# Protezione del mirroring e del backup sul cluster locale

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/s3-snapmirror/create-local-mirror-new-bucket-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

# Sommario

Protezione del mirroring e del backup sul cluster locale . . . . . 1
Creare una relazione di mirroring per un nuovo bucket di ONTAP S3 nel cluster locale . . . . . 1
Creare una relazione di mirroring per un bucket ONTAP S3 esistente nel cluster locale . . . . . 5
Takeover del bucket ONTAP S3 di destinazione nel cluster locale . . . . . 9
Ripristino di un bucket ONTAP S3 dalla SVM di destinazione sul cluster locale . . . . . 10

# Protezione del mirroring e del backup sul cluster locale

## Creare una relazione di mirroring per un nuovo bucket di ONTAP S3 nel cluster locale

Quando crei nuovi bucket S3, puoi proteggerli immediatamente in una destinazione SnapMirror S3 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 del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e 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 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 per aggiungere utenti ai gruppi, nelle VM di storage di origine e di destinazione: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** e quindi su sotto S3.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.

3. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio 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 **continuo** per le relazioni SnapMirror S3.
      - 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. In questo caso si tratta della prima relazione di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi utente root per le SVM di origine e di destinazione e rigenerarle, se non:
   `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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi 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 criterio per le relazioni SnapMirror S3 (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.

      Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Crea 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`

**Informazioni correlate**

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

# Creare una relazione di mirroring per un bucket ONTAP S3 esistente nel 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 del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e 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 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 gli utenti e i gruppi esistenti siano presenti e che abbiano accesso corretto sia nelle VM di storage di origine che di destinazione: Selezionare **Storage > Storage VM,** quindi selezionare la VM di storage, quindi la scheda **Settings**. Infine, individuare il riquadro **S3**, selezionare e selezionare la scheda **utenti**, quindi la scheda **gruppi** per visualizzare le impostazioni di accesso degli utenti e dei gruppi.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.
3. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio 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 **continuo** per le relazioni SnapMirror S3.
      - 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 **Edit**, quindi su **Add** in **Permissions**.
      - **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. Proteggere una benna esistente con SnapMirror S3:
   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. In questo caso si tratta della prima relazione di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi utente root per le SVM di origine e di destinazione e rigenerarle, se non:
   `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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi 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 criterio per le relazioni SnapMirror S3 (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.

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Crea 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`

**Informazioni correlate**

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

# Takeover del bucket ONTAP S3 di destinazione nel 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 SnapMirror S3.

Quando il bucket sorgente disabilitato è nuovamente disponibile, SnapMirror S3 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 **SnapMirror S3**.
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
```

**Informazioni correlate**

- "avvio del failover di SnapMirror"
- "spettacolo snapmirror"

# Ripristino di un bucket ONTAP S3 dalla SVM di destinazione sul 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 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 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 del 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 cloud per un nuovo bucket ONTAP S3".
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
```

Ulteriori informazioni su `snapmirror restore` nella "Riferimento al comando ONTAP".

**Informazioni sul copyright**

Copyright © 2026 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.