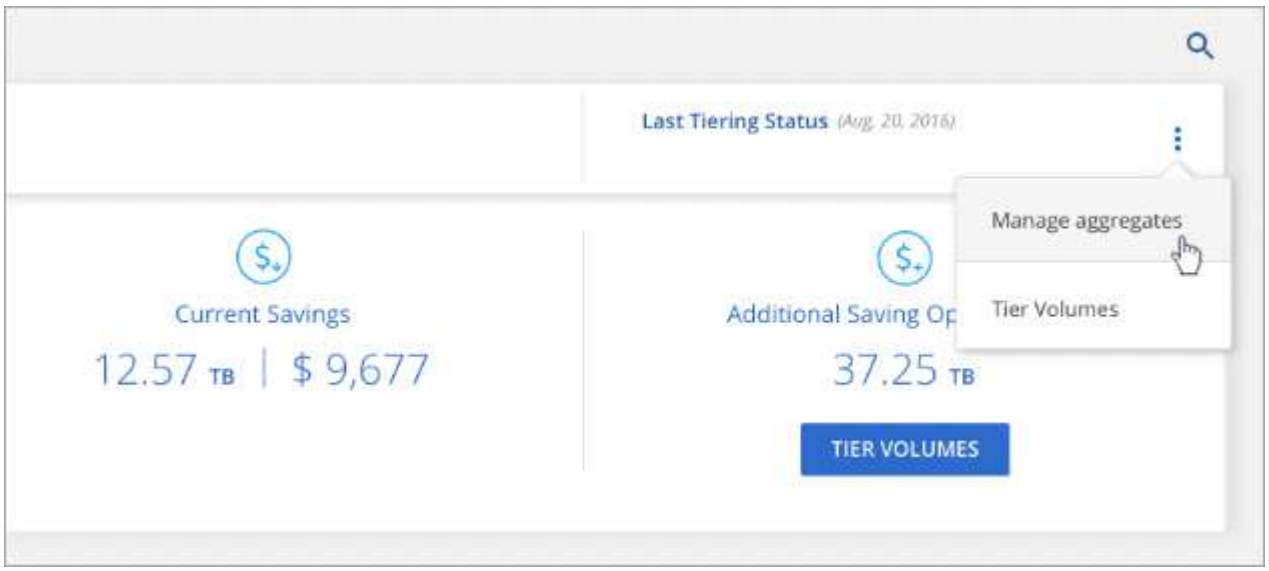
Reporting dei dati inattivi

Il reporting dei dati inattivi (IDR) utilizza un periodo di raffreddamento di 31 giorni per determinare quali dati sono considerati inattivi. La quantità di dati cold a più livelli dipende dalle policy di tiering impostate sui volumi. Questa quantità potrebbe essere diversa dalla quantità di dati cold rilevata dall'IDR utilizzando un periodo di raffreddamento di 31 giorni.

È meglio mantenere l'IDR abilitato perché aiuta a identificare i dati inattivi e le opportunità di risparmio. IDR deve rimanere abilitato se il tiering dei dati è stato attivato su un aggregato.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Tiering**.
2. Dalla pagina **Cloud Tiering**, fare clic sull'icona del menu di un cluster e selezionare **Manage aggregates** (Gestisci aggregati).



3. Nella pagina **Manage aggregates** (Gestisci aggregati), fare clic su per un aggregato nella tabella.
4. Modificare la soglia di fullness e scegliere se attivare o disattivare il reporting dei dati inattivi.

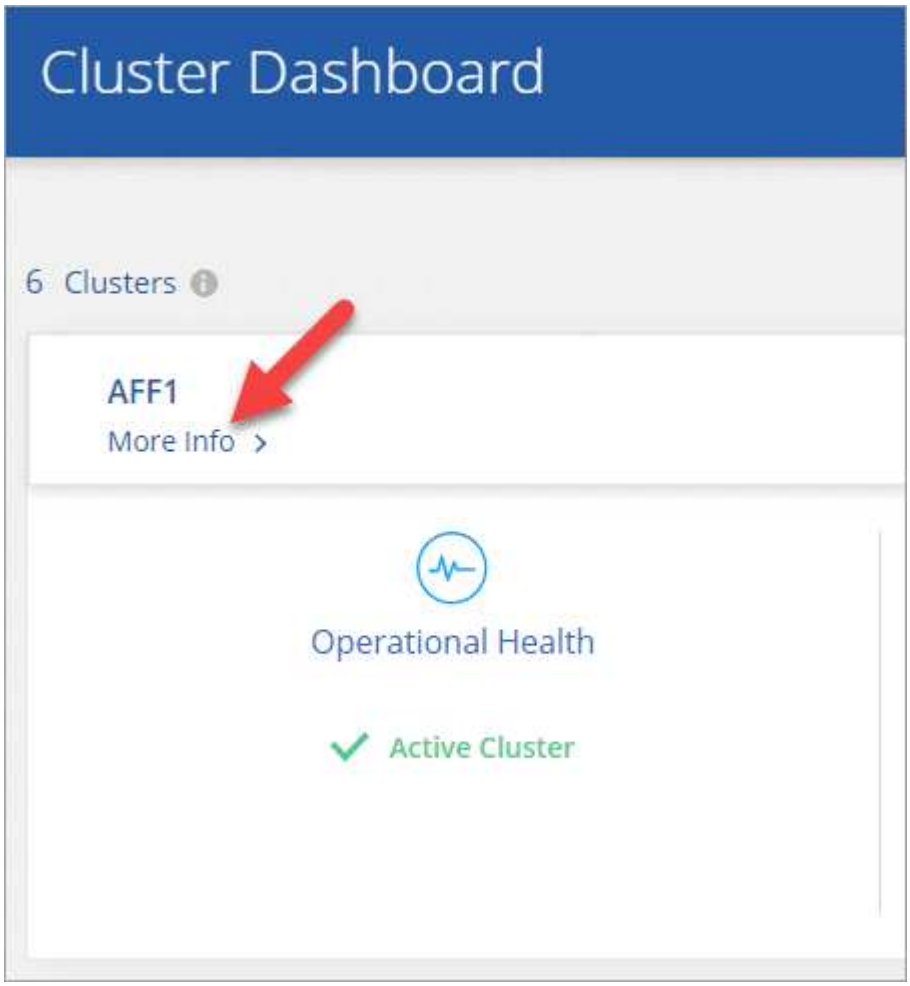
5. Fare clic su **Apply** (Applica).

Revisione delle informazioni di tiering per un cluster

Potresti voler vedere la quantità di dati nel Tier cloud e la quantità di dati presenti sui dischi. In alternativa, è possibile visualizzare la quantità di dati hot e cold sui dischi del cluster. Cloud Tiering fornisce queste informazioni per ogni cluster.

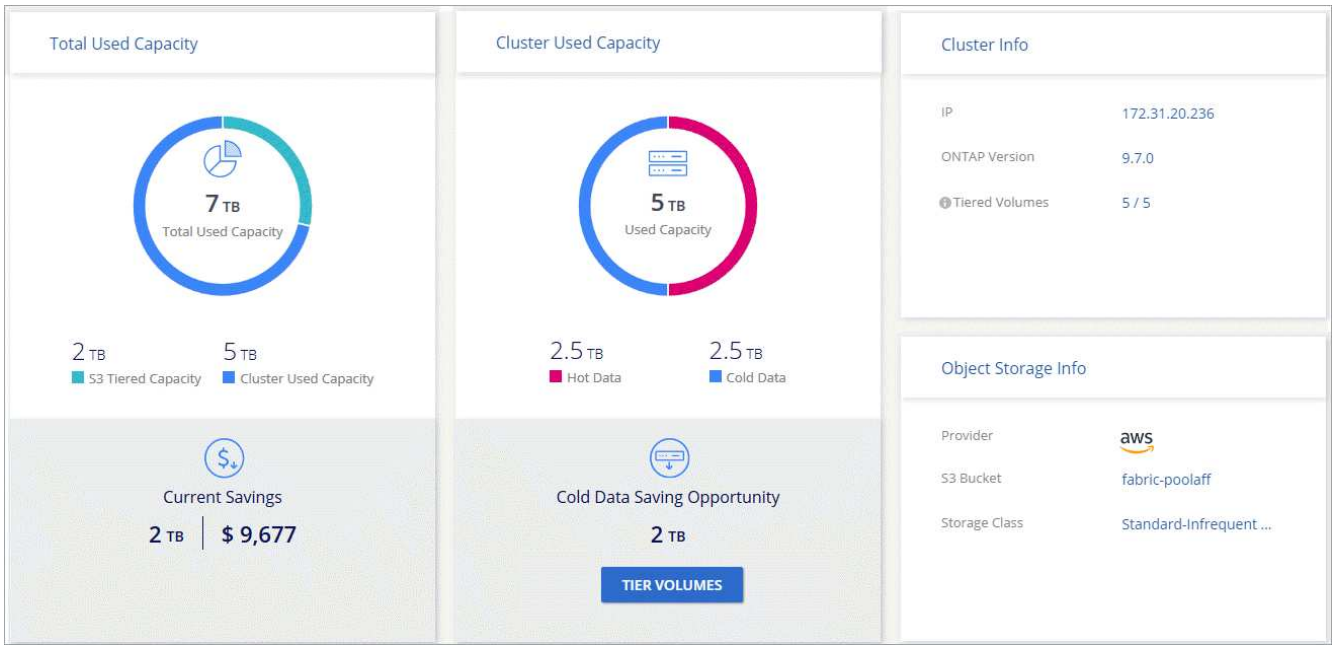
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Tiering**.
2. Dal pannello di controllo del cluster, fare clic su **ulteriori informazioni** per un cluster.



3. Esaminare i dettagli del cluster.

   Ecco un esempio:

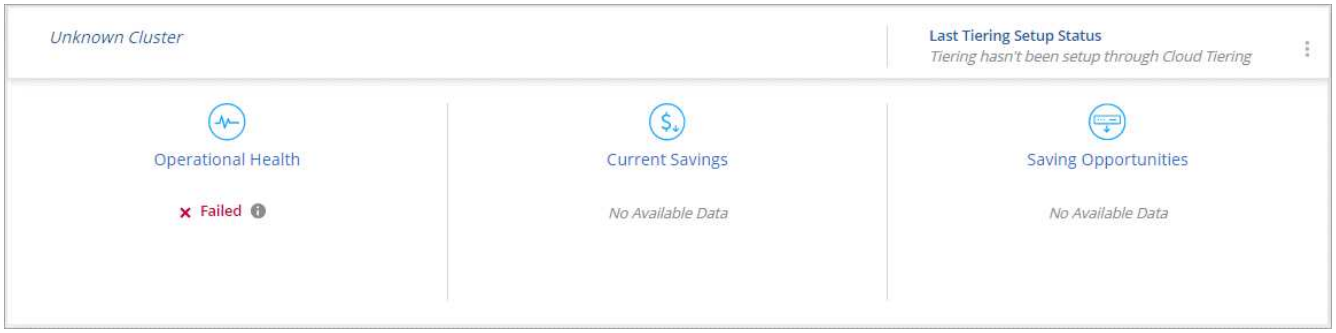


Correzione dello stato operativo

Possono verificarsi errori. Quando lo fanno, il Cloud Tiering visualizza uno stato di salute operativo "non riuscito" sul pannello di controllo del cluster. Lo stato di salute riflette lo stato del sistema ONTAP e di Cloud Manager.

Fasi

1. Identificare tutti i cluster con stato operativo "Failed" (guasto).



2. Passare il mouse su per visualizzare il motivo del guasto.
3. Correggere il problema:
   a. Verificare che il cluster ONTAP sia operativo e che disponga di una connessione in entrata e in uscita con il provider di storage a oggetti.
   b. Verificare che Cloud Manager disponga di connessioni in uscita al servizio di tiering cloud, all'archivio di oggetti e ai cluster ONTAP che rileva.

FAQ tecniche su Cloud Tiering

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

ONTAP

Le seguenti domande si riferiscono a ONTAP.

Quali sono i requisiti per il cluster ONTAP?

Dipende dalla posizione in cui si suddividere i dati cold. Fare riferimento a quanto segue:

- "Tiering dei dati dai cluster ONTAP on-premise ad Amazon S3"
- "Tiering dei dati dai cluster ONTAP on-premise allo storage Azure Blob"
- "Tiering dei dati dai cluster ONTAP on-premise allo storage cloud Google"
- "Tiering dei dati dai cluster ONTAP on-premise a StorageGRID"

Il Cloud Tiering consente il reporting dei dati inattivi?

Sì, il Cloud Tiering consente il reporting dei dati inattivi su ciascun aggregato. Questa impostazione consente di identificare la quantità di dati inattivi che possono essere suddivisi in livelli per lo storage a oggetti a basso costo.

È possibile tierare i dati dai volumi NAS e SAN?

È possibile utilizzare il tiering cloud per tiering dei dati dai volumi NAS al cloud pubblico e dai volumi SAN a un cloud privato utilizzando StorageGRID.

E Cloud Volumes ONTAP?

Se disponi di sistemi Cloud Volumes ONTAP, puoi trovarli nella dashboard dei cluster per vedere una vista completa del tiering dei dati nella tua infrastruttura di cloud ibrido.

Dalla dashboard del cluster, è possibile visualizzare informazioni di tiering simili a quelle di un cluster ONTAP on-premise: Stato operativo, risparmi attuali, opportunità di risparmio, dettagli su volumi e aggregati e altro ancora.

I sistemi Cloud Volumes ONTAP sono di sola lettura dal cloud tiering. Non puoi impostare il tiering dei dati su Cloud Volumes ONTAP dal cloud tiering. Il tiering verrà comunque impostato nello stesso modo: Dall'ambiente di lavoro in Cloud Manager.

Storage a oggetti

Le seguenti domande si riferiscono allo storage a oggetti.

Quali provider di storage a oggetti sono supportati?

Amazon S3, Azure Blob storage, Google Cloud Storage e StorageGRID che utilizzano il protocollo S3 sono supportati.

Posso usare il mio bucket/container?

Sì, è possibile. Quando si imposta il tiering dei dati, è possibile aggiungere un nuovo bucket/container o selezionare un bucket/container esistente.

Quali regioni sono supportate?

- "Regioni AWS supportate"
- "Aree Azure supportate"
- "Aree di Google Cloud supportate"

Quali classi di storage S3 sono supportate?

Cloud Tiering supporta il tiering dei dati per le classi di storage *Standard*, *Standard-infrequent Access*, *One zone-IA* o *Intelligent*. Vedere "Classi di storage S3 supportate" per ulteriori dettagli.

Quali livelli di accesso di Azure Blob sono supportati?

Cloud Tiering utilizza automaticamente il Tier di accesso *Hot* per i dati inattivi.

Quali classi di storage sono supportate per Google Cloud Storage?

Cloud Tiering utilizza la classe di storage *Standard* per i dati inattivi.

Il Cloud Tiering utilizza un archivio di oggetti per l'intero cluster o uno per aggregato?

Un archivio di oggetti per l'intero cluster.

Posso applicare policy al mio archivio di oggetti per spostare i dati indipendentemente dal tiering?

No, il Cloud Tiering non supporta le regole di gestione del ciclo di vita degli oggetti che spostano o eliminano i dati dagli archivi di oggetti.

Connettori

Le seguenti domande si riferiscono ai connettori.

Dove deve essere installato il connettore?

- Quando si esegue il tiering dei dati in S3, un connettore può risiedere in un VPC AWS o in sede.
- Quando si esegue il tiering dei dati nello storage Blob, un connettore deve risiedere in un Azure VNET.
- Quando si esegue il tiering dei dati su Google Cloud Storage, un connettore deve risiedere in un VPC Google Cloud Platform.
- Quando si esegue il tiering dei dati su StorageGRID, un connettore deve risiedere su un host Linux on-premise.

Networking

Le seguenti domande si riferiscono al networking.

Quali sono i requisiti di rete?

- Il cluster ONTAP avvia una connessione HTTPS sulla porta 443 al provider di storage a oggetti.

  ONTAP legge e scrive i dati da e verso lo storage a oggetti. Lo storage a oggetti non viene mai avviato, ma risponde.

- Per StorageGRID, il cluster ONTAP avvia una connessione HTTPS a StorageGRID tramite una porta specificata dall'utente (la porta è configurabile durante la configurazione del tiering).
- Un connettore richiede una connessione HTTPS in uscita sulla porta 443 ai cluster ONTAP, all'archivio di oggetti e al servizio di tiering cloud.

Per ulteriori informazioni, consulta:

- "Tiering dei dati dai cluster ONTAP on-premise ad Amazon S3"
- "Tiering dei dati dai cluster ONTAP on-premise allo storage Azure Blob"
- "Tiering dei dati dai cluster ONTAP on-premise allo storage cloud Google"
- "Tiering dei dati dai cluster ONTAP on-premise a StorageGRID"

Permessi

Le seguenti domande si riferiscono alle autorizzazioni.

Quali autorizzazioni sono richieste in AWS?

Sono necessarie le autorizzazioni "Per gestire il bucket S3".

Quali autorizzazioni sono richieste in Azure?

Non sono necessarie autorizzazioni aggiuntive al di fuori delle autorizzazioni necessarie per Cloud Manager.

Quali autorizzazioni sono richieste in Google Cloud Platform?

Le autorizzazioni di amministrazione dello storage sono necessarie per un account di servizio che dispone di chiavi di accesso allo storage.

Quali autorizzazioni sono richieste per StorageGRID?

"Sono necessarie le autorizzazioni S3".

Riferimento

Classi e regioni di storage S3 supportate

Cloud Tiering supporta diverse classi di storage S3 e la maggior parte delle regioni.

Classi di storage S3 supportate

Cloud Tiering può applicare una regola del ciclo di vita in modo che i dati transitino dalla classe di storage *Standard* a un'altra classe di storage dopo 30 giorni. È possibile scegliere tra le seguenti classi di storage:

- Standard-infrequent Access (accesso standard-non frequente)
- Una zona-IA
- Intelligente

Se si sceglie Standard, i dati rimangono in quella classe di storage.

"Scopri le classi di storage S3".

Regioni AWS supportate

Cloud Tiering supporta le seguenti aree AWS.

Asia Pacifico

- Mumbai
- Seul
- Singapore
- Sydney
- Tokyo

Europa

- Francoforte
- Irlanda
- Londra
- Parigi
- Stoccolma

Nord America

- Canada centrale
- GovCloud (USA-ovest) – a partire da ONTAP 9.3
- US East (N. Virginia)
- USA Est (Ohio)
- US West (N. California)
- STATI UNITI occidentali (Oregon)

America del Sud

- São Paolo

Aree e livelli di accesso supportati da Azure Blob

Cloud Tiering supporta il Tier di accesso *Hot* e la maggior parte delle regioni.

Livelli di accesso supportati da Azure Blob

Quando si imposta il tiering dei dati su Azure, il tiering cloud utilizza automaticamente il Tier di accesso *Hot* per i dati inattivi.

Aree Azure supportate

Cloud Tiering supporta le seguenti aree Azure.

Africa

- Sud Africa, Nord

Asia Pacifico

- Australia Est
- Australia sud-orientale
- Asia orientale
- Giappone Est
- Giappone occidentale
- Corea centrale
- Corea del Sud
- Sud-est asiatico

Europa

- Francia centrale
- Germania centrale
- Germania Nord-est
- Nord Europa
- Regno Unito sud
- Regno Unito, ovest
- Europa occidentale

Nord America

- Canada centrale
- Canada Est
- Stati Uniti centrali
- Stati Uniti orientali
- Est US 2
- Stati Uniti centro-nord
- Stati Uniti centro-sud
- Stati Uniti occidentali
- Stati Uniti occidentali 2
- Stati Uniti centro-occidentali

America del Sud

- Brasile Sud

Classi e regioni di storage Google Cloud supportate

Cloud Tiering supporta la classe di storage standard e la maggior parte delle aree di Google Cloud.

Livelli di accesso supportati

Cloud Tiering utilizza il Tier di accesso *Standard* per i dati inattivi.

Aree di Google Cloud supportate

Cloud Tiering supporta le seguenti aree geografiche.

Americhe

- Iowa
- Los Angeles
- Montreal
- N. Virginia
- Oregon
- San Paolo
- Carolina del Sud

Asia Pacifico

- Hong Kong
- Mumbai
- Osaka
- Singapore
- Sydney
- Taiwan
- Tokyo

Europa

- Belgio
- Finlandia
- Francoforte
- Londra
- Paesi Bassi
- Zurigo

Visualizzazione dei bucket Amazon S3

Dopo aver installato un connettore in AWS, Cloud Manager è in grado di rilevare automaticamente le informazioni sui bucket Amazon S3 che risiedono nell'account AWS in cui è installato.

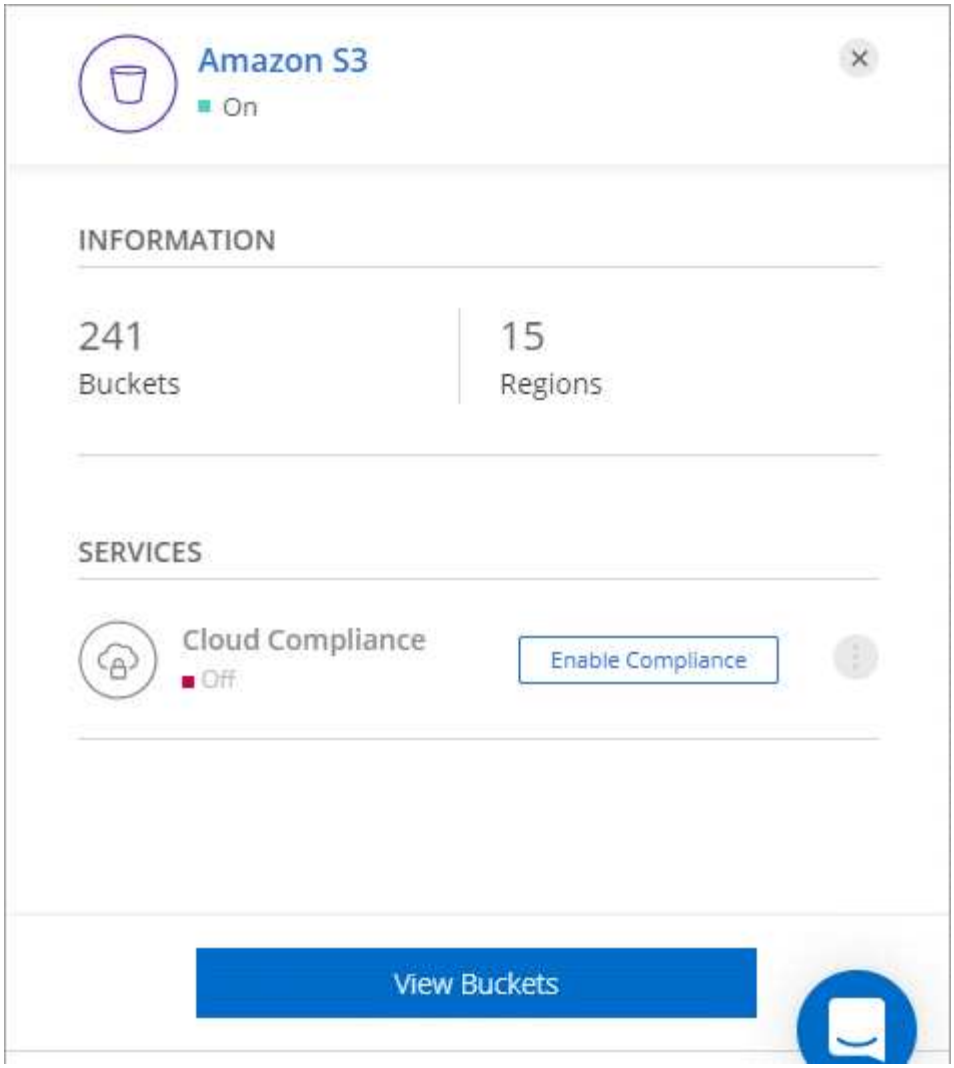
Puoi vedere i dettagli sui bucket S3, tra cui la regione, il livello di accesso, la classe di storage e se il bucket viene utilizzato con Cloud Volumes ONTAP per backup o tiering dei dati. Inoltre, puoi eseguire la scansione dei bucket S3 con la conformità al cloud.

Fasi

1. "Installare un connettore" Nell'account AWS in cui si desidera visualizzare i bucket Amazon S3.

   Subito dopo, viene visualizzato automaticamente un ambiente di lavoro Amazon S3.

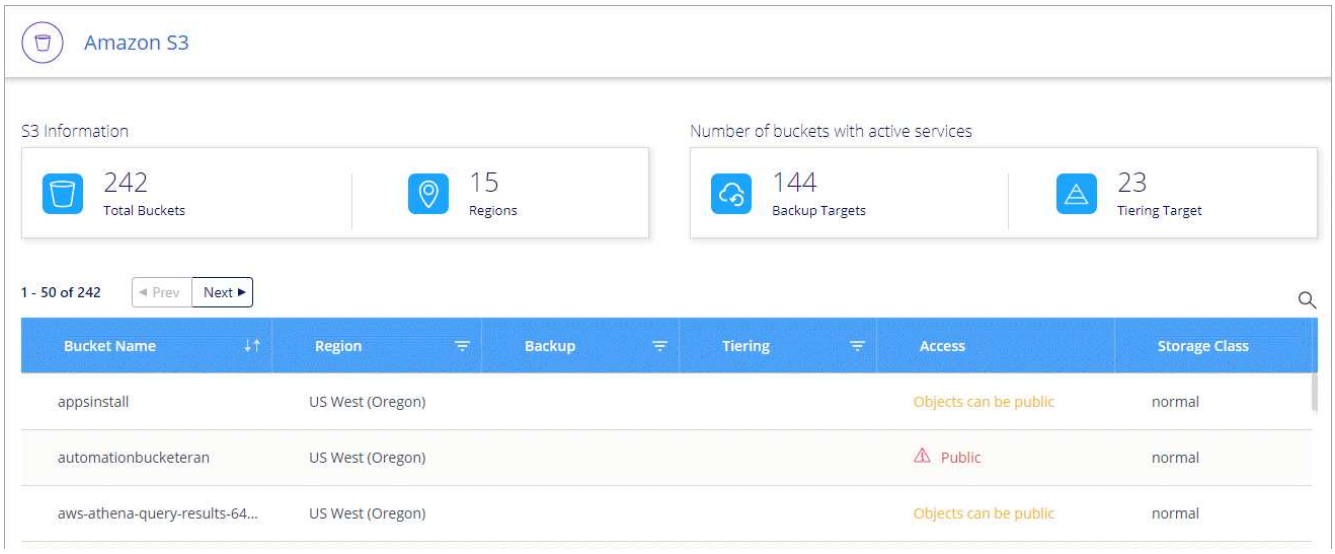
2. Fare clic sull'ambiente di lavoro e selezionare un'azione dal riquadro di destra.



3. Fare clic su **Enable Compliance** (attiva compliance) per eseguire la scansione dei bucket S3 alla ricerca di dati personali e sensibili.

   Per ulteriori informazioni, vedere "Introduzione alla conformità cloud per Amazon S3".

4. Fare clic su **View Bucket** (Visualizza bucket) per visualizzare i dettagli sui bucket S3 nel proprio account AWS.


Amazon S3
S3 Information
242
Total Buckets
15
Regions
Number of buckets with active services
144
Backup Targets
23
Tiering Target
1 - 50 of 242
Prev
Next
Bucket Name
Region
Backup
Tiering
Access
Storage Class
appsinstall
US West (Oregon)
Objects can be public
normal
automationbucketeran
US West (Oregon)
Public
normal
aws-athena-query-results-64...
US West (Oregon)
Objects can be public
normal

Amministrare Cloud Manager

Individuazione dell'ID di sistema di Cloud Manager

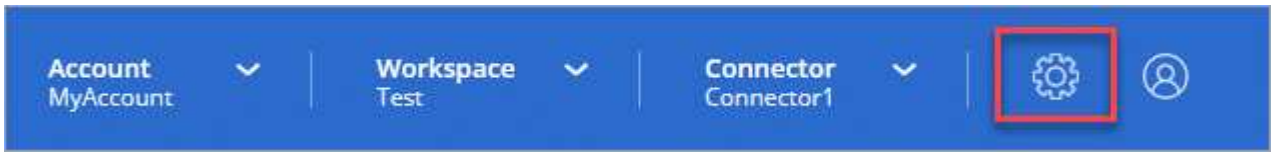
Per aiutarti a iniziare, il tuo rappresentante NetApp potrebbe richiedere l'ID di sistema Cloud Manager. L'ID viene generalmente utilizzato a scopo di licensing e troubleshooting.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

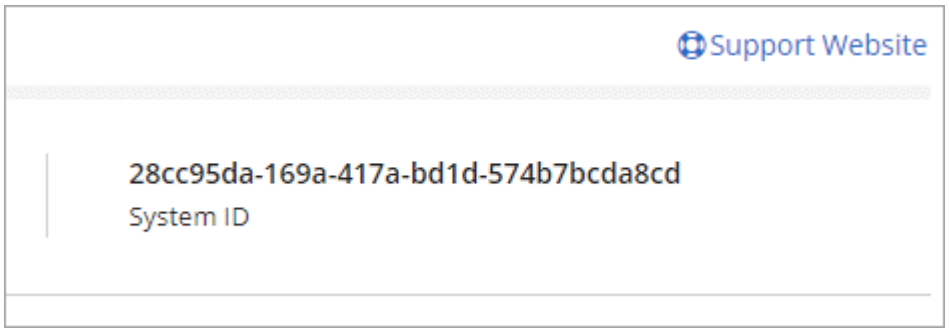
1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni.



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

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

   Esempio



Gestire i connettori

Gestione dei connettori esistenti

Dopo aver creato uno o più connettori, è possibile gestirli passando da connettori a interfacce utente locali in esecuzione su un connettore e altro ancora.

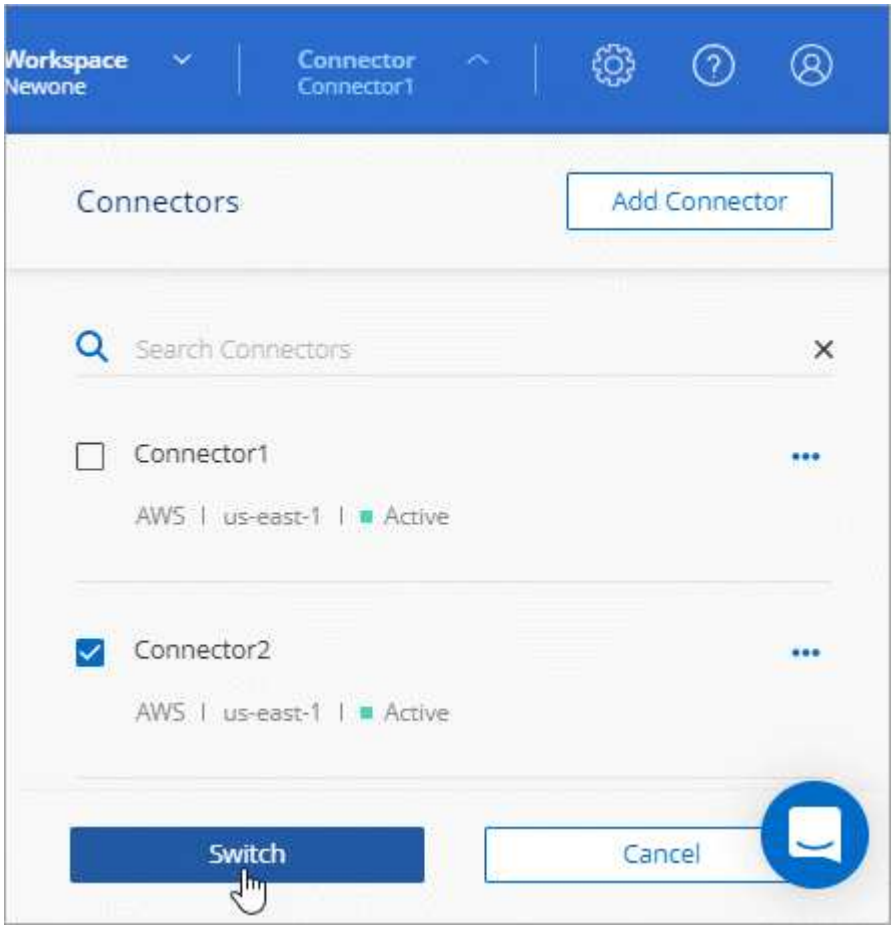
Passaggio da un connettore all'altro

Se si dispone di più connettori, è possibile passare da un connettore all'altro per visualizzare gli ambienti di lavoro associati a uno specifico connettore.

Ad esempio, supponiamo di lavorare in un ambiente multi-cloud. In AWS potrebbe essere presente un connettore e in Google Cloud un altro connettore. Per gestire i sistemi Cloud Volumes ONTAP in esecuzione in tali cloud, è necessario passare da un connettore all'altro.

Fase

1. Fare clic sull'elenco a discesa **Connector**, selezionare un altro connettore, quindi fare clic su **Switch**.



Cloud Manager aggiorna e mostra gli ambienti di lavoro associati al connettore selezionato.

Accesso all'interfaccia utente locale

Sebbene sia necessario eseguire quasi tutte le attività dall'interfaccia utente SaaS, sul connettore è ancora disponibile un'interfaccia utente locale. Questa interfaccia è necessaria per alcune attività che devono essere eseguite dal connettore stesso:

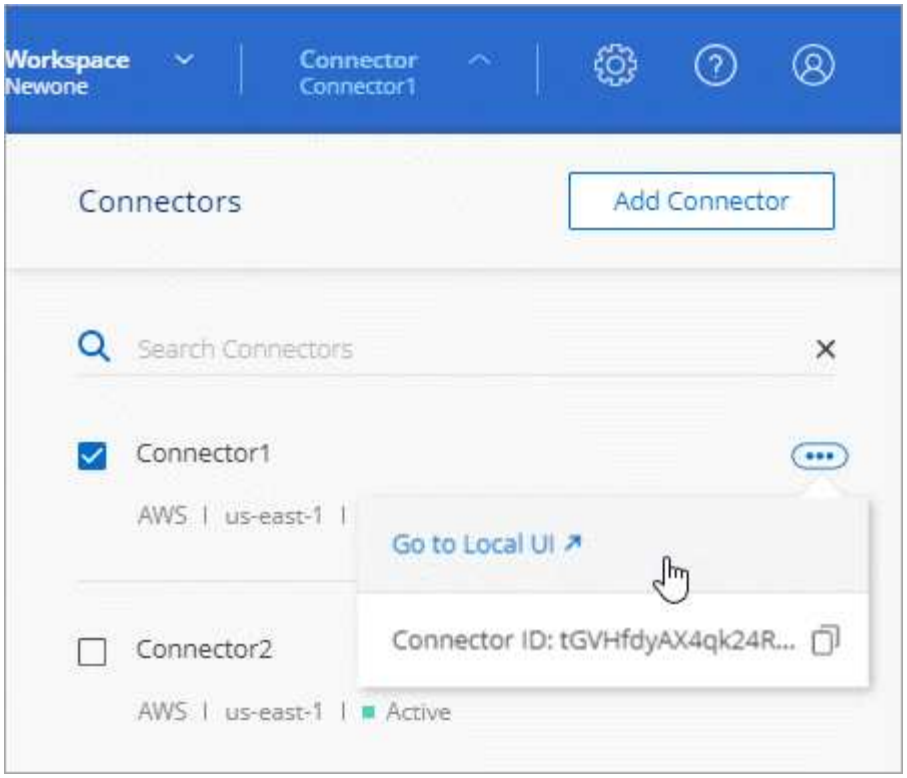
- "Impostazione di un server proxy"
- Installazione di una patch (in genere collaborerete con il personale NetApp per installare una patch)
- Download dei messaggi AutoSupport (solitamente indirizzati dal personale NetApp in caso di problemi)

Fasi

1. "Accedere all'interfaccia SaaS di Cloud Manager" Da un computer che dispone di una connessione di rete all'istanza del connettore.

   Se il connettore non dispone di un indirizzo IP pubblico, è necessaria una connessione VPN oppure è necessario connettersi da un host di collegamento che si trova nella stessa rete del connettore.

2. Fare clic sull'elenco a discesa **Connector**, selezionare il menu delle azioni di un connettore, quindi fare clic su **Go to Local UI** (Vai all'interfaccia utente locale).



L'interfaccia di Cloud Manager in esecuzione sul connettore viene caricata in una nuova scheda del browser.

Rimozione dei connettori da Cloud Manager

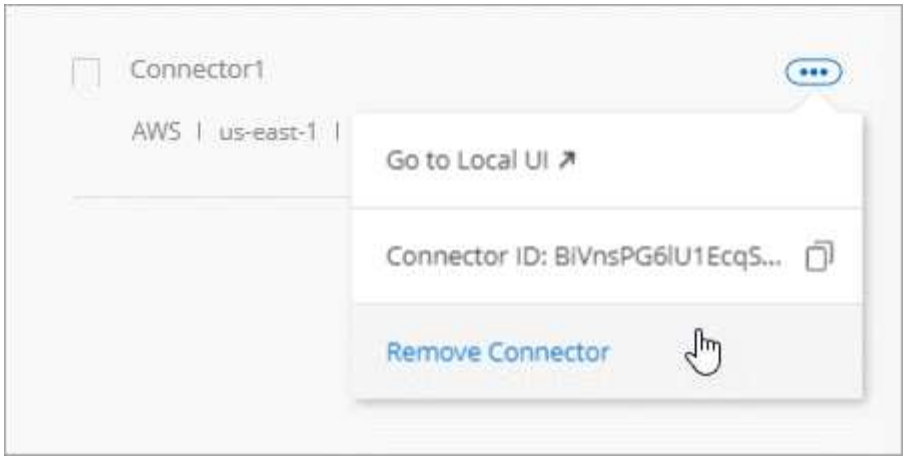
Se un connettore non è attivo, è possibile rimuoverlo dall'elenco dei connettori in Cloud Manager. Questa operazione può essere eseguita se la macchina virtuale Connector è stata eliminata o se il software Connector è stato disinstallato.

Tenere presente quanto segue per la rimozione di un connettore:

- Questa azione non elimina la macchina virtuale.
- Questa azione non può essere ripristinata - una volta rimosso un connettore da Cloud Manager, non puoi aggiungerlo di nuovo a Cloud Manager.

Fasi

1. Fare clic sull'elenco a discesa Connector dall'intestazione Cloud Manager.
2. Fare clic sul menu delle azioni per un connettore inattivo e fare clic su **Remove Connector** (Rimuovi connettore).



3. Inserire il nome del connettore da confermare, quindi fare clic su Remove (Rimuovi).

Risultato

Cloud Manager rimuove il connettore dai record.

Disinstallazione del software Connector

Il connettore 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.

Fase

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

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

   silent esegue lo script senza richiedere conferma.

E gli aggiornamenti software?

Il connettore aggiorna automaticamente il software alla versione più recente, a patto che sia disponibile "accesso a internet in uscita" per ottenere l'aggiornamento software.

Altri modi per creare connettori

Requisiti host del connettore

Il software del connettore deve essere eseguito su un host che soddisfi i requisiti specifici del sistema operativo, della RAM, dei requisiti delle porte e così via.

È richiesto un host dedicato

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

CPU

4 core o 4 vCPU

RAM

14 GB

Tipo di istanza AWS EC2

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare t3.xlarge e quel tipo di istanza quando si implementa il connettore direttamente da Cloud Manager.

Dimensione delle macchine virtuali Azure

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare DS3 v2 e le dimensioni delle macchine virtuali quando si implementa il connettore direttamente da Cloud Manager.

Tipo di macchina GCP

Un tipo di istanza che soddisfa i requisiti di CPU e RAM indicati in precedenza. Si consiglia di utilizzare n1-standard-4 e questo tipo di macchina quando si implementa il connettore direttamente da Cloud Manager.

Sistemi operativi supportati

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  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 del connettore.

  Il connettore 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?"^]

Spazio su disco in /opz

Devono essere disponibili 100 GB di spazio

Accesso a Internet in uscita

L'accesso a Internet in uscita è necessario per installare il connettore e per gestire le risorse e i processi all'interno dell'ambiente di cloud pubblico. Per un elenco degli endpoint, vedere "Requisiti di rete per il connettore".

Creazione di un connettore da AWS Marketplace

Si consiglia di creare un connettore direttamente da Cloud Manager, ma è possibile avviare un connettore da AWS Marketplace, se non si desidera specificare le chiavi di accesso AWS. Dopo aver creato e configurato il connettore, Cloud Manager lo utilizzerà automaticamente quando si creano nuovi ambienti di lavoro.

Fasi

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

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

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

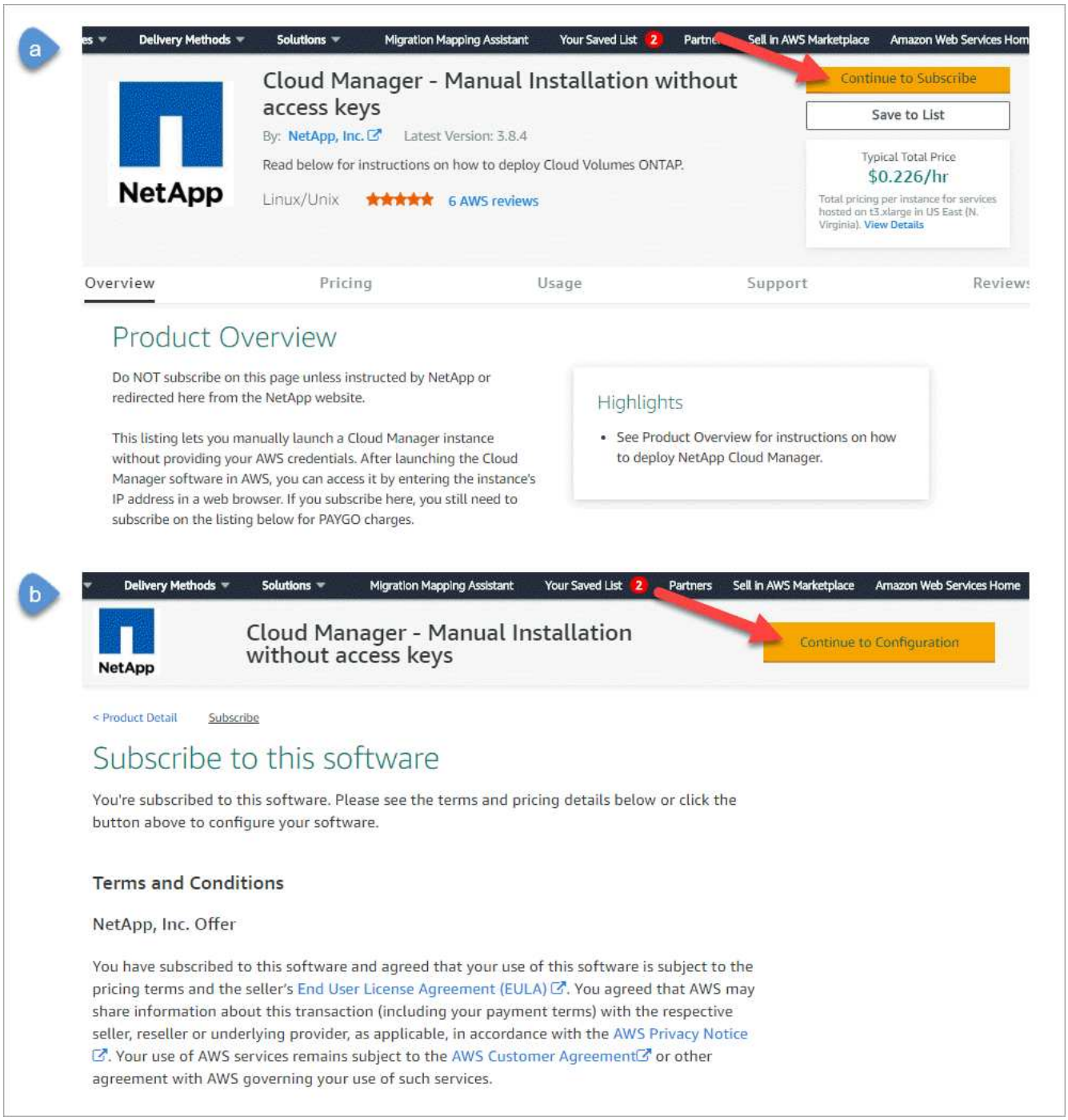
b. Dalla console IAM, creare la propria policy copiando e incollando il testo dalla policy IAM di Cloud Manager.

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

2. Passare alla "Pagina Cloud Manager su AWS Marketplace" Per implementare Cloud Manager da un AMI.

   L'utente IAM deve disporre delle autorizzazioni AWS Marketplace per iscriversi e annullare l'iscrizione.

3. Nella pagina Marketplace, fare clic su **Continue to Subscribe**, quindi fare clic su **Continue to Configuration**.



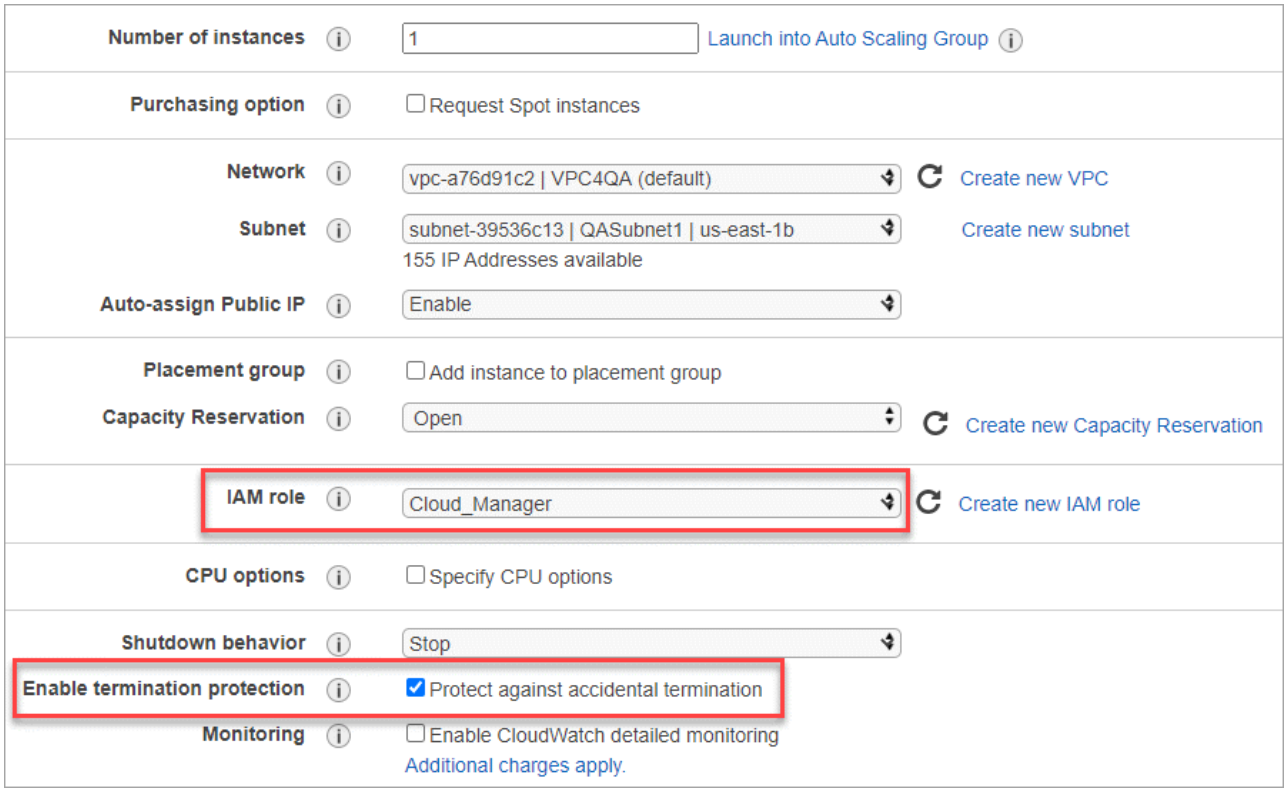
4. Modificare una delle opzioni predefinite e fare clic su **Continue to Launch** (continua fino all'avvio).
5. In **Choose Action** (Scegli azione), selezionare **Launch through EC2** (Avvia tramite EC2*), quindi fare clic su **Launch** (Avvia).

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

6. Seguire le istruzioni per configurare e implementare l'istanza:
   - **Choose Instance Type** (Scegli tipo di istanza): A seconda della disponibilità della regione, scegliere uno dei tipi di istanza supportati (si consiglia t3.xlarge).

"Esaminare i requisiti dell'istanza".

- **Configure Instance** (Configura istanza): Selezionare un VPC e una subnet, scegliere il ruolo IAM creato al punto 1, abilitare la protezione di terminazione (scelta consigliata) e scegliere qualsiasi altra opzione di configurazione che soddisfi i requisiti.



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

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

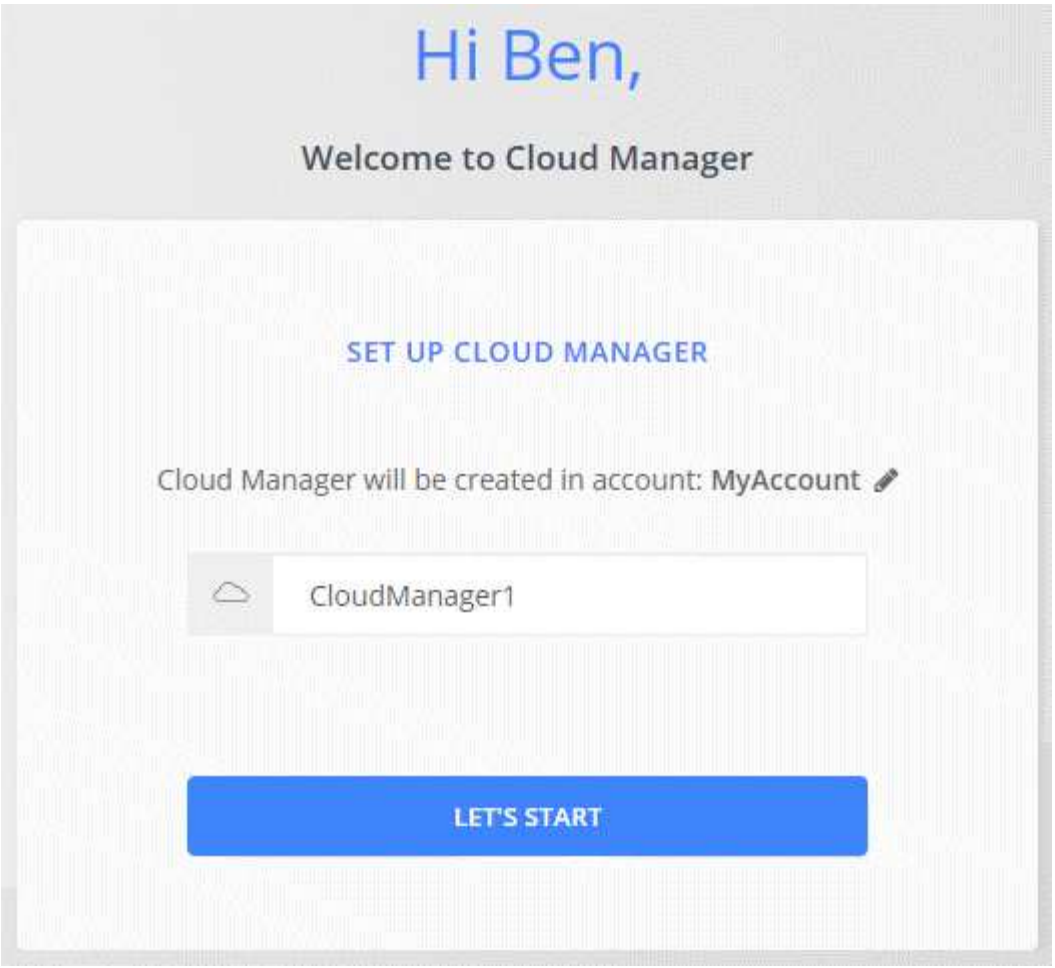
7. Aprire un browser Web da un host connesso all'istanza del connettore e immettere il seguente URL:

   http://ipaddress:80

8. Dopo aver effettuato l'accesso, configurare il connettore:
   a. Specificare l'account Cloud Central da associare al connettore.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Il connettore è ora installato e configurato con il tuo account Cloud Central. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro. Tuttavia, se si dispone di più connettori, è necessario "passare da un'opzione all'altra".

Creazione di un connettore da Azure Marketplace

Si consiglia di creare un connettore direttamente da Cloud Manager, ma è possibile avviare un connettore da Azure Marketplace, se si preferisce. Dopo aver creato e configurato il connettore, Cloud Manager lo utilizzerà automaticamente quando si creano nuovi ambienti di lavoro.

Creazione di un connettore in Azure

Implementare il connettore in Azure utilizzando l'immagine in Azure Marketplace, quindi accedere al connettore per specificare l'account Cloud Central.

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.
- Scegli una macchina virtuale che soddisfi i requisiti di CPU e RAM. Si consiglia DS3 v2.

  "Esaminare i requisiti delle macchine virtuali".

- Per il gruppo di protezione della rete, il connettore richiede connessioni in entrata utilizzando SSH, HTTP e HTTPS.

  "Scopri di più sulle regole dei gruppi di sicurezza per il connettore".

- In **Management**, abilitare **System Assigned Managed Identity** per il connettore selezionando **ON**.

  Questa impostazione è importante perché un'identità gestita consente alla macchina virtuale del connettore 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 del connettore dovrebbero essere in esecuzione in circa cinque minuti.

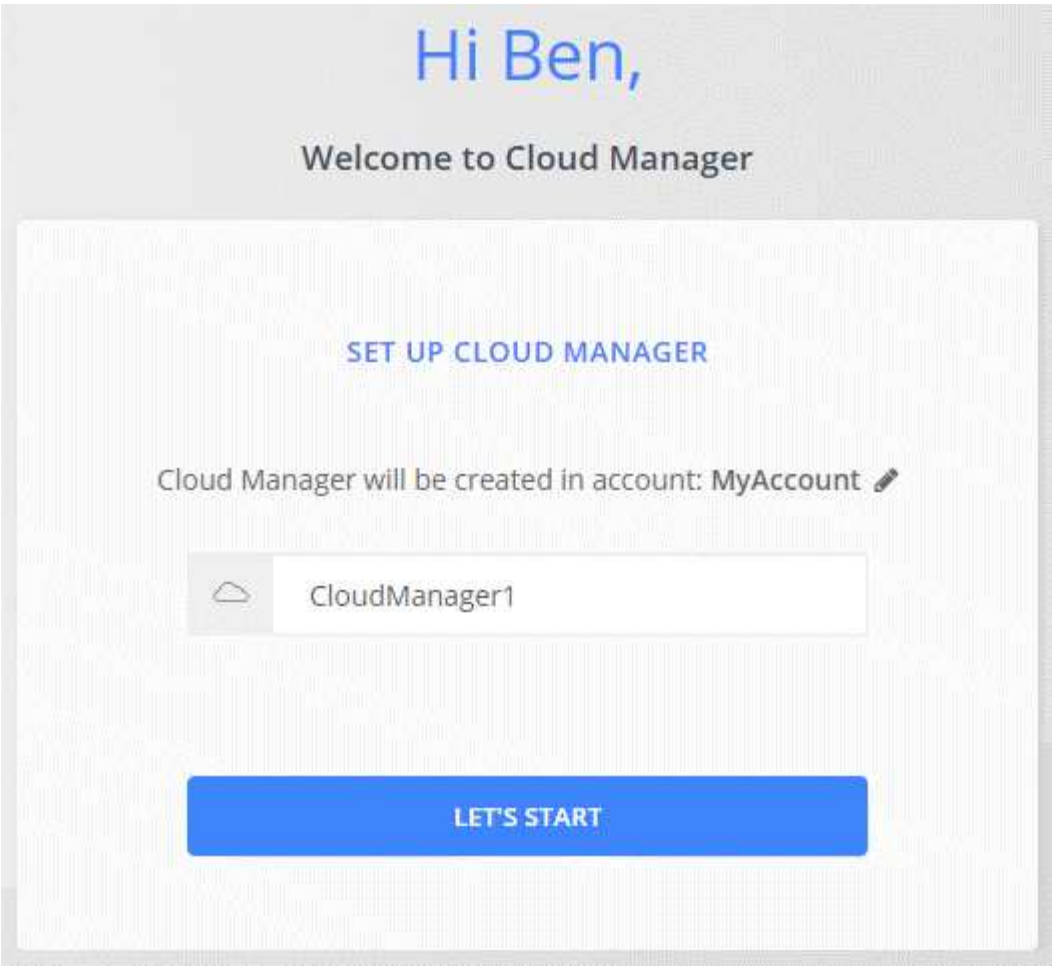
5. Aprire un browser Web da un host connesso alla macchina virtuale Connector e immettere il seguente URL:

   http://ipaddress:80

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

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

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

Concessione delle autorizzazioni Azure

Quando si implementa il connettore in Azure, è necessario aver attivato un "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 del connettore 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_3.8.7.json
   ```

Ora dovresti avere un ruolo personalizzato chiamato Cloud Manager Operator che puoi assegnare alla macchina virtuale del connettore.

2. Assegnare il ruolo alla macchina virtuale Connector 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 **Cloud Manager Operator**.

        Cloud Manager Operator 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 Connector.
      - Selezionare la macchina virtuale Connector.
      - 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

Il connettore dispone ora delle autorizzazioni necessarie all'IT per gestire risorse e processi all'interno del tuo ambiente di cloud pubblico. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro. Tuttavia, se si dispone di più connettori, è necessario "passare da un'opzione all'altra".

Installazione del software del connettore su un host Linux esistente

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

Se si desidera creare un sistema Cloud Volumes ONTAP in Google Cloud, è necessario disporre di un connettore in esecuzione anche in Google Cloud. Non è possibile utilizzare un connettore in esecuzione in un'altra posizione.

Requisiti

- L'host deve soddisfare "Requisiti per il connettore".
- 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.

- Il programma di installazione di Connector accede a diversi URL durante il processo di installazione. È necessario assicurarsi che l'accesso a Internet in uscita sia consentito a questi endpoint:
  - 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

    L'host potrebbe tentare di aggiornare i pacchetti del sistema operativo durante l'installazione. L'host può contattare diversi siti di mirroring per questi pacchetti di sistemi operativi.

A proposito di questa attività

- Per installare il connettore non sono necessari i privilegi di root.
- L'installazione installa gli strumenti della riga di comando AWS (awscli) per abilitare le procedure di ripristino dal supporto NetApp.

  Se viene visualizzato un messaggio che indica che l'installazione di awscli non è riuscita, ignorare il messaggio. Il connettore può funzionare correttamente senza gli strumenti.
- Il programma di installazione disponibile sul NetApp Support Site potrebbe essere una versione precedente. Dopo l'installazione, il connettore si aggiorna automaticamente se è disponibile una nuova versione.

Fasi

1. Scaricare il software Cloud Manager da "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".

2. Assegnare le autorizzazioni per eseguire lo script.

   Esempio

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Eseguire lo script di installazione:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent esegue l'installazione senza richiedere informazioni.

   proxy è richiesto se l'host 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.

3. 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.

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.

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

   https://ipaddress:port

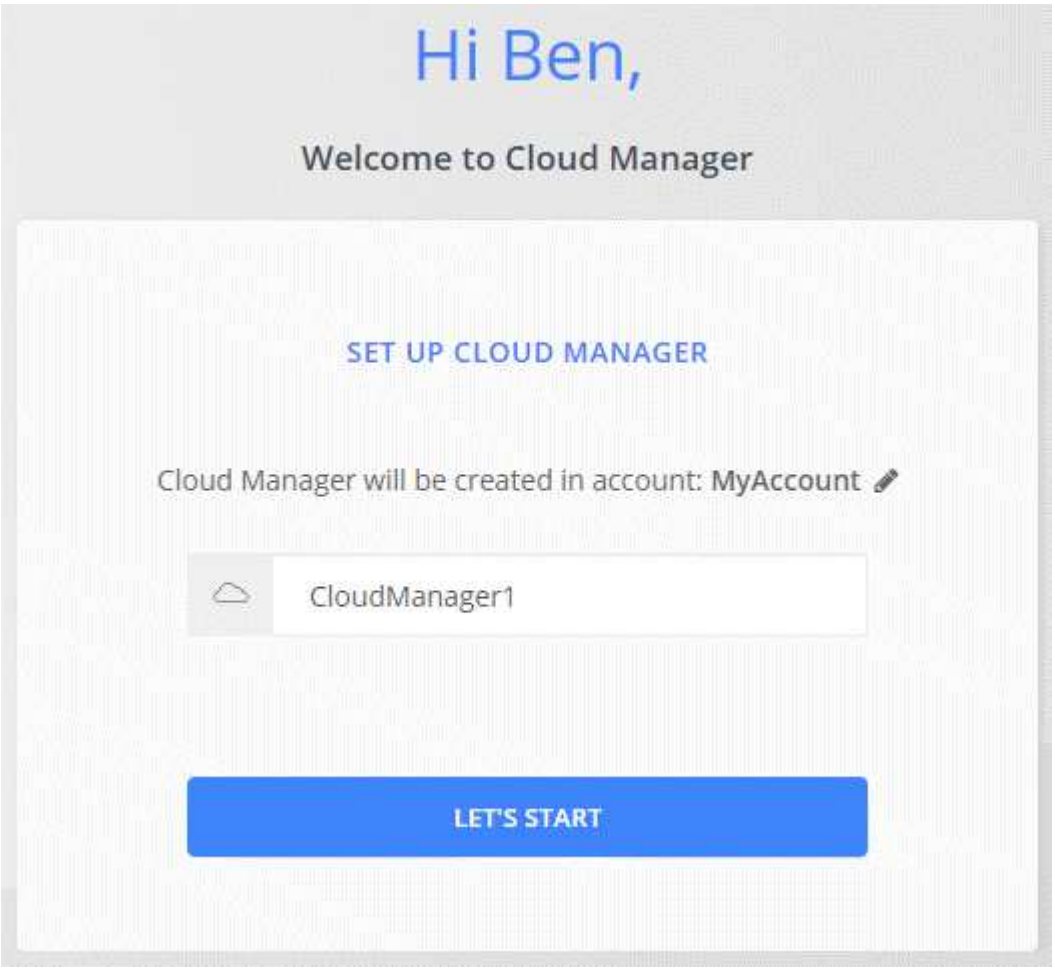
   Ipaddress può essere localhost, un indirizzo IP privato o un indirizzo IP pubblico, a seconda della configurazione dell'host. Ad esempio, se il connettore si trova nel cloud pubblico senza un indirizzo IP pubblico, è necessario inserire un indirizzo IP privato da un host che ha una connessione all'host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

   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

5. Iscriviti a NetApp Cloud Central o effettua l'accesso.
6. Dopo aver effettuato l'accesso, configurare Cloud Manager:
   a. Specificare l'account Cloud Central da associare al connettore.

      "Scopri di più sugli account Cloud Central".

   b. Immettere un nome per il sistema.



Risultato

Il connettore è ora installato e configurato con il tuo account Cloud Central. Cloud Manager utilizza automaticamente questo connettore quando crei nuovi ambienti di lavoro.

Al termine

Imposta le autorizzazioni in modo che Cloud Manager possa gestire risorse e processi all'interno del tuo ambiente di cloud pubblico:

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

Configurazione predefinita per il connettore

Se è necessario risolvere i problemi del connettore, potrebbe essere utile comprendere come è configurato.

- Se hai implementato il connettore da Cloud Manager (o direttamente dal mercato di un cloud provider), prendi nota di quanto segue:
  - In AWS, il nome utente per l'istanza EC2 Linux è ec2-user.
  - Il sistema operativo per l'immagine è il seguente:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      Il sistema operativo non include una GUI. Per accedere al sistema, è necessario utilizzare un terminale.
- La cartella di installazione del connettore 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
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Tirare
  - Wget
- Il connettore utilizza le seguenti porte sull'host Linux:
  - 80 per l'accesso HTTP
  - 443 per l'accesso HTTPS
  - 3306 per il database Cloud Manager
  - 8080 per il proxy API Cloud Manager
  - 8666 per l'API di Service Manager
  - 8777 per l'API del servizio container Health-Checker

Gestire le credenziali

AWS

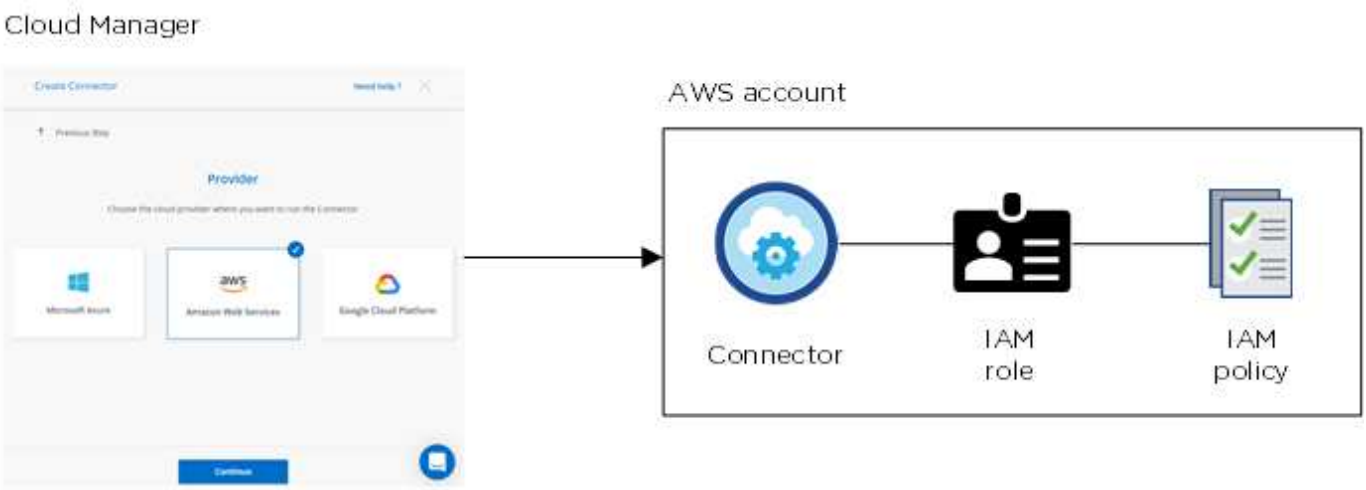
Credenziali e autorizzazioni AWS

Cloud Manager consente di scegliere le credenziali AWS da utilizzare durante l'implementazione di Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali AWS iniziali oppure aggiungere credenziali aggiuntive.

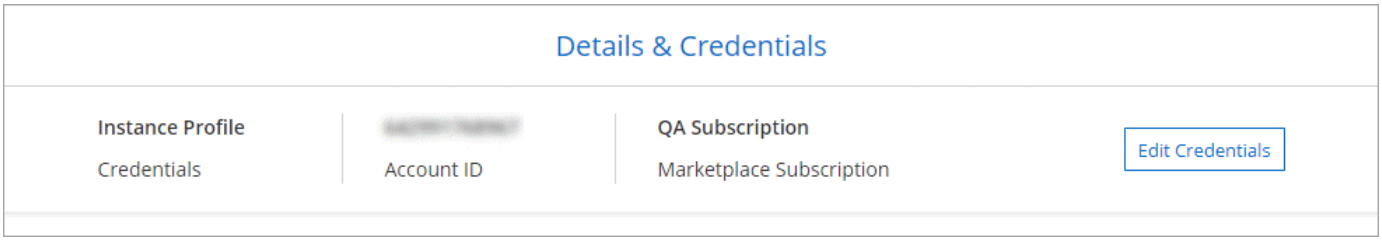
Credenziali AWS iniziali

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

Quando Cloud Manager avvia l'istanza del connettore 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 gestire risorse e processi all'interno di tale account AWS. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".

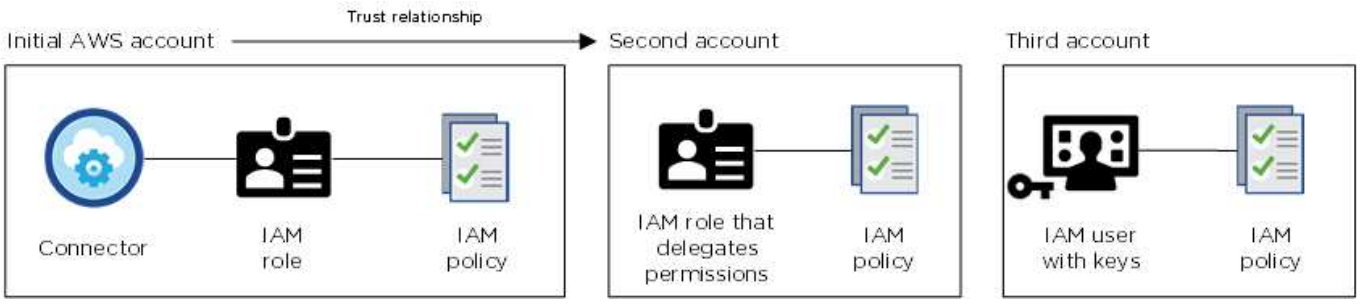


Cloud Manager seleziona queste credenziali AWS per impostazione predefinita quando crei un nuovo ambiente di lavoro per Cloud Volumes ONTAP:



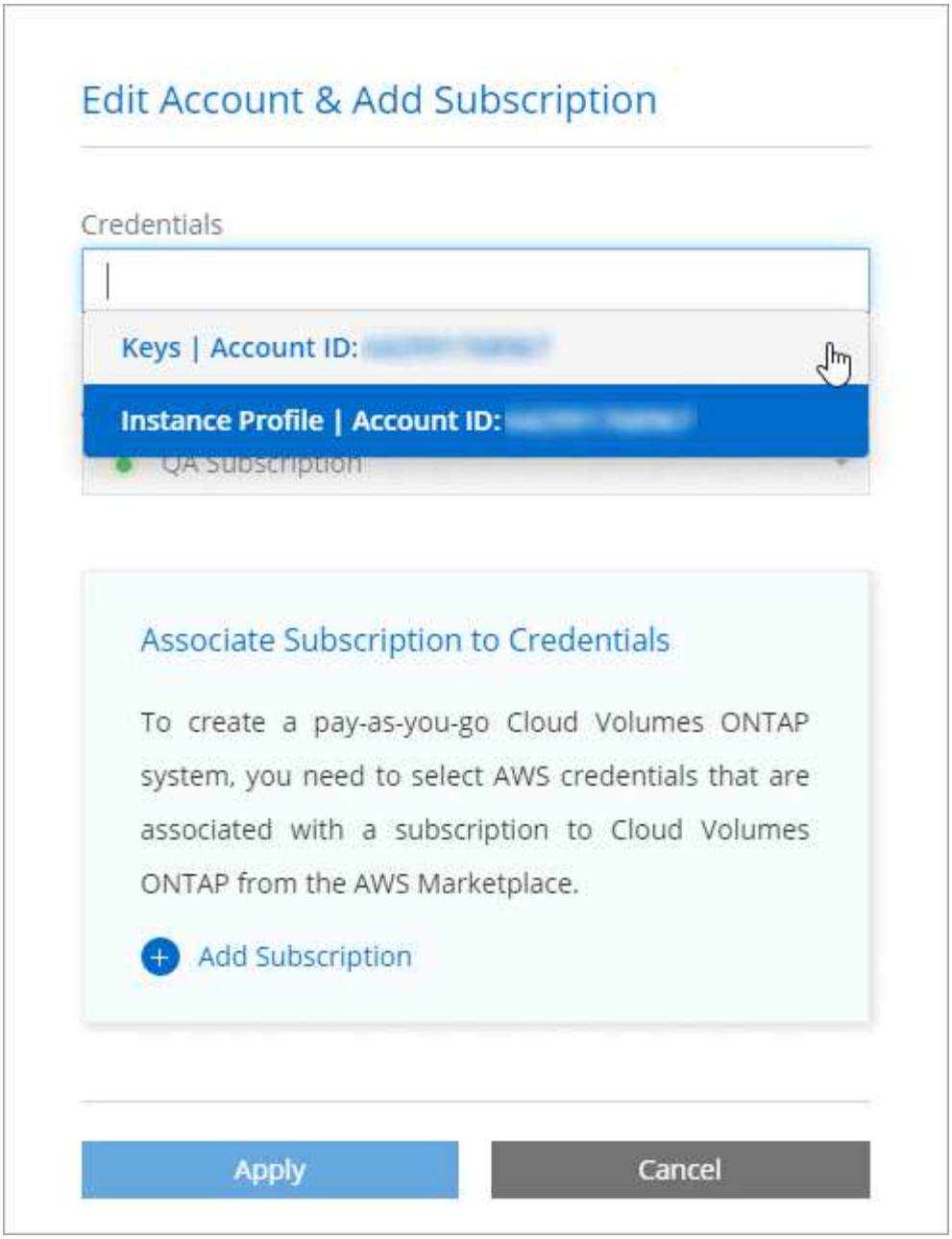
Credenziali AWS aggiuntive

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 "Aggiungere le credenziali dell'account 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 set di credenziali, è possibile passare a queste quando si crea un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, che proviene da Cloud Manager. È inoltre possibile implementare un connettore in AWS da "Mercato AWS" e puoi farlo "Installare il connettore on-premise".

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

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

Come si possono ruotare in modo sicuro le credenziali AWS?

Come descritto in precedenza, Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le

chiavi di accesso AWS.

Con le prime due opzioni, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice: È automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Gestione delle credenziali AWS e delle sottoscrizioni per Cloud Manager

Quando si crea un sistema Cloud Volumes ONTAP, è necessario selezionare le credenziali e l'abbonamento AWS da utilizzare con tale sistema. Se si gestiscono più sottoscrizioni AWS, è possibile assegnarle a diverse credenziali AWS dalla pagina credenziali.

Prima di aggiungere le credenziali AWS a Cloud Manager, è necessario fornire le autorizzazioni necessarie per tale account. Le autorizzazioni consentono a Cloud Manager di gestire risorse e processi all'interno di tale account AWS. La modalità di fornitura delle autorizzazioni dipende dal fatto che si desideri fornire a Cloud Manager le chiavi AWS o l'ARN di un ruolo in un account attendibile.

Quando hai implementato un connettore da Cloud Manager, Cloud Manager ha aggiunto automaticamente le credenziali AWS per l'account in cui hai implementato il connettore. Questo account iniziale non viene aggiunto se il software Connector è stato installato manualmente su un sistema esistente. "Scopri le credenziali e le autorizzazioni AWS".

Scelte

- Concessione delle autorizzazioni fornendo le chiavi AWS
- Concessione delle autorizzazioni assumendo ruoli IAM in altri account

Come si possono ruotare in modo sicuro le credenziali AWS?

Cloud Manager consente di fornire le credenziali AWS in diversi modi: Un ruolo IAM associato all'istanza del connettore, assumendo un ruolo IAM in un account attendibile o fornendo le chiavi di accesso AWS. "Scopri di più sulle credenziali e le autorizzazioni AWS".

Con le prime due opzioni, Cloud Manager utilizza AWS Security Token Service per ottenere credenziali temporanee che ruotano costantemente. Questo processo è la Best practice, è automatico e sicuro.

Se si forniscono a Cloud Manager le chiavi di accesso AWS, è necessario ruotarle aggiornandole in Cloud Manager a intervalli regolari. Si tratta di un processo completamente manuale.

Concessione delle autorizzazioni fornendo le chiavi AWS

Se si desidera fornire a Cloud Manager le chiavi AWS per un utente IAM, è necessario concedere le autorizzazioni necessarie a tale utente. La policy IAM di Cloud Manager definisce le azioni e le risorse AWS che Cloud Manager può utilizzare.

Fasi

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

Manager.

"Documentazione AWS: Creazione di policy IAM"

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

Risultato

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

Concessione delle autorizzazioni assumendo ruoli IAM in altri account

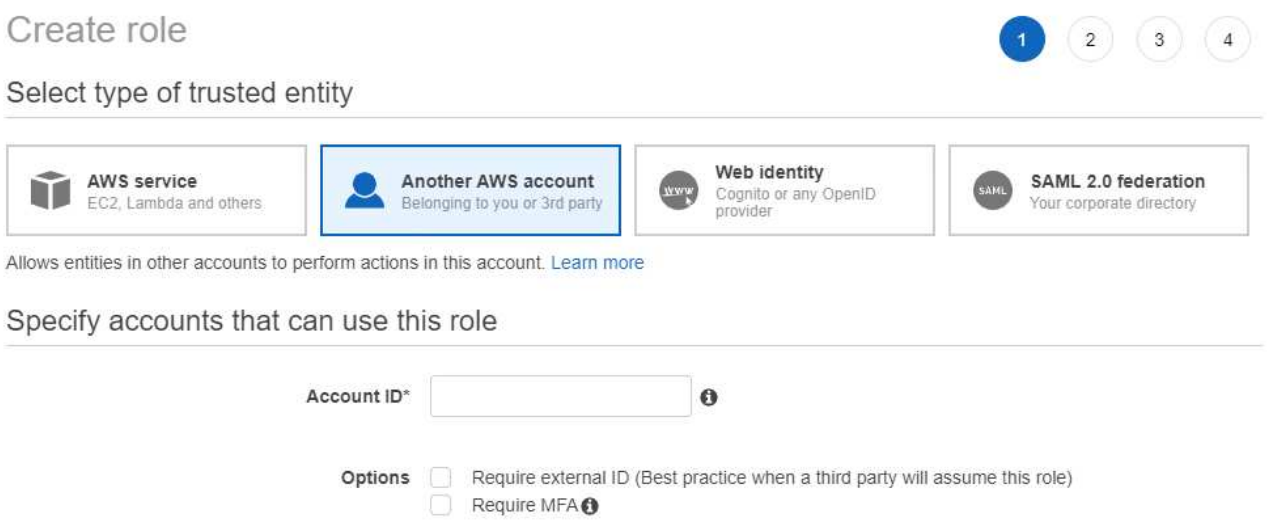
È possibile impostare una relazione di trust tra l'account AWS di origine in cui è stata implementata l'istanza di Connector e altri account AWS utilizzando i ruoli IAM. In seguito, fornirai a Cloud Manager l'ARN dei ruoli IAM degli account attendibili.

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 Connector.
   - 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 Connector e selezionare il ruolo IAM associato all'istanza.

   a. Fare clic su **Allega policy**, quindi su **Crea policy**.

   b. Creare una policy che includa 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

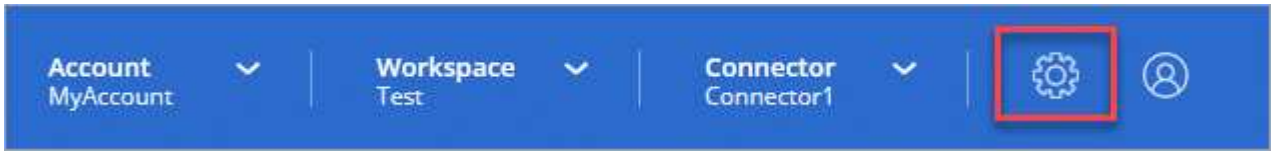
L'account dispone ora delle autorizzazioni necessarie. Ora puoi aggiungerlo a Cloud Manager.

Aggiunta di credenziali AWS a Cloud Manager

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

Fasi

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



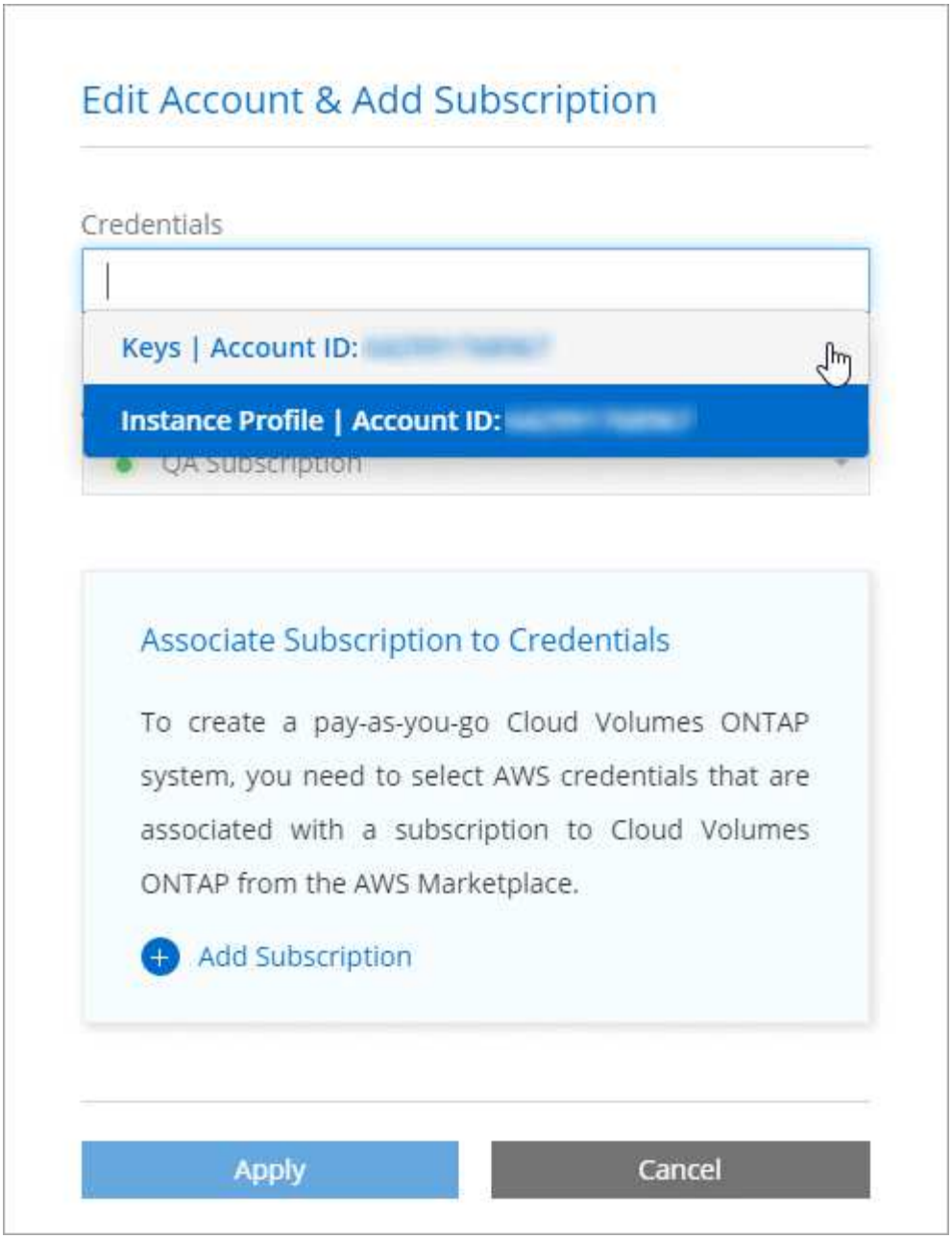
2. Fare clic su **Add Credentials** (Aggiungi credenziali) e selezionare **AWS**.
3. Fornire le chiavi AWS o l'ARN di un ruolo IAM attendibile.
4. Confermare che i requisiti della policy sono stati soddisfatti e fare clic su **continua**.
5. Scegli l'abbonamento pay-as-you-go che desideri associare alle credenziali o fai clic su **Aggiungi abbonamento** se non ne hai ancora uno.

   Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, le credenziali AWS devono essere associate a un abbonamento a Cloud Volumes ONTAP da AWS Marketplace.

6. Fare clic su **Aggiungi**.

Risultato

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



Associazione di un abbonamento AWS alle credenziali

Dopo aver aggiunto le credenziali AWS a Cloud Manager, è possibile associare un abbonamento AWS Marketplace a tali credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

Esistono due scenari in cui è possibile associare un abbonamento AWS Marketplace dopo aver aggiunto le credenziali a Cloud Manager:

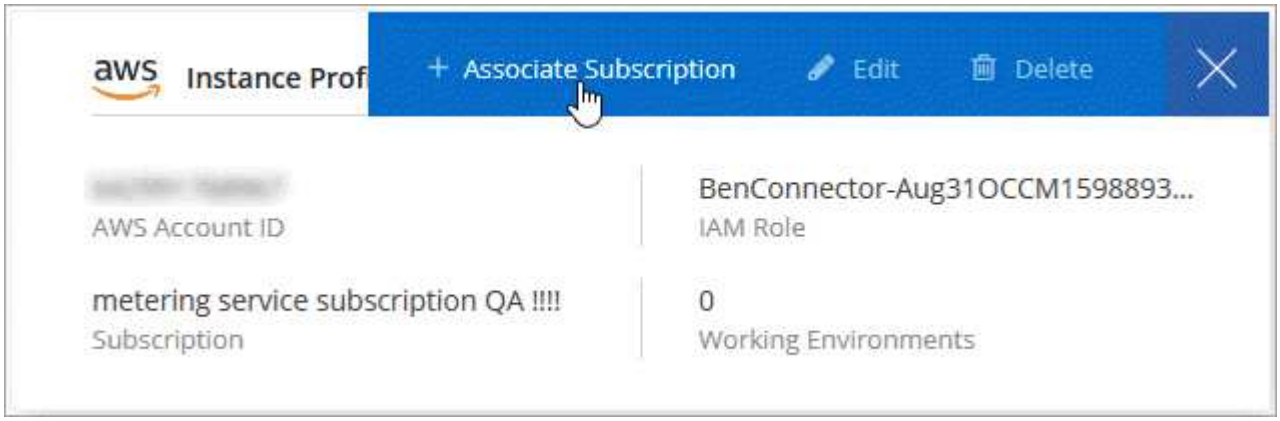
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento AWS Marketplace esistente con un nuovo abbonamento.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Passare il mouse su un set di credenziali e fare clic sul menu delle azioni.
3. Dal menu, fare clic su **Associa abbonamento**.



4. Selezionare un abbonamento dall'elenco a discesa oppure fare clic su **Aggiungi abbonamento** e seguire la procedura per creare un nuovo abbonamento.

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

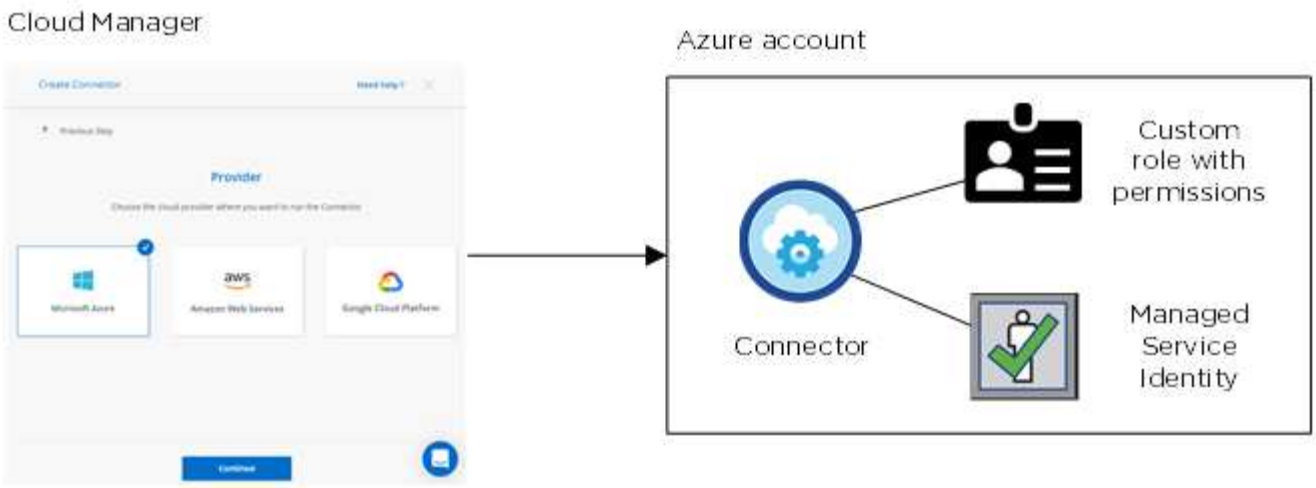
Credenziali e permessi di Azure

Cloud Manager consente di scegliere le credenziali Azure da utilizzare durante l'implementazione di Cloud Volumes ONTAP. È possibile implementare tutti i sistemi Cloud Volumes ONTAP utilizzando le credenziali iniziali di Azure oppure aggiungere ulteriori credenziali.

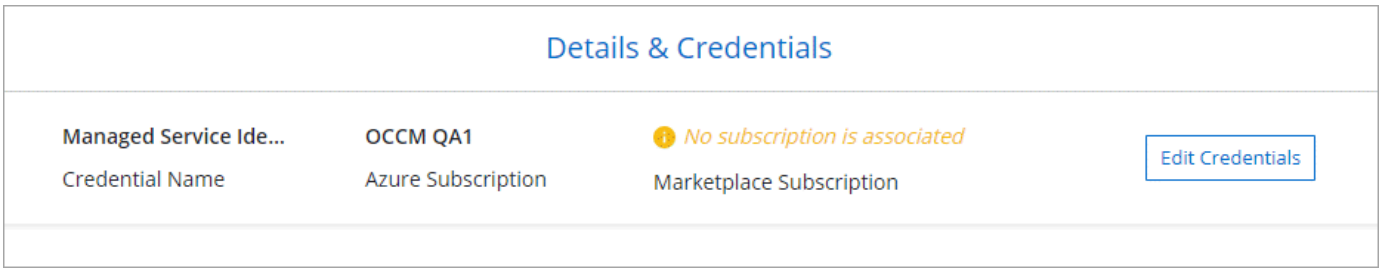
Credenziali iniziali di Azure

Quando si implementa un connettore da Cloud Manager, è necessario utilizzare un account Azure che disponga delle autorizzazioni necessarie per implementare la macchina virtuale del connettore. Le autorizzazioni richieste sono elencate nella "Policy di implementazione del connettore per Azure".

Quando Cloud Manager implementa la macchina virtuale del connettore in Azure, abilita una "identità gestita assegnata dal sistema" sulla macchina virtuale, crea un ruolo personalizzato e lo assegna alla macchina virtuale. Il ruolo fornisce a Cloud Manager le autorizzazioni per gestire risorse e processi all'interno dell'abbonamento Azure. "Analisi dell'utilizzo delle autorizzazioni da parte di Cloud Manager".



Cloud Manager seleziona queste credenziali Azure per impostazione predefinita quando crei un nuovo ambiente di lavoro per Cloud Volumes ONTAP:

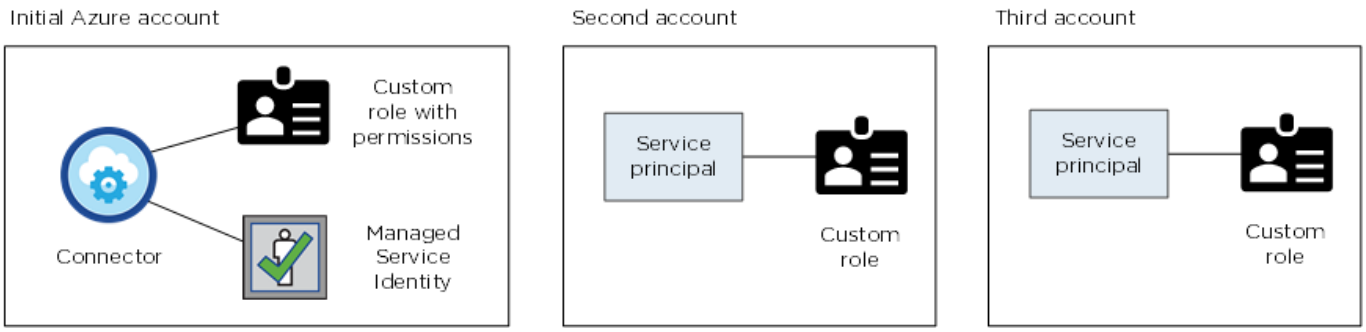


Abbonamenti Azure aggiuntivi per un'identità gestita

L'identità gestita è associata all'abbonamento con cui è stato avviato il connettore. Se si desidera selezionare un abbonamento Azure diverso, è necessario "associare l'identità gestita a tali sottoscrizioni".

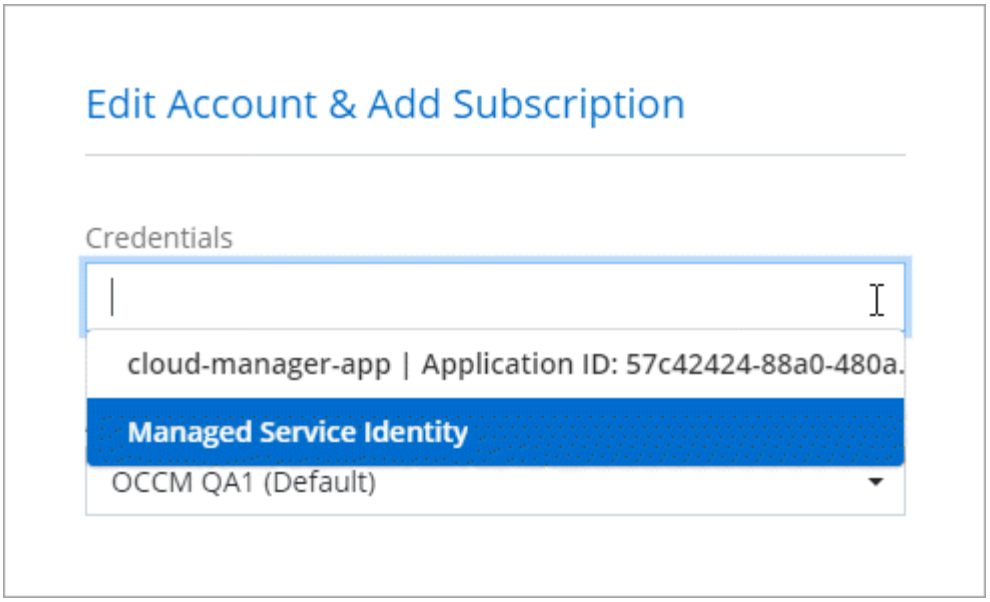
Credenziali Azure aggiuntive

Se si desidera implementare Cloud Volumes ONTAP utilizzando credenziali Azure diverse, 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 "Aggiungere le credenziali dell'account a Cloud Manager" Fornendo dettagli sull'identità del servizio ad.

Dopo aver aggiunto un altro set di credenziali, è possibile passare a queste quando si crea un nuovo ambiente di lavoro:



E le implementazioni di Marketplace e on-premise?

Le sezioni precedenti descrivono il metodo di implementazione consigliato per il connettore, che proviene da NetApp Cloud Central. È inoltre possibile implementare un connettore in Azure da "Azure Marketplace"e puoi farlo "Installare il connettore on-premise".

Se si utilizza Marketplace, le autorizzazioni vengono fornite nello stesso modo. È sufficiente creare e configurare manualmente l'identità gestita per il connettore, quindi fornire le autorizzazioni per eventuali account aggiuntivi.

Per le implementazioni on-premise, non è possibile impostare un'identità gestita per il connettore, ma è possibile fornire autorizzazioni esattamente come per gli account aggiuntivi utilizzando un'entità del servizio.

Gestione delle credenziali e delle sottoscrizioni di Azure per Cloud Manager

Quando si crea un sistema Cloud Volumes ONTAP, è necessario selezionare le credenziali Azure e l'abbonamento Marketplace da utilizzare con tale sistema. Se si gestiscono più sottoscrizioni Azure Marketplace, è possibile assegnarle a diverse credenziali Azure dalla pagina credenziali.

Esistono due modi per gestire le credenziali Azure in Cloud Manager. Innanzitutto, se si desidera implementare Cloud Volumes ONTAP in diversi account Azure, è necessario fornire le autorizzazioni necessarie e aggiungere le credenziali a Cloud Manager. Il secondo metodo consiste nell'associare sottoscrizioni aggiuntive all'identità gestita da Azure.

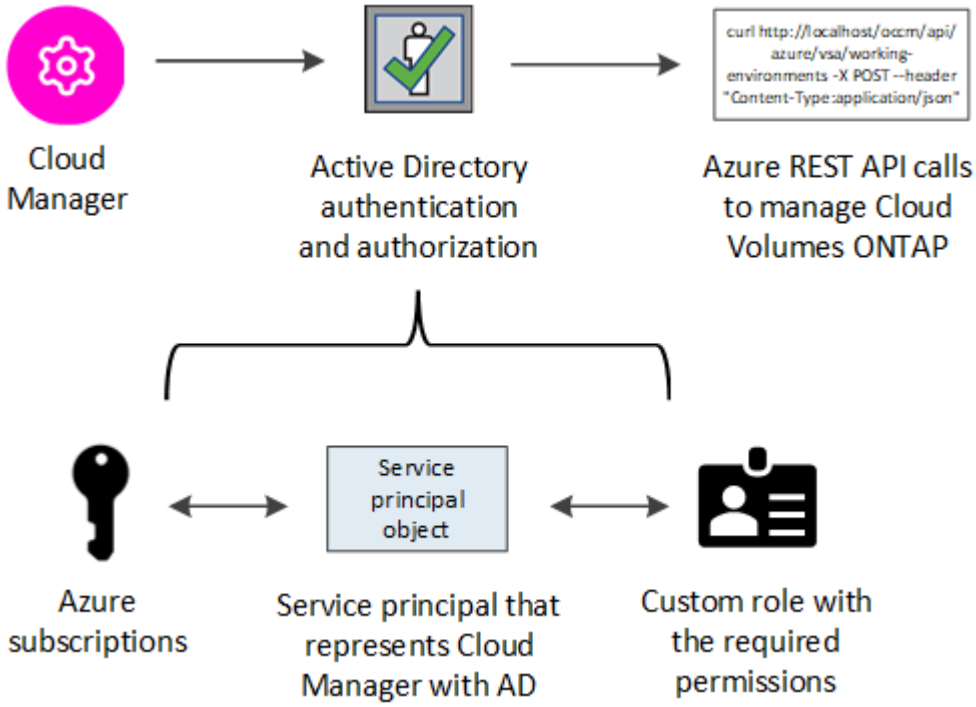
Quando si implementa un connettore da Cloud Manager, Cloud Manager aggiunge automaticamente l'account Azure in cui è stato implementato il connettore. Se il software Connector è stato installato manualmente su un sistema esistente, non viene aggiunto un account iniziale. "Scopri gli account e le autorizzazioni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

Concessione delle autorizzazioni di Azure mediante un'entità del servizio

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

A proposito di questa attività

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



Fasi

1. Creare un'applicazione Azure Active Directory.
2. Assegnare l'applicazione a un ruolo.
3. Aggiungere le autorizzazioni API per la gestione dei servizi Windows Azure.
4. Ottenere l'ID dell'applicazione e l'ID della directory.
5. Creare un client segreto.

Creazione di un'applicazione Azure Active Directory

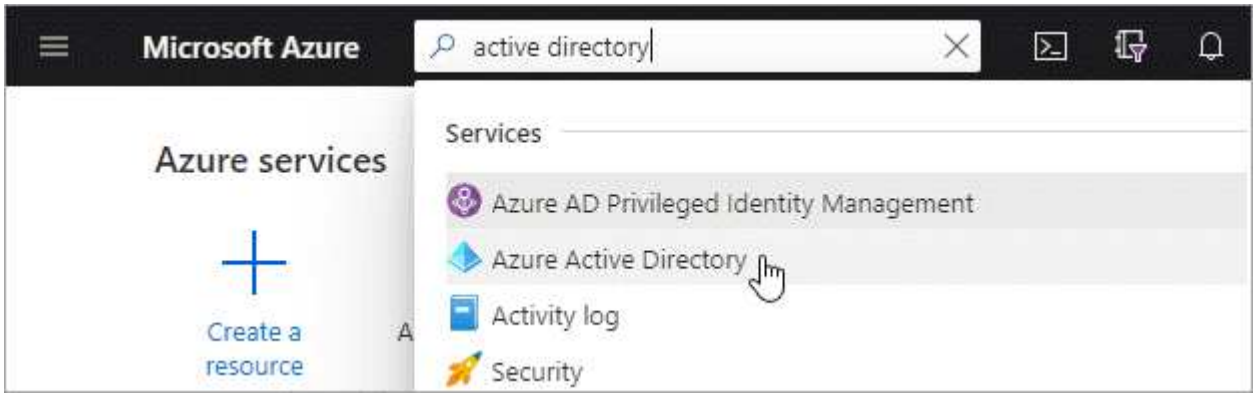
Creare un'applicazione e un service principal Azure Active Directory (ad) che Cloud Manager può utilizzare per il controllo degli accessi in base al ruolo.

Prima di iniziare

Per creare un'applicazione Active Directory e assegnarla a un ruolo, è necessario disporre delle autorizzazioni appropriate in Azure. Per ulteriori informazioni, fare riferimento a. "Documentazione di Microsoft Azure: Autorizzazioni richieste".

Fasi

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



2. Nel menu, fare clic su **App Registrations**.
3. Fare clic su **Nuova registrazione**.
4. Specificare i dettagli dell'applicazione:
   - **Nome**: Immettere un nome per l'applicazione.
   - **Tipo di account**: Selezionare un tipo di account (qualsiasi verrà utilizzato con Cloud Manager).
   - **Redirect URI** (reindirizzamento URI): Selezionare **Web** e inserire un URL qualsiasi, ad esempio https://url
5. Fare clic su **Registra**.

Risultato

Hai creato l'applicazione ad e il service principal.

Assegnazione dell'applicazione a un ruolo

È necessario associare l'entità del servizio a una o più sottoscrizioni Azure e assegnarle il ruolo personalizzato di "operatore cloud manager OnCommand" in modo che quest'ultimo disponga delle autorizzazioni.

Fasi

1. Creare un ruolo personalizzato:

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

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

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

   Esempio

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

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

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

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Ora dovresti avere un ruolo personalizzato chiamato *Cloud Manager Operator*.

2. Assegnare l'applicazione al ruolo:

   a. Dal portale Azure, aprire il servizio **Subscriptions**.

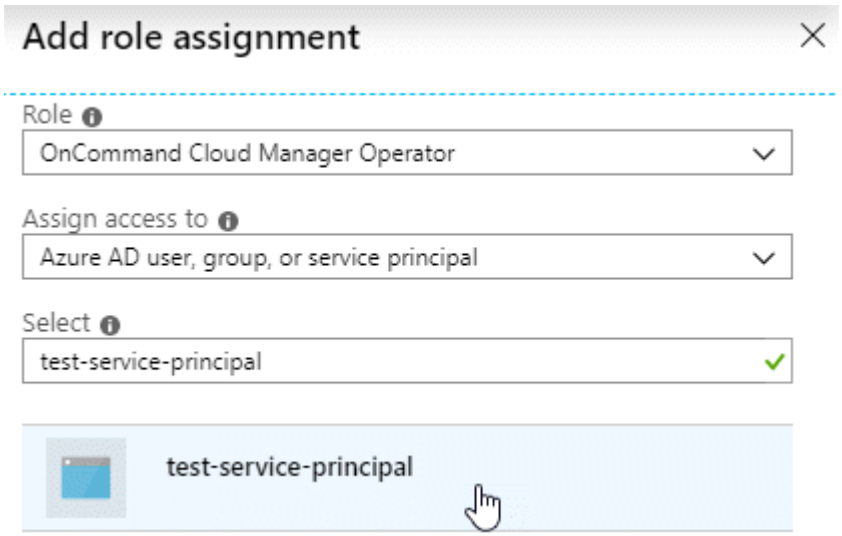
   b. Selezionare l'abbonamento.

   c. Fare clic su **Access control (IAM) > Add > Add role assignment** (controllo accesso (IAM) > Add > Add role assign

   d. Selezionare il ruolo **Cloud Manager Operator**.

   e. Mantieni selezionata l'opzione **Azure ad user, group o service principal**.

   f. Cercare il nome dell'applicazione (non è possibile trovarla nell'elenco scorrendo).



   g. Selezionare l'applicazione e fare clic su **Save** (Salva).

      Il service principal per Cloud Manager dispone ora delle autorizzazioni Azure necessarie per tale abbonamento.

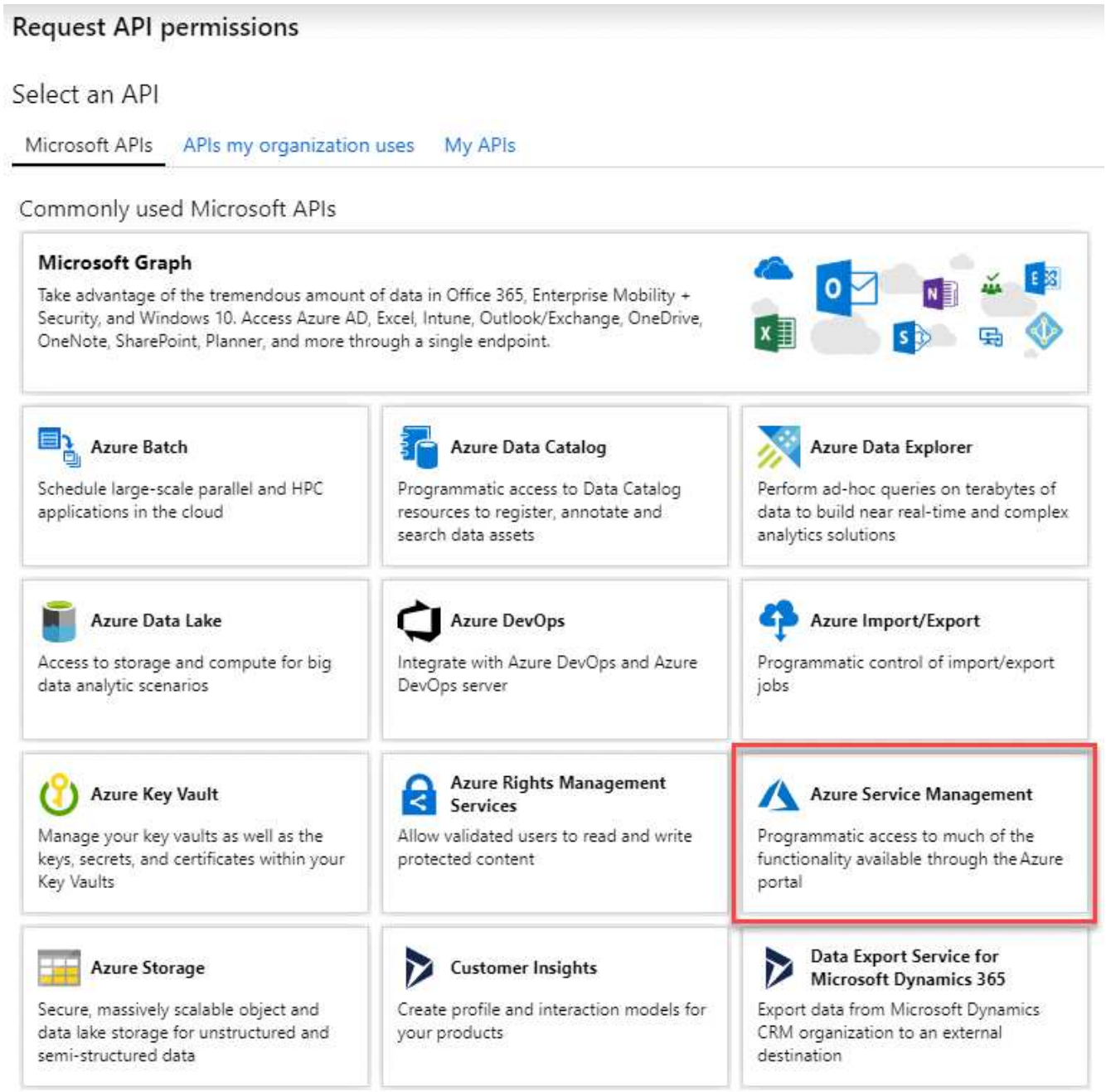
Se si desidera implementare Cloud Volumes ONTAP da più sottoscrizioni Azure, è necessario associare l'entità del servizio a ciascuna di queste sottoscrizioni. Cloud Manager consente di selezionare l'abbonamento che si desidera utilizzare durante l'implementazione di Cloud Volumes ONTAP.

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

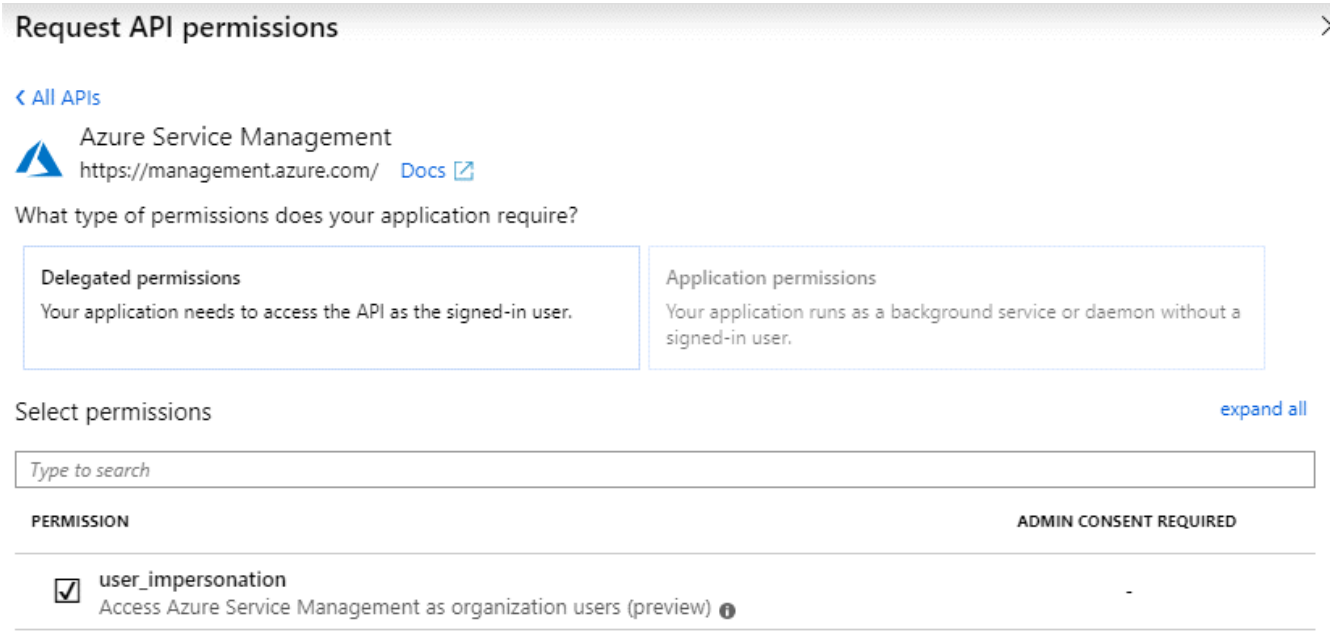
L'entità del servizio deve disporre delle autorizzazioni "API di gestione dei servizi Windows Azure".

Fasi

1. Nel servizio **Azure Active Directory**, fare clic su **App Registrations** e selezionare l'applicazione.
2. Fare clic su **API permissions > Add a permission** (autorizzazioni API > Aggiungi autorizzazione)
3. In **Microsoft API**, selezionare **Azure Service Management**.



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

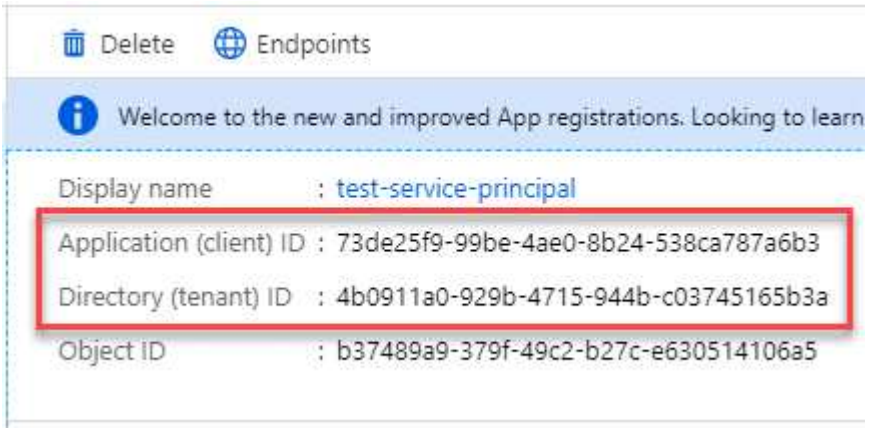


Ottenere l'ID dell'applicazione e l'ID della directory

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

Fasi

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



Creazione di un client segreto

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

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

Fasi

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

Risultato

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

Aggiunta di credenziali Azure a Cloud Manager

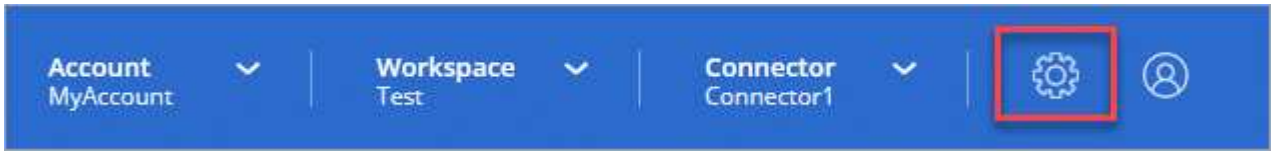
Dopo aver fornito un account Azure con le autorizzazioni richieste, è possibile aggiungere le credenziali per tale account a Cloud Manager. Ciò consente di avviare i sistemi Cloud Volumes ONTAP in tale account.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

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



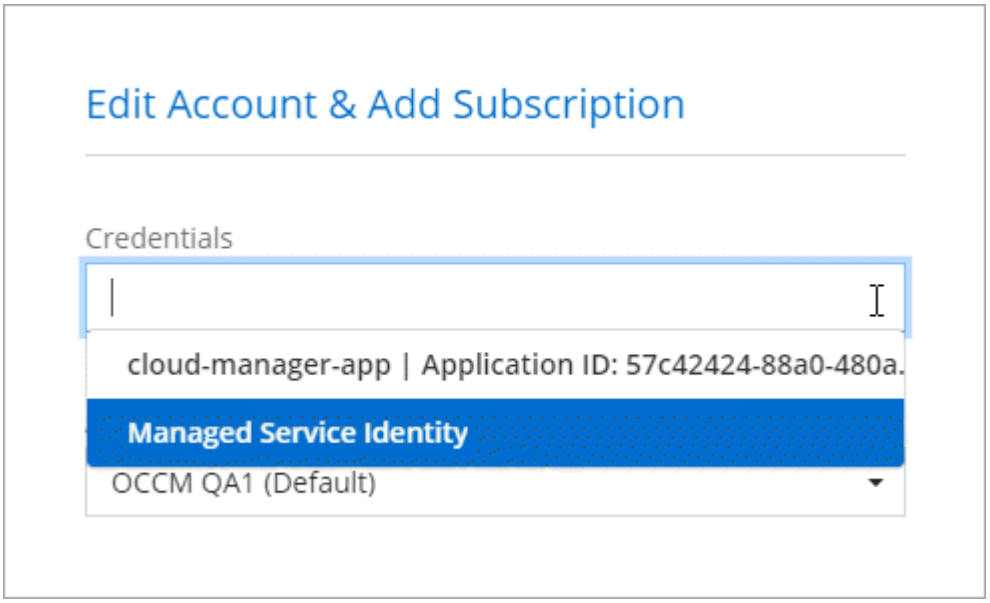
2. Fare clic su **Aggiungi credenziali** e selezionare **Microsoft Azure**.
3. Immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
   - ID applicazione (client): Vedere Ottenere l'ID dell'applicazione e l'ID della directory.
   - ID directory (tenant): Vedere Ottenere l'ID dell'applicazione e l'ID della directory.
   - Segreto del client: Vedere Creazione di un client segreto.
4. Confermare che i requisiti della policy sono stati soddisfatti, quindi fare clic su **continua**.
5. Scegli l'abbonamento pay-as-you-go che desideri associare alle credenziali o fai clic su **Aggiungi abbonamento** se non ne hai ancora uno.

Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, le credenziali Azure devono essere associate a un abbonamento a Cloud Volumes ONTAP da Azure Marketplace.

6. Fare clic su **Aggiungi**.

Risultato

È ora possibile passare a un set di credenziali diverso dalla pagina Dettagli e credenziali "quando si crea un nuovo ambiente di lavoro":



Associazione di un abbonamento a Azure Marketplace alle credenziali

Dopo aver aggiunto le tue credenziali Azure a Cloud Manager, puoi associare un abbonamento a Azure Marketplace a tali credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

Esistono due scenari in cui è possibile associare un abbonamento a Azure Marketplace dopo aver aggiunto le credenziali a Cloud Manager:

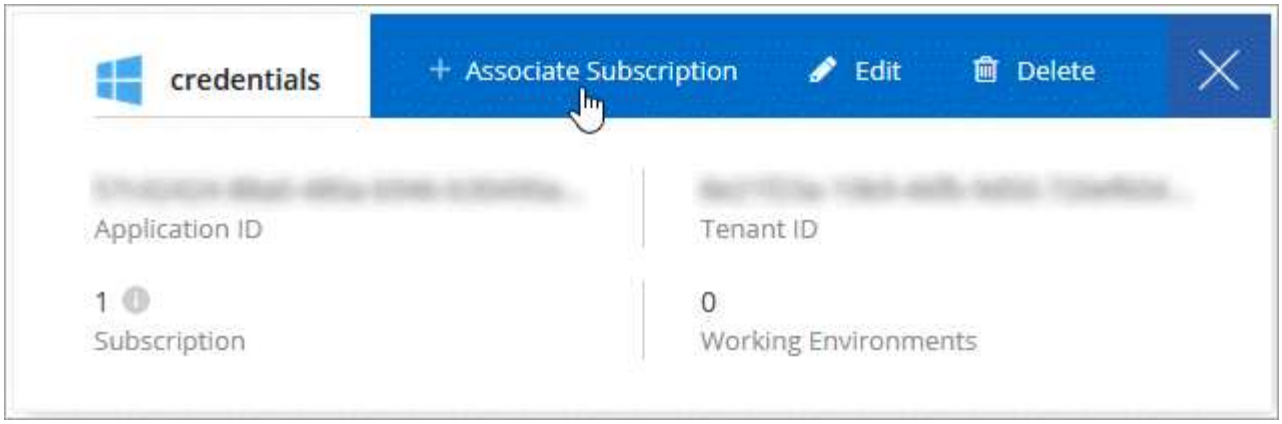
- Non hai associato un abbonamento quando inizialmente hai aggiunto le credenziali a Cloud Manager.
- Si desidera sostituire un abbonamento a Azure Marketplace esistente con un nuovo abbonamento.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Passare il mouse su un set di credenziali e fare clic sul menu delle azioni.
3. Dal menu, fare clic su **Associa abbonamento**.



4. Selezionare un abbonamento dall'elenco a discesa oppure fare clic su **Aggiungi abbonamento** e seguire la procedura per creare un nuovo abbonamento.

   Il seguente video inizia dal contesto della procedura guidata dell'ambiente di lavoro, ma mostra lo stesso flusso di lavoro dopo aver fatto clic su **Add Subscription** (Aggiungi abbonamento):

   ► https://docs.netapp.com/it-it/occm38//media/video_subscribing_azure.mp4 *(video)*

Associazione di sottoscrizioni Azure aggiuntive a un'identità gestita

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

A proposito di questa attività

Un'identità gestita è "L'account Azure iniziale" Quando si implementa un connettore da Cloud Manager. Quando hai implementato il connettore, Cloud Manager ha creato il ruolo Cloud Manager Operator e lo ha assegnato alla macchina virtuale del connettore.

Fasi

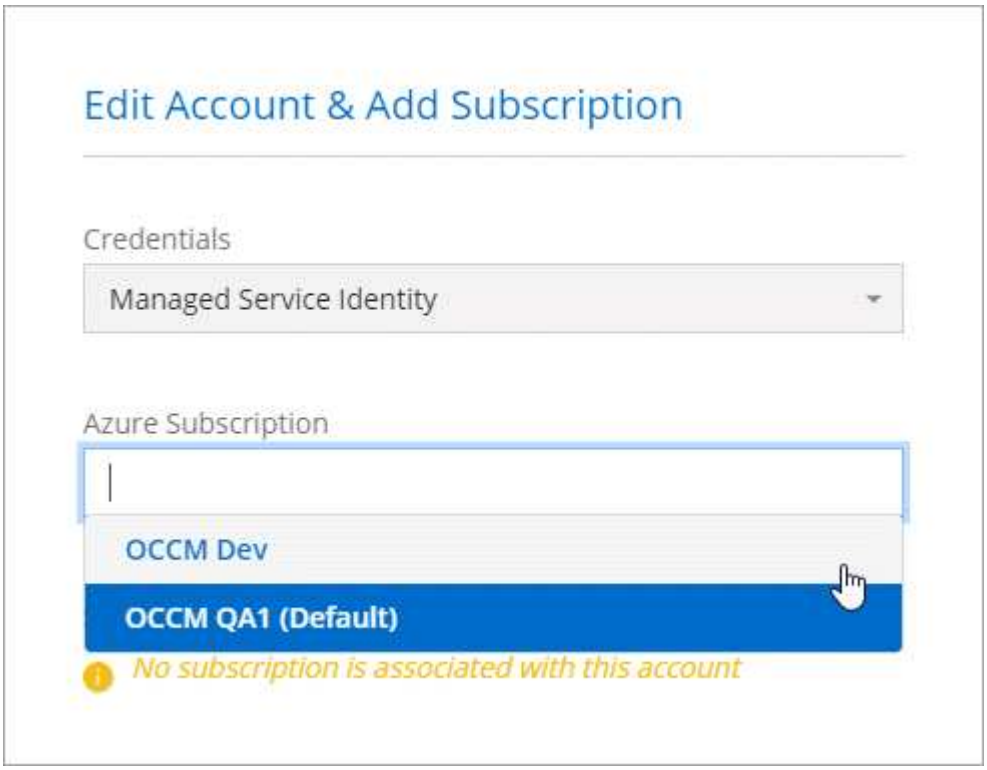
1. Accedere al portale Azure.
2. Aprire il servizio **Abbonamenti** e selezionare l'abbonamento in cui si desidera implementare Cloud Volumes ONTAP.
3. Fare clic su **controllo di accesso (IAM)**.
   a. Fare clic su **Aggiungi** > **Aggiungi assegnazione ruolo** e aggiungere le autorizzazioni:
     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

        Cloud Manager Operator 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 Connector.
      - Selezionare la macchina virtuale Connector.
      - 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.



GCP

Progetti, autorizzazioni e account Google Cloud

Un account di servizio fornisce a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP nello stesso progetto di Cloud Manager o in progetti diversi.

Progetto e permessi per Cloud Manager

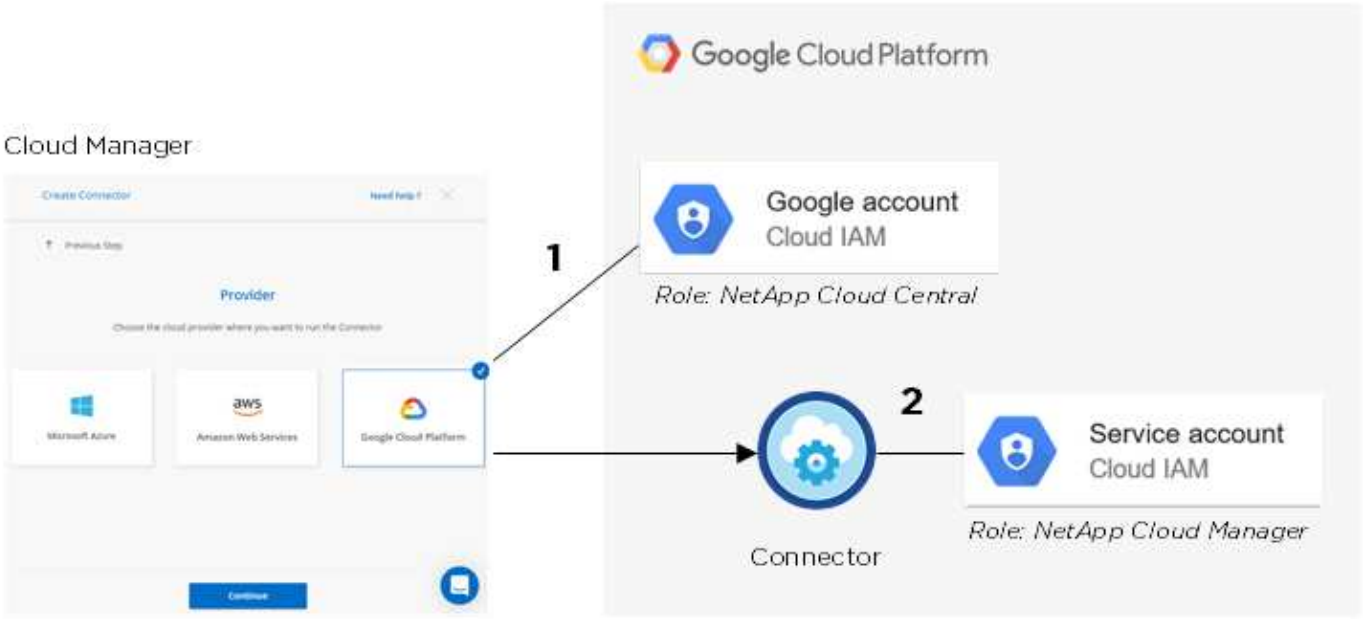
Prima di poter implementare Cloud Volumes ONTAP in Google Cloud, devi prima implementare un connettore in un progetto Google Cloud. Il connettore non può essere in esecuzione in sede o in un altro cloud provider.

Prima di implementare un connettore direttamente da Cloud Manager, è necessario disporre di due set di autorizzazioni:

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

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

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



Progetto per Cloud Volumes ONTAP

Cloud Volumes ONTAP può risiedere nello stesso progetto del connettore o in un progetto diverso. Per implementare Cloud Volumes ONTAP in un progetto diverso, è necessario prima aggiungere l'account e il ruolo del servizio Connector a tale progetto.

- "Informazioni su come configurare l'account di servizio (vedere il passaggio 2)".
- "Scopri come implementare Cloud Volumes ONTAP in GCP e selezionare un progetto".

Account per il tiering dei dati

Cloud Manager richiede un account GCP per Cloud Volumes ONTAP 9.6, ma non per la versione 9.7 e successive. Se si desidera utilizzare il tiering dei dati con Cloud Volumes ONTAP 9.7, seguire il passaggio 4 in "Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google".

Per abilitare il tiering dei dati su un sistema Cloud Volumes ONTAP 9.6, è necessario aggiungere un account Google Cloud a Cloud Manager. Il tiering dei dati esegue automaticamente il tiering dei dati cold in uno storage a oggetti a basso costo, consentendoti di recuperare spazio sullo storage primario e ridurre lo storage secondario.

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

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

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

Gestione delle credenziali GCP e delle sottoscrizioni per Cloud Manager

È possibile gestire due tipi di credenziali di Google Cloud Platform da Cloud Manager: Le

credenziali associate all'istanza di Connector VM e le chiavi di accesso allo storage utilizzate con un sistema Cloud Volumes ONTAP 9.6 per "tiering dei dati".

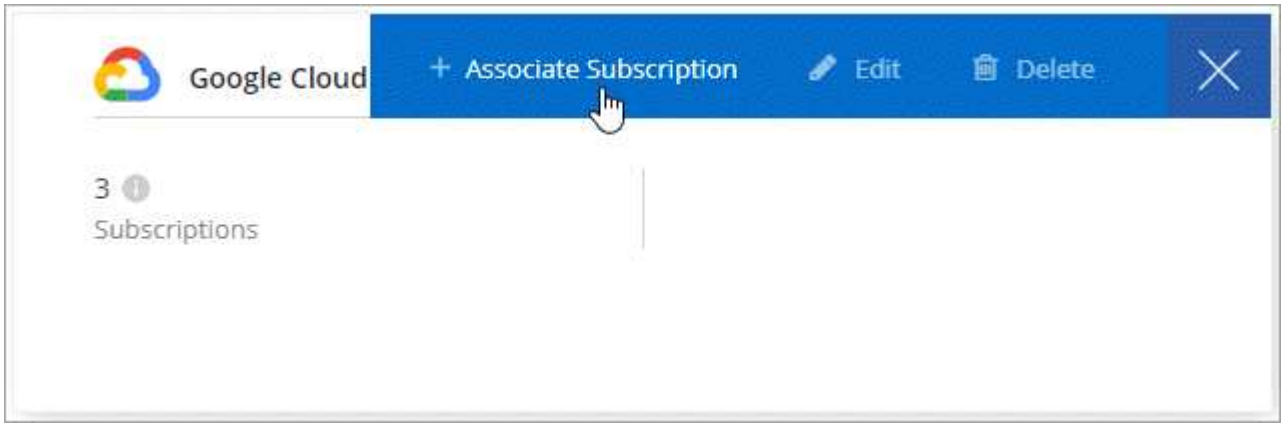
Associazione di un abbonamento a Marketplace con le credenziali GCP

Quando si implementa un connettore in GCP, Cloud Manager crea un set predefinito di credenziali associate all'istanza della macchina virtuale del connettore. Queste sono le credenziali utilizzate da Cloud Manager per implementare Cloud Volumes ONTAP.

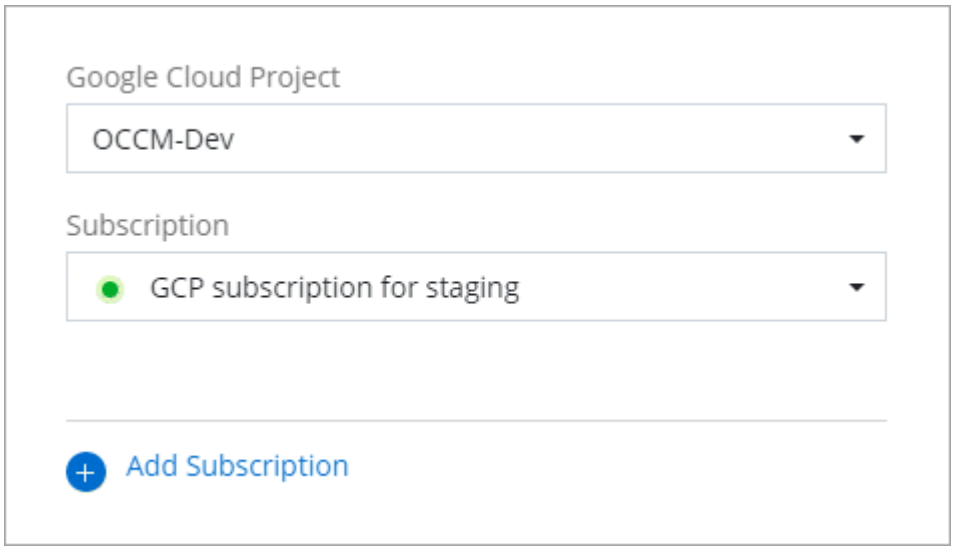
In qualsiasi momento, è possibile modificare l'abbonamento Marketplace associato a queste credenziali. L'abbonamento consente di creare un sistema Cloud Volumes ONTAP pay-as-you-go e di utilizzare altri servizi cloud NetApp.

Fasi

1. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.
2. Passare il mouse su un set di credenziali e fare clic sul menu delle azioni.
3. Dal menu, fare clic su **Associa abbonamento**.



4. Seleziona un progetto Google Cloud e un abbonamento dall'elenco a discesa oppure fai clic su **Aggiungi abbonamento** e segui la procedura per creare un nuovo abbonamento.



5. Fare clic su **Associa**.

Impostazione e aggiunta di account GCP per il tiering dei dati con Cloud Volumes ONTAP 9.6

Se si desidera attivare un sistema Cloud Volumes ONTAP 9.6 per "tiering dei dati", È necessario fornire a Cloud Manager una chiave di accesso allo storage per un account di servizio che dispone delle autorizzazioni Storage Admin. Cloud Manager utilizza le chiavi di accesso per configurare e gestire un bucket di cloud storage per il tiering dei dati.

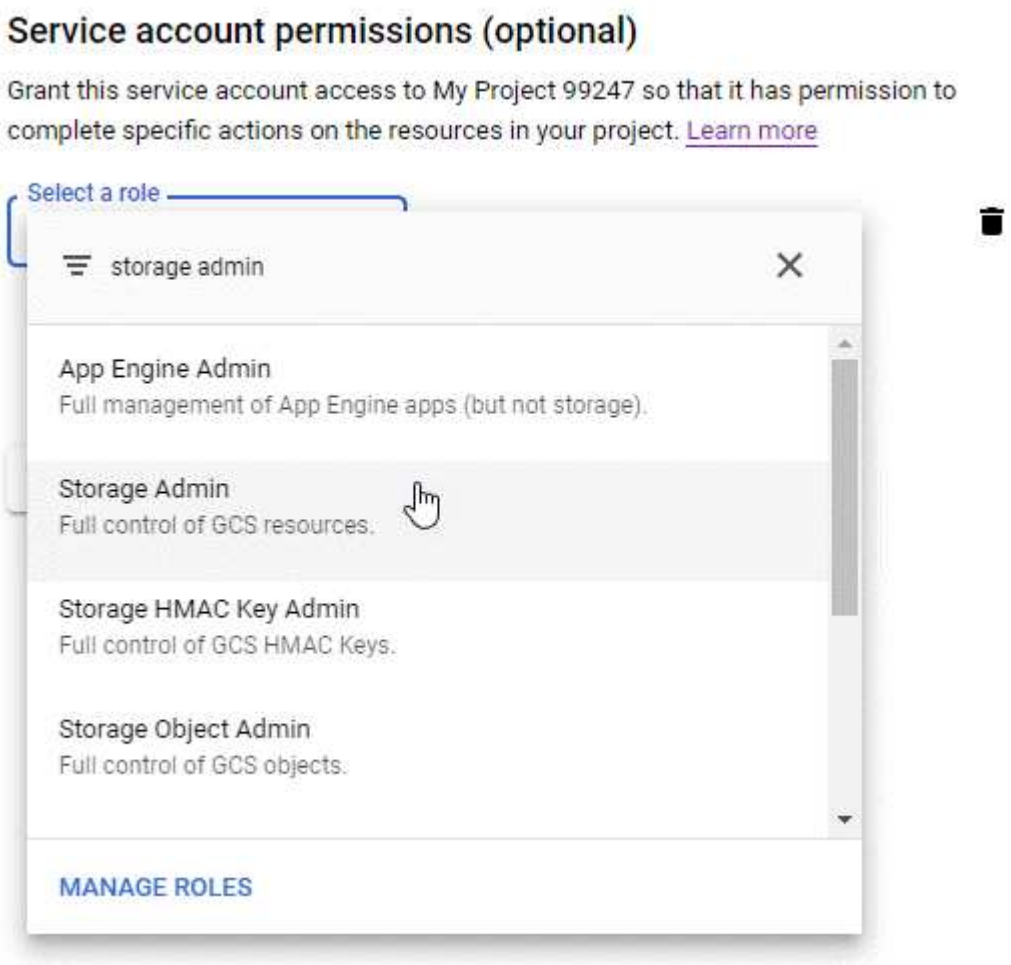
Se si desidera utilizzare il tiering dei dati con Cloud Volumes ONTAP 9.7, seguire il passaggio 4 in "Introduzione a Cloud Volumes ONTAP nella piattaforma cloud di Google".

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

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

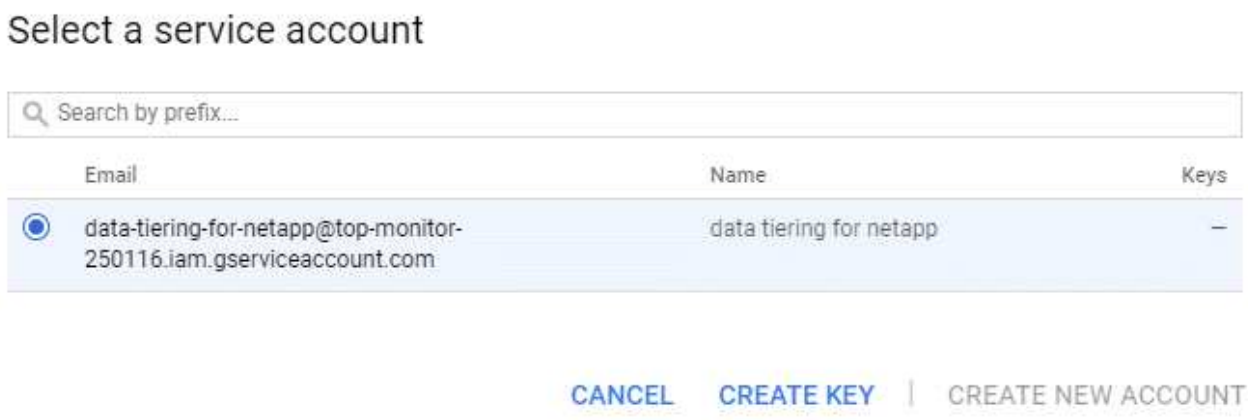
Fasi

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



2. Passare a. "Impostazioni storage GCP".
3. Se richiesto, selezionare un progetto.
4. Fare clic sulla scheda **interoperabilità**.
5. Se non è già stato fatto, fare clic su **Enable Interoperability access** (attiva accesso all'interoperabilità).

6. In **chiavi di accesso per gli account di servizio**, fare clic su **Crea una chiave per un account di servizio**.
7. Selezionare l'account di servizio creato al punto 1.



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

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

Aggiunta di un account GCP a Cloud Manager

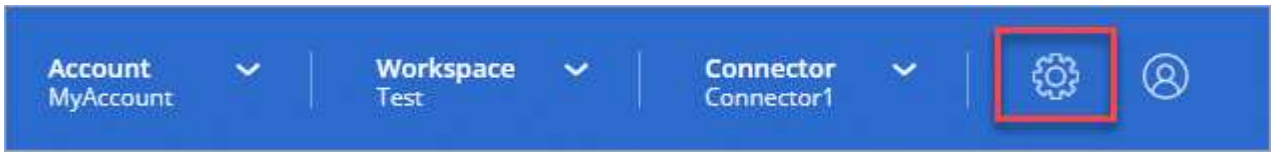
Ora che si dispone di una chiave di accesso per un account di servizio, è possibile aggiungerla a Cloud Manager.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

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



2. Fare clic su **Aggiungi credenziali** e selezionare **Google Cloud**.
3. Inserire la chiave di accesso e il segreto per l'account del servizio.

   Le chiavi consentono a Cloud Manager di configurare un bucket di cloud storage per il tiering dei dati.

4. Verificare che i requisiti della policy siano stati soddisfatti, quindi fare clic su **Create account** (Crea account).

Quali sono le prossime novità?

È ora possibile attivare il tiering dei dati su singoli volumi su un sistema Cloud Volumes ONTAP 9.6 quando vengono creati, modificati o replicati. Per ulteriori informazioni, vedere "Tiering dei dati inattivi su storage a

oggetti a basso costo".

Prima di procedere, assicurarsi che la subnet in cui risiede Cloud Volumes ONTAP sia configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access".

Aggiunta di account NetApp Support Site a Cloud Manager

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

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

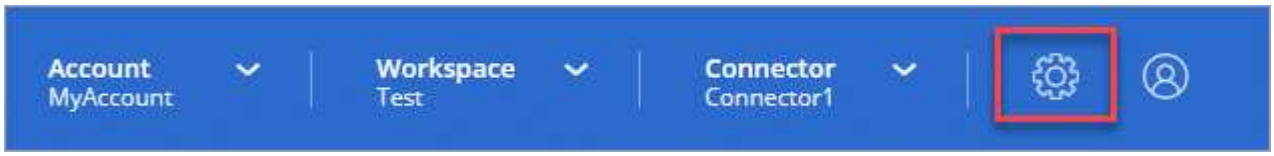
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

1. Se non disponi ancora di un account NetApp Support Site, "registratevi per uno".
2. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **credenziali**.



3. Fare clic su **Aggiungi credenziali** e selezionare **NetApp Support Site**.
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"

Gestione di utenti, aree di lavoro, connettori e sottoscrizioni

"Dopo aver eseguito la configurazione iniziale", Potrebbe essere necessario amministrare le impostazioni dell'account in un secondo momento gestendo utenti, aree di lavoro, connettori e sottoscrizioni.

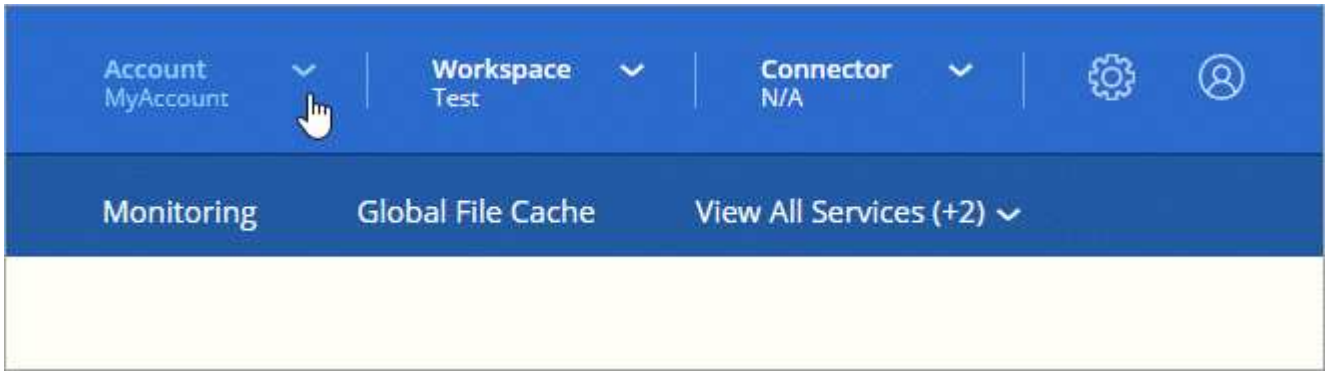
"Scopri di più sul funzionamento degli account Cloud Central".

Aggiunta di utenti

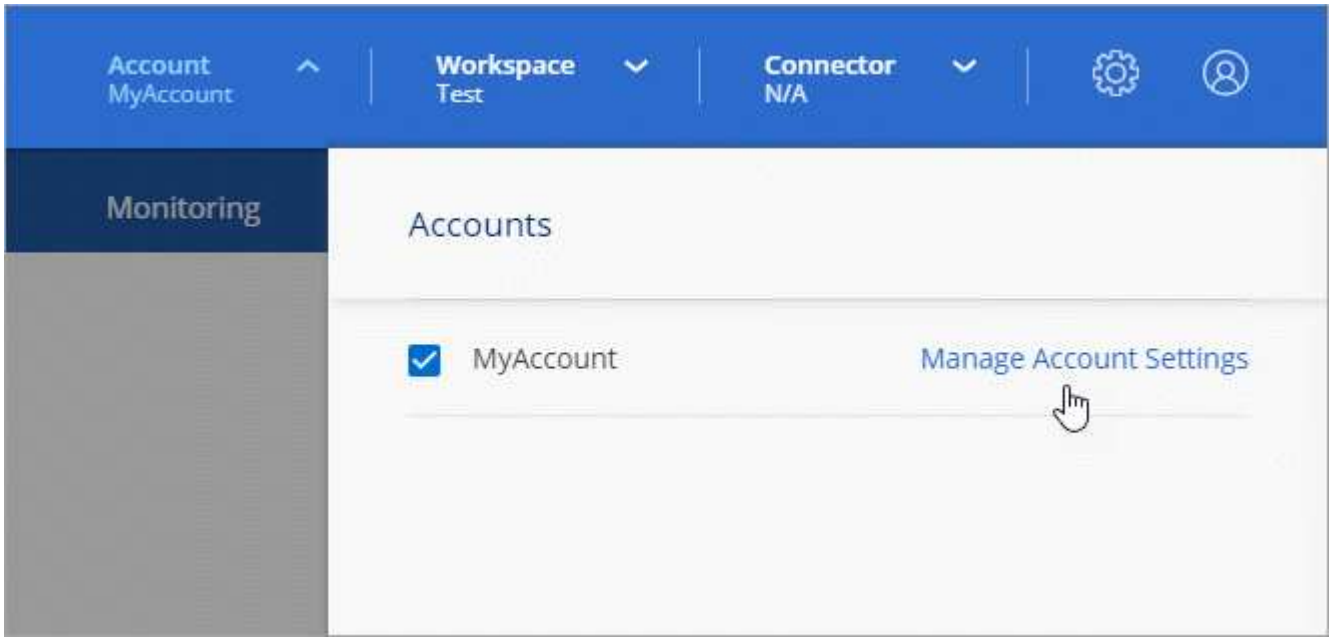
Associa gli utenti di Cloud Central all'account Cloud Central in modo che questi utenti possano creare e gestire ambienti di lavoro in Cloud Manager.

Fasi

1. Se l'utente non l'ha già fatto, chiedere all'utente di accedere a. "NetApp Cloud Central" e iscriverti.
2. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account**.



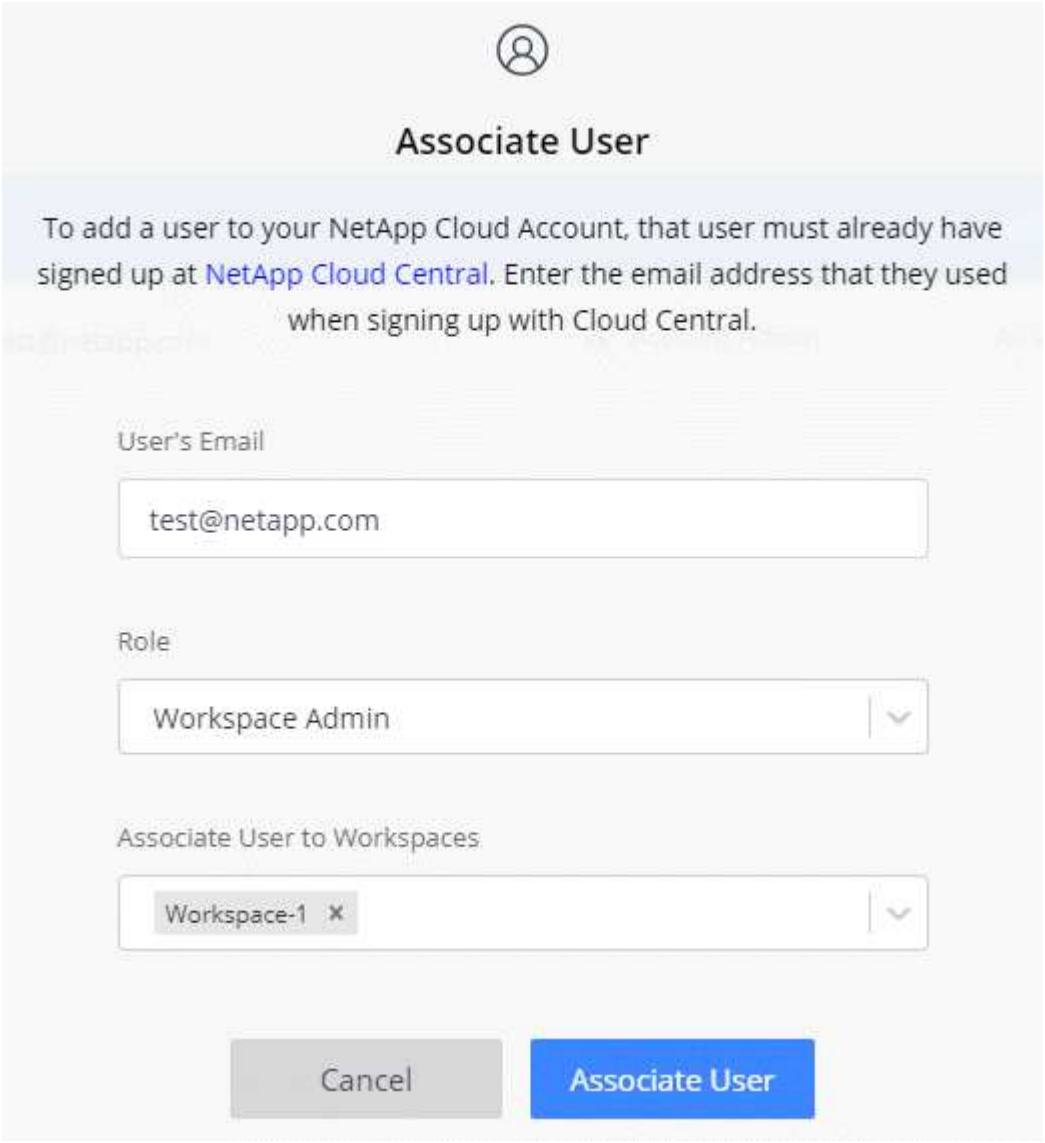
3. Fare clic su **Manage account** (Gestisci account) accanto all'account attualmente selezionato.



4. Dalla scheda Users (utenti), fare clic su **associate User** (Associa utente).
5. Inserire l'indirizzo e-mail dell'utente e selezionare un ruolo per l'utente:

- **Account Admin**: Può eseguire qualsiasi azione in Cloud Manager.
- **Workspace Admin**: Consente di creare e gestire le risorse nelle aree di lavoro assegnate.
- **Compliance Viewer**: È in grado di visualizzare solo le informazioni di conformità e generare report per le aree di lavoro a cui sono autorizzati ad accedere.

6. Se si seleziona Workspace Admin (Amministratore area di lavoro) o Compliance Viewer (Visualizzatore conformità), selezionare una o più aree di lavoro da associare all'utente.



7. Fare clic su **Associa utente**.

Risultato

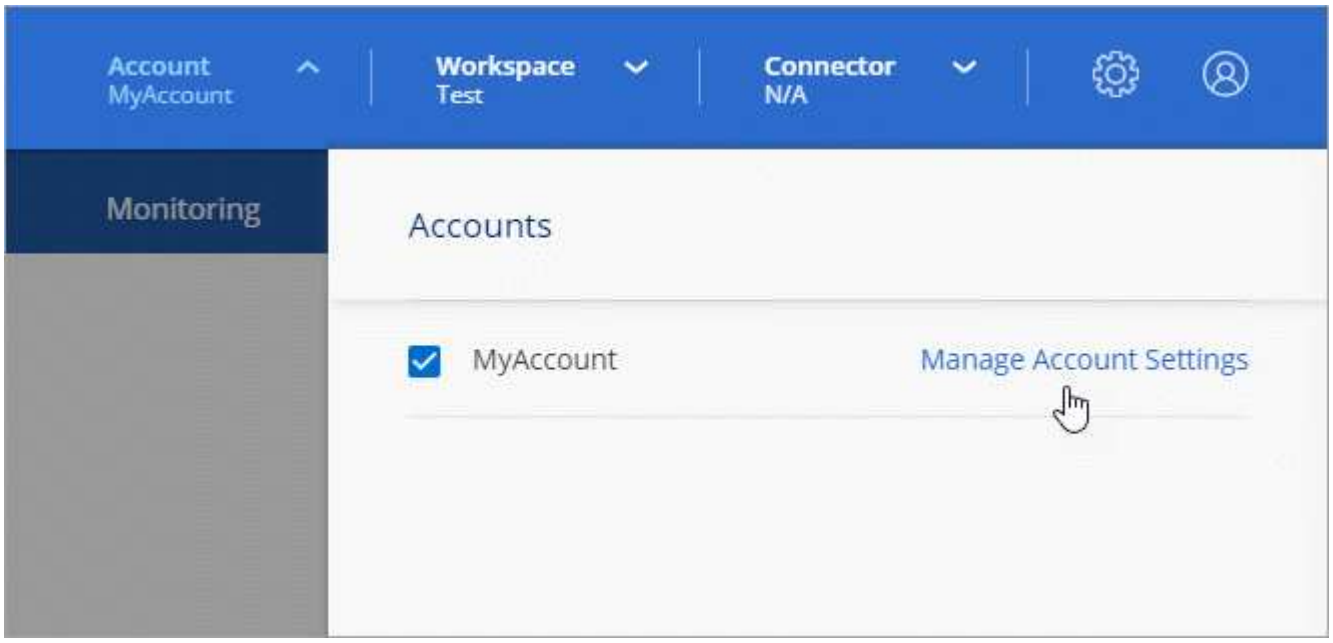
L'utente deve ricevere un'e-mail da NetApp Cloud Central intitolata "account Association". L'e-mail include le informazioni necessarie per accedere a Cloud Manager.

Rimozione degli utenti

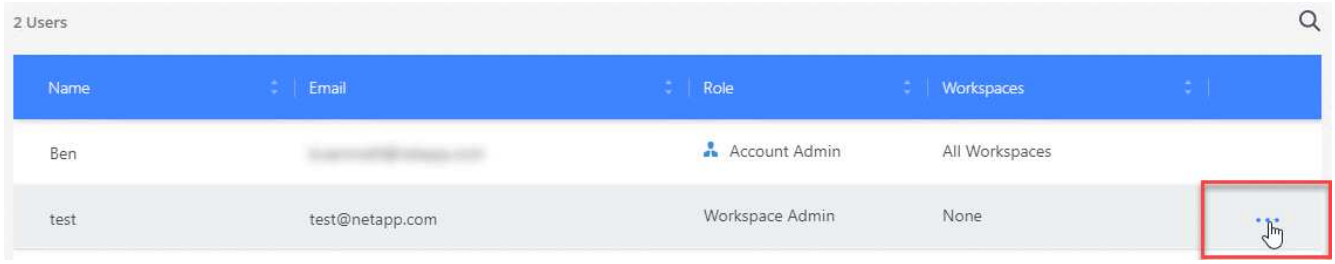
La disassociazione di un utente lo rende in modo che non possa più accedere alle risorse in un account Cloud Central.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Dalla scheda Users (utenti), fare clic sul menu delle azioni nella riga corrispondente all'utente.



3. Fare clic su **dissocia utente** e fare clic su **dissocia** per confermare.

Risultato

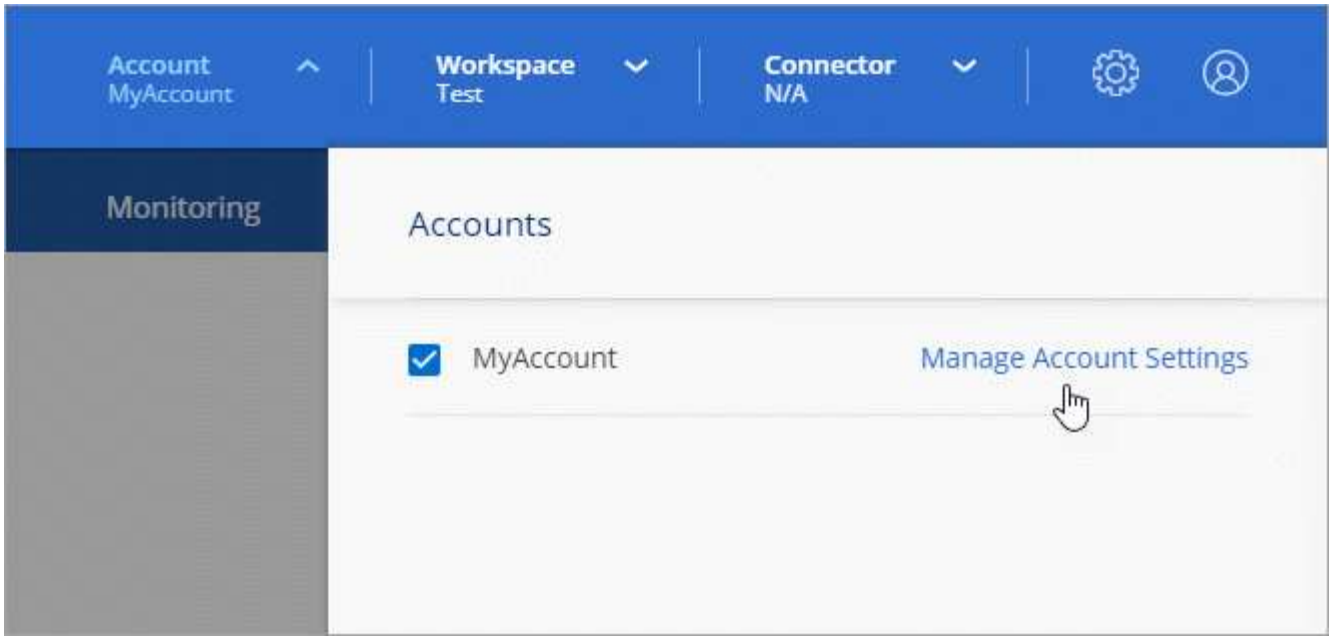
L'utente non può più accedere alle risorse di questo account Cloud Central.

Gestione delle aree di lavoro di un amministratore dell'area di lavoro

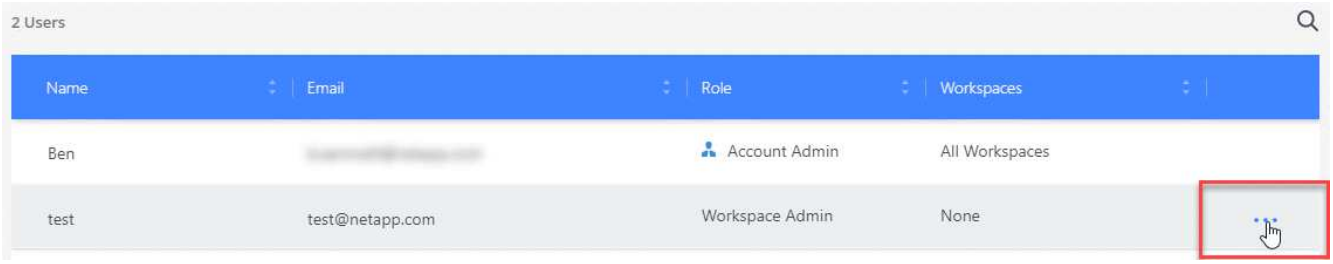
È possibile associare e disassociare gli amministratori Workspace alle aree di lavoro in qualsiasi momento. L'associazione dell'utente consente di creare e visualizzare gli ambienti di lavoro in tale area di lavoro.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).



2. Dalla scheda Users (utenti), fare clic sul menu delle azioni nella riga corrispondente all'utente.



3. Fare clic su **Gestisci aree di lavoro**.
4. Selezionare le aree di lavoro da associare all'utente e fare clic su **Apply** (Applica).

Risultato

L'utente può ora accedere a tali aree di lavoro da Cloud Manager, purché il connettore sia stato associato anche alle aree di lavoro.

Gestione delle aree di lavoro

Gestisci le tue aree di lavoro creando, rinominando ed eliminando le aree di lavoro. Nota: Non è possibile eliminare un'area di lavoro se contiene risorse. Deve essere vuoto.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Workspaces**.
3. Scegliere una delle seguenti opzioni:
   - Fare clic su **Add New Workspace** (Aggiungi nuova area di lavoro) per creare una nuova area di lavoro.
   - Fare clic su **Rename** (Rinomina) per rinominare l'area di lavoro.
   - Fare clic su **Delete** (Elimina) per eliminare l'area di lavoro.

Gestione delle aree di lavoro di un connettore

È necessario associare il connettore alle aree di lavoro in modo che gli amministratori di Workspace possano accedere a tali aree di lavoro da Cloud Manager.

Se si dispone solo di account Admins, non è necessario associare il connettore alle aree di lavoro. Gli amministratori degli account hanno la possibilità di accedere a tutte le aree di lavoro in Cloud Manager per impostazione predefinita.

"Scopri di più su utenti, aree di lavoro e connettori".

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Connector** (connettore).
3. Fare clic su **Manage Workspaces** (Gestisci aree di lavoro) per il connettore che si desidera associare.
4. Selezionare le aree di lavoro da associare al connettore e fare clic su **Apply** (Applica).

Gestione delle sottoscrizioni

Dopo aver effettuato l'iscrizione dal marketplace di un provider cloud, ogni abbonamento è disponibile dal widget Impostazioni account. È possibile rinominare un abbonamento e disassociarlo da uno o più account.

Ad esempio, supponiamo di avere due account e di fatturarvi ciascuno tramite abbonamenti separati. Potresti disassociare un abbonamento da uno degli account, in modo che gli utenti di quell'account non scelgano accidentalmente l'abbonamento sbagliato quando crei un ambiente di lavoro Cloud Volume ONTAP.

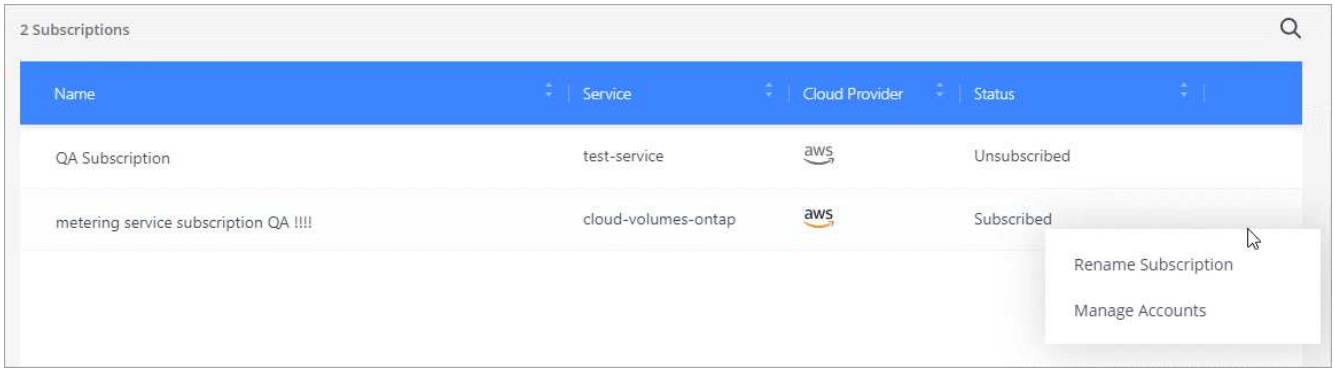
"Scopri di più sugli abbonamenti".

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Fare clic su **Abbonamenti**.

   Verranno visualizzati solo gli abbonamenti associati all'account attualmente visualizzato.

3. Fare clic sul menu delle azioni nella riga corrispondente all'abbonamento che si desidera gestire.



4. Scegliere di rinominare l'abbonamento o di gestire gli account associati all'abbonamento.

Modifica del nome dell'account

Modificare il nome dell'account in qualsiasi momento per modificarlo in un elemento significativo per l'utente.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Nella scheda **Panoramica**, fare clic sull'icona di modifica accanto al nome dell'account.
3. Digitare un nuovo nome account e fare clic su **Salva**.

Attivazione o disattivazione della piattaforma SaaS

Si consiglia di non disattivare la piattaforma SaaS a meno che non sia necessario per rispettare le policy di sicurezza della propria azienda. La disattivazione della piattaforma SaaS limita la tua capacità di utilizzare i servizi cloud integrati di NetApp.

I seguenti servizi non sono disponibili da Cloud Manager se si disattiva la piattaforma SaaS:

- Conformità al cloud
- Kubernetes
- Tiering nel cloud
- Global file cache
- Monitoraggio (Cloud Insights)

Fasi

1. Nella parte superiore di Cloud Manager, fare clic sull'elenco a discesa **account** e fare clic su **Manage account** (Gestisci account).
2. Nella scheda **Panoramica**, attivare l'opzione Usa la piattaforma SaaS.

Gestione 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.

Prima di iniziare

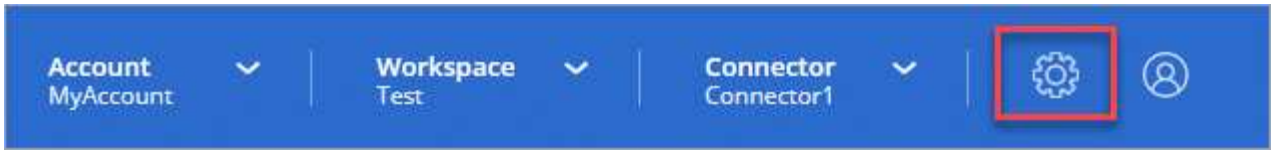
È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Installazione di un certificato HTTPS

Installare un certificato firmato da una CA per un accesso sicuro.

Fasi

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

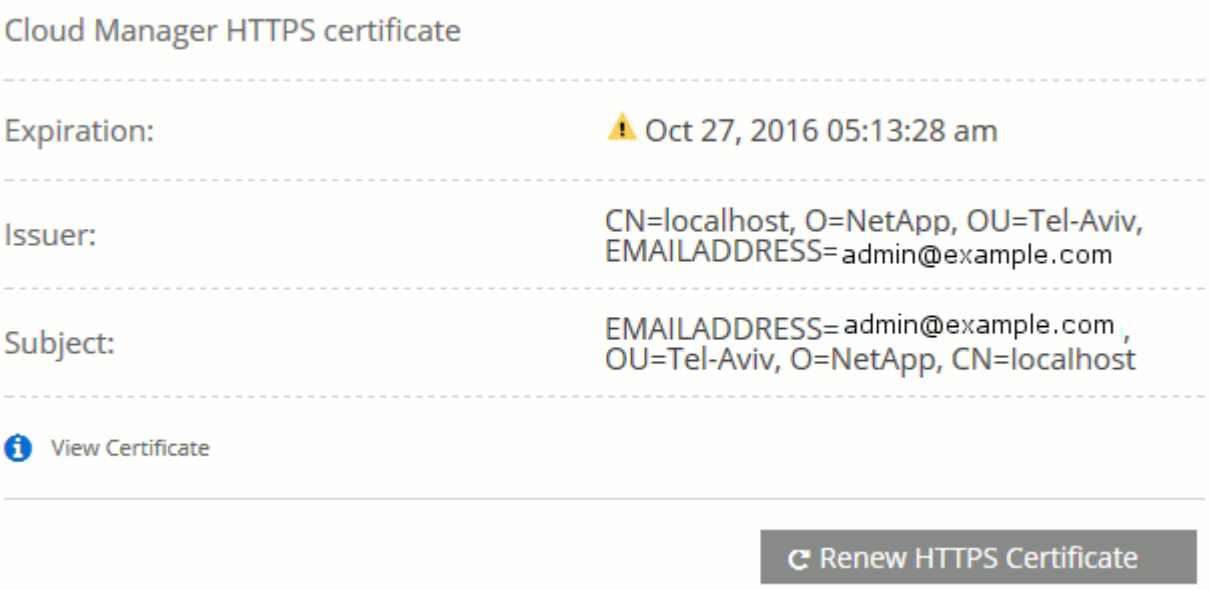


2. Nella pagina HTTPS Setup (Configurazione HTTPS), installare un certificato generando una richiesta di firma del certificato (CSR) o installando il proprio certificato firmato dalla CA:

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

Risultato

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



Rinnovo del certificato HTTPS di Cloud Manager

È necessario rinnovare il certificato HTTPS di Cloud Manager prima della scadenza per garantire un accesso sicuro alla console Web di Cloud Manager. Se il certificato non viene rinnovato prima della scadenza, viene visualizzato un avviso quando gli utenti accedono alla console Web utilizzando HTTPS.

Fasi

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

   Vengono visualizzati i dettagli del certificato Cloud Manager, inclusa la data di scadenza.

2. Fare clic su **Renew HTTPS Certificate** (Rinnova certificato HTTPS) e seguire la procedura per generare una CSR o installare un certificato CA personalizzato.

Risultato

Cloud Manager utilizza il nuovo certificato firmato dalla CA per fornire un accesso HTTPS sicuro.

Rimozione degli ambienti di lavoro Cloud Volumes ONTAP

L'amministratore dell'account può rimuovere un ambiente di lavoro Cloud Volumes ONTAP per spostarlo in un altro sistema o per risolvere i problemi di rilevamento.

A proposito di questa attività

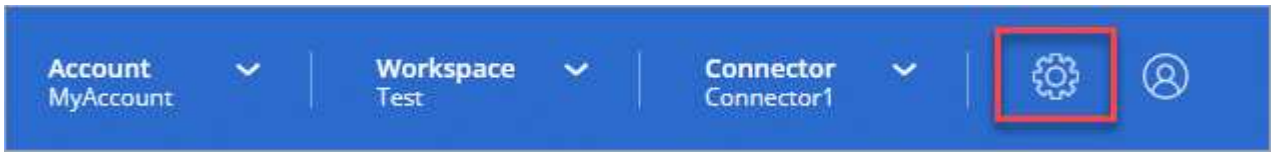
La rimozione di un ambiente di lavoro Cloud Volumes ONTAP lo rimuove da Cloud Manager. Non elimina il sistema Cloud Volumes ONTAP. In seguito, sarà possibile riscoprire l'ambiente di lavoro.

La rimozione di un ambiente di lavoro da Cloud Manager consente di effettuare le seguenti operazioni:

- Riscoprirla in un altro spazio di lavoro
- Riscoprilo da un altro sistema Cloud Manager
- Riscoprirla se si sono verificati problemi durante il rilevamento iniziale

Fasi

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



2. Dalla pagina Tools (Strumenti), fare clic su **Launch** (Avvia).
3. Selezionare l'ambiente di lavoro Cloud Volumes ONTAP che si desidera rimuovere.
4. Nella pagina Review and Approve (esamina e approva), fare clic su **Go** (Vai).

Risultato

Cloud Manager rimuove l'ambiente di lavoro. Gli utenti possono riscoprire questo ambiente di lavoro dalla pagina ambienti di lavoro in qualsiasi momento.

Configurazione di un connettore per l'utilizzo di un server proxy

Se le policy aziendali stabiliscono che si utilizza un server proxy per tutte le comunicazioni HTTP a Internet, è necessario configurare i connettori in modo che utilizzino tale server proxy. Il server proxy può trovarsi nel cloud o nella rete.

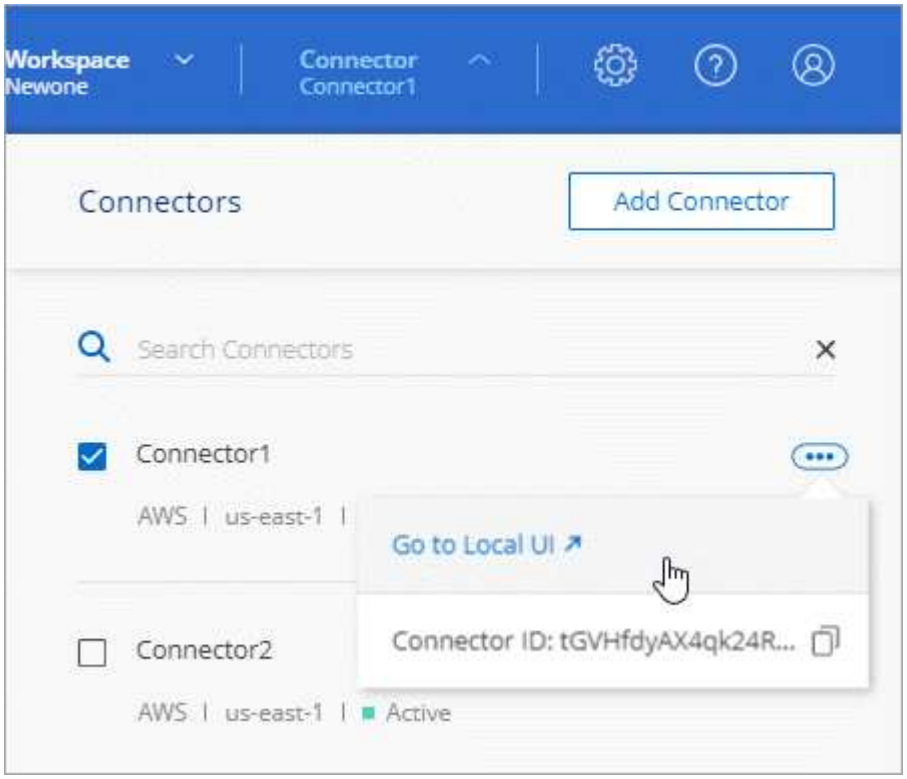
Quando si configura un connettore per l'utilizzo di un server proxy, il connettore e i sistemi Cloud Volumes ONTAP gestiti (inclusi i mediatori ha) utilizzano tutti il server proxy.

Fasi

1. "Accedere all'interfaccia SaaS di Cloud Manager" Da un computer che dispone di una connessione di rete all'istanza del connettore.

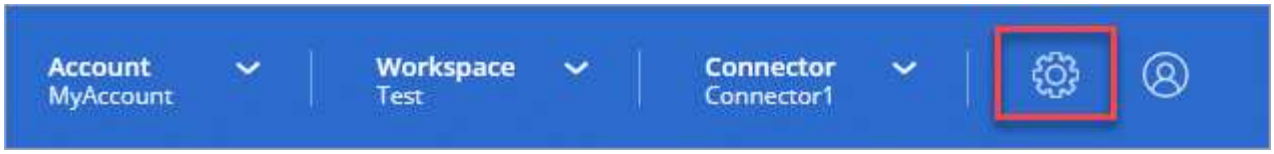
   Se il connettore non dispone di un indirizzo IP pubblico, è necessaria una connessione VPN oppure è necessario connettersi da un host di collegamento che si trova nella stessa rete del connettore.

2. Fare clic sull'elenco a discesa **Connector** (connettore), quindi fare clic su **Go to local UI** (Vai all'interfaccia utente locale) per un connettore specifico.



   L'interfaccia di Cloud Manager in esecuzione sul connettore viene caricata in una nuova scheda del browser.

3. Nella parte superiore destra della console di Cloud Manager, fare clic sull'icona Impostazioni e selezionare **Impostazioni Cloud Manager**.



4. 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 è stato specificato il server proxy prima che gli utenti creino sistemi Cloud Volumes ONTAP, devono utilizzare Gestione sistema per impostare manualmente il server proxy nelle opzioni AutoSupport per ciascun sistema.

Esclusione dei blocchi CIFS per Cloud Volumes ONTAP ha in Azure

L'amministratore dell'account può attivare un'impostazione in Cloud Manager che impedisce i problemi di failover dello storage Cloud Volumes ONTAP durante gli eventi di manutenzione di Azure. Quando si attiva questa impostazione, Cloud Volumes ONTAP esegue il veto di CIFS e ripristina le sessioni CIFS attive.

A proposito di questa attività

Microsoft Azure pianifica gli eventi di manutenzione periodica sulle macchine virtuali. Quando si verifica un evento di manutenzione su un nodo di una coppia Cloud Volumes ONTAP ha, la coppia ha avvia il Takeover dello storage. Se durante questo evento di manutenzione sono presenti sessioni CIFS attive, i blocchi sui file CIFS possono impedire il failover dello storage.

Se si attiva questa impostazione, Cloud Volumes ONTAP veto i blocchi e ripristina le sessioni CIFS attive. Di conseguenza, la coppia ha può completare il failover dello storage durante questi eventi di manutenzione.

Questo processo potrebbe interrompere i client CIFS. I dati non impegnati dai client CIFS potrebbero andare persi.

Di cosa hai bisogno

È necessario creare un connettore prima di poter modificare le impostazioni di Cloud Manager. "Scopri come".

Fasi

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

2. In **ha CIFS Locks**, selezionare la casella di controllo e fare clic su **Save** (Salva).

Riferimento

Ruoli

I ruoli account Admin (Amministratore account), Workspace Admin (Amministratore area di lavoro) e Cloud Compliance Viewer (Visualizzatore conformità cloud) forniscono autorizzazioni specifiche agli utenti.

Attività	Amministratore account	Amministratore dello spazio di lavoro	Cloud Compliance Viewer
Gestire gli ambienti di lavoro	Sì	Sì	No
Abilitare i servizi negli ambienti di lavoro	Sì	Sì	No
Visualizzare lo stato della replica dei dati	Sì	Sì	No
Visualizza la timeline	Sì	Sì	No
Passare da un'area di lavoro all'altra	Sì	Sì	Sì
Visualizzare i risultati della scansione Compliance	Sì	Sì	Sì
Eliminare gli ambienti di lavoro	Sì	No	No
Connettere i cluster Kubernetes agli ambienti di lavoro	Sì	No	No
Ricevere il report Cloud Volumes ONTAP	Sì	No	No
Creare connettori	Sì	No	No
Gestire gli account Cloud Central	Sì	No	No
Gestire le credenziali	Sì	No	No
Modificare le impostazioni di Cloud Manager	Sì	No	No
Visualizza e gestisci la dashboard di supporto	Sì	No	No
Rimuovere gli ambienti di lavoro da Cloud Manager	Sì	No	No
Installare un certificato HTTPS	Sì	No	No

Link correlati

- "Impostazione di aree di lavoro e utenti nell'account Cloud Central"
- "Gestione degli spazi di lavoro e degli utenti nell'account Cloud Central"

In che modo Cloud Manager utilizza le autorizzazioni del cloud provider

Cloud Manager richiede autorizzazioni per eseguire azioni nel tuo cloud provider. Queste autorizzazioni sono incluse in "Le policy fornite da NetApp". Potresti voler capire cosa fa Cloud Manager con queste autorizzazioni.

Cosa fa Cloud Manager con le autorizzazioni AWS

Cloud Manager utilizza un account AWS per effettuare chiamate API a diversi servizi AWS, tra cui EC2, S3, CloudFormation, IAM, Il servizio token di protezione (STS) e il servizio di gestione delle chiavi (KMS).

Azioni	Scopo
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescripbeInstances", "ec2:DescripbeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Avvia un'istanza di Cloud Volumes ONTAP e interrompe, avvia e monitora l'istanza.
"ec2:DescripbeInstanceAttribute",	Verifica che la rete avanzata sia abilitata per i tipi di istanze supportati.
"ec2:DescripbeRouteTable", "ec2:DescripbeImages",	Avvia una configurazione Cloud Volumes ONTAP ha.
"ec2:CreateTags",	Contrassegna ogni risorsa creata da Cloud Manager con i tag "WorkingEnvironment" e "WorkingEnvironmentId". Cloud Manager utilizza questi tag per la manutenzione e l'allocazione dei costi.
"ec2:CreateVolume", "ec2:DescripbeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestisce i volumi EBS utilizzati da Cloud Volumes ONTAP come storage back-end.
"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", "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicAccessBlock"	Gestisce il bucket S3 utilizzato da un sistema Cloud Volumes ONTAP come Tier di capacità per il tiering dei dati.
"Kms:List*", "kms:ReEncrypt*", "kms:descrive*", "kms:CreateGrant",	Attiva la crittografia dei dati di Cloud Volumes ONTAP utilizzando il servizio di gestione delle chiavi AWS (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Ottiene i dati dei costi AWS per Cloud Volumes ONTAP.

Azioni	Scopo
"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.
"ec2:DescripteReservedInstancesOfferings" (ec2:DescripteReservedInstancesOff	Cloud Manager utilizza l'autorizzazione come parte dell'implementazione di Cloud Compliance per scegliere il tipo di istanza da utilizzare.
"s3:Deletebucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "s3:GetObject", "s3:ListBucket", "s3:ListAllMyBucket", "s3:GetBucketTagging", "s3:GetBucketLocation" "s3:GetBucketPolicyStatus", "s3:GetBucketPublicAccessBlock", "s3:GetBucketAcl", "s3:GetBucketPolicy", "s3:PutBucketPublicicAccessBlock"	Cloud Manager utilizza queste autorizzazioni quando si attiva il servizio Backup in S3.

Cosa fa Cloud Manager con le autorizzazioni Azure

La policy di Cloud Manager Azure include le autorizzazioni necessarie per implementare e gestire Cloud Volumes ONTAP in Azure.

Azioni	Scopo
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Crea Cloud Volumes ONTAP e arresta, avvia, elimina e ottiene lo stato del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Consente l'implementazione di Cloud Volumes ONTAP da un VHD.
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/Read", "Microsoft.Storage/Operations/Read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/Read", "Microsoft.Storage/storageAccounts/rigeneratekey/action", "Microsoft.Storage/storageAccounts/write", "Microsoft.Storage/uses/Read",	Gestisce gli account e i dischi dello storage Azure e li collega a Cloud Volumes ONTAP.

Azioni	Scopo
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Crea e gestisce le interfacce di rete per Cloud Volumes ONTAP nella subnet di destinazione.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action", 	Crea gruppi di sicurezza di rete predefiniti per Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/locations/Read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action", 	Ottiene informazioni di rete relative alle regioni, alla rete virtuale di destinazione e alla subnet e aggiunge Cloud Volumes ONTAP ai reti virtuali.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Attiva gli endpoint del servizio VNET per il tiering dei dati.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Deployments/write",	Implementa Cloud Volumes ONTAP da un modello.
"Microsoft.Resources/Deployments/Operations/Read", "Microsoft.Resources/Deployments/Read", "Microsoft.Resources/Read", "Microsoft.Resources/subscriptions/operationresults/Read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/Read", "Microsoft.Resources/subscriptions/resourceGroups/write",	Crea e gestisce gruppi di risorse per Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Crea e gestisce snapshot gestite da Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Crea e gestisce i set di disponibilità per Cloud Volumes ONTAP.
"Microsoft.MarketplaceOrdering/offers/publisher/offers/plans/agreements/Read", "Microsoft.MarketplaceOrdering/offers/plans/agreements/write"	Consente implementazioni programmatiche da Azure Marketplace.

Azioni	Scopo
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Gestisce un bilanciamento del carico Azure per le coppie ha.
"Microsoft.Authorization/Blocks/*"	Consente la gestione dei blocchi sui dischi Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestisce il failover per le coppie ha.
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/Read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Consente la gestione di endpoint privati. Gli endpoint privati vengono utilizzati quando la connettività non viene fornita all'esterno della subnet. Cloud Manager crea l'account storage per ha con solo connettività interna all'interno della subnet.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Consente a Cloud Manager di eliminare i volumi per Azure NetApp Files.
"Microsoft.Resources/Deployments/OperationStatuses/Read"	Azure richiede questa autorizzazione per alcune implementazioni di macchine virtuali (dipende dall'hardware fisico sottostante utilizzato durante l'implementazione).
"Microsoft.Resources/Deployments/OperationStatuses/Read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Resources/Deployments/delete",	Consente di utilizzare Global file cache.

Azioni	Scopo
"Microsoft.Compute/diskEncryptionSets/read"	Consente a Cloud Manager di crittografare i dischi gestiti da Azure su sistemi Cloud Volumes ONTAP a nodo singolo utilizzando chiavi esterne di un altro account. Questa funzionalità è supportata tramite API.

Cosa fa Cloud Manager con le autorizzazioni GCP

La policy di Cloud Manager per GCP include le autorizzazioni necessarie a Cloud Manager per implementare e gestire Cloud Volumes ONTAP.

Azioni	Scopo
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Per creare e gestire dischi per Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Per creare regole firewall per Cloud Volumes ONTAP.
- Compute.globalOperations.get	Per ottenere lo stato delle operazioni.
- Compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Per ottenere immagini per istanze di macchine virtuali.
- compute.instances.attachDisk - compute.instances.detachDisk	Per collegare e scollegare i dischi a Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Per creare ed eliminare istanze di Cloud Volumes ONTAP VM.
- compute.instances.get	Per elencare le istanze di macchine virtuali.
- compute.instances.getSerialPortOutput	Per ottenere i log della console.
- compute.instances.list	Per recuperare l’elenco di istanze in una zona.
- compute.instances.setDeletionProtection	Per impostare la protezione di eliminazione sull’istanza.
- compute.instances.setLabels	Per aggiungere etichette.
- compute.instances.setMachineType	Per modificare il tipo di macchina per Cloud Volumes ONTAP.
- compute.instances.setMetadata	Per aggiungere metadati.
- compute.instances.setTags	Per aggiungere tag per le regole del firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Per avviare e arrestare Cloud Volumes ONTAP.
- Compute.machineTypes.get	Per ottenere il numero di core per controllare le qoutas.
- compute.projects.get	Per supportare progetti multipli.

Azioni	Scopo
- Compute.Snapshot.create - compute.snapshots.delete - compute.Snapshot.get - compute.Snapshot.list - compute.snapshots.setLabels	Per creare e gestire snapshot di dischi persistenti.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zone.list	Per ottenere le informazioni di rete necessarie per creare una nuova istanza di macchina virtuale Cloud Volumes ONTAP.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.typeopers.get.get.get - deploymentmanager.get.list	Per implementare l'istanza della macchina virtuale Cloud Volumes ONTAP utilizzando Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Per ottenere unità di log stack.
- resourcemanager.projects.get	Per supportare progetti multipli.
- storage.bucket.create - storage.buckets.delete - storage.bucket.get - storage.bucket.list - storage.bucket.update	Per creare e gestire un bucket di storage Google Cloud per il tiering dei dati.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptKeys.get - cloudkms.cryptKeys.list - cloudkms.keyrings.list	Per utilizzare le chiavi di crittografia gestite dal cliente dal servizio di gestione delle chiavi cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Per impostare un account di servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud.

Pagine del marketplace AWS per Cloud Manager e Cloud Volumes ONTAP

Nel marketplace AWS sono disponibili diverse offerte per Cloud Manager e Cloud Volumes ONTAP. Se hai bisogno di aiuto per comprendere lo scopo di ciascuna pagina, leggi le descrizioni riportate di seguito.

In tutti i casi, non è possibile avviare Cloud Volumes ONTAP in AWS dal marketplace AWS. È necessario avviarlo direttamente da Cloud Manager.

Obiettivo	Pagina AWS Marketplace da utilizzare	Ulteriori informazioni
Abilita l'utilizzo di PAYGO Cloud Volumes ONTAP, Tier cloud, conformità cloud e altri servizi aggiuntivi	"Cloud Manager - implementazione di gestione dei servizi dati cloud NetApp"	Questo abbonamento consente di addebitare il costo per LA versione PAYGO di Cloud Volumes ONTAP 9.6 e versioni successive. Consente inoltre di addebitare costi per il Cloud Tiering, la Cloud Compliance e altri servizi aggiuntivi. Devi iscriverti a questa offerta quando Cloud Manager ti richiede e ti reindirizza alla pagina. Cloud Manager visualizza un messaggio nella procedura guidata ambiente di lavoro o quando si aggiungono nuove credenziali in Impostazioni. Questa pagina non consente di avviare Cloud Manager in AWS. Questo dovrebbe essere fatto da "NetApp Cloud Central", O in alternativa utilizzando l'AMI elencato nella riga 3 di questa tabella.
Abilita l'utilizzo di PAYGO Cloud Volumes ONTAP, Tier cloud, conformità cloud e altri servizi aggiuntivi *utilizzando un contratto annuale*	"Cloud Manager (contratti) - implementa Gestisci NetApp Cloud Data Services"	Questo abbonamento è un'alternativa all'abbonamento della prima riga. Consente di ottenere un pagamento anticipato annuale per gli elenchi. È principalmente per i partner NetApp.
Implementare Cloud Manager da AWS Marketplace utilizzando un AMI	"Cloud Manager - Installazione manuale senza chiavi di accesso"	Si consiglia di avviare Cloud Manager in AWS da "NetApp Cloud Central", Ma è possibile avviarlo da questa pagina di AWS Marketplace, se si preferisce.
Implementazione di Cloud Volumes ONTAP PAYGO (9.5 o precedente)	• "Cloud Volumes ONTAP per AWS" • "Cloud Volumes ONTAP per AWS - alta disponibilità"	Queste pagine di AWS Marketplace consentono di sottoscrivere le versioni a nodo singolo o ha di Cloud Volumes ONTAP PAYGO per le versioni 9.5 e precedenti. A partire dalla versione 9.6, è necessario iscriversi alla pagina AWS Marketplace elencata nella riga 1 di questa tabella per le implementazioni PAYGO.

Utilizzare API e automazione

Risorse 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. Uno di questi strumenti è Terraform. Abbiamo sviluppato un provider di terraform che i team DevOps possono utilizzare con Cloud Manager per automatizzare e integrare Cloud Volumes ONTAP con l'infrastruttura come codice.

"Visualizza il provider netapp-cloud-mmanager".

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"

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.

- "Supporto NetApp Cloud Volumes ONTAP"

  Accedi alle risorse di supporto per ottenere assistenza e risolvere i problemi relativi a Cloud Volumes ONTAP.

- "Video per Cloud Manager e Cloud Volumes ONTAP"

  Guarda i video che mostrano come implementare e gestire Cloud Volumes ONTAP e come replicare i dati nel tuo cloud ibrido.

- "Policy per Cloud Manager"

  Scarica i file JSON che includono le autorizzazioni necessarie a Cloud Manager per eseguire azioni in un cloud provider.

- "Guida per sviluppatori API di Cloud Manager"

  Leggi una panoramica delle API, esempi di come utilizzarle e un riferimento API.

- Training per Cloud Volumes ONTAP
  - "Nozioni di base su Cloud Volumes ONTAP"
  - "Implementazione e gestione di Cloud Volumes ONTAP per Azure"
  - "Implementazione e gestione di Cloud Volumes ONTAP per AWS"
- Report tecnici
  - "Report tecnico di NetApp 4383: Caratterizzazione delle performance di Cloud Volumes ONTAP nei servizi Web Amazon con carichi di lavoro delle applicazioni"
  - "Report tecnico di NetApp 4671: Caratterizzazione delle performance di Cloud Volumes ONTAP in Azure con carichi di lavoro applicativi"
  - "Report tecnico NetApp 4816: Caratterizzazione delle performance di Cloud Volumes ONTAP per Google Cloud"
- Disaster recovery SVM

  Il disaster recovery SVM è il mirroring asincrono dei dati SVM e della configurazione da una SVM di origine a una SVM di destinazione. È possibile attivare rapidamente una SVM di destinazione per l'accesso ai dati se la SVM di origine non è più disponibile.

  - "Guida rapida alla preparazione del disaster recovery per Cloud Volumes ONTAP 9 SVM"

    Descrive come configurare rapidamente una SVM di destinazione in preparazione al disaster recovery.

  - "Guida rapida al disaster recovery di Cloud Volumes ONTAP 9 SVM"

    Descrive come attivare rapidamente una SVM di destinazione dopo un disastro e riattivare la SVM di origine.

- "Guida all’alimentazione di FlexCache Volumes per un accesso più rapido ai dati"

  Descrive come creare e gestire volumi FlexCache nello stesso cluster o in un cluster diverso del volume di origine per accelerare l’accesso ai dati.

- "Avvisi di sicurezza"

  Identificare le vulnerabilità note (CVE) per i prodotti NetApp, incluso ONTAP. Si noti che è possibile correggere le vulnerabilità di sicurezza per Cloud Volumes ONTAP seguendo la documentazione di ONTAP.

- "Centro documentazione di ONTAP 9"

  Accedi alla documentazione del prodotto per ONTAP, che può aiutarti a utilizzare Cloud Volumes ONTAP.

- "Community NetApp: Servizi dati cloud"

  Connettiti con i colleghi, fai domande, scambia idee, trova risorse e condividi le Best practice.

- "NetApp Cloud Central"

  Informazioni su ulteriori prodotti e soluzioni NetApp per il cloud.

- "Documentazione sui prodotti NetApp"

  Cerca nella documentazione dei prodotti NetApp istruzioni, risorse e risposte.

Versioni precedenti della documentazione di Cloud Manager

La documentazione relativa alle release precedenti di Cloud Manager è disponibile nel caso in cui non si utilizzi la versione più recente.

- "Cloud Manager 3.7"
- "Cloud Manager 3.6"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

http://www.netapp.com/us/legal/netapptmlist.aspx

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/us/media/patents-page.pdf

Direttiva sulla privacy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Cloud Manager 3.8.7"
- "Avviso per Cloud Manager 3.8.6"
- "Avviso per Cloud Manager 3.8.5"
- "Avviso per Cloud Manager 3.8.4"
- "Avviso per Cloud Manager 3.8.3"
- "Avviso per Cloud Manager 3.8.2"
- "Avviso per Cloud Manager 3.8.1"
- "Avviso per Cloud Manager 3.8"
- "Avviso per Cloud Backup Service"
- "Avviso per Global file cache"
- "Avviso per la conformità del cloud"

Informazioni sul copyright

Informazioni sul marchio commerciale