



Proteggi i bucket con S3 SnapMirror

ONTAP 9

NetApp
April 24, 2024

Sommario

- Proteggi i bucket con S3 SnapMirror 1
 - Panoramica di S3 SnapMirror 1
 - Protezione del mirroring e del backup su un cluster remoto 3
 - Protezione del mirroring e del backup sul cluster locale 14
 - Protezione del backup con destinazioni cloud 25
 - Modificare una policy mirror 34

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		✓
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; s 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
```

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.