



# **Protezione dei dati con System Manager**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommario

|  |    |
|--|----|
| Protezione dei dati con System Manager .....                                       | 1  |
| Panoramica sulla protezione dei dati con System Manager .....                      | 1  |
| Creare policy di protezione dei dati personalizzate .....                          | 1  |
| Configurare le copie Snapshot .....  | 2  |
| Calcola lo spazio recuperabile prima di eliminare le copie Snapshot .....          | 2  |
| Attivare o disattivare l'accesso del client alla directory di copia Snapshot ..... | 2  |
| Preparazione per il mirroring e il vaulting .....                                  | 3  |
| Configurare mirror e vault .....   | 4  |
| Risincronizzare una relazione di protezione .....                                  | 5  |
| Ripristinare un volume da una copia Snapshot precedente .....                      | 5  |
| Ripristino da copie Snapshot .....   | 6  |
| Ripristinare su un nuovo volume .....  | 6  |
| Risincronizzazione inversa di una relazione di protezione .....                    | 6  |
| Fornire i dati da una destinazione SnapMirror .....                                | 7  |
| Configurare il disaster recovery delle macchine virtuali dello storage .....       | 8  |
| Fornire i dati da una destinazione DR SVM .....                                    | 8  |
| Riattivare una VM di storage di origine .....                                      | 9  |
| Risincronizzare una VM di storage di destinazione .....                            | 9  |
| Eseguire il backup dei dati nel cloud utilizzando SnapMirror .....                 | 10 |
| Eseguire il backup dei dati utilizzando Cloud Backup .....                         | 12 |

# Protezione dei dati con System Manager

## Panoramica sulla protezione dei dati con System Manager

Gli argomenti di questa sezione illustrano come configurare e gestire la protezione dei dati con Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione sistema in ONTAP 9.7 o versioni precedenti, vedere ["Documentazione classica di Gestore di sistema ONTAP"](#)

Proteggi i tuoi dati creando e gestendo copie Snapshot, mirror, vault e relazioni mirror-and-vault.

*SnapMirror* è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o mirror, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

Un *vault* è progettato per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

A partire da ONTAP 9.10.1, è possibile creare relazioni di protezione dei dati tra i bucket S3 utilizzando S3 SnapMirror. I bucket di destinazione possono essere su sistemi ONTAP locali o remoti o su sistemi non ONTAP come StorageGRID e AWS. Per ulteriori informazioni, vedere ["Panoramica di S3 SnapMirror"](#).

## Creare policy di protezione dei dati personalizzate

È possibile creare policy di protezione dei dati personalizzate con System Manager quando le policy di protezione predefinite esistenti non sono adatte alle proprie esigenze. A partire da ONTAP 9.11.1, è possibile utilizzare Gestore di sistema per creare policy personalizzate di mirroring e vault, per visualizzare e selezionare policy legacy. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.

Creare policy di protezione personalizzate sul cluster di origine e di destinazione.

### Fasi

1. Fare clic su **Protection > Local Policy Settings** (protezione > Impostazioni policy locali).
2. Nella sezione **Criteri di protezione**, fare clic su ➔.
3. Nel riquadro **Criteri di protezione**, fare clic su + Add.
4. Inserire il nuovo nome del criterio e selezionare l'ambito del criterio.
5. Scegliere un tipo di policy. Per aggiungere una policy di solo vault o solo mirror, scegliere **Asynchronous** e fare clic su **Usa un tipo di policy legacy**.
6. Compilare i campi obbligatori.
7. Fare clic su **Save** (Salva).
8. Ripetere questi passaggi sull'altro cluster.

# Configurare le copie Snapshot

È possibile creare policy di copia Snapshot per specificare il numero massimo di copie Snapshot create automaticamente e la frequenza di creazione. Il criterio specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome.

Questa procedura crea un criterio di copia Snapshot solo sul cluster locale.

## Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali**.
2. In **Snapshot Policies**, fare clic su ➔, quindi fare clic su **+ Add**.
3. Digitare il nome del criterio, selezionare l'ambito del criterio e in **Pianificazioni**, fare clic su **+ Add** per inserire i dettagli della pianificazione.

# Calcola lo spazio recuperabile prima di eliminare le copie Snapshot

A partire da ONTAP 9.10.1, è possibile utilizzare Gestore di sistema per selezionare le copie Snapshot che si desidera eliminare e calcolare lo spazio recuperabile prima di eliminarle.

## Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume dal quale si desidera eliminare le copie Snapshot.
3. Fare clic su **copie Snapshot**.
4. Selezionare una o più copie Snapshot.
5. Fare clic su **Calcola spazio recuperabile**.

# Attivare o disattivare l'accesso del client alla directory di copia Snapshot


A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per attivare o disattivare i sistemi client per accedere a una directory di copia Snapshot su un volume. L'abilitazione dell'accesso rende la directory di copia Snapshot visibile ai client e consente ai client Windows di mappare un disco alla directory Snapshot Copies per visualizzarne e accedervi.

È possibile attivare o disattivare l'accesso alla directory di copia Snapshot di un volume modificando le impostazioni del volume o le impostazioni di condivisione del volume.

## Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando un volume

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.


## Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.
3. Fare clic su  E selezionare **Modifica**.
4. Nella sezione **Snapshot Copies (Local) Settings**, selezionare o deselezionare **Show the Snapshot Copies directory to clients** (Mostra la directory Snapshot Copies ai client).
5. Fare clic su **Save** (Salva).

## Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando una condivisione

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.

### Fasi

1. Fare clic su **Storage > Shares**.
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.
3. Fare clic su  E selezionare **Modifica**.
4. Nella sezione **Proprietà condivisione**, selezionare o deselezionare **Consenti ai client di accedere alla directory Snapshot Copies**.
5. Fare clic su **Save** (Salva).


## Preparazione per il mirroring e il vaulting



È possibile proteggere i dati replicandoli in un cluster remoto per il backup dei dati e il disaster recovery.

Sono disponibili diversi criteri di protezione predefiniti. Se si desidera utilizzare policy personalizzate, è necessario aver creato le policy di protezione.



### Fasi

1. Nel cluster locale, fare clic su **protezione > Panoramica**.
2. Espandere **Impostazioni Intercluster**. Fare clic su **Add Network Interfaces** (Aggiungi interfacce di rete) e aggiungere interfacce di rete intercluster per il cluster.  
  
Ripetere questo passaggio sul cluster remoto.
3. Nel cluster remoto, fare clic su **protezione > Panoramica**. Fare clic su  Nella sezione Cluster Peers (peer cluster), fare clic su **generate Passphrase** (genera passphrase)
4. Copiare la passphrase generata e incollarla nel cluster locale.
5. Nel cluster locale, in Cluster Peers, fare clic su **Peer Clusters** e eseguire il peer dei cluster locali e remoti.

6. In alternativa, sotto Storage VM Peers, fare clic su  E poi **Peer Storage VM** per eseguire il peer delle VM di storage.
  7. Fare clic su **Protect Volumes** (Proteggi volumi) per proteggere i volumi. Per proteggere i LUN, fare clic su **Storage > LUN**, selezionare un LUN da proteggere, quindi fare clic su  **Protect**.
- Selezionare la policy di protezione in base al tipo di protezione dei dati desiderata.
8. Per verificare che i volumi e le LUN siano protetti correttamente dal cluster locale, fare clic su **Storage > Volumes** o **Storage > LUN** e espandere la vista volume/LUN.

## Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                      | Guarda questo contenuto...   |
|--|--|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica sulla preparazione del disaster recovery dei volumi"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Creare una relazione peer del cluster"</a>                          |

## Configurare mirror e vault

Creare un mirror e un vault di un volume per proteggere i dati in caso di disastro e avere più versioni archiviate dei dati su cui eseguire il rollback. A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per selezionare policy di vault e mirror pre-create e personalizzate, per visualizzare e selezionare policy legacy e per ignorare le pianificazioni di trasferimento definite in una policy di protezione quando si proteggono volumi e macchine virtuali di storage. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.




Se si utilizza ONTAP 9.8P12 o versione successiva della patch per ONTAP 9.8 e si configura SnapMirror utilizzando Gestione di sistema, è necessario utilizzare ONTAP 9.9.1P13 o versione successiva e ONTAP 9.10.1P10 o versioni successive se si intende eseguire l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1.

Questa procedura crea un criterio di protezione dei dati su un cluster remoto. Il cluster di origine e il cluster di destinazione utilizzano interfacce di rete intercluster per lo scambio di dati. La procedura presuppone ["vengono create le interfacce di rete tra cluster e i cluster contenenti i volumi vengono peering"](#) (accoppiato). È inoltre possibile eseguire il peer delle macchine virtuali storage per la protezione dei dati; tuttavia, se le macchine virtuali storage non sono in peering, ma le autorizzazioni sono attivate, le macchine virtuali storage vengono automaticamente messe in peering quando viene creata la relazione di protezione.



### Fasi

1. Selezionare il volume o il LUN da proteggere: Fare clic su **Storage > Volumes** o **Storage > LUN**, quindi fare clic sul nome del volume o del LUN desiderato.
2. Fare clic su  **Protect**.

3. Selezionare il cluster di destinazione e la VM di storage.
4. Il criterio asincrono viene selezionato per impostazione predefinita. Per selezionare un criterio sincrono, fare clic su **altre opzioni**.
5. Fare clic su **Protect** (protezione).
6. Fare clic sulla scheda **SnapMirror (locale o remoto)** del volume o LUN selezionato per verificare che la protezione sia impostata correttamente.

#### Informazioni correlate

- ["Creazione ed eliminazione di volumi di test del failover SnapMirror"](#).

## Altri modi per farlo in ONTAP


| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                       |
|--|--|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica del backup del volume con SnapVault"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Creare una relazione di replica"</a>                |

## Risincronizzare una relazione di protezione

Quando il volume di origine è nuovamente disponibile dopo un disastro, è possibile risincronizzare i dati dal volume di destinazione e ristabilire la relazione di protezione.

Questa procedura sostituisce i dati nel volume di origine originale in una relazione asincrona, in modo da poter iniziare nuovamente a servire i dati dal volume di origine e riprendere la relazione di protezione originale.

#### Fasi


1. Fare clic su **protezione > Relazioni**, quindi sulla relazione interrotta che si desidera risincronizzare.
2. Fare clic su  Quindi selezionare **Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione controllando lo stato della relazione. Lo stato diventa "mirrored" al termine della risincronizzazione.

## Ripristinare un volume da una copia Snapshot precedente

In caso di perdita o danneggiamento dei dati in un volume, è possibile eseguire il rollback dei dati eseguendo il ripristino da una copia Snapshot precedente.

Questa procedura sostituisce i dati correnti sul volume di origine con i dati di una versione di copia Snapshot precedente. Eseguire questa attività sul cluster di destinazione.

#### Fasi

1. Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume di origine.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), il volume di origine viene selezionato per impostazione predefinita. Fare clic su **Other Volume** (Altro volume) se si desidera scegliere un volume diverso dall'origine.
4. In **destinazione**, scegliere la copia Snapshot che si desidera ripristinare.

5. Se l'origine e la destinazione si trovano in cluster diversi, sul cluster remoto fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

## Altri modi per farlo in ONTAP


| Per eseguire queste attività con...                                      | Guarda questo contenuto...  |
|--|---|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica del ripristino del volume con SnapVault"</a>                    |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Ripristinare il contenuto di un volume da una destinazione SnapMirror"</a> |

## Ripristino da copie Snapshot

È possibile ripristinare un volume a un punto precedente eseguendo il ripristino da una copia Snapshot.

Questa procedura ripristina un volume da una copia Snapshot.

### Fasi


1. Fare clic su **Storage** e selezionare un volume.
2. In **Snapshot Copies**, fare clic su  Accanto alla copia Snapshot che si desidera ripristinare e selezionare **Restore** (Ripristina).

## Ripristinare su un nuovo volume

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per ripristinare i dati di backup sul volume di destinazione su un volume diverso dall'origine originale.

Quando si esegue il ripristino su un volume diverso, è possibile selezionare un volume esistente o crearne uno nuovo.

### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su  E fare clic su **Restore**.
3. Nella sezione **origine**, selezionare **Altro volume** e selezionare il cluster e la Storage VM.
4. Selezionare **Existing volume** (volume esistente) o **Create a new volume** (Crea nuovo volume).
5. Se si sta creando un nuovo volume, immettere il nome del volume.
6. Nella sezione **destinazione**, selezionare la copia Snapshot da ripristinare.
7. Fare clic su **Save** (Salva).
8. In **Relazioni**, monitorare l'avanzamento del ripristino visualizzando **Stato trasferimento** per la relazione.

## Risincronizzazione inversa di una relazione di protezione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per eseguire un'operazione di risincronizzazione inversa per eliminare una relazione di protezione




esistente e invertire le funzioni dei volumi di origine e di destinazione. Quindi si utilizza il volume di destinazione per fornire i dati durante la riparazione o la sostituzione dell'origine, l'aggiornamento dell'origine e il ripristino della configurazione originale dei sistemi.



System Manager non supporta la risincronizzazione inversa con relazioni intracluster. È possibile utilizzare l'interfaccia utente di ONTAP per eseguire operazioni di risincronizzazione inversa con relazioni intracluster.

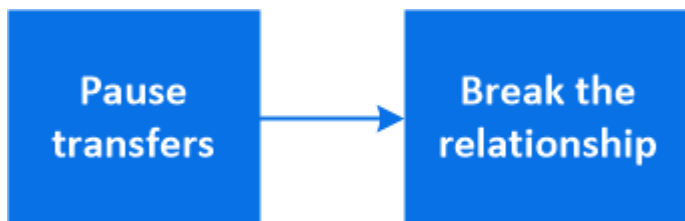
Quando si esegue un'operazione di risincronizzazione inversa, tutti i dati sul volume di origine più recenti dei dati nella copia Snapshot comune vengono cancellati.

#### Fasi


1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su  E fare clic su **Reverse Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione inversa visualizzando **Stato trasferimento** per la relazione.

## Fornire i dati da una destinazione SnapMirror

Per fornire dati da una destinazione mirror quando un'origine non è disponibile, interrompere i trasferimenti pianificati verso la destinazione, quindi interrompere la relazione SnapMirror per rendere la destinazione scrivibile.



#### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume desiderato.
2. Fare clic su .
3. Stop scheduled transfer (Interrompi trasferimenti pianificati): Fare clic su **Pause**
4. Rendere scrivibile la destinazione: Fare clic su **Interrompi**.
5. Andare alla pagina principale **Relazioni** per verificare che lo stato della relazione sia visualizzato come "interrotto".

#### Fasi successive:

Quando il volume di origine disattivato è nuovamente disponibile, è necessario risincronizzare la relazione per copiare i dati correnti nel volume di origine originale. Questo processo sostituisce i dati sul volume di origine originale.

## Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                    |
|--|---|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica sul disaster recovery dei volumi"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Attivare il volume di destinazione"</a>          |

## Configurare il disaster recovery delle macchine virtuali dello storage

Con System Manager, è possibile creare una relazione di disaster recovery per le macchine virtuali di storage (DR per le macchine virtuali di storage) per replicare una configurazione delle macchine virtuali di storage in un'altra. In caso di disastro nel sito primario, è possibile attivare rapidamente la VM di storage di destinazione.

Completare questa procedura dalla destinazione. Se è necessario creare un nuovo criterio di protezione, ad esempio, quando la VM dello storage di origine ha SMB configurato, è necessario utilizzare System Manager per creare il criterio e selezionare l'opzione **Identity Preserve** nella finestra **Add Protection Policy**. Per ulteriori informazioni, vedere ["Creare policy di protezione dei dati personalizzate"](#).



### Fasi

1. Nel cluster di destinazione, fare clic su **protezione > Relazioni**.
2. In **Relazioni**, fare clic su Proteggi e scegliere **Storage VM (DR)**.
3. Selezionare un criterio di protezione. Se è stato creato un criterio di protezione personalizzato, selezionarlo, quindi scegliere il cluster di origine e la VM di storage che si desidera replicare. È inoltre possibile creare una nuova VM di storage di destinazione immettendo un nuovo nome per la VM di storage.
4. Fare clic su **Save** (Salva).

## Fornire i dati da una destinazione DR SVM

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per attivare una VM di storage di destinazione dopo un disastro. L'attivazione della VM di storage di destinazione rende i volumi di destinazione SVM scrivibili e consente di inviare i dati ai client.

### Fasi

1. Se il cluster di origine è accessibile, verificare che SVM sia stato arrestato: Selezionare **Storage > Storage VM** e selezionare la colonna **state** per SVM.
2. Se lo stato SVM di origine è "in esecuzione", interromperlo: Selezionare  E scegliere **Stop**.
3. Sul cluster di destinazione, individuare la relazione di protezione desiderata: Accedere a **protezione > Relazioni**.
4. Fare clic su  E scegliere **Activate Destination Storage VM**.

# Riattivare una VM di storage di origine


A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per riattivare una VM di storage di origine dopo un disastro. La riattivazione della VM di storage di origine interrompe la VM di storage di destinazione e riattiva la replica dall'origine alla destinazione.

## A proposito di questa attività

Quando si riattiva la VM dello storage di origine, System Manager esegue le seguenti operazioni in background:

- Crea una relazione DR SVM inversa dalla destinazione originale all'origine utilizzando la risincronizzazione di SnapMirror
- Arresta la SVM di destinazione
- Aggiorna la relazione di SnapMirror
- Interrompe la relazione di SnapMirror
- Riavvia la SVM originale
- Effettua una risincronizzazione di SnapMirror dell'origine originale verso la destinazione originale
- Elimina le relazioni di SnapMirror

## Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su  E fare clic su **Riattiva VM storage di origine**.
3. In **Relazioni**, monitorare l'avanzamento della riattivazione dell'origine visualizzando **Stato trasferimento** per la relazione di protezione.


# Risincronizzare una VM di storage di destinazione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per risincronizzare i dati e i dettagli di configurazione dalla VM di storage di origine alla VM di storage di destinazione in una relazione di protezione interrotta e ristabilire la relazione.

ONTAP 9.11.1 introduce un'opzione per evitare la ricostruzione completa del data warehouse quando si esegue una prova di disaster recovery, consentendo di tornare più rapidamente alla produzione.

L'operazione di risincronizzazione viene eseguita solo dalla destinazione della relazione originale. La risincronizzazione elimina tutti i dati nella VM di storage di destinazione più recenti dei dati nella VM di storage di origine.

## Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Facoltativamente, selezionare **Perform a quick resync** (Esegui una risincronizzazione rapida) per ignorare la ricostruzione completa del data warehouse durante una prova di disaster recovery.
3. Fare clic su  E fare clic su **Resync**.
4. In **Relazioni**, monitorare l'avanzamento della risincronizzazione visualizzando **Stato trasferimento** per la relazione.

# Eseguire il backup dei dati nel cloud utilizzando SnapMirror

A partire da ONTAP 9.9.1, puoi eseguire il backup dei dati nel cloud e ripristinare i dati dal cloud storage a un volume diverso utilizzando Gestione di sistema. Puoi utilizzare StorageGRID o ONTAP S3 come archivio di oggetti cloud.

Prima di utilizzare la funzione SnapMirror Cloud, è necessario richiedere una chiave di licenza API di SnapMirror Cloud al sito di supporto NetApp: ["Richiedere la chiave di licenza API di SnapMirror Cloud"](#). Seguendo le istruzioni, fornisci una semplice descrizione dell'opportunità di business e richiedi la chiave API inviando un'email all'indirizzo email fornito. Entro 24 ore riceverai una risposta via email con ulteriori istruzioni su come acquisire la chiave API.

## Aggiungere un archivio di oggetti cloud

Prima di configurare i backup di SnapMirror Cloud, è necessario aggiungere un archivio di oggetti cloud StorageGRID o ONTAP S3.

### Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Fare clic su **+ Add**.

## Eseguire il backup utilizzando il criterio predefinito

È possibile configurare rapidamente un backup di SnapMirror Cloud per un volume esistente utilizzando la policy di protezione cloud predefinita, DailyBackup.

### Fasi

1. Fare clic su **protezione > Panoramica** e selezionare **Backup dei volumi nel cloud**.
2. Se è la prima volta che si esegue il backup nel cloud, inserire la chiave di licenza API di SnapMirror Cloud nel campo della licenza, come indicato.
3. Fare clic su **Authenticate and Continue** (autentica e continua)
4. Selezionare un volume di origine.
5. Selezionare un archivio di oggetti cloud.
6. Fare clic su **Save** (Salva).

## Creare una policy di backup cloud personalizzata

Se non si desidera utilizzare la policy cloud predefinita di DailyBackup per i backup di SnapMirror Cloud, è possibile creare una policy personalizzata.

### Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali** e selezionare **Criteri di protezione**.
2. Fare clic su **Add** (Aggiungi) e inserire i nuovi dettagli della policy.
3. Nella sezione **Policy Type**, selezionare **Backup to Cloud** per indicare che si sta creando una policy cloud.
4. Fare clic su **Save** (Salva).

## Creare un backup dalla pagina volumi

È possibile utilizzare la pagina System Manager **Volumes** per selezionare e creare backup cloud per più volumi contemporaneamente o quando si desidera utilizzare una policy di protezione personalizzata.

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare i volumi di cui si desidera eseguire il backup nel cloud e fare clic su **Protect**.
3. Nella finestra **Protect Volume** (Proteggi volume), fare clic su **More Options** (altre opzioni).
4. Selezionare un criterio.


È possibile selezionare il criterio predefinito, DailyBackup o un criterio cloud personalizzato creato.

5. Selezionare un archivio di oggetti cloud.
6. Fare clic su **Save** (Salva).

## Eseguire il ripristino dal cloud

È possibile utilizzare System Manager per ripristinare i dati di backup dallo storage cloud a un volume diverso nel cluster di origine.


### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare la scheda **Backup nel cloud**.
3. Fare clic su  Accanto al volume di origine che si desidera ripristinare e selezionare **Restore** (Ripristina).
4. In **Source** (origine), selezionare una VM di storage e immettere il nome del volume in cui si desidera ripristinare i dati.
5. In **destinazione**, selezionare la copia Snapshot che si desidera ripristinare.
6. Fare clic su **Save** (Salva).

## Eliminare una relazione SnapMirror Cloud

È possibile utilizzare System Manager per eliminare una relazione cloud.


### Fasi

1. Fare clic su **Storage > Volumes** (archiviazione > volumi) e selezionare il volume che si desidera eliminare.
2. Fare clic su  Accanto al volume di origine e selezionare **Delete** (Elimina).
3. Selezionare **Delete the cloud object store endpoint (opzionale)** se si desidera eliminare l'endpoint dell'archivio di oggetti cloud.
4. Fare clic su **Delete** (Elimina).

## Rimuovere un archivio di oggetti cloud

È possibile utilizzare System Manager per rimuovere un archivio di oggetti cloud se non fa parte di una relazione di backup cloud. Quando un archivio di oggetti cloud fa parte di una relazione di backup cloud, non può essere cancellato.

### Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Selezionare l'archivio di oggetti che si desidera eliminare, quindi fare clic su  E selezionare **Delete** (Elimina).

## Eseguire il backup dei dati utilizzando Cloud Backup

A partire da ONTAP 9.9.1, puoi utilizzare Gestione sistema per eseguire il backup dei dati nel cloud utilizzando il backup nel cloud.



Cloud Backup supporta volumi di lettura/scrittura FlexVol e volumi di protezione dei dati (DP). I volumi FlexGroup e SnapLock non sono supportati.

### Prima di iniziare

Per creare un account in BlueXP, attenersi alle seguenti procedure. Per l'account di servizio, è necessario creare il ruolo di "account Admin". (Gli altri ruoli dell'account di servizio non dispongono dei privilegi necessari per stabilire una connessione da System Manager).

1. ["Creare un account in BlueXP"](#).
2. ["Creare un connettore in BlueXP"](#) con uno dei seguenti cloud provider:
  - Microsoft Azure
  - Amazon Web Services (AWS)
  - Piattaforma Google Cloud (GCP)
  - StorageGRID (ONTAP 9.10.1)



A partire da ONTAP 9.10.1, è possibile selezionare StorageGRID come provider di backup cloud, ma solo se BlueXP è implementato on-premise. BlueXP Connector deve essere installato on-premise e disponibile tramite l'applicazione Software-as-a-Service (SaaS) BlueXP.

3. ["Iscriviti a Cloud Backup Service in BlueXP"](#) (richiede la licenza appropriata).
4. ["Generare una chiave di accesso e una chiave segreta utilizzando BlueXP"](#).

## Registrare il cluster con BlueXP

È possibile registrare il cluster con BlueXP utilizzando BlueXP o System Manager.

### Fasi

1. In System Manager, accedere a **Panoramica sulla protezione**.
2. In **Cloud Backup Service**, fornire i seguenti dettagli:
  - ID client
  - Chiave segreta del client
3. Selezionare **Registra e continua**.

## Attiva Cloud Backup

Una volta registrato il cluster con BlueXP, è necessario attivare Cloud Backup e avviare il primo backup nel

cloud.

## Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.
2. Inserire **ID client** e **Segreto client**.



A partire da ONTAP 9.10.1, puoi scoprire il costo dell'utilizzo del cloud facendo clic su **ulteriori informazioni sul costo dell'utilizzo del cloud**.

3. Fare clic su **Connetti e attiva Cloud Backup Service**.
4. Nella pagina **Enable Cloud Backup Service** (attiva protocollo), fornire i seguenti dettagli, a seconda del provider selezionato.

| Per questo cloud provider...   | Inserire i seguenti dati...  |
|--|--|
| Azure  | <ul style="list-style-type: none"><li>• ID abbonamento Azure</li><li>• Regione</li><li>• Nome del gruppo di risorse (esistente o nuovo)</li></ul>                                |
| AWS  | <ul style="list-style-type: none"><li>• ID account AWS</li><li>• Tasto di accesso</li><li>• Chiave segreta</li><li>• Regione</li></ul>   |
| Google Cloud Project (GCP)   | <ul style="list-style-type: none"><li>• Nome del progetto Google Cloud</li><li>• Chiave Google Cloud Access</li><li>• Chiave segreta di Google Cloud</li><li>• Regione</li></ul> |
| StorageGRID (ONTAP 9.10.1 e versioni successive e solo per l'implementazione on-premise di BlueXP) | <ul style="list-style-type: none"><li>• Server</li><li>• Chiave di accesso SG</li><li>• Chiave segreta SG</li></ul>  |

5. Selezionare una **policy di protezione**:
  - **Policy esistente**: Scegliere una policy esistente.
  - **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.



A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.



Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.


Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

- Il numero di giorni trascorsi i quali il volume viene archiviato.
  - Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
  - Per AWS, selezionare la classe di storage di archiviazione.
6. Selezionare i volumi di cui si desidera eseguire il backup.
  7. Selezionare **Salva**.

## Modificare il criterio di protezione utilizzato per Cloud Backup

È possibile modificare i criteri di protezione utilizzati con Cloud Backup.

### Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.
2. Fare clic su , Quindi **Modifica**.
3. Selezionare una **policy di protezione**:
  - **Policy esistente**: Scegliere una policy esistente.
  - **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.



A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.



Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.

Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

- Il numero di giorni trascorsi i quali il volume viene archiviato.
  - Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
  - Per AWS, selezionare la classe di storage di archiviazione.
4. Selezionare **Salva**.

## Proteggere nuovi volumi o LUN sul cloud

Quando si crea un nuovo volume o LUN, è possibile stabilire una relazione di protezione di SnapMirror che consenta il backup nel cloud per il volume o il LUN.

### Prima di iniziare

- È necessario disporre di una licenza SnapMirror.
- È necessario configurare le LIF di intercluster.
- NTP deve essere configurato.
- Il cluster deve eseguire ONTAP 9.9.1.

### A proposito di questa attività

Non è possibile proteggere nuovi volumi o LUN sul cloud per le seguenti configurazioni di cluster:



- Il cluster non può trovarsi in un ambiente MetroCluster.
- SVM-DR non supportato.
- Impossibile eseguire il backup di FlexGroups utilizzando Cloud Backup.

#### Fasi

1. Quando si effettua il provisioning di un volume o di un LUN, nella pagina **Protection** di System Manager, selezionare la casella di controllo **Enable SnapMirror (Local or Remote)** (attiva SnapMirror (locale o remoto)\*).
2. Selezionare il tipo di criterio Cloud Backup.
3. Se il backup cloud non è attivato, selezionare **Enable Cloud Backup Service** (attiva backup cloud).

## Proteggere i volumi o le LUN esistenti nel cloud

È possibile stabilire una relazione di protezione di SnapMirror per i volumi e le LUN esistenti.

#### Fasi

1. Selezionare un volume o un LUN esistente e fare clic su **Protect** (protezione).
2. Nella pagina **Protect Volumes**, specificare **Backup using Cloud Backup Service** per il criterio di protezione.
3. Fare clic su **Protect** (protezione).
4. Nella pagina **protezione**, selezionare la casella di controllo **attiva SnapMirror (locale o remoto)**.
5. Selezionare **Enable Cloud Backup Service** (attiva protocollo).

## Ripristinare i dati dai file di backup

È possibile eseguire operazioni di gestione del backup, come il ripristino dei dati, l'aggiornamento delle relazioni e l'eliminazione delle relazioni, solo quando si utilizza l'interfaccia BlueXP. Fare riferimento a. ["Ripristino dei dati dai file di backup"](#) per ulteriori informazioni.

## 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.