Replica e protezione dei dati

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

Replica e protezione dei dati

Rilevamento e gestione dei cluster ONTAP

Cloud Manager è in grado di rilevare i cluster ONTAP nel tuo ambiente on-premise, in una configurazione di storage privato NetApp e nel cloud IBM. La scoperta di questi cluster ti consente di replicare facilmente i dati nel tuo ambiente di cloud ibrido direttamente da Cloud Manager.

Alla scoperta dei cluster ONTAP

Il rilevamento di un cluster ONTAP in Cloud Manager ti consente di eseguire il provisioning dello storage e di replicare i dati nel cloud ibrido.

Prima di iniziare

Per aggiungere il cluster a Cloud Manager, è necessario disporre dell'indirizzo IP di gestione del cluster e della password dell'account utente admin.

Cloud Manager rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti:

- L'host Cloud Manager deve consentire l'accesso HTTPS in uscita attraverso la porta 443.

  Se Cloud Manager si trova in AWS, tutte le comunicazioni in uscita sono consentite dal gruppo di sicurezza predefinito.

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

  Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questa policy predefinita è stata modificata o se è stata creata una policy firewall personalizzata, è necessario associare il protocollo HTTPS a tale policy e abilitare l'accesso dall'host Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Discover** e selezionare **cluster ONTAP**.
2. Nella pagina **Dettagli cluster ONTAP**, inserire l'indirizzo IP di gestione del cluster, la password per l'account utente admin e la posizione del cluster.

3. Nella pagina Dettagli, immettere un nome e una descrizione per l'ambiente di lavoro, quindi fare clic su **Go**.

Risultato

Cloud Manager rileva il cluster. È ora possibile creare volumi, replicare i dati da e verso il cluster e avviare Gestione di sistema di OnCommand per eseguire attività avanzate.

Provisioning di volumi su cluster ONTAP

Cloud Manager consente di eseguire il provisioning di volumi NFS e CIFS su cluster ONTAP.

Prima di iniziare

NFS o CIFS devono essere impostati sul cluster. È possibile configurare NFS e CIFS utilizzando System Manager o CLI.

A proposito di questa attività

È possibile creare volumi su aggregati esistenti. Non è possibile creare nuovi aggregati da Cloud Manager.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sul nome del cluster ONTAP su cui si desidera eseguire il provisioning dei volumi.
2. Fare clic su **Add New Volume** (Aggiungi nuovo volume).
3. Nella pagina Create New Volume (Crea nuovo volume), inserire i dettagli del volume, quindi fare clic su **Create** (Crea).

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

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

Replica dei dati tra sistemi

È possibile replicare i dati tra ambienti di lavoro scegliendo una replica dei dati una tantum per il trasferimento dei dati o una pianificazione ricorrente per il disaster recovery o la conservazione a lungo termine. Ad esempio, è possibile configurare la replica dei dati da un sistema ONTAP on-premise a Cloud Volumes ONTAP per il disaster recovery.

Cloud Manager semplifica la replica dei dati tra volumi su sistemi separati utilizzando le tecnologie SnapMirror e SnapVault. È sufficiente identificare il volume di origine e il volume di destinazione, quindi scegliere una policy e una pianificazione di replica. Cloud Manager acquista i dischi richiesti, configura le relazioni, applica la policy di replica e avvia il trasferimento di riferimento tra i volumi.

Il trasferimento di riferimento include una copia completa dei dati di origine. I trasferimenti successivi contengono copie differenziali dei dati di origine.

Requisiti di replica dei dati

Prima di poter replicare i dati, è necessario verificare che i requisiti specifici siano soddisfatti sia per i sistemi Cloud Volumes ONTAP che per i cluster ONTAP.

Requisiti di versione

Prima di eseguire la replica dei dati, verificare che i volumi di origine e di destinazione eseguano versioni ONTAP compatibili. Per ulteriori informazioni, vedere "Guida all'alimentazione per la protezione dei dati".

Requisiti specifici di Cloud Volumes ONTAP

- Il gruppo di protezione dell'istanza deve includere le regole in entrata e in uscita richieste, in particolare le regole per ICMP e le porte 10000, 11104 e 11105.

  Queste regole sono incluse nel gruppo di protezione predefinito.

- Per replicare i dati tra due sistemi Cloud Volumes ONTAP in diverse subnet, è necessario instradare insieme le subnet (impostazione predefinita).
- Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e un sistema in Azure, è necessario disporre di una connessione VPN tra AWS VPC e Azure VNET.

Requisiti specifici dei cluster ONTAP

- È necessario installare una licenza SnapMirror attiva.
- Se il cluster si trova all'interno della propria sede, si dovrebbe disporre di una connessione dalla rete aziendale ad AWS o Azure, che in genere è una connessione VPN.
- I cluster ONTAP devono soddisfare ulteriori requisiti di subnet, porta, firewall e cluster.

  Per ulteriori informazioni, consultare la Guida rapida di peering di cluster e SVM per la versione di ONTAP in uso.

Configurazione della replica dei dati tra sistemi

Puoi replicare i dati tra sistemi Cloud Volumes ONTAP e cluster ONTAP scegliendo una replica dei dati una tantum, che può aiutarti a spostare i dati da e verso il cloud, o una pianificazione ricorrente, che può aiutarti con il disaster recovery o la conservazione a lungo termine.

A proposito di questa attività

Cloud Manager supporta configurazioni di protezione dei dati semplici, fanout e a cascata:

- In una configurazione semplice, la replica avviene dal volume A al volume B.
- In una configurazione fanout, la replica avviene dal volume A a più destinazioni.
- In una configurazione a cascata, la replica avviene dal volume A al volume B e dal volume B al volume C.

È possibile configurare configurazioni fanout e a cascata in Cloud Manager impostando più repliche di dati tra sistemi. Ad esempio, replicando un volume dal sistema A al sistema B e replicando lo stesso volume dal sistema B al sistema C.

Fasi

1. Nella pagina ambienti di lavoro, selezionare l'ambiente di lavoro che contiene il volume di origine, quindi trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume:

2. Se vengono visualizzate le pagine Source (origine) e Destination peering Setup (Configurazione peering destinazione), selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.

   La rete intercluster deve essere configurata in modo che i peer del cluster dispongano di una *connettività full-mesh a coppie*, il che significa che ogni coppia di cluster in una relazione peer del cluster dispone di connettività tra tutte le proprie LIF intercluster.

   Queste pagine vengono visualizzate se l'origine o la destinazione è un cluster ONTAP con più LIF.

3. Nella pagina Source Volume Selection (selezione volume di origine), selezionare il volume che si desidera replicare.
4. Nella pagina Destination Volume Name and Tiering (Nome volume di destinazione e tiering), specificare il nome del volume di destinazione, scegliere un tipo di disco sottostante, modificare una delle opzioni avanzate e fare clic su **Continue** (continua).

   Se la destinazione è un cluster ONTAP, è necessario specificare anche la SVM di destinazione e l'aggregato.

5. Nella pagina velocità di trasferimento massima, specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.
6. Nella pagina Replication Policy (Criteri di replica), scegliere uno dei criteri predefiniti o fare clic su **Additional Policies** (Criteri aggiuntivi), quindi selezionare uno dei criteri avanzati.

   Per ulteriori informazioni, vedere "Scelta di un criterio di replica".

   Se si sceglie un criterio di backup personalizzato (SnapVault), le etichette associate al criterio devono corrispondere alle etichette delle copie Snapshot sul volume di origine. Per ulteriori informazioni, vedere "Come funzionano le policy di backup".

7. Nella pagina Pianificazione, scegliere una copia singola o una pianificazione ricorrente.

   Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione nel cluster *destination* utilizzando System Manager.

8. Nella pagina Review (esamina), rivedere le selezioni, quindi fare clic su **Go** (Vai).

Risultato

Cloud Manager avvia il processo di replica dei dati. È possibile visualizzare i dettagli relativi alla replica nella pagina Replication Status (Stato replica).

Gestione delle pianificazioni e delle relazioni di replica dei dati

Dopo aver configurato la replica dei dati tra due sistemi, è possibile gestire la pianificazione e la relazione della replica dei dati da Cloud Manager.

Fasi

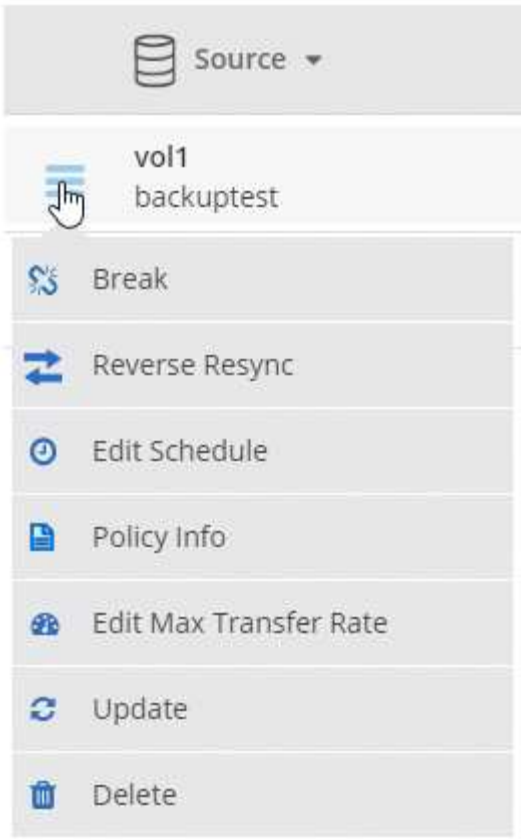
1. Nella pagina ambienti di lavoro, visualizzare lo stato della replica per tutti gli ambienti di lavoro nell'area di lavoro o per un ambiente di lavoro specifico:

Opzione	Azione
Tutti gli ambienti di lavoro nello spazio di lavoro	Nella parte superiore di Cloud Manager, fare clic su **Replication Status** (Stato replica).
Un ambiente di lavoro specifico	Aprire l'ambiente di lavoro e fare clic su **Replications** (repliche).

2. Esaminare lo stato delle relazioni di replica dei dati per verificare che siano integre.

   Se lo stato di una relazione è inattivo e lo stato di mirroring non è inizializzato, è necessario inizializzare la relazione dal sistema di destinazione per eseguire la replica dei dati in base alla pianificazione definita. È possibile inizializzare la relazione utilizzando System Manager o l'interfaccia della riga di comando (CLI). Questi stati possono essere visualizzati quando il sistema di destinazione non funziona e poi torna in linea.

3. Selezionare l'icona del menu accanto al volume di origine, quindi scegliere una delle azioni disponibili.



La seguente tabella descrive le azioni disponibili:

Azione	Descrizione
Rompere	Interrompe la relazione tra i volumi di origine e di destinazione e attiva il volume di destinazione per l'accesso ai dati. Questa opzione viene generalmente utilizzata quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline. Per informazioni sulla configurazione di un volume di destinazione per l'accesso ai dati e la riattivazione di un volume di origine, consultare la Guida rapida al disaster recovery di ONTAP 9.
Risincronizzare	Consente di ripristinare una relazione interrotta tra i volumi e di riprendere la replica dei dati in base alla pianificazione definita. Quando si risincronizzano i volumi, i contenuti del volume di destinazione vengono sovrascritti dai contenuti del volume di origine. Per eseguire una risincronizzazione inversa, che risincronizza i dati dal volume di destinazione al volume di origine, vedere la "Guida rapida per il disaster recovery dei volumi di ONTAP 9".
Risincronizzazione inversa	Inverte i ruoli dei volumi di origine e di destinazione. Il contenuto del volume di origine originale viene sovrascritto dal contenuto del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline. Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.

Azione	Descrizione
Modifica pianificazione	Consente di scegliere una pianificazione diversa per la replica dei dati.
Info policy	Mostra il criterio di protezione assegnato alla relazione di replica dei dati.
Modifica velocità di trasferimento massima	Consente di modificare la velocità massima (in kilobyte al secondo) alla quale è possibile trasferire i dati.
Aggiornare	Avvia un trasferimento incrementale per aggiornare il volume di destinazione.
Eliminare	Elimina la relazione di protezione dei dati tra i volumi di origine e di destinazione, il che significa che la replica dei dati non avviene più tra i volumi. Questa azione non attiva il volume di destinazione per l'accesso ai dati. Questa azione elimina anche la relazione peer del cluster e la relazione peer SVM (Storage Virtual Machine), se non sono presenti altre relazioni di protezione dei dati tra i sistemi.

Risultato

Dopo aver selezionato un'azione, Cloud Manager aggiorna la relazione o la pianificazione.

Scelta di un criterio di replica

Quando si imposta la replica dei dati in Cloud Manager, potrebbe essere necessario un aiuto nella scelta di una policy di replica. Un criterio di replica definisce il modo in cui il sistema storage replica i dati da un volume di origine a un volume di destinazione.

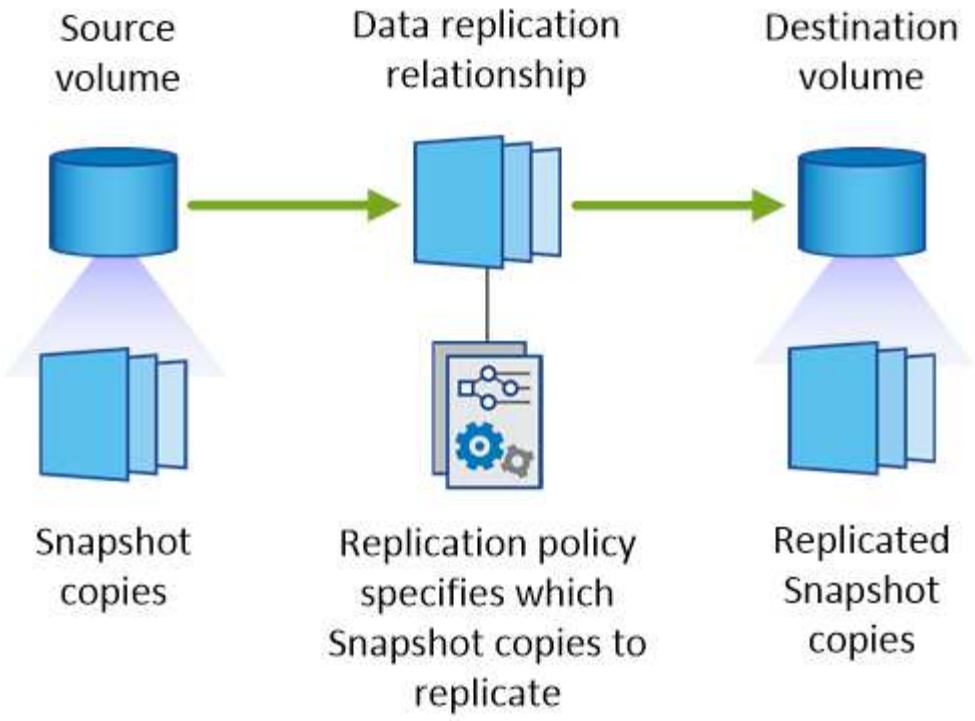
Quali sono le funzioni delle policy di replica

Il sistema operativo ONTAP crea automaticamente i backup denominati copie Snapshot. Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato del file system in un momento specifico.

Quando si replicano i dati tra sistemi, si replicano le copie Snapshot da un volume di origine a un volume di destinazione. Un criterio di replica specifica quali copie Snapshot replicare dal volume di origine al volume di destinazione.

Le policy di replica sono anche denominate policy di *protezione*, in quanto sono basate sulle tecnologie SnapMirror e SnapVault, che forniscono protezione dal disaster recovery e backup e ripristino disk-to-disk.

La seguente immagine mostra la relazione tra le copie Snapshot e i criteri di replica:



Tipi di policy di replica

Esistono tre tipi di policy di replica:

- Un criterio *Mirror* replica le nuove copie Snapshot create in un volume di destinazione.

  È possibile utilizzare queste copie Snapshot per proteggere il volume di origine in preparazione al disaster recovery o alla replica dei dati una tantum. È possibile attivare il volume di destinazione per l'accesso ai dati in qualsiasi momento.

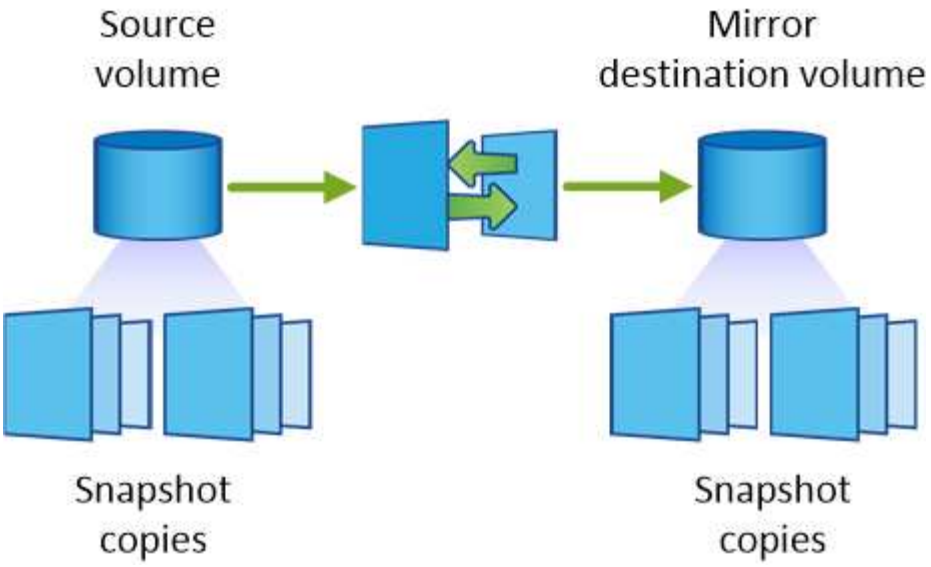
- Un criterio *Backup* replica copie Snapshot specifiche in un volume di destinazione e le conserva per un periodo di tempo più lungo rispetto al volume di origine.

  È possibile ripristinare i dati da queste copie Snapshot quando i dati vengono danneggiati o persi e conservarli per la conformità agli standard e altri scopi correlati alla governance.

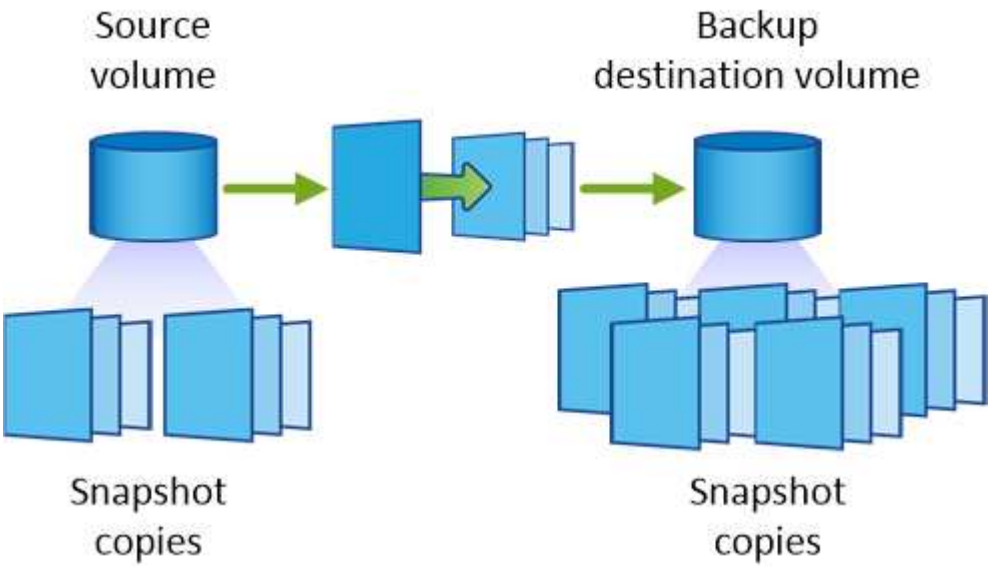
- Una policy di *Mirror e Backup* fornisce sia il disaster recovery che la conservazione a lungo termine.

  Ogni sistema include una policy di backup e mirroring predefinita, che funziona bene per molte situazioni. Se hai bisogno di policy personalizzate, puoi crearle usando System Manager.

Le seguenti immagini mostrano la differenza tra i criteri Mirror e Backup. Un criterio Mirror esegue il mirroring delle copie Snapshot disponibili sul volume di origine.



Una policy di backup conserva in genere le copie Snapshot più a lungo di quanto non vengano conservate nel volume di origine:



Come funzionano le policy di backup

A differenza dei criteri di mirroring, i criteri di backup (SnapVault) replicano copie Snapshot specifiche in un volume di destinazione. È importante comprendere il funzionamento dei criteri di backup se si desidera utilizzare i propri criteri invece dei criteri predefiniti.

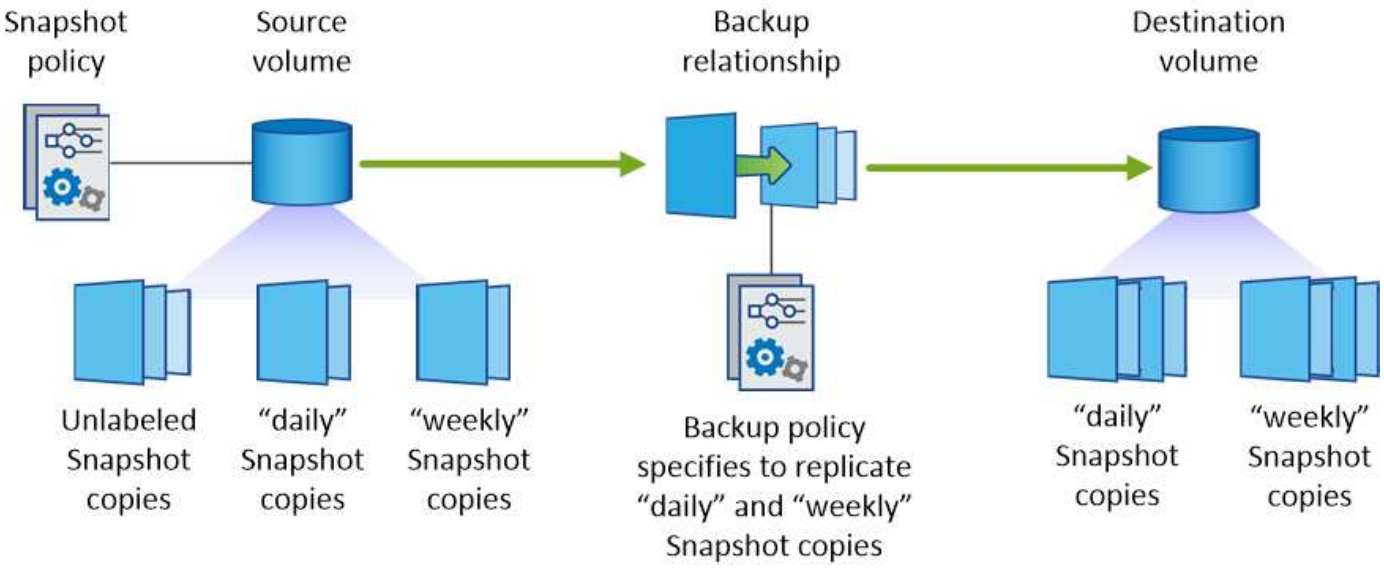
Comprensione della relazione tra le etichette delle copie Snapshot e le policy di backup

Una policy Snapshot definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare e come etichettarle. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti ed etichettarle "ogni giorno".

Un criterio di backup include regole che specificano le copie Snapshot etichettate da replicare in un volume di destinazione e il numero di copie da conservare. Le etichette definite in un criterio di backup devono corrispondere a una o più etichette definite in un criterio Snapshot. In caso contrario, il sistema non può

replicare alcuna copia Snapshot.

Ad esempio, una policy di backup che include le etichette "giornaliere" e "settimanali" produce la replica delle copie Snapshot che includono solo quelle etichette. Non vengono replicate altre copie Snapshot, come mostrato nell'immagine seguente:



Policy predefinite e policy personalizzate

La policy Snapshot predefinita crea copie Snapshot orarie, giornaliere e settimanali, conservando sei copie Snapshot orarie, due giornaliere e due copie Snapshot settimanali.

È possibile utilizzare facilmente un criterio di backup predefinito con il criterio Snapshot predefinito. Le policy di backup predefinite replicano copie Snapshot giornaliere e settimanali, conservando sette copie Snapshot giornaliere e 52 copie Snapshot settimanali.

Se si creano criteri personalizzati, le etichette definite da tali criteri devono corrispondere. È possibile creare policy personalizzate utilizzando System Manager.

Backup dei dati su Amazon S3

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

Quando si attiva Backup in S3, il servizio esegue un backup completo dei dati. Tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e nuovi.

"Visita NetApp Cloud Central per i dettagli sui prezzi".

Si noti che è necessario utilizzare Cloud Manager per tutte le operazioni di backup e ripristino. Qualsiasi azione intrapresa direttamente da ONTAP o da Amazon S3 comporta una configurazione non supportata.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

Verificare il supporto per la configurazione

Verificare quanto segue:

- Cloud Volumes ONTAP 9.4 o versione successiva viene eseguito in una regione AWS supportata: N. Virginia, Oregon, Irlanda, Francoforte o Sydney
- Sei iscritto al nuovo "Offerta Cloud Manager Marketplace"
- La porta TCP 5010 è aperta per il traffico in uscita nel gruppo di sicurezza per Cloud Volumes ONTAP (è aperta per impostazione predefinita)
- La porta TCP 8088 è aperta per il traffico in uscita nel gruppo di sicurezza per Cloud Manager (è aperta per impostazione predefinita)
- Il seguente endpoint è accessibile da Cloud Manager:

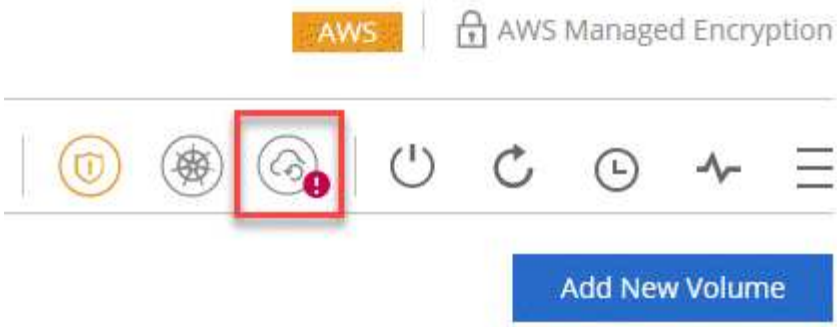
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Cloud Manager può allocare fino a due endpoint VPC di interfaccia nel VPC (il limite AWS per VPC è 20)
- Cloud Manager dispone dell'autorizzazione per utilizzare le autorizzazioni endpoint VPC elencate nella più recente "Policy di Cloud Manager":

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

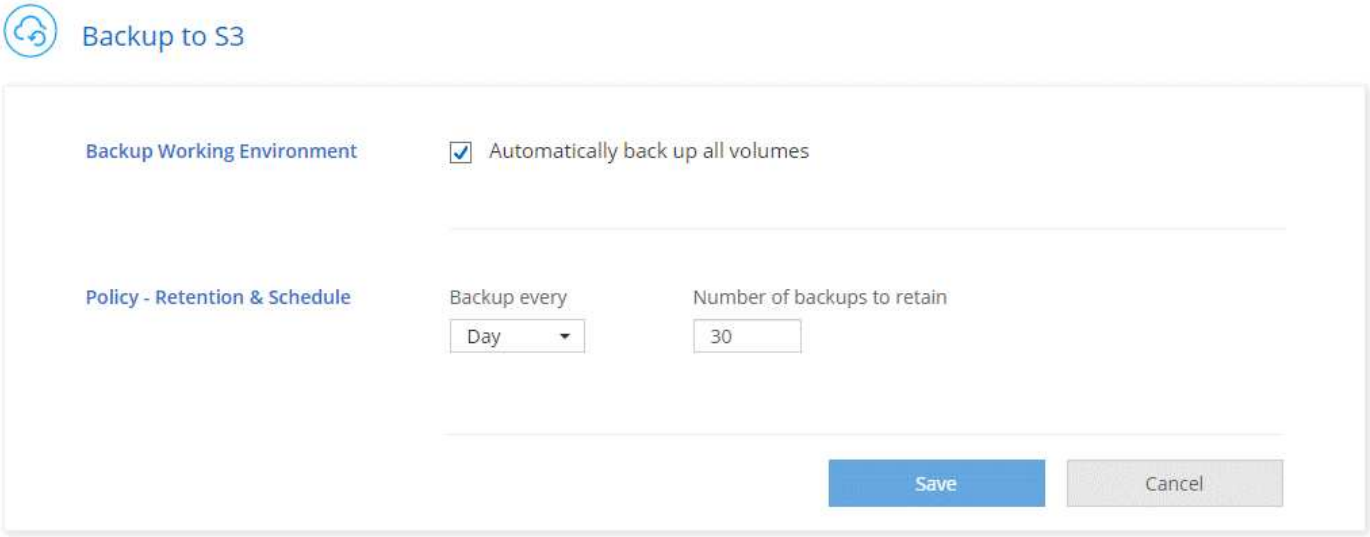
Abilitare Backup su S3 sul sistema nuovo o esistente

- Nuovi sistemi: La funzione Backup in S3 è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.
- Sistemi esistenti: Aprire l'ambiente di lavoro, fare clic sull'icona delle impostazioni di backup e abilitare i backup.



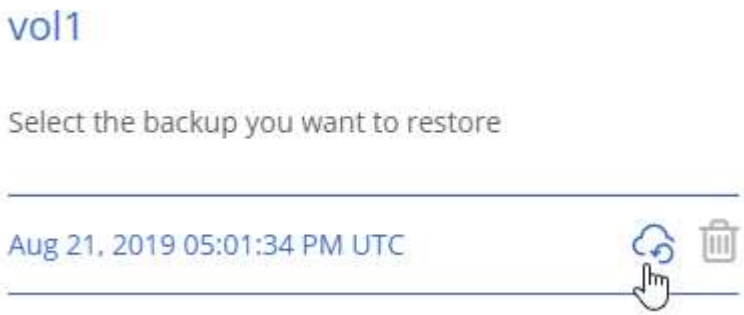
Se necessario, modificare il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva 30 copie di backup per ogni volume. Se necessario, è possibile modificare il numero di copie di backup da conservare.



Ripristinare i dati, se necessario

Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**, selezionare un volume, selezionare un backup, quindi ripristinare i dati dal backup in un nuovo volume.



Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi in S3.

Versioni di ONTAP supportate

Il backup su S3 è supportato con Cloud Volume ONTAP 9.4 e versioni successive.

Regioni AWS supportate

Il backup su S3 è supportato con Cloud Volumes ONTAP nelle seguenti aree AWS:

- US East (N. Virginia)
- STATI UNITI occidentali (Oregon)
- UE (Irlanda)
- UE (Francoforte)
- Asia Pacifico (Sydney)

Autorizzazioni AWS richieste

Il ruolo IAM che fornisce le autorizzazioni a Cloud Manager deve includere quanto segue:

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

Requisito di abbonamento AWS

A partire dalla versione 3.7.3, è disponibile un nuovo abbonamento a Cloud Manager in AWS Marketplace. Questo abbonamento consente l'implementazione di sistemi PAYGO Cloud Volumes ONTAP 9.6 e versioni successive e la funzionalità di backup in S3. È necessario "Iscriviti a questo nuovo abbonamento a Cloud Manager" Prima di attivare Backup su S3. La fatturazione per la funzione Backup in S3 viene effettuata tramite questo abbonamento.

Requisiti delle porte

- La porta TCP 5010 deve essere aperta per il traffico in uscita da Cloud Volumes ONTAP al servizio di backup.
- La porta TCP 8088 deve essere aperta per il traffico in uscita nel gruppo di sicurezza di Cloud Manager.

  Queste porte sono già aperte se sono stati utilizzati i gruppi di protezione predefiniti. Tuttavia, se hai utilizzato le tue, dovrai aprire queste porte.

Accesso a Internet in uscita

Assicurarsi che il seguente endpoint sia accessibile da Cloud Manager: https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager contatta questo endpoint per aggiungere il tuo ID account AWS all'elenco degli utenti autorizzati per Backup in S3.

Interfaccia endpoint VPC

Quando si attiva la funzione Backup in S3, Cloud Manager crea un endpoint VPC di interfaccia nel VPC in cui è in esecuzione Cloud Volumes ONTAP. Questo *endpoint di backup* si connette al VPC NetApp in cui è in esecuzione Backup in S3. Se ripristini un volume, Cloud Manager crea un endpoint VPC con interfaccia aggiuntiva, ovvero l' *endpoint di ripristino*.

Tutti i sistemi Cloud Volumes ONTAP aggiuntivi del VPC utilizzano questi due endpoint VPC.

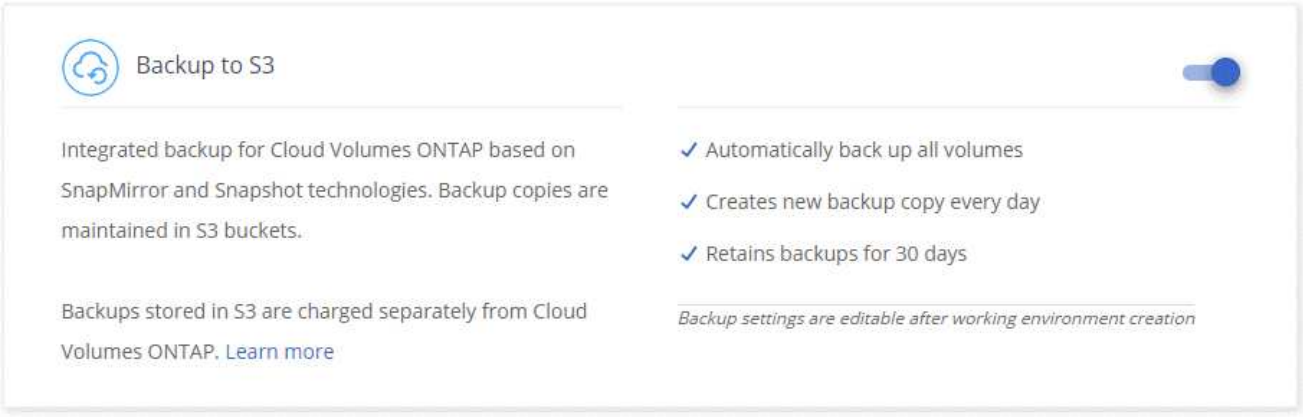
"Il limite predefinito per gli endpoint VPC dell'interfaccia è 20 per VPC". Assicurarsi che il VPC non abbia raggiunto il limite prima di attivare la funzione.

Abilitazione dei backup in S3 su un nuovo sistema

La funzione Backup in S3 è attivata per impostazione predefinita nella procedura guidata dell'ambiente di lavoro. Assicurarsi di mantenere l'opzione attivata.

Fasi

1. Fare clic su **Crea Cloud Volumes ONTAP**.
2. Selezionare Amazon Web Services come provider cloud, quindi scegliere un singolo nodo o sistema ha.
3. Compila la pagina Dettagli e credenziali.
4. Nella pagina Backup in S3, lasciare attivata la funzione e fare clic su **continua**.



5. Completare le pagine della procedura guidata per implementare il sistema.

Risultato

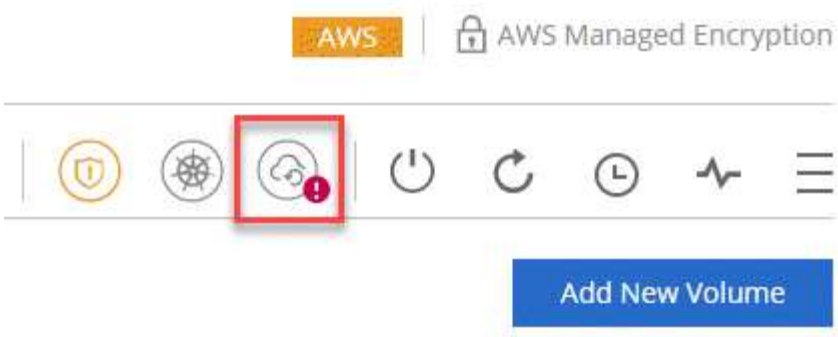
La funzione Backup in S3 è attivata sul sistema e consente di eseguire il backup dei volumi ogni giorno, conservando 30 copie di backup. Scopri come modificare la conservazione dei backup.

Abilitazione dei backup in S3 su un sistema esistente

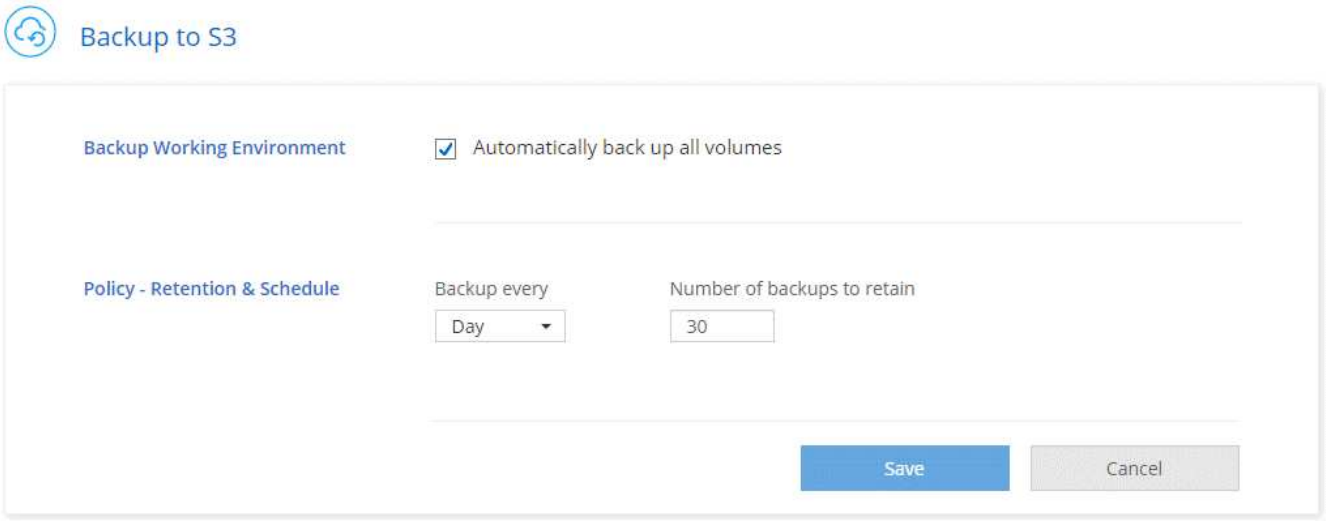
È possibile abilitare i backup in S3 su un sistema Cloud Volumes ONTAP esistente, purché sia in esecuzione una configurazione supportata. Per ulteriori informazioni, vedere Requisiti.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Selezionare **backup automatico di tutti i volumi**.
4. Scegliere la conservazione del backup e fare clic su **Save** (Salva).



Risultato

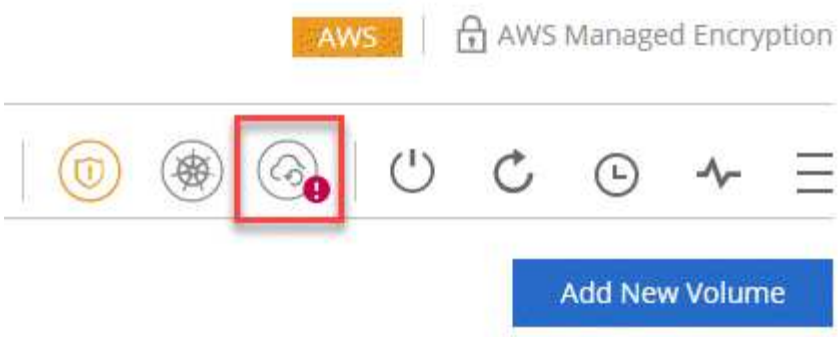
La funzionalità Backup in S3 inizia a eseguire i backup iniziali di ciascun volume.

Modifica della conservazione del backup

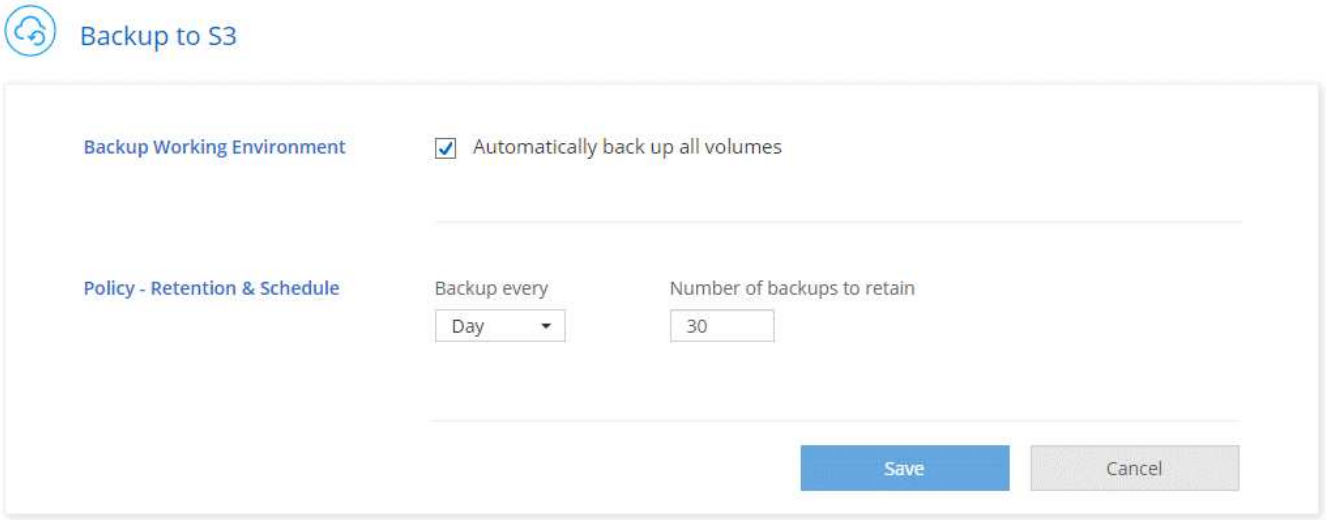
Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva 30 copie di backup per ogni volume. È possibile modificare il numero di copie di backup da conservare.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Modificare la conservazione del backup, quindi fare clic su **Save** (Salva).



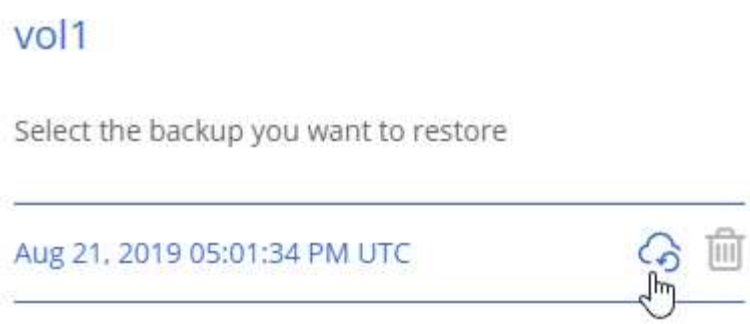
Ripristino di un volume

Quando ripristini i dati da un backup, Cloud Manager esegue un ripristino completo del volume in un volume *new*. È possibile ripristinare i dati nello stesso ambiente di lavoro o in un ambiente di lavoro diverso.

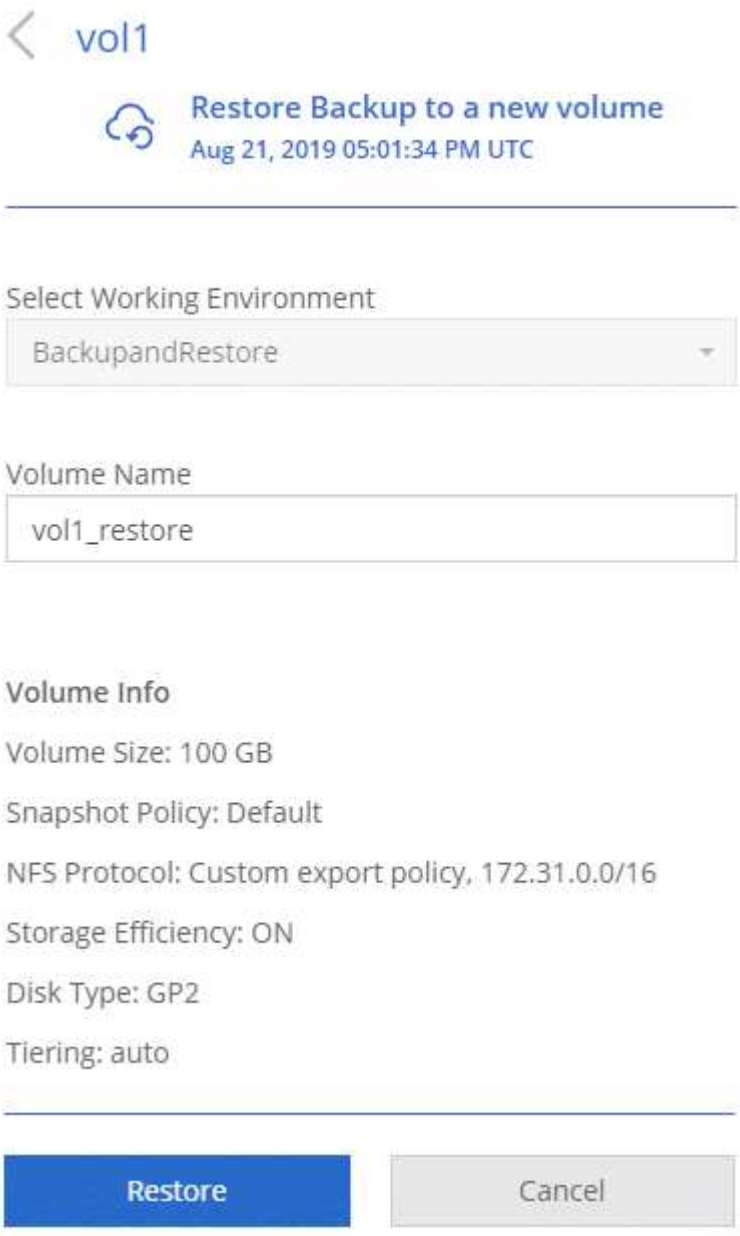
Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**.
2. Selezionare il volume che si desidera ripristinare.

3. Individuare il backup da cui si desidera eseguire il ripristino e fare clic sull'icona di ripristino.



4. Selezionare l'ambiente di lavoro in cui si desidera ripristinare il volume.
5. Immettere un nome per il volume.
6. Fare clic su **Restore** (Ripristina).

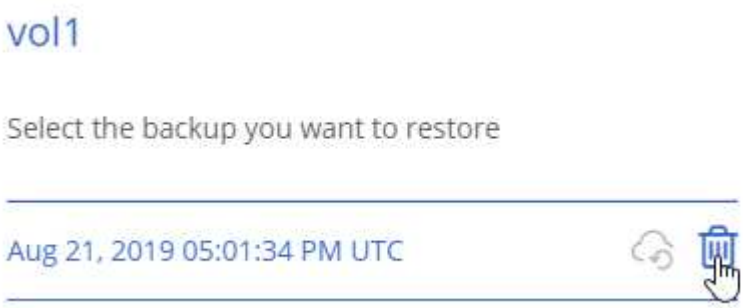


Eliminazione dei backup

Tutti i backup vengono conservati in S3 fino a quando non vengono eliminati da Cloud Manager. I backup non vengono cancellati quando si elimina un volume o quando si elimina il sistema Cloud Volumes ONTAP.

Fasi

1. Nella parte superiore di Cloud Manager, fare clic su **Backup & Restore**.
2. Selezionare un volume.
3. Individuare il backup che si desidera eliminare e fare clic sull'icona di eliminazione.



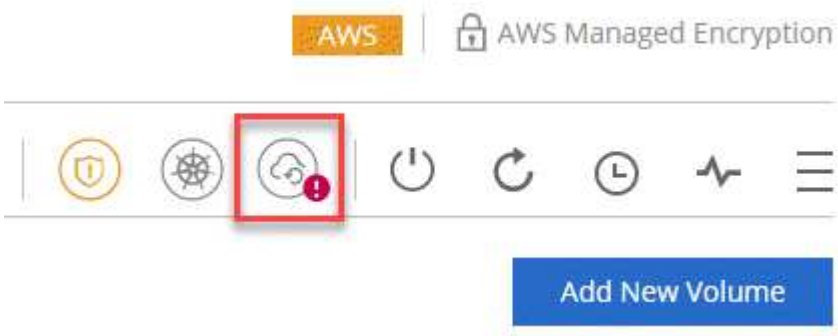
4. Confermare che si desidera eliminare il backup.

Disattivazione dei backup in S3

La disattivazione dei backup in S3 disattiva i backup di ciascun volume nel sistema. I backup esistenti non verranno eliminati.

Fasi

1. Aprire l'ambiente di lavoro.
2. Fare clic sull'icona delle impostazioni di backup.



3. Disattiva **Esegui automaticamente il backup di tutti i volumi**, quindi fai clic su **Salva**.

Funzionamento di Backup in S3

Le sezioni seguenti forniscono ulteriori informazioni sulla funzione Backup in S3.

Dove risiedono i backup

Le copie di backup vengono memorizzate in un bucket S3 di proprietà di NetApp, nella stessa regione in cui si trova il sistema Cloud Volumes ONTAP.

I backup sono incrementali

Dopo il backup completo iniziale dei dati, tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e dei nuovi blocchi.

I backup vengono eseguiti a mezzanotte

I backup giornalieri iniziano ogni giorno dopo la mezzanotte. Al momento, non è possibile pianificare le operazioni di backup in un orario specificato dall'utente.

Le copie di backup sono associate al tuo account Cloud Central

Le copie di backup sono associate a "Account Cloud Central" In cui risiede Cloud Manager.

Se si dispone di più sistemi Cloud Manager nello stesso account Cloud Central, ciascun sistema Cloud Manager visualizzerà lo stesso elenco di backup. Che include i backup associati alle istanze di Cloud Volumes ONTAP da altri sistemi di Cloud Manager.

Il criterio di backup è esteso a tutto il sistema

Il numero di backup da conservare viene definito a livello di sistema. Non è possibile impostare criteri diversi per ciascun volume del sistema.

Sicurezza

I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.

I dati viaggiano attraverso collegamenti protetti con Direct Connect al servizio ed è protetto da crittografia AES a 256 bit. I dati crittografati vengono quindi scritti nel cloud utilizzando connessioni HTTPS TLS 1.2. I dati viaggiano anche su Amazon S3 solo attraverso connessioni endpoint VPC sicure, quindi non viene inviato traffico su Internet.

A ciascun utente viene assegnata una chiave tenant, oltre a una chiave di crittografia generale di proprietà del servizio. Questo requisito è simile alla necessità di una coppia di chiavi per aprire un cliente in una banca. Tutte le chiavi, come credenziali cloud, sono memorizzate in modo sicuro dal servizio e sono limitate solo al personale NetApp responsabile della manutenzione del servizio.

Limitazioni

- Se si utilizza uno dei seguenti tipi di istanza, un sistema Cloud Volumes ONTAP può eseguire il backup di un massimo di 20 volumi in S3:
  - m4.xlange
  - m5.xlange
  - r4.xlange
  - r5.xlange
- Il backup dei volumi creati al di fuori di Cloud Manager non viene eseguito automaticamente su S3.

Ad esempio, se si crea un volume dall'interfaccia CLI di ONTAP, dall'API di ONTAP o da Gestore di sistema, il backup del volume non verrà eseguito automaticamente.

Se si desidera eseguire il backup di questi volumi, è necessario disattivare Backup in S3 e riattivarlo.

- Quando ripristini i dati da un backup, Cloud Manager esegue un ripristino completo del volume in un volume *new*. Il backup di questo nuovo volume non viene eseguito automaticamente su S3.

  Se si desidera eseguire il backup dei volumi creati da un'operazione di ripristino, è necessario disattivare Backup in S3 e riattivarlo.

- È possibile eseguire il backup di volumi di dimensioni pari o inferiori a 50 TB.
- Il backup su S3 può mantenere fino a 245 backup totali di un volume.
- Lo storage WORM non è supportato su un sistema Cloud Volumes ONTAP quando è attivato il backup su S3.

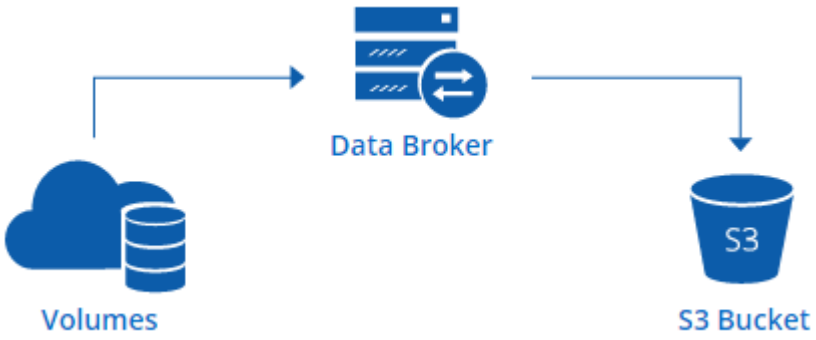
Sincronizzazione dei dati su Amazon S3

Puoi sincronizzare i dati dai volumi ONTAP a un bucket Amazon S3 integrando un ambiente di lavoro con "NetApp Cloud Sync". È quindi possibile utilizzare i dati sincronizzati come copia secondaria o per l'elaborazione dei dati utilizzando servizi AWS come EMR e Redshift.

Come funziona la funzione di sincronizzazione con S3

È possibile integrare un ambiente di lavoro con il servizio Cloud Sync in qualsiasi momento. Quando si integra un ambiente di lavoro, il servizio Cloud Sync sincronizza i dati dai volumi selezionati in un singolo bucket S3. L'integrazione funziona con gli ambienti di lavoro di Cloud Volumes ONTAP e con i cluster ONTAP on-premise o che fanno parte di una configurazione di storage privato NetApp (NPS).

Per sincronizzare i dati, il servizio avvia un'istanza del broker di dati nel VPC. Cloud Sync utilizza un data broker per ambiente di lavoro per sincronizzare i dati dai volumi a un bucket S3. Dopo la sincronizzazione iniziale, il servizio sincronizza tutti i dati modificati una volta al giorno a mezzanotte.



Se si desidera eseguire azioni Cloud Sync avanzate, accedere direttamente al servizio Cloud Sync. Da qui è possibile eseguire azioni come la sincronizzazione da S3 a un server NFS, la scelta di diversi bucket S3 per i volumi e la modifica delle pianificazioni.

14 giorni di prova gratuita

Se sei un nuovo utente Cloud Sync, i primi 14 giorni sono gratuiti. Al termine della prova gratuita, devi pagare ogni *relazione di sincronizzazione* a una tariffa oraria o acquistando licenze. Ogni volume sincronizzato con un bucket S3 è considerato una relazione di sincronizzazione. È possibile impostare entrambe le opzioni di pagamento direttamente da Cloud Sync nella pagina Impostazioni di licenza.

Come ottenere aiuto

Utilizzare le seguenti opzioni per qualsiasi supporto relativo alla funzione di sincronizzazione con S3 di Cloud Manager o per Cloud Sync in generale:

- Feedback generale sui prodotti: ng-cloudsync-contact@netapp.com
- Opzioni di supporto tecnico:
  - Community NetApp Cloud Sync
  - Chat in-product (angolo in basso a destra di Cloud Manager)

Integrazione di un ambiente di lavoro con il servizio Cloud Sync

Se si desidera sincronizzare i volumi su Amazon S3 direttamente da Cloud Manager, è necessario integrare l'ambiente di lavoro con il servizio Cloud Sync.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Fasi

1. Aprire un ambiente di lavoro e fare clic su **Sync to S3**.
2. Fare clic su **Sync** e seguire le istruzioni per sincronizzare i dati su S3.

Non è possibile sincronizzare i volumi di protezione dei dati in S3. I volumi devono essere scrivibili.

Gestione delle relazioni di sincronizzazione dei volumi

Dopo aver integrato un ambiente di lavoro con il servizio Cloud Sync, è possibile sincronizzare volumi aggiuntivi, interrompere la sincronizzazione di un volume e rimuovere l'integrazione con Cloud Sync.

Fasi

1. Nella pagina ambienti di lavoro, fare doppio clic sull'ambiente di lavoro su cui si desidera gestire le relazioni di sincronizzazione.
2. Se si desidera attivare o disattivare la sincronizzazione con S3 per un volume, selezionare il volume e fare clic su **Sync to S3** o **Delete Sync Relationship**.
3. Se si desidera eliminare tutte le relazioni di sincronizzazione per un ambiente di lavoro, fare clic sulla scheda **Sync to S3**, quindi fare clic su **Delete Sync** (Elimina sincronizzazione).

   Questa azione non elimina i dati sincronizzati dal bucket S3. Se il data broker non viene utilizzato in altre relazioni di sincronizzazione, il servizio Cloud Sync elimina il data broker.

Informazioni sul copyright

Informazioni sul marchio commerciale