



Gestione dello storage a oggetti S3

ONTAP 9

NetApp
April 24, 2024

Sommario

- Gestione dello storage a oggetti S3 1
 - Scopri il supporto S3 in ONTAP 9 1
 - Pianificare. 4
 - Configurare. 8
 - Proteggi i bucket con S3 SnapMirror 58
 - Controllare gli eventi S3 92

Gestione dello storage a oggetti S3

Scopri il supporto S3 in ONTAP 9

Panoramica della configurazione S3

A partire da ONTAP 9.8, è possibile attivare un server di storage a oggetti S3 (Simple Storage Service) di ONTAP in un cluster ONTAP.

ONTAP supporta due scenari di casi d'utilizzo on-premise per il servizio dello storage a oggetti S3:

- Tier FabricPool per un bucket su cluster locale (Tier to a local bucket) o cluster remoto (Tier cloud).
- Accesso dell'applicazione client S3 a un bucket sul cluster locale o su un cluster remoto.

A partire da ONTAP 9.14.1, è possibile abilitare un server per lo storage a oggetti S3 su una SVM in un aggregato con mirroring o senza mirror nelle configurazioni IP e FC di MetroCluster.

A partire da ONTAP 9.12.1, è possibile abilitare un server di storage a oggetti S3 su una SVM in un aggregato senza mirror in una configurazione IP MetroCluster. Per ulteriori informazioni sulle limitazioni degli aggregati senza mirror nelle configurazioni MetroCluster IP, vedere ["Considerazioni per gli aggregati senza mirror"](#).

Utilizzare queste procedure se si desidera configurare lo storage a oggetti S3 nel modo seguente:

- Si desidera fornire lo storage a oggetti S3 da un cluster esistente che esegue ONTAP.

ONTAP S3 è adatto per le funzionalità S3 sui cluster esistenti senza hardware e gestione aggiuntivi. Tuttavia, il software NetApp StorageGRID continua a essere la soluzione NetApp di punta per lo storage a oggetti. Per ulteriori informazioni, consultare ["Documentazione StorageGRID"](#).

- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

Configurazione S3 con Gestore di sistema e CLI ONTAP

È possibile configurare e gestire ONTAP S3 con Gestore di sistema e l'interfaccia utente di ONTAP. Quando si attiva S3 e si creano bucket utilizzando Gestione sistema, ONTAP seleziona le impostazioni predefinite delle Best practice per una configurazione semplificata. Se è necessario specificare i parametri di configurazione, è possibile utilizzare l'interfaccia utente di ONTAP. Se si configurano il server S3 e i bucket dalla CLI, è comunque possibile gestirli con System Manager, se lo si desidera, o viceversa.

Quando si crea un bucket S3 utilizzando Gestione di sistema, ONTAP configura un livello di servizio delle performance predefinito il più alto disponibile sul sistema. Ad esempio, su un sistema AFF, l'impostazione predefinita è **estrema**. I livelli di servizio delle performance sono gruppi di criteri QoS (Quality of Service) adattivi predefiniti. Invece di uno dei livelli di servizio predefiniti, è possibile specificare un gruppo di criteri QoS personalizzato o nessun gruppo di criteri.

I gruppi di policy QoS adattivi predefiniti sono:

- **Extreme:** Utilizzato per le applicazioni che si aspettano la latenza più bassa e le performance più elevate.
- **Performance:** Utilizzato per applicazioni con esigenze di performance e latenza modeste.
- **Valore:** Utilizzato per applicazioni per le quali throughput e capacità sono più importanti della latenza.
- **Custom:** Specificare un criterio QoS personalizzato o nessun criterio QoS.

Se si seleziona **Use for Tiering** (Usa per il tiering), non viene selezionato alcun livello di servizio delle performance e il sistema tenta di selezionare supporti a basso costo con performance ottimali per i dati a più livelli.

Vedere anche: ["Utilizzare gruppi di policy QoS adattivi"](#).

ONTAP tenta di eseguire il provisioning di questo bucket su Tier locali che dispongono dei dischi più appropriati, soddisfacendo il livello di servizio scelto. Tuttavia, se è necessario specificare quali dischi includere nel bucket, è consigliabile configurare lo storage a oggetti S3 dalla CLI specificando i Tier locali (aggregato). Se si configura il server S3 dalla CLI, è comunque possibile gestirlo con System Manager, se necessario.

Se si desidera specificare gli aggregati da utilizzare per i bucket, è possibile farlo solo utilizzando la CLI.

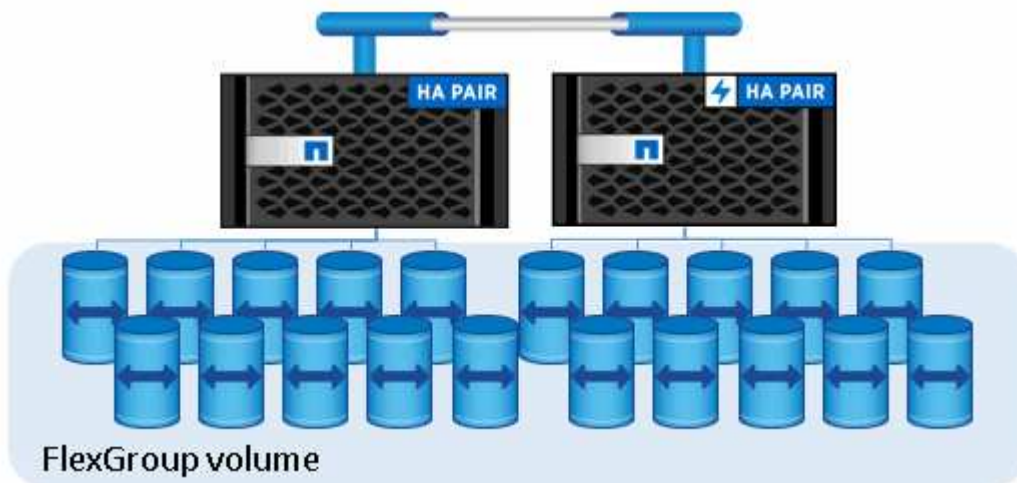
Configurazione dei bucket S3 su Cloud Volumes ONTAP

Se si desidera utilizzare i bucket di Cloud Volumes ONTAP, si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza. Pertanto, negli ambienti Cloud Volumes ONTAP, è necessario [Configurare i bucket S3 dalla CLI](#).

In caso contrario, i server S3 su Cloud Volumes ONTAP vengono configurati e mantenuti allo stesso modo in Cloud Volumes ONTAP come negli ambienti on-premise.

Architettura

In ONTAP, l'architettura sottostante per un bucket è un volume FlexGroup, ovvero un singolo namespace costituito da più volumi membri costituenti, ma gestito come un singolo volume.

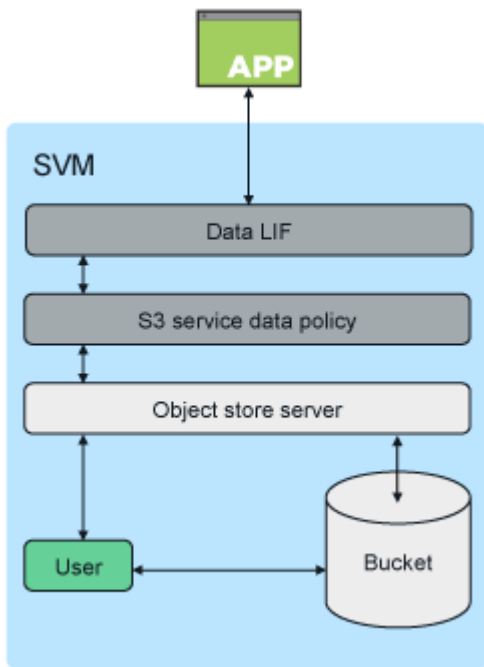


I bucket sono limitati solo dai massimi fisici dell'hardware sottostante e i massimi architetturici potrebbero essere più elevati. I bucket possono sfruttare il dimensionamento elastico di FlexGroup per far crescere automaticamente un componente di un volume FlexGroup se lo spazio è esaurito. Esiste un limite di 1000 bucket per volume FlexGroup o di 1/3 della capacità del volume FlexGroup (per tenere conto della crescita dei dati nei bucket).



Non è consentito l'accesso al protocollo NAS o SAN al volume FlexGroup che contiene bucket S3.

L'accesso al bucket viene fornito tramite utenti autorizzati e applicazioni client.



Casi di utilizzo

Esistono tre casi di utilizzo principali per l'accesso client ai servizi ONTAP S3:

- Per i sistemi ONTAP che utilizzano ONTAP S3 come Tier di capacità FabricPool remota (cloud)

Il server S3 e il bucket contenente il Tier di capacità (per *cold* dati) si trovano su un cluster diverso dal Tier di performance (per *hot* dati).

- Per i sistemi ONTAP che utilizzano ONTAP S3 come Tier FabricPool locale

Il server S3 e il bucket contenente il Tier di capacità si trovano sullo stesso cluster, ma su una coppia ha diversa, come il Tier di performance.

- Per applicazioni client S3 esterne

ONTAP S3 serve applicazioni client S3 eseguite su sistemi non NetApp.

È consigliabile fornire l'accesso ai bucket ONTAP S3 utilizzando HTTPS. Quando HTTPS è attivato, i certificati di sicurezza sono necessari per la corretta integrazione con SSL/TLS. Gli utenti client' devono quindi autenticare l'utente con ONTAP S3 e autorizzare le autorizzazioni di accesso degli utenti' per le operazioni in ONTAP S3. L'applicazione client deve anche avere accesso al certificato CA principale (certificato firmato dal server ONTAP S3) per poter autenticare il server e creare una connessione sicura tra client e server.

Gli utenti vengono creati all'interno della SVM abilitata per S3 e le relative autorizzazioni di accesso possono essere controllate a livello di bucket o SVM, ovvero possono avere accesso a uno o più bucket all'interno della SVM.

HTTPS è attivato per impostazione predefinita sui server ONTAP S3. È possibile disattivare HTTPS e attivare HTTP per l'accesso al client, nel qual caso non è richiesta l'autenticazione mediante certificati CA. Tuttavia, quando HTTP è attivato e HTTPS è disattivato, tutte le comunicazioni con il server ONTAP S3 vengono inviate

sulla rete in testo non crittografato.

Per ulteriori informazioni, vedere ["Report tecnico: Le Best practice S3 in ONTAP"](#)

Informazioni correlate

["Gestione dei volumi FlexGroup"](#)

Pianificare

Supporto della versione di ONTAP per lo storage a oggetti S3

ONTAP supporta lo storage a oggetti S3 per ambienti on-premise a partire da ONTAP 9.8. Cloud Volumes ONTAP supporta lo storage a oggetti S3 per ambienti cloud a partire da ONTAP 9.9.1.

Supporto S3 con Cloud Volumes ONTAP

ONTAP S3 è configurato e funziona allo stesso modo in Cloud Volumes ONTAP come negli ambienti on-premise, con un'eccezione:

- Gli aggregati sottostanti devono provenire da un solo nodo. Scopri di più ["Creazione di bucket in ambienti CVO"](#).

Provider di cloud	Versione di ONTAP
Azure	ONTAP 9.9.1 e versioni successive
AWS	ONTAP 9.11.0 e versioni successive
Google Cloud	ONTAP 9.12.1 e versioni successive

Anteprima pubblica S3 in ONTAP 9.7

In ONTAP 9.7, lo storage a oggetti S3 è stato introdotto come anteprima pubblica. Tale versione non era destinata agli ambienti di produzione e non sarà più aggiornata a partire da ONTAP 9.8. Solo ONTAP 9.8 e versioni successive supportano lo storage a oggetti S3 negli ambienti di produzione.

I bucket S3 creati con l'anteprima pubblica 9.7 possono essere utilizzati in ONTAP 9.8 e versioni successive, ma non possono sfruttare i miglioramenti delle funzionalità. Se si dispone di bucket creati con l'anteprima pubblica 9.7, è necessario migrare il contenuto di tali bucket in 9.8 bucket per il supporto delle funzionalità, la sicurezza e i miglioramenti delle performance.

Azioni supportate da ONTAP S3

Le azioni di ONTAP S3 sono supportate dalle API REST S3 standard, ad eccezione di quanto indicato di seguito. Per ulteriori informazioni, vedere ["Riferimento API Amazon S3"](#).

Operazioni della benna

In ONTAP sono supportate le seguenti operazioni utilizzando le API AWS S3:

Funzionamento della benna	Supporto ONTAP a partire da
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1 + * sono supportate solo le azioni di scadenza
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
HeadBucket	ONTAP 9.8
ListBucket	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
PutBucket	<ul style="list-style-type: none"> • ONTAP 9.11.1 • ONTAP 9,8: Supportato solo con API REST ONTAP
PutBucketLifecycleConfiguration	ONTAP 9.13.1 + * sono supportate solo le azioni di scadenza
PutBucketPolicy	ONTAP 9.12.1

Operazioni a oggetti

A partire da ONTAP 9.9.1, ONTAP S3 supporta metadati e tagging degli oggetti.

- PutObject e CreateMultipartUpload includono coppie chiave-valore utilizzando `x-amz-meta-<key>`.

Ad esempio: `x-amz-meta-project: ontap_s3`.

- GetObject. E HeadObject restituiscono metadati definiti dall'utente.
- A differenza dei metadati, i tag possono essere letti indipendentemente dagli oggetti utilizzando:
 - PutObjectTagging
 - GetObjectTagging
 - DeleteObjectTagging

A partire da ONTAP 9.11.1, ONTAP S3 supporta il controllo della versione degli oggetti e le azioni associate a queste API ONTAP:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

Operazione a oggetti	Supporto ONTAP a partire da
AbortMultipartUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
Oggetto CopyObject	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9.8
DeleteObject (Elimina oggetto)	ONTAP 9.8
DeleteObjects	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetention	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
HeadObject (oggetto intestazione)	ONTAP 9.8
ListMultipartUpload	ONTAP 9.8
ListObjects (oggetti elenco)	ONTAP 9.8
ListObjectsV2	ONTAP 9.8
ListBucketVersions	ONTAP 9.11.1
ListParts	ONTAP 9.8
PutBucketVersioning	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObjectRetention	ONTAP 9.14.1
PutObjectTagging	ONTAP 9.9.1
UploadPart	ONTAP 9.8
UploadPartCopy	ONTAP 9.12.1

Policy di gruppo

Queste operazioni non sono specifiche di S3 e sono generalmente associate ai processi di identità e gestione (IAM). ONTAP supporta questi comandi ma non utilizza le API REST IAM.

- Crea policy
- Policy AttachGroup

Gestione degli utenti

Queste operazioni non sono specifiche di S3 e sono generalmente associate ai processi IAM.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

Interoperabilità di ONTAP S3

Il server ONTAP S3 interagisce normalmente con altre funzionalità di ONTAP, ad eccezione di quanto indicato in questa tabella.

Area delle funzioni	Supportato	Non supportato
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Client Azure in ONTAP 9.9.1 e versioni successive • Client AWS in ONTAP 9.11.0 e versioni successive • Client Google Cloud in ONTAP 9.12.1 e versioni successive 	<ul style="list-style-type: none"> • Cloud Volumes ONTAP per qualsiasi client in ONTAP 9.8 e versioni precedenti
Protezione dei dati	<ul style="list-style-type: none"> • Cloud Sync • "Versione degli oggetti" (A partire da ONTAP 9.11.1) • "S3 SnapMirror" (A partire da ONTAP 9.10.1) • Configurazioni IP MetroCluster (a partire da ONTAP 9.12.1) • SnapLock (a partire da ONTAP 9.14.1) • WORM (a partire da ONTAP 9.14.1) 	<ul style="list-style-type: none"> • Erasure coding • Gestione del ciclo di vita delle informazioni • NDMP • SMTape • SnapMirror Cloud • Disaster recovery SVM • SyncMirror • Copie Snapshot create dall'utente
Crittografia	<ul style="list-style-type: none"> • NetApp aggregate Encryption (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL 	<ul style="list-style-type: none"> • SCORIE
Efficienza dello storage	<ul style="list-style-type: none"> • Deduplica • Compressione • Compattazione 	<ul style="list-style-type: none"> • Efficienze a livello di aggregato • Clone di volume del volume FlexGroup contenente i bucket ONTAP S3
Virtualizzazione dello storage	-	Virtualizzazione NetApp FlexArray

Area delle funzioni	Supportato	Non supportato
Qualità del servizio (QoS)	<ul style="list-style-type: none"> • QoS massimi (limiti) • QoS minimi (piani) 	-
Funzionalità aggiuntive	<ul style="list-style-type: none"> • "Controllare gli eventi S3" (A partire da ONTAP 9.10.1) 	<ul style="list-style-type: none"> • Volumi FlexCache • FPolicy • Qtree • Quote

Soluzioni di terze parti validate da ONTAP S3

NetApp ha validato le seguenti soluzioni di terze parti per l'utilizzo con ONTAP S3. Se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

Soluzioni di terze parti validate su ONTAP S3

NetApp ha testato queste soluzioni in collaborazione con i rispettivi partner.

- Amazon SageMaker
- Client Apache Hadoop S3A
- Apache Kafka
- CommVault (V11)
- Kafka confluyente
- Red Hat Quay
- Rubrik
- Fiocco di neve
- Trino
- Veeam (V12)

Configurare

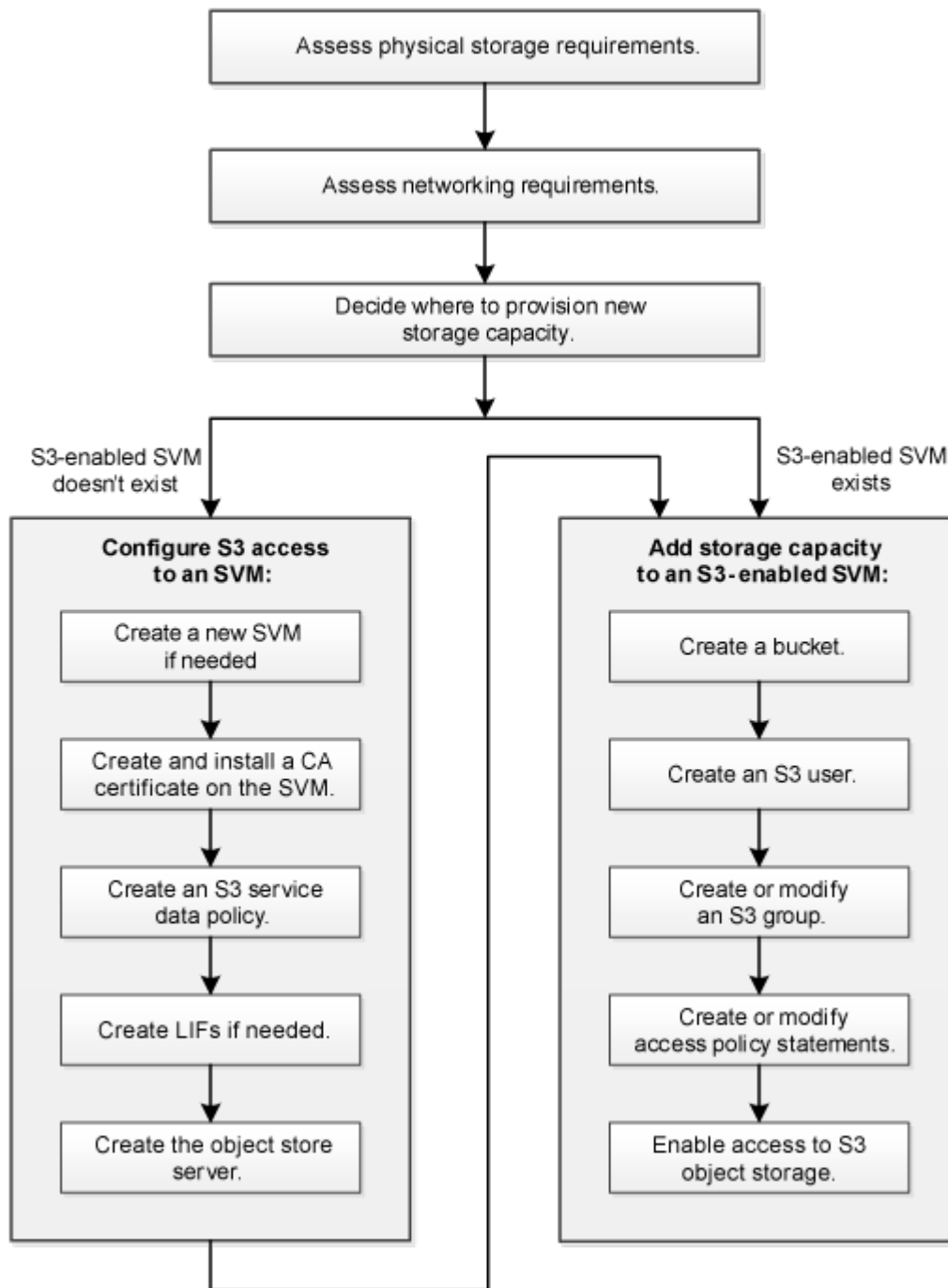
Informazioni sul processo di configurazione S3

Workflow di configurazione S3

La configurazione di S3 implica la valutazione dei requisiti di storage fisico e di rete, quindi la scelta di un workflow specifico per il tuo obiettivo: Configurare l'accesso S3 a una SVM nuova o esistente oppure aggiungere un bucket e utenti a una SVM esistente già completamente configurata per l'accesso S3.

Quando si configura l'accesso S3 a una nuova macchina virtuale di storage utilizzando System Manager, viene richiesto di inserire le informazioni relative a certificato e rete e di creare la macchina virtuale di storage e il

server di storage a oggetti S3 in una singola operazione.



Valutare i requisiti di storage fisico

Prima di eseguire il provisioning dello storage S3 per i client, è necessario assicurarsi che vi sia spazio sufficiente negli aggregati esistenti per il nuovo archivio di oggetti. In caso contrario, è possibile aggiungere dischi agli aggregati esistenti o creare nuovi aggregati del tipo e della posizione desiderati.

A proposito di questa attività

Quando si crea un bucket S3 in una SVM abilitata per S3, viene creato automaticamente un volume FlexGroup per supportare il bucket. È possibile lasciare che ONTAP Select gli aggregati sottostanti e i componenti

FlexGroup automaticamente (impostazione predefinita) oppure selezionare gli aggregati sottostanti e i componenti FlexGroup autonomamente.

Se si decide di specificare gli aggregati e i componenti FlexGroup, ad esempio se si dispone di requisiti di performance specifici per i dischi sottostanti, è necessario assicurarsi che la configurazione dell'aggregato sia conforme alle linee guida delle Best practice per il provisioning di un volume FlexGroup. Scopri di più:

- ["Gestione dei volumi FlexGroup"](#)
- ["Report tecnico NetApp 4571-a: Best practice per il volume NetApp ONTAP FlexGroup"](#)

Se si utilizzano bucket di Cloud Volumes ONTAP, si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza. Scopri di più ["Creazione di bucket per Cloud Volumes ONTAP"](#).

È possibile utilizzare il server ONTAP S3 per creare un Tier di capacità FabricPool locale, ovvero nello stesso cluster del Tier di performance. Questo può essere utile, ad esempio, se si dispone di dischi SSD collegati a una coppia ha e si desidera eseguire il tiering dei dati *cold* su dischi HDD in un'altra coppia ha. In questo caso di utilizzo, il server S3 e il bucket contenente il Tier di capacità locale devono pertanto trovarsi in una coppia ha diversa dal Tier di performance. Il tiering locale non è supportato nei cluster a un nodo e a due nodi.

Fasi

1. Visualizzare lo spazio disponibile negli aggregati esistenti:

```
storage aggregate show
```

Se esiste un aggregato con spazio sufficiente o una posizione del nodo richiesta, registrare il nome della configurazione S3.

```
cluster-1::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_4	239.0GB	238.9GB	95%	online	5	node3	raid_dp, normal
aggr_5	239.0GB	239.0GB	95%	online	4	node4	raid_dp, normal

6 entries were displayed.

2. Se non sono presenti aggregati con spazio sufficiente o posizione del nodo richiesta, aggiungere i dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

Valutare i requisiti di rete

Prima di fornire storage S3 ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning S3.

Prima di iniziare

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

A proposito di questa attività

Per i Tier di capacità FabricPool (cloud) remoti e i client S3 remoti, è necessario utilizzare una SVM di dati e configurare le LIF di dati. Per i livelli cloud FabricPool, è necessario configurare anche le LIF tra cluster; il peering dei cluster non è richiesto.

Per i Tier di capacità FabricPool locali, è necessario utilizzare la SVM di sistema (chiamata "Cluster"), ma sono disponibili due opzioni per la configurazione LIF:

- È possibile utilizzare le LIF del cluster.

In questa opzione, non è richiesta alcuna ulteriore configurazione LIF, ma il traffico sulle LIF del cluster aumenterà. Inoltre, il Tier locale non sarà accessibile ad altri cluster.

- È possibile utilizzare le LIF di dati e intercluster.

Questa opzione richiede un'ulteriore configurazione, inclusa l'abilitazione delle LIF per il protocollo S3, ma il Tier locale sarà accessibile anche come Tier cloud FabricPool remoto ad altri cluster.

Fasi

1. Visualizzare le porte fisiche e virtuali disponibili:

```
network port show
```

- Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
- Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.

2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti:

```
network subnet show
```

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

3. Visualizzare gli spazi IP disponibili:

```
network ipspace show
```

È possibile utilizzare l'IPSpace predefinito o un IPSpace personalizzato.

4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster:

```
network options ipv6 show
```

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

Decidere dove eseguire il provisioning della nuova capacità di storage S3

Prima di creare un nuovo bucket S3, è necessario decidere se posizionarlo in una SVM nuova o esistente. Questa decisione determina il tuo flusso di lavoro.

Scelte

- Se si desidera eseguire il provisioning di un bucket in un nuovo SVM o SVM non abilitato per S3, completare la procedura descritta nei seguenti argomenti.

["Creare una SVM per S3"](#)

["Creare un bucket per S3"](#)

Sebbene S3 possa coesistere in una SVM con NFS e SMB, è possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando S3 su un cluster per la prima volta.
 - Esistono SVM in un cluster in cui non si desidera attivare il supporto S3.
 - Si dispone di una o più SVM abilitate per S3 in un cluster e si desidera un altro server S3 con caratteristiche di performance diverse. Dopo aver attivato S3 sulla SVM, procedere con il provisioning di un bucket.
- Se si desidera eseguire il provisioning del bucket iniziale o di un bucket aggiuntivo su una SVM abilitata S3 esistente, completare la procedura descritta nel seguente argomento.

["Creare un bucket per S3"](#)

Configurare l'accesso S3 a una SVM

Creare una SVM per S3

Sebbene S3 possa coesistere con altri protocolli in una SVM, potrebbe essere necessario creare una nuova SVM per isolare lo spazio dei nomi e il carico di lavoro.

A proposito di questa attività

Se si fornisce solo lo storage a oggetti S3 da una SVM, il server S3 non richiede alcuna configurazione DNS. Tuttavia, se si utilizzano altri protocolli, è possibile configurare il DNS sulla SVM.

Quando si configura l'accesso S3 a una nuova macchina virtuale di storage utilizzando System Manager, viene richiesto di inserire le informazioni relative a certificato e rete e di creare la macchina virtuale di storage e il

server di storage a oggetti S3 in una singola operazione.

Esempio 1. Fasi

System Manager

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

Se si utilizza un certificato firmato da una CA esterna, viene richiesto di inserirlo durante questa procedura; è inoltre possibile utilizzare un certificato generato dal sistema.

1. Abilitare S3 su una VM di storage.

- a. Aggiungere una nuova VM di storage: Fare clic su **Storage > Storage VMS**, quindi fare clic su **Add** (Aggiungi).

Se si tratta di un nuovo sistema senza macchine virtuali di storage esistenti, fare clic su **Dashboard > Configure Protocols** (Configura protocolli).

Se si aggiunge un server S3 a una VM di storage esistente: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **S3**.

- a. Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- b. Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

- c. Inserire le interfacce di rete.

2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.

- La chiave segreta non viene visualizzata di nuovo.
- Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

CLI

1. Verificare che S3 sia concesso in licenza sul cluster:

```
system license show -package s3
```

In caso contrario, contattare il rappresentante commerciale.

2. Creare una SVM:


```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- Utilizzare l'impostazione UNIX per `-rootvolume-security-style` opzione.
- Utilizzare il C.UTF-8 predefinito `-language` opzione.
- Il `ipSPACE` l'impostazione è facoltativa.

3. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver <svm_name>
```

Il `Vserver Operational State` il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPSPACE `ipSPACEA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipSPACE ipSPACEA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione. Per impostazione predefinita, l'account utente `vsadmin` viene creato e si trova in `locked` stato. Il ruolo `vsadmin` viene assegnato all'account utente `vsadmin` predefinito.

```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

Creare e installare un certificato CA sulla SVM

Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority).

A proposito di questa attività

Sebbene sia possibile configurare un server S3 in modo che utilizzi solo HTTP e sebbene sia possibile configurare i client senza un requisito di certificato CA, è consigliabile proteggere il traffico HTTPS ai server ONTAP S3 con un certificato CA.

Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

Le istruzioni di questa procedura consentono di creare e installare un certificato autofirmato ONTAP. Sono supportati anche i certificati CA di fornitori terzi; per ulteriori informazioni, consultare la documentazione di autenticazione dell'amministratore.

"Autenticazione amministratore e RBAC"

Vedere `security certificate` pagine man per ulteriori opzioni di configurazione.

Fasi

1. Creare un certificato digitale autofirmato:

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

Il `-type root-ca` L'opzione crea e installa un certificato digitale autofirmato per firmare altri certificati agendo come autorità di certificazione (CA).

Il `-common-name` L'opzione crea il nome dell'autorità di certificazione (CA) di SVM e verrà utilizzata per generare il nome completo del certificato.

La dimensione predefinita del certificato è 2048 bit.

Esempio

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

The certificate's generated name for reference:
svm1_ca_159D1587CE21E9D4_svm1_ca

Quando viene visualizzato il nome generato del certificato, assicurarsi di salvarlo per i passaggi successivi di questa procedura.

2. Generare una richiesta di firma del certificato:

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

Il `-common-name` Il parametro per la richiesta di firma deve essere il nome del server S3 (FQDN).

Se lo si desidera, è possibile fornire la posizione e altre informazioni dettagliate sulla SVM.

Viene richiesto di conservare una copia della richiesta di certificato e della chiave privata per riferimenti futuri.

3. Firmare la CSR utilizzando SVM_CA per generare il certificato del server S3:

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Immettere le opzioni di comando utilizzate nei passaggi precedenti:

- `-ca` — il nome comune della CA immesso nel passaggio 1.
- `-ca-serial` — il numero di serie della CA dal punto 1. Ad esempio, se il nome del certificato CA è `svm1_ca_159D1587CE21E9D4_svm1_ca`, il numero di serie è `159D1587CE21E9D4`.

Per impostazione predefinita, il certificato firmato scadrà tra 365 giorni. È possibile selezionare un altro valore e specificare altri dettagli della firma.

Quando richiesto, copiare e inserire la stringa di richiesta del certificato salvata nel passaggio 2.

Viene visualizzato un certificato firmato; salvarlo per un utilizzo successivo.

4. Installare il certificato firmato sulla SVM abilitata per S3:

```
security certificate install -type server -vserver svm_name
```

Quando richiesto, inserire il certificato e la chiave privata.

Se si desidera inserire una catena di certificati, è possibile immettere i certificati intermedi.

Quando vengono visualizzate la chiave privata e il certificato digitale firmato dalla CA, salvarle per riferimenti futuri.

5. Ottenere il certificato della chiave pubblica:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Salvare il certificato della chiave pubblica per una configurazione successiva lato client.

Esempio

```

cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca -instance

                Name of Vserver: svm1.example.com
                FQDN or Custom Common Name: svm1_ca
                Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                Type of Certificate: root-ca
                (DEPRECATED)-Certificate Subtype: -
                Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
                Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
                State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
                Self-Signed Certificate: true
                Is System Internal Certificate: false

```

Creare una policy sui dati del servizio S3

È possibile creare policy di servizio per i dati S3 e i servizi di gestione. Per abilitare il traffico dati S3 su LIF, è necessaria una policy dei dati del servizio S3.

A proposito di questa attività

Se si utilizzano LIF di dati e LIF di intercluster, è necessaria una policy sui dati di servizio S3. Non è necessario se si utilizzano le LIF del cluster per il caso di utilizzo del tiering locale.

Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di protocolli dati per la LIF.

Sebbene sia possibile configurare più protocolli per SVM e LIFF, è consigliabile che S3 sia l'unico protocollo per la fornitura di dati a oggetti.

Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Creare una policy sui dati del servizio:

```
network interface service-policy create -vserver svm_name -policy policy_name  
-services data-core,data-s3-server
```

Il data-core e. data-s3-server I servizi sono gli unici necessari per abilitare ONTAP S3, anche se è possibile includere altri servizi in base alle esigenze.

Creazione di LIF di dati

Se hai creato una nuova SVM, le LIF dedicate create per l'accesso S3 dovrebbero essere le LIF dei dati.

Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- La politica di servizio LIF deve già esistere.

A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- Se si abilita il tiering remoto della capacità FabricPool (cloud), è necessario configurare anche le LIF intercluster.

Fasi

1. Creare una LIF:

```
network interface create -vserver svm_name -lif lif_name -service-policy  
service_policy_names -home-node node_name -home-port port_name {-address  
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy  
data -auto-revert {true|false}
```

- -home-node È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- -home-port È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.

- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.
- Il `-service-policy` l'opzione specifica la policy creata per i dati e i servizi di gestione e qualsiasi altra policy necessaria.

2. Se si desidera assegnare un indirizzo IPv6 in `-address` opzione:

- Utilizzare `network ndp prefix show` Per visualizzare l'elenco dei prefissi RA appresi su varie interfacce.

Il `network ndp prefix show` il comando è disponibile a livello di privilegio avanzato.

- Utilizzare il formato `prefix:id` Per costruire manualmente l'indirizzo IPv6.

`prefix` è il prefisso appreso sulle varie interfacce.

Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

3. Verificare che la LIF sia stata creata correttamente utilizzando `network interface show` comando.

4. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

Esempi

Il comando seguente mostra come creare una LIF di dati S3 assegnata a `my-S3-policy` politica di servizio:

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF datalif1 e datalif3 sono configurati con indirizzi IPv4 e datalif4 è configurato con un indirizzo IPv6:

```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port
Home					
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
true					
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
true					
	datalif4	up/up	2001::2/64	node-2	e0c
true					

5 entries were displayed.

Creazione di LIF intercluster per tiering FabricPool remoto

Se si abilita il tiering della capacità FabricPool remota (cloud) utilizzando ONTAP S3, è necessario configurare le LIF tra cluster. È possibile configurare le LIF di intercluster sulle

porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- La politica di servizio LIF deve già esistere.

A proposito di questa attività

Le LIF intercluster non sono richieste per il tiering del pool di fabric locale o per la fornitura di applicazioni S3 esterne.

Fasi

1. Elencare le porte nel cluster:

```
network port show
```

L'esempio seguente mostra le porte di rete in cluster01:

```
cluster01::> network port show
```

(Mbps)					Speed	
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper

cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

2. Creazione di LIF intercluster sulla SVM di sistema:

```
network interface create -vserver Cluster -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

Nell'esempio seguente vengono create le LIF tra cluster cluster01_icl01 e cluster01_icl02:

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

3. Verificare che le LIF dell'intercluster siano state create:

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

4. Verificare che le LIF dell'intercluster siano ridondanti:

```
network interface show -service-policy default-intercluster -failover
```

L'esempio seguente mostra che le LIF dell'intercluster cluster01_icl01 e cluster01_icl02 su e0c viene eseguito il failover della porta su e0d porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01				
	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-01:e0c,	
			cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-02:e0c,	
			cluster01-02:e0d	

Creare il server archivio oggetti S3

Il server di archiviazione a oggetti ONTAP gestisce i dati come oggetti S3, invece dello storage a blocchi o file fornito dai server NAS e SAN ONTAP.

Prima di iniziare

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN non deve iniziare con un nome bucket.

È necessario disporre di un certificato CA autofirmato (creato nei passaggi precedenti) o di un certificato firmato da un vendor CA esterno. Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

A proposito di questa attività

Quando viene creato un server archivio oggetti, viene creato un utente root con UID 0. Per questo utente root non viene generata alcuna chiave di accesso o chiave segreta. L'amministratore di ONTAP deve eseguire `object-store-server users regenerate-keys` per impostare la chiave di accesso e la chiave segreta per questo utente.



Come Best practice NetApp, non utilizzare questo utente root. Qualsiasi applicazione client che utilizza la chiave di accesso o la chiave segreta dell'utente root ha accesso completo a tutti i bucket e gli oggetti nell'archivio di oggetti.

Vedere `vserver object-store-server` pagine man per ulteriori opzioni di configurazione e visualizzazione.


Esempio 2. Fasi

System Manager

Utilizzare questa procedura se si aggiunge un server S3 a una VM di storage esistente. Per aggiungere un server S3 a una nuova VM di storage, vedere ["Creare una SVM di storage per S3"](#).

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

1. Abilitare S3 su una VM di storage esistente.

- Selezionare la VM di storage: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **S3**.
- Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

d. Inserire le interfacce di rete.

2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.

- La chiave segreta non viene visualizzata di nuovo.
- Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

CLI

1. Creare il server S3:

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- In caso di configurazione del tiering locale, il nome della SVM può essere un nome di una SVM dati o di una SVM di sistema (cluster).
- Il nome del certificato deve essere il nome del certificato del server (certificato dell'utente finale o del foglio) e non il certificato della CA del server (certificato della CA intermedia o di origine).
- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con `-secure-listener-port` opzione.

Quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.

- HTTP è disattivato per impostazione predefinita. Quando questa opzione è attivata, il server è in attesa sulla porta 80. È possibile attivarlo con `-is-http-enabled` oppure modificare il numero di porta con il `-listener-port` opzione.

Quando HTTP è attivato, la richiesta e le risposte vengono inviate in rete in formato non

crittografato.

2. Verificare che S3 sia configurato:

```
vserver object-store-server show
```

Esempio

Questo comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show

Vserver: vs1

      Object Store Server Name: s3.example.com
      Administrative State: up
      Listener Port For HTTP: 80
      Secure Listener Port For HTTPS: 443
      HTTP Enabled: false
      HTTPS Enabled: true
      Certificate for HTTPS Connections: svm1_ca
      Comment: Server comment
```

Aggiungere capacità di storage a una SVM abilitata per S3

Creare un bucket

Gli oggetti S3 sono conservati in *bucket*. Non sono nidificati come file all'interno di una directory all'interno di altre directory.

Prima di iniziare

Una VM di storage contenente un server S3 deve già esistere.

A proposito di questa attività

- A partire da ONTAP 9.14.1, il ridimensionamento automatico è stato abilitato sui volumi FlexGroup S3 quando vengono creati i bucket su di essi. In questo modo si elimina l'allocazione eccessiva di capacità durante la creazione del bucket su volumi FlexGroup nuovi ed esistenti. I volumi FlexGroup vengono ridimensionati a una dimensione minima richiesta in base alle seguenti linee guida. La dimensione minima richiesta è la dimensione totale di tutti i bucket S3 in un volume FlexGroup.
 - A partire da ONTAP 9.14.1, se viene creato un volume FlexGroup S3 come parte di una nuova creazione di bucket, il volume FlexGroup viene creato con le dimensioni minime richieste.
 - Se è stato creato un volume S3 FlexGroup prima di ONTAP 9.14.1, il primo bucket creato o eliminato successivamente a ONTAP 9.14.1 ridimensiona il volume FlexGroup alla dimensione minima richiesta.
 - Se un volume S3 FlexGroup è stato creato prima di ONTAP 9.14.1 e aveva già le dimensioni minime richieste, la creazione o l'eliminazione di un bucket successivo a ONTAP 9.14.1 mantiene le dimensioni del volume S3 FlexGroup.
- I livelli di servizio dello storage sono gruppi di criteri QoS (Quality of Service) adattivi predefiniti, con livelli

predefiniti *value*, *performance* e *Extreme*. Invece di uno dei livelli di servizio storage predefiniti, è possibile definire un gruppo di policy QoS personalizzato e applicarlo a un bucket. Per ulteriori informazioni sulle definizioni dei servizi di archiviazione, vedere ["Definizioni dei servizi di storage"](#). Per ulteriori informazioni sulla gestione delle prestazioni, vedere ["Gestione delle performance"](#).

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

- Se stai configurando il tiering locale della capacità, creerai bucket e utenti in una VM per lo storage dei dati, non nella VM di storage del sistema in cui si trova il server S3.
- Per l'accesso client remoto, è necessario configurare i bucket in una VM di storage abilitata per S3. Se si crea un bucket in una VM storage non abilitata per S3, sarà disponibile solo per il tiering locale.
- A partire da ONTAP 9.14.1, è possibile ["Crea un bucket su un aggregato con mirroring o senza mirror in una configurazione MetroCluster"](#).
- Per la CLI, quando si crea un bucket, sono disponibili due opzioni di provisioning:
 - Lasciare ONTAP Select gli aggregati sottostanti e i componenti FlexGroup (impostazione predefinita)
 - ONTAP crea e configura un volume FlexGroup per il primo bucket selezionando automaticamente gli aggregati. Verrà selezionato automaticamente il livello di servizio più alto disponibile per la piattaforma oppure sarà possibile specificare il livello di servizio storage. Tutti i bucket aggiuntivi che Aggiungi in seguito nella VM di storage avranno lo stesso volume FlexGroup sottostante.
 - In alternativa, è possibile specificare se il bucket verrà utilizzato per il tiering, nel qual caso ONTAP tenta di selezionare supporti a basso costo con performance ottimali per i dati su più livelli.
 - Si selezionano gli aggregati sottostanti e i componenti FlexGroup (richiede opzioni avanzate dei comandi con privilegi): Si può selezionare manualmente gli aggregati in cui deve essere creato il bucket e il volume FlexGroup contenente, quindi specificando il numero dei componenti in ogni aggregato. Quando si aggiungono bucket aggiuntivi:
 - Se si specificano aggregati e costituenti per un nuovo bucket, verrà creato un nuovo FlexGroup per il nuovo bucket.
 - Se non si specificano aggregati e componenti per un nuovo bucket, il nuovo bucket verrà aggiunto a un FlexGroup esistente. Vedere [Gestione dei volumi FlexGroup](#) per ulteriori informazioni.

Quando si specificano aggregati e costituenti durante la creazione di un bucket, non vengono applicati gruppi di criteri QoS, predefiniti o personalizzati. È possibile farlo in un secondo momento con `vserver object-store-server bucket modify` comando.

Vedere ["vserver object-store-server modifica bucket"](#) per ulteriori informazioni.

Nota: se si utilizzano bucket da Cloud Volumes ONTAP, è necessario utilizzare la procedura CLI. Si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza.

Crea bucket S3 con l'interfaccia a riga di comando di ONTAP

1. Se si prevede di selezionare autonomamente aggregati e componenti FlexGroup, impostare il livello di privilegio su Advanced (altrimenti, il livello di privilegio admin è sufficiente): `set -privilege advanced`
2. Creare un bucket:

```
vserver object-store-server bucket create -vserver svm_name -bucket
```

```
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Il nome della macchina virtuale storage può essere una macchina virtuale per lo storage dei dati o. Cluster (Il nome della VM di storage del sistema) se si sta configurando il tiering locale.

Se non si specifica alcuna opzione, ONTAP crea un bucket 800GB con il livello di servizio al livello più alto disponibile per il sistema.

Se si desidera che ONTAP crei un bucket in base alle performance o all'utilizzo, utilizzare una delle seguenti opzioni:

- livello di servizio

Includere il `-storage-service-level` con uno dei seguenti valori: `value`, `performance`, o, `extreme`.

- tiering

Includere il `-used-as-capacity-tier true` opzione.

Se si desidera specificare gli aggregati su cui creare il volume FlexGroup sottostante, utilizzare le seguenti opzioni:

- Il `-aggr-list` Parametro specifica l'elenco di aggregati da utilizzare per i componenti del volume FlexGroup.

Ogni voce dell'elenco crea un costituente nell'aggregato specificato. È possibile specificare un aggregato più volte per creare più costituenti sull'aggregato.

Per ottenere performance costanti nel volume FlexGroup, tutti gli aggregati devono utilizzare lo stesso tipo di disco e le stesse configurazioni del gruppo RAID.

- Il `-aggr-list-multiplier` il parametro specifica il numero di iterazioni degli aggregati elencati con `-aggr-list` Quando si crea un volume FlexGroup.

Il valore predefinito di `-aggr-list-multiplier` il parametro è 4.

3. Aggiungere un gruppo di criteri QoS, se necessario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. Verificare la creazione del bucket:

```
vserver object-store-server bucket show [-instance]
```

Esempio

L'esempio seguente crea un bucket per VM di storage `vs1` di dimensione 1TB e specificando l'aggregato:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Crea bucket S3 con System Manager

1. Aggiungi un nuovo bucket su una VM di storage abilitata per S3.
 - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
 - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.
 - Se si fa clic su **Save** (Salva) a questo punto, viene creato un bucket con le seguenti impostazioni predefinite:
 - A nessun utente viene concesso l'accesso al bucket, a meno che non siano già in vigore policy di gruppo.



Non utilizzare l'utente root S3 per gestire lo storage a oggetti ONTAP e condividerne le autorizzazioni, in quanto dispone di accesso illimitato all'archivio di oggetti. Creare invece un utente o un gruppo con privilegi amministrativi assegnati.

- Un livello di qualità del servizio (performance) il più alto disponibile per il sistema.
- Fare clic su **Salva** per creare un bucket con questi valori predefiniti.

Configurare autorizzazioni e restrizioni aggiuntive

È possibile fare clic su **altre opzioni** per configurare le impostazioni per il blocco degli oggetti, le autorizzazioni utente e il livello di prestazioni quando si configura il bucket oppure è possibile modificare queste impostazioni in un secondo momento.

Se si intende utilizzare l'archivio di oggetti S3 per il tiering FabricPool, si consiglia di selezionare **Use for Tiering** (utilizzare supporti a basso costo con performance ottimali per i dati a più livelli) piuttosto che un livello di servizio per le performance.

Se si desidera abilitare il controllo delle versioni per gli oggetti per un successivo ripristino, selezionare **Abilita controllo versioni**. La versione è abilitata per impostazione predefinita se si attiva il blocco degli oggetti nel bucket. Per informazioni sulla versione oggetto, vedere la ["Utilizzo della versione in bucket S3 per Amazon"](#).

A partire dalla versione 9.14.1, il blocco degli oggetti è supportato su bucket S3. S3 il blocco degli oggetti richiede una licenza SnapLock standard. Questa licenza è inclusa con ["ONTAP uno"](#).

Prima di ONTAP One, la licenza SnapLock era inclusa nel pacchetto sicurezza e conformità. Il bundle Security and Compliance non è più offerto, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo ["Eseguire l'aggiornamento a ONTAP One"](#).

Se si attiva il blocco degli oggetti su un bucket, è necessario ["Verificare che sia installata una licenza SnapLock"](#). Se non è installata una licenza SnapLock, è necessario ["installare"](#) prima di poter attivare il blocco degli oggetti.

Una volta verificata l'installazione della licenza SnapLock, per evitare che gli oggetti nel bucket vengano eliminati o sovrascritti, selezionare **attiva blocco oggetti**. Il blocco può essere abilitato su tutte le versioni o versioni specifiche di oggetti, e solo quando il clock di conformità SnapLock viene inizializzato per i nodi del cluster. Attenersi alla seguente procedura:

1. Se il clock di conformità SnapLock non è inizializzato su nessun nodo del cluster, viene visualizzato il pulsante **Inizializza orologio di conformità SnapLock**. Fare clic su **Inizializza orologio conformità**

SnapLock per inizializzare il clock di conformità SnapLock sui nodi del cluster.

2. Selezionare la modalità **Governance** per attivare un blocco basato sul tempo che consenta *Write Once, Read Many (WORM)* autorizzazioni sugli oggetti. Anche in modalità *Governance*, gli oggetti possono essere eliminati dagli utenti amministratori con autorizzazioni specifiche.
3. Selezionare la modalità **conformità** se si desidera assegnare regole più severe di eliminazione e aggiornamento sugli oggetti. In questa modalità di blocco degli oggetti, gli oggetti possono essere scaduti solo al termine del periodo di conservazione specificato. A meno che non venga specificato un periodo di conservazione, gli oggetti rimangono bloccati a tempo indeterminato.
4. Specificare il mantenimento per il blocco in giorni o anni se si desidera che il blocco sia efficace per un determinato periodo.



Il bloccaggio è applicabile alle benne S3 versione e non versione. Il blocco degli oggetti non è applicabile agli oggetti NAS.

È possibile configurare le impostazioni di protezione e autorizzazione e il livello di servizio delle prestazioni per il bucket.



È necessario aver già creato utenti e gruppi prima di configurare le autorizzazioni.

Per ulteriori informazioni, vedere ["Crea mirror per il nuovo bucket"](#).

Verificare l'accesso alla benna

Nelle applicazioni client S3 (ONTAP S3 o un'applicazione esterna di terze parti), è possibile verificare l'accesso al bucket appena creato immettendo quanto segue:

- Certificato CA del server S3.
- La chiave di accesso e la chiave segreta dell'utente.
- Il nome FQDN e il nome bucket del server S3.

Crea un bucket su un aggregato con mirroring o senza mirror in una configurazione MetroCluster

A partire da ONTAP 9.14.1, è possibile eseguire il provisioning di un bucket su un aggregato con mirroring o senza mirror nelle configurazioni FC e IP di MetroCluster.

A proposito di questa attività

- Per impostazione predefinita, i bucket sono in provisioning su aggregati con mirroring.
- Le stesse linee guida per il provisioning delineate in ["Creare un bucket"](#) Applicare per creare un bucket in un ambiente MetroCluster.
- Le seguenti funzioni di storage a oggetti S3 sono **non** supportate negli ambienti MetroCluster:
 - S3 SnapMirror
 - S3 Gestione del ciclo di vita della benna
 - S3 blocco degli oggetti in modalità **conformità**



S3 è supportato il blocco degli oggetti in modalità **Governance**.

- Tiering FabricPool locale

Prima di iniziare

Una SVM contenente un server S3 deve già esistere.

Processo per la creazione di bucket

CLI

1. Se si prevede di selezionare autonomamente aggregati e componenti FlexGroup, impostare il livello di privilegio su Advanced (altrimenti, il livello di privilegio admin è sufficiente): `set -privilege advanced`
2. Creare un bucket:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

Impostare `-use-mirrored-aggregates` opzione a. `true` oppure `false` a seconda che si desideri utilizzare un aggregato con mirroring o senza mirror.



Per impostazione predefinita, il `-use-mirrored-aggregates` l'opzione è impostata su `true`.

- Il nome della SVM deve essere una SVM dati.
- Se non si specifica alcuna opzione, ONTAP crea un bucket 800GB con il livello di servizio al livello più alto disponibile per il sistema.
- Se si desidera che ONTAP crei un bucket in base alle performance o all'utilizzo, utilizzare una delle seguenti opzioni:
 - `livello di servizio`

Includere il `-storage-service-level` con uno dei seguenti valori: `value`, `performance`, o. `extreme`.
 - `tiering`

Includere il `-used-as-capacity-tier true` opzione.
- Se si desidera specificare gli aggregati su cui creare il volume FlexGroup sottostante, utilizzare le seguenti opzioni:
 - Il `-aggr-list` Parametro specifica l'elenco di aggregati da utilizzare per i componenti del volume FlexGroup.

Ogni voce dell'elenco crea un costituente nell'aggregato specificato. È possibile specificare un aggregato più volte per creare più costituenti sull'aggregato.

Per ottenere performance costanti nel volume FlexGroup, tutti gli aggregati devono utilizzare lo stesso tipo di disco e le stesse configurazioni del gruppo RAID.

- Il `-aggr-list-multiplier` il parametro specifica il numero di iterazioni degli aggregati elencati con `-aggr-list` Quando si crea un volume FlexGroup.

Il valore predefinito di `-aggr-list-multiplier` il parametro è 4.

3. Aggiungere un gruppo di criteri QoS, se necessario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

4. Verificare la creazione del bucket:

```
vserver object-store-server bucket show [-instance]
```

Esempio

L'esempio seguente crea un bucket per SVM VS1 di dimensione 1TB su un aggregato mirrorato:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```

System Manager

1. Aggiungi un nuovo bucket su una VM di storage abilitata per S3.
 - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
 - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Per impostazione predefinita, il bucket è in provisioning su un aggregato con mirroring. Se si desidera creare un bucket su un aggregato senza mirror, selezionare **altre opzioni** e deselezionare la casella **Usa il livello SyncMirror in protezione** come mostrato nell'immagine seguente:

- Se si fa clic su **Save** (Salva) a questo punto, viene creato un bucket con le seguenti impostazioni predefinite:
 - A nessun utente viene concesso l'accesso al bucket, a meno che non siano già in vigore policy di gruppo.

Non utilizzare l'utente root S3 per gestire lo storage a oggetti ONTAP e condividerne le autorizzazioni, in quanto dispone di accesso illimitato all'archivio di oggetti. Creare invece un utente o un gruppo con privilegi amministrativi assegnati.

- 35

- È necessario aver già creato utenti e gruppi prima di utilizzare **altre opzioni** per configurare le relative autorizzazioni.
 - Se si intende utilizzare l'archivio di oggetti S3 per il tiering FabricPool, si consiglia di selezionare **Use for Tiering** (utilizzare supporti a basso costo con performance ottimali per i dati a più livelli) piuttosto che un livello di servizio per le performance.
2. Sulle applicazioni client S3 – un altro sistema ONTAP o un'applicazione esterna di terze parti – verificare l'accesso al nuovo bucket immettendo quanto segue:
- Certificato CA del server S3.
 - La chiave di accesso e la chiave segreta dell'utente.
 - Il nome FQDN e il nome bucket del server S3.

Creare una regola di gestione del ciclo di vita del bucket

A partire da ONTAP 9.13.1, puoi creare regole di Lifecycle management per gestire i cicli di vita degli oggetti nei tuoi bucket S3. È possibile definire regole di eliminazione per oggetti specifici in un bucket e, attraverso queste regole, scadono tali oggetti bucket. Ciò consente di soddisfare i requisiti di conservazione e di gestire in modo efficiente lo storage a oggetti complessivo S3.



Se il blocco degli oggetti è attivato per gli oggetti bucket, le regole di gestione del ciclo di vita per la scadenza degli oggetti non verranno applicate agli oggetti bloccati. Per informazioni sul blocco degli oggetti, vedere ["Creare un bucket"](#).

Prima di iniziare

Una SVM abilitata per S3 contenente un server S3 e un bucket deve già esistere. Vedere ["Creare una SVM per S3"](#) per ulteriori informazioni.

A proposito di questa attività

Quando si creano le regole di gestione del ciclo di vita, è possibile applicare le seguenti azioni di eliminazione agli oggetti bucket:

- Eliminazione delle versioni correnti - questa azione scade gli oggetti identificati dalla regola. Se il controllo delle versioni è abilitato nel bucket, S3 rende non disponibili tutti gli oggetti scaduti. Se il controllo delle versioni non è abilitato, questa regola elimina gli oggetti in modo permanente. L'azione CLI è `Expiration`.
- Eliminazione di versioni non correnti - questa azione specifica quando S3 può rimuovere in modo permanente oggetti non correnti. L'azione CLI è `NoncurrentVersionExpiration`.
- Eliminazione dei marcatori di eliminazione scaduti - questa azione elimina i marcatori di eliminazione degli oggetti scaduti.
Nei bucket abilitati per le versioni, gli oggetti con marcatori di eliminazione diventano le versioni correnti degli oggetti. Gli oggetti non vengono eliminati e non è possibile eseguire alcuna azione su di essi. Questi oggetti diventano scaduti quando non sono associate versioni correnti. L'azione CLI è `Expiration`.
- Eliminazione dei caricamenti di più parti incompleti - questa azione imposta il tempo massimo (in giorni) per il quale si desidera consentire il caricamento di più parti. Successivamente, vengono eliminati. L'azione CLI è `AbortIncompleteMultipartUpload`.

La procedura seguente dipende dall'interfaccia utilizzata. Con ONTAP 9.13,1, è necessario utilizzare la CLI. A

partire da ONTAP 9.14.1, è possibile utilizzare anche Gestione sistema.

Gestisci le regole di Lifecycle management con la CLI

A partire da ONTAP 9.13.1, puoi utilizzare l'interfaccia a riga di comando di ONTAP per creare regole di Lifecycle management per scadere gli oggetti nei bucket S3.

Prima di iniziare

Per la CLI, è necessario definire i campi obbligatori per ogni tipo di azione di scadenza quando si crea una regola di gestione del ciclo di vita bucket. Questi campi possono essere modificati dopo la creazione iniziale. Nella seguente tabella vengono visualizzati i campi univoci per ciascun tipo di azione.

Tipo di azione	Campi univoci
NonCurrentVersionExpiration (scadenza versione non attuale)	<ul style="list-style-type: none">• <code>-non-curr-days</code> - Numero di giorni dopo i quali verranno eliminate le versioni non correnti• <code>-new-non-curr-versions</code> - Numero di versioni non correnti più recenti da conservare
Scadenza	<ul style="list-style-type: none">• <code>-obj-age-days</code> - Numero di giorni dalla creazione, dopo i quali è possibile eliminare la versione corrente degli oggetti• <code>-obj-exp-date</code> - Data specifica in cui gli oggetti devono scadere• <code>-expired-obj-del-markers</code> - Pulisci i marcatori di eliminazione degli oggetti
AbortIncompleteMultipartUpload	<ul style="list-style-type: none">• <code>-after-initiation-days</code> - Numero di giorni di avvio, dopo i quali è possibile interrompere il caricamento

Affinché la regola di gestione del ciclo di vita del bucket venga applicata solo a un sottoinsieme specifico di oggetti, gli amministratori devono impostare ciascun filtro durante la creazione della regola. Se questi filtri non vengono impostati durante la creazione della regola, la regola verrà applicata a tutti gli oggetti all'interno del bucket.

Tutti i filtri possono essere modificati dopo la creazione iniziale *tranne* per i seguenti elementi: +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Fasi

1. Utilizzare `vserver object-store-server bucket lifecycle-management-rule create` comando con campi obbligatori per il tipo di azione di scadenza per creare la regola di gestione del ciclo di vita del bucket.

Esempio

Il seguente comando crea una regola di gestione del ciclo di vita del bucket `NonCurrentVersionExpiration`:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Esempio

Il seguente comando crea una regola di gestione del ciclo di vita del bucket di scadenza:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Esempio


Il seguente comando crea una regola di gestione del ciclo di vita del bucket AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gestisci le regole di Lifecycle management con System Manager

A partire da ONTAP 9.14.1, è possibile scade S3 oggetti utilizzando Gestione sistema. È possibile aggiungere, modificare ed eliminare regole di Lifecycle management per gli oggetti S3. Inoltre, è possibile importare una regola del ciclo di vita creata per un bucket e utilizzarla per gli oggetti in un altro bucket. È possibile disattivare una regola attiva e attivarla in un secondo momento.

Aggiungere una regola di gestione del ciclo di vita

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera specificare la regola di scadenza.
3. Fare clic su  E selezionare **Gestisci regole del ciclo di vita**.
4. Fare clic su **Aggiungi > regola ciclo di vita**.
5. Nella pagina Add a Lifecycle rule (Aggiungi una regola del ciclo di vita), aggiungere il nome della regola.

6. Definire l'ambito della regola, se si desidera che venga applicata a tutti gli oggetti nel bucket o a oggetti specifici. Se si desidera specificare gli oggetti, aggiungere almeno uno dei seguenti criteri di filtro:
 - a. **Prefix (prefisso):** Specificare un prefisso dei nomi delle chiavi dell'oggetto a cui applicare la regola. In genere si tratta del percorso o della cartella dell'oggetto. È possibile immettere un prefisso per regola. A meno che non venga fornito un prefisso valido, la regola si applica a tutti gli oggetti in un bucket.
 - b. **Tag:** Specificare fino a tre coppie chiave e valore (tag) per gli oggetti a cui la regola deve essere applicata. Per il filtraggio vengono utilizzate solo chiavi valide. Il valore è facoltativo. Tuttavia, se si aggiungono valori, assicurarsi di aggiungere solo valori validi per le chiavi corrispondenti.
 - c. **Dimensioni:** È possibile limitare l'ambito tra le dimensioni minime e massime degli oggetti. È possibile immettere uno o entrambi i valori. L'unità predefinita è MiB.
7. Specificare l'azione:
 - a. **Scade la versione corrente degli oggetti:** Impostare una regola per rendere tutti gli oggetti correnti permanentemente non disponibili dopo un numero specifico di giorni dalla loro creazione o in una data specifica. Questa opzione non è disponibile se è selezionata l'opzione **Elimina marcatori eliminazione oggetto scaduto**.
 - b. **Eliminare definitivamente le versioni non correnti:** Specificare il numero di giorni dopo il quale la versione diventa non corrente e successivamente può essere eliminata, e il numero di versioni da conservare.
 - c. **Elimina marcatori di eliminazione oggetto scaduto:** Selezionare questa azione per eliminare gli oggetti con marcatori di eliminazione scaduti, ovvero i marcatori di eliminazione senza un oggetto corrente associato.



Questa opzione non è disponibile quando si seleziona l'opzione **scadenza della versione corrente degli oggetti** che elimina automaticamente tutti gli oggetti dopo il periodo di conservazione. Questa opzione diventa anche non disponibile quando si utilizzano i tag degli oggetti per il filtraggio.

- d. **Elimina upload multiparte incompleti:** Consente di impostare il numero di giorni dopo il quale i caricamenti multiparte incompleti devono essere eliminati. Se i caricamenti multiparte in corso non riescono entro il periodo di conservazione specificato, è possibile eliminare i caricamenti multiparte incompleti. Questa opzione diventa non disponibile quando si utilizzano i tag degli oggetti per il filtraggio.
- e. Fare clic su **Save** (Salva).

Importare una regola del ciclo di vita

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera importare la regola di scadenza.
3. Fare clic su **:** E selezionare **Gestisci regole del ciclo di vita**.
4. Fare clic su **Aggiungi > Importa una regola**.
5. Selezionare il bucket dal quale si desidera importare la regola. Vengono visualizzate le regole di gestione del ciclo di vita definite per il bucket selezionato.
6. Selezionare la regola che si desidera importare. È possibile selezionare una regola alla volta, mentre la selezione predefinita è la prima regola.
7. Fare clic su **Importa**.

Modificare, eliminare o disattivare una regola

È possibile modificare solo le azioni di Lifecycle management associate alla regola. Se la regola è stata filtrata con tag Object, le opzioni **Delete Expired Object DELETE Marker** e **Delete incomplete Multipart Uploads** non sono disponibili.

Quando si elimina una regola, tale regola non verrà più applicata agli oggetti precedentemente associati.

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera modificare, eliminare o disattivare la regola di gestione del ciclo di vita.
3. Fare clic su **:** E selezionare **Gestisci regole del ciclo di vita**.
4. Selezionare la regola richiesta. È possibile modificare e disattivare una regola alla volta. È possibile eliminare più regole contemporaneamente.
5. Selezionare **Modifica**, **Elimina** o **Disabilita** e completare la procedura.

Creare un utente S3

Per limitare la connettività ai client autorizzati, è necessaria l'autorizzazione dell'utente in tutti gli archivi di oggetti ONTAP.

Prima di iniziare.

Una macchina virtuale per lo storage abilitata per S3 deve già esistere.

A proposito di questa attività

A un utente S3 può essere concesso l'accesso a qualsiasi bucket in una VM di storage. Quando si crea un utente S3, vengono generate anche una chiave di accesso e una chiave segreta per l'utente. Devono essere condivisi con l'utente insieme all'FQDN dell'archivio oggetti e al nome del bucket. Con è possibile visualizzare le chiavi di un utente S3 `vserver object-store-server user show` comando.

È possibile concedere autorizzazioni di accesso specifiche agli utenti S3 in un criterio bucket o in un criterio del server di oggetti.



Quando si crea un nuovo server archivio oggetti, ONTAP crea un utente root (UID 0), che è un utente con privilegi con accesso a tutti i bucket. Invece di amministrare ONTAP S3 come utente root, NetApp consiglia di creare un ruolo di utente amministratore con privilegi specifici.

CLI

1. Creare un utente S3:

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```

- L'aggiunta di un commento è facoltativa.
- A partire da ONTAP 9.14.1, è possibile definire il periodo di validità della chiave in `-key-time-to-live` parametro. È possibile aggiungere il periodo di conservazione in questo formato, per indicare il periodo dopo il quale la chiave di accesso scade:

`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`


Ad esempio, se si desidera immettere un periodo di conservazione di un giorno, due ore, tre minuti e quattro secondi, immettere il valore come `P1DT2H3M4S`. Se non specificato, la chiave è valida per un periodo di tempo indeterminato.

Nell'esempio riportato di seguito viene creato un utente con nome `sm_user1` Sulla VM di storage `vs0`, con un periodo di conservazione della chiave di una settimana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

- ### 2. Assicurarsi di salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

System Manager

1. Fare clic su **Storage > Storage VM** (Storage > Storage VM). Selezionare la VM di archiviazione a cui si desidera aggiungere un utente, selezionare **Impostazioni** e fare clic su  Sotto S3.
2. Per aggiungere un utente, fare clic su **utenti > Aggiungi**.
3. Immettere un nome per l'utente.
4. A partire da ONTAP 9.14.1, è possibile specificare il periodo di conservazione delle chiavi di accesso create per l'utente. È possibile specificare il periodo di conservazione in giorni, ore, minuti o secondi, dopo il quale le chiavi scadono automaticamente. Per impostazione predefinita, il valore è impostato su 0 ciò indica che la chiave è valida a tempo indeterminato.
5. Fare clic su **Save** (Salva). L'utente viene creato e vengono generate una chiave di accesso e una chiave segreta per l'utente.
6. Scaricare o salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

Passi successivi

- [Creare o modificare gruppi S3](#)

Creare o modificare gruppi S3

È possibile semplificare l'accesso bucket creando gruppi di utenti con autorizzazioni di accesso appropriate.

Prima di iniziare

Gli utenti S3 in una SVM abilitata per S3 devono già esistere.

A proposito di questa attività

Gli utenti di un gruppo S3 possono avere accesso a qualsiasi bucket di una SVM, ma non a più SVM. Le autorizzazioni di accesso al gruppo possono essere configurate in due modi:


- A livello di benna

Dopo aver creato un gruppo di utenti S3, specificare le autorizzazioni di gruppo nelle istruzioni dei criteri bucket e applicarle solo a quel bucket.

- A livello di SVM

Dopo aver creato un gruppo di utenti S3, specificare i nomi dei criteri del server di oggetti nella definizione di gruppo. Tali policy determinano i bucket e l'accesso per i membri del gruppo.

System Manager

1. Modificare la VM di storage: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.
2. Aggiungere un gruppo: Selezionare **gruppi**, quindi selezionare **Aggiungi**.
3. Immettere un nome di gruppo e selezionarlo da un elenco di utenti.
4. È possibile selezionare un criterio di gruppo esistente o aggiungerne uno ora oppure aggiungerne uno in un secondo momento.

CLI

1. Creare un gruppo S3:

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(\s\) [-policies policy_names] [-comment text\]\`Il \`-  
policies
```

l'opzione può essere omessa nelle configurazioni con un solo bucket in un archivio di oggetti; il nome del gruppo può essere aggiunto al criterio bucket. Il `-policies` l'opzione può essere aggiunta in seguito con `vserver object-store-server group modify` comando dopo la creazione dei criteri del server di storage a oggetti.

Rigenerare le chiavi e modificarne il periodo di conservazione

Le chiavi di accesso e le chiavi segrete vengono generate automaticamente durante la creazione dell'utente per abilitare l'accesso client S3. È possibile rigenerare le chiavi di un utente se una chiave è scaduta o compromessa.

Per informazioni sulla generazione delle chiavi di accesso, vedere ["Creare un utente S3"](#).



CLI

1. Rigenerare le chiavi di accesso e segrete di un utente eseguendo `vserver object-store-server user regenerate-keys` comando.
2. Per impostazione predefinita, le chiavi generate sono valide a tempo indeterminato. A partire da 9.14.1, è possibile modificare il periodo di conservazione, dopo il quale le chiavi scadono automaticamente. È possibile aggiungere il periodo di conservazione in questo formato:
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Ad esempio, se si desidera immettere un periodo di conservazione di un giorno, due ore, tre minuti e quattro secondi, immettere il valore come `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. Salvare le chiavi di accesso e le chiavi segrete. Saranno richiesti per l'accesso da S3 client.

System Manager

1. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
2. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
3. Nella scheda **utenti**, verificare che non vi sia alcuna chiave di accesso o che la chiave sia scaduta per l'utente.
4. Se si desidera rigenerare la chiave, fare clic su  Accanto all'utente, quindi fare clic su **Rigenera chiave**.
5. Per impostazione predefinita, le chiavi generate sono valide per un periodo di tempo indefinito. A partire da 9.14.1, è possibile modificare il periodo di conservazione, dopo il quale le chiavi scadono automaticamente. Immettere il periodo di conservazione in giorni, ore, minuti o secondi.
6. Fare clic su **Save** (Salva). La chiave viene rigenerata. Qualsiasi modifica del periodo di conservazione della chiave ha effetto immediato.
7. Scaricare o salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

Creare o modificare le dichiarazioni dei criteri di accesso

Informazioni sulle policy dei server bucket e degli archivi di oggetti

L'accesso degli utenti e dei gruppi alle risorse S3 è controllato dalle policy del server bucket e dell'archivio di oggetti. Se si dispone di un numero limitato di utenti o gruppi, probabilmente è sufficiente controllare l'accesso a livello di bucket, ma se si dispone di molti utenti e gruppi, è più semplice controllare l'accesso a livello di server dell'archivio di oggetti.

Modificare una policy bucket

È possibile aggiungere regole di accesso al criterio bucket predefinito. L'ambito del controllo degli accessi è il bucket contenente, quindi è più appropriato quando è presente

un singolo bucket.

Prima di iniziare

Una VM di storage abilitata per S3 contenente un server S3 e un bucket deve già esistere.

Prima di concedere le autorizzazioni, è necessario aver già creato utenti o gruppi.

A proposito di questa attività

È possibile aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server bucket policy` pagine man.

Le autorizzazioni per utenti e gruppi possono essere concesse al momento della creazione del bucket o in seguito in base alle necessità. È inoltre possibile modificare la capacità del bucket e l'assegnazione del gruppo di policy QoS.

A partire da ONTAP 9.9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Fasi

1. Modificare il bucket: Fare clic su **Storage > Bucket**, fare clic sul bucket desiderato, quindi su **Edit** (Modifica). Quando si aggiungono o modificano le autorizzazioni, è possibile specificare i seguenti parametri:

- **Principal**: L'utente o il gruppo a cui viene concesso l'accesso.
- **Effect**: Consente o nega l'accesso a un utente o a un gruppo.
- **Azioni**: Azioni consentite nel bucket per un dato utente o gruppo.
- **Resources**: Percorsi e nomi degli oggetti all'interno del bucket per i quali viene concesso o negato l'accesso.

I valori predefiniti **bucketname** e **bucketname/*** concedono l'accesso a tutti gli oggetti nel bucket. È inoltre possibile concedere l'accesso a singoli oggetti, ad esempio **nome_carico di lavoro/*_readme.txt**.

- **Condizioni** (opzionale): Espressioni che vengono valutate al tentativo di accesso. Ad esempio, è possibile specificare un elenco di indirizzi IP per i quali l'accesso verrà consentito o negato.



A partire da ONTAP 9.14.1, è possibile specificare le variabili per il criterio bucket nel campo **risorse**. Queste variabili sono segnaposto che vengono sostituiti con valori contestuali quando il criterio viene valutato. Ad esempio, se `${aws:username}` viene specificata come variabile per un criterio, quindi questa variabile viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente.

CLI

Fasi

1. Aggiungere una dichiarazione a una policy bucket:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

I seguenti parametri definiscono le autorizzazioni di accesso:

-effect	L'istruzione può consentire o negare l'accesso
-action	È possibile specificare * per tutte le azioni o un elenco di una o più delle seguenti azioni: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, e. ListMultipartUploadParts.

-principal	<p>Un elenco di uno o più utenti o gruppi S3.</p> <ul style="list-style-type: none"> • È possibile specificare un massimo di 10 utenti o gruppi. • Se viene specificato un gruppo S3, deve essere nel modulo <code>group/group_name</code>. • * può essere specificato per indicare l'accesso pubblico, ovvero l'accesso senza chiave di accesso e chiave segreta. • Se non viene specificato alcun principal, a tutti gli utenti S3 nella VM di storage viene concesso l'accesso.
-resource	<p>Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly * e . ? può essere utilizzato per formare un'espressione regolare per specificare una risorsa. Per una risorsa, è possibile specificare le variabili in un criterio. Si tratta di variabili dei criteri, che vengono sostituite con i valori contestuali al momento della valutazione del criterio.</p>

È possibile specificare una stringa di testo come commento con `-sid` opzione.

Esempi

Nell'esempio seguente viene creata un'istruzione del criterio del bucket del server di archiviazione oggetti per la VM di archiviazione `svm1.example.com` e `bucket1` che specifica l'accesso consentito a una cartella `Leggimi` per l'utente del server di archiviazione oggetti `user1`.

```
cluster1:> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

Nell'esempio seguente viene creata un'istruzione dei criteri del bucket server di archivio oggetti per la VM di storage `svm1.example.com` e `bucket1` che specifica l'accesso consentito a tutti gli oggetti per il gruppo di server di archivio oggetti `group1`.

```
cluster1:> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partire da ONTAP 9.14.1, è possibile specificare le variabili per un criterio bucket. Nell'esempio seguente viene creata un'istruzione del criterio bucket server per la VM di storage `svm1` e `bucket1`, e specifica `${aws:username}` come variabile per una risorsa di criterio. Quando il criterio viene valutato, la variabile di criterio viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente. Ad esempio, quando viene valutata la seguente istruzione di criterio, `${aws:username}` Viene sostituito con l'utente che esegue l'operazione S3. Se un utente `user1` esegue l'operazione, a cui l'utente può accedere `bucket1` come `bucket1/user1/*`.


```
cluster1::> object-store-server bucket policy statement create -vserver  
svml -bucket bucket1 -effect allow -action * -principal - -resource  
bucket1,bucket1/${aws:username}/*##
```

Creare o modificare un criterio del server di archiviazione oggetti

È possibile creare policy applicabili a uno o più bucket in un archivio di oggetti. È possibile collegare le policy del server dell'archivio di oggetti a gruppi di utenti, semplificando in tal modo la gestione dell'accesso alle risorse in più bucket.

Prima di iniziare

Una SVM abilitata per S3 contenente un server S3 e un bucket deve già esistere.

A proposito di questa attività

È possibile attivare i criteri di accesso a livello di SVM specificando un criterio predefinito o personalizzato in un gruppo di server di storage a oggetti. I criteri non hanno effetto fino a quando non vengono specificati nella definizione di gruppo.



Quando si utilizzano i criteri del server di storage a oggetti, si specificano le entità (ovvero utenti e gruppi) nella definizione di gruppo, non nel criterio stesso.

Esistono tre criteri predefiniti di sola lettura per l'accesso alle risorse di ONTAP S3:

- Accesso completo
- NoS3Accesso
- ReadOnlyAccess

È inoltre possibile creare nuovi criteri personalizzati, quindi aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server policy` ["riferimento al comando"](#).


A partire da ONTAP 9.9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per creare o modificare un criterio del server archivio oggetti

Fasi

1. Modificare la VM di storage: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.
2. Aggiungere un utente: Fare clic su **Policies**, quindi su **Add**.
 - a. Inserire un nome di policy e selezionarlo da un elenco di gruppi.
 - b. Selezionare un criterio predefinito esistente o aggiungerne uno nuovo.

Quando si aggiunge o si modifica un criterio di gruppo, è possibile specificare i seguenti parametri:

- **Group (Gruppo):** I gruppi ai quali viene concesso l'accesso.
- **Effetto:** Consente o nega l'accesso a uno o più gruppi.
- **Azioni:** Azioni consentite in uno o più bucket per un dato gruppo.
- **Resources (risorse):** Percorsi e nomi di oggetti all'interno di uno o più bucket per i quali l'accesso viene concesso o negato. Ad esempio:
 - * Garantisce l'accesso a tutti i bucket nella VM di storage.
 - **bucketname e bucketname/*** concedono l'accesso a tutti gli oggetti in un bucket specifico.
 - **bucketname/readme.txt** concede l'accesso a un oggetto in un bucket specifico.
- c. Se lo si desidera, aggiungere le istruzioni ai criteri esistenti.

CLI

Utilizzare la CLI per creare o modificare un criterio del server archivio oggetti

Fasi

1. Creare un criterio del server di storage a oggetti:

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. Creare un'istruzione per la policy:

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

I seguenti parametri definiscono le autorizzazioni di accesso:

-effect	L'istruzione può consentire o negare l'accesso
---------	--

-action	È possibile specificare * per tutte le azioni o un elenco di una o più delle seguenti azioni: getObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, e. ListMultipartUploadParts.
-resource	Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly * e. ? può essere utilizzato per formare un'espressione regolare per specificare una risorsa.

È possibile specificare una stringa di testo come commento con -sid opzione.

Per impostazione predefinita, le nuove dichiarazioni vengono aggiunte alla fine dell'elenco delle dichiarazioni, che vengono elaborate in ordine. Quando si aggiungono o modificano le dichiarazioni in un secondo momento, è possibile modificarle -index impostazione per modificare l'ordine di elaborazione.

Configurare l'accesso S3 per i servizi di directory esterni

A partire da ONTAP 9.14.1, i servizi per le directory esterne sono stati integrati con lo storage a oggetti ONTAP S3. Questa integrazione semplifica la gestione degli utenti e degli accessi tramite servizi di directory esterni.

È possibile fornire ai gruppi utente appartenenti a un servizio di directory esterno l'accesso all'ambiente di storage a oggetti ONTAP. LDAP (Lightweight Directory Access Protocol) è un'interfaccia per la comunicazione con i servizi di directory, come Active Directory, che forniscono un database e servizi per la gestione delle identità e degli accessi (IAM). Per fornire l'accesso, è necessario configurare i gruppi LDAP nell'ambiente ONTAP S3. Dopo aver configurato l'accesso, i membri del gruppo dispongono delle autorizzazioni per i bucket di ONTAP S3. Per informazioni su LDAP, vedere ["Panoramica sull'utilizzo di LDAP"](#).

È inoltre possibile configurare i gruppi di utenti di Active Directory per la modalità di associazione rapida, in modo che le credenziali utente possano essere convalidate e le applicazioni S3 di terze parti e open-source possano essere autenticate tramite connessioni LDAP.

Prima di iniziare

Prima di configurare i gruppi LDAP e attivare la modalità di associazione rapida per l'accesso ai gruppi, verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere ["Creare una SVM per S3"](#).
2. È stato creato un bucket in quella VM per lo storage. Vedere ["Creare un bucket"](#).
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere ["Configurare i servizi DNS"](#).
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere ["Installare il certificato della CA principale autofirmato su SVM"](#).
5. Un client LDAP è configurato con TLS attivato nella SVM. Vedere ["Creare una configurazione del client"](#).

LDAP" e. ["Associare la configurazione del client LDAP alle SVM per ottenere informazioni"](#).

Configurare l'accesso S3 per i servizi di directory esterni

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Creare un'istruzione del criterio del bucket dell'archivio oggetti con il `principal` Impostare sul gruppo LDAP a cui si desidera concedere l'accesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Esempio: Nell'esempio seguente viene creata un'istruzione criterio bucket per `buck1`. Il criterio consente l'accesso al gruppo LDAP `group1` alla risorsa (bucket e relativi oggetti) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verificare che un utente del gruppo LDAP `group1` È in grado di eseguire operazioni S3 dal client S3.

Utilizzare la modalità di associazione rapida LDAP per l'autenticazione

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Assicurarsi che un utente LDAP che accede al bucket S3 disponga delle autorizzazioni definite nei criteri bucket. Per ulteriori informazioni, vedere ["Modificare una policy bucket"](#).
3. Verificare che un utente del gruppo LDAP possa eseguire le seguenti operazioni:
 - a. Configurare la chiave di accesso sul client S3 in questo formato:
`"NTAPFASTBIND" + base64-encode(user-name:password)`
Esempio: `"NTAPFASTBIND" + base64-encode(ldapuser:password)`, che risulta in
`NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`



Il client S3 potrebbe richiedere una chiave segreta. In assenza di una chiave segreta, è possibile immettere qualsiasi password di almeno 16 caratteri.

- b. Eseguire operazioni S3 di base dal client S3 per cui l'utente dispone delle autorizzazioni.

Consentire agli utenti LDAP o di dominio di generare le proprie chiavi di accesso S3

A partire da ONTAP 9.14.1, in qualità di amministratore ONTAP, è possibile creare ruoli personalizzati e concederli a gruppi locali o di dominio o a gruppi LDAP (Lightweight Directory Access Protocol), in modo che gli utenti appartenenti a tali gruppi possano generare le proprie chiavi di accesso e segrete per l'accesso client S3.

Devi eseguire alcuni passaggi di configurazione sulla macchina virtuale di storage, in modo che sia possibile creare e assegnare il ruolo personalizzato all'utente che richiama l'API per la generazione delle chiavi di accesso.

Prima di iniziare

Verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere ["Creare una SVM per S3"](#).
2. È stato creato un bucket in quella VM per lo storage. Vedere ["Creare un bucket"](#).
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere ["Configurare i servizi DNS"](#).
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere ["Installare il certificato della CA principale autofirmato su SVM"](#).
5. Un client LDAP è configurato con TLS attivato sulla macchina virtuale di storage. Vedere ["Creare una configurazione del client LDAP"](#) e .
6. Associare la configurazione del client al Vserver. Vedere ["Associare la configurazione del client LDAP alle SVM"](#) e ["creazione ldap del nome del servizio vserver"](#).
7. Se stai utilizzando una macchina virtuale per lo storage dei dati, crea un'interfaccia di rete di gestione (LIF) e una macchina virtuale, oltre a una policy di servizio per la LIF. Vedere ["creazione dell'interfaccia di rete"](#) e ["creazione della politica di servizio dell'interfaccia di rete"](#) comandi.

Configurare gli utenti per la generazione delle chiavi di accesso

1. Specificare LDAP come *name service database* della VM di archiviazione per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Creare un ruolo personalizzato con accesso all'endpoint API REST per S3 utenti:

```
security login rest-role create -vserver <vserver-name> -role <custom-role-
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

In questo esempio, il `s3-role` Viene generato un ruolo per gli utenti sulla VM di storage `svm-1`, a cui vengono concessi tutti i diritti di accesso, lettura, creazione e aggiornamento.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

Per ulteriori informazioni su questo comando, vedere ["accesso di sicurezza creazione ruolo di pausa"](#) comando.

3. Creare un gruppo di utenti LDAP con il comando di accesso alla sicurezza e aggiungere il nuovo ruolo personalizzato per accedere all'endpoint dell'API REST utente S3. Per ulteriori informazioni su questo comando, vedere ["creazione dell'accesso di sicurezza"](#) comando.

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

In questo esempio, il gruppo LDAP `ldap-group-1` viene creato in `svm-1` e il ruolo personalizzato `s3role` Viene aggiunto per accedere all'endpoint API, oltre ad abilitare l'accesso LDAP in modalità di associazione rapida.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Per ulteriori informazioni, vedere ["Utilizza il binding rapido LDAP per l'autenticazione nsswitch"](#).

L'aggiunta del ruolo personalizzato al dominio o al gruppo LDAP consente agli utenti di quel gruppo di accedere in modo limitato a ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpoint. Richiamando l'API, gli utenti del dominio o del gruppo LDAP possono generare il proprio accesso e le proprie chiavi segrete per accedere al client S3. Possono generare le chiavi solo per se stessi e non per altri utenti.

Come utente S3 o LDAP, generare le proprie chiavi di accesso

A partire da ONTAP 9.14.1, è possibile generare le proprie chiavi di accesso e segrete per l'accesso ai client S3, se l'amministratore ha concesso il ruolo di generazione delle proprie chiavi. Puoi generare le chiavi solo per te utilizzando il seguente endpoint dell'API REST ONTAP.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti. Per informazioni sugli altri metodi di questo endpoint, vedere il riferimento ["Documentazione API"](#).

Metodo HTTP	Percorso
POST	/api/protocolli/s3/servizi/{svm.uuid}/utenti

Esempio di arricciamento

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name": "_name_"}'
```

Esempio di output JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

Abilitare l'accesso del client allo storage a oggetti S3

Abilitare l'accesso ONTAP S3 per il tiering FabricPool remoto

Per utilizzare ONTAP S3 come Tier di capacità FabricPool remota (cloud), l'amministratore di ONTAP S3 deve fornire informazioni sulla configurazione del server S3 all'amministratore remoto del cluster ONTAP.

A proposito di questa attività

Per configurare i livelli cloud FabricPool sono necessarie le seguenti informazioni sul server S3:

- Nome server (FQDN)
- nome bucket
- Certificato CA
- tasto di accesso
- password (chiave di accesso segreta)

Inoltre, è necessaria la seguente configurazione di rete:

- Nel server DNS configurato per la SVM amministrativa deve essere presente una voce per il nome host del server ONTAP S3 remoto, compreso il nome FQDN del server S3 e gli indirizzi IP sui relativi LIF.

- Le LIF di intercluster devono essere configurate sul cluster locale, anche se non è richiesto il peering del cluster.

Consultare la documentazione di FabricPool sulla configurazione di ONTAP S3 come Tier cloud.

"Gestione dei Tier di storage mediante FabricPool"

Abilitare l'accesso ONTAP S3 per il tiering FabricPool locale

Per utilizzare ONTAP S3 come Tier di capacità FabricPool locale, è necessario definire un archivio di oggetti in base al bucket creato e quindi associare l'archivio di oggetti a un aggregato di Tier di performance per creare un FabricPool.

Prima di iniziare

È necessario disporre del nome del server ONTAP S3 e del nome del bucket e il server S3 deve essere stato creato utilizzando le LIF del cluster (con `-vserver Cluster` parametro).

A proposito di questa attività

La configurazione dell'archivio di oggetti contiene informazioni sul Tier di capacità locale, inclusi i nomi dei server S3 e dei bucket e i requisiti di autenticazione.

Una volta creata, la configurazione di un archivio di oggetti non deve essere riassociata a un altro archivio di oggetti o bucket. È possibile creare più bucket per i Tier locali, ma non è possibile creare più archivi di oggetti in un singolo bucket.

Non è richiesta una licenza FabricPool per un livello di capacità locale.

Fasi

1. Creare l'archivio di oggetti per il livello di capacità locale:

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- Il `-container-name` È il bucket S3 creato.
- Il `-access-key` Il parametro autorizza le richieste al server ONTAP S3.
- Il `-secret-password` Il parametro (chiave di accesso segreta) autentica le richieste al server ONTAP S3.
- È possibile impostare `-is-certificate-validation-enabled` parametro a `false` Per disattivare il controllo dei certificati per ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Visualizzare e verificare le informazioni di configurazione dell'archivio di oggetti:

```
storage aggregate object-store config show
```

3. Facoltativo: Per verificare la quantità di dati inattivi in un volume, seguire la procedura descritta in ["Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi"](#).

La visualizzazione della quantità di dati inattivi in un volume consente di decidere quale aggregato utilizzare per il tiering locale di FabricPool.

4. Collegare l'archivio di oggetti a un aggregato:

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
```

È possibile utilizzare `allow-flexgroup true` Possibilità di collegare aggregati che contengono componenti del volume FlexGroup.

```
cluster1::> storage aggregate object-store attach  
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Visualizzare le informazioni sull'archivio di oggetti e verificare che l'archivio di oggetti collegato sia disponibile:

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

Abilitare l'accesso client da un'applicazione S3

Affinché le applicazioni client S3 possano accedere al server ONTAP S3, l'amministratore di ONTAP S3 deve fornire le informazioni di configurazione all'utente S3.

Prima di iniziare

L'applicazione client S3 deve essere in grado di eseguire l'autenticazione con il server ONTAP S3 utilizzando le seguenti versioni delle firme AWS:

- Signature versione 4, ONTAP 9.8 e versioni successive
- Signature versione 2, ONTAP 9.11.1 e versioni successive

ONTAP S3 non supporta altre versioni delle firme.

L'amministratore di ONTAP S3 deve aver creato gli utenti S3 e concesso loro le autorizzazioni di accesso, come singoli utenti o come membro di gruppo, nella policy del bucket o nella policy del server di storage a oggetti.

L'applicazione client S3 deve essere in grado di risolvere il nome del server ONTAP S3, il che richiede che l'amministratore di ONTAP S3 fornisca il nome del server S3 (FQDN) e gli indirizzi IP per le LIF del server S3.

A proposito di questa attività

Per accedere a un bucket ONTAP S3, un utente dell'applicazione client S3 inserisce le informazioni fornite dall'amministratore di ONTAP S3.

A partire da ONTAP 9.9.1, il server ONTAP S3 supporta le seguenti funzionalità del client AWS:

- metadati degli oggetti definiti dall'utente

Un insieme di coppie chiave-valore può essere assegnato agli oggetti come metadati quando vengono creati usando PUT (o POST). Quando viene eseguita un'operazione GET/HEAD sull'oggetto, i metadati definiti dall'utente vengono restituiti insieme ai metadati di sistema.

- tagging degli oggetti

È possibile assegnare un insieme separato di coppie chiave-valore come tag per la classificazione degli oggetti. A differenza dei metadati, i tag vengono creati e letti con API REST indipendentemente dall'oggetto e implementati quando gli oggetti vengono creati o in qualsiasi momento.



Per consentire ai client di ottenere e inserire informazioni di tagging, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

Per ulteriori informazioni, consultare la documentazione di AWS S3.

Fasi

1. Autenticare l'applicazione client S3 con il server ONTAP S3 immettendo il nome del server S3 e il certificato CA.
2. Autenticare un utente sull'applicazione client S3 inserendo le seguenti informazioni:
 - Nome server S3 (FQDN) e nome bucket
 - la chiave di accesso e la chiave segreta dell'utente

Definizioni dei servizi di storage

ONTAP include servizi di storage predefiniti mappati ai corrispondenti fattori di performance minimi.

L'insieme effettivo di servizi storage disponibili in un cluster o SVM è determinato dal tipo di storage che costituisce un aggregato nella SVM.

La seguente tabella mostra come i fattori minimi di performance sono mappati ai servizi di storage predefiniti:

Servizio di storage	IOPS previsti (SLA)	IOPS di picco (SLO)	Volume minimo IOPS	Latenza stimata	Gli IOPS previsti sono applicati?
valore	128 per TB	512 per TB	75	17 ms.	Su AFF: Sì Altrimenti: No
performance	2048 per TB	4096 per TB	500	2 ms.	Sì

Servizio di storage	IOPS previsti (SLA)	IOPS di picco (SLO)	Volume minimo IOPS	Latenza stimata	Gli IOPS previsti sono applicati?
estremo	6144 per TB	12288 per TB	1000	1 ms.	Sì

La seguente tabella definisce il livello di servizio dello storage disponibile per ciascun tipo di supporto o nodo:

Media o nodo	Livello di servizio dello storage disponibile
Disco	valore
Disco della macchina virtuale	valore
LUN FlexArray	valore
Ibrido	valore
Flash ottimizzato per la capacità	valore
Solid-state Drive (SSD) - non AFF	valore
Flash ottimizzata per le performance - SSD (AFF)	estremi, performance, valore

Proteggi i bucket con S3 SnapMirror

Panoramica di S3 SnapMirror

A partire da ONTAP 9.10.1, puoi proteggere i bucket in archivi di oggetti ONTAP S3 usando la funzionalità di mirroring e backup di SnapMirror. A differenza di SnapMirror standard, S3 SnapMirror consente il mirroring e i backup in destinazioni non NetApp come AWS S3.

S3 SnapMirror supporta mirror attivi e Tier di backup dai bucket ONTAP S3 alle seguenti destinazioni:

Destinazione	Supporta mirror attivi e Takeover?	Supporta backup e ripristino?
ONTAP S3 <ul style="list-style-type: none"> • Bucket nella stessa SVM • Bucket in diverse SVM sullo stesso cluster • Bucket in SVM su cluster diversi 	✓	✓
StorageGRID		✓
AWS S3		✓

Destinazione	Supporta mirror attivi e Takeover?	Supporta backup e ripristino?
Cloud Volumes ONTAP per Azure	✓	✓
Cloud Volumes ONTAP per AWS	✓	✓
Cloud Volumes ONTAP per Google Cloud	✓	✓

È possibile proteggere i bucket esistenti sui server ONTAP S3 o creare nuovi bucket con la protezione dei dati attivata immediatamente.

Requisiti di S3 SnapMirror

- Versione di ONTAP
ONTAP 9.10.1 o versione successiva deve essere in esecuzione sui cluster di origine e di destinazione.
- Licenze i seguenti bundle di licenze sono richiesti sui sistemi di origine e destinazione ONTAP:
 - Bundle principale per protocollo e storage ONTAP S3.
 - Bundle per la protezione dei dati per S3 SnapMirror destinato ad altri archivi di oggetti NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP).
 - Bundle di data Protection e bundle cloud ibrido
Per S3 SnapMirror è destinato ad archivi di oggetti di terze parti, tra cui AWS S3.
- ONTAP S3
 - I server ONTAP S3 devono eseguire SVM di origine e di destinazione.
 - Si consiglia, ma non è obbligatorio, di installare i certificati CA per l'accesso TLS sui sistemi che ospitano server S3.
 - I certificati CA utilizzati per firmare i certificati dei server S3 devono essere installati nella VM di storage amministrativa dei cluster che ospitano server S3.
 - È possibile utilizzare un certificato CA autofirmato o un certificato firmato da un fornitore CA esterno.
 - Se le VM di storage di origine o di destinazione non sono in ascolto su HTTPS, non è necessario installare i certificati CA.
- Peering (per target ONTAP S3)
 - È necessario configurare le LIF di intercluster (per le destinazioni ONTAP remote).
 - I cluster di origine e di destinazione vengono peering (per le destinazioni ONTAP remote).
 - Le VM storage di origine e di destinazione sono in peering (per tutte le destinazioni ONTAP).
- Policy di SnapMirror
 - Per tutte le relazioni di S3 SnapMirror è necessario un criterio SnapMirror specifico di S3, ma è possibile utilizzare lo stesso criterio per più relazioni.
 - È possibile creare un criterio personalizzato o accettare il criterio **continuo** predefinito, che include i seguenti valori:
 - Throttle (limite superiore di throughput/larghezza di banda) - illimitato.
 - Tempo per l'obiettivo del punto di ripristino: 1 ora (3600 secondi).
- Le chiavi utente root Storage VM root sono necessarie per le relazioni S3 SnapMirror; ONTAP non le assegna per impostazione predefinita. La prima volta che si crea una relazione SnapMirror S3, è necessario verificare che le chiavi esistano sia sulle macchine virtuali storage di origine che di destinazione

e rigenerarle in caso contrario. Se è necessario rigenerarli, è necessario assicurarsi che tutti i client e tutte le configurazioni dell'archivio di oggetti SnapMirror che utilizzano la coppia di chiavi di accesso e segrete siano aggiornati con le nuove chiavi.

Per informazioni sulla configurazione del server S3, consultare i seguenti argomenti:

- ["Abilitare un server S3 su una VM di storage"](#)
- ["Informazioni sul processo di configurazione S3"](#)

Per informazioni sul peering delle macchine virtuali di storage e cluster, consultare il seguente argomento:

- ["Preparazione per il mirroring e il vaulting \(System Manager, fasi 1-6\)"](#)
- ["Peering cluster e SVM \(CLI\)"](#)

Relazioni SnapMirror supportate

S3 SnapMirror supporta le relazioni fan-out e cascata. Per una panoramica, vedere ["Implementazioni di protezione dei dati fan-out e cascata"](#).

S3 SnapMirror non supporta le implementazioni fan-in (relazioni di data Protection tra più bucket di origine e un singolo bucket di destinazione). S3 SnapMirror può supportare più mirror bucket da più cluster a un singolo cluster secondario, ma ogni bucket di origine deve avere un proprio bucket di destinazione sul cluster secondario.

Controllare l'accesso alle benne S3

Quando si creano nuovi bucket, è possibile controllare l'accesso creando utenti e gruppi. Per ulteriori informazioni, consulta i seguenti argomenti:

- ["Aggiunta di utenti e gruppi S3 \(System Manager\)"](#)
- ["Creazione di un utente S3 \(CLI\)"](#)
- ["Creare o modificare gruppi S3 \(CLI\)"](#)

Protezione del mirroring e del backup su un cluster remoto

Creare una relazione mirror per un nuovo bucket (cluster remoto)

Quando si creano nuovi bucket S3, è possibile proteggerli immediatamente a una destinazione S3 SnapMirror su un cluster remoto.



A proposito di questa attività


È necessario eseguire attività sui sistemi di origine e di destinazione.

Prima di iniziare


- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
 - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
 - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
 - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
 - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi, sia nelle VM di storage di origine che di destinazione:

Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare il criterio predefinito:
 - a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
 - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
 - Immettere il nome e la descrizione della policy.
 - Selezionare l'ambito del criterio, il cluster o SVM
 - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
 - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
 - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
 - b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
 - c. In **Permissions**, fare clic su **Add** (Aggiungi).
 - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni**- assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (*bucketname*, *bucketname/**) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:

- Destinazione
 - **DESTINAZIONE: Sistema ONTAP**
 - **CLUSTER**: Selezionare il cluster remoto.
 - **STORAGE VM**: Selezionare una storage VM sul cluster remoto.
 - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato *source*.
- Origine
 - **CERTIFICATO CA del SERVER S3**: copiare e incollare il contenuto del certificato *destination*.

5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare bucket nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket create -vserver svm_name -bucket
```



```
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Aggiungere regole di accesso alle policy di bucket predefinite nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Esempio

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Nella SVM di origine, crea una policy SnapMirror S3 se non ne hai già una e non vuoi utilizzare la policy predefinita:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri:

- tipo continuous - L'unico tipo di policy per le relazioni SnapMirror S3 (obbligatorio).
- -rpo - specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- -throttle - specifica il limite superiore di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulle SVM amministrative dei cluster di origine e di destinazione:

- a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3 *destination*:

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

- b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3 *source*:

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Se si utilizza un certificato firmato da un vendor CA esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.

Vedere `security certificate install` pagina man per i dettagli.

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy  
test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

Creare una relazione mirror per un bucket esistente (cluster remoto)

È possibile iniziare a proteggere i bucket S3 esistenti in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1.

A proposito di questa attività

Devi eseguire i task sui cluster di origine e destinazione.




Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.



Fasi

È possibile creare una relazione di mirroring utilizzando System Manager o l'interfaccia a riga di comando di ONTAP.

System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
 - a. Selezionare **Storage > Storage VM**, quindi selezionare la VM di storage.
 - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
 - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
 - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. non rigenerare la chiave se ne esiste già una.
2. Verificare che l'accesso a utenti e gruppi sia corretto sia nelle macchine virtuali storage di origine che di destinazione:
Selezionare **Storage > Storage VM**, quindi selezionare la VM di archiviazione, quindi **Settings**. Infine, selezionare  Sotto **S3**.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare il criterio predefinito:
 - a. Selezionare **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
 - b. Selezionare  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
 - c. Immettere il nome e la descrizione della policy.
 - d. Selezionare l'ambito del criterio, il cluster o SVM
 - e. Selezionare **Continuous** per le relazioni di S3 SnapMirror.
 - f. Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
 - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
 - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
 - **Principal and Effect** (principale ed effetto): Selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni**: Verificare che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse**: Utilizzare le impostazioni predefinite (*bucketname*, *bucketname/**) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

5. Proteggi un bucket esistente con la protezione di S3 SnapMirror:
 - a. Fare clic su **Storage > Bucket**, quindi selezionare il bucket che si desidera proteggere.
 - b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:

- Destinazione
 - **DESTINAZIONE:** Sistema ONTAP
 - **CLUSTER:** Selezionare il cluster remoto.
 - **STORAGE VM:** Selezionare una storage VM sul cluster remoto.
 - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato *source*.
 - Origine
 - **Certificato CA server S3:** Copia e incolla il contenuto del certificato *destination*.
6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
 7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
 8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

`vserver object-store-server user show+` verificare la presenza di una chiave di accesso per l'utente root. In caso contrario, immettere:

`vserver object-store-server user regenerate-keys -vserver svm_name -user root+` non rigenerare la chiave se ne esiste già una.

2. Creare un bucket sulla SVM di destinazione come destinazione mirror:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Verificare che le regole di accesso delle policy di bucket predefinite siano corrette sia nelle SVM di origine che di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
```

```
text] [-index integer]
```

Esempio

```
src_cluster::> vserver object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. Sulla SVM di origine, creare un criterio S3 SnapMirror se non si dispone di uno esistente e non si desidera utilizzare il criterio predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Parametri:

- continuous – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- -rpo – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- -throttle – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
src_cluster::> snapmirror policy create -vserver vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati CA sulle SVM amministrative dei cluster di origine e di destinazione:

- a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3
destination:

```
security certificate install -type server-ca -vserver src_admin_svm  
-cert-name dest_server_certificate
```

- b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3
source:

```
security certificate install -type server-ca -vserver dest_admin_svm  
-cert-name src_server_certificate+ se si utilizza un certificato firmato da un vendor CA  
esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...] [-policy  
policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

Acquisizione e distribuzione dei dati dal bucket di destinazione (cluster remoto)

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

A proposito di questa attività


Quando viene eseguita un'operazione di Takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione di S3 SnapMirror.

Quando il bucket di origine disattivato è nuovamente disponibile, S3 SnapMirror risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror dei volumi.

L'operazione di Takeover deve essere avviata dal cluster remoto.

System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su , Selezionare **failover**, quindi fare clic su **failover**.

CLI

1. Avviare un'operazione di failover per il bucket di destinazione:

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```
2. Verificare lo stato dell'operazione di failover:

```
snapmirror show -fields status
```

Esempio

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

Ripristinare un bucket dalla VM di storage di destinazione (cluster remoto)

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile

ripopolare i dati ripristinando gli oggetti da un bucket di destinazione.

A proposito di questa attività

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande dello spazio utilizzato logico del bucket di destinazione.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

L'operazione di ripristino deve essere avviata dal cluster remoto.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
 - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
 - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
 - Selezionare il bucket esistente.
 - Copiare e incollare il contenuto del certificato CA del server *S3 destination*.
 - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
 - Il cluster e la VM di storage per ospitare il nuovo bucket.
 - Il nome, la capacità e il livello di servizio delle prestazioni della nuova benna. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
 - Il contenuto del certificato CA del server *S3 destination*.
4. In **destinazione**, copiare e incollare il contenuto del certificato CA del server *S3 origine*.
5. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket:** Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente:** Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket:** Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un nuovo bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```


Esempio

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

Protezione del mirroring e del backup sul cluster locale


Creare una relazione mirror per un nuovo bucket (cluster locale)

Quando si creano nuovi bucket S3, è possibile proteggerli immediatamente a una destinazione S3 SnapMirror sullo stesso cluster. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.


Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
 - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
 - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro S3.
 - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root
 - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi, sia nelle VM di storage di origine che di destinazione: Fare clic su **Storage > VM di storage**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere ["Aggiungere utenti e gruppi S3"](#) per ulteriori informazioni.

3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
 - a. Fare clic su **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
 - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
 - Immettere il nome e la descrizione della policy.
 - Selezionare l'ambito del criterio, il cluster o SVM
 - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
 - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
 - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi su **Add** (Aggiungi).
 - b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
 - c. In **Permissions**, fare clic su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
 - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (`bucketname`, `bucketname/*`) o altri valori di cui hai bisogno

Vedere ["Gestire l'accesso degli utenti ai bucket"](#) per ulteriori informazioni su questi campi.

- d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:

- Destinazione
 - **DESTINAZIONE:** Sistema ONTAP
 - **CLUSTER:** Selezionare il cluster locale.
 - **VM di STORAGE:** Selezionare una VM di storage sul cluster locale.
 - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato di origine.
 - Origine
 - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato di destinazione.
5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
 6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
 7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare bucket nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Aggiungere regole di accesso alle policy di bucket predefinite nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri:

- continuous – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- -rpo – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- -throttle – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulla SVM amministrativa:

a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate+ se si utilizza un certificato firmato da un vendor CA
esterno, è necessario installare questo certificato solo sulla SVM amministrativa.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]`
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror  
-policy test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```




Creare una relazione mirror per un bucket esistente (cluster locale)

È possibile iniziare a proteggere i bucket S3 esistenti sullo stesso cluster in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.



Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
 - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
 - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
 - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
 - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una
2. Verificare che l'accesso a utenti e gruppi sia corretto sia nelle macchine virtuali storage di origine che di destinazione:
 - Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
 - a. Fare clic su **protezione > Panoramica**, quindi su **impostazione policy locale**.
 - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
 - Immettere il nome e la descrizione della policy.
 - Selezionare l'ambito del criterio, il cluster o SVM
 - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
 - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente continui a soddisfare le proprie esigenze:
 - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
 - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
 - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (*bucketname*, *bucketname/**) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

5. Proteggi un bucket esistente con S3 SnapMirror:
 - a. Fare clic su **Storage > Bucket** e selezionare il bucket che si desidera proteggere.

b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:

- Destinazione
 - **DESTINAZIONE:** Sistema ONTAP
 - **CLUSTER:** Selezionare il cluster locale.
 - **STORAGE VM:** Consente di selezionare la stessa o una diversa storage VM.
 - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato *source*.
 - Origine
 - **Certificato CA server S3:** Copia e incolla il contenuto del certificato *destination*.
6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
 7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
 8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare un bucket sulla SVM di destinazione come destinazione mirror:

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Verificare che le regole di accesso alle policy di bucket predefinite siano corrette sia nelle SVM di

origine che di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri:

- ° continuous – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- ° -rpo – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- ° -throttle – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulla SVM amministrativa:

- a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

- b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate+ se si utilizza un certificato firmato da un vendor CA
esterno, è necessario installare questo certificato solo sulla SVM amministrativa.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
```



```
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

Acquisizione e distribuzione dei dati dal bucket di destinazione (cluster locale)

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

A proposito di questa attività


Quando viene eseguita un'operazione di Takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione di S3 SnapMirror.

Quando il bucket di origine disattivato è nuovamente disponibile, S3 SnapMirror risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror di volumi standard.

Se il bucket di destinazione si trova su un cluster remoto, l'operazione di Takeover deve essere avviata dal cluster remoto.

System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su , Selezionare **failover**, quindi fare clic su **failover**.

CLI

1. Avviare un'operazione di failover per il bucket di destinazione:

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```
2. Verificare lo stato dell'operazione di failover:

```
snapmirror show -fields status
```

Esempio

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-bucket-mirror
```

Ripristino di un bucket dalla VM di storage di destinazione (cluster locale)

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ripopolare i dati ripristinando gli oggetti da un bucket di destinazione.

A proposito di questa attività

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande del bucket di destinazione; lo spazio logico utilizzato.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

L'operazione di ripristino deve essere avviata dal cluster locale.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare il bucket.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
 - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
 - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
 - Selezionare il bucket esistente.
4. Copiare e incollare il contenuto del certificato CA del server S3 di destinazione.
 - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
 - Il cluster e la VM di storage per ospitare il nuovo bucket.
 - Il nome, la capacità e il livello di servizio delle prestazioni della nuova benna. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
 - Contenuto del certificato CA del server S3 di destinazione.
5. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 di origine.
6. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket:** Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente:** Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket:** Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

CLI

1. Se si ripristinano oggetti in un nuovo bucket, creare il nuovo bucket. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un nuovo bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

Esempio

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

Protezione del backup con destinazioni cloud

Requisiti per le relazioni di destinazione del cloud

Assicurati che gli ambienti di origine e di destinazione soddisfino i requisiti per la protezione di backup di S3 SnapMirror verso le destinazioni cloud.

Per accedere al bucket di dati, è necessario disporre di credenziali account valide con il provider dell'archivio di oggetti.

Le interfacce di rete tra cluster e un IPspace devono essere configurati sul cluster prima che il cluster possa connettersi a un archivio di oggetti cloud. È necessario creare interfacce di rete del cluster di invio su ciascun nodo per trasferire senza problemi i dati dallo storage locale all'archivio di oggetti cloud.

Per gli obiettivi StorageGRID, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Inoltre, il certificato CA utilizzato per firmare il certificato del server StorageGRID deve essere installato sulla macchina virtuale di storage amministrativa del cluster ONTAP S3 utilizzando `security certificate install` command. Per ulteriori informazioni, vedere ["Installazione di un certificato CA"](#) Se si utilizza StorageGRID.

Per i target AWS S3, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Il server DNS per la VM di storage amministrativa del cluster ONTAP deve essere in grado di risolvere gli FQDN (se utilizzati) in indirizzi IP.

Creare una relazione di backup per un nuovo bucket (target cloud)


Quando crei nuovi bucket S3, puoi eseguirne immediatamente il backup su un bucket di destinazione di S3 SnapMirror su un provider di archivi di oggetti, che può essere un sistema StorageGRID o un'implementazione di Amazon S3.

Prima di iniziare

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPSpace sono state configurate sul sistema di origine.
- • La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere il FQDN della destinazione.

System Manager

1. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi:

- a. Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto **S3**.


Vedere ["Aggiungere utenti e gruppi S3"](#) per ulteriori informazioni.

2. Aggiungere un Cloud Object Store sul sistema di origine:

- a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Stores**.
- b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **StorageGRID**.
- c. Immettere i seguenti valori:

- Nome archivio oggetti cloud
- Stile URL (path o virtual-hosted)
- Storage VM (abilitato per S3)
- Nome server archivio oggetti (FQDN)
- Certificato dell'archivio di oggetti
- Tasto di accesso
- Chiave segreta
- Nome del container (bucket)

3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

- a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
- b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.

- Immettere il nome e la descrizione della policy.
- Selezionare l'ambito del criterio, il cluster o SVM
- Selezionare **Continuous** per le relazioni di S3 SnapMirror.
- Inserire i valori **Throttle** e **Recovery Point Objective**.

4. Crea un bucket con la protezione SnapMirror:

- a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
- b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
- c. In **Permissions**, fare clic su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
 - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- **Risorse** - utilizzare le impostazioni predefinite `_(bucketname, bucketname/*)` o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

- d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**, selezionare **archiviazione cloud**, quindi selezionare **Archivio oggetti cloud**.

Facendo clic su **Save** (Salva), viene creato un nuovo bucket nella VM dello storage di origine e viene eseguito il backup nell'archivio di oggetti cloud.

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:
`vserver object-store-server user show+` confermare che esiste una chiave di accesso per l'utente root. In caso contrario, immettere:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root+` non rigenerare la chiave se ne esiste già una.

2. Creare un bucket nella SVM di origine:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Aggiungere regole di accesso alla policy bucket predefinita:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri: * `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

5. Se la destinazione è un sistema StorageGRID, installare il certificato del server CA StorageGRID sulla SVM amministrativa del cluster di origine:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Vedere `security certificate install` pagina man per i dettagli.

6. Definire l'archivio di oggetti di destinazione di S3 SnapMirror:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Parametri: * `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. * `-usage` – utilizzare `data` per questo flusso di lavoro. * `-provider-type` – `AWS_S3` e `SGWS` Sono supportati i target (StorageGRID). * `-server` – L'indirizzo FQDN o IP del server di destinazione. * `-is-ssl-enabled` – L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

Esempio

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl-  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

Parametri:

* `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```



Creare una relazione di backup per un bucket esistente (target cloud)

È possibile iniziare il backup dei bucket S3 esistenti in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1.



Prima di iniziare

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPspace sono state configurate sul sistema di origine.
- La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere l'FQDN della destinazione.

System Manager

1. Verificare che gli utenti e i gruppi siano definiti correttamente: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni) e quindi su  Sotto S3.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

2. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
 - a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
 - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
 - c. Immettere il nome e la descrizione della policy.
 - d. Selezionare l'ambito del criterio, il cluster o SVM
 - e. Selezionare **Continuous** per le relazioni di S3 SnapMirror.
 - f. Inserire i valori **Throttle** e **Recovery Point Objective**.
3. Aggiungere un Cloud Object Store sul sistema di origine:
 - a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Store**.
 - b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **altri** per StorageGRID webscale.
 - c. Immettere i seguenti valori:
 - Nome archivio oggetti cloud
 - Stile URL (path o virtual-hosted)
 - Storage VM (abilitato per S3)
 - Nome server archivio oggetti (FQDN)
 - Certificato dell'archivio di oggetti
 - Tasto di accesso
 - Chiave segreta
 - Nome del container (bucket)
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
 - a. Fare clic su **Storage > Bucket** e selezionare il bucket che si desidera proteggere.
 - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
 - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
 - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Risorse** - utilizzare le impostazioni predefinite (`bucketname, bucketname/*`) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

5. Eseguire il backup del bucket utilizzando S3 SnapMirror:
 - a. Fare clic su **Storage > Bucket**, quindi selezionare il bucket di cui si desidera eseguire il backup.

- b. Fare clic su **Protect**, selezionare **Cloud Storage** sotto **Target**, quindi selezionare **Cloud Object Store**.

Facendo clic su **Save** (Salva), viene eseguito il backup del bucket esistente nell'archivio di oggetti cloud.

CLI

1. Verificare che le regole di accesso nel criterio bucket predefinito siano corrette:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement  
-bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

2. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Parametri: * `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

3. Se la destinazione è un sistema StorageGRID, installare il certificato CA StorageGRID sulla SVM amministrativa del cluster di origine:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Vedere `security certificate install` pagina man per i dettagli.

4. Definire l'archivio di oggetti di destinazione di S3 SnapMirror:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Parametri: * `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. * `-usage` – utilizzare data per questo flusso di lavoro. * `-provider-type` – AWS_S3 e. SGWS Sono supportati i target (StorageGRID). * `-server` – L'indirizzo FQDN o IP del server di destinazione. * `-is-ssl-enabled` –L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

Esempio

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

Parametri:

* `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

È possibile utilizzare un criterio creato o accettare quello predefinito.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

Ripristinare un bucket da un target cloud

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ricompilare i dati ripristinandoli da un bucket di destinazione.


A proposito di questa attività

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande dello spazio logico utilizzato del bucket di destinazione.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
 - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
 - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
 - Selezionare il bucket esistente.
 - Copiare e incollare il contenuto del certificato CA del server S3 *destination*.
 - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
 - Il cluster e la VM di storage per ospitare il nuovo bucket.
 - Il nome, la capacità e il livello di servizio delle performance del nuovo bucket. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
 - Contenuto del certificato CA del server S3 di destinazione.
4. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 *origine*.
5. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

Procedura CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path object_store_name:/objstore -destination  
-path svm_name:/bucket/bucket_name
```

Esempio

Nell'esempio seguente viene ripristinato un bucket di destinazione in un bucket esistente.


```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```

Modificare una policy mirror

È possibile modificare una policy di mirroring S3, ad esempio se si desidera regolare i valori RPO e THROTTLE.

System Manager

Se si desidera modificare questi valori, è possibile modificare un criterio di protezione esistente.

1. Fare clic su **protezione > Relazioni**, quindi selezionare il criterio di protezione per la relazione che si desidera modificare.
2. Fare clic su  Accanto al nome del criterio, quindi fare clic su **Modifica**.

CLI

Modifica di un criterio SnapMirror S3:

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

Parametri:

- `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi.
- `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Controllare gli eventi S3

Controllare gli eventi S3

A partire da ONTAP 9.10.1, è possibile controllare i dati e gli eventi di gestione negli ambienti ONTAP S3. La funzionalità di audit S3 è simile alle funzionalità di auditing NAS esistenti e l'auditing S3 e NAS può coesistere in un cluster.

Quando si crea e si attiva una configurazione di controllo S3 su una SVM, gli eventi S3 vengono registrati in un file di registro. È possibile specificare i seguenti eventi da registrare:

- Eventi di accesso a oggetti (dati)
GetObject, PutObject e DeleteObject
- Eventi di gestione
Putbucket e Deletebucket

Il formato del log è JavaScript Object Notation (JSON).

Il limite combinato per le configurazioni di controllo S3 e NFS è di 50 SVM per cluster.

È richiesto il seguente bundle di licenza:

- Bundle core, per protocollo e storage ONTAP S3

Per ulteriori informazioni, vedere ["Come funziona il processo di audit di ONTAP"](#).

Auditing garantito

Per impostazione predefinita, è garantito il controllo S3 e NAS. ONTAP garantisce la registrazione di tutti gli eventi di accesso al bucket verificabili, anche se un nodo non è disponibile. Un'operazione bucket richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.

Requisiti di spazio per il controllo

Nel sistema di audit ONTAP, i record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

I file di staging vengono memorizzati in un volume di staging dedicato, creato da ONTAP al momento della creazione della configurazione di audit. Esiste un volume di staging per aggregato.

È necessario pianificare uno spazio disponibile sufficiente nella configurazione di controllo:

- Per i volumi di staging in aggregati che contengono bucket controllati.
- Per il volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

È possibile controllare il numero di registri eventi e quindi lo spazio disponibile nel volume utilizzando uno dei due metodi per creare la configurazione di controllo S3:

- Un limite numerico; il `-rotate-limit` parametro controlla il numero minimo di file di audit che devono essere conservati.
- Un limite di tempo; il `-retention-duration` parametro controlla il periodo massimo di conservazione dei file.

In entrambi i parametri, una volta superato il valore configurato, è possibile eliminare i file di audit più vecchi per fare spazio a quelli più recenti. Per entrambi i parametri, il valore è 0, a indicare che tutti i file devono essere mantenuti. Per garantire uno spazio sufficiente, è quindi consigliabile impostare uno dei parametri su un valore diverso da zero.

A causa del controllo garantito, se lo spazio disponibile per i dati di audit si esaurisce prima del limite di rotazione, non è possibile creare dati di audit più recenti, con conseguente impossibilità per i client di accedere ai dati. Pertanto, la scelta di questo valore e dello spazio allocato per l'audit deve essere scelta con attenzione, ed è necessario rispondere agli avvisi sullo spazio disponibile dal sistema di audit.

Per ulteriori informazioni, vedere ["Concetti di controllo di base"](#).

Pianificare una configurazione di controllo S3

È necessario specificare una serie di parametri per la configurazione di controllo S3 o accettare le impostazioni predefinite. In particolare, è necessario considerare quali parametri di rotazione del log contribuiranno a garantire un adeguato spazio libero.

Vedere `vserver object-store-server audit create` pagina man per i dettagli della sintassi.

Parametri generali

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. È possibile specificare anche tre parametri opzionali.

Tipo di informazione	Opzione	Obbligatorio
Nome SVM Nome della SVM su cui creare la configurazione di controllo. La SVM deve già esistere ed essere abilitata per S3.	<code>-verserver svm_name</code>	Sì
Percorso di destinazione del registro Specifica dove sono memorizzati i log di audit convertiti. Il percorso deve già esistere sulla SVM. Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura. Se il percorso non è valido, il comando di configurazione del controllo non riesce.	<code>-destination text</code>	Sì
Categorie di eventi da controllare È possibile verificare le seguenti categorie di eventi: <ul style="list-style-type: none">• Eventi Data GetObject, PutObject e DeleteObject• Gestione degli eventi Putbucket e Deletebucket L'impostazione predefinita prevede solo l'audit degli eventi dati.	<code>-events {data management}, ...</code>	No

È possibile inserire uno dei seguenti parametri per controllare il numero di file di log di audit. Se non viene immesso alcun valore, tutti i file di registro vengono conservati.

Tipo di informazione	Opzione	Obbligatorio
Limite di rotazione dei file di log Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette il valore 5, vengono conservati gli ultimi cinque file di registro. Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.	<code>-rotate-limit integer</code>	No

<p>Limite di durata dei file di log</p> <p>Determina per quanto tempo un file di log può essere conservato prima di essere cancellato. Ad esempio, se si immette un valore di 5d0h0m, i registri più vecchi di 5 giorni vengono cancellati.</p> <p>Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.</p>	<p><code>-retention duration integer_time</code></p>	<p>No</p>
---	--	-----------

Parametri per la rotazione del registro di controllo

È possibile ruotare i registri di audit in base alle dimensioni o alla pianificazione. L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

Ruotare i registri in base alle dimensioni del registro

Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log. La dimensione predefinita del registro è 100 MB.

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata.

Se si desidera ripristinare la rotazione solo in base alle dimensioni del log, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Ruotare i registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
 - `-rotate-schedule-month`
 - `-rotate-schedule-dayofweek`
 - `-rotate-schedule-day`
 - `-rotate-schedule-hour`
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo. Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.
- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate-schedule-month` e `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, sono considerati indipendenti.

Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e `-rotate-schedule-day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ripristinare la rotazione solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni del log e a una pianificazione impostando sia il parametro `-rotate-size` che i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

Creare e abilitare una configurazione di controllo S3

Per implementare il controllo S3, creare prima una configurazione di controllo dell'archivio di oggetti persistente su una SVM abilitata per S3, quindi attivare la configurazione.

Di cosa hai bisogno

- Una SVM abilitata per S3.
- Spazio sufficiente per lo staging dei volumi nell'aggregato.

A proposito di questa attività

Per ogni SVM contenente i bucket S3 che si desidera controllare è necessaria una configurazione di controllo. È possibile attivare il controllo S3 su server S3 nuovi o esistenti. Le configurazioni di controllo persistono in un ambiente S3 fino a quando non vengono rimosse dal comando **`vserver object-store-server audit delete`**.

La configurazione di controllo S3 si applica a tutti i bucket della SVM selezionati per il controllo. Una SVM abilitata all'audit può contenere bucket controllati e non verificati.

Si consiglia di configurare il controllo S3 per la rotazione automatica del log, determinata dalle dimensioni del log o da una pianificazione. Se non si configura la rotazione automatica del log, tutti i file di log vengono conservati per impostazione predefinita. È inoltre possibile ruotare manualmente i file di log S3 utilizzando il comando **`vserver object-store-server audit rotate-log`**.

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

Procedura

1. Creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del registro o a una pianificazione.

Se si desidera ruotare i registri di audit di...	Inserisci...
Dimensione del log	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [- retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate-size {integer[KB MB GB TB PB]}]</pre>
Un calendario	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [- retention-duration [integerd][integerh] [integerm][_integers]]] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [- rotate-schedule-day chron_dayofmonth] [-rotate- schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>Il <code>-rotate-schedule-minute</code> il parametro è obbligatorio se si configura la rotazione del log di audit basata sul tempo.</p>

2. Abilita controllo S3:

```
vserver object-store-server audit enable -vserver svm_name
```

Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3 (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. I registri vengono memorizzati nella directory `/audit_log`. Il limite delle dimensioni del file di log è di 200 MB. I log vengono ruotati quando raggiungono le dimensioni di 200 MB.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3 (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il limite delle dimensioni del file di registro è di 100 MB (impostazione predefinita) e i registri vengono conservati per 5 giorni prima di essere cancellati.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla gli eventi di gestione S3 e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è 5.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Selezionare i bucket per il controllo S3

È necessario specificare quali bucket eseguire il controllo in una SVM abilitata per l'audit.

Di cosa hai bisogno

- SVM abilitato per il controllo S3.

A proposito di questa attività

Le configurazioni di controllo S3 sono abilitate per SVM, ma è necessario selezionare i bucket nelle SVM che sono abilitati per l'audit. Se si aggiungono bucket alla SVM e si desidera che i nuovi bucket vengano controllati, è necessario selezionarli con questa procedura. È inoltre possibile avere bucket non controllati in una SVM abilitata per il controllo S3.

Le configurazioni di controllo persistono per i bucket fino a quando non vengono rimosse da `vserver object-store-server audit object-select delete` comando.

Procedura

Seleziona un bucket per l'audit S3:

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-only|deny-only|all}]
```

- `-access` - specifica il tipo di accesso all'evento da sottoporre a verifica: `read-only`, `write-only` oppure `all` (il valore predefinito è `all`).
- `-permission` - specifica il tipo di autorizzazione all'evento da sottoporre a verifica: `allow-only`, `deny-only` oppure `all` (il valore predefinito è `all`).

Esempio

Nell'esempio seguente viene creata una configurazione di controllo del bucket che registra solo gli eventi consentiti con accesso in sola lettura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1 -bucket test-bucket -access read-only -permission allow-only
```

Modificare una configurazione di controllo S3

È possibile modificare i parametri di controllo dei singoli bucket o la configurazione di controllo di tutti i bucket selezionati per l'audit nella SVM.

Se si desidera modificare la configurazione dell'audit per...	Inserisci...
Bucket individuali	<code>vserver object-store-server audit event-selector modify -vserver <i>svm_name</i> [-bucket <i>bucket_name</i>] [<i>parameters to modify</i>]</code>
Tutti i bucket di SVM	<code>vserver object-store-server audit modify -vserver <i>svm_name</i> [<i>parameters to modify</i>]</code>

Esempi

Nell'esempio seguente viene modificata una singola configurazione di controllo del bucket per controllare solo gli eventi di accesso di sola scrittura:

```
cluster1:> vserver object-store-server audit event-selector modify  
-vserver vs1 -bucket test-bucket -access write-only
```

Nell'esempio riportato di seguito viene modificata la configurazione di controllo di tutti i bucket di SVM per modificare il limite delle dimensioni dei log a 10 MB e conservare 3 file di log prima della rotazione.

```
cluster1:> vserver object-store-server audit modify -vserver vs1 -rotate  
-size 10MB -rotate-limit 3
```

Mostrare le configurazioni di controllo S3

Una volta completata la configurazione di controllo, è possibile verificare che il controllo sia configurato correttamente e sia attivato. È inoltre possibile visualizzare informazioni su tutte le configurazioni di controllo dell'archivio di oggetti nel cluster.

A proposito di questa attività

È possibile visualizzare informazioni sulle configurazioni di controllo bucket e SVM.

- **Bucket** – utilizzare `vserver object-store-server audit event-selector show` comando

Senza alcun parametro, il comando visualizza le seguenti informazioni sui bucket in tutte le SVM del cluster con configurazioni di controllo degli archivi di oggetti:

- Nome SVM
- Nome bucket
- Valori di accesso e autorizzazione

- **SVM**: Utilizzare `vserver object-store-server audit show` comando

Senza alcun parametro, il comando visualizza le seguenti informazioni su tutte le SVM nel cluster con configurazioni di controllo degli archivi di oggetti:

- Nome SVM
- Stato di audit
- Directory di destinazione

È possibile specificare `-fields` parametro per specificare le informazioni di configurazione di controllo da visualizzare.

Procedura

Mostra informazioni sulle configurazioni di controllo S3:

Se si desidera modificare la configurazione per...	Inserisci...
Bucket	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVM	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a un singolo bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
```

Vserver	Bucket	Access	Permission
-----	-----	-----	-----
vs1	bucket1	read-only	allow-only

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i bucket di una SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1
```

Vserver	:vs1
Bucket	:test-bucket
Access	:all
Permission	:all

Nell'esempio riportato di seguito vengono visualizzati il nome, lo stato di controllo, i tipi di evento, il formato del registro e la directory di destinazione di tutte le SVM.

```
cluster1::> vserver object-store-server audit show
```

Vserver	State	Event Types	Log Format	Target Directory
-----	-----	-----	-----	-----
vs1	false	data	json	/audit_log

Nell'esempio seguente vengono visualizzati i nomi e i dettagli SVM relativi al registro di controllo per tutte le SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details
```

Vserver	Rotation File Size	Rotation Schedule	Rotation Limit
vs1	100MB	-	0

Nell'esempio riportato di seguito vengono visualizzate tutte le informazioni di configurazione dell'audit relative a tutte le SVM.

```
cluster1::> vserver object-store-server audit show -instance
```

```

    Vserver: vs1
    Auditing state: true
    Log Destination Path: /audit_log
    Categories of Events to Audit: data
    Log Format: json
    Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
    Log Rotation Schedule: Day of Week: -
    Log Rotation Schedule: Day: -
    Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
    Rotation Schedules: -
    Log Files Rotation Limit: 0
    Log Retention Time: 0s
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.