# Amministrazione del cluster

ONTAP 9

NetApp
April 24, 2024

# Sommario

# Amministrazione del cluster

## Gestione del cluster con System Manager

### Panoramica sull'amministrazione con System Manager

System Manager è un'interfaccia di gestione grafica basata su HTML5 che consente di utilizzare un browser Web per gestire i sistemi di storage e gli oggetti di storage (come dischi, volumi e Tier di storage) ed eseguire attività di gestione comuni relative ai sistemi di storage.

Le procedure descritte in questa sezione consentono di gestire il cluster con Gestione di sistema in ONTAP 9.7 e versioni successive.

- System Manager è incluso nel software ONTAP come servizio Web, abilitato per impostazione predefinita e accessibile tramite un browser.
- Il nome di Gestore di sistema è stato modificato a partire da ONTAP 9.6. In ONTAP 9.5 e nelle versioni precedenti era chiamato Gestore di sistema di OnCommand. A partire da ONTAP 9.6 e versioni successive, si chiama Gestore di sistema.
- Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. "System Manager Classic (ONTAP da 9.0 a 9.7)"

Utilizzando la dashboard di System Manager, è possibile visualizzare informazioni immediate su avvisi e notifiche importanti, l'efficienza e la capacità dei livelli e dei volumi di storage, i nodi disponibili in un cluster, lo stato dei nodi in una coppia ha, le applicazioni e gli oggetti più attivi, e le metriche delle performance di un cluster o di un nodo.

System Manager consente di eseguire numerose attività comuni, ad esempio:

- Creare un cluster, configurare una rete e impostare i dettagli di supporto per il cluster.
- Configurare e gestire oggetti storage, come dischi, Tier locali, volumi, qtree, e quote.
- Configurare protocolli, come SMB e NFS, ed eseguire il provisioning della condivisione dei file.
- Configurare protocolli come FC, FCoE, NVMe e iSCSI per l'accesso a blocchi.
- Creare e configurare componenti di rete, come subnet, domini di broadcast, interfacce di gestione e dati e gruppi di interfacce.
- Impostare e gestire le relazioni di mirroring e vaulting.
- Eseguire operazioni di gestione del cluster, dei nodi di storage e delle macchine virtuali di storage (VM di storage).
- Creare e configurare le VM di storage, gestire gli oggetti storage associati alle VM di storage e gestire i servizi di VM di storage.
- Monitorare e gestire le configurazioni ad alta disponibilità (ha) in un cluster.
- Configurare i service processor per accedere, gestire, monitorare e amministrare il nodo in remoto, indipendentemente dallo stato del nodo.

#### Terminologia di System Manager

Per alcune funzionalità delle chiavi ONTAP, System Manager utilizza una terminologia diversa da CLI.

- **Tier locale** – un set di dischi fisici a stato solido o dischi rigidi su cui memorizzare i dati. Potresti conoscere questi come aggregati. Infatti, se si utilizza l'interfaccia CLI di ONTAP, si vedrà comunque il termine *aggregate* utilizzato per rappresentare un Tier locale.
- **Tier cloud** – storage nel cloud utilizzato da ONTAP quando si desidera avere alcuni dati off-premise per uno dei diversi motivi. Se stai pensando alla parte cloud di un FabricPool, l'hai già capito. E se utilizzi un sistema StorageGRID, il tuo cloud potrebbe non essere off-premise. (Un'esperienza on-premise simile al cloud si chiama *cloud privato*).
- **Storage VM** – una macchina virtuale in esecuzione in ONTAP che fornisce servizi di storage e dati ai client. Potresti sapere che si tratta di un *SVM* o di un *vserver*.
- **Interfaccia di rete** - Indirizzo e proprietà assegnati a una porta di rete fisica. Questo potrebbe essere un'interfaccia logica (LIF)_.
- **Pause** - azione che interrompe le operazioni. Prima di ONTAP 9.8, in altre versioni di Gestore di sistema potrebbe essere stato fatto riferimento a *quiesce*.

## Utilizzare System Manager per accedere a un cluster

Se si preferisce utilizzare un'interfaccia grafica invece dell'interfaccia della riga di comando (CLI) per accedere e gestire un cluster, è possibile farlo utilizzando Gestione di sistema, che è incluso in ONTAP come servizio Web, è attivato per impostazione predefinita ed è accessibile tramite un browser.

> A partire da ONTAP 9.12.1, System Manager è completamente integrato con BlueXP.
>
> Con BlueXP, puoi gestire la tua infrastruttura multicloud ibrida da un singolo piano di controllo mantenendo la familiare dashboard di System Manager.
>
> Vedere "Integrazione di System Manager con BlueXP".

#### A proposito di questa attività

È possibile utilizzare un'interfaccia di rete per la gestione del cluster (LIF) o un'interfaccia di rete per la gestione dei nodi (LIF) per accedere a System Manager. Per un accesso ininterrotto a System Manager, è necessario utilizzare un'interfaccia di rete per la gestione del cluster (LIF).

#### Prima di iniziare

- È necessario disporre di un account utente del cluster configurato con il ruolo "admin" e i tipi di applicazione "http" e "console".
- È necessario abilitare i cookie e i dati del sito nel browser.

#### Fasi

1. Puntare il browser Web sull'indirizzo IP dell'interfaccia di rete per la gestione del cluster:
   - Se si utilizza IPv4: **`https://`*`cluster-mgmt-LIF`***
   - Se si utilizza IPv6: **`https://[`*`cluster-mgmt-LIF`*`]`**

     > Solo HTTPS è supportato per l'accesso tramite browser di System Manager.

Se il cluster utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile riconoscere il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) sul cluster per l'autenticazione del server.

2. **Opzionale:** se è stato configurato un banner di accesso mediante l'interfaccia CLI, leggere il messaggio visualizzato nella finestra di dialogo **Avviso** e scegliere l'opzione desiderata per procedere.

   Questa opzione non è supportata nei sistemi in cui è attivata l'autenticazione SAML (Security Assertion Markup Language).

   - Se non si desidera continuare, fare clic su **Annulla** e chiudere il browser.
   - Se si desidera continuare, fare clic su **OK** per accedere alla pagina di accesso di System Manager.
3. Accedere a System Manager utilizzando le credenziali di amministratore del cluster.

   > A partire da ONTAP 9.11.1, quando si accede a Gestore di sistema, è possibile specificare le impostazioni internazionali. Le impostazioni internazionali specificano alcune impostazioni di localizzazione, ad esempio lingua, valuta, formato data e ora e impostazioni simili. Per ONTAP 9.10.1 e versioni precedenti, le impostazioni internazionali di Gestione sistema vengono rilevate dal browser. Per modificare le impostazioni internazionali di System Manager, è necessario modificare le impostazioni internazionali del browser.

4. **Opzionale**: A partire da ONTAP 9.12.1, è possibile specificare le proprie preferenze per l'aspetto di Gestore di sistema:
   a. Nell'angolo in alto a destra di System Manager, fare clic su per gestire le opzioni utente.
   b. Posizionare l'interruttore a levetta **System Theme** (tema sistema) in base alle proprie preferenze:

| Alternare la posizione | Impostazione dell'aspetto |
|---|---|
| (sinistra) | Tema chiaro (sfondo chiaro con testo scuro) |
| Sistema operativo (centrale) | Per impostazione predefinita, viene utilizzata la preferenza per il tema impostata per le applicazioni del sistema operativo (di solito l'impostazione del tema per il browser utilizzato per accedere a System Manager). |
| (destra) | Tema scuro (sfondo scuro con testo chiaro) |

**Informazioni correlate**

"Gestione dell'accesso ai servizi Web"

"Accesso ai file di log, core dump e MIB di un nodo mediante un browser Web"

## Abilitare le nuove funzioni aggiungendo le chiavi di licenza

Nelle versioni precedenti a ONTAP 9.10.1, le funzioni di ONTAP sono abilitate con chiavi di licenza e le funzioni di ONTAP 9.10.1 e versioni successive sono abilitate con un file di licenza NetApp. È possibile aggiungere chiavi di licenza e file di licenza NetApp utilizzando Gestione sistema.

A partire da ONTAP 9.10.1, si utilizza Gestione di sistema per installare un file di licenza NetApp per abilitare più funzionalità con licenza contemporaneamente. L'utilizzo di un file di licenza NetApp semplifica l'installazione delle licenze, in quanto non è più necessario aggiungere chiavi di licenza per funzionalità separate. È possibile scaricare il file di licenza NetApp dal sito di supporto NetApp.

Se si dispone già di chiavi di licenza per alcune funzioni e si sta eseguendo l'aggiornamento a ONTAP 9.10.1, è possibile continuare a utilizzare tali chiavi di licenza.

**Fasi**

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **licenze**, selezionare →.
3. Selezionare **Sfoglia**. Scegliere il file di licenza NetApp scaricato.
4. Se si desidera aggiungere chiavi di licenza, selezionare **Usa chiavi di licenza di 28 caratteri** e immettere le chiavi.

## Scaricare una configurazione del cluster

A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per scaricare la configurazione di un cluster.

**Fasi**

1. Fare clic su **Cluster > Overview** (Cluster > Panoramica).
2. Fare clic su 

per visualizzare il menu a discesa.
3. Selezionare **Download Configuration** (Scarica configurazione).
4. Selezionare le coppie ha, quindi fare clic su **Download**.

   La configurazione viene scaricata come foglio di calcolo Excel.

   - Il primo foglio contiene i dettagli del cluster.
   - Gli altri fogli contengono i dettagli del nodo.

## Assegnare tag a un cluster

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per assegnare tag a un cluster e identificare gli oggetti appartenenti a una categoria, ad esempio progetti o centri di costo.

**A proposito di questa attività**

È possibile assegnare un tag a un cluster. Innanzitutto, è necessario definire e aggiungere il tag. Quindi, è anche possibile modificare o eliminare il tag.

È possibile aggiungere tag durante la creazione di un cluster o aggiungerli in un secondo momento.

È possibile definire un tag specificando una chiave e associando un valore utilizzando il formato "`key:value'". Ad esempio: "dept:engineering" o "`location:san-jose'".

Quando si creano tag, è necessario tenere in considerazione quanto segue:

- Le chiavi hanno una lunghezza minima di un carattere e non possono essere nulle. I valori possono essere nulli.
- Una chiave può essere associata a più valori separando i valori con una virgola, ad esempio, “location:san-jose,toronto”
- I tag possono essere utilizzati per più risorse.
- I tasti devono iniziare con una lettera minuscola.

**Fasi**

Per gestire i tag, procedere come segue:

1. In System Manager, fare clic su **Cluster** per visualizzare la pagina di panoramica.

   I tag sono elencati nella sezione **Tag**.

2. Fare clic su **Gestisci tag** per modificare i tag esistenti o aggiungerne di nuovi.

   È possibile aggiungere, modificare o eliminare i tag.

| Per eseguire questa azione… | Eseguire questa procedura… |
|---|---|
| Aggiungere un tag | a. Fare clic su **Aggiungi tag**.<br>b. Specificare una chiave e il suo valore o i suoi valori (separare più valori con virgole).<br>c. Fare clic su **Save** (Salva). |
| Modificare un tag | a. Modificare il contenuto nei campi **chiave** e **valori (facoltativo)**.<br>b. Fare clic su **Save** (Salva). |
| Eliminare un tag | a. Fare clic su accanto al tag che si desidera eliminare. |

## Visualizzare e inviare i casi di supporto

A partire da ONTAP 9.9.1, è possibile visualizzare i casi di supporto da Active IQ associati al cluster. È inoltre possibile copiare i dettagli del cluster necessari per inviare un nuovo caso di supporto sul sito del supporto NetApp. A partire da ONTAP 9.10.1, è possibile attivare la registrazione telemetrica, che aiuta il personale di supporto a risolvere i problemi.

> Per ricevere avvisi sugli aggiornamenti del firmware, è necessario essere registrati presso Active IQ Unified Manager. Fare riferimento a. "Risorse di documentazione Active IQ Unified Manager".

**Fasi**

1. In System Manager, selezionare **Support**.

   Viene visualizzato un elenco di casi di supporto aperti associati a questo cluster.

2. Fare clic sui seguenti collegamenti per eseguire le procedure:
    - **Numero del caso**: Visualizza i dettagli del caso.
    - **Vai al sito del supporto NetApp**: Vai alla pagina **My AutoSupport** del sito del supporto NetApp per visualizzare gli articoli della Knowledge base o inviare un nuovo caso di supporto.
    - **Visualizza i miei casi**: Accedere alla pagina **i miei casi** sul sito del supporto NetApp.
    - **Visualizza dettagli cluster**: Consente di visualizzare e copiare le informazioni necessarie per l'invio di un nuovo caso.

#### Abilitare la registrazione di telemetria

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per attivare la registrazione della telemetria. Quando è consentita la registrazione della telemetria, ai messaggi registrati da System Manager viene assegnato un identificatore di telemetria specifico che indica l'esatto processo che ha attivato il messaggio. Tutti i messaggi emessi relativi a tale processo hanno lo stesso identificativo, che consiste nel nome del flusso di lavoro operativo e in un numero (ad esempio "add-volume-1941290").

In caso di problemi di performance, è possibile attivare la registrazione della telemetria, che consente al personale di supporto di identificare più facilmente il processo specifico per il quale è stato emesso un messaggio. Quando si aggiungono identificatori di telemetria ai messaggi, il file di registro viene ingrandito solo leggermente.

**Fasi**

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **UI Settings** (Impostazioni interfaccia utente), fare clic sulla casella di controllo **Allow Telemetry logging** (Consenti registrazione telemetria).

## Gestire il limite massimo di capacità di una VM di storage in System Manager

A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare un limite massimo di capacità per una VM di storage e impostare una soglia per attivare avvisi quando lo storage utilizzato raggiunge una determinata percentuale della capacità massima.

#### Abilitare un limite massimo di capacità per una VM di storage

A partire da ONTAP 9.13.1, è possibile specificare la capacità massima che può essere allocata per tutti i volumi in una VM di storage. È possibile abilitare la capacità massima quando si aggiunge una VM di storage o quando si modifica una VM di storage esistente.

**Fasi**

1. Selezionare **Storage** > **Storage VM**.
2. Eseguire una delle seguenti operazioni:
    - Per aggiungere una VM di storage, fare clic su + Add .
    - Per modificare una VM di storage, fare clic su ⋮ Accanto al nome della VM di storage, quindi fare clic su **Edit** (Modifica).
3. Immettere o modificare le impostazioni per la VM di storage, quindi selezionare la casella di controllo "Enable maximum Capacity limit" (Abilita limite massimo di capacità).

4. Specificare la dimensione massima della capacità.
5. Specificare la percentuale della capacità massima che si desidera utilizzare come soglia per attivare gli avvisi.
6. Fare clic su **Save** (Salva).

#### Modificare il limite massimo di capacità di una VM di storage

A partire da ONTAP 9.13.1, è possibile modificare il limite di capacità massima di una VM di storage esistente, se è stato attivato il limite massimo di capacità già.

**Fasi**

1. Selezionare **Storage** > **Storage VM**.
2. Fare clic su ⋮ Accanto al nome della VM di storage, quindi fare clic su **Edit** (Modifica).

   La casella di controllo "Enable maximum Capacity limit" (Abilita limite massimo di capacità) è già selezionata.

3. Eseguire una delle seguenti operazioni:

| Azione | Fasi |
|---|---|
| Disattivare il limite di capacità massima | 1. Deselezionare la casella di controllo.<br>2. Fare clic su **Save** (Salva). |
| Modificare il limite di capacità massima | 1. Specificare la nuova dimensione massima della capacità. Non è possibile specificare una dimensione inferiore allo spazio già allocato nella VM di storage.<br>2. Specificare la nuova percentuale della capacità massima che si desidera utilizzare come soglia per attivare gli avvisi.<br>3. Fare clic su **Save** (Salva). |

**Informazioni correlate**

- "Visualizzare il limite massimo di capacità di una VM di storage"
- "Misurazioni della capacità in System Manager"
- "Gestire i limiti di capacità SVM utilizzando l'interfaccia CLI di ONTAP"

## Monitorare la capacità in System Manager

Con System Manager, è possibile monitorare la quantità di capacità di storage utilizzata e la quantità ancora disponibile per un cluster, un Tier locale o una VM di storage.

Con ogni versione di ONTAP, System Manager fornisce informazioni di monitoraggio della capacità più affidabili:

- A partire da ONTAP 9.10.1, System Manager consente di visualizzare i dati storici sulla capacità del cluster e le proiezioni relative alla quantità di capacità che verrà utilizzata o disponibile in futuro. È inoltre possibile monitorare la capacità dei volumi e dei Tier locali.
- A partire da ONTAP 9.12.1, System Manager visualizza la quantità di capacità impegnata per un Tier

locale.

- A partire da ONTAP 9.13.1, è possibile attivare un limite massimo di capacità per una VM di storage e impostare una soglia per attivare avvisi quando lo storage utilizzato raggiunge una determinata percentuale della capacità massima.

> Le misurazioni della capacità utilizzata vengono visualizzate in modo diverso a seconda della versione di ONTAP in uso. Scopri di più in "Misurazioni della capacità in System Manager".

### Visualizzare la capacità di un cluster

È possibile visualizzare le misurazioni della capacità di un cluster nella dashboard di System Manager.

#### Prima di iniziare

Per visualizzare i dati relativi alla capacità nel cloud, è necessario disporre di un account presso Active IQ Digital Advisor ed essere connessi.

#### Fasi

1. In System Manager, fare clic su **Dashboard**.
2. Nella sezione **capacità**, è possibile visualizzare quanto segue:
   - Capacità totale utilizzata del cluster
   - Capacità totale disponibile del cluster
   - Percentuali di capacità utilizzata e disponibile.
   - Rapporto di riduzione dei dati.
   - Quantità di capacità utilizzata nel cloud.
   - Cronologia dell'utilizzo della capacità.
   - Proiezione dell'utilizzo della capacità

   > In System Manager, le rappresentazioni della capacità non tengono conto delle capacità del Tier storage root (aggregato).

3. Fare clic sul grafico per visualizzare ulteriori dettagli sulla capacità del cluster.

   Le misurazioni della capacità vengono visualizzate in due diagrammi a barre:

   - Il grafico in alto mostra la capacità fisica: La dimensione dello spazio fisico utilizzato, riservato e disponibile.
   - Il grafico in basso mostra la capacità logica: La dimensione dei dati del client, le copie Snapshot e i cloni e lo spazio logico totale utilizzato.

   Sotto i grafici a barre sono riportate le misurazioni per la riduzione dei dati:

   - Rapporto di riduzione dei dati solo per i dati del client (copie Snapshot e cloni non inclusi).
   - Rapporto complessivo di riduzione dei dati.

Per ulteriori informazioni, vedere "Misurazioni della capacità in System Manager".

### Visualizzare la capacità di un Tier locale

È possibile visualizzare i dettagli sulla capacità dei Tier locali. A partire da ONTAP 9.12.1, la vista **capacità** include anche la quantità di capacità impegnata per un Tier locale, consentendo di determinare se è necessario aggiungere capacità al Tier locale per soddisfare la capacità impegnata ed evitare di esaurire lo spazio libero.

#### Fasi

1. Fare clic su **Storage > Tier**.
2. Selezionare il nome del Tier locale.
3. Nella pagina **Panoramica**, nella sezione **capacità**, la capacità viene visualizzata in un grafico a barre con tre misurazioni:
   - Capacità utilizzata e riservata
   - Capacità disponibile
   - Capacità impegnata (a partire da ONTAP 9.12.1)
4. Fare clic sul grafico per visualizzare i dettagli sulla capacità del Tier locale.

   Le misurazioni della capacità vengono visualizzate in due diagrammi a barre:

   - Il grafico a barre superiore visualizza la capacità fisica: La dimensione dello spazio fisico utilizzato, riservato e disponibile.
   - Il grafico a barre inferiore mostra la capacità logica: La dimensione dei dati del client, le copie Snapshot e i cloni e il totale dello spazio logico utilizzato.

   Sotto i grafici a barre sono riportati i rapporti di misurazione per la riduzione dei dati:

   - Rapporto di riduzione dei dati solo per i dati del client (copie Snapshot e cloni non inclusi).
   - Rapporto complessivo di riduzione dei dati.

Per ulteriori informazioni, vedere "Misurazioni della capacità in System Manager".

#### Azioni facoltative

- Se la capacità impegnata è superiore alla capacità del Tier locale, è possibile aggiungere capacità al Tier locale prima che esaurisca lo spazio libero. Vedere "Aggiunta di capacità a un Tier locale (aggiunta di dischi a un aggregato)".
- È inoltre possibile visualizzare lo storage utilizzato da volumi specifici nel Tier locale selezionando la scheda **Volumes**.

### Visualizzare la capacità dei volumi in una VM di storage

È possibile visualizzare la quantità di storage utilizzata dai volumi in una VM di storage e la quantità di capacità ancora disponibile. La misurazione totale dello storage utilizzato e disponibile viene chiamata "capacità su più volumi".

#### Fasi

1. Selezionare **Storage** > **Storage VM**.
2. Fare clic sul nome della VM di storage.
3. Scorrere fino alla sezione **capacità**, che mostra un grafico a barre con le seguenti misurazioni:

- **Fisico utilizzato**: Somma dello storage fisico utilizzato in tutti i volumi di questa VM di storage.
- **Disponibile**: Somma della capacità disponibile in tutti i volumi di questa VM di storage.
- **Logica utilizzata**: Somma dello storage logico utilizzato in tutti i volumi di questa VM di storage.

Per ulteriori informazioni sulle misurazioni, vedere "Misurazioni della capacità in System Manager".

#### Visualizzare il limite massimo di capacità di una VM di storage

A partire da ONTAP 9.13.1, è possibile visualizzare il limite massimo di capacità di una VM di storage.

**Prima di iniziare**

È necessario "Abilitare il limite massimo di capacità di una VM di storage" prima di visualizzarlo.

**Fasi**

1. Selezionare **Storage** > **Storage VM**.

   È possibile visualizzare le misurazioni della capacità massima in due modi:

   - Nella riga relativa alla VM di storage, visualizzare la colonna **capacità massima** che contiene un grafico a barre che mostra la capacità utilizzata, la capacità disponibile e la capacità massima.
   - Fare clic sul nome della VM di storage. Nella scheda **Panoramica**, scorrere per visualizzare i valori di soglia di avviso relativi alla capacità massima, alla capacità allocata e alla capacità nella colonna di sinistra.

**Informazioni correlate**

- "Modificare il limite massimo di capacità di una VM di storage"
- "Misurazioni della capacità in System Manager"

## Visualizzare le configurazioni hardware per determinare i problemi

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per visualizzare la configurazione dell'hardware sulla rete e determinare lo stato dei sistemi hardware e le configurazioni di cablaggio.

**Fasi**

Per visualizzare le configurazioni hardware, attenersi alla seguente procedura:

1. In System Manager, selezionare **Cluster > hardware**.
2. Passare il mouse sui componenti per visualizzare lo stato e altri dettagli.

   È possibile visualizzare diversi tipi di informazioni:

   - Informazioni sui controller
   - Informazioni sugli shelf di dischi
   - Informazioni sugli switch storage
3. A partire da ONTAP 9.12.1, è possibile visualizzare le informazioni sul cablaggio in Gestione sistema. Fare clic sulla casella di controllo **Mostra cavi** per visualizzare il cablaggio, quindi passare il mouse su un cavo per visualizzare le informazioni di connettività.

- Informazioni sul cablaggio

**Informazioni sui controller**

È possibile visualizzare quanto segue:

**Nodi**

**Nodi**:

- È possibile visualizzare la vista anteriore e posteriore.
- Per i modelli con shelf di dischi interno, è anche possibile visualizzare il layout del disco nella vista frontale.
- È possibile visualizzare le seguenti piattaforme:

| Piattaforma | Supportato in Gestione di sistema nella versione ONTAP… | | | | | | |
|---|---|---|---|---|---|---|---|
| | 9.14.1 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9.8 (solo modalità di anteprima) |
| AFF A150 | Sì | Sì | | | | | |
| AFF A220 | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| AFF A250 | Sì | Sì | Sì | Sì | Sì | Sì | |
| AFF A300 | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| AFF A320 | Sì | Sì | Sì | Sì | Sì | Sì | |
| AFF A400 | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| AFF A700 | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| AFF A700 | Sì | Sì | Sì | Sì | Sì | Sì | |
| AFF A800 | Sì | Sì | Sì | Sì | Sì | Sì | |
| AFF C190 | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| AFF C250 | Sì | Sì | Sì e#42; | Sì e#42; | Sì e#42; | | |
| AFF C400 | Sì | Sì | Sì e#42; | Sì e#42; | Sì e#42; | | |
| AFF C800 | Sì | Sì | Sì e#42; | Sì e#42; | Sì e#42; | | |
| ASA A150 | Sì | Sì | | | | | |
| ASA A250 | Sì | Sì | | | | | |
| ASA A400 | Sì | Sì | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ASA A800 | Sì | Sì | | | | | |
| ASA A900 | Sì | Sì | | | | | |
| ASA C250 | Sì | Sì | | | | | |
| ASA C400 | Sì | Sì | | | | | |
| ASA C800 | Sì | Sì | | | | | |
| FAS500f | Sì | Sì | Sì | Sì | Sì | Sì | |
| FAS2720 | Sì | Sì | Sì | Sì | | | |
| FAS2750 | Sì | Sì | Sì | Sì | | | |
| FAS8300 | Sì | Sì | Sì | Sì | | | |
| FAS8700 | Sì | Sì | Sì | Sì | | | |
| FAS9000 | Sì | Sì | Sì | Sì | | | |
| FAS9500 | Sì | Sì | Sì | Sì | | | |

**Porte**

**Porte**:

- Se la porta non è disponibile, viene evidenziata in rosso.
- Quando si passa il puntatore del mouse sulla porta, è possibile visualizzare lo stato di una porta e altri dettagli.
- Non è possibile visualizzare le porte della console.

  **Note**:

  - Per ONTAP 9.10.1 e versioni precedenti, le porte SAS vengono evidenziate in rosso quando sono disattivate.
  - A partire da ONTAP 9.11.1, le porte SAS verranno evidenziate in rosso solo se si trovano in uno stato di errore o se una porta cablata utilizzata diventa offline. Le porte vengono visualizzate in bianco se non sono in linea e non sono cablate.

**FRU**

**FRU**:

Le informazioni sulle FRU vengono visualizzate solo quando lo stato di una FRU non è ottimale.

- PSU guasti nei nodi o nello chassis.

- Temperature elevate rilevate nei nodi.
- Ventole guaste sui nodi o sullo chassis.

**Schede adattatore**

**Schede adattatore**:

- Se sono state inserite schede esterne, negli slot vengono visualizzati i campi relativi ai numeri di parte definiti.
- Le porte vengono visualizzate sulle schede.
- Per una scheda supportata, è possibile visualizzare le immagini di tale scheda. Se la scheda non è presente nell'elenco dei codici prodotto supportati, viene visualizzata una grafica generica.

### Informazioni sugli shelf di dischi

È possibile visualizzare quanto segue:

**Shelf di dischi**

**Shelf di dischi**:

- È possibile visualizzare le viste anteriore e posteriore.
- È possibile visualizzare i seguenti modelli di shelf di dischi:

| Se il sistema è in esecuzione… | Quindi, è possibile utilizzare System Manager per visualizzare… |
|---|---|
| ONTAP 9.9.1 e versioni successive | Tutti gli shelf che *non* sono stati designati come "fine del servizio" o "fine della disponibilità" |
| ONTAP 9.8 | DS4243, DS486, DS212C, DS2246, DS224C, E NS224 |

**Porte per shelf**

**Porte shelf**:

- È possibile visualizzare lo stato della porta.
- Se la porta è collegata, è possibile visualizzare le informazioni sulla porta remota.

**FRU dello shelf**

**FRU shelf**:

- Vengono visualizzate le informazioni relative al guasto della PSU.

### Informazioni sugli switch storage

È possibile visualizzare quanto segue:

**Switch storage**

**Switch storage**:

- Il display mostra gli switch che fungono da switch storage utilizzati per collegare gli shelf ai nodi.
- A partire da ONTAP 9.9.1, System Manager visualizza le informazioni relative a uno switch che agisce sia come switch storage che come cluster, che possono essere condivise anche tra i nodi di una coppia ha.
- Vengono visualizzate le seguenti informazioni:
  - Nome dello switch
  - Indirizzo IP
  - Numero di serie
  - Versione SNMP
  - Versione del sistema
- È possibile visualizzare i seguenti modelli di switch storage:

| Se il sistema è in esecuzione… | Quindi, è possibile utilizzare System Manager per visualizzare… |
|---|---|
| ONTAP 9.11.1 o versione successiva | Cisco Nexus 3232C<br>Cisco Nexus 9336C-FX2<br>Mellanox SN2100 |
| ONTAP 9.9.1 e 9.10.1 | Cisco Nexus 3232C<br>Cisco Nexus 9336C-FX2 |
| ONTAP 9.8 | Cisco Nexus 3232C |

**Porte dello switch di storage**

**Porte dello switch di storage**

- Vengono visualizzate le seguenti informazioni:
  - Nome dell'identità
  - Indice di identità
  - Stato
  - Connessione remota
  - Altri dettagli

### Informazioni sul cablaggio

A partire da ONTAP 9.12.1, è possibile visualizzare le seguenti informazioni sul cablaggio:

- **Cablaggio** tra controller, switch e shelf quando non vengono utilizzati bridge di storage
- **Connettività** che mostra gli ID e gli indirizzi MAC delle porte su entrambe le estremità del cavo

## Gestire i nodi con System Manager

Con System Manager è possibile aggiungere nodi a un cluster e rinominarli. È inoltre possibile riavviare, sostituire e restituire i nodi.

### Aggiungere nodi a un cluster

È possibile aumentare le dimensioni e le funzionalità del cluster aggiungendo nuovi nodi.

#### Prima di iniziare

I nuovi nodi dovrebbero essere già stati cablati al cluster.

#### A proposito di questa attività

Esistono procedure separate per l'utilizzo di Gestione sistema in ONTAP 9,7 o ONTAP 9,8 e versioni successive.

**Procedura ONTAP 9,8 e successive**

**Aggiunta di nodi a un cluster con Gestione sistema (ONTAP 9,8 e versioni successive)**

**Fasi**

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).

   I nuovi controller vengono visualizzati come nodi collegati alla rete del cluster ma non nel cluster.

2. Selezionare **Aggiungi**.
   - I nodi vengono aggiunti al cluster.
   - Lo storage viene allocato implicitamente.

**Procedura ONTAP 9,7**

**Aggiunta di nodi a un cluster con Gestione sistema (ONTAP 9,7)**

**Fasi**

1. Selezionare **(ritorna alla versione classica)**.
2. Selezionare **configurazioni > espansione cluster**.

   System Manager rileva automaticamente i nuovi nodi.

3. Selezionare **passa alla nuova esperienza**.
4. Selezionare **Cluster > Overview** per visualizzare i nuovi nodi.

### Arrestare, riavviare o modificare il Service Processor

Al riavvio o all'arresto di un nodo, il partner ha esegue automaticamente un takeover.

#### Fasi

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).
2. In **nodi**, selezionare ⋮.
3. Selezionare il nodo, quindi selezionare **Arresta il sistema**, **Riavvia** o **Modifica Service Processor**.

Se un nodo è stato riavviato ed è in attesa di giveback, è disponibile anche l'opzione **Giveback**.

Se si seleziona **Modifica Service Processor**, è possibile scegliere **Manuale** per immettere l'indirizzo IP, la maschera di sottorete e il gateway oppure è possibile scegliere **DHCP** per la configurazione dinamica dell'host.

#### Rinomina nodi

A partire da ONTAP 9.14.1, è possibile rinominare un nodo dalla pagina di panoramica del cluster.

**Fasi**

1. Selezionare **Cluster**. Viene visualizzata la pagina di panoramica del cluster.
2. Scorri verso il basso fino alla sezione **nodi**.
3. Accanto al nodo che si desidera rinominare, selezionare ⋮ E selezionare **Rinomina**.
4. Modificare il nome del nodo, quindi selezionare **Rinomina**.

# Gestione delle licenze

## Panoramica delle licenze ONTAP

Una licenza è un record di una o più autorizzazioni software. A partire da ONTAP 9.10.1, tutte le licenze vengono fornite come file di licenza NetApp (NLF), che è un singolo file che abilita più funzioni. A partire da maggio 2023, tutti i sistemi AFF (sia A-series che C-series) e i sistemi FAS vengono venduti con la suite software ONTAP One o la suite software ONTAP base; a partire da giugno 2023, tutti i sistemi ASA vengono venduti con ONTAP One per SAN. Ogni suite software viene fornita come un unico NLF, sostituendo i pacchetti NLF separati introdotti per la prima volta in ONTAP 9.10.1.

#### Licenze incluse con ONTAP ONE

ONTAP One contiene tutte le funzionalità disponibili con licenza. Contiene una combinazione dei contenuti del precedente bundle Core, del bundle Data Protection, del bundle Security and Compliance, del bundle Hybrid Cloud e del bundle Encryption, come mostrato nella tabella. La crittografia non è disponibile nei paesi con restrizioni.

| Nome del bundle precedente | Chiavi ONTAP incluse |
|---|---|
| Bundle principale | FlexClone |
| | SnapRestore |
| | NFS, SMB, S3 |
| | FC, iSCSI |
| | NVME-of |
| Bundle di sicurezza e conformità | Protezione ransomware autonoma |
| | MTKM |
| | SnapLock |

| | |
|---|---|
| Bundle di data Protection | SnapMirror (asincrono, sincrono, business continuity) |
| | SnapCenter |
| | S3 SnapMirror per destinazioni NetApp |
| Bundle cloud ibrido | SnapMirror Cloud |
| | S3 SnapMirror per destinazioni non NetApp |
| Bundle di crittografia | Crittografia dei volumi NetApp |
| | Modulo Trusted Platform |

### Licenze non incluse in ONTAP ONE

ONTAP One non include i servizi erogati nel cloud di NetApp, come ad esempio:

- Tiering BlueXP
- Cloud Insights
- Backup BlueXP
- Governance dei dati

### ONTAP uno per i sistemi esistenti

Se si dispone di sistemi esistenti che sono attualmente supportati da NetApp ma non sono stati aggiornati a ONTAP One, le licenze esistenti su tali sistemi sono ancora valide e continuano a funzionare come previsto. Ad esempio, se la licenza SnapMirror è già installata su sistemi esistenti, non è necessario eseguire l'aggiornamento a ONTAP One per ottenere una nuova licenza SnapMirror. Tuttavia, se non si dispone di una licenza SnapMirror installata su un sistema esistente, l'unico modo per ottenere tale licenza è eseguire l'aggiornamento a ONTAP One a un costo aggiuntivo.

A partire da giugno 2023, è possibile utilizzare anche i sistemi ONTAP che utilizzano chiavi di licenza di 28 caratteri "Eseguire l'aggiornamento al bundle di compatibilità ONTAP One o ONTAP base".

### Licenze incluse con ONTAP base

ONTAP base è una suite software opzionale alternativa a ONTAP One per i sistemi ONTAP. È per casi d'utilizzo specifici in cui non sono richieste tecnologie di data Protection come SnapMirror e SnapCenter, nonché funzionalità di sicurezza come il ransomware autonomo, come i sistemi non di produzione per ambienti di test o sviluppo dedicati. Non è possibile aggiungere licenze aggiuntive alla ONTAP base. Per licenze aggiuntive, come SnapMirror, è necessario eseguire l'aggiornamento a ONTAP One.

| Nome del bundle precedente | Chiavi ONTAP incluse |
|---|---|
| Bundle principale | FlexClone |
| | SnapRestore |
| | NFS, SMB, S3 |
| | FC, iSCSI |
| | NVME-of |

| | |
|---|---|
| Bundle di crittografia | Crittografia dei volumi NetApp |
| | Modulo Trusted Platform |

#### Licenze incluse in ONTAP One per SAN

ONTAP One per SAN è disponibile per i sistemi ASA serie A e C-series. Questa è l'unica suite software disponibile per SAN. ONTAP ONE per SAN contiene le seguenti licenze:

| |
|---|
| Chiavi ONTAP incluse |
| FlexClone |
| SnapRestore |
| FC, iSCSI |
| NVME-of |
| MTKM |
| SnapLock |
| SnapMirror (asincrono, sincrono, business continuity) |
| SnapCenter |
| SnapMirror Cloud |
| Crittografia dei volumi NetApp |
| Modulo Trusted Platform |

#### Altri metodi di distribuzione delle licenze

In ONTAP 8.2 fino a ONTAP 9.9.1, le chiavi di licenza vengono fornite sotto forma di stringhe di 28 caratteri ed è disponibile una chiave per funzione ONTAP. Utilizzare l'interfaccia CLI di ONTAP per installare le chiavi di licenza se si utilizza ONTAP 8,2 tramite ONTAP 9,9.1.

> ONTAP 9.10.1 supporta l'installazione di chiavi di licenza di 28 caratteri utilizzando Gestione di sistema o CLI. Tuttavia, se è installata una licenza NLF per una funzione, non è possibile installare una chiave di licenza di 28 caratteri sul file di licenza NetApp per la stessa funzione. Per informazioni sull'installazione di NLF o chiavi di licenza con System Manager, vedere "Installare le licenze ONTAP".

#### Informazioni correlate

"Come ottenere una licenza ONTAP One quando il sistema dispone già di NLF"

"Come verificare le autorizzazioni software ONTAP e le relative chiavi di licenza utilizzando il sito di assistenza"

"NetApp: Stato del rischio di licenza ONTAP"

## Scaricare i file di licenza NetApp (NLF) dal sito del supporto NetApp

Se il sistema esegue ONTAP 9.10.1 o versione successiva, è possibile aggiornare i file di licenza bundle sui sistemi esistenti scaricando NLF per ONTAP ONE o ONTAP Core dal

sito di supporto NetApp.

> Le licenze SnapMirror Cloud e S3 SnapMirror non sono incluse in ONTAP ONE. Fanno parte del pacchetto di compatibilità ONTAP One, che è possibile ottenere gratuitamente se si dispone di ONTAP One e. "da richiedere separatamente".

**Fasi**

È possibile scaricare i file di licenza di ONTAP ONE per sistemi con pacchetti di file di licenza NetApp esistenti e per sistemi con chiavi di licenza di 28 caratteri che sono stati convertiti in file di licenza NetApp su sistemi che eseguono ONTAP 9.10.1 e versioni successive. A pagamento, puoi anche aggiornare i sistemi da ONTAP base a ONTAP One.

**Aggiornare l'NLF esistente**

1. Contatta il tuo team di vendita NetApp e richiedi il bundle del file di licenza che desideri aggiornare o convertire (ad esempio, da ONTAP base a ONTAP One o bundle core e data Protection in ONTAP One).

   Una volta elaborata la richiesta, l'utente riceverà un'e-mail da netappsw@netapp.com con l'oggetto "notifica della licenza software NetApp per SO# [numero SO]" e l'e-mail includerà un allegato PDF che include il numero di serie della licenza.

2. Accedere a. "Sito di supporto NetApp".
3. Selezionare **sistemi > licenze software**.
4. Dal menu, scegliere **numero di serie**, inserire il numero di serie ricevuto e fare clic su **Nuova ricerca**.
5. Individuare il pacchetto di licenze che si desidera convertire.
6. Fare clic su **Ottieni file di licenza NetApp** per ogni pacchetto di licenze e scaricare i file NLF quando sono disponibili.
7. "Installare" Il file ONTAP ONE.

**Aggiornamento NLF convertito dalla chiave di licenza**

1. Accedere a. "Sito di supporto NetApp".
2. Selezionare **sistemi > licenze software**.
3. Dal menu, scegliere **numero di serie**, inserire il numero di serie del sistema e fare clic su **Nuova ricerca**.
4. Individuare la licenza che si desidera convertire e, nella colonna **idoneità**, fare clic su **Controlla**.
5. In **Check Eligibility Form**, fare clic su **generate Licenses for 9,10.x e versioni successive**.
6. Chiudere il modulo **verifica idoneità**.

   È necessario attendere almeno 2 ore per la generazione delle licenze.

7. Ripetere i passaggi da 1 a 3.
8. Individuare la licenza di ONTAP One, fare clic su **Ottieni file di licenza NetApp** e scegliere il metodo di distribuzione.
9. "Installare" Il file ONTAP ONE.

## Installare le licenze ONTAP

È possibile installare i file di licenza NetApp (NLF) e le chiavi di licenza utilizzando Gestione sistema, il metodo preferito per l'installazione di NLF, oppure utilizzare la CLI di ONTAP per installare le chiavi di licenza. In ONTAP 9.10.1 e versioni successive, le funzioni sono abilitate con un file di licenza NetApp e nelle versioni precedenti a ONTAP 9.10.1, le funzioni ONTAP sono abilitate con chiavi di licenza.

### Fasi

Se lo hai già fatto "File di licenza NetApp scaricati" O chiavi di licenza, puoi usare System Manager o la CLI di ONTAP per installare NLF e chiavi di licenza di 28 caratteri.

**Gestione di sistema - ONTAP 9,8 e versioni successive**

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **licenze**, selezionare →.
3. Selezionare **Sfoglia**. Scegliere il file di licenza NetApp scaricato.
4. Se si desidera aggiungere chiavi di licenza, selezionare **Usa chiavi di licenza di 28 caratteri** e immettere le chiavi.

**Gestore di sistema - ONTAP 9,7 e versioni precedenti**

1. Selezionare **Configurazione > Cluster > licenze**.
2. In **licenze**, selezionare →.
3. Nella finestra **pacchetti**, fare clic su **Aggiungi**.
4. Nella finestra di dialogo **Aggiungi pacchetti di licenza**, fare clic su **Scegli file** per selezionare il file di licenza NetApp scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

**CLI**

1. Aggiungere una o più chiavi di licenza:

   ```
   system license add
   ```

   Nell'esempio seguente vengono installate le licenze dal nodo locale "/mroot/etc/lic_file" se il file esiste in questa posizione:

   ```
   cluster1::> system license add -use-license-file true
   ```

   Nell'esempio seguente viene aggiunto al cluster un elenco di licenze con le chiavi AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBB
   ```

**Informazioni correlate**

"Pagina man per il comando di aggiunta della licenza di sistema".

## Gestire le licenze ONTAP

Puoi utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per visualizzare e gestire le licenze installate nel sistema, inclusa la visualizzazione del numero seriale della licenza, la verifica dello stato di una licenza e la rimozione di una licenza.

### Consente di visualizzare i dettagli di una licenza

**Fasi**

La modalità di visualizzazione dei dettagli di una licenza dipende dalla versione di ONTAP in uso e dall'utilizzo di System Manager o dell'interfaccia a riga di comando di ONTAP.

**Gestione di sistema - ONTAP 9,8 e versioni successive**

1. Per visualizzare i dettagli relativi a una licenza di funzione specifica, selezionare **Cluster > Impostazioni**.
2. In **licenze**, selezionare →.
3. Selezionare **funzioni**.
4. Individuare la funzione concessa in licenza che si desidera visualizzare e selezionare ⌄ per visualizzare i dettagli della licenza.

**Gestore di sistema - ONTAP 9,7 e versioni precedenti**

1. Selezionare **Configurazione > Cluster > licenze**.
2. Nella finestra **Licenses**, eseguire l'azione appropriata:
3. Fare clic sulla scheda **Dettagli**.

**CLI**

1. Visualizzare i dettagli relativi a una licenza installata:

```
system license show
```

### Eliminare una licenza

**Gestione di sistema - ONTAP 9,8 e versioni successive**

1. Per eliminare una licenza, selezionare **Cluster > Impostazioni**.
2. In **licenze**, selezionare →.
3. Selezionare **funzioni**.
4. Selezionare la funzione concessa in licenza che si desidera eliminare e **Elimina chiave legacy**.

**Gestore di sistema - ONTAP 9,7 e versioni precedenti**

1. Selezionare **Configurazione > Cluster > licenze**.
2. Nella finestra **Licenses**, eseguire l'azione appropriata:

| Se si desidera… | Eseguire questa operazione… |
|---|---|
| Eliminare un pacchetto di licenza specifico su un nodo o una licenza master | Fare clic sulla scheda **Dettagli**. |
| Eliminare un pacchetto di licenza specifico in tutti i nodi del cluster | Fare clic sulla scheda **pacchetti**. |

3. Selezionare il pacchetto di licenza software che si desidera eliminare, quindi fare clic su **Delete** (Elimina).

   È possibile eliminare un solo pacchetto di licenza alla volta.

4. Selezionare la casella di controllo di conferma, quindi fare clic su **Elimina**.

**CLI**

1. Eliminare una licenza:

```
system license delete
```

Nell'esempio riportato di seguito viene eliminata una licenza denominata CIFS e il numero di serie 1-81-0000000000000000000123456 dal cluster:

```
cluster1::> system license delete -serial-number 1-81-
0000000000000000000123456 -package CIFS
```

Nell'esempio riportato di seguito vengono eliminate dal cluster tutte le licenze sotto il Core Bundle con licenza installata per il numero di serie 123456789:

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

**Informazioni correlate**

"Comandi CLI di ONTAP per la gestione delle licenze"

"Comandi di ONTAP 9"

## Tipi di licenza e metodo concesso in licenza

La comprensione dei tipi di licenza e del metodo concesso in licenza consente di gestire le licenze in un cluster.

### Tipi di licenza

Un pacchetto può avere uno o più dei seguenti tipi di licenza installati nel cluster. Il `system license show` il comando visualizza il tipo o i tipi di licenza installati per un pacchetto.

- Licenza standard (`license`)

  Una licenza standard è una licenza con blocco a nodo. Viene emesso per un nodo con un numero di serie di sistema specifico (noto anche come *numero di serie del controller*). Una licenza standard è valida solo per il nodo che ha il numero seriale corrispondente.

  L'installazione di una licenza standard bloccata da nodo consente a un nodo di accedere alla funzionalità concessa in licenza. Affinché il cluster utilizzi la funzionalità concessa in licenza, è necessario che almeno un nodo sia concesso in licenza per tale funzionalità. L'utilizzo della funzionalità concessa in licenza su un nodo che non dispone di diritti per tale funzionalità potrebbe essere fuori conformità.

- Licenza del sito (`site`)

  Una licenza di sito non è legata a un numero seriale di sistema specifico. Quando si installa una licenza di sito, tutti i nodi del cluster hanno diritto alla funzionalità concessa in licenza. Il `system license show` il comando visualizza le licenze del sito sotto il numero di serie del cluster.

  Se il cluster dispone di una licenza di sito e si rimuove un nodo dal cluster, il nodo non dispone della licenza di sito e non ha più diritto alla funzionalità concessa in licenza. Se si aggiunge un nodo a un cluster che dispone di una licenza di sito, il nodo avrà automaticamente diritto alla funzionalità concessa dalla licenza di sito.

- Licenza di valutazione (`demo`)

  Una licenza di valutazione è una licenza temporanea che scade dopo un determinato periodo di tempo (indicato da `system license show` comando). Consente di provare alcune funzionalità software senza acquistare alcun diritto. Si tratta di una licenza a livello di cluster e non è legata a un numero seriale specifico di un nodo.

  Se il cluster dispone di una licenza di valutazione per un pacchetto e si rimuove un nodo dal cluster, il nodo non dispone della licenza di valutazione.

### Metodo concesso in licenza

È possibile installare sia una licenza a livello di cluster (il `site` oppure `demo` e una licenza bloccata dal nodo (il `license` digitare) per un pacchetto. Pertanto, un pacchetto installato può avere diversi tipi di licenza nel cluster. Tuttavia, per il cluster, esiste un solo *metodo concesso in licenza* per un pacchetto. Il `licensed method` campo di `system license status show` il comando visualizza i diritti utilizzati per un pacchetto. Il comando determina il metodo concesso in licenza come segue:

- Se un pacchetto ha un solo tipo di licenza installato nel cluster, il tipo di licenza installato è il metodo concesso in licenza.
- Se un pacchetto non dispone di licenze installate nel cluster, il metodo concesso in licenza è `none`.
- Se nel cluster sono installati più tipi di licenza, il metodo concesso in licenza viene determinato nel seguente ordine di priorità del tipo di licenza.-`site`, `license`, e. `demo`.

  Ad esempio:

  - Se si dispone di una licenza per sito, di una licenza standard e di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `site`.
  - Se si dispone di una licenza standard e di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `license`.
  - Se si dispone solo di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `demo`.

## Comandi per la gestione delle licenze

È possibile utilizzare l'interfaccia CLI di ONTAP `system license` comandi per gestire le licenze delle funzioni per il cluster. Si utilizza `system feature-usage` comandi per monitorare l'utilizzo delle funzioni.

Nella tabella seguente sono elencati alcuni dei comandi CLI più comuni per la gestione delle licenze e i collegamenti alle pagine man dei comandi per ulteriori informazioni.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Visualizzare tutti i pacchetti che richiedono licenze e il relativo stato di licenza corrente, inclusi i seguenti:<br>• Il nome del pacchetto<br>• Il metodo concesso in licenza<br>• La data di scadenza, se applicabile | "stato di visualizzazione della licenza di sistema" |
| Visualizzare o rimuovere le licenze scadute o inutilizzate | "pulizia della licenza di sistema" |
| Visualizza il riepilogo dell'utilizzo delle funzionalità nel cluster in base al nodo | "riepilogo delle funzioni del sistema" |
| Visualizzazione dello stato di utilizzo delle funzioni nel cluster per nodo e per settimana | "cronologia degli eventi di utilizzo delle funzioni del sistema" |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizzare lo stato del rischio di licenza per ciascun pacchetto di licenza | "diritti della licenza di sistema-risk show" |

**Informazioni correlate**

"Comandi di ONTAP 9"

"Articolo della Knowledge base: Panoramica sulle licenze di ONTAP 9.10.1 e versioni successive"

"Utilizzare Gestione sistema per installare un file di licenza NetApp"

# Gestione del cluster con la CLI

## Panoramica sull'amministrazione con la CLI

È possibile amministrare i sistemi ONTAP con l'interfaccia a riga di comando (CLI). È possibile utilizzare le interfacce di gestione di ONTAP, accedere al cluster, gestire i nodi e molto altro ancora.

Attenersi alle seguenti procedure nei seguenti casi:

- Vuoi conoscere la gamma di funzionalità di amministratore di ONTAP.
- Si desidera utilizzare la CLI, non System Manager o uno strumento di scripting automatico.

**Informazioni correlate**

Per informazioni dettagliate sulla sintassi e l'utilizzo della CLI, consultarehttp://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html["Riferimento alla pagina di manuale di ONTAP 9"^] documentazione.

## Amministratori di cluster e SVM

### Amministratori di cluster e SVM

Gli amministratori dei cluster amministrano l'intero cluster e le macchine virtuali dello storage (SVM, precedentemente note come Vserver) in esso contenute. Gli amministratori di SVM amministrano solo le proprie SVM di dati.

Gli amministratori dei cluster possono amministrare l'intero cluster e le relative risorse. Possono anche configurare le SVM dei dati e delegare l'amministrazione SVM agli amministratori SVM. Le funzionalità specifiche di cui dispongono gli amministratori dei cluster dipendono dai ruoli di controllo degli accessi. Per impostazione predefinita, un amministratore del cluster con il nome dell'account "admin" o il nome del ruolo dispone di tutte le funzionalità per la gestione del cluster e delle SVM.

Gli amministratori di SVM possono amministrare solo le proprie risorse di storage e di rete SVM, come volumi, protocolli, LIF e servizi. Le funzionalità specifiche di cui dispongono gli amministratori SVM dipendono dai ruoli di controllo degli accessi assegnati dagli amministratori del cluster.

L'interfaccia della riga di comando (CLI) di ONTAP continua a utilizzare il termine *Vserver* nell'output, e. `vserver` poiché il nome di un comando o di un parametro non è stato modificato.

#### Gestire l'accesso a System Manager

È possibile attivare o disattivare l'accesso di un browser Web a System Manager. È inoltre possibile visualizzare il log di System Manager.

È possibile controllare l'accesso di un browser Web a System Manager utilizzando `vserver services web modify -name sysmgr -vserver` *`cluster_name`* `-enabled` [`true`|`false`].

La registrazione di System Manager viene registrata in `/mroot/etc/log/mlog/sysmgr.log` File del nodo che ospita la LIF di gestione del cluster al momento dell'accesso a System Manager. È possibile visualizzare i file di log utilizzando un browser. Il log di Gestione sistema è incluso anche nei messaggi AutoSupport.

#### Che cos'è il server di gestione del cluster

Il server di gestione del cluster, chiamato anche *admin*SVM, è un'implementazione SVM (Storage Virtual Machine) specializzata che presenta il cluster come una singola entità gestibile. Oltre a fungere da dominio amministrativo di livello più elevato, il server di gestione del cluster possiede risorse che non appartengono logicamente a una SVM di dati.

Il server di gestione del cluster è sempre disponibile sul cluster. È possibile accedere al server di gestione del cluster tramite la console o la LIF di gestione del cluster.

In caso di guasto della porta della rete domestica, la LIF di gestione del cluster esegue automaticamente il failover su un altro nodo del cluster. A seconda delle caratteristiche di connettività del protocollo di gestione in uso, il failover potrebbe essere notato o meno. Se si utilizza un protocollo senza connessione (ad esempio, SNMP) o si dispone di una connessione limitata (ad esempio HTTP), non si noterà il failover. Tuttavia, se si utilizza una connessione a lungo termine (ad esempio SSH), sarà necessario riconnettersi al server di gestione del cluster dopo il failover.

Quando si crea un cluster, vengono configurate tutte le caratteristiche della LIF di gestione del cluster, inclusi l'indirizzo IP, la netmask, il gateway e la porta.

A differenza di un SVM di dati o di un SVM di nodo, un server di gestione del cluster non dispone di un volume root o di volumi utente host (anche se può ospitare volumi di sistema). Inoltre, un server di gestione del cluster può avere solo LIF del tipo di gestione del cluster.

Se si esegue `vserver show` il server di gestione del cluster viene visualizzato nell'elenco di output del comando.

#### Tipi di SVM

Un cluster è costituito da quattro tipi di SVM, che consentono di gestire il cluster, le sue risorse e l'accesso ai dati ai client e alle applicazioni.

Un cluster contiene i seguenti tipi di SVM:

- SVM amministratore

Il processo di installazione del cluster crea automaticamente la SVM amministrativa per il cluster. La SVM amministrativa rappresenta il cluster.

- SVM del nodo

  Un nodo SVM viene creato quando il nodo si unisce al cluster e il nodo SVM rappresenta i singoli nodi del cluster.

- SVM di sistema (avanzato)

  Viene creata automaticamente una SVM di sistema per le comunicazioni a livello di cluster in un IPSpace.

- SVM dei dati

  Un SVM di dati rappresenta i dati che servono le SVM. Dopo la configurazione del cluster, un amministratore del cluster deve creare SVM di dati e aggiungere volumi a queste SVM per facilitare l'accesso ai dati dal cluster.

  Un cluster deve disporre di almeno una SVM di dati per fornire i dati ai propri client.

> Se non diversamente specificato, il termine SVM si riferisce a una SVM (data-serving).
>
> Nella CLI, le SVM vengono visualizzate come Vserver.

## Accedere al cluster utilizzando la CLI (solo amministratori del cluster)

### Accedere al cluster utilizzando la porta seriale

È possibile accedere al cluster direttamente da una console collegata alla porta seriale di un nodo.

#### Fasi

1. Nella console, premere Invio.

   Il sistema risponde con la richiesta di accesso.

2. Al prompt di accesso, eseguire una delle seguenti operazioni:

| Per accedere al cluster con… | Immettere il seguente nome account… |
|---|---|
| L'account cluster predefinito | **`admin`** |
| Un account utente amministrativo alternativo | *`username`* |

   Il sistema risponde con la richiesta della password.

3. Immettere la password per l'account amministratore o amministrativo, quindi premere Invio.

### Accedere al cluster utilizzando SSH

È possibile inviare richieste SSH al cluster per eseguire attività amministrative. SSH è

attivato per impostazione predefinita.

**Di cosa hai bisogno**

- È necessario disporre di un account utente configurato per l'utilizzo `ssh` come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Il `security login` "pagine man" contengono informazioni aggiuntive.

- Se si utilizza un account utente di dominio Active Directory (ad) per accedere al cluster, è necessario configurare un tunnel di autenticazione per il cluster tramite una VM di storage abilitata CIFS e aggiungere anche l'account utente di dominio ad al cluster con `ssh` come metodo di accesso e. `domain` come metodo di autenticazione.
- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

  Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

**A proposito di questa attività**

- È necessario utilizzare un client OpenSSH 5.7 o successivo.
- È supportato solo il protocollo SSH v2; SSH v1 non è supportato.
- ONTAP supporta un massimo di 64 sessioni SSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- ONTAP supporta solo gli algoritmi di crittografia AES e 3DES (noti anche come *cifrari*) per SSH.

  AES è supportato con 128, 192 e 256 bit di lunghezza della chiave. 3DES ha una lunghezza della chiave di 56 bit come nel DES originale, ma viene ripetuto tre volte.

- Quando la modalità FIPS è attiva, i client SSH devono negoziare con gli algoritmi a chiave pubblica ECDSA (Elliptic Curve Digital Signature Algorithm) per consentire la connessione.
- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utility di terze parti, ad esempio putty.
- Se si utilizza un nome utente Windows ad per accedere a ONTAP, utilizzare le stesse lettere maiuscole o minuscole utilizzate al momento della creazione del nome utente e del nome di dominio ad in ONTAP.

  I nomi utente E i nomi di dominio AD non sono sensibili al maiuscolo/minuscolo. Tuttavia, i nomi utente ONTAP distinguono tra maiuscole e minuscole. La mancata corrispondenza tra il nome utente creato in ONTAP e il nome utente creato in ad comporta un errore di accesso.

**Opzioni di autenticazione SSH**

- A partire da ONTAP 9.3, è possibile "Abilitare l'autenticazione a più fattori SSH" per gli account dell'amministratore locale.

  Quando l'autenticazione a più fattori SSH è attivata, gli utenti vengono autenticati utilizzando una chiave pubblica e una password.

- A partire da ONTAP 9.4, è possibile "Abilitare l'autenticazione a più fattori SSH" Per utenti remoti LDAP e NIS.
- A partire da ONTAP 9.13.1, è possibile aggiungere facoltativamente la convalida del certificato al processo di autenticazione SSH per migliorare la sicurezza di accesso. A tal fine, "Associare un certificato X.509 alla chiave pubblica" utilizzato da un account. Se si accede utilizzando SSH sia con una chiave pubblica SSH che con un certificato X.509, ONTAP verifica la validità del certificato X.509 prima di autenticarsi con la chiave pubblica SSH. L'accesso SSH viene rifiutato se il certificato è scaduto o revocato e la chiave pubblica SSH viene disattivata automaticamente.
- A partire da ONTAP 9.14.1, è possibile aggiungere facoltativamente l'autenticazione a due fattori Cisco Duo al processo di autenticazione SSH per migliorare la sicurezza dell'accesso. Al primo accesso dopo aver attivato l'autenticazione Cisco Duo, gli utenti dovranno registrare un dispositivo per fungere da autenticatore per le sessioni SSH. Fare riferimento a. "Configurare Cisco Duo 2FA per gli accessi SSH" Per ulteriori informazioni sulla configurazione dell'autenticazione SSH Cisco Duo per ONTAP.

**Fasi**

1. Da un host di amministrazione, immettere `ssh` comando in uno dei seguenti formati:
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

Se si utilizza un account utente di dominio ad, è necessario specificare *`username`* nel formato di *`domainname`*`\\`*`AD_accountname`* (con barre rovesciate doppie dopo il nome di dominio) o. `"`*`domainname`*`\`*`AD_accountname`*`"` (racchiuso tra virgolette doppie e con una barra rovesciata singola dopo il nome di dominio).

*`hostname_or_IP`* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

*`command`* Non è richiesto per le sessioni interattive SSH.

**Esempi di richieste SSH**

I seguenti esempi mostrano come l'account utente "joe" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

I seguenti esempi mostrano come l'account utente "john" del dominio "DOMAIN1" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

L'esempio seguente mostra come l'account utente "joe" può inviare una richiesta SSH MFA per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

**Informazioni correlate**

"Autenticazione amministratore e RBAC"

### Sicurezza di accesso SSH

A partire da ONTAP 9.5, è possibile visualizzare le informazioni sugli accessi precedenti, i tentativi di accesso non riusciti e le modifiche ai privilegi dall'ultimo accesso riuscito.

Le informazioni relative alla sicurezza vengono visualizzate quando si effettua l'accesso come utente amministratore SSH. L'utente viene avvisato delle seguenti condizioni:

- L'ultima volta in cui è stato effettuato l'accesso al nome dell'account.
- Il numero di tentativi di accesso non riusciti dall'ultimo accesso riuscito.
- Se il ruolo è cambiato dall'ultimo accesso (ad esempio, se il ruolo dell'account admin è cambiato da "admin" a "backup").
- Se le funzionalità di aggiunta, modifica o eliminazione del ruolo sono state modificate dall'ultimo accesso.

> Se una delle informazioni visualizzate è sospetta, contattare immediatamente il reparto di sicurezza.

Per ottenere queste informazioni al momento dell'accesso, devono essere soddisfatti i seguenti prerequisiti:

- Il provisioning dell'account utente SSH deve essere eseguito in ONTAP.
- È necessario creare l'accesso di sicurezza SSH.
- Il tentativo di accesso deve essere riuscito.

#### Restrizioni e altre considerazioni per la sicurezza dell'accesso SSH

Le seguenti restrizioni e considerazioni si applicano alle informazioni di sicurezza per l'accesso SSH:

- Le informazioni sono disponibili solo per gli accessi basati su SSH.
- Per gli account admin basati su gruppo, come ad esempio gli account LDAP/NIS e ad, gli utenti possono visualizzare le informazioni di accesso SSH se il gruppo di cui fanno parte è configurato come account admin in ONTAP.

  Tuttavia, gli avvisi relativi alle modifiche al ruolo dell'account utente non possono essere visualizzati per questi utenti. Inoltre, gli utenti appartenenti a un gruppo ad che è stato fornito come account admin in ONTAP non possono visualizzare il numero di tentativi di accesso non riusciti che si sono verificati dall'ultimo accesso.

- Le informazioni conservate per un utente vengono eliminate quando l'account utente viene cancellato da ONTAP.
- Le informazioni non vengono visualizzate per le connessioni ad applicazioni diverse da SSH.

#### Esempi di informazioni di sicurezza per l'accesso SSH

I seguenti esempi mostrano il tipo di informazioni visualizzate dopo l'accesso.

- Questo messaggio viene visualizzato dopo ogni accesso riuscito:

```
Last Login : 7/19/2018 06:11:32
```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti dall'ultimo accesso riuscito:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti e i privilegi sono stati modificati dall'ultimo accesso riuscito:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

#### Abilitare l'accesso Telnet o RSH al cluster

Come Best practice per la sicurezza, Telnet e RSH sono disattivati nella policy predefinita del firewall di gestione (`mgmt`). Per consentire al cluster di accettare richieste Telnet o RSH, è necessario creare un nuovo criterio firewall di gestione con Telnet o RSH attivato, quindi associare il nuovo criterio alla LIF di gestione del cluster.

##### A proposito di questa attività

ONTAP impedisce di modificare le policy firewall predefinite, ma è possibile creare una nuova policy clonando quelle predefinite `mgmt` Policy del firewall di gestione, quindi abilitazione di Telnet o RSH in base alla nuova policy. Tuttavia, Telnet e RSH non sono protocolli sicuri, pertanto si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

Per abilitare l'accesso Telnet o RSH ai cluster, attenersi alla seguente procedura:

##### Fasi

1. Accedere alla modalità avanzata dei privilegi:
   **`set advanced`**
2. Abilitare un protocollo di sicurezza (RSH o Telnet):
   **`security protocol modify -application`** ***`security_protocol`*** **`-enabled true`**
3. Creare una nuova policy del firewall di gestione basata su `mgmt` policy del firewall di gestione:
   **`system services firewall policy clone -policy mgmt -destination-policy`** ***`policy-name`***
4. Abilitare Telnet o RSH nella nuova policy del firewall di gestione:
   **`system services firewall policy create -policy`** ***`policy-name`*** **`-service`** ***`security_protocol`*** **`-action allow -ip-list`** ***`ip_address/netmask`***`` `Per consentire tutti gli indirizzi IP, specificare `-ip-list 0.0.0.0/0 ``
5. Associare la nuova policy alla LIF di gestione del cluster:
   **`network interface modify -vserver`** ***`cluster_management_LIF`*** **`-lif cluster_mgmt`**

**-firewall-policy *policy-name***

### Accedere al cluster utilizzando Telnet

È possibile inviare richieste Telnet al cluster per eseguire attività amministrative. Telnet è disattivato per impostazione predefinita.

#### Di cosa hai bisogno

Prima di poter utilizzare Telnet per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare Telnet come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

- Telnet deve essere già attivato nel criterio del firewall di gestione utilizzato dalle LIF di gestione del cluster o dei nodi, in modo che le richieste Telnet possano passare attraverso il firewall.

  Per impostazione predefinita, Telnet è disattivato. Il `system services firewall policy show` con il `-service telnet` Parametro indica se Telnet è stato attivato in un criterio firewall. Per ulteriori informazioni, consultare `system services firewall policy` pagine man.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

  Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

#### A proposito di questa attività

- Telnet non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni Telnet simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utility di terze parti, ad esempio putty.

#### Fasi

1. Da un host di amministrazione, immettere il seguente comando:

   **telnet *hostname_or_IP***

   *`hostname_or_IP`* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

#### Esempio di richiesta Telnet

L'esempio seguente mostra come l'utente "joe", configurato con accesso Telnet, può inviare una richiesta Telnet per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

### Accedere al cluster utilizzando RSH

È possibile inviare richieste RSH al cluster per eseguire attività amministrative. RSH non è un protocollo sicuro ed è disattivato per impostazione predefinita.

#### Di cosa hai bisogno

Prima di poter utilizzare RSH per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare RSH come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

- RSH deve essere già abilitato nella policy del firewall di gestione utilizzata dalle LIF di gestione del cluster o dei nodi, in modo che le richieste RSH possano passare attraverso il firewall.

  Per impostazione predefinita, RSH è disattivato. Il `system services firewall policy show` con il `-service rsh` Parametro indica se RSH è stato attivato in una policy firewall. Per ulteriori informazioni, consultare `system services firewall policy` pagine man.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

  Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

#### A proposito di questa attività

- RSH non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni RSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

**Fasi**

1. Da un host di amministrazione, immettere il seguente comando:

   ***rsh hostname_or_IP -l username:passwordcommand***

   *`hostname_or_IP`* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

   *`command`* È il comando che si desidera eseguire su RSH.

**Esempio di richiesta RSH**

L'esempio seguente mostra come l'utente "joe", che è stato configurato con accesso RSH, può emettere una richiesta RSH per eseguire `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

## Utilizzare l'interfaccia della riga di comando di ONTAP

**Utilizzando l'interfaccia della riga di comando di ONTAP**

L'interfaccia a riga di comando (CLI) di ONTAP fornisce una vista basata su comandi dell'interfaccia di gestione. I comandi vengono immessi al prompt del sistema di storage e i risultati dei comandi vengono visualizzati in testo.

Il prompt dei comandi CLI è rappresentato come `cluster_name::>`.

Se si imposta il livello di privilegio (ovvero, l' `-privilege` del parametro `set` comando) a. `advanced`, il prompt include un asterisco (*), ad esempio:

```
cluster_name::*>
```

**Informazioni sulle diverse shell per i comandi CLI (solo amministratori del cluster)**

Il cluster dispone di tre diverse shell per i comandi CLI, la *clustershell*, la *nodeshell* e la *systemshell*. Le shell hanno scopi diversi, ognuno dei quali ha un set di comandi diverso.

- La shell clustershell è la shell nativa che viene avviata automaticamente quando si accede al cluster.

  Fornisce tutti i comandi necessari per configurare e gestire il cluster. La guida CLI della shell del

clustershell (attivata da `?` al prompt di clustershell) visualizza i comandi disponibili di clustershell. Il `man command_name` il comando nella shell clustershell visualizza la pagina man del comando clustershell specificato.

- Il nodeshell è una shell speciale per i comandi che hanno effetto solo a livello di nodo.

  Il nodeshell è accessibile attraverso `system node run` comando.

  Il nodeshell CLI help (attivato da `?` oppure `help` al prompt nodeshell) visualizza i comandi nodeshell disponibili. Il `man command_name` nel nodeshell viene visualizzata la pagina man del comando nodeshell specificato.

  Molti comandi e opzioni nodeshell comunemente utilizzati sono tunneled o aliased nella clustershell e possono essere eseguiti anche dalla clustershell.

- Systemshell è una shell di basso livello che viene utilizzata solo per scopi di diagnostica e troubleshooting.

  La shell di sistema e l'account associato "diag" sono destinati a scopi diagnostici di basso livello. Il loro accesso richiede il livello di privilegio diagnostico ed è riservato solo al supporto tecnico per eseguire le attività di risoluzione dei problemi.

#### Accesso a comandi e opzioni nodeshell nella shell dei clustershell

I comandi e le opzioni di Nodeshell sono accessibili attraverso il nodeshell:

`system node run -node nodename`

Molti comandi e opzioni nodeshell comunemente utilizzati sono tunneled o aliased nella clustershell e possono essere eseguiti anche dalla clustershell.

È possibile accedere alle opzioni Nodeshell supportate nella shell clustershell utilizzando `vserver options clustershell` comando. Per visualizzare queste opzioni, è possibile effettuare una delle seguenti operazioni:

- Eseguire una query della CLI della shell del clustershell con `vserver options -vserver nodename_or_clustername -option-name ?`
- Accedere a. `vserver options` Man page nella CLI della shell del clustershell con `man vserver options`

Se si immette un comando o un'opzione nodeshell o legacy nella clustershell e il comando o l'opzione ha un comando clustershell equivalente, ONTAP informa dell'utilizzo del comando clustershell.

Se si immette un comando o un'opzione legacy o nodeshell non supportato nella shell del clustershell, ONTAP indica lo stato "Not Supported" (non supportato) per il comando o l'opzione.

#### Visualizza i comandi nodeshell disponibili

Puoi ottenere un elenco dei comandi nodeshell disponibili usando l'aiuto CLI del nodeshell.

**Fasi**

1. Per accedere al nodeshell, immettere il seguente comando al prompt di sistema della shell:

   **`system node run -node {nodename|local}`**

`local` è il nodo utilizzato per accedere al cluster.

> Il `system node run` il comando dispone di un comando alias, `run`.

2. Immettere il seguente comando nel nodeshell per visualizzare l'elenco dei comandi nodeshell disponibili:

   **[*commandname*] help**

   ```
   `_commandname_` è il nome del comando di cui si desidera visualizzare la
   disponibilità. Se non si include `_commandname_`, La CLI visualizza
   tutti i comandi nodeshell disponibili.
   ```

   Viene immesso `exit` In alternativa, digitare Ctrl-d per tornare alla CLI della shell cluster.

**Esempio di visualizzazione dei comandi nodeshell disponibili**

Nell'esempio seguente viene effettuato l'accesso al nodeshell di un nodo denominato node2 e vengono visualizzate le informazioni relative al comando nodeshell `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

**Metodi per navigare nelle directory dei comandi CLI**

## I comandi nella CLI sono organizzati in una gerarchia in base alle directory dei comandi. È possibile eseguire i comandi nella gerarchia inserendo il percorso completo dei comandi o navigando nella struttura della directory.

Quando si utilizza l'interfaccia CLI, è possibile accedere alla directory dei comandi digitando il nome della directory al prompt e premendo Invio. Il nome della directory viene quindi incluso nel testo del prompt per indicare che si sta interagendo con la directory dei comandi appropriata. Per approfondire la gerarchia dei comandi, digitare il nome di una sottodirectory dei comandi, quindi premere Invio. Il nome della sottodirectory viene quindi incluso nel testo del prompt e il contesto viene spostato in tale sottodirectory.

È possibile navigare attraverso diverse directory di comandi immettendo l'intero comando. Ad esempio, è possibile visualizzare le informazioni relative ai dischi immettendo il `storage disk show` al prompt. È inoltre possibile eseguire il comando esplorando una directory di comandi alla volta, come illustrato nell'esempio seguente:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

È possibile abbreviare i comandi immettendo solo il numero minimo di lettere in un comando che rende il comando unico per la directory corrente. Ad esempio, per abbreviare il comando nell'esempio precedente, è possibile immettere `st d sh`. È inoltre possibile utilizzare il tasto Tab per espandere i comandi abbreviati e visualizzare i parametri di un comando, inclusi i valori dei parametri predefiniti.

È possibile utilizzare `top` per passare al livello superiore della gerarchia di comandi e a. `up` comando o. `..` per salire di un livello nella gerarchia di comandi.

> I comandi e le opzioni di comando preceduti da un asterisco (*) nella CLI possono essere eseguiti solo a livello di privilegio avanzato o superiore.

**Regole per specificare i valori nella CLI**

La maggior parte dei comandi include uno o più parametri obbligatori o opzionali. Molti parametri richiedono di specificare un valore per essi. Esistono alcune regole per specificare i valori nella CLI.

- Un valore può essere un numero, un identificatore booleano, una selezione da un elenco enumerato di valori predefiniti o una stringa di testo.

  Alcuni parametri possono accettare un elenco separato da virgole di due o più valori. Gli elenchi di valori separati da virgole non devono essere tra virgolette (" "). Ogni volta che si specifica il testo, uno spazio o un carattere di query (quando non si intende una query o un testo che inizia con un simbolo minore o maggiore di), è necessario racchiudere l'entità tra virgolette.

- L'interfaccia CLI interpreta un punto interrogativo ("?") come comando per visualizzare le informazioni della guida per un determinato comando.
- Alcuni testi immessi nella CLI, come i nomi dei comandi, i parametri e alcuni valori, non fanno distinzione tra maiuscole e minuscole.

  Ad esempio, quando si immettono i valori dei parametri per `vserver cifs` comandi, le maiuscole vengono ignorate. Tuttavia, la maggior parte dei valori dei parametri, come i nomi dei nodi, le macchine virtuali di storage (SVM), gli aggregati, i volumi e le interfacce logiche, è sensibile al maiuscolo/minuscolo.

- Se si desidera cancellare il valore di un parametro che prende una stringa o un elenco, specificare un set vuoto di virgolette ("") o un trattino ("-").
- Il simbolo cancelletto ("` n.`"), noto anche come simbolo cancelletto, indica un commento per un input della riga di comando; se utilizzato, dovrebbe essere visualizzato dopo l'ultimo parametro in una riga di comando.

  L'interfaccia CLI ignora il testo tra "` n.`" e la fine della riga.

Nell'esempio seguente, viene creata una SVM con un commento di testo. La SVM viene quindi modificata per eliminare il commento:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

Nell'esempio seguente, un commento della riga di comando che utilizza il segno "` n.`" indica la funzione del comando.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

#### Metodi di visualizzazione della cronologia dei comandi e di reinvio dei comandi

Ogni sessione CLI conserva una cronologia di tutti i comandi in essa emessi. È possibile visualizzare la cronologia dei comandi della sessione corrente. È inoltre possibile emettere nuovamente i comandi.

Per visualizzare la cronologia dei comandi, è possibile utilizzare `history` comando.

Per riemettere un comando, è possibile utilizzare `redo` comando con uno dei seguenti argomenti:

- Stringa che corrisponde a parte di un comando precedente

  Ad esempio, se solo `volume` il comando eseguito è `volume show`, è possibile utilizzare `redo volume` per eseguire nuovamente il comando.

- L'ID numerico di un comando precedente, come elencato dal `history` comando

  Ad esempio, è possibile utilizzare `redo 4` comando per emettere nuovamente il quarto comando nell'elenco della cronologia.

- Offset negativo dalla fine dell'elenco della cronologia

  Ad esempio, è possibile utilizzare `redo -2` comando per emettere nuovamente il comando eseguito due comandi fa.

Ad esempio, per ripetere il comando che è il terzo dalla fine della cronologia dei comandi, immettere il seguente comando:

```
cluster1::> redo -3
```

#### Tasti di scelta rapida per la modifica dei comandi CLI

Il comando al prompt dei comandi corrente è il comando attivo. L'utilizzo dei tasti di scelta rapida consente di modificare rapidamente il comando attivo. Questi tasti di scelta rapida sono simili a quelli della shell UNIX tcsh e dell'editor Emacs.

La seguente tabella elenca i tasti di scelta rapida per la modifica dei comandi CLI. "Ctrl-" indica che si tiene premuto il tasto Ctrl mentre si digita il carattere specificato. "Esc-" indica che si preme e si rilascia il tasto Esc, quindi si digita il carattere specificato.

| Se si desidera… | Utilizzare la seguente scelta rapida da tastiera… |
|---|---|
| Spostare il cursore indietro di un carattere | Ctrl-B. |
| Freccia indietro | Spostare il cursore in avanti di un carattere |
| Ctrl-F. | Freccia avanti |
| Spostare il cursore indietro di una parola | ESC-B. |
| Spostare il cursore in avanti di una parola | ESC-F. |
| Spostare il cursore all'inizio della riga | Ctrl-A. |
| Spostare il cursore alla fine della riga | Ctrl-E. |
| Rimuovere il contenuto della riga di comando dall'inizio della riga al cursore e salvarlo nel buffer di taglio. Il buffer cut agisce come una memoria temporanea, simile a quella che viene chiamata *clipboard* in alcuni programmi. | Ctrl-U |
| Rimuovere il contenuto della riga di comando dal cursore alla fine della riga e salvarlo nel buffer di taglio | Ctrl-K. |
| Rimuovere il contenuto della riga di comando dal cursore alla fine della parola seguente e salvarlo nel buffer di taglio | ESC-D |
| Rimuovere la parola prima del cursore e salvarla nel buffer di taglio | Ctrl-W. |
| Inserire il contenuto del buffer di taglio e inserirlo nella riga di comando del cursore | Ctrl-Y |
| Consente di eliminare il carattere che precede il cursore | Ctrl-H |

| Se si desidera… | Utilizzare la seguente scelta rapida da tastiera… |
| --- | --- |
| Backspace | Consente di eliminare il carattere in cui si trova il cursore |
| Ctrl-D | Eliminare la linea |
| Ctrl-C. | Cancellare lo schermo |
| Ctrl-L. | Sostituire il contenuto corrente della riga di comando con la voce precedente nell'elenco della cronologia.<br><br>Ad ogni ripetizione del tasto di scelta rapida, il cursore della cronologia passa alla voce precedente. |
| Ctrl-P. | ESC-P. |
| Freccia su | Sostituire il contenuto corrente della riga di comando con la voce successiva nell'elenco della cronologia. Ad ogni ripetizione del tasto di scelta rapida, il cursore della cronologia passa alla voce successiva. |
| Ctrl-N. | ESC-N. |
| Freccia giù | Espandere un comando o un elenco di input validi inseriti parzialmente dalla posizione di modifica corrente |
| Scheda | Ctrl-I. |
| Visualizza la guida sensibile al contesto | ? |
| Escape the special mapping for the question mark ("?") character. For instance, to enter a question mark into a command's argument, press Esc and then the "?" carattere. | ESC-? |
| Avviare l'output TTY | Ctrl-Q. |
| Interrompere l'output TTY | Ctrl-S. |

#### Utilizzo dei livelli di privilegio amministrativi

I comandi e i parametri ONTAP sono definiti a tre livelli di privilegio: *Admin*, *Advanced* e *Diagnostic*. I livelli di privilegio riflettono i livelli di competenza richiesti per l'esecuzione delle attività.

- **admin**

La maggior parte dei comandi e dei parametri è disponibile a questo livello. Vengono utilizzati per attività comuni o di routine.

- **avanzato**

  I comandi e i parametri di questo livello vengono utilizzati raramente, richiedono conoscenze avanzate e possono causare problemi se utilizzati in modo non appropriato.

  I comandi o i parametri avanzati vengono utilizzati solo con la consulenza del personale di supporto.

- **diagnostica**

  I comandi e i parametri diagnostici possono causare interruzioni. Vengono utilizzati solo dal personale di supporto per diagnosticare e risolvere i problemi.

#### Impostare il livello di privilegio nella CLI

È possibile impostare il livello di privilegio nella CLI utilizzando `set` comando. Le modifiche alle impostazioni del livello di privilegio si applicano solo alla sessione in corso. Non sono persistenti tra le sessioni.

##### Fasi

1. Per impostare il livello di privilegio nella CLI, utilizzare `set` con il `-privilege` parametro.

##### Esempio di impostazione del livello di privilegio

Nell'esempio seguente viene impostato il livello di privilegio su Advanced (avanzato) e quindi su admin (admin):

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

#### Impostare le preferenze di visualizzazione nella CLI

È possibile impostare le preferenze di visualizzazione per una sessione CLI utilizzando `set` comando e. `rows` comando. Le preferenze impostate si applicano solo alla sessione in cui ci si trova. Non sono persistenti tra le sessioni.

##### A proposito di questa attività

È possibile impostare le seguenti preferenze di visualizzazione CLI:

- Il livello di privilegio della sessione di comando
- Se vengono emesse conferme per comandi potenzialmente disgregativi
- Se `show` i comandi visualizzano tutti i campi
- Il carattere o i caratteri da utilizzare come separatore di campo

- L'unità predefinita quando si riferiscono le dimensioni dei dati
- Il numero di righe visualizzate nella sessione CLI corrente prima che l'interfaccia sospende l'output

  Se il numero preferito di righe non viene specificato, viene regolato automaticamente in base all'altezza effettiva del terminale. Se l'altezza effettiva non è definita, il numero predefinito di righe è 24.

- La SVM (Storage Virtual Machine) o il nodo predefinito
- Se un comando che continua deve arrestarsi in caso di errore

**Fasi**

1. Per impostare le preferenze di visualizzazione CLI, utilizzare `set` comando.

   Per impostare il numero di righe visualizzate nella sessione CLI corrente, è possibile utilizzare anche il `rows` comando.

   Per ulteriori informazioni, consultare le pagine man del `set` comando e. `rows` comando.

**Esempio di impostazione delle preferenze di visualizzazione nella CLI**

Nell'esempio seguente viene impostata una virgola come separatore di campo, set `GB` come unità predefinita per la dimensione dei dati e imposta il numero di righe su 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

**Metodi di utilizzo degli operatori di query**

## L'interfaccia di gestione supporta query e modelli in stile UNIX e caratteri jolly per consentire la corrispondenza di più valori negli argomenti dei parametri di comando.

La seguente tabella descrive gli operatori di query supportati:

| Operatore | Descrizione |
|---|---|
| * | Carattere jolly che corrisponde a tutte le voci.<br><br>Ad esempio, il comando `volume show -volume *tmp*` visualizza un elenco di tutti i volumi i cui nomi includono la stringa `tmp`. |
| ! | NON operatore.<br><br>Indica un valore che non deve essere associato; ad esempio, **`!vs0`** indica di non corrispondere al valore `vs0`. |
| | |

| Operatore | Descrizione |
|---|---|
| O operatore .<br><br>Separa due valori da confrontare; ad esempio, `*vs0 | vs2*` corrisponde a vs0 o vs2. È possibile specificare più istruzioni OR, ad esempio `a |
| b* | *c*` corrisponde alla voce `a`, qualsiasi voce che inizia con `b`e qualsiasi voce che includa `c`. |
| .. | Operatore del raggio d'azione.<br><br>Ad esempio, **`5..10`** corrisponde a qualsiasi valore da `5` a. `10`, incluso. |
| < | Meno dell'operatore.<br><br>Ad esempio, **`<20`** corrisponde a qualsiasi valore inferiore a. `20`. |
| > | Maggiore rispetto all'operatore.<br><br>Ad esempio, **`>5`** corrisponde a qualsiasi valore maggiore di `5`. |
| ⇐ | Minore o uguale all'operatore.<br><br>Ad esempio, ⇐**`5`** corrisponde a qualsiasi valore minore o uguale a. `5`. |
| >= | Maggiore o uguale all'operatore.<br><br>Ad esempio, **`>=5`** corrisponde a qualsiasi valore maggiore o uguale a. `5`. |
| {`query`} | Query estesa.<br><br>Una query estesa deve essere specificata come primo argomento dopo il nome del comando, prima di qualsiasi altro parametro.<br><br>Ad esempio, il comando `volume modify {-volume *tmp*} -state offline` imposta offline tutti i volumi i cui nomi includono la stringa `tmp`. |

Se si desidera analizzare i caratteri di query come valori letterali, è necessario racchiudere i caratteri tra virgolette doppie (ad esempio, `"<10"`, `"0..100"`, `"*abc*"`, o. `"a|b"`) per restituire i risultati corretti.

È necessario racchiudere i nomi dei file raw tra virgolette doppie per impedire l'interpretazione di caratteri speciali. Questo vale anche per i caratteri speciali utilizzati dalla shell.

È possibile utilizzare più operatori di query in un'unica riga di comando. Ad esempio, il comando `volume show -size >1GB -percent-used <50 -vserver !vs1` Visualizza tutti i volumi con dimensioni superiori a 1 GB, meno del 50% utilizzati e non nella macchina virtuale di storage (SVM) denominata "vs1".

**Informazioni correlate**

"Tasti di scelta rapida per la modifica dei comandi CLI"

**Metodi di utilizzo delle query estese**

## È possibile utilizzare query estese per associare ed eseguire operazioni sugli oggetti che hanno valori specificati.

Le query estese vengono specificate racchiudendole tra parentesi graffe ({}). Una query estesa deve essere specificata come primo argomento dopo il nome del comando, prima di qualsiasi altro parametro. Ad esempio, per impostare offline tutti i volumi i cui nomi includono la stringa `tmp`, eseguire il comando nel seguente esempio:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Le query estese sono generalmente utili solo con `modify` e. `delete` comandi. Non hanno alcun significato in `create` oppure `show` comandi.

La combinazione di query e operazioni di modifica è uno strumento utile. Tuttavia, se implementato in modo errato, potrebbe causare confusione ed errori. Ad esempio, utilizzando (privilegio avanzato) `system node image modify` il comando per impostare l'immagine software predefinita di un nodo imposta automaticamente l'altra immagine software in modo che non sia quella predefinita. Il comando nell'esempio seguente è effettivamente un'operazione nulla:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Questo comando imposta l'immagine predefinita corrente come immagine non predefinita, quindi imposta la nuova immagine predefinita (l'immagine precedente non predefinita) sull'immagine non predefinita, mantenendo le impostazioni predefinite originali. Per eseguire correttamente l'operazione, utilizzare il comando riportato nell'esempio seguente:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

**Metodi di personalizzazione dell'output del comando show utilizzando i campi**

## Quando si utilizza `-instance` parametro con a. `show` comando per visualizzare i dettagli, l'output può essere lungo e includere più informazioni di quante ne hai bisogno. Il `-fields` parametro di a. `show` il comando consente di visualizzare solo le informazioni specificate.

Ad esempio, in esecuzione `volume show -instance` è probabile che si traducono in diverse schermate di informazioni. È possibile utilizzare `volume show -fields` *`fieldname[,fieldname…]`* per personalizzare l'output in modo che includa solo il campo o i campi specificati (oltre ai campi predefiniti sempre visualizzati). È

possibile utilizzare `-fields ?` per visualizzare i campi validi per a. `show` comando.

L'esempio seguente mostra la differenza di output tra `-instance` e il `-fields` parametro:

```
cluster1::> volume show -instance

                                   Vserver Name: cluster1-1
                                    Volume Name: vol0
                                 Aggregate Name: aggr0
                                    Volume Size: 348.3GB
                             Volume Data Set ID: -
                      Volume Master Data Set ID: -
                                   Volume State: online
                                    Volume Type: RW
                                   Volume Style: flex
                                          ...
                          Space Guarantee Style: volume
                      Space Guarantee in Effect: true
                                          ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- -----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

#### Informazioni sui parametri di posizione

È possibile sfruttare la funzionalità dei parametri di posizione della CLI ONTAP per aumentare l'efficienza nell'input dei comandi. È possibile eseguire una query su un comando per identificare i parametri posizionali per il comando.

#### Che cos'è un parametro posizionale

- Un parametro posizionale è un parametro che non richiede di specificare il nome del parametro prima di specificare il valore del parametro.
- Un parametro posizionale può essere intervallato con parametri non posizionali nell'input del comando, purché osservi la sua sequenza relativa con altri parametri posizionali nello stesso comando, come indicato nella ***command_name ?*** output.
- Un parametro posizionale può essere un parametro obbligatorio o facoltativo per un comando.
- Un parametro può essere posizionale per un comando ma non posizionale per un altro.

> L'utilizzo della funzionalità dei parametri di posizione negli script non è consigliato, in particolare quando i parametri di posizione sono facoltativi per il comando o hanno parametri facoltativi elencati prima di essi.

#### Identificare un parametro di posizione

È possibile identificare un parametro di posizione in ***command_name ?*** output del comando. Un parametro di posizione ha parentesi quadre che circondano il nome del parametro, in uno dei seguenti formati:

- [`-`*`parameter_name`*] *`parameter_value`* mostra un parametro obbligatorio posizionale.
- [.[`-`*`parameter_name`*] *`parameter_value`*] mostra un parametro opzionale posizionale.

Ad esempio, se visualizzato come segue in ***command_name ?*** output, il parametro è posizionale per il comando in cui viene visualizzato:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

Tuttavia, quando viene visualizzato come segue, il parametro non è posizionale per il comando in cui viene visualizzato:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

#### Esempi di utilizzo dei parametri di posizione

Nell'esempio seguente, il ***volume create ?*** l'output mostra che tre parametri sono posizionali per il comando: `-volume`, `-aggregate`, e. `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

Nell'esempio seguente, il `volume create` il comando viene specificato senza sfruttare la funzionalità del parametro di posizione:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

Gli esempi seguenti utilizzano la funzionalità del parametro di posizione per aumentare l'efficienza dell'input del comando. I parametri di posizione sono intervallati da parametri non posizionali in `volume create` e i valori dei parametri di posizione vengono specificati senza i nomi dei parametri. I parametri di posizione vengono specificati nella stessa sequenza indicata da **`volume create ?`** output. Questo è il valore per `-volume` viene specificato prima di `-aggregate`, a sua volta specificata prima di quella di `-size`.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

#### Metodi di accesso alle pagine man di ONTAP

Le pagine man (manual) di ONTAP spiegano come utilizzare i comandi CLI di ONTAP. Queste pagine sono disponibili nella riga di comando e sono pubblicate anche nei *riferimenti ai comandi* specifici della release.

Nella riga di comando ONTAP, utilizzare `man command_name` per visualizzare la pagina manuale del comando specificato. Se non si specifica un nome di comando, viene visualizzato l'indice della pagina manuale. È possibile utilizzare `man man` per visualizzare informazioni su `man` comando stesso. È possibile uscire da una pagina man immettendo **`q`**.

Fare riferimento a. Riferimento al comando per la versione di ONTAP 9 in uso Per ulteriori informazioni sui comandi ONTAP a livello amministrativo e avanzato disponibili nella release.

## Gestire le sessioni CLI

È possibile registrare una sessione CLI in un file con un nome e una dimensione specificati, quindi caricare il file in una destinazione FTP o HTTP. È inoltre possibile visualizzare o eliminare i file in cui sono state precedentemente registrate le sessioni CLI.

### Registrare una sessione CLI

Il record di una sessione CLI termina quando si interrompe la registrazione o si termina la sessione CLI o quando il file raggiunge il limite di dimensione specificato. Il limite predefinito per le dimensioni del file è di 1 MB. La dimensione massima del file è di 2 GB.

La registrazione di una sessione CLI è utile, ad esempio, se si sta risolvendo un problema e si desidera salvare informazioni dettagliate o se si desidera creare una registrazione permanente dell'utilizzo dello spazio in un momento specifico.

#### Fasi

1. Avviare la registrazione della sessione CLI corrente in un file:

   ```
   system script start
   ```

   Per ulteriori informazioni sull'utilizzo di `system script start` vedere la pagina man.

   ONTAP avvia la registrazione della sessione CLI nel file specificato.

2. Procedere con la sessione CLI.
3. Al termine, interrompere la registrazione della sessione:

   ```
   system script stop
   ```

   Per ulteriori informazioni sull'utilizzo di `system script stop` vedere la pagina man.

   ONTAP interrompe la registrazione della sessione CLI.

### Comandi per la gestione dei record delle sessioni CLI

Si utilizza `system script` Comandi per gestire i record delle sessioni CLI.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Avviare la registrazione della sessione CLI corrente in un file specificato | `system script start` |
| Interrompere la registrazione della sessione CLI corrente | `system script stop` |
| Visualizza le informazioni sui record delle sessioni CLI | `system script show` |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Caricare un record di una sessione CLI su una destinazione FTP o HTTP | `system script upload` |
| Eliminare un record di una sessione CLI | `system script delete` |

**Informazioni correlate**

"Comandi di ONTAP 9"

### Comandi per la gestione del periodo di timeout automatico delle sessioni CLI

Il valore di timeout specifica per quanto tempo una sessione CLI rimane inattiva prima di essere terminata automaticamente. Il valore di timeout CLI è esteso a tutto il cluster. Ovvero, ogni nodo di un cluster utilizza lo stesso valore di timeout CLI.

Per impostazione predefinita, il periodo di timeout automatico delle sessioni CLI è di 30 minuti.

Si utilizza `system timeout` Comandi per gestire il periodo di timeout automatico delle sessioni CLI.

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizza il periodo di timeout automatico per le sessioni CLI | `system timeout show` |
| Modificare il periodo di timeout automatico per le sessioni CLI | `system timeout modify` |

**Informazioni correlate**

"Comandi di ONTAP 9"

## Gestione cluster (solo amministratori cluster)

### Visualizza le informazioni sui nodi di un cluster

È possibile visualizzare i nomi dei nodi, verificare che i nodi siano integri e se sono idonei a partecipare al cluster. A livello di privilegi avanzati, è anche possibile visualizzare se un nodo contiene epsilon.

**Fasi**

1. Per visualizzare informazioni sui nodi di un cluster, utilizzare `cluster show` comando.

   Se si desidera che l'output mostri se un nodo contiene epsilon, eseguire il comando al livello di privilegio avanzato.

**Esempi di visualizzazione dei nodi in un cluster**

Nell'esempio seguente vengono visualizzate informazioni su tutti i nodi di un cluster a quattro nodi:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sul nodo denominato "node1" a livello di privilegi avanzati:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

#### Visualizzare gli attributi del cluster

È possibile visualizzare l'identificatore univoco (UUID), il nome, il numero di serie, la posizione e le informazioni di contatto di un cluster.

#### Fasi

1. Per visualizzare gli attributi di un cluster, utilizzare `cluster identity show` comando.

#### Esempio di visualizzazione degli attributi del cluster

Nell'esempio seguente vengono visualizzati il nome, il numero di serie, la posizione e le informazioni di contatto di un cluster.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

### Modificare gli attributi del cluster

È possibile modificare gli attributi di un cluster, ad esempio il nome del cluster, la posizione e le informazioni di contatto, in base alle necessità.

#### A proposito di questa attività

Non è possibile modificare l'UUID di un cluster, impostato al momento della creazione del cluster.

#### Fasi

1. Per modificare gli attributi del cluster, utilizzare `cluster identity modify` comando.

   Il `-name` parametro specifica il nome del cluster. Il `cluster identity modify` la pagina man descrive le regole per specificare il nome del cluster.

   Il `-location` parametro specifica la posizione del cluster.

   Il `-contact` parametro specifica le informazioni di contatto, ad esempio un nome o un indirizzo e-mail.

#### Esempio di ridenominazione di un cluster

Il seguente comando rinomina il cluster corrente ("cluster1") in "cluster2":

```
cluster1::> cluster identity modify -name cluster2
```

### Visualizza lo stato degli anelli di replica del cluster

È possibile visualizzare lo stato degli anelli di replica del cluster per diagnosticare i problemi a livello di cluster. In caso di problemi nel cluster, il personale di supporto potrebbe richiedere di eseguire questa attività per agevolare la risoluzione dei problemi.

#### Fasi

1. Per visualizzare lo stato degli anelli di replica del cluster, utilizzare `cluster ring show` al livello di privilegio avanzato.

#### Esempio di visualizzazione dello stato di replica del cluster

Nell'esempio seguente viene visualizzato lo stato dell'anello di replica VLDB su un nodo denominato node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

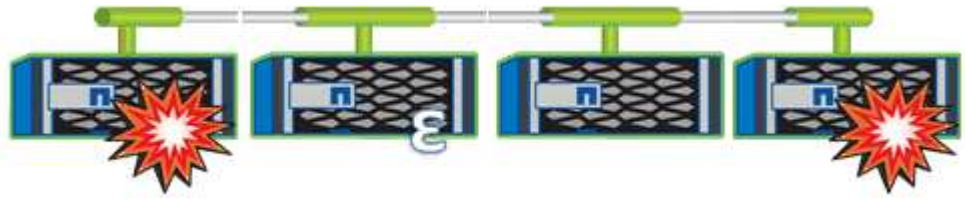
**Informazioni su quorum ed epsilon**

## Il quorum e l'epsilon sono misure importanti per lo stato e la funzione dei cluster che indicano insieme come i cluster affrontano le potenziali sfide di comunicazione e connettività.

*Quorum* è una condizione preliminare per un cluster completamente funzionante. Quando un cluster si trova in quorum, la maggior parte dei nodi è in buone condizioni e può comunicare tra loro. In caso di perdita del quorum, il cluster perde la capacità di eseguire le normali operazioni del cluster. Solo un insieme di nodi può avere il quorum alla volta, perché tutti i nodi condividono collettivamente una singola vista dei dati. Pertanto, se a due nodi non comunicanti è consentito modificare i dati in modo divergente, non è più possibile riconciliare i dati in una singola vista dati.

Ogni nodo del cluster partecipa a un protocollo di voting che elegge un nodo *master*; ogni nodo rimanente è un *secondario*. Il nodo master è responsabile della sincronizzazione delle informazioni nel cluster. Una volta formato, il quorum viene mantenuto con il voto continuo. Se il nodo master non è in linea e il cluster è ancora in quorum, viene selezionato un nuovo master dai nodi che rimangono in linea.

Poiché esiste la possibilità di un legame in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario aggiuntivo chiamato *epsilon*. Se la connettività tra due parti uguali di un cluster di grandi dimensioni non riesce, il gruppo di nodi che contiene epsilon mantiene il quorum, presupponendo che tutti i nodi siano integri. Ad esempio, la seguente illustrazione mostra un cluster a quattro nodi in cui due dei nodi sono guasti. Tuttavia, poiché uno dei nodi sopravvissuti contiene epsilon, il cluster rimane in quorum anche se non esiste una semplice maggioranza di nodi sani.



Epsilon viene assegnato automaticamente al primo nodo al momento della creazione del cluster. Se il nodo che contiene epsilon diventa inintegro, assume il controllo del partner ad alta disponibilità o viene sostituito dal partner ad alta disponibilità, epsilon viene automaticamente riassegnato a un nodo integro in una coppia ha diversa.

L'utilizzo offline di un nodo può influire sulla capacità del cluster di rimanere in quorum. Pertanto, ONTAP emette un messaggio di avviso se si tenta di eseguire un'operazione che toglie il quorum al cluster o se si mette fuori servizio un'operazione per evitare la perdita del quorum. È possibile disattivare i messaggi di avviso del quorum utilizzando `cluster quorum-service options modify` al livello di privilegio avanzato.

In generale, supponendo una connettività affidabile tra i nodi del cluster, un cluster più grande è più stabile di un cluster più piccolo. Il requisito di quorum di una semplice maggioranza della metà dei nodi più epsilon è più semplice da gestire in un cluster di 24 nodi che in un cluster di due nodi.

Un cluster a due nodi presenta alcune sfide specifiche per il mantenimento del quorum. I cluster a due nodi utilizzano *cluster ha*, in cui nessuno dei due nodi contiene epsilon; invece, entrambi i nodi vengono continuamente interrogati per garantire che, in caso di guasto di un nodo, l'altro disponga dell'accesso completo in lettura/scrittura ai dati, nonché dell'accesso alle interfacce logiche e alle funzioni di gestione.

**Quali sono i volumi di sistema**

I volumi di sistema sono volumi FlexVol che contengono metadati speciali, ad esempio metadati per i log di audit dei servizi file. Questi volumi sono visibili nel cluster in modo da poter tenere pienamente conto dell'utilizzo dello storage nel cluster.

I volumi di sistema sono di proprietà del server di gestione del cluster (chiamato anche SVM di amministrazione) e vengono creati automaticamente quando viene attivato il controllo dei file service.

È possibile visualizzare i volumi di sistema utilizzando `volume show` ma la maggior parte delle altre operazioni del volume non è consentita. Ad esempio, non è possibile modificare un volume di sistema utilizzando `volume modify` comando.

Questo esempio mostra quattro volumi di sistema sulla SVM amministrativa, che sono stati creati automaticamente quando è stato attivato il controllo dei servizi file per una SVM di dati nel cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

## Gestire i nodi

### Aggiungere nodi al cluster

Una volta creato un cluster, è possibile espanderlo aggiungendo nodi. È possibile aggiungere un solo nodo alla volta.

#### Di cosa hai bisogno

- Se si aggiungono nodi a un cluster a più nodi, tutti i nodi esistenti nel cluster devono essere integri (indicati da `cluster show`).
- Se stai aggiungendo nodi a un cluster senza switch a due nodi, devi convertire il cluster senza switch a due nodi in un cluster con switch usando uno switch cluster supportato da NetApp.

  La funzionalità cluster senza switch è supportata solo in un cluster a due nodi.

- Se si aggiunge un secondo nodo a un cluster a nodo singolo, il secondo nodo deve essere stato installato e la rete del cluster deve essere stata configurata.
- Se nel cluster è attivata la configurazione automatica SP, la subnet specificata per il SP deve disporre di risorse disponibili per consentire al nodo di Unione di utilizzare la subnet specificata per configurare automaticamente il SP.
- Per la LIF di gestione dei nodi del nuovo nodo è necessario aver raccolto le seguenti informazioni:
  - Porta
  - Indirizzo IP
  - Netmask
  - Gateway predefinito

**A proposito di questa attività**

I nodi devono essere in numeri pari in modo da poter formare coppie ha. Dopo aver iniziato ad aggiungere un nodo al cluster, è necessario completare il processo. Il nodo deve far parte del cluster prima di poter aggiungere un altro nodo.

**Fasi**

1. Accendere il nodo che si desidera aggiungere al cluster.

   Il nodo viene avviato e la procedura guidata Node Setup viene avviata sulla console.

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. Uscire dalla procedura guidata Node Setup (Configurazione nodo): `exit`

   La procedura guidata Node Setup (Configurazione nodo) viene chiusa e viene visualizzato un prompt di accesso che avvisa che le attività di installazione non sono state completate.

3. Accedere all'account admin utilizzando `admin` nome utente.
4. Avviare l'installazione guidata del cluster:

   **`cluster setup`**

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

Per ulteriori informazioni sulla configurazione di un cluster mediante la GUI di installazione, consultare "System Manager" guida in linea.

5. Premere Invio per utilizzare l'interfaccia CLI per completare l'attività. Quando viene richiesto di creare un nuovo cluster o di unirsi a un cluster esistente, immettere **`join`**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

Se la versione di ONTAP eseguita sul nuovo nodo è diversa dalla versione in esecuzione sul cluster esistente, il sistema riporta un `System checks Error: Cluster join operation cannot be performed at this time` errore. Questo è il comportamento previsto. Per continuare, eseguire `add-node -allow-mixed-version-join new_node_name` comando a livello di privilegi avanzati da un nodo esistente nel cluster.

6. Seguire le istruzioni per configurare il nodo e unirsi al cluster:
   - Per accettare il valore predefinito di un prompt, premere Invio.
   - Per immettere un valore personalizzato per un prompt, immettere il valore, quindi premere Invio.
7. Ripetere i passaggi precedenti per ogni nodo aggiuntivo che si desidera aggiungere.

**Al termine**

Dopo aver aggiunto nodi al cluster, è necessario attivare il failover dello storage per ogni coppia ha.

**Informazioni correlate**

"Cluster ONTAP a versione mista"

### Rimuovere i nodi dal cluster

È possibile rimuovere i nodi indesiderati da un cluster, un nodo alla volta. Dopo aver rimosso un nodo, è necessario rimuovere anche il partner di failover. Se si rimuove un nodo, i relativi dati diventano inaccessibili o cancellati.

#### Prima di iniziare

Prima di rimuovere i nodi dal cluster, devono essere soddisfatte le seguenti condizioni:

- Più della metà dei nodi nel cluster deve essere integro.
- Tutti i dati sul nodo che si desidera rimuovere devono essere stati svuotati.
  - Ciò potrebbe includere "eliminazione dei dati da un volume crittografato".
- Tutti i volumi non root lo sono "spostato" da aggregati di proprietà del nodo.
- Tutti gli aggregati non root sono stati "cancellato" dal nodo.
- Se il nodo possiede dischi FIPS (Federal Information Processing Standards) o dischi con crittografia automatica (SED), "la crittografia del disco è stata rimossa" riportando i dischi in modalità non protetta.
  - Potrebbe anche essere utile "Sanificare i dischi FIPS o i SED".
- I dati LIF lo sono "cancellato" oppure "trasferito" dal nodo.
- Le LIF di gestione del cluster lo sono state "trasferito" dal nodo e le porte home sono cambiate.
- Tutte le LIF intercluster sono state "rimosso".
  - Quando si rimuovono le LIF di intercluster, viene visualizzato un avviso che può essere ignorato.
- Il failover dello storage è stato così "disattivato" per il nodo.
- Tutte le regole di failover LIF lo sono state "modificato" per rimuovere le porte sul nodo.
- Tutte le VLAN sul nodo sono state "cancellato".
- Se si dispone di LUN sul nodo da rimuovere, è necessario "Modificare l'elenco dei nodi di reporting della mappa LUN selettiva (SLM)" prima di rimuovere il nodo.

  Se non si rimuove il nodo e il relativo partner ha dall'elenco dei nodi di reporting SLM, l'accesso alle LUN precedentemente presenti sul nodo può andare perso anche se i volumi contenenti le LUN sono stati spostati in un altro nodo.

Si consiglia di inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la rimozione del nodo è in corso.

**Nota:** non è necessario eseguire operazioni come `cluster remove-node`, `cluster unjoin`, e. `node rename` Quando è in corso un aggiornamento automatico di ONTAP.

#### A proposito di questa attività

- Se si esegue un cluster a versione mista, è possibile rimuovere l'ultimo nodo a versione bassa utilizzando uno dei comandi di privilegio avanzati che iniziano con ONTAP 9.3:
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9.4 e versioni successive: `cluster remove-node -skip-last-low-version-node -check`
- Se si disuniscono 2 nodi da un cluster a 4 nodi, il cluster ha viene attivato automaticamente sui due nodi rimanenti.

> Tutti i dati del sistema e dell'utente, provenienti da tutti i dischi collegati al nodo, devono essere resi inaccessibili agli utenti prima di rimuovere un nodo dal cluster. Se un nodo non è stato collegato correttamente da un cluster, contattare il supporto NetApp per assistenza con le opzioni di ripristino.

**Fasi**

1. Impostare il livello di privilegio su avanzato:

```
set -privilege advanced
```

2. Verificare se un nodo sul cluster contiene epsilon:

```
cluster show -epsilon true
```

3. Se un nodo nel cluster contiene epsilon e quel nodo verrà disaccoppiato, spostare epsilon in un nodo che non verrà disaccoppiato:
   a. Spostare epsilon dal nodo che si intende disunire

   ```
   cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
   ```

   b. Spostare epsilon in un nodo che non verrà disUnito:

   ```
   cluster modify -node <node_name> -epsilon true
   ```

4. Identificare il nodo master corrente:

```
cluster ring show
```

   Il nodo master è il nodo che contiene processi come "mgmt", "vldb", "vifmgr", "bcomd" e "crs".

5. Se il nodo che si desidera rimuovere è il nodo master corrente, abilitare l'elezione di un altro nodo nel cluster come nodo master:
   a. Rendere il nodo master corrente non idoneo a partecipare al cluster:

   ```
   cluster modify – node <node_name> -eligibility false
   ```

   Quando il nodo master non è idoneo, uno dei nodi rimanenti viene selezionato dal quorum del cluster come nuovo master.

   b. Rendere il nodo master precedente idoneo a partecipare nuovamente al cluster:

```
cluster modify – node <node_name> -eligibility true
```

6. Accedere alla LIF di gestione dei nodi remoti o alla LIF di gestione dei cluster su un nodo diverso da quello da rimuovere.
7. Rimuovere il nodo dal cluster:

| Per questa versione di ONTAP… | Utilizzare questo comando… |
|---|---|
| ONTAP 9.3 | `cluster unjoin` |
| ONTAP 9.4 e versioni successive | `cluster remove-node*` |

Se si dispone di un cluster con versione mista e si sta rimuovendo l'ultimo nodo della versione inferiore, utilizzare `-skip-last-low-version-node-check` con questi comandi.

Il sistema informa l'utente di quanto segue:

- È inoltre necessario rimuovere il partner di failover del nodo dal cluster.
- Una volta rimosso il nodo e prima di poterlo riconnettare a un cluster, è necessario utilizzare l'opzione del menu di avvio (4) pulizia della configurazione e inizializzazione di tutti i dischi o l'opzione (9) Configurazione della partizione avanzata del disco per cancellare la configurazione del nodo e inizializzare tutti i dischi.

  Viene generato un messaggio di errore se si verificano condizioni che è necessario risolvere prima di rimuovere il nodo. Ad esempio, il messaggio potrebbe indicare che il nodo dispone di risorse condivise che è necessario rimuovere o che si trova in una configurazione ha del cluster o in una configurazione di failover dello storage che è necessario disattivare.

Se il nodo è il master del quorum, il cluster perderà brevemente e tornerà al quorum. Questa perdita di quorum è temporanea e non influisce sulle operazioni dei dati.

8. Se un messaggio di errore indica condizioni di errore, risolvere tali condizioni ed eseguire nuovamente il `cluster remove-node` oppure `cluster unjoin` comando.

   Il nodo viene riavviato automaticamente dopo che è stato rimosso dal cluster.

9. Se si sta ridisponendo il nodo, cancellare la configurazione del nodo e inizializzare tutti i dischi:
   a. Durante il processo di avvio, premere Ctrl-C per visualizzare il menu di avvio quando richiesto.
   b. Selezionare l'opzione del menu di avvio (4) pulizia della configurazione e inizializzazione di tutti i dischi.
10. Torna al livello di privilegio admin:

```
set -privilege admin
```

11. Ripetere i passaggi precedenti per rimuovere il partner di failover dal cluster.

### Accedere ai file di log, core dump e MIB di un nodo utilizzando un browser Web

L'infrastruttura del Service Processor (`spi`) È attivato per impostazione predefinita per consentire a un browser Web di accedere ai file log, core dump e MIB di un nodo del cluster. I file rimangono accessibili anche quando il nodo non è attivo, a condizione che il nodo venga sostituito dal partner.

#### Di cosa hai bisogno

- La LIF di gestione del cluster deve essere attiva.

  È possibile utilizzare la LIF di gestione del cluster o di un nodo per accedere a. `spi` servizio web. Tuttavia, si consiglia di utilizzare la LIF di gestione del cluster.

  Il `network interface show` Il comando visualizza lo stato di tutte le LIF nel cluster.

- Per accedere a, è necessario utilizzare un account utente locale `spi` servizio web, gli account utente di dominio non sono supportati.
- Se l'account utente non ha il ruolo "admin" (che ha accesso a. `spi` servizio web per impostazione predefinita), al ruolo di controllo degli accessi deve essere concesso l'accesso a `spi` servizio web.

  Il `vserver services web access show` il comando mostra i ruoli a cui viene concesso l'accesso a quali servizi web.

- Se non si utilizza l'account utente "admin" (che include `http` access method (metodo di accesso), l'account utente deve essere impostato con `http` metodo di accesso.

  Il `security login show` il comando mostra i metodi di accesso e accesso degli account utente e i ruoli di controllo degli accessi.

- Se si desidera utilizzare HTTPS per un accesso Web sicuro, è necessario attivare SSL e installare un certificato digitale.

  Il `system services web show` il comando visualizza la configurazione del motore del protocollo web a livello di cluster.

#### A proposito di questa attività

Il `spi` il servizio web è attivato per impostazione predefinita ed è possibile disattivarlo manualmente (`vserver services web modify -vserver * -name spi -enabled false`).

Al ruolo "admin" viene concesso l'accesso a `spi` servizio web per impostazione predefinita e l'accesso può essere disattivato manualmente (`services web access delete -vserver` *`cluster_name`* `-name spi -role admin`).

#### Fasi

1. Puntare il browser Web su `spi` URL del servizio web in uno dei seguenti formati:
   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

`cluster-mgmt-LIF` È l'indirizzo IP della LIF di gestione del cluster.

2. Quando richiesto dal browser, inserire l'account utente e la password.

   Una volta autenticato l'account, il browser visualizza i collegamenti a `/mroot/etc/log/`, `/mroot/etc/crash/`, e. `/mroot/etc/mib/` directory di ciascun nodo del cluster.

### Accedere alla console di sistema di un nodo

Se un nodo si trova nel menu di boot o nel prompt dell'ambiente di boot, è possibile accedervi solo dalla console di sistema (chiamata anche *console seriale*). È possibile accedere alla console di sistema di un nodo da una connessione SSH all'SP del nodo o al cluster.

#### A proposito di questa attività

Sia SP che ONTAP offrono comandi che consentono di accedere alla console di sistema. Tuttavia, dal provider di servizi Internet, è possibile accedere solo alla console di sistema del proprio nodo. Dal cluster, è possibile accedere alla console di sistema di qualsiasi nodo del cluster.

#### Fasi

1. Accedere alla console di sistema di un nodo:

| Se si è in… | Immettere questo comando… |
|---|---|
| CLI SP del nodo | `system console` |
| CLI ONTAP | `system node run-console` |

2. Quando richiesto, accedere alla console di sistema.
3. Per uscire dalla console di sistema, premere Ctrl-D.

#### Esempi di accesso alla console di sistema

Nell'esempio riportato di seguito viene illustrato il risultato dell'immissione di `system console` Al prompt "SP node2". La console di sistema indica che node2 è in sospeso al prompt dell'ambiente di boot. Il `boot_ontap` Il comando viene immesso nella console per avviare il nodo su ONTAP. Premere Ctrl-D per uscire dalla console e tornare all'SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

Premere Ctrl-D per uscire dalla console di sistema.

```
Connection to 123.12.123.12 closed.
SP node2>
```

Nell'esempio riportato di seguito viene illustrato il risultato dell'immissione di `system node run-console` Comando da ONTAP per accedere alla console di sistema di node2, che si trova al prompt dell'ambiente di boot. Il `boot_ontap` Il comando viene immesso nella console per avviare node2 in ONTAP. Premere Ctrl-D per uscire dalla console e tornare a ONTAP.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

Premere Ctrl-D per uscire dalla console di sistema.

```
Connection to 123.12.123.12 closed.
cluster1::>
```

## Gestire i volumi root dei nodi e gli aggregati root

Il volume root di un nodo è un volume FlexVol installato in fabbrica o dal software di installazione. È riservato ai file di sistema, ai file di log e ai file principali. Il nome della directory è `/mroot`, accessibile solo attraverso la shell di sistema dal supporto tecnico. La dimensione minima del volume root di un nodo dipende dal modello di piattaforma.

### Panoramica delle regole che disciplinano i volumi root dei nodi e gli aggregati root

Il volume root di un nodo contiene directory e file speciali per quel nodo. L'aggregato root contiene il volume root. Alcune regole governano il volume root e l'aggregato root di un nodo.

- Le seguenti regole governano il volume root del nodo:
  - A meno che il supporto tecnico non lo richieda, non modificare la configurazione o il contenuto del volume root.
  - Non memorizzare i dati dell'utente nel volume root.

    L'archiviazione dei dati dell'utente nel volume root aumenta il tempo di giveback dello storage tra i nodi di una coppia ha.

  - È possibile spostare il volume root in un altro aggregato. Vedere [relocate-root].
- L'aggregato root è dedicato solo al volume root del nodo.

  ONTAP impedisce la creazione di altri volumi nell'aggregato root.

"NetApp Hardware Universe"

### Liberare spazio sul volume root di un nodo

Quando il volume root di un nodo è pieno o quasi pieno, viene visualizzato un messaggio di avviso. Il nodo non può funzionare correttamente quando il volume root è pieno. È possibile liberare spazio sul volume root di un nodo eliminando i file core dump, i file di traccia dei pacchetti e le copie Snapshot del volume root.

**Fasi**

1. Visualizzare i file core dump del nodo e i relativi nomi:

   ```
   system node coredump show
   ```

2. Eliminare i file core dump indesiderati dal nodo:

   ```
   system node coredump delete
   ```

3. Accedi al nodeshell:

   **`system node run -node nodename`**

   *`nodename`* è il nome del nodo di cui si desidera liberare spazio nel volume root.

4. Passa al livello di privilegio avanzato più incondiscendente dal nodeshell:

   **`priv set advanced`**

5. Visualizzare ed eliminare i file di traccia dei pacchetti del nodo attraverso il nodeshell:
   a. Visualizza tutti i file nel volume root del nodo:

      **`ls /etc`**

   b. Se vi sono file di traccia dei pacchetti (`*.trc`) si trovano nel volume root del nodo, eliminarli singolarmente:

      **`rm /etc/log/packet_traces/`*`file_name.trc`***

6. Identificare ed eliminare le copie Snapshot del volume root del nodo attraverso il nodeshell:
   a. Identificare il nome del volume root:

      **`vol status`**

      Il volume root è indicato dalla parola “root” nella colonna “Options” di `vol status` output del comando.

      Nell’esempio seguente, il volume root è `vol0`:

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   a. Visualizza copie Snapshot del volume root:

      **`snap list root_vol_name`**

   b. Eliminare le copie Snapshot del volume root indesiderate:

      **`snap delete root_vol_namesnapshot_name`**

7. Uscire dal nodeshell e tornare alla shell di clustershell:

   **`exit`**

#### Spostare i volumi root in nuovi aggregati

La procedura di sostituzione root migra l’aggregato root corrente in un altro set di dischi senza interruzioni.

**A proposito di questa attività**

Per spostare i volumi root, è necessario abilitare il failover dello storage. È possibile utilizzare `storage failover modify -node` *`nodename`* `-enable true` comando per abilitare il failover.

È possibile modificare la posizione del volume root in un nuovo aggregato nei seguenti scenari:

- Quando gli aggregati root non si trovano sul disco, si preferisce

- Quando si desidera riorganizzare i dischi collegati al nodo
- Quando si esegue una sostituzione degli shelf degli shelf di dischi EOS

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set privilege advanced
   ```

2. Spostare l'aggregato root:

   ```
   system node migrate-root -node nodename -disklist disklist -raid-type raid-type
   ```

   - **-nodo**

     Specifica il nodo proprietario dell'aggregato root che si desidera migrare.

   - **-disklist**

     Specifica l'elenco dei dischi su cui verrà creato il nuovo aggregato root. Tutti i dischi devono essere spare e di proprietà dello stesso nodo. Il numero minimo di dischi richiesto dipende dal tipo di RAID.

   - **-raid-type**

     Specifica il tipo RAID dell'aggregato root. Il valore predefinito è `raid-dp`.

3. Monitorare l'avanzamento del lavoro:

   ```
   job show -id jobid -instance
   ```

**Risultati**

Se tutti i controlli preliminari hanno esito positivo, il comando avvia un processo di sostituzione del volume root ed esce. Attendere il riavvio del nodo.

### Consente di avviare o interrompere una panoramica dei nodi

Potrebbe essere necessario avviare o arrestare un nodo per motivi di manutenzione o risoluzione dei problemi. È possibile eseguire questa operazione dall'interfaccia utente di ONTAP, dal prompt dell'ambiente di avvio o dall'interfaccia utente di SP.

Utilizzando il comando SP CLI `system power off` oppure `system power cycle` Per spegnere o spegnere e riaccendere un nodo potrebbe causare un arresto non corretto del nodo (chiamato anche *shutdown anomalo*) e non sostituire un arresto corretto mediante ONTAP `system node halt` comando.

#### Riavviare un nodo al prompt del sistema

È possibile riavviare un nodo in modalità normale dal prompt di sistema. Un nodo è configurato per l'avvio dal dispositivo di avvio, ad esempio una scheda PC CompactFlash.

**Fasi**

1. Se il cluster contiene quattro o più nodi, verificare che il nodo da riavviare non contenga epsilon:

a. Impostare il livello di privilegio su Advanced (avanzato):

   **`set -privilege advanced`**

b. Determinare quale nodo contiene epsilon:

   **`cluster show`**

   Il seguente esempio mostra che “node1” contiene epsilon:

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

a. Se il nodo da riavviare contiene epsilon, rimuovere epsilon dal nodo:

   **`cluster modify -node node_name -epsilon false`**

b. Assegnare epsilon a un nodo diverso che rimarrà attivo:

   **`cluster modify -node node_name -epsilon true`**

c. Tornare al livello di privilegio admin:

   **`set -privilege admin`**

2. Utilizzare `system node reboot` comando per riavviare il nodo.

   Se non si specifica `-skip-lif-migration` Il comando tenta di migrare i dati e le LIF di gestione del cluster in modo sincrono su un altro nodo prima del riavvio. Se la migrazione LIF non riesce o si interrompe, il processo di riavvio viene interrotto e ONTAP visualizza un errore per indicare che la migrazione LIF non è riuscita.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

   Il nodo avvia il processo di riavvio. Viene visualizzato il prompt di accesso di ONTAP, che indica che il processo di riavvio è stato completato.

#### Boot ONTAP al prompt dell’ambiente di boot

È possibile avviare la release corrente o la release di backup di ONTAP quando si è al prompt dell’ambiente di boot di un nodo.

**Fasi**

1. Accedere al prompt dell'ambiente di boot dal prompt del sistema di storage utilizzando `system node halt` comando.

   La console del sistema di storage visualizza il prompt dell'ambiente di boot.

2. Al prompt dell'ambiente di boot, immettere uno dei seguenti comandi:

| Per avviare… | Inserisci… |
|---|---|
| L'attuale release di ONTAP | `boot_ontap` |
| L'immagine principale di ONTAP dal dispositivo di avvio | `boot_primary` |
| Immagine di backup di ONTAP dal dispositivo di avvio | `boot_backup` |

   In caso di dubbi sull'immagine da utilizzare, è necessario utilizzarla `boot_ontap` in primo luogo.

#### Chiudere un nodo

È possibile arrestare un nodo se non risponde o se il personale di supporto lo ha indicato come parte delle attività di risoluzione dei problemi.

**Fasi**

1. Se il cluster contiene quattro o più nodi, verificare che il nodo da arrestare non contenga epsilon:

   a. Impostare il livello di privilegio su Advanced (avanzato):

      **`set -privilege advanced`**

   b. Determinare quale nodo contiene epsilon:

      **`cluster show`**

      Il seguente esempio mostra che "node1" contiene epsilon:

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

   a. Se il nodo da spegnere contiene epsilon, rimuovere epsilon dal nodo:

      **`cluster modify -node node_name -epsilon false`**

b. Assegnare epsilon a un nodo diverso che rimarrà attivo:

**`cluster modify -node node_name -epsilon true`**

c. Tornare al livello di privilegio admin:

**`set -privilege admin`**

2. Utilizzare `system node halt` comando per arrestare il nodo.

   Se non si specifica `-skip-lif-migration` Il comando tenta di migrare i dati e le LIF di gestione del cluster in modo sincrono su un altro nodo prima dello shutdown. Se la migrazione LIF non riesce o va in timeout, il processo di arresto viene interrotto e ONTAP visualizza un errore per indicare che la migrazione LIF non è riuscita.

   È possibile attivare manualmente un core dump con lo shutdown utilizzando entrambi `-dump` parametro.

   Nell'esempio seguente viene chiuso il nodo "node1" per la manutenzione dell'hardware:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

#### Gestire un nodo utilizzando il menu di boot

È possibile utilizzare il menu di avvio per correggere i problemi di configurazione su un nodo, reimpostare la password di amministratore, inizializzare i dischi, ripristinare la configurazione del nodo e ripristinare le informazioni di configurazione del nodo sul dispositivo di avvio.

> Se è in uso una coppia ha "Crittografia dei dischi SAS o NVMe (SED, NSE, FIPS)", è necessario seguire le istruzioni riportate nell'argomento "Ripristino di un'unità FIPS o SED in modalità non protetta" Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

**Fasi**

1. Riavviare il nodo per accedere al menu di avvio utilizzando `system node reboot` al prompt del sistema.

   Il nodo avvia il processo di riavvio.

2. Durante il processo di riavvio, premere Ctrl-C per visualizzare il menu di avvio quando richiesto.

   Il nodo visualizza le seguenti opzioni per il menu di boot:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

Opzione del menu di boot (2) l'avvio senza /etc/rc è obsoleto e non ha alcun effetto sul sistema.

3. Selezionare una delle seguenti opzioni immettendo il numero corrispondente:

| Per… | Selezionare… |
| --- | --- |
| Continuare ad avviare il nodo in modalità normale | 1) Avvio normale |
| Modificare la password del nodo, che è anche la password dell'account "admin" | 3) modificare la password |

| Per… | Selezionare… |
| --- | --- |
| Inizializzare i dischi del nodo e creare un volume root per il nodo | 4) pulire la configurazione e inizializzare tutti i dischi<br><br>Questa opzione di menu cancella tutti i dati presenti sui dischi del nodo e ripristina la configurazione del nodo alle impostazioni predefinite.<br><br>Selezionare questa voce di menu solo dopo che il nodo è stato rimosso da un cluster (non Unito) e non è stato Unito a un altro cluster.<br><br>Per un nodo con shelf di dischi interni o esterni, viene inizializzato il volume root sui dischi interni. Se non sono presenti shelf di dischi interni, viene inizializzato il volume root sui dischi esterni.<br><br>Per un sistema che esegue la virtualizzazione FlexArray con shelf di dischi interni o esterni, le LUN degli array non vengono inizializzate. Tutti i dischi nativi sugli shelf interni o esterni vengono inizializzati.<br><br>Per un sistema che esegue la virtualizzazione FlexArray con solo LUN di array e senza shelf di dischi interni o esterni, il volume root sulle LUN degli array di storage viene inizializzato, vedere "Installazione di FlexArray".<br><br>Se il nodo che si desidera inizializzare dispone di dischi partizionati per la partizione dei dati root, i dischi devono essere dispartizionati prima che il nodo possa essere inizializzato, vedere **9) Configurazione della partizione avanzata dei dischi** e. "Gestione di dischi e aggregati". |
| Eseguire operazioni di manutenzione di aggregati e dischi e ottenere informazioni dettagliate su aggregati e dischi. | 5) Avvio in modalità di manutenzione<br><br>Per uscire dalla modalità di manutenzione, utilizzare `halt` comando. |
| Ripristinare le informazioni di configurazione dal volume root del nodo al dispositivo di avvio, ad esempio una scheda PC CompactFlash | 6) aggiornare la flash dalla configurazione di backup<br><br>ONTAP memorizza alcune informazioni di configurazione del nodo sul dispositivo di avvio. Quando il nodo viene riavviato, viene eseguito automaticamente il backup delle informazioni sul dispositivo di avvio sul volume root del nodo. Se il dispositivo di boot risulta corrotto o deve essere sostituito, utilizzare questa opzione di menu per ripristinare le informazioni di configurazione dal volume root del nodo al dispositivo di boot. |

| Per… | Selezionare… |
| --- | --- |
| Installare il nuovo software sul nodo | 7) installare prima il nuovo software<br><br>Se il software ONTAP sul dispositivo di boot non include il supporto per lo storage array che si desidera utilizzare per il volume root, è possibile utilizzare questa opzione di menu per ottenere una versione del software che supporti lo storage array e installarla sul nodo.<br><br>Questa opzione di menu consente di installare una versione più recente del software ONTAP su un nodo che non dispone di un volume root installato. Non utilizzare questa opzione di menu per aggiornare ONTAP. |
| Riavviare il nodo | 8) riavviare il nodo |
| Dispartizionare tutti i dischi e rimuovere le informazioni di proprietà o pulire la configurazione e inizializzare il sistema con dischi interi o partizionati | 9) configurare la partizione avanzata dei dischi<br><br>A partire da ONTAP 9.2, l'opzione di partizione avanzata dei dischi offre funzionalità di gestione aggiuntive per i dischi configurati per la partizione root-data o root-data-data. Le seguenti opzioni sono disponibili dall'opzione di avvio 9:<br><br>`(9a) Unpartition all disks and remove their ownership information.`<br>`(9b) Clean configuration and initialize system with partitioned disks.`<br>`(9c) Clean configuration and initialize system with whole disks.`<br>`(9d) Reboot the node.`<br>`(9e) Return to main boot menu.` |

### Visualizza gli attributi del nodo

È possibile visualizzare gli attributi di uno o più nodi nel cluster, ad esempio il nome, il proprietario, la posizione, numero di modello, numero di serie, durata dell'esecuzione del nodo, stato di salute e idoneità a partecipare a un cluster.

#### Fasi

1. Per visualizzare gli attributi di un nodo specifico o di tutti i nodi di un cluster, utilizzare `system node show` comando.

#### Esempio di visualizzazione di informazioni su un nodo

Nell'esempio seguente vengono visualizzate informazioni dettagliate sul nodo 1:

```
cluster1::> system node show -node node1
                          Node: node1
                         Owner: Eng IT
                      Location: Lab 5
                         Model: model_number
                 Serial Number: 12345678
                     Asset Tag: -
                        Uptime: 23 days 04:42
               NVRAM System ID: 118051205
                     System ID: 0118051205
                        Vendor: NetApp
                        Health: true
                   Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

#### Modificare gli attributi del nodo

È possibile modificare gli attributi di un nodo in base alle esigenze. Gli attributi che è possibile modificare includono le informazioni sul proprietario del nodo, le informazioni sulla posizione, il tag delle risorse e l'idoneità a partecipare al cluster.

##### A proposito di questa attività

L'idoneità di un nodo a partecipare al cluster può essere modificata a livello di privilegio avanzato utilizzando `-eligibility` del parametro `system node modify` oppure `cluster modify` comando. Se si imposta l'idoneità di un nodo su `false`, il nodo diventa inattivo nel cluster.

> Non è possibile modificare localmente l'idoneità del nodo. Deve essere modificato da un nodo diverso. L'eleggienza del nodo non può essere modificata anche con una configurazione cluster ha.

> Evitare di impostare l'idoneità di un nodo su `false`, ad eccezione di situazioni come il ripristino della configurazione del nodo o la manutenzione prolungata del nodo. L'accesso AI dati SAN e NAS al nodo potrebbe essere compromesso quando il nodo non è idoneo.

##### Fasi

1. Utilizzare `system node modify` per modificare gli attributi di un nodo.

##### Esempio di modifica degli attributi del nodo

Il seguente comando modifica gli attributi del nodo "node1". Il proprietario del nodo è impostato su "Joe Smith" e il relativo tag asset è impostato su "js1234":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

### Rinominare un nodo

È possibile modificare il nome di un nodo in base alle esigenze.

#### Fasi

1. Per rinominare un nodo, utilizzare `system node rename` comando.

   Il `-newname` parametro specifica il nuovo nome del nodo. Il `system node rename` la pagina man descrive le regole per specificare il nome del nodo.

   Se si desidera rinominare più nodi nel cluster, è necessario eseguire il comando per ciascun nodo singolarmente.

   > Il nome del nodo non può essere “all” perché “all” è un nome riservato al sistema.

#### Esempio di ridenominazione di un nodo

Il seguente comando rinomina il nodo “node1” in “node1a”:

```
cluster1::> system node rename -node node1 -newname node1a
```

### Gestisci cluster a nodo singolo

Un cluster a nodo singolo è un’implementazione speciale di un cluster in esecuzione su un nodo standalone. I cluster a nodo singolo non sono consigliati, in quanto non forniscono ridondanza. Se il nodo si guasta, l’accesso ai dati viene perso.

> Per la tolleranza agli errori e le operazioni senza interruzioni, è consigliabile configurare il cluster con "Alta disponibilità (coppie ha)".

Se scegli di configurare o eseguire l’upgrade di un cluster a nodo singolo, devi conoscere i seguenti aspetti:

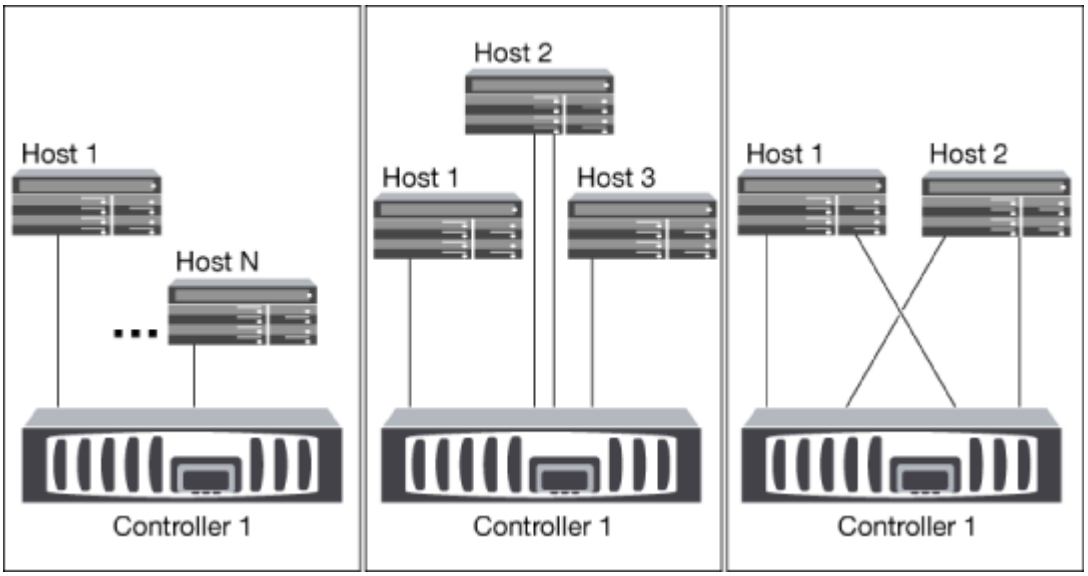
- La crittografia del volume root non è supportata su cluster a nodo singolo.
- Se si rimuovono i nodi per avere un cluster a nodo singolo, è necessario modificare le porte del cluster per erogare traffico dati modificando le porte del cluster in modo che siano porte dati e creando quindi LIF dati sulle porte per dati.
- Per i cluster a nodo singolo, puoi specificare la destinazione di backup della configurazione durante la configurazione del software. Dopo l’installazione, è possibile modificare tali impostazioni utilizzando i comandi ONTAP.
- Se al nodo sono connessi più host, è possibile configurare ciascun host con un sistema operativo diverso, ad esempio Windows o Linux. Se sono presenti più percorsi dall’host al controller, ALUA deve essere abilitato sull’host.

#### Modi per configurare host SAN iSCSI con nodi singoli

È possibile configurare gli host SAN iSCSI in modo che si connettano direttamente a un singolo nodo o tramite uno o più switch IP. Il nodo può avere più connessioni iSCSI allo switch.

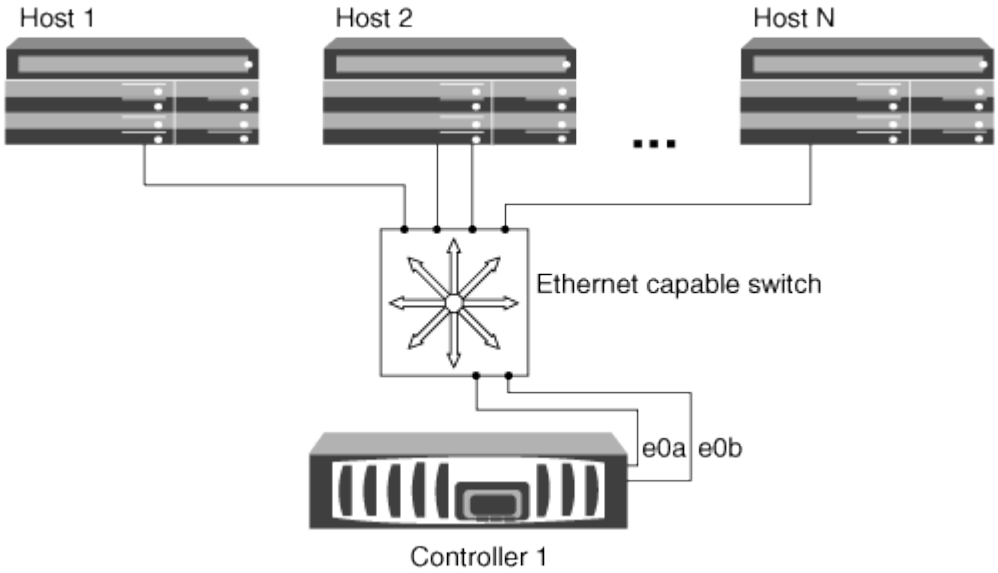
**Configurazioni a nodo singolo direct-attached**

Nelle configurazioni a nodo singolo direct-attached, uno o più host sono connessi direttamente al nodo.



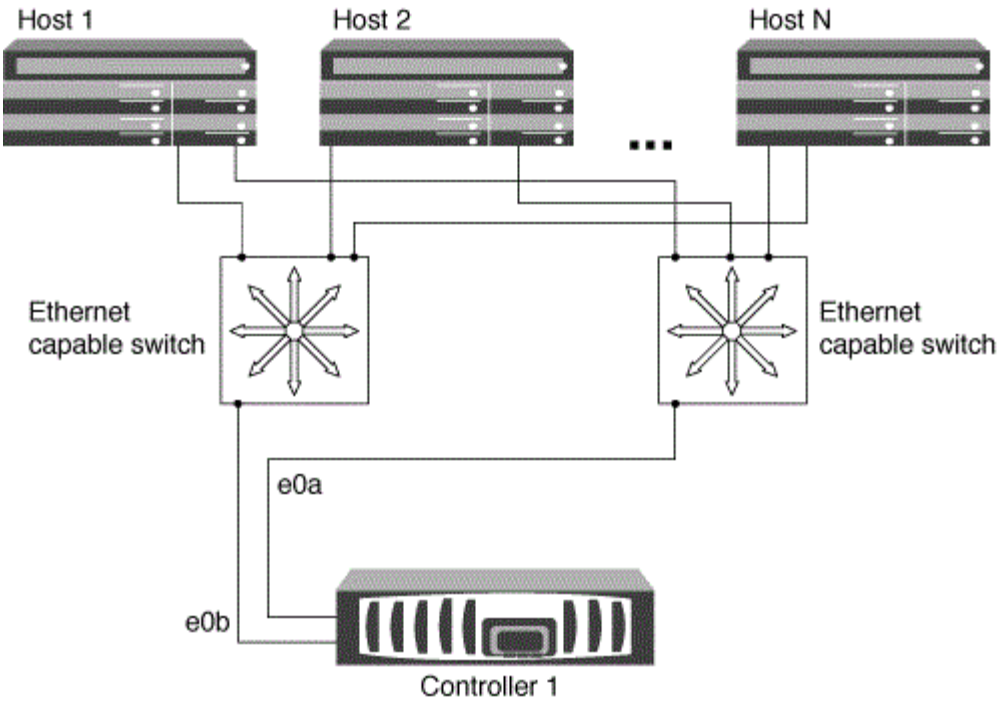

**Configurazioni a nodo singolo di rete**

Nelle configurazioni a nodo singolo di rete, uno switch connette un singolo nodo a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.




**Configurazioni multi-rete a nodo singolo**

Nelle configurazioni multi-network a nodo singolo, due o più switch collegano un singolo nodo a uno o più host. Poiché esistono più switch, questa configurazione è completamente ridondante.




**Modi per configurare host FC e SAN FC-NVMe con nodi singoli**

È possibile configurare host FC e SAN FC-NVMe con nodi singoli attraverso uno o più fabric. N-Port ID Virtualization (NPIV) è necessario e deve essere attivato su tutti gli switch FC del fabric. Non è possibile collegare direttamente host SAN FC o FC-NMVE a nodi singoli senza utilizzare uno switch FC.

**Configurazioni single-fabric a nodo singolo**

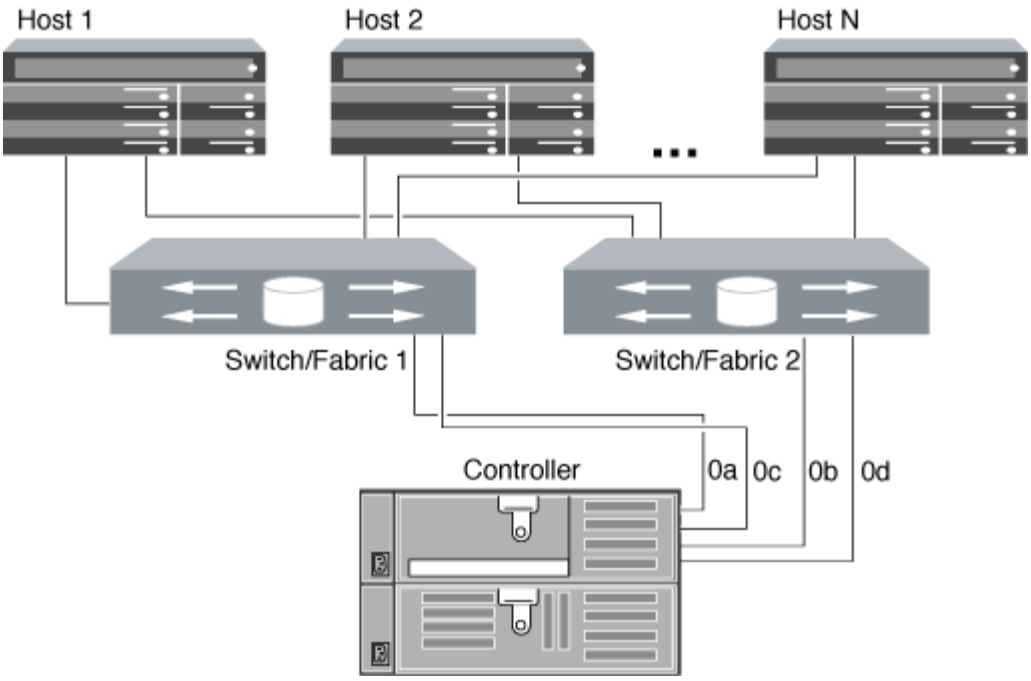
Nelle configurazioni a nodo singolo con fabric singolo, è disponibile uno switch che collega un singolo nodo a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.

Nelle configurazioni a nodo singolo con fabric singolo, il software di multipathing non è necessario se si dispone di un solo percorso dall'host al nodo.

**Configurazioni multi-nodo singolo**

Nelle configurazioni multi-nodo singolo, sono presenti due o più switch che collegano un singolo nodo a uno o più host. Per semplicità, la figura seguente mostra una configurazione multi-nodo singolo con solo due fabric, ma è possibile avere due o più fabric in qualsiasi configurazione multifabrica. In questa figura, lo storage controller è montato nello chassis superiore e quello inferiore può essere vuoto o può avere un modulo IOMX, come in questo esempio.

Le porte di destinazione FC (0a, 0c, 0b, 0d) nelle figure sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.




**Informazioni correlate**

"Report tecnico NetApp 4684: Implementazione e configurazione di SAN moderne con NVMe-of"

#### Upgrade ONTAP per cluster a nodo singolo

A partire da ONTAP 9,2, puoi utilizzare l'interfaccia a riga di comando di ONTAP per eseguire un update automatico di un cluster a nodo singolo. Poiché i cluster a nodo singolo non hanno ridondanza, gli aggiornamenti sono sempre di tipo disgregativo. Non è possibile eseguire upgrade con interruzioni usando System Manager.

**Prima di iniziare**

È necessario completare l'aggiornamento "preparazione" fasi.

**Fasi**

1. Eliminare il pacchetto software ONTAP precedente:

```
cluster image package delete -version previous_package_version
```

2. Scarica il pacchetto software ONTAP di destinazione:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. Verificare che il pacchetto software sia disponibile nel repository dei pacchetti del cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. Verificare che il cluster sia pronto per l'aggiornamento:

```
cluster image validate -version package_version_number
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Monitorare l'avanzamento della convalida:

```
cluster image show-update-progress
```

6. Completare tutte le azioni richieste identificate dalla convalida.
7. Facoltativamente, generare una stima dell'aggiornamento del software:

```
cluster image update -version package_version_number -estimate-only
```

La stima dell'aggiornamento software visualizza i dettagli relativi a ciascun componente da aggiornare e la durata stimata dell'aggiornamento.

8. Eseguire l'aggiornamento del software:

```
cluster image update -version package_version_number
```

> Se si verifica un problema, l'aggiornamento viene messo in pausa e richiede di intraprendere un'azione correttiva. È possibile utilizzare il comando show-update-progress dell'immagine del cluster per visualizzare i dettagli relativi a eventuali problemi e allo stato di avanzamento dell'aggiornamento. Dopo aver corretto il problema, è possibile riprendere l'aggiornamento utilizzando il comando resume-update dell'immagine del cluster.

9. Visualizzare l'avanzamento dell'aggiornamento del cluster:

```
cluster image show-update-progress
```

Il nodo viene riavviato come parte dell'aggiornamento e non è possibile accedervi durante il riavvio.

10. Attivare una notifica:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

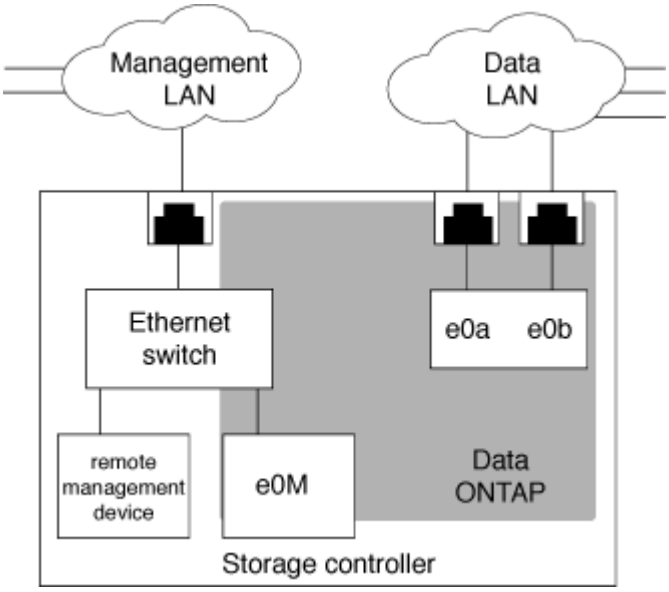
Se il cluster non è configurato per l'invio di messaggi, una copia della notifica viene salvata localmente.

## Configurare la rete SP/BMC

### Isolare il traffico di rete di gestione

Si consiglia di configurare SP/BMC e l'interfaccia di gestione e0M su una subnet dedicata al traffico di gestione. L'esecuzione del traffico dati sulla rete di gestione può causare il peggioramento delle performance e problemi di routing.

La porta Ethernet di gestione della maggior parte dei controller di storage (indicata dall'icona di una chiave a tubo sul retro dello chassis) è collegata a uno switch Ethernet interno. Lo switch interno fornisce la connettività a SP/BMC e all'interfaccia di gestione e0M, che è possibile utilizzare per accedere al sistema di storage tramite protocolli TCP/IP come Telnet, SSH e SNMP.




Se si intende utilizzare sia il dispositivo di gestione remota che e0M, è necessario configurarli sulla stessa subnet IP. Poiché si tratta di interfacce a bassa larghezza di banda, la procedura migliore consiste nel configurare SP/BMC ed e0M su una subnet dedicata al traffico di gestione.

Se non è possibile isolare il traffico di gestione o se la rete di gestione dedicata è insolitamente grande, si consiglia di mantenere il volume di traffico di rete il più basso possibile. Un traffico broadcast o multicast in entrata eccessivo può compromettere le prestazioni di SP/BMC.

Alcuni storage controller, come AFF A800, dispongono di due porte esterne, una per BMC e l'altra per e0M. Per questi controller, non è necessario configurare BMC ed e0M sulla stessa subnet IP.

**Considerazioni per la configurazione di rete SP/BMC**

## È possibile attivare la configurazione di rete automatica a livello di cluster per l'SP (consigliato). È inoltre possibile lasciare disattivata la configurazione di rete automatica SP (impostazione predefinita) e gestire la configurazione di rete SP manualmente a livello di nodo. Esistono alcune considerazioni per ciascun caso.

Questo argomento si applica sia all'SP che al BMC.

La configurazione automatica della rete SP consente all'SP di utilizzare le risorse di indirizzo (inclusi l'indirizzo IP, la subnet mask e l'indirizzo del gateway) della subnet specificata per configurare automaticamente la rete. Con la configurazione automatica della rete SP, non è necessario assegnare manualmente gli indirizzi IP per l'SP di ciascun nodo. Per impostazione predefinita, la configurazione di rete automatica SP è disattivata, poiché l'abilitazione della configurazione richiede che la subnet venga utilizzata per la configurazione sia definita nel cluster.

Se si attiva la configurazione di rete automatica SP, si applicano le seguenti considerazioni e scenari:

- Se l'SP non è mai stato configurato, la rete SP viene configurata automaticamente in base alla subnet specificata per la configurazione automatica della rete SP.
- Se l'SP è stato precedentemente configurato manualmente o se la configurazione di rete SP esistente si basa su una subnet diversa, la rete SP di tutti i nodi del cluster viene riconfigurata in base alla subnet specificata nella configurazione di rete automatica dell'SP.

  La riconfigurazione potrebbe comportare l'assegnazione di un indirizzo diverso al SP, che potrebbe avere un impatto sulla configurazione DNS e sulla capacità di risolvere i nomi host SP. Di conseguenza, potrebbe essere necessario aggiornare la configurazione DNS.

- Un nodo che si unisce al cluster utilizza la subnet specificata per configurare automaticamente la propria rete SP.
- Il `system service-processor network modify` Il comando non consente di modificare l'indirizzo IP SP.

  Quando la configurazione di rete automatica SP è attivata, il comando consente solo di attivare o disattivare l'interfaccia di rete SP.

  - Se la configurazione di rete automatica SP era precedentemente abilitata, disattivando l'interfaccia di rete SP la risorsa di indirizzo assegnata viene rilasciata e restituita alla subnet.
  - Se si disattiva e si riattiva l'interfaccia di rete SP, quest'ultima potrebbe essere riconfigurata con un indirizzo diverso.

Se la configurazione di rete automatica SP è disattivata (impostazione predefinita), si applicano le seguenti situazioni e considerazioni:

- Se l'SP non è mai stato configurato, per impostazione predefinita la configurazione di rete IPv4 SP utilizza DHCP IPv4 e IPv6 è disattivato.

Un nodo che si unisce al cluster utilizza anche IPv4 DHCP per la configurazione di rete SP per impostazione predefinita.

- Il `system service-processor network modify` Il comando consente di configurare l'indirizzo IP SP di un nodo.

  Quando si tenta di configurare manualmente la rete SP con gli indirizzi assegnati a una subnet, viene visualizzato un messaggio di avviso. Ignorare l'avviso e procedere con l'assegnazione manuale dell'indirizzo potrebbe comportare uno scenario con indirizzi duplicati.

Se la configurazione di rete automatica SP viene disattivata dopo essere stata attivata in precedenza, si applicano le seguenti situazioni e considerazioni:

- Se la configurazione di rete automatica SP ha la famiglia di indirizzi IPv4 disattivata, la rete SP IPv4 utilizza per impostazione predefinita DHCP e il `system service-processor network modify` Il comando consente di modificare la configurazione SP IPv4 per i singoli nodi.
- Se la configurazione di rete automatica SP ha la famiglia di indirizzi IPv6 disattivata, anche la rete IPv6 SP viene disattivata e l' `system service-processor network modify` Il comando consente di attivare e modificare la configurazione di IPv6 SP per i singoli nodi.

**Attivare la configurazione automatica di rete SP/BMC**

È preferibile abilitare l'SP per l'utilizzo della configurazione di rete automatica rispetto alla configurazione manuale della rete SP. Poiché la configurazione automatica della rete SP è estesa a tutto il cluster, non è necessario gestire manualmente la rete SP per i singoli nodi.

Questa attività si applica sia all'SP che al BMC.

- La subnet che si desidera utilizzare per la configurazione automatica della rete SP deve essere già definita nel cluster e non deve presentare conflitti di risorse con l'interfaccia di rete SP.

  Il `network subnet show` il comando visualizza le informazioni sulla subnet del cluster.

  Il parametro che forza l'associazione della subnet (il `-force-update-lif-associations` del parametro `network subnet` ) è supportato solo su LIF di rete e non sull'interfaccia di rete SP.

- Se si desidera utilizzare le connessioni IPv6 per l'SP, IPv6 deve essere già configurato e abilitato per ONTAP.

  Il `network options ipv6 show` Il comando visualizza lo stato corrente delle impostazioni IPv6 per ONTAP.

**Fasi**

1. Specificare la famiglia di indirizzi IPv4 o IPv6 e il nome della subnet che si desidera utilizzare con l'SP `system service-processor network auto-configuration enable` comando.
2. Visualizzare la configurazione di rete automatica SP utilizzando `system service-processor network auto-configuration show` comando.
3. Se in seguito si desidera disattivare o riabilitare l'interfaccia di rete SP IPv4 o IPv6 per tutti i nodi che si trovano in quorum, utilizzare `system service-processor network modify` con il `-address`

`-family` [`IPv4`|`IPv6`] e. `-enable` [`true`|`false`].

Quando la configurazione di rete automatica SP è attivata, non è possibile modificare l'indirizzo IP SP per un nodo che si trova in quorum. È possibile attivare o disattivare solo l'interfaccia di rete SP IPv4 o IPv6.

Se un nodo non ha raggiunto il quorum, è possibile modificare la configurazione di rete SP del nodo, incluso l'indirizzo IP SP, eseguendo `system service-processor network modify` Dal nodo e confermando che si desidera eseguire l'override della configurazione di rete automatica SP per il nodo. Tuttavia, quando il nodo si unisce al quorum, viene eseguita la riconfigurazione automatica dell'SP per il nodo in base alla subnet specificata.

### Configurare la rete SP/BMC manualmente

## Se non si dispone della configurazione di rete automatica impostata per l'SP, è necessario configurare manualmente la rete SP di un nodo affinché l'SP sia accessibile utilizzando un indirizzo IP.

#### Di cosa hai bisogno

Se si desidera utilizzare le connessioni IPv6 per l'SP, IPv6 deve essere già configurato e abilitato per ONTAP. Il `network options ipv6` I comandi gestiscono le impostazioni IPv6 per ONTAP.

> Questa attività si applica sia all'SP che al BMC.

È possibile configurare l'SP in modo che utilizzi IPv4, IPv6 o entrambi. La configurazione SP IPv4 supporta l'indirizzamento statico e DHCP, mentre la configurazione SP IPv6 supporta solo l'indirizzamento statico.

Se è stata impostata la configurazione di rete automatica SP, non è necessario configurare manualmente la rete SP per i singoli nodi e il `system service-processor network modify` Il comando consente di attivare o disattivare solo l'interfaccia di rete SP.

#### Fasi

1. Configurare la rete SP per un nodo utilizzando `system service-processor network modify` comando.
   - Il `-address-family` Parametro specifica se modificare la configurazione IPv4 o IPv6 dell'SP.
   - Il `-enable` Il parametro attiva l'interfaccia di rete della famiglia di indirizzi IP specificata.
   - Il `-dhcp` Parametro specifica se utilizzare la configurazione di rete dal server DHCP o dall'indirizzo di rete fornito.

     È possibile attivare DHCP (tramite l'impostazione `-dhcp` a. `v4`) Solo se si utilizza IPv4. Non è possibile attivare DHCP per le configurazioni IPv6.
   - Il `-ip-address` Parametro specifica l'indirizzo IP pubblico per l'SP.

     Quando si tenta di configurare manualmente la rete SP con gli indirizzi assegnati a una subnet, viene visualizzato un messaggio di avviso. Ignorare l'avviso e procedere con l'assegnazione manuale dell'indirizzo potrebbe causare un'assegnazione duplicata dell'indirizzo.
   - Il `-netmask` Parametro specifica la netmask per l'SP (se si utilizza IPv4).
   - Il `-prefix-length` Parametro specifica la lunghezza del prefisso di rete della subnet mask per l'SP (se si utilizza IPv6).

- Il `-gateway` Parametro specifica l'indirizzo IP del gateway per l'SP.

2. Configurare la rete SP per i nodi rimanenti nel cluster ripetendo il passaggio 1.
3. Visualizzare la configurazione di rete SP e verificare lo stato di configurazione SP utilizzando `system service-processor network show` con il `-instance` oppure `-field setup-status` parametri.

   Lo stato di setup SP per un nodo può essere uno dei seguenti:

   - `not-setup` — non configurato
   - `succeeded` — Configurazione riuscita
   - `in-progress` — Configurazione in corso
   - `failed` — Configurazione non riuscita

**Esempio di configurazione della rete SP**

Nell'esempio seguente viene configurato l'SP di un nodo per l'utilizzo di IPv4, viene attivato l'SP e viene visualizzata la configurazione di rete SP per verificare le impostazioni:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                              Node: node1
                      Address Type: IPv4
                  Interface Enabled: true
                     Type of Device: SP
                             Status: online
                        Link Status: up
                        DHCP Status: none
                         IP Address: 192.168.123.98
                        MAC Address: ab:cd:ef:fe:ed:02
                            Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

#### Modificare la configurazione del servizio API SP

L'API SP è un'API di rete sicura che consente a ONTAP di comunicare con l'SP sulla rete. È possibile modificare la porta utilizzata dal servizio API SP, rinnovare i certificati utilizzati dal servizio per la comunicazione interna o disattivare completamente il servizio. È necessario modificare la configurazione solo in situazioni rare.

#### A proposito di questa attività

- Il servizio API SP utilizza la porta `50000` per impostazione predefinita.

  È possibile modificare il valore della porta se, ad esempio, ci si trova in un'impostazione di rete dove porta `50000` Viene utilizzato per la comunicazione da parte di un'altra applicazione di rete oppure si desidera differenziare tra il traffico proveniente da altre applicazioni e il traffico generato dal servizio API SP.

- I certificati SSL e SSH utilizzati dal servizio API SP sono interni al cluster e non distribuiti esternamente.

Nell'improbabile eventualità che i certificati vengano compromessi, è possibile rinnovarli.

- Il servizio API SP è attivato per impostazione predefinita.

  È necessario disattivare il servizio API SP solo in situazioni rare, ad esempio in una LAN privata in cui l'SP non è configurato o utilizzato e si desidera disattivare il servizio.

  Se il servizio API SP è disattivato, l'API non accetta connessioni in entrata. Inoltre, funzionalità come gli aggiornamenti del firmware SP basati sulla rete e la raccolta di log SP "dOwn System" basata sulla rete non sono più disponibili. Il sistema passa all'utilizzo dell'interfaccia seriale.

**Fasi**

1. Passare al livello di privilegio avanzato utilizzando `set -privilege advanced` comando.
2. Modificare la configurazione del servizio API SP:

| Se si desidera… | Utilizzare il seguente comando… |
|---|---|
| Modificare la porta utilizzata dal servizio API SP | `system service-processor api-service modify` con `-port` {`49152..65535`} parametro |
| Rinnovare i certificati SSL e SSH utilizzati dal servizio API SP per la comunicazione interna | • Per ONTAP 9.5 o versioni successive `system service-processor api-service renew-internal-certificate`<br>• Per ONTAP 9.4 e versioni precedenti<br>• `system service-processor api-service renew-certificates`<br><br>Se non viene specificato alcun parametro, vengono rinnovati solo i certificati host (inclusi i certificati client e server).<br><br>Se il `-renew-all true` Viene specificato il parametro, i certificati host e il certificato CA principale vengono rinnovati. |
| com | |
| Disattivare o riabilitare il servizio API SP | `system service-processor api-service modify` con `-is-enabled` {`true` |

3. Visualizzare la configurazione del servizio API SP utilizzando `system service-processor api-service show` comando.

## Gestire i nodi in remoto utilizzando SP/BMC

### Gestire un nodo in remoto utilizzando la panoramica SP/BMC

È possibile gestire un nodo in remoto utilizzando un controller integrato, denominato

Service Processor (SP) o Baseboard Management Controller (BMC). Questo controller di gestione remota è incluso in tutti gli attuali modelli di piattaforma. Il controller rimane operativo indipendentemente dallo stato operativo del nodo.

Le seguenti piattaforme supportano BMC anziché SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700
- AFF A400
- AFF A320
- AFF A220
- AFF C190

**A proposito di SP**

Service Processor (SP) è un dispositivo di gestione remota che consente di accedere, monitorare e risolvere i problemi di un nodo in remoto.

Le funzionalità principali del SP includono:

- L'SP consente di accedere a un nodo in remoto per diagnosticare, spegnere, spegnere e riaccendere o riavviare il nodo, indipendentemente dallo stato del controller del nodo.

  L'SP è alimentato da una tensione di standby, disponibile a condizione che il nodo abbia alimentazione in ingresso da almeno uno dei suoi alimentatori.

  È possibile accedere al SP utilizzando un'applicazione client Secure Shell da un host di amministrazione. È quindi possibile utilizzare l'interfaccia CLI SP per monitorare e risolvere i problemi del nodo in remoto. Inoltre, è possibile utilizzare l'SP per accedere alla console seriale ed eseguire i comandi ONTAP in remoto.

  È possibile accedere all'SP dalla console seriale o dalla console seriale dall'SP. SP consente di aprire contemporaneamente una sessione CLI SP e una sessione console separata.

  Ad esempio, quando un sensore di temperatura diventa estremamente alto o basso, ONTAP attiva l'SP per spegnere la scheda madre in modo corretto. La console seriale non risponde, ma è comunque possibile premere Ctrl-G sulla console per accedere alla CLI SP. È quindi possibile utilizzare `system power on` oppure `system power cycle` Comando dall'SP per accendere o spegnere e riaccendere il nodo.

- L'SP monitora i sensori ambientali e registra gli eventi per aiutarti a intraprendere azioni di servizio tempestive ed efficaci.

  L'SP monitora i sensori ambientali, ad esempio le temperature del nodo, le tensioni, le correnti e la velocità della ventola. Quando un sensore ambientale ha raggiunto una condizione anomala, l'SP registra le letture anomale, notifica il problema a ONTAP e invia avvisi e notifiche "sistema proprio `d`" secondo necessità attraverso un messaggio AutoSupport, indipendentemente dal fatto che il nodo possa inviare messaggi AutoSupport.

L'SP registra anche eventi come l'avanzamento dell'avvio, le modifiche delle FRU (Field Replaceable Unit), gli eventi generati da ONTAP e la cronologia dei comandi SP. È possibile richiamare manualmente un messaggio AutoSupport per includere i file di log SP raccolti da un nodo specifico.

Oltre a generare questi messaggi per conto di un nodo inattivo e allegare informazioni diagnostiche aggiuntive ai messaggi AutoSupport, il SP non ha alcun effetto sulla funzionalità AutoSupport. Le impostazioni di configurazione di AutoSupport e il comportamento del contenuto dei messaggi sono ereditati da ONTAP.

> L'SP non si basa su `-transport` impostazione dei parametri di `system node autosupport modify` comando per inviare notifiche. L'SP utilizza solo il protocollo SMTP (Simple Mail Transport Protocol) e richiede la configurazione AutoSupport dell'host per includere le informazioni sull'host di posta.

Se SNMP è attivato, l'SP genera trap SNMP per gli host trap configurati per tutti gli eventi "dproprio sistema".

- L'SP dispone di un buffer di memoria non volatile che memorizza fino a 4,000 eventi in un registro eventi di sistema (SEL) per facilitare la diagnosi dei problemi.

  Il SEL memorizza ogni voce del registro di controllo come evento di audit. Viene memorizzato nella memoria flash integrata dell'SP. L'elenco degli eventi del SEL viene inviato automaticamente dall'SP a destinatari specificati tramite un messaggio AutoSupport.

  Il SEL contiene le seguenti informazioni:

  - Eventi hardware rilevati dall'SP, ad esempio lo stato del sensore relativo a alimentatori, tensione o altri componenti
  - Errori rilevati dall'SP, ad esempio un errore di comunicazione, un guasto alla ventola o un errore della memoria o della CPU
  - Eventi software critici inviati al SP dal nodo, ad esempio un panico, un errore di comunicazione, un errore di avvio o un "dsistema proprio" attivato dall'utente come risultato dell'emissione del SP `system reset` oppure `system power cycle` comando
- SP monitora la console seriale indipendentemente dal fatto che gli amministratori siano connessi o connessi alla console.

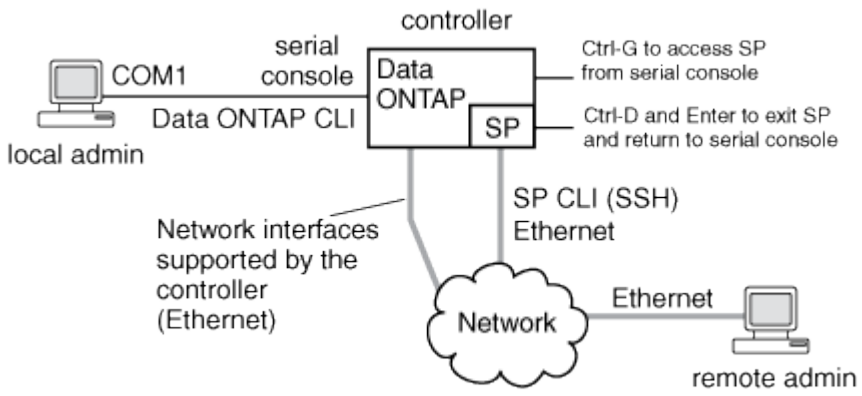
  Quando i messaggi vengono inviati alla console, il SP li memorizza nel log della console. Il registro della console rimane attivo fino a quando l'SP è alimentato da uno degli alimentatori del nodo. Poiché l'SP funziona con l'alimentazione in standby, rimane disponibile anche quando il nodo viene spento e riacceso o spento.

- Il Takeover assistito dall'hardware è disponibile se il SP è configurato.
- Il servizio API SP consente a ONTAP di comunicare con il provider di servizi di rete.

  Il servizio migliora la gestione ONTAP dell'SP supportando funzionalità basate sulla rete, ad esempio l'utilizzo dell'interfaccia di rete per l'aggiornamento del firmware SP, consentendo a un nodo di accedere alla funzionalità SP di un altro nodo o alla console di sistema e caricando il registro SP da un altro nodo.

  È possibile modificare la configurazione del servizio API SP modificando la porta utilizzata dal servizio, rinnovando i certificati SSL e SSH utilizzati dal servizio per la comunicazione interna o disattivando completamente il servizio.

Il seguente diagramma illustra l'accesso a ONTAP e all'SP di un nodo. L'accesso all'interfaccia SP avviene tramite la porta Ethernet (indicata dall'icona di una chiave a tubo sul retro dello chassis):




**Funzionalità di Baseboard Management Controller**

A partire da ONTAP 9.1, su alcune piattaforme hardware, il software viene personalizzato per supportare un nuovo controller integrato denominato Baseboard Management Controller (BMC). BMC dispone di comandi CLI (Command-Line Interface) che è possibile utilizzare per gestire il dispositivo in remoto.

Il BMC funziona in modo simile al Service Processor (SP) e utilizza molti degli stessi comandi. BMC consente di effettuare le seguenti operazioni:

- Configurare le impostazioni di rete BMC.
- Accedere a un nodo in remoto ed eseguire attività di gestione dei nodi come diagnosticare, spegnere, spegnere e riaccendere o riavviare il nodo.

Esistono alcune differenze tra SP e BMC:

- Il BMC controlla completamente il monitoraggio ambientale di elementi di alimentazione, elementi di raffreddamento, sensori di temperatura, sensori di tensione e sensori di corrente. Il BMC riporta le informazioni del sensore a ONTAP tramite IPMI.
- Alcuni comandi di alta disponibilità (ha) e storage sono diversi.
- BMC non invia messaggi AutoSupport.

Gli aggiornamenti automatici del firmware sono disponibili anche quando si esegue ONTAP 9.2 GA o versioni successive con i seguenti requisiti:

- È necessario installare la revisione del firmware BMC 1.15 o successiva.

  È necessario un aggiornamento manuale per aggiornare il firmware BMC dalla versione 1.12 alla 1.15 o successiva.

- BMC si riavvia automaticamente al termine di un aggiornamento del firmware.

  Le operazioni del nodo non vengono influenzate durante il riavvio di BMC.

#### Metodi di gestione degli aggiornamenti del firmware SP/BMC

ONTAP include un'immagine del firmware SP denominata *immagine di riferimento*. Se successivamente diventa disponibile una nuova versione del firmware SP, è possibile scaricarla e aggiornarla alla versione scaricata senza aggiornare la versione di ONTAP.

> Questo argomento si applica sia all'SP che al BMC.

ONTAP offre i seguenti metodi per la gestione degli aggiornamenti del firmware SP:

- La funzionalità di aggiornamento automatico SP è attivata per impostazione predefinita, consentendo l'aggiornamento automatico del firmware SP nei seguenti scenari:
  - Quando si esegue l'aggiornamento a una nuova versione di ONTAP

    Il processo di aggiornamento di ONTAP include automaticamente l'aggiornamento del firmware SP, a condizione che la versione del firmware SP fornita con ONTAP sia più recente della versione SP in esecuzione sul nodo.

    > ONTAP rileva un aggiornamento automatico SP guasto e attiva un'azione correttiva per riprovare l'aggiornamento automatico SP fino a tre volte. Se tutti e tre i tentativi falliscono, consultare l'articolo della Knowledge base: Health Monitor SPAutoUpgrade FailedMajorAlert SP upgrade fails - AutoSupport message.

  - Quando si scarica una versione del firmware SP dal NetApp Support Site e la versione scaricata è più recente di quella attualmente in esecuzione sul SP
  - Quando si esegue il downgrade o si torna a una versione precedente di ONTAP

    Il firmware SP viene aggiornato automaticamente alla versione più recente compatibile supportata dalla versione di ONTAP a cui si è eseguito il ripristino o il downgrade. Non è richiesto un aggiornamento manuale del firmware SP.

  È possibile disattivare la funzionalità di aggiornamento automatico SP utilizzando `system service-processor image modify` comando. Tuttavia, si consiglia di lasciare attivata la funzionalità. La disattivazione della funzionalità può causare combinazioni non ottimali o non qualificate tra l'immagine ONTAP e l'immagine del firmware SP.

- ONTAP consente di attivare manualmente un aggiornamento SP e di specificare la modalità di esecuzione dell'aggiornamento utilizzando `system service-processor image update` comando.

  È possibile specificare le seguenti opzioni:

  - Il pacchetto firmware SP da utilizzare (`-package`)

    È possibile aggiornare il firmware SP a un pacchetto scaricato specificando il nome del file del pacchetto. Il progresso `system image package show` Comando Visualizza tutti i file di pacchetto (inclusi i file per il pacchetto firmware SP) disponibili su un nodo.

  - Se utilizzare il pacchetto firmware SP di base per l'aggiornamento SP (`-baseline`)

    È possibile aggiornare il firmware SP alla versione di base fornita con la versione attualmente in esecuzione di ONTAP.

> Se si utilizzano alcune opzioni o parametri di aggiornamento più avanzati, le impostazioni di configurazione del BMC potrebbero essere temporaneamente cancellate. Dopo il riavvio, ONTAP può impiegare fino a 10 minuti per ripristinare la configurazione BMC.

- ONTAP consente di visualizzare lo stato dell'ultimo aggiornamento del firmware SP attivato da ONTAP utilizzando `system service-processor image update-progress show` comando.

Qualsiasi connessione esistente all'SP viene interrotta quando il firmware dell'SP viene aggiornato. Questo è il caso se l'aggiornamento del firmware SP viene attivato automaticamente o manualmente.

**Informazioni correlate**

"Download NetApp: Firmware di sistema e diagnostica"

### Quando SP/BMC utilizza l'interfaccia di rete per gli aggiornamenti del firmware

Un aggiornamento del firmware SP attivato da ONTAP con SP con versione 1.5, 2.5, 3.1 o successiva supporta l'utilizzo di un meccanismo di trasferimento file basato su IP sull'interfaccia di rete SP.

> Questo argomento si applica sia all'SP che al BMC.

Un aggiornamento del firmware SP tramite l'interfaccia di rete è più veloce di un aggiornamento tramite l'interfaccia seriale. Riduce la finestra di manutenzione durante la quale viene aggiornato il firmware SP e non comporta interruzioni per il funzionamento di ONTAP. Le versioni SP che supportano questa funzionalità sono incluse in ONTAP. Sono inoltre disponibili sul sito di supporto NetApp e possono essere installati su controller che eseguono una versione compatibile di ONTAP.

Se si utilizza SP versione 1.5, 2.5, 3.1 o successiva, si applicano le seguenti procedure di aggiornamento del firmware:

- Un aggiornamento del firmware SP che viene *automaticamente* attivato da ONTAP utilizza per impostazione predefinita l'interfaccia di rete per l'aggiornamento; tuttavia, l'aggiornamento automatico SP passa all'utilizzo dell'interfaccia seriale per l'aggiornamento del firmware se si verifica una delle seguenti condizioni:
  - L'interfaccia di rete SP non è configurata o non è disponibile.
  - Il trasferimento dei file basato su IP non riesce.
  - Il servizio API SP è disattivato.

Indipendentemente dalla versione SP in esecuzione, un aggiornamento del firmware SP attivato dall'interfaccia di rete SP utilizza sempre l'interfaccia di rete SP per l'aggiornamento.

**Informazioni correlate**

"Download NetApp: Firmware di sistema e diagnostica"

### Account che possono accedere al SP

Quando si tenta di accedere al SP, viene richiesto di immettere le credenziali. Account utente del cluster creati con `service-processor` Il tipo di applicazione ha accesso alla CLI SP su qualsiasi nodo del cluster. Gli account utente SP sono gestiti da ONTAP e autenticati mediante password. A partire da ONTAP 9.9.1, gli account utente SP devono

disporre di `admin` ruolo.

Gli account utente per l'accesso al SP vengono gestiti da ONTAP invece che dall'interfaccia utente di servizio (CLI) SP. Un account utente del cluster può accedere al SP se creato con `-application` del parametro `security login create` comando impostato su `service-processor` e a. `-authmethod` parametro impostato su `password`. L'SP supporta solo l'autenticazione tramite password.

Specificare `-role` Parametro durante la creazione di un account utente SP.

- In ONTAP 9.9.1 e versioni successive, è necessario specificare `admin` per `-role` e qualsiasi modifica apportata a un account richiede `admin` ruolo. Altri ruoli non sono più consentiti per motivi di sicurezza.
  - Se si esegue l'aggiornamento a ONTAP 9.9.1 o versioni successive, vedere "Modifica degli account utente che possono accedere al Service Processor".
  - Se si torna a ONTAP 9.8 o versioni precedenti, vedere "Verificare gli account utente che possono accedere al Service Processor".
- In ONTAP 9.8 e versioni precedenti, qualsiasi ruolo può accedere al SP, ma `admin` è consigliato.

Per impostazione predefinita, l'account utente del cluster "admin" include `service-processor` Tipo di applicazione e ha accesso al SP.

ONTAP impedisce di creare account utente con nomi riservati al sistema (ad esempio "root" e "naroot"). Non è possibile utilizzare un nome riservato al sistema per accedere al cluster o al SP.

È possibile visualizzare gli account utente SP correnti utilizzando `-application service-processor` del parametro `security login show` comando.

#### Accedere a SP/BMC da un host di amministrazione

## È possibile accedere all'SP di un nodo da un host di amministrazione per eseguire attività di gestione dei nodi in remoto.

**Di cosa hai bisogno**

Devono essere soddisfatte le seguenti condizioni:

- L'host di amministrazione utilizzato per accedere al SP deve supportare SSHv2.
- L'account utente deve essere già configurato per accedere al SP.

  Per accedere al SP, l'account utente deve essere stato creato con `-application` del parametro `security login create` comando impostato su `service-processor` e a. `-authmethod` parametro impostato su `password`.

> Questa attività si applica sia all'SP che al BMC.

Se l'SP è configurato per utilizzare un indirizzo IPv4 o IPv6 e se cinque tentativi di accesso SSH da un host falliscono consecutivamente entro 10 minuti, l'SP rifiuta le richieste di accesso SSH e sospende la comunicazione con l'indirizzo IP dell'host per 15 minuti. La comunicazione riprende dopo 15 minuti ed è possibile tentare di nuovo di accedere all'SP.

ONTAP impedisce di creare o utilizzare nomi riservati al sistema (come "root" e "naroot") per accedere al cluster o al SP.

**Fasi**

1. Dall'host di amministrazione, accedere all'SP:

   **`ssh username@SP_IP_address`**

2. Quando richiesto, immettere la password per `username`.

   Viene visualizzato il prompt SP, che indica che si dispone dell'accesso alla CLI SP.

**Esempi di accesso SP da un host di amministrazione**

Nell'esempio seguente viene illustrato come accedere al SP con un account utente `joe`, Che è stato configurato per accedere al SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Gli esempi seguenti mostrano come utilizzare l'indirizzo globale IPv6 o l'indirizzo pubblicizzato dal router IPv6 per accedere all'SP su un nodo con SSH impostato per IPv6 e l'SP configurato per IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

**Accedere a SP/BMC dalla console di sistema**

È possibile accedere all'SP dalla console di sistema (chiamata anche *console seriale*) per eseguire attività di monitoraggio o risoluzione dei problemi.

**A proposito di questa attività**

Questa attività si applica sia all'SP che al BMC.

**Fasi**

1. Accedere alla CLI SP dalla console di sistema premendo Ctrl-G al prompt.
2. Accedere all'interfaccia CLI SP quando richiesto.

   Viene visualizzato il prompt SP, che indica che si dispone dell'accesso alla CLI SP.

3. Uscire dalla CLI SP e tornare alla console di sistema premendo Ctrl-D, quindi premere Invio.

**Esempio di accesso alla CLI SP dalla console di sistema**

L'esempio seguente mostra il risultato della pressione di Ctrl-G dalla console di sistema per accedere alla CLI SP. Il `help system power` Al prompt SP viene immesso il comando, quindi premere Ctrl-D e Invio per tornare alla console di sistema.

```
cluster1::>
```

Premere Ctrl-G per accedere alla CLI SP.

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

Premere Ctrl-D e Invio per tornare alla console di sistema.

```
cluster1::>
```

#### Relazione tra le sessioni di SP CLI, console SP e console di sistema

È possibile aprire una sessione SP CLI per gestire un nodo in remoto e aprire una sessione separata della console SP per accedere alla console del nodo. La sessione della console SP esegue il mirroring dell'output visualizzato in una sessione della console di sistema simultanea. SP e la console di sistema dispongono di ambienti shell indipendenti con autenticazione di accesso indipendente.

Comprendere come sono correlate le sessioni di SP CLI, console SP e console di sistema aiuta a gestire un nodo in remoto. Di seguito viene descritta la relazione tra le sessioni:

- Solo un amministratore può accedere alla sessione SP CLI alla volta; tuttavia, il SP consente di aprire contemporaneamente una sessione SP CLI e una sessione SP console separata.

  La CLI SP viene indicata con il prompt SP (`SP>`). Da una sessione CLI SP, è possibile utilizzare l'SP `system console` Per avviare una sessione della console SP. Allo stesso tempo, è possibile avviare una sessione CLI SP separata tramite SSH. Se si preme Ctrl-D per uscire dalla sessione della console SP, si torna automaticamente alla sessione della CLI SP. Se esiste già una sessione CLI SP, viene visualizzato un messaggio che chiede se terminare la sessione CLI SP esistente. Se si immette "y", la sessione CLI SP esistente viene terminata, consentendo di tornare dalla console SP alla CLI SP. Questa azione viene registrata nel registro eventi SP.

  In una sessione CLI ONTAP connessa tramite SSH, è possibile passare alla console di sistema di un nodo

eseguendo ONTAP `system node run-console` comando da un altro nodo.

- Per motivi di sicurezza, la sessione CLI SP e la sessione della console di sistema dispongono di un'autenticazione di accesso indipendente.

  Quando si avvia una sessione della console SP dalla CLI SP (utilizzando l'SP `system console` (comando), viene richiesta la credenziale della console di sistema. Quando si accede alla CLI SP da una sessione della console di sistema (premendo Ctrl-G), viene richiesta la credenziale CLI SP.

- La sessione della console SP e la sessione della console di sistema hanno ambienti shell indipendenti.

  La sessione della console SP esegue il mirroring dell'output visualizzato in una sessione della console di sistema simultanea. Tuttavia, la sessione della console di sistema simultanea non esegue il mirroring della sessione della console SP.

  La sessione della console SP non esegue il mirroring dell'output delle sessioni SSH simultanee.

#### Gestire gli indirizzi IP che possono accedere al SP

Per impostazione predefinita, l'SP accetta richieste di connessione SSH da host di amministrazione di qualsiasi indirizzo IP. È possibile configurare l'SP in modo che accetti le richieste di connessione SSH solo dagli host di amministrazione che hanno gli indirizzi IP specificati. Le modifiche apportate si applicano all'accesso SSH all'SP di qualsiasi nodo del cluster.

**Fasi**

1. Concedere l'accesso SP solo agli indirizzi IP specificati utilizzando `system service-processor ssh add-allowed-addresses` con il `-allowed-addresses` parametro.

   - Il valore di `-allowed-addresses` il parametro deve essere specificato nel formato di `address /netmask`e multipli `address/netmask` le coppie devono essere separate da virgole, ad esempio `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Impostazione di `-allowed-addresses` parametro a. `0.0.0.0/0, ::/0` Consente a tutti gli indirizzi IP di accedere all'SP (impostazione predefinita).

   - Quando si modifica l'impostazione predefinita limitando l'accesso SP solo agli indirizzi IP specificati, ONTAP richiede di confermare che si desidera che gli indirizzi IP specificati sostituiscano l'impostazione predefinita "Allow All" (`0.0.0.0/0, ::/0`).

   - Il `system service-processor ssh show` Il comando visualizza gli indirizzi IP che possono accedere al SP.

2. Se si desidera impedire a un indirizzo IP specificato di accedere all'SP, utilizzare `system service-processor ssh remove-allowed-addresses` con il `-allowed-addresses` parametro.

   Se si impedisce a tutti gli indirizzi IP di accedere al SP, il SP diventa inaccessibile da qualsiasi host di amministrazione.

#### Esempi di gestione degli indirizzi IP che possono accedere al SP

I seguenti esempi mostrano l'impostazione predefinita per l'accesso SSH all'SP, modificano l'impostazione predefinita limitando l'accesso SP solo agli indirizzi IP specificati, rimuovono gli indirizzi IP specificati dall'elenco di accesso e ripristinano l'accesso SP per tutti gli indirizzi IP:

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

#### Utilizzare la guida in linea di SP/BMC CLI

La guida in linea visualizza i comandi e le opzioni della CLI SP/BMC.

**A proposito di questa attività**

Questa attività si applica sia all'SP che al BMC.

**Fasi**

1. Per visualizzare le informazioni della guida per i comandi SP/BMC, immettere quanto segue:

| Per accedere alla guida SP… | Per accedere alla guida BMC… |
| --- | --- |
| Tipo `help` Al prompt SP. | Tipo `system` Al prompt di BMC. |

L'esempio seguente mostra la guida in linea di SP CLI.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

L'esempio seguente mostra la guida in linea di BMC CLI.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Per visualizzare le informazioni della guida relative all'opzione di un comando SP/BMC, immettere `help` Prima o dopo il comando SP/BMC.

   L'esempio seguente mostra la guida in linea di SP CLI per SP `events` comando.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

Nell'esempio seguente viene illustrata la guida in linea di BMC CLI per BMC `system power` comando.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

#### Comandi per la gestione remota di un nodo

È possibile gestire un nodo in remoto accedendo al relativo SP ed eseguendo comandi SP CLI per eseguire attività di gestione dei nodi. Per diverse attività di gestione remota dei nodi eseguite di frequente, è possibile utilizzare i comandi ONTAP da un altro nodo del cluster. Alcuni comandi SP sono specifici della piattaforma e potrebbero non essere disponibili sulla piattaforma.

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| Visualizza i comandi SP disponibili o i sottocomandi di un comando SP specificato | `help` [`command`] | | |
| Visualizza il livello di privilegio corrente per la CLI SP | `priv show` | | |
| Impostare il livello di privilegio per accedere alla modalità specificata per la CLI SP | `priv set` {`admin` | `advanced` | `diag`} |
| | | Visualizzare la data e l'ora del sistema | `date` |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| | date | Visualizza gli eventi registrati dall'SP | events {all |
| info | newest number | oldest number | search keyword} |
| | | Visualizzazione dello stato SP e delle informazioni di configurazione della rete | sp status [-v |
| -d]<br><br>Il -v L'opzione visualizza le statistiche SP in forma dettagliata. Il -d L'opzione aggiunge il registro di debug SP al display. | bmc status [-v | -d]<br><br>Il -v L'opzione visualizza le statistiche SP in forma dettagliata. Il -d L'opzione aggiunge il registro di debug SP al display. | system service-processor show |
| Visualizza il periodo di tempo in cui il SP è rimasto attivo e il numero medio di lavori nella coda di esecuzione negli ultimi 1, 5 e 15 minuti | sp uptime | bmc uptime | |
| Visualizzare i log della console di sistema | system log | | |
| Visualizzare gli archivi del registro SP o i file in un archivio | sp log history show [-archive {latest | {all | archive-name}] [-dump {all |
| file-name}] | bmc log history show [-archive {latest | {all | archive-name}] [-dump {all |
| file-name}] | | Visualizza lo stato di alimentazione del controller di un nodo | system power status |
| | system node power show | Visualizza le informazioni sulla batteria | system battery show |
| | | Visualizza le informazioni ACP o lo stato dei sensori di espansione | system acp [show |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| `sensors show`] | | | Elencare tutte le FRU del sistema e i relativi ID |
| `system fru list` | | | Visualizzare le informazioni sul prodotto per la FRU specificata |
| `system fru show fru_id` | | | Visualizzare il registro della cronologia dei dati FRU |
| `system fru log show` (livello di privilegio avanzato) | | | Visualizzare lo stato dei sensori ambientali, inclusi i relativi stati e valori correnti |
| `system sensors` oppure `system sensors show` | | `system node environment sensors show` | Visualizza lo stato e i dettagli del sensore specificato |
| `system sensors get sensor_name`<br><br>È possibile ottenere `sensor_name` utilizzando `system sensors` o il `system sensors show` comando. | | | Visualizza le informazioni sulla versione del firmware SP |
| `version` | | `system service-processor image show` | Visualizza la cronologia dei comandi SP |
| `sp log audit` (livello di privilegio avanzato) | `bmc log audit` | | Visualizza le informazioni di debug SP |
| `sp log debug` (livello di privilegio avanzato) | `bmc log debug` (livello di privilegio avanzato) | | Visualizza il file dei messaggi SP |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| `sp log messages` (livello di privilegio avanzato) | `bmc log messages` (livello di privilegio avanzato) | | Consente di visualizzare le impostazioni per la raccolta di dati forensi del sistema in un evento di ripristino del watchdog, visualizzare le informazioni forensi del sistema raccolte durante un evento di ripristino del watchdog o cancellare le informazioni forensi del sistema raccolte |
| `system forensics` [`show` | `log dump` | `log clear`] | |
| | Accedere alla console di sistema | `system console` | |
| `system node run-console` | Premere Ctrl-D per uscire dalla sessione della console di sistema. | Accendere o spegnere il nodo oppure eseguire un ciclo di alimentazione (spegnendo e riaccendendo l'alimentazione) | `system power on` |
| | `system node power on` (livello di privilegio avanzato) | `system power off` | |
| | `system power cycle` | | |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| L'alimentazione in standby rimane attiva per mantenere l'SP in funzione senza interruzioni. Durante il ciclo di alimentazione, si verifica una breve pausa prima di riaccendere il prodotto.<br><br>L'utilizzo di questi comandi per spegnere o spegnere e riaccendere il nodo potrebbe causare un arresto non corretto del nodo (chiamato anche *shutdown anomalo*) e non può sostituire un arresto corretto mediante ONTAP `system node halt` comando. | Creare un core dump e ripristinare il nodo | `system core` [`-f`]<br><br>Il `-f` l'opzione forza la creazione di un core dump e il ripristino del nodo. | |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| `system node coredump trigger`<br><br>(livello di privilegio avanzato) | Questi comandi hanno lo stesso effetto della pressione del pulsante NMI (non-maskable Interrupt) su un nodo, causando un arresto anomalo del nodo e forzando un dump dei file core quando si arresta il nodo. Questi comandi sono utili quando ONTAP sul nodo è bloccato o non risponde a comandi come `system node shutdown`. I file core dump generati vengono visualizzati nell'output di `system node coredump show` comando. L'SP rimane operativo fino a quando l'alimentazione in ingresso al nodo non viene interrotta. | Riavviare il nodo con un'immagine del firmware del BIOS (primaria, di backup o corrente) opzionale per eseguire il ripristino in caso di problemi come un'immagine danneggiata del dispositivo di avvio del nodo | `system reset` {`primary` |
| `backup` | `current`} | | `system node reset` con `-firmware` {`primary` |
| `backup` | `current`} parameter(livello di privilegio avanzato)<br><br>`system node reset` | Questa operazione causa un arresto anomalo del nodo.<br><br>Se non viene specificata alcuna immagine del firmware del BIOS, l'immagine corrente viene utilizzata per il riavvio. L'SP rimane operativo fino a quando l'alimentazione in ingresso al nodo non viene interrotta. | Consente di visualizzare lo stato dell'aggiornamento automatico del firmware della batteria oppure di attivare o disattivare l'aggiornamento automatico del firmware della batteria al successivo avvio SP |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| `system battery auto_update` [`status` | `enable` | `disable`]<br><br>(livello di privilegio avanzato) | |
| | Confrontare l'immagine del firmware corrente della batteria con un'immagine del firmware specificata | `system battery verify` [`image_URL`]<br><br>(livello di privilegio avanzato)<br><br>Se `image_URL` non specificato, viene utilizzata l'immagine del firmware della batteria predefinita per il confronto. | |
| | Aggiornare il firmware della batteria dall'immagine nella posizione specificata | `system battery flash image_URL`<br><br>(livello di privilegio avanzato)<br><br>Utilizzare questo comando se il processo di aggiornamento automatico del firmware della batteria non è riuscito per qualche motivo. | |
| | Aggiornare il firmware SP utilizzando l'immagine nella posizione specificata | `sp update image_URL` `image_URL` non deve superare i 200 caratteri. | `bmc update image_URL` `image_URL` non deve superare i 200 caratteri. |
| `system service-processor image update` | Riavviare il SP | `sp reboot` | |
| `system service-processor reboot-sp` | Cancellare il contenuto della memoria flash NVRAM | `system nvram flash clear` (livello di privilegio avanzato)<br><br>Questo comando non può essere avviato quando il controller è spento (`system power off`). | |

| Se si desidera… | Utilizza questo comando SP… | Utilizza questo comando BMC… | Oppure questo comando ONTAP … |
|---|---|---|---|
| | Uscire dalla CLI SP | `exit` | |

**Informazioni sulle letture del sensore SP basate sulla soglia e sui valori di stato dell'output del comando dei sensori di sistema**

I sensori basati su soglie rilevano periodicamente una vasta gamma di componenti del sistema. SP confronta la lettura di un sensore basato su soglia con i suoi limiti di soglia prefissati che definiscono le condizioni operative accettabili di un componente.

In base alla lettura del sensore, l'SP visualizza lo stato del sensore per consentire il monitoraggio delle condizioni del componente.

Esempi di sensori basati su soglia includono sensori per temperature, tensioni, correnti e velocità delle ventole del sistema. L'elenco specifico dei sensori basati su soglia dipende dalla piattaforma.

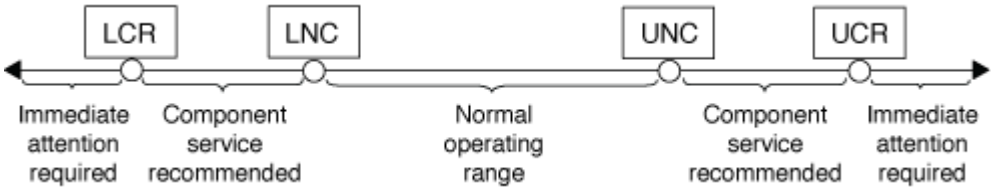
I sensori basati su soglia presentano le seguenti soglie, visualizzate nell'output dell'SP `system sensors` comando:

- LCR (Lower Critical)
- LNC (Lower non-critical)
- Uncritical superiore (UNC)
- Superiore critico (UCR)

Un valore del sensore tra LNC e LCR o tra UNC e UCR indica che il componente mostra segni di un problema e che potrebbe verificarsi un guasto al sistema. Pertanto, è consigliabile pianificare presto il servizio di componenti.

Un valore del sensore inferiore a LCR o superiore a UCR indica che il componente non funziona correttamente e che si sta per verificare un guasto al sistema. Pertanto, il componente richiede un'attenzione immediata.

Il seguente diagramma illustra gli intervalli di severità specificati dalle soglie:




La lettura di un sensore basato su soglia si trova sotto `Current` nella colonna `system sensors` output del comando. Il `system sensors get sensor_name` il comando visualizza ulteriori dettagli per il sensore specificato. Quando la lettura di un sensore basato su soglia supera gli intervalli di soglia non critici e critici, il sensore segnala un problema di gravità crescente. Quando il valore supera un limite di soglia, lo stato del sensore in `system sensors` l'output del comando cambia da `ok` a. `nc` (non critico) o. `cr` (Critico) a seconda del superamento della soglia e della registrazione di un messaggio di evento nel registro eventi SEL.

Alcuni sensori basati su soglia non hanno tutti e quattro i livelli di soglia. Per questi sensori, vengono visualizzate le soglie mancanti `na` come i loro limiti in `system sensors` Output del comando, che indica che il sensore specifico non presenta alcun problema di limite o gravità per la soglia data e che l'SP non monitora il

sensore per tale soglia.

**Esempio di output del comando dei sensori di sistema**

Nell'esempio riportato di seguito vengono illustrate alcune informazioni visualizzate da `system sensors` Nell'interfaccia CLI SP:

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR       | LNC
| UNC       | UCR
-----------------+------------+------------+-------+-----------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000     | 10.000
| 42.000    | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000     | 10.000
| 59.000    | 68.000
CPU1_Error       | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na        | na
| na        | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048
| 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844
| 1.348     | 1.368
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116
| 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465
| 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707
| 1.892     | 1.911
…
```

**Esempio di output del comando SENSOR_NAME dei sensori di sistema per un sensore basato su soglia**

L'esempio seguente mostra il risultato dell'immissione `system sensors get sensor_name` Nella CLI SP per il sensore basato su soglia 5V:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID              : 5V (0x13)
 Entity ID             : 7.97
 Sensor Type (Analog)  : Voltage
 Sensor Reading        : 5.002 (+/- 0) Volts
 Status                : ok
 Lower Non-Recoverable : na
 Lower Critical        : 4.246
 Lower Non-Critical    : 4.490
 Upper Non-Critical    : 5.490
 Upper Critical        : 5.758
 Upper Non-Recoverable : na
 Assertion Events      :
 Assertions Enabled    : lnc- lcr- ucr+
 Deassertions Enabled  : lnc- lcr- ucr+
```

#### Informazioni sui valori di stato del sensore SP discreto dell'output del comando dei sensori di sistema

I sensori discreti non hanno soglie. I relativi valori, visualizzati sotto `Current` Nella colonna SP CLI `system sensors` Output del comando, non portano significati effettivi e quindi vengono ignorati dal SP. Il `Status` nella colonna `system sensors` l'output del comando visualizza i valori di stato dei sensori discreti in formato esadecimale.

Esempi di sensori discreti includono sensori per la ventola, guasti all'alimentatore e guasti al sistema. L'elenco specifico di sensori discreti dipende dalla piattaforma.

È possibile utilizzare la CLI SP `system sensors get sensor_name` comando per l'interpretazione dei valori di stato per la maggior parte dei sensori discreti. I seguenti esempi mostrano i risultati dell'immissione `system sensors get sensor_name` Per i sensori discreti CPU0_Error e io_Slot1_Present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                        [Device Present]
```

Anche se il `system sensors get sensor_name` Command visualizza le informazioni di stato per la maggior parte dei sensori discreti, non fornisce informazioni di stato per i sensori discreti System_FW_Status, System_Watchdog, PSU1_Input_Type e PSU2_Input_Type. È possibile utilizzare le seguenti informazioni per interpretare i valori di stato di questi sensori.

#### System_FW_Status

La condizione del sensore System_FW_Status viene visualizzata sotto forma di `0xAABB`. È possibile combinare le informazioni di `AA` e. `BB` per determinare le condizioni del sensore.

`AA` può avere uno dei seguenti valori:

| Valori | Condizione del sensore |
|---|---|
| 01 | Errore del firmware di sistema |
| 02 | Il firmware di sistema si blocca |
| 04 | Avanzamento del firmware di sistema |

`BB` può avere uno dei seguenti valori:

| Valori | Condizione del sensore |
|---|---|
| 00 | Il software di sistema si è arrestato correttamente |
| 01 | Inizializzazione della memoria in corso |
| 02 | Inizializzazione NVMEM in corso (quando è presente NVMEM) |
| 04 | Ripristino dei valori MCH (Memory Controller Hub) (quando è presente NVMEM) |
| 05 | L'utente ha inserito il programma di installazione |
| 13 | Avviare il sistema operativo o IL CARICATORE |

| Valori | Condizione del sensore |
|---|---|
| 1F | BIOS in fase di avvio |
| 20 | IL CARICATORE è in esecuzione |
| 21 | IL CARICATORE sta programmando il firmware principale del BIOS. Non spegnere il sistema. |
| 22 | IL CARICATORE sta programmando il firmware alternativo del BIOS. Non spegnere il sistema. |
| 2F | ONTAP è in esecuzione |
| 60 | SP ha spento il sistema |
| 61 | SP ha acceso il sistema |
| 62 | SP ha ripristinato il sistema |
| 63 | Spegnere e riaccendere il watchdog SP |
| 64 | Ripristino a freddo del watchdog SP |

Ad esempio, lo stato del sensore System_FW_Status 0x042F indica "System firmware Progress (04), ONTAP is running (2F)" (avanzamento del firmware di sistema ().

#### System_Watchdog

Il sensore System_Watchdog può avere una delle seguenti condizioni:

- **0x0080**

  Lo stato di questo sensore non è cambiato

| Valori | Condizione del sensore |
|---|---|
| 0x0081 | Interruzione del timer |
| 0x0180 | Timer scaduto |
| 0x0280 | Reimpostazione a freddo |
| 0x0480 | Spegnere |
| 0x0880 | Spegnere e riaccendere |

Ad esempio, lo stato del sensore System_Watchdog 0x0880 indica che si verifica un timeout di watchdog e provoca un ciclo di alimentazione del sistema.

#### PSU1_Input_Type e PSU2_Input_Type

Per gli alimentatori a corrente continua (CC), i sensori PSU1_Input_Type e PSU2_Input_Type non sono applicabili. Per gli alimentatori a corrente alternata (CA), lo stato dei sensori può avere uno dei seguenti valori:

| Valori | Condizione del sensore |
|---|---|
| 0x01 xx | Tipo di PSU da 220 V. |
| 0x02 xx | Tipo di PSU da 110 V. |

Ad esempio, lo stato del sensore PSU1_Input_Type 0x0280 indica che il sensore segnala che il tipo di PSU è 110 V.

### Comandi per la gestione dell'SP da ONTAP

ONTAP fornisce comandi per la gestione dell'SP, tra cui la configurazione della rete SP, l'immagine del firmware SP, l'accesso SSH all'SP e l'amministrazione generale dell'SP.

#### Comandi per la gestione della configurazione di rete SP

| Se si desidera… | Eseguire questo comando ONTAP… |
|---|---|
| Abilitare la configurazione di rete automatica SP per l'SP per utilizzare la famiglia di indirizzi IPv4 o IPv6 della subnet specificata | `system service-processor network auto-configuration enable` |
| Disattiva la configurazione di rete automatica SP per la famiglia di indirizzi IPv4 o IPv6 della subnet specificata per l'SP | `system service-processor network auto-configuration disable` |
| Visualizza la configurazione di rete automatica SP | `system service-processor network auto-configuration show` |

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Configurare manualmente la rete SP per un nodo, tra cui:<br>• La famiglia di indirizzi IP (IPv4 o IPv6)<br>• Se attivare l'interfaccia di rete della famiglia di indirizzi IP specificata<br>• Se si utilizza IPv4, specificare se utilizzare la configurazione di rete dal server DHCP o l'indirizzo di rete specificato<br>• L'indirizzo IP pubblico per l'SP<br>• La netmask per l'SP (se si utilizza IPv4)<br>• La lunghezza del prefisso di rete della subnet mask per l'SP (se si utilizza IPv6)<br>• L'indirizzo IP del gateway per l'SP | `system service-processor network modify` |
| Visualizzare la configurazione di rete SP, tra cui:<br>• La famiglia di indirizzi configurata (IPv4 o IPv6) e se è attivata<br>• Il tipo di dispositivo di gestione remota<br>• Lo stato SP corrente e lo stato del collegamento<br>• Configurazione di rete, ad esempio indirizzo IP, indirizzo MAC, netmask, lunghezza prefisso della subnet mask, indirizzo IP assegnato dal router, indirizzo IP locale di collegamento e indirizzo IP del gateway<br>• L'ora dell'ultimo aggiornamento del SP<br>• Il nome della subnet utilizzata per la configurazione automatica SP<br>• Se l'indirizzo IP assegnato dal router IPv6 è attivato<br>• Stato di setup della rete SP<br>• Motivo dell'errore di configurazione della rete SP | `system service-processor network show`<br><br>La visualizzazione dei dettagli completi della rete SP richiede `-instance` parametro. |
| Modificare la configurazione del servizio API SP, includendo quanto segue:<br>• Modifica della porta utilizzata dal servizio API SP<br>• Attivazione o disattivazione del servizio API SP | `system service-processor api-service modify`<br><br>(livello di privilegio avanzato) |

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Visualizzare la configurazione del servizio API SP | `system service-processor api-service show`<br><br>(livello di privilegio avanzato) |
| Rinnovare i certificati SSL e SSH utilizzati dal servizio API SP per la comunicazione interna | • Per ONTAP 9.5 o versioni successive: `system service-processor api-service renew-internal-certificates`<br>• Per ONTAP 9.4 o versioni precedenti: `system service-processor api-service renew-certificates`<br><br>(livello di privilegio avanzato) |

**Comandi per la gestione dell'immagine del firmware SP**

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Visualizza i dettagli dell'immagine del firmware SP attualmente installata, tra cui:<br><br>• Il tipo di dispositivo di gestione remota<br>• L'immagine (principale o di backup) da cui viene avviato il SP, il suo stato e la versione del firmware<br>• Se l'aggiornamento automatico del firmware è attivato e lo stato dell'ultimo aggiornamento | `system service-processor image show`<br><br>Il `-is-current` Parametro indica l'immagine (primaria o di backup) da cui è attualmente avviato il SP, non se la versione del firmware installata è più recente. |
| Attiva o disattiva l'aggiornamento automatico del firmware SP | `system service-processor image modify`<br><br>Per impostazione predefinita, il firmware SP viene aggiornato automaticamente con l'aggiornamento di ONTAP o quando viene scaricata manualmente una nuova versione del firmware SP. La disattivazione dell'aggiornamento automatico non è consigliata, in quanto può causare combinazioni non ottimali o non qualificate tra l'immagine ONTAP e l'immagine del firmware SP. |

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Scaricare manualmente un'immagine del firmware SP su un nodo | `system node image get`<br><br>Prima di eseguire `system node image` è necessario impostare il livello di privilegio su advanced (avanzato) (`set -privilege advanced`), immettendo **y** quando viene richiesto di continuare.<br><br>L'immagine del firmware SP viene fornita con ONTAP. Non è necessario scaricare manualmente il firmware SP, a meno che non si desideri utilizzare una versione del firmware SP diversa da quella fornita con ONTAP. |
| Visualizza lo stato dell'ultimo aggiornamento del firmware SP attivato da ONTAP, incluse le seguenti informazioni:<br><br>• L'ora di inizio e di fine dell'ultimo aggiornamento del firmware SP<br>• Se è in corso un aggiornamento e la percentuale di completamento | `system service-processor image update-progress show` |

**Comandi per la gestione dell'accesso SSH al SP**

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Concedere l'accesso SP solo agli indirizzi IP specificati | `system service-processor ssh add-allowed-addresses` |
| Impedisce agli indirizzi IP specificati di accedere al SP | `system service-processor ssh remove-allowed-addresses` |
| Visualizza gli indirizzi IP che possono accedere all'SP | `system service-processor ssh show` |

**Comandi per l'amministrazione SP generale**

| Se si desidera… | Eseguire questo comando ONTAP… |
| --- | --- |
| Visualizza informazioni generali sull'SP, tra cui:<br>• Il tipo di dispositivo di gestione remota<br>• Lo stato SP corrente<br>• Se la rete SP è configurata<br>• Informazioni di rete, ad esempio l'indirizzo IP pubblico e l'indirizzo MAC<br>• La versione del firmware SP e la versione dell'interfaccia di gestione della piattaforma intelligente (IPMI)<br>• Se l'aggiornamento automatico del firmware SP è attivato | `system service-processor show` La visualizzazione delle informazioni SP complete richiede `-instance` parametro. |
| Riavviare il SP su un nodo | `system service-processor reboot-sp` |
| Generare e inviare un messaggio AutoSupport che includa i file di log SP raccolti da un nodo specificato | `system node autosupport invoke-splog` |
| Visualizzare la mappa di allocazione dei file di log SP raccolti nel cluster, inclusi i numeri di sequenza dei file di log SP che risiedono in ciascun nodo di raccolta | `system service-processor log show-allocations` |

**Informazioni correlate**

"Comandi di ONTAP 9"

**Comandi ONTAP per la gestione BMC**

## Questi comandi ONTAP sono supportati dal Baseboard Management Controller (BMC).

Il BMC utilizza alcuni degli stessi comandi del Service Processor (SP). I seguenti comandi SP sono supportati su BMC.

| Se si desidera… | Utilizzare questo comando |
| --- | --- |
| Visualizzare le informazioni BMC | **`system service-processor show`** |
| Visualizzare/modificare la configurazione di rete BMC | **`system service-processor network show/modify`** |
| Ripristinare il BMC | **`system service-processor reboot-sp`** |
| Consente di visualizzare/modificare i dettagli dell'immagine del firmware BMC attualmente installata | **`system service-processor image show/modify`** |

| Se si desidera… | Utilizzare questo comando |
| --- | --- |
| Aggiornare il firmware BMC | **`system service-processor image update`** |
| Visualizza lo stato dell'ultimo aggiornamento del firmware BMC | **`system service-processor image update-progress show`** |
| Abilitare la configurazione di rete automatica per il BMC per l'utilizzo di un indirizzo IPv4 o IPv6 nella subnet specificata | **`system service-processor network auto-configuration enable`** |
| Disattivare la configurazione di rete automatica per un indirizzo IPv4 o IPv6 nella subnet specificata per BMC | **`system service-processor network auto-configuration disable`** |
| Visualizza la configurazione automatica di rete BMC | **`system service-processor network auto-configuration show`** |

Per i comandi non supportati dal firmware BMC, viene visualizzato il seguente messaggio di errore.

```
::> Error: Command not supported on this platform.
```

#### Comandi BMC CLI

È possibile accedere al BMC utilizzando SSH. I seguenti comandi sono supportati dalla riga di comando BMC.

| Comando | Funzione |
| --- | --- |
| sistema | Visualizza un elenco di tutti i comandi. |
| console di sistema | Connettersi alla console del sistema. Utilizzare `Ctrl+D` per uscire dalla sessione. |
| core di sistema | Eseguire il dump del core di sistema e ripristinarlo. |
| spegnere e riaccendere il sistema | Spegnere e riaccendere il sistema. |
| spegnimento del sistema | Spegnere il sistema. |
| accensione del sistema | Accendere il sistema. |
| stato di alimentazione del sistema | Stampare lo stato di alimentazione del sistema. |
| ripristino del sistema | Ripristinare il sistema. |

| Comando | Funzione |
| --- | --- |
| log di sistema | Stampare i registri della console del sistema |
| fru di sistema mostra [id] | Scarica tutte le informazioni FRU (Field Replaceable Unit) selezionate. |

## Gestire il tempo del cluster (solo amministratori del cluster)

I problemi possono verificarsi quando il tempo del cluster non è preciso. Sebbene ONTAP consenta di impostare manualmente fuso orario, data e ora sul cluster, è necessario configurare i server NTP (Network Time Protocol) per sincronizzare l'ora del cluster.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

NTP è sempre attivato. Tuttavia, la configurazione è ancora necessaria per la sincronizzazione del cluster con un'origine temporale esterna. ONTAP consente di gestire la configurazione NTP del cluster nei seguenti modi:

- È possibile associare al cluster un massimo di 10 server NTP esterni (`cluster time-service ntp server create`).
  - Per garantire la ridondanza e la qualità del servizio nel tempo, è necessario associare almeno tre server NTP esterni al cluster.
  - È possibile specificare un server NTP utilizzando il relativo indirizzo IPv4 o IPv6 o il nome host completo.
  - È possibile specificare manualmente la versione NTP (v3 o v4) da utilizzare.

    Per impostazione predefinita, ONTAP seleziona automaticamente la versione di NTP supportata per un determinato server NTP esterno.

  Se la versione NTP specificata non è supportata per il server NTP, non è possibile eseguire lo scambio di ore.

  - A livello di privilegi avanzati, è possibile specificare un server NTP esterno associato al cluster come origine temporale principale per la correzione e la regolazione dell'ora del cluster.
- È possibile visualizzare i server NTP associati al cluster (`cluster time-service ntp server show`).
- È possibile modificare la configurazione NTP del cluster (`cluster time-service ntp server modify`).
- È possibile disassociare il cluster da un server NTP esterno (`cluster time-service ntp server delete`).
- A livello di privilegi avanzati, è possibile ripristinare la configurazione annullando l'associazione di tutti i server NTP esterni al cluster (`cluster time-service ntp server reset`).

Un nodo che si unisce a un cluster adotta automaticamente la configurazione NTP del cluster.

Oltre a utilizzare NTP, ONTAP consente anche di gestire manualmente il tempo del cluster. Questa funzionalità è utile quando è necessario correggere un tempo errato (ad esempio, l'ora di un nodo è diventata significativamente errata dopo un riavvio). In tal caso, è possibile specificare un periodo di tempo

approssimativo per il cluster fino a quando NTP non può essere sincronizzato con un server di riferimento orario esterno. Il tempo impostato manualmente ha effetto su tutti i nodi del cluster.

È possibile gestire manualmente l'ora del cluster nei seguenti modi:

- È possibile impostare o modificare il fuso orario, la data e l'ora sul cluster (`cluster date modify`).
- È possibile visualizzare le impostazioni correnti di fuso orario, data e ora del cluster (`cluster date show`).

> Le pianificazioni dei processi non si adattano alle modifiche manuali di data e ora del cluster. Questi processi vengono pianificati per essere eseguiti in base all'ora corrente del cluster in cui è stato creato il processo o quando è stato eseguito più di recente. Pertanto, se si modifica manualmente la data o l'ora del cluster, è necessario utilizzare `job show` e. `job history show` comandi per verificare che tutti i processi pianificati siano messi in coda e completati in base alle proprie esigenze.

**Comandi per la gestione del tempo del cluster**

Si utilizza `cluster time-service ntp server` Comandi per gestire i server NTP per il cluster. Si utilizza `cluster date` comandi per gestire manualmente l'ora del cluster.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

I seguenti comandi consentono di gestire i server NTP per il cluster:

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Associare il cluster a un server NTP esterno senza autenticazione simmetrica | `cluster time-service ntp server create -server server_name` |
| Associare il cluster a un server NTP esterno con autenticazione simmetrica disponibile in ONTAP 9.5 o versione successiva | `cluster time-service ntp server create -server server_ip_address -key-id key_id`<br>Il `key_id` deve fare riferimento a una chiave condivisa esistente configurata con '`chiave ntp cluster time-service'. |
| Abilitare l'autenticazione simmetrica per un server NTP esistente. È possibile modificare il server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.<br><br>Disponibile in ONTAP 9.5 o versione successiva | `cluster time-service ntp server modify -server server_name -key-id key_id` |
| Disattiva autenticazione simmetrica | `cluster time-service ntp server modify -server server_name -is-authentication -enabled false` |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Configurare una chiave NTP condivisa | `cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value`<br>Le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP |
| Visualizza le informazioni sui server NTP associati al cluster | `cluster time-service ntp server show` |
| Modificare la configurazione di un server NTP esterno associato al cluster | `cluster time-service ntp server modify` |
| Dissocare un server NTP dal cluster | `cluster time-service ntp server delete` |
| Ripristinare la configurazione annullando l'associazione di tutti i server NTP esterni al cluster | `cluster time-service ntp server reset`<br>Questo comando richiede il livello di privilegio avanzato. |

I seguenti comandi consentono di gestire manualmente l'ora del cluster:

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Impostare o modificare il fuso orario, la data e l'ora | `cluster date modify` |
| Visualizza le impostazioni relative a fuso orario, data e ora del cluster | `cluster date show` |

**Informazioni correlate**

"Comandi di ONTAP 9"

## Gestire il banner e MOTD

### Gestire il banner e la panoramica MOTD

ONTAP consente di configurare un banner di accesso o un messaggio del giorno (MOTD) per comunicare le informazioni amministrative agli utenti CLI del cluster o della macchina virtuale di storage (SVM).

Un banner viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) prima che venga richiesto all'utente di eseguire l'autenticazione, ad esempio una password. Ad esempio, è possibile utilizzare il banner per visualizzare un messaggio di avviso come il seguente a qualcuno che tenta di accedere al sistema:

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

Un MOTD viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o a SVM) dopo l'autenticazione di un utente, ma prima della visualizzazione del prompt della shell dei cluster. Ad esempio, è possibile utilizzare MOTD per visualizzare un messaggio di benvenuto o informativo, ad esempio:

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

È possibile creare o modificare il contenuto del banner o di MOTD utilizzando `security login banner modify` oppure `security login motd modify` di comando, rispettivamente, nei seguenti modi:

- È possibile utilizzare la CLI in modo interattivo o non interattivo per specificare il testo da utilizzare per il banner o MOTD.

  La modalità interattiva, avviata quando si utilizza il comando senza `-message` oppure `-uri` parametro, consente di utilizzare newline (note anche come fine delle righe) nel messaggio.

  La modalità non interattiva, che utilizza `-message` parametro per specificare la stringa del messaggio, non supporta newlines.

- È possibile caricare il contenuto da una posizione FTP o HTTP da utilizzare per il banner o MOTD.
- È possibile configurare il MOTD per visualizzare il contenuto dinamico.

  Di seguito sono riportati alcuni esempi di elementi che è possibile configurare per la visualizzazione dinamica di MOTD:

  - Nome del cluster, nome del nodo o nome SVM
  - Data e ora del cluster
  - Nome dell'utente che effettua l'accesso
  - Ultimo accesso per l'utente su qualsiasi nodo del cluster
  - Nome o indirizzo IP del dispositivo di accesso
  - Nome del sistema operativo
  - Versione del software
  - Stringa della versione effettiva del cluster `security login motd modify` La pagina man descrive

le sequenze di escape che è possibile utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente.

Il banner non supporta il contenuto dinamico.

È possibile gestire il banner e il MOTD a livello di cluster o SVM:

- I seguenti fatti si applicano al banner:
  - Il banner configurato per il cluster viene utilizzato anche per tutte le SVM che non hanno un messaggio banner definito.
  - È possibile configurare un banner a livello di SVM per ogni SVM.

    Se è stato configurato un banner a livello di cluster, questo viene ignorato dal banner a livello di SVM per la SVM indicata.
- I seguenti fatti si applicano al MOTD:
  - Per impostazione predefinita, il MOTD configurato per il cluster è abilitato anche per tutte le SVM.
  - Inoltre, è possibile configurare un MOTD a livello di SVM per ogni SVM.

    In questo caso, gli utenti che accedono a SVM vedranno due MOTD, uno definito a livello di cluster e l'altro a livello di SVM.
  - Il MOTD a livello di cluster può essere attivato o disattivato per SVM dall'amministratore del cluster.

    Se l'amministratore del cluster disattiva il MOTD a livello di cluster per una SVM, un utente che accede a SVM non vedrà il MOTD a livello di cluster.

#### Creare un banner

È possibile creare un banner per visualizzare un messaggio a qualcuno che tenta di accedere al cluster o alla SVM. Il banner viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) prima che venga richiesta l'autenticazione a un utente.

**Fasi**

1. Utilizzare `security login banner modify` Comando per creare un banner per il cluster o SVM:

| Se si desidera… | Quindi… |
|---|---|
| Specificare un messaggio che sia una singola riga | Utilizzare `-message` "`text`" per specificare il testo. |
| Includere le newline (note anche come fine delle righe) nel messaggio | Utilizzare il comando senza `-message` oppure `-uri` parametro per avviare la modalità interattiva per la modifica del banner. |
| Carica il contenuto da una posizione da utilizzare per il banner | Utilizzare `-uri` Parametro per specificare la posizione FTP o HTTP del contenuto. |

La dimensione massima di un banner è di 2,048 byte, incluse le newline.

Banner creato utilizzando `-uri` il parametro è statico. Non viene aggiornato automaticamente per riflettere le modifiche successive del contenuto di origine.

Il banner creato per il cluster viene visualizzato anche per tutte le SVM che non dispongono di un banner esistente. Qualsiasi banner creato successivamente per una SVM sovrascrive il banner a livello di cluster per tale SVM. Specifica di `-message` parametro con un trattino tra virgolette doppie (`"-"`) Per SVM ripristina la SVM per l'utilizzo del banner a livello di cluster.

2. Verificare che il banner sia stato creato visualizzandolo con `security login banner show` comando.

   Specifica di `-message` parametro con una stringa vuota (`""`) visualizza i banner che non hanno contenuto.

   Specifica di `-message` parametro con `"-"` Visualizza tutte le SVM (admin o data) che non hanno un banner configurato.

**Esempi di creazione di banner**

Nell'esempio seguente viene utilizzata la modalità non interattiva per creare un banner per il cluster "cluster1":

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

Nell'esempio seguente viene utilizzata la modalità interattiva per creare un banner per "`svm1`"SVM:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

Nell'esempio seguente vengono visualizzati i banner creati:

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

**Informazioni correlate**

Gestione del banner

**Gestione del banner**

È possibile gestire il banner a livello di cluster o SVM. Il banner configurato per il cluster viene utilizzato anche per tutte le SVM che non hanno un messaggio banner definito. Un banner creato successivamente per una SVM sovrascrive il banner del cluster per tale SVM.

**Scelte**

- Gestire il banner a livello di cluster:

| Se si desidera… | Quindi… |
|---|---|
| Creare un banner da visualizzare per tutte le sessioni di accesso CLI | Impostare un banner a livello di cluster:<br><br>`*security login banner modify -vserver *cluster_name* { [-message "text"] |
| [*-uri ftp_or_http_addr*] }*` | Rimuovere il banner per tutti gli accessi (cluster e SVM) |
| Impostare il banner su una stringa vuota (`""`):<br><br>**`security login banner modify -vserver * -message ""`** | Eseguire l'override di un banner creato da un amministratore SVM |

| Se si desidera… | Quindi… |
| --- | --- |
| Modificare il messaggio banner SVM:<br><br>`*security login banner modify -vserver *svm_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }*` |

- Gestire il banner a livello di SVM:

  Specificare `-vserver svm_name` Non è richiesto nel contesto SVM.

| Se si desidera… | Quindi… |
| --- | --- |
| Eseguire l'override del banner fornito dall'amministratore del cluster con un banner diverso per SVM | Creare un banner per SVM:<br><br>`*security login banner modify -vserver *svm_name* { [-message "text"] |
| [-uri ftp_or_http_addr] }*` | Eliminare il banner fornito dall'amministratore del cluster in modo che non venga visualizzato alcun banner per SVM |
| Impostare il banner SVM su una stringa vuota per SVM:<br><br>**`security login banner modify -vserver svm_name -message ""`** | Utilizzare il banner a livello di cluster quando SVM utilizza attualmente un banner a livello di SVM |

#### Creare un MOTD

È possibile creare un messaggio del giorno (MOTD) per comunicare informazioni agli utenti CLI autenticati. Il MOTD viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) dopo l'autenticazione di un utente, ma prima della visualizzazione del prompt della shell dei cluster.

#### Fasi

1. Utilizzare `security login motd modify` Comando per creare un MOTD per il cluster o SVM:

| Se si desidera… | Quindi… |
| --- | --- |
| Specificare un messaggio che sia una singola riga | Utilizzare `-message` "`text`" per specificare il testo. |
| Includi newline (nota anche come fine delle righe) | Utilizzare il comando senza `-message` oppure `-uri` Parametro per avviare la modalità interattiva per la modifica del MOTD. |

| Se si desidera… | Quindi… |
| --- | --- |
| Caricare il contenuto da una posizione da utilizzare per il MOTD | Utilizzare `-uri` Parametro per specificare la posizione FTP o HTTP del contenuto. |

La dimensione massima di un MOTD è di 2,048 byte, incluse le newline.

Il `security login motd modify` La pagina man descrive le sequenze di escape che è possibile utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente.

Un MOTD creato utilizzando `-uri` il parametro è statico. Non viene aggiornato automaticamente per riflettere le modifiche successive del contenuto di origine.

Un MOTD creato per il cluster viene visualizzato anche per tutti gli accessi SVM per impostazione predefinita, insieme a un MOTD a livello di SVM che è possibile creare separatamente per un determinato SVM. Impostazione di `-is-cluster-message-enabled` parametro a. `false` Per una SVM impedisce la visualizzazione del MOTD a livello di cluster per tale SVM.

2. Verificare che il MOTD sia stato creato visualizzandolo con il `security login motd show` comando.

   Specifica di `-message` parametro con una stringa vuota (`""`) Visualizza i MOTD non configurati o privi di contenuto.

   Vedere "modifica del motd di accesso di sicurezza" Pagina man Command per un elenco di parametri da utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente. Controllare la pagina man specifica della versione di ONTAP.

**Esempi di creazione di MOTD**

Nell'esempio seguente viene utilizzata la modalità non interattiva per creare un MOTD per il cluster "cluster1":

```
cluster1::> security login motd modify -message "Greetings!"
```

Nell'esempio seguente viene utilizzata la modalità interattiva per creare un MOTD per la SVM "`svm1`"che utilizza sequenze di escape per visualizzare il contenuto generato dinamicamente:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

Nell'esempio seguente vengono visualizzati i MOTD creati:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-----------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

#### Gestire il MOTD

È possibile gestire il messaggio del giorno (MOTD) a livello di cluster o SVM. Per impostazione predefinita, il MOTD configurato per il cluster è abilitato anche per tutte le SVM. Inoltre, è possibile configurare un MOTD a livello di SVM per ogni SVM. Il MOTD a livello di cluster può essere attivato o disattivato per ogni SVM dall'amministratore del cluster.

Per un elenco delle sequenze di escape che possono essere utilizzate per generare dinamicamente il contenuto per il MOTD, vedere "riferimento al comando".

#### Scelte

- Gestire il MOTD a livello di cluster:

| Se si desidera… | Quindi… |
|---|---|
| Creare un MOTD per tutti gli accessi quando non esiste un MOTD | Impostare un MOTD a livello di cluster:<br><br>`*security login motd modify -vserver *cluster_name* { [-message "*text*"] |
| [-uri *ftp_or_http_addr*] }*` | Modificare il MOTD per tutti gli accessi quando non sono configurati MOTD a livello di SVM |

| Se si desidera… | Quindi… |
| --- | --- |
| Modificare il MOTD a livello di cluster:<br><br>`*security login motd modify -vserver *cluster_name* { [-message "*text*"] } | [-uri ftp_or_http_addr] }*` |
| Rimuovere il MOTD per tutti gli accessi quando non sono configurati MOTD a livello di SVM | Impostare MOTD a livello di cluster su una stringa vuota (`""`):<br><br>**`security login motd modify -vserver *cluster_name* -message ""`** |
| Ogni SVM deve visualizzare il MOTD a livello di cluster invece di utilizzare il MOTD a livello di SVM | Impostare un MOTD a livello di cluster, quindi impostare tutti i MOTD a livello di SVM su una stringa vuota con il MOTD a livello di cluster abilitato:<br><br>a. `*security login motd modify -vserver *cluster_name* { [-message "*text*"] |
| [-uri *ftp_or_http_addr*] }*`<br>.. **`security login motd modify { -vserver !"*cluster_name*" } -message "" -is -cluster-message-enabled true`** | Visualizzare un MOTD solo per le SVM selezionate e non utilizzare alcun MOTD a livello di cluster |
| Impostare MOTD a livello di cluster su una stringa vuota, quindi impostare MOTD a livello di SVM per le SVM selezionate:<br><br>a. **`security login motd modify -vserver *cluster_name* -message ""`**<br>b. `*security login motd modify -vserver *svm_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }*`<br>+<br>È possibile ripetere questo passaggio per ogni SVM in base alle necessità. |
| Utilizzare lo stesso MOTD a livello di SVM per tutte le SVM (dati e amministratore) | Impostare il cluster e tutte le SVM in modo che utilizzino lo stesso MOTD:<br><br>`*security login motd modify *-vserver* * { [-message "*text*"] |
| [-uri *ftp_or_http_addr*] }*`<br><br>[NOTE]<br>====<br>Se si utilizza la modalità interattiva, l'interfaccia CLI richiede di immettere il MOTD singolarmente per il cluster e per ciascuna SVM. È possibile incollare lo stesso MOTD in ogni istanza quando richiesto.<br><br>==== | Disporre di un MOTD a livello di cluster disponibile come opzione per tutte le SVM, ma non si desidera che il MOTD venga visualizzato per gli accessi al cluster |

| Se si desidera… | Quindi… |
| --- | --- |
| Impostare un MOTD a livello di cluster, ma disattivarne la visualizzazione per il cluster:<br><br>`*security login motd modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false*` |
| Rimuovere tutti i MOTD a livello di cluster e SVM quando solo alcune SVM dispongono di MOTD a livello di cluster e SVM | Impostare il cluster e tutte le SVM in modo che utilizzino una stringa vuota per il MOTD:<br><br>**`security login motd modify -vserver * -message ""`** |
| Modificare il MOTD solo per le SVM che hanno una stringa non vuota, quando altre SVM utilizzano una stringa vuota e quando viene utilizzato un MOTD diverso a livello di cluster | Utilizzare le query estese per modificare il MOTD in modo selettivo:<br><br>`*security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"] |
| [-uri *ftp_or_http_addr*] }*` | Visualizza tutti i MOTD che contengono testo specifico (ad esempio “gennaio” seguito da “2015”) in qualsiasi punto di un messaggio singolo o multilinea, anche se il testo è diviso su righe diverse |
| Utilizzare una query per visualizzare i MOTD:<br><br>**`security login motd show -message *"January"*"2015"*`** | Creare in modo interattivo un MOTD che includa più newline consecutive (noto anche come fine delle righe, o EOLS) |

- Gestire il MOTD a livello di SVM:

  Specificare `-vserver svm_name` Non è richiesto nel contesto SVM.

| Se si desidera… | Quindi… |
| --- | --- |
| Utilizzare un MOTD a livello di SVM diverso, quando SVM dispone già di un MOTD a livello di SVM | Modificare il MOTD a livello di SVM:<br><br>`*security login motd modify -vserver *svm_name* { [-message "*text*"] |
| [-uri *ftp_or_http_addr*] }*` | Utilizzare solo il MOTD a livello di cluster per SVM, quando SVM dispone già di un MOTD a livello di SVM |

| Se si desidera… | Quindi… |
| --- | --- |
| Impostare MOTD a livello di SVM su una stringa vuota, quindi chiedere all'amministratore del cluster di attivare MOTD a livello di cluster per SVM:<br>a. **`security login motd modify -vserver *svm_name* -message ""`**<br>b. (Per l'amministratore del cluster) **`security login motd modify -vserver *svm_name* -is-cluster-message-enabled true`** | Non visualizzare alcun MOTD sul display SVM, quando per SVM sono attualmente visualizzati sia i MOTD a livello di cluster che quelli a livello di SVM |

## Gestire i lavori e pianificare

I lavori vengono inseriti in una coda di lavoro ed eseguiti in background quando le risorse sono disponibili. Se un lavoro consuma troppe risorse del cluster, è possibile interromperlo o metterlo in pausa fino a quando non si verifica una minore domanda sul cluster. È inoltre possibile monitorare e riavviare i lavori.

### Categorie di lavoro

È possibile gestire tre categorie di lavori: Affiliati a server, affiliati a cluster e privati.

Un lavoro può essere in una delle seguenti categorie:

- **Lavori affiliati al server**

  Questi job vengono messi in coda dal framework di gestione a un nodo specifico da eseguire.

- **Lavori affiliati a cluster**

  Questi processi vengono messi in coda dal framework di gestione a qualsiasi nodo del cluster da eseguire.

- **Lavori privati**

  Questi lavori sono specifici di un nodo e non utilizzano il database replicato (RDB) o altri meccanismi del cluster. I comandi che gestiscono i processi privati richiedono un livello di privilegio avanzato o superiore.

### Comandi per la gestione dei lavori

Quando si immette un comando che richiama un processo, in genere, il comando informa che il processo è stato messo in coda e ritorna al prompt dei comandi CLI. Tuttavia, alcuni comandi riportano invece l'avanzamento del processo e non ritornano al prompt dei comandi CLI fino al completamento del processo. In questi casi, è possibile premere Ctrl-C per spostare il job in background.

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizza informazioni su tutti i lavori | `job show` |
| Visualizza le informazioni sui job in base al nodo | `job show bynode` |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizzare le informazioni sui job affiliati al cluster | `job show-cluster` |
| Visualizza le informazioni sui lavori completati | `job show-completed` |
| Visualizza le informazioni sulla cronologia dei lavori | `job history show`<br><br>Per ciascun nodo del cluster vengono memorizzati fino a 25,000 record di processi. Di conseguenza, il tentativo di visualizzare l'intera cronologia dei lavori potrebbe richiedere molto tempo. Per evitare tempi di attesa potenzialmente lunghi, è necessario visualizzare i lavori per nodo, SVM (Storage Virtual Machine) o ID record. |
| Visualizzare l'elenco dei processi privati | `job private show` (livello di privilegio avanzato) |
| Visualizza le informazioni sui processi privati completati | `job private show-completed` (livello di privilegio avanzato) |
| Visualizza le informazioni sullo stato di inizializzazione per i job manager | `job initstate show` (livello di privilegio avanzato) |
| Monitorare l'avanzamento di un lavoro | `job watch-progress` |
| Monitorare l'avanzamento di un processo privato | `job private watch-progress` (livello di privilegio avanzato) |
| Mettere in pausa un lavoro | `job pause` |
| Mettere in pausa un processo privato | `job private pause` (livello di privilegio avanzato) |
| Riprendere un processo in pausa | `job resume` |
| Riprendere un processo privato in pausa | `job private resume` (livello di privilegio avanzato) |
| Interrompere un lavoro | `job stop` |
| Interruzione di un processo privato | `job private stop` (livello di privilegio avanzato) |
| Eliminare un lavoro | `job delete` |
| Eliminare un processo privato | `job private delete` (livello di privilegio avanzato) |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Disassociare un lavoro affiliato al cluster a un nodo non disponibile che lo possiede, in modo che un altro nodo possa assumere la proprietà di tale lavoro | `job unclaim` (livello di privilegio avanzato) |

È possibile utilizzare `event log show` per determinare il risultato di un lavoro completato.

**Informazioni correlate**

"Comandi di ONTAP 9"

### Comandi per la gestione delle pianificazioni dei processi

Molte attività, ad esempio le copie Snapshot dei volumi, possono essere configurate per l'esecuzione su pianificazioni specificate.le pianificazioni eseguite in orari specifici sono denominate *cron* schedules (simili a UNIX `cron` pianificazioni). Le pianificazioni eseguite a intervalli sono denominate *interval* schedules. Si utilizza `job schedule` comandi per gestire le pianificazioni dei processi.

Le pianificazioni dei processi non vengono regolate in base alle modifiche manuali della data e dell'ora del cluster. Questi processi vengono pianificati per essere eseguiti in base all'ora corrente del cluster in cui è stato creato il processo o quando è stato eseguito più di recente. Pertanto, se si modifica manualmente la data o l'ora del cluster, utilizzare `job show` e. `job history show` comandi per verificare che tutti i processi pianificati siano messi in coda e completati in base alle proprie esigenze.

Se il cluster fa parte di una configurazione MetroCluster, le pianificazioni dei processi su entrambi i cluster devono essere identiche. Pertanto, se si crea, modifica o elimina una pianificazione del processo, è necessario eseguire la stessa operazione sul cluster remoto.

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizza le informazioni su tutti i programmi | `job schedule show` |
| Visualizza l'elenco dei lavori in base alla pianificazione | `job schedule show-jobs` |
| Visualizza le informazioni sulle pianificazioni cron | `job schedule cron show` |
| Visualizza le informazioni sulle pianificazioni degli intervalli | `job schedule interval show` |
| Creare un calendario di cron | `job schedule cron create`<br><br>A partire da ONTAP 9.10.1, puoi includere la SVM per la pianificazione del lavoro. |
| Creare una pianificazione a intervalli | `job schedule interval create`<br><br>Specificare almeno uno dei seguenti parametri: `-days`, `-hours`, `-minutes`, o. `-seconds`. |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Modificare una pianificazione cron | `job schedule cron modify` |
| Modificare una pianificazione di intervalli | `job schedule interval modify` |
| Eliminare un programma | `job schedule delete` |
| Eliminare una pianificazione cron | `job schedule cron delete` |
| Eliminare una pianificazione di intervalli | `job schedule interval delete` |

**Informazioni correlate**

"Comandi di ONTAP 9"

## Backup e ripristino delle configurazioni del cluster (solo amministratori del cluster)

### Quali sono i file di backup della configurazione

I file di backup della configurazione sono file di archivio (.7z) che contengono informazioni per tutte le opzioni configurabili necessarie per il corretto funzionamento del cluster e dei nodi al suo interno.

Questi file memorizzano la configurazione locale di ciascun nodo, oltre alla configurazione replicata a livello di cluster. I file di backup della configurazione vengono utilizzati per eseguire il backup e il ripristino della configurazione del cluster.

Esistono due tipi di file di backup della configurazione:

- **File di backup della configurazione del nodo**

  Ogni nodo integro nel cluster include un file di backup della configurazione del nodo, che contiene tutte le informazioni di configurazione e i metadati necessari per il funzionamento corretto del nodo nel cluster.

- **File di backup della configurazione del cluster**

  Questi file includono un archivio di tutti i file di backup della configurazione del nodo nel cluster, oltre alle informazioni di configurazione del cluster replicate (il database replicato o il file RDB). I file di backup della configurazione del cluster consentono di ripristinare la configurazione dell'intero cluster o di qualsiasi nodo del cluster. I programmi di backup della configurazione del cluster creano automaticamente questi file e li memorizzano su diversi nodi del cluster.

> I file di backup della configurazione contengono solo informazioni di configurazione. Non includono dati dell'utente. Per informazioni sul ripristino dei dati utente, vedere "Protezione dei dati".

### Modalità di backup automatico delle configurazioni del nodo e del cluster

Tre pianificazioni separate creano automaticamente i file di backup della configurazione

del cluster e del nodo e li replicano tra i nodi del cluster.

I file di backup della configurazione vengono creati automaticamente in base alle seguenti pianificazioni:

- Ogni 8 ore
- Ogni giorno
- Settimanale

In ciascuna di queste situazioni, viene creato un file di backup della configurazione del nodo su ciascun nodo integro del cluster. Tutti questi file di backup della configurazione del nodo vengono quindi raccolti in un singolo file di backup della configurazione del cluster insieme alla configurazione del cluster replicata e salvati su uno o più nodi del cluster.

#### Comandi per la gestione delle pianificazioni di backup della configurazione

### È possibile utilizzare `system configuration backup settings` comandi per gestire le pianificazioni di backup della configurazione.

Questi comandi sono disponibili a livello di privilegio avanzato.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Modificare le impostazioni per una pianificazione di backup della configurazione:<br>• Specificare un URL remoto (HTTP, HTTPS, FTP, FTPS o TFTP ) in cui verranno caricati i file di backup della configurazione oltre alle posizioni predefinite nel cluster<br>• Specificare un nome utente da utilizzare per accedere all'URL remoto<br>• Impostare il numero di backup da conservare per ogni pianificazione di backup della configurazione | `system configuration backup settings modify`<br><br>Quando si utilizza HTTPS nell'URL remoto, utilizzare `-validate-certification` opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita.<br><br>Il server Web su cui si sta caricando il file di backup della configurazione deve avere ATTIVATO le operazioni HTTP e POST per HTTPS. Per ulteriori informazioni, consultare la documentazione del server Web. |
| Impostare la password da utilizzare per accedere all'URL remoto | `system configuration backup settings set-password` |
| Visualizzare le impostazioni per la pianificazione del backup della configurazione | `system configuration backup settings show`<br><br>Impostare `-instance` parametro per visualizzare il nome utente e il numero di backup da conservare per ciascuna pianificazione. |

#### Comandi per la gestione dei file di backup della configurazione

Si utilizza `system configuration backup` comandi per gestire i file di backup della configurazione del cluster e del nodo.

Questi comandi sono disponibili a livello di privilegio avanzato.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Creare un nuovo file di backup della configurazione del nodo o del cluster | `system configuration backup create` |
| Copiare un file di backup della configurazione da un nodo a un altro nel cluster | `system configuration backup copy` |
| Caricare un file di backup della configurazione da un nodo del cluster a un URL remoto (FTP, HTTP, HTTPS, TFTP o FTPS) | `system configuration backup upload`<br><br>Quando si utilizza HTTPS nell'URL remoto, utilizzare `-validate-certification` opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita.<br><br>Il server Web su cui si sta caricando il file di backup della configurazione deve avere ATTIVATO le operazioni HTTP e POST per HTTPS. Alcuni server Web potrebbero richiedere l'installazione di un modulo aggiuntivo. Per ulteriori informazioni, consultare la documentazione del server Web. I formati URL supportati variano in base alla versione di ONTAP. Consultare la guida della riga di comando per la versione di ONTAP in uso. |
| Scaricare un file di backup della configurazione da un URL remoto a un nodo del cluster e, se specificato, validare il certificato digitale | `system configuration backup download`<br><br>Quando si utilizza HTTPS nell'URL remoto, utilizzare `-validate-certification` opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita. |
| Rinominare un file di backup della configurazione su un nodo del cluster | `system configuration backup rename` |
| Visualizzare i file di backup della configurazione del nodo e del cluster per uno o più nodi nel cluster | `system configuration backup show` |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Eliminare un file di backup della configurazione su un nodo | `system configuration backup delete`<br>Questo comando elimina il file di backup della configurazione solo sul nodo specificato. Se il file di backup della configurazione esiste anche su altri nodi del cluster, rimane su questi nodi. |

#### Trovare un file di backup della configurazione da utilizzare per il ripristino di un nodo

Per ripristinare la configurazione di un nodo, si utilizza un file di backup della configurazione situato in un URL remoto o su un nodo del cluster.

**A proposito di questa attività**

È possibile utilizzare un file di backup della configurazione del cluster o del nodo per ripristinare la configurazione di un nodo.

**Fase**

1. Rendere disponibile il file di backup della configurazione nel nodo per il quale si desidera ripristinare la configurazione.

| Se si trova il file di backup della configurazione… | Quindi… |
| --- | --- |
| A un URL remoto | Utilizzare `system configuration backup download` al livello di privilegio avanzato per scaricarlo nel nodo di ripristino. |
| Su un nodo del cluster | a. Utilizzare `system configuration backup show` al livello di privilegio avanzato per visualizzare l'elenco dei file di backup della configurazione disponibili nel cluster che contiene la configurazione del nodo di ripristino.<br>b. Se il file di backup della configurazione identificato non esiste nel nodo di ripristino, utilizzare `system configuration backup copy` comando per copiarlo nel nodo di ripristino. |

Se in precedenza è stato ricreato il cluster, è necessario scegliere un file di backup della configurazione creato dopo la ricreazione del cluster. Se è necessario utilizzare un file di backup della configurazione creato prima della ricostruzione del cluster, dopo il ripristino del nodo, è necessario ricreare il cluster.

#### Ripristinare la configurazione del nodo utilizzando un file di backup della configurazione

La configurazione del nodo viene ripristinata utilizzando il file di backup della

configurazione identificato e reso disponibile al nodo di ripristino.

**A proposito di questa attività**

Eseguire questa attività solo per eseguire il ripristino da un disastro che ha causato la perdita dei file di configurazione locale del nodo.

**Fasi**

1. Passare al livello di privilegio avanzato:

   `set -privilege advanced`

2. Se il nodo è integro, utilizzare il livello di privilegio avanzato di un nodo diverso `cluster modify` con il `-node` e. `-eligibility` parametri per contrassegnarlo come non idoneo e isolarlo dal cluster.

   Se il nodo non è integro, saltare questo passaggio.

   Questo esempio modifica il node2 in modo che non sia idoneo a partecipare al cluster in modo che la sua configurazione possa essere ripristinata:

   ```
   cluster1::*> cluster modify -node node2 -eligibility false
   ```

3. Utilizzare `system configuration recovery node restore` al livello di privilegio avanzato per ripristinare la configurazione del nodo da un file di backup della configurazione.

   Se il nodo perde la propria identità, compreso il nome, utilizzare il `-nodename-in-backup` parametro per specificare il nome del nodo nel file di backup della configurazione.

   Questo esempio ripristina la configurazione del nodo utilizzando uno dei file di backup della configurazione memorizzati nel nodo:

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
            command only to recover from a disaster that resulted
            in the loss of the local configuration files.
            The node will reboot after restoring the local configuration.
   Do you want to continue? {y|n}: y
   ```

   La configurazione viene ripristinata e il nodo viene riavviato.

4. Se il nodo è stato contrassegnato come non idoneo, utilizzare `system configuration recovery cluster sync` per contrassegnare il nodo come idoneo e sincronizzarlo con il cluster.
5. Se si utilizza un ambiente SAN, utilizzare `system node reboot` Comando per riavviare il nodo e ristabilire il quorum SAN.

**Al termine**

Se in precedenza è stato ricreato il cluster e si sta ripristinando la configurazione del nodo utilizzando un file di backup della configurazione creato prima della ricreazione del cluster, è necessario ricrearlo di nuovo.

### Trovare una configurazione da utilizzare per il ripristino di un cluster

## La configurazione viene utilizzata da un nodo del cluster o da un file di backup della configurazione del cluster per ripristinare un cluster.

#### Fasi

1. Scegliere un tipo di configurazione per ripristinare il cluster.

   - Un nodo nel cluster

     Se il cluster è costituito da più di un nodo e uno di essi ha una configurazione del cluster da quando il cluster si trovava nella configurazione desiderata, è possibile ripristinare il cluster utilizzando la configurazione memorizzata su tale nodo.

     Nella maggior parte dei casi, il nodo contenente l'anello di replica con l'ID transazione più recente è il nodo migliore da utilizzare per ripristinare la configurazione del cluster. Il `cluster ring show` il comando a livello di privilegio avanzato consente di visualizzare un elenco degli anelli replicati disponibili su ciascun nodo del cluster.

   - Un file di backup della configurazione del cluster

     Se non si riesce a identificare un nodo con la corretta configurazione del cluster o se il cluster è costituito da un singolo nodo, è possibile utilizzare un file di backup della configurazione del cluster per ripristinare il cluster.

   Se si sta ripristinando il cluster da un file di backup della configurazione, le modifiche apportate alla configurazione dopo l'esecuzione del backup andranno perse. Dopo il ripristino, è necessario risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione attuale. Consultare l'articolo della Knowledge base "Guida alla risoluzione dei problemi di backup per la configurazione di ONTAP" per indicazioni sulla risoluzione dei problemi.

2. Se si sceglie di utilizzare un file di backup della configurazione del cluster, rendere il file disponibile per il nodo che si intende utilizzare per ripristinare il cluster.

| Se si trova il file di backup della configurazione… | Quindi… |
|---|---|
| A un URL remoto | Utilizzare `system configuration backup download` al livello di privilegio avanzato per scaricarlo nel nodo di ripristino. |

| Se si trova il file di backup della configurazione… | Quindi… |
| --- | --- |
| Su un nodo del cluster | a. Utilizzare `system configuration backup show` al livello di privilegio avanzato per trovare un file di backup della configurazione del cluster creato quando il cluster si trovava nella configurazione desiderata.<br>b. Se il file di backup della configurazione del cluster non si trova nel nodo che si intende utilizzare per ripristinare il cluster, utilizzare `system configuration backup copy` comando per copiarlo nel nodo di ripristino. |

#### Ripristinare una configurazione del cluster da una configurazione esistente

Per ripristinare una configurazione del cluster da una configurazione esistente in seguito a un errore del cluster, ricrearlo utilizzando la configurazione del cluster scelta e resa disponibile al nodo di ripristino, quindi riconnettersi ciascun nodo aggiuntivo al nuovo cluster.

**A proposito di questa attività**

Questa attività deve essere eseguita solo per il ripristino da un disastro che ha causato la perdita della configurazione del cluster.

> Se si sta ricreando il cluster da un file di backup della configurazione, contattare il supporto tecnico per risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione presente nel cluster.
>
> Se si sta ripristinando il cluster da un file di backup della configurazione, le modifiche apportate alla configurazione dopo l'esecuzione del backup andranno perse. Dopo il ripristino, è necessario risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione attuale. Consultare l'articolo della Knowledge base "Guida alla risoluzione dei problemi per il backup della configurazione di ONTAP".

**Fasi**

1. Disattivare il failover dello storage per ciascuna coppia ha:

   ```
   storage failover modify -node node_name -enabled false
   ```

   È necessario disattivare il failover dello storage una sola volta per ogni coppia ha. Quando si disattiva il failover dello storage per un nodo, anche il failover dello storage viene disattivato sul partner del nodo.

2. Arrestare ciascun nodo ad eccezione del nodo di ripristino:

   ```
   system node halt -node node_name -reason "text"
   ```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Impostare il livello di privilegio su Advanced (avanzato):

   **`set -privilege advanced`**

4. Nel nodo di ripristino, utilizzare **`system configuration recovery cluster recreate`** per ricreare il cluster.

   In questo esempio viene ricreato il cluster utilizzando le informazioni di configurazione memorizzate nel nodo di ripristino:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

   Viene creato un nuovo cluster sul nodo di ripristino.

5. Se si sta ricreando il cluster da un file di backup della configurazione, verificare che il ripristino del cluster sia ancora in corso:

   **`system configuration recovery cluster show`**

   Non è necessario verificare lo stato di ripristino del cluster se si sta ricreando il cluster da un nodo integro.

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. Avviare ogni nodo che deve essere ricongiungersi al cluster ricreato.

   È necessario riavviare i nodi uno alla volta.

7. Per ogni nodo che deve essere Unito al cluster ricreato, procedere come segue:

   a. Da un nodo integro nel cluster ricreato, ricongiungersi al nodo di destinazione:

      **`system configuration recovery cluster rejoin -node node_name`**

      Questo esempio ricongiunge il nodo di destinazione “node2” al cluster ricreato:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Il nodo di destinazione viene riavviato e quindi Unito al cluster.

b. Verificare che il nodo di destinazione sia integro e che abbia formato il quorum con gli altri nodi del cluster:

   **`cluster show -eligibility true`**

   Il nodo di destinazione deve riconnettersi al cluster ricreato prima di poter riconnettersi a un altro nodo.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. Se il cluster è stato ricreato da un file di backup della configurazione, impostare lo stato di ripristino su complete (completo):

   **`system configuration recovery cluster modify -recovery-status complete`**

9. Tornare al livello di privilegio admin:

   **`set -privilege admin`**

10. Se il cluster è costituito da due soli nodi, utilizzare **`cluster ha modify`** Comando per riabilitare il cluster ha.

11. Utilizzare **`storage failover modify`** Comando per riabilitare il failover dello storage per ogni coppia ha.

**Al termine**

Se il cluster dispone di relazioni peer SnapMirror, è necessario ricrearle. Per ulteriori informazioni, vedere "Protezione dei dati".

### Sincronizzare un nodo con il cluster

Se esiste un quorum a livello di cluster, ma uno o più nodi non sono sincronizzati con il

cluster, è necessario sincronizzare il nodo per ripristinare il database replicato (RDB) sul nodo e portarlo in quorum.

**Fase**

1. Da un nodo integro, utilizzare `system configuration recovery cluster sync` al livello di privilegio avanzato per sincronizzare il nodo non sincronizzato con la configurazione del cluster.

   Questo esempio sincronizza un nodo (*node2*) con il resto del cluster:

   ```
   cluster1::*> system configuration recovery cluster sync -node node2

   Warning: This command will synchronize node "node2" with the cluster
            configuration, potentially overwriting critical cluster
            configuration files on the node. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress. This
            command will cause all the cluster applications on node
            "node2" to restart, interrupting administrative CLI and Web
            interface on that node.
   Do you want to continue? {y|n}: y
   All cluster applications on node "node2" will be restarted. Verify that
   the cluster applications go online.
   ```

**Risultato**

L'RDB viene replicato nel nodo e il nodo diventa idoneo a partecipare al cluster.

## Gestire i core dump (solo amministratori del cluster)

Quando un nodo esegue il panic, si verifica un core dump e il sistema crea un core dump file che il supporto tecnico può utilizzare per risolvere il problema. È possibile configurare o visualizzare gli attributi di core dump. È inoltre possibile salvare, visualizzare, segmentare, caricare o eliminare un file core dump.

Puoi gestire i core dump nei seguenti modi:

- Configurazione dei core dump e visualizzazione delle impostazioni di configurazione
- Visualizzazione delle informazioni di base, dello stato e degli attributi dei core dump

  I file di dump e i report principali vengono memorizzati in `/mroot/etc/crash/` directory di un nodo. È possibile visualizzare il contenuto della directory utilizzando `system node coredump` o un browser web.

- Salvare il contenuto del core dump e caricare il file salvato in una posizione specifica o nel supporto tecnico

  ONTAP impedisce di avviare il salvataggio di un file di dump core durante un takeover, un trasferimento aggregato o un giveback.

- Eliminazione dei file core dump non più necessari

### Comandi per la gestione dei core dump

Si utilizza `system node coredump config` comandi per gestire la configurazione dei core dump, il `system node coredump` comandi per gestire i file core dump e il `system node coredump reports` comandi per gestire i report principali dell'applicazione.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Configurare i core dump | `system node coredump config modify` |
| Visualizzare le impostazioni di configurazione per i core dump | `system node coredump config show` |
| Visualizza informazioni di base sui core dump | `system node coredump show` |
| Attivare manualmente un core dump quando si riavvia un nodo | `system node reboot` con entrambi `-dump` e. `-skip-lif-migration-before-reboot` parametri<br>Il `skip-lif-migration-before-reboot` Parametro specifica che la migrazione LIF prima di un riavvio verrà ignorata. |
| Attivare manualmente un core dump quando si chiude un nodo | `system node halt` con entrambi `-dump` e. `-skip-lif-migration-before-shutdown` parametri<br>Il `skip-lif-migration-before-shutdown` Parametro specifica che la migrazione LIF prima di un arresto verrà ignorata. |
| Salvare un core dump specificato | `system node coredump save` |
| Salva tutti i core dump non salvati che si trovano su un nodo specificato | `system node coredump save-all` |
| Generare e inviare un messaggio AutoSupport con un file core dump specificato | `system node autosupport invoke-core-upload`<br>Il `-uri` Il parametro opzionale specifica una destinazione alternativa per il messaggio AutoSupport. |
| Visualizza informazioni sullo stato dei core dump | `system node coredump status` |
| Eliminare un core dump specificato | `system node coredump delete` |

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Eliminare tutti i core dump non salvati o tutti i file core salvati su un nodo | `system node coredump delete-all` |
| Visualizza i report di dump del core dell'applicazione | `system node coredump reports show` |
| Eliminare un report di dump del core dell'applicazione | `system node coredump reports delete` |

**Informazioni correlate**

"Comandi di ONTAP 9"

# Gestione di dischi e Tier (aggregato)

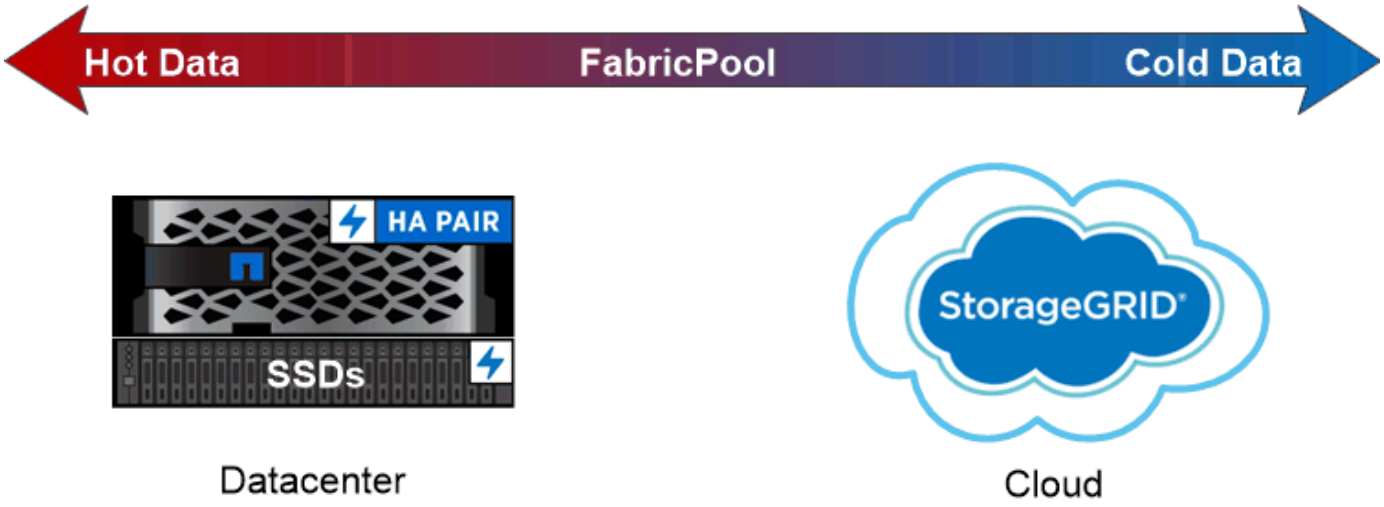
## Panoramica su dischi e Tier locali (aggregati)

È possibile gestire lo storage fisico di ONTAP utilizzando Gestione di sistema e l'interfaccia CLI. È possibile creare, espandere e gestire i Tier locali (aggregati), lavorare con i Tier locali di Flash Pool (aggregati), gestire i dischi e gestire le policy RAID.

### Quali sono i Tier locali (aggregati)

*Tier locali* (denominati anche *aggregati*) sono contenitori per i dischi gestiti da un nodo. È possibile utilizzare i Tier locali per isolare i carichi di lavoro con esigenze di performance diverse, per tierare i dati con diversi modelli di accesso o per separare i dati per scopi normativi.

- Per le applicazioni business-critical che richiedono la latenza più bassa possibile e le performance più elevate, è possibile creare un Tier locale composto interamente da SSD.
- Per tierare i dati con diversi modelli di accesso, è possibile creare un *Tier locale ibrido*, implementando la flash come cache dalle performance elevate per un set di dati funzionante, utilizzando al contempo HDD a basso costo o storage a oggetti per i dati ad accesso meno frequente.
  - Un *Flash Pool* è costituito da SSD e HDD.
  - Un *FabricPool* è costituito da un Tier locale all-SSD con un archivio di oggetti collegato.
- Se è necessario separare i dati archiviati dai dati attivi per scopi normativi, è possibile utilizzare un Tier locale costituito da HDD con capacità o una combinazione di HDD con capacità e performance.




*You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.*

**Lavorare con i Tier locali (aggregati)**

È possibile eseguire le seguenti operazioni:

- "Gestire i Tier locali (aggregati)"
- "Gestire i dischi"
- "Gestire le configurazioni RAID"
- "Gestire i Tier di Flash Pool"

Eseguire queste attività se si verificano le seguenti condizioni:

- Non si desidera utilizzare uno strumento di scripting automatico.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si dispone di una configurazione MetroCluster e si stanno seguendo le procedure descritte in "MetroCluster" documentazione per la configurazione iniziale e linee guida per tier locali (aggregati) e gestione dei dischi.

**Informazioni correlate**

- "Gestire i Tier cloud FabricPool"

## Gestire i Tier locali (aggregati)

**Gestire i Tier locali (aggregati)**

Puoi utilizzare System Manager o la CLI di ONTAP per aggiungere Tier locali (aggregati), gestirne l'utilizzo e aggiungere capacità (dischi) agli stessi.

È possibile eseguire le seguenti operazioni:

- "Aggiungere (creare) un Tier locale (aggregato)"

  Per aggiungere un Tier locale, si segue un workflow specifico. Si determina il numero di dischi o partizioni di dischi necessari per il Tier locale e si decide quale metodo utilizzare per creare il Tier locale. È possibile aggiungere automaticamente i Tier locali consentendo a ONTAP di assegnare la configurazione oppure specificarla manualmente.

- "Gestire l'utilizzo di Tier locali (aggregati)"

  Per i Tier locali esistenti, è possibile rinominarli, impostarne i costi dei supporti o determinare le informazioni sul disco e sul gruppo RAID. È possibile modificare la configurazione RAID di un Tier locale e assegnare Tier locali alle VM di storage (SVM). È possibile modificare la configurazione RAID di un Tier locale e assegnare Tier locali alle VM di storage (SVM). È possibile determinare quali volumi risiedono su un Tier locale e la quantità di spazio utilizzata su un Tier locale. È possibile controllare lo spazio che i volumi possono utilizzare. È possibile trasferire la proprietà del Tier locale con una coppia ha. È anche possibile eliminare un Tier locale.

- "Aggiunta di capacità (dischi) a un Tier locale (aggregato)"

  Utilizzando metodi diversi, si segue un workflow specifico per aggiungere capacità. È possibile aggiungere dischi a un Tier locale e dischi a un nodo o a uno shelf. Se necessario, è possibile correggere le partizioni spare disallineate.

## Aggiungere (creare) un Tier locale (aggregato)

### Aggiunta di un Tier locale (creazione di un aggregato)

Per aggiungere un Tier locale (creare un aggregato), si segue un workflow specifico.

Si determina il numero di dischi o partizioni di dischi necessari per il Tier locale e si decide quale metodo utilizzare per creare il Tier locale. È possibile aggiungere automaticamente i Tier locali consentendo a ONTAP di assegnare la configurazione oppure specificarla manualmente.

- "Workflow per aggiungere un Tier locale (aggregato)"
- "Determinare il numero di dischi o partizioni richiesto per un Tier locale (aggregato)"
- "Decidere quale metodo di creazione del Tier locale (aggregato) utilizzare"
- "Aggiungere automaticamente i Tier locali (aggregati)"
- "Aggiungere manualmente i Tier locali (aggregati)"

### Workflow per aggiungere un Tier locale (aggregato)

La creazione di Tier locali (aggregati) fornisce storage ai volumi del sistema.

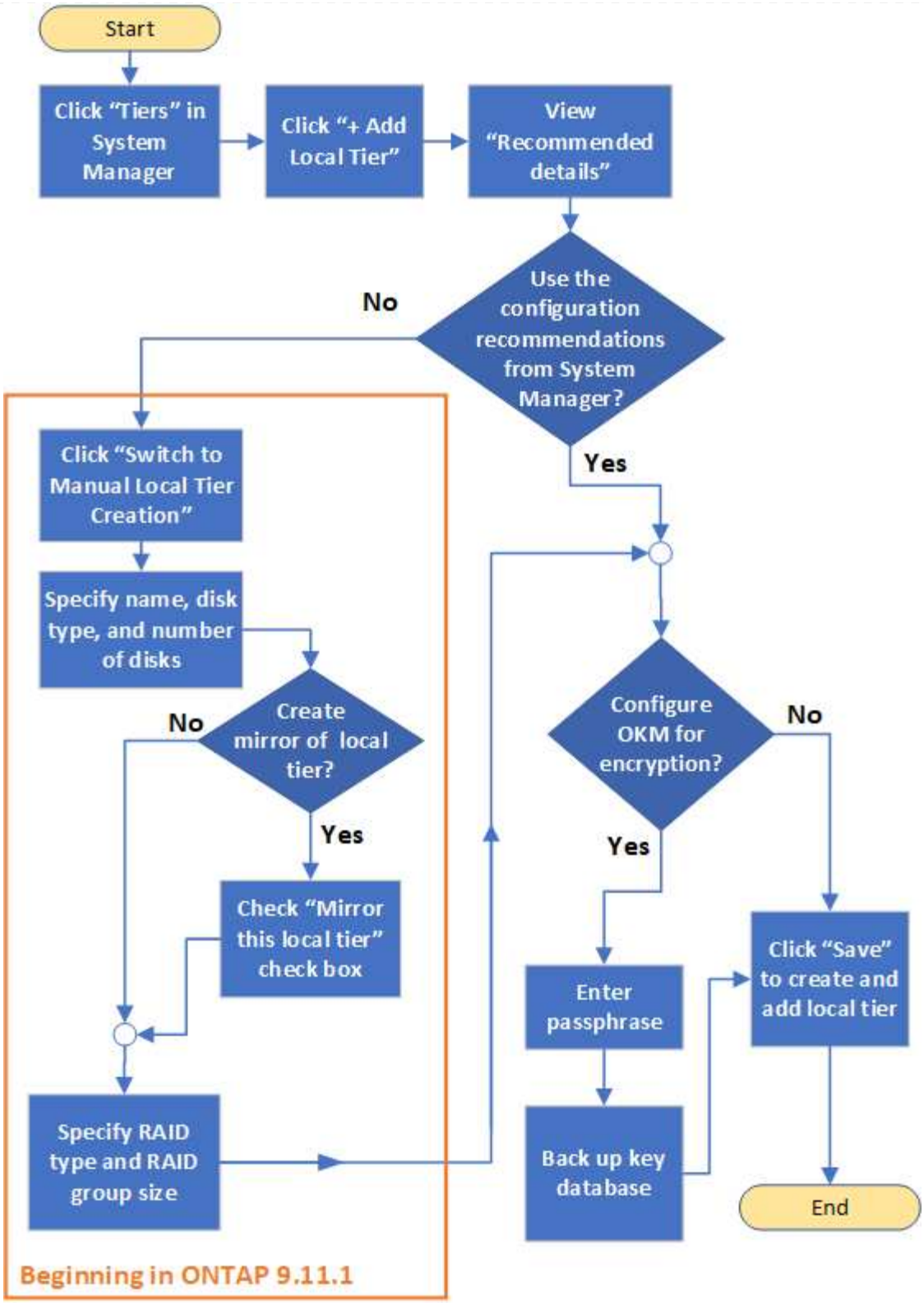
Il flusso di lavoro per la creazione di Tier locali (aggregati) è specifico dell'interfaccia utilizzata: System Manager o CLI:

**Workflow di System Manager**

### Utilizzare System Manager per aggiungere (creare) un Tier locale

System Manager crea Tier locali in base alle Best practice consigliate per la configurazione dei Tier locali.

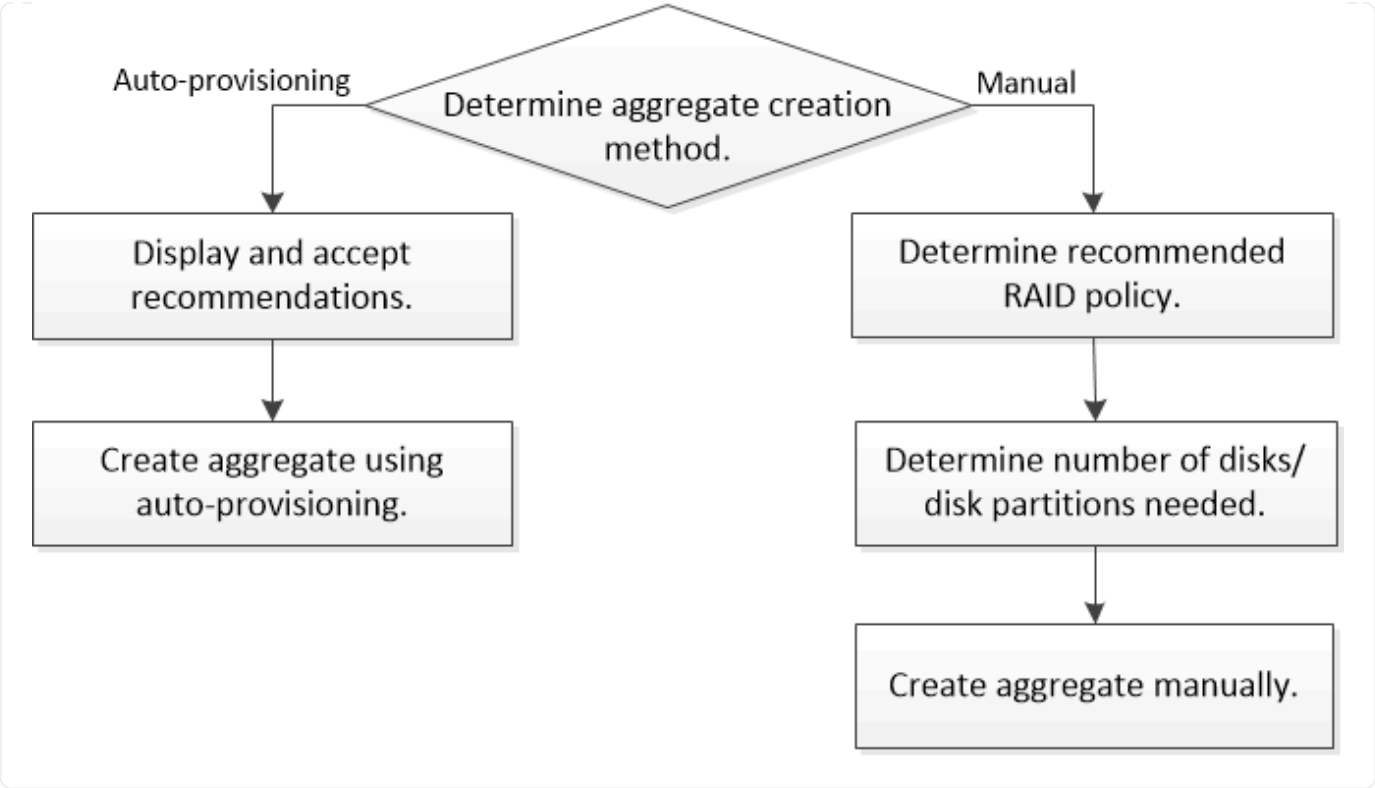
A partire da ONTAP 9.11.1, è possibile configurare manualmente i Tier locali se si desidera una configurazione diversa da quella consigliata durante il processo automatico per aggiungere un Tier locale.




**Workflow CLI**

**Utilizzare la CLI per aggiungere (creare) un aggregato**

A partire da ONTAP 9.2, ONTAP è in grado di fornire le configurazioni consigliate per la creazione di aggregati (provisioning automatico). Se le configurazioni consigliate, basate sulle Best practice, sono appropriate nel proprio ambiente, è possibile accettarle per creare gli aggregati. In caso contrario, è possibile creare gli aggregati manualmente.




#### Determinare il numero di dischi o partizioni richiesto per un Tier locale (aggregato)

È necessario disporre di un numero di dischi o partizioni di dischi sufficiente nel Tier locale (aggregato) per soddisfare i requisiti di sistema e di business. Per ridurre al minimo il potenziale di perdita di dati, si consiglia di utilizzare il numero consigliato di dischi hot spare o partizioni hot spare.

La partizione dei dati root è attivata per impostazione predefinita in alcune configurazioni. I sistemi con partizione dei dati root abilitata utilizzano partizioni di dischi per creare Tier locali. I sistemi che non hanno la partizione dei dati root abilitata utilizzano dischi non partizionati.

È necessario disporre di dischi o partizioni sufficienti per soddisfare il numero minimo richiesto per la policy RAID e per soddisfare i requisiti minimi di capacità.

> In ONTAP, lo spazio utilizzabile del disco è inferiore alla capacità fisica del disco. È possibile trovare lo spazio utilizzabile di un disco specifico e il numero minimo di dischi o partizioni richiesto per ogni criterio RAID in "Hardware Universe".

#### Determinare lo spazio utilizzabile di un disco specifico

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

**System Manager**

**Utilizzare System Manager per determinare lo spazio utilizzabile dei dischi**

Per visualizzare le dimensioni utilizzabili di un disco, procedere come segue:

**Fasi**

1. Accedere a **Storage > Tier**
2. Fare clic su ⋮ accanto al nome del tier locale.
3. Selezionare la scheda **Disk Information** (informazioni disco).

**CLI**

**Utilizzare la CLI per determinare lo spazio utilizzabile dei dischi**

Per visualizzare le dimensioni utilizzabili di un disco, procedere come segue:

**Fase**

1. Visualizzare le informazioni sul disco spare:

```
storage aggregate show-spare-disks
```

Oltre al numero di dischi o partizioni di dischi necessari per creare il gruppo RAID e soddisfare i requisiti di capacità, è necessario disporre del numero minimo di dischi hot spare o di partizioni di dischi hot spare consigliato per l'aggregato:

- Per tutti gli aggregati flash, è necessario disporre di almeno un disco hot spare o di una partizione del disco.

  > Per impostazione predefinita, AFF C190 non dispone di unità spare. Questa eccezione è completamente supportata.

- Per gli aggregati omogenei non flash, è necessario disporre di almeno due dischi hot spare o partizioni di dischi.
- Per i pool di storage SSD, è necessario disporre di almeno un disco hot spare per ogni coppia ha.
- Per gli aggregati Flash Pool, è necessario disporre di almeno due dischi di riserva per ogni coppia ha. Per ulteriori informazioni sui criteri RAID supportati per gli aggregati di Flash Pool, consultare la sezione "Hardware Universe".
- Per supportare l'utilizzo del Centro di manutenzione ed evitare problemi causati da guasti a più dischi simultanei, è necessario disporre di un minimo di quattro hot spare nei carrier multi-disco.

**Informazioni correlate**

"NetApp Hardware Universe"

"Report tecnico di NetApp 3838: Guida alla configurazione del sottosistema di storage"

#### Decidere quale metodo utilizzare per creare Tier locali (aggregati)

Sebbene ONTAP fornisca consigli sulle Best practice per l'aggiunta automatica di Tier locali (creazione di aggregati con provisioning automatico), è necessario determinare se

le configurazioni consigliate sono supportate nel proprio ambiente. In caso contrario, è necessario prendere decisioni in merito alla policy RAID e alla configurazione del disco, quindi creare manualmente i Tier locali.

Quando viene creato automaticamente un Tier locale, ONTAP analizza i dischi spare disponibili nel cluster e genera un consiglio su come utilizzare i dischi spare per aggiungere Tier locali in base alle Best practice. ONTAP visualizza le configurazioni consigliate. È possibile accettare i consigli o aggiungere manualmente i Tier locali.

#### Prima di poter accettare le raccomandazioni ONTAP

In presenza di una delle seguenti condizioni di disco, è necessario affrontarle prima di accettare le raccomandazioni di ONTAP:

- Dischi mancanti
- Fluttuazione nei numeri dei dischi spare
- Dischi non assegnati
- Parti di ricambio non azzerate
- Dischi sottoposti a test di manutenzione

Il `storage aggregate auto-provision` la pagina man contiene ulteriori informazioni su questi requisiti.

#### Quando è necessario utilizzare il metodo manuale

In molti casi, il layout consigliato del Tier locale sarà ottimale per il tuo ambiente. Tuttavia, se nel cluster è in esecuzione ONTAP 9.1 o versioni precedenti o se l'ambiente include le seguenti configurazioni, è necessario creare il Tier locale utilizzando il metodo manuale.

> A partire da ONTAP 9.11.1, è possibile aggiungere manualmente i Tier locali con Gestore di sistema.

- Aggregati che utilizzano LUN di array di terze parti
- Dischi virtuali con Cloud Volumes ONTAP o ONTAP Select
- Sistema MetroCluster
- SyncMirror
- Dischi MSATA
- Tier FlashPool (aggregati)
- Al nodo sono collegati diversi tipi o dimensioni di dischi

#### Selezionare il metodo per creare Tier locali (aggregati)

Scegliere il metodo da utilizzare:

- "Aggiungere (creare) livelli locali (aggregati) automaticamente"
- "Aggiungere (creare) Tier locali (aggregati) manualmente"

#### Informazioni correlate

"Comandi di ONTAP 9"

#### Aggiunta automatica di Tier locali (creazione di aggregati con provisioning automatico)

Se il consiglio delle Best practice fornito da ONTAP per l'aggiunta automatica di un Tier locale (creazione di un aggregato con provisioning automatico) è appropriato nel tuo ambiente, puoi accettare il consiglio e lasciare che ONTAP aggiunga il Tier locale.

**Prima di iniziare**

I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato). Se il cluster non è configurato per l'utilizzo dell'assegnazione automatica della proprietà del disco, è necessario "assegnare la proprietà manualmente".

**System Manager**

**Fasi**

1. In System Manager, fare clic su **Storage > Tier**.
2. Nella pagina **Tier**, fare clic su + Add Local Tier per creare un nuovo tier locale:

   La pagina **Add Local Tier** mostra il numero consigliato di Tier locali che possono essere creati sui nodi e lo storage utilizzabile disponibile.

3. Fare clic su **Recommended details** (Dettagli consigliati) per visualizzare la configurazione consigliata da System Manager.

   System Manager visualizza le seguenti informazioni a partire da ONTAP 9.8:

   - **Nome livello locale** (è possibile modificare il nome del livello locale che inizia con ONTAP 9.10.1)
   - **Nome nodo**
   - **Dimensione utilizzabile**
   - **Tipo di storage**

     A partire da ONTAP 9.10.1, vengono visualizzate ulteriori informazioni:

   - **Dischi**: Indica il numero, la dimensione e il tipo dei dischi
   - **Layout**: Mostra il layout del gruppo RAID, inclusi i dischi di parità o dati e gli slot non utilizzati.
   - **Dischi di riserva**: Indica il nome del nodo, il numero e la dimensione dei dischi di riserva e il tipo di storage.
4. Eseguire una delle seguenti operazioni:

| Se si desidera… | Quindi eseguire questa operazione… |
|---|---|
| Accettare i consigli di System Manager. | Passare a. La procedura per la configurazione di Onboard Key Manager per la crittografia. |
| Configurare manualmente i Tier locali e ***NOT*** utilizzare i consigli di System Manager. | Passare a. "Aggiungere manualmente un Tier locale (creare aggregato)":<br>• Per ONTAP 9.10.1 e versioni precedenti, seguire la procedura per utilizzare la CLI.<br>• A partire da ONTAP 9.11.1, seguire la procedura per utilizzare Gestione sistema. |

5. (opzionale): Se è stato installato Onboard Key Manager, è possibile configurarlo per la crittografia. Selezionare la casella di controllo **Configura Onboard Key Manager per la crittografia**.
   a. Inserire una passphrase.
   b. Immettere nuovamente la passphrase per confermarla.
   c. Salvare la passphrase per utilizzarla in futuro in caso di ripristino del sistema.
   d. Eseguire il backup del database delle chiavi per un utilizzo futuro.
6. Fare clic su **Save** (Salva) per creare il Tier locale e aggiungerlo alla soluzione di storage.

**CLI**

Viene eseguito il `storage aggregate auto-provision` comando per generare consigli di layout aggregati. È quindi possibile creare aggregati dopo aver esaminato e approvato i consigli di ONTAP.

**Di cosa hai bisogno**

ONTAP 9.2 o versione successiva deve essere in esecuzione sul cluster.

**A proposito di questa attività**

Il riepilogo predefinito generato con `storage aggregate auto-provision` il comando elenca gli aggregati consigliati da creare, inclusi i nomi e le dimensioni utilizzabili. È possibile visualizzare l'elenco e determinare se si desidera creare gli aggregati consigliati quando richiesto.

È inoltre possibile visualizzare un riepilogo dettagliato utilizzando `-verbose` che visualizza i seguenti report:

- Riepilogo per nodo dei nuovi aggregati da creare, delle riserve rilevate e dei dischi e delle partizioni di riserva rimanenti dopo la creazione dell'aggregato
- Nuovi aggregati di dati da creare con il numero di dischi e partizioni da utilizzare
- Layout del gruppo RAID che mostra come verranno utilizzati i dischi e le partizioni spare nei nuovi aggregati di dati da creare
- Dettagli sui dischi e le partizioni spare rimanenti dopo la creazione dell'aggregato

Se si conosce il metodo di provisioning automatico e l'ambiente è stato preparato correttamente, è possibile utilizzare `-skip-confirmation` opzione per creare l'aggregato consigliato senza visualizzazione e conferma. Il `storage aggregate auto-provision` La sessione CLI non influisce sul comando `-confirmations` impostazione.

Il[`storage aggregate auto-provision` man page^] contiene ulteriori informazioni sui suggerimenti per il layout aggregato.

**Fasi**

1. Eseguire `storage aggregate auto-provision` con le opzioni di visualizzazione desiderate.
   - Nessuna opzione: Visualizza il riepilogo standard
   - `-verbose` Opzione: Visualizza un riepilogo dettagliato
   - `-skip-confirmation` Opzione: Creazione di aggregati consigliati senza visualizzazione o conferma
2. Eseguire una delle seguenti operazioni:

| Se si desidera… | Quindi eseguire questa operazione… |
|---|---|

| | |
|---|---|
| Accetta le raccomandazioni di ONTAP. | Esaminare la visualizzazione degli aggregati consigliati, quindi rispondere alla richiesta di creare gli aggregati consigliati.<br><br>`myA400-44556677::> storage aggregate auto-provision`<br>`Node  New Data Aggregate  Usable Size`<br>`------------------  ----------------------------  ------------`<br>`myA400-364  myA400_364_SSD_1  3.29TB`<br>`myA400-363  myA400_363_SSD_1  1.46TB`<br>`------------------  ----------------------------  ------------`<br>`Total:  2  new data aggregates  4.75TB`<br><br>`Do you want to create recommended aggregates? {y` |
| n}: y<br><br>Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress.<br><br>myA400-44556677::><br><br>---- | Configurare manualmente i Tier locali e ***NOT*** utilizzare i consigli di ONTAP. |

**Informazioni correlate**

"Comandi di ONTAP 9"

#### Aggiungere manualmente i Tier locali (creare aggregati)

Se non si desidera aggiungere un Tier locale (creare un aggregato) utilizzando le Best practice di ONTAP, è possibile eseguire il processo manualmente.

**Prima di iniziare**

I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato). Se il cluster non è configurato per l'utilizzo dell'assegnazione automatica della proprietà del disco, è necessario "assegnare la proprietà manualmente".

**System Manager**

A partire da ONTAP 9.11.1, se non si desidera utilizzare la configurazione consigliata da Gestore di sistema per creare un Tier locale, è possibile specificare la configurazione desiderata.

**Fasi**

1. In System Manager, fare clic su **Storage > Tier**.
2. Nella pagina **Tier**, fare clic su + Add Local Tier per creare un nuovo tier locale:

   La pagina **Add Local Tier** mostra il numero consigliato di Tier locali che possono essere creati sui nodi e lo storage utilizzabile disponibile.

3. Quando System Manager visualizza le raccomandazioni relative allo storage per il Tier locale, fare clic su **Switch to Manual Local Tier Creation** (passa alla creazione manuale del Tier locale) nella sezione **Spare Disks**.

   La pagina **Add Local Tier** (Aggiungi livello locale) visualizza i campi utilizzati per configurare il livello locale.

4. Nella prima sezione della pagina **Add Local Tier** (Aggiungi livello locale), completare quanto segue:
   a. Immettere il nome del Tier locale.
   b. (Facoltativo): Selezionare la casella di controllo **Mirror this local Tier** (Esegui mirroring del livello locale) se si desidera eseguire il mirroring del livello locale.
   c. Selezionare un tipo di disco.
   d. Selezionare il numero di dischi.
5. Nella sezione **Configurazione RAID**, completare quanto segue:
   a. Selezionare il tipo di RAID.
   b. Selezionare la dimensione del gruppo RAID.
   c. Fare clic su RAID allocation (allocazione RAID) per visualizzare la modalità di allocazione dei dischi nel gruppo.
6. (Facoltativo): Se Onboard Key Manager è stato installato, è possibile configurarlo per la crittografia nella sezione **Encryption** della pagina. Selezionare la casella di controllo **Configura Onboard Key Manager per la crittografia**.
   a. Inserire una passphrase.
   b. Immettere nuovamente la passphrase per confermarla.
   c. Salvare la passphrase per utilizzarla in futuro in caso di ripristino del sistema.
   d. Eseguire il backup del database delle chiavi per un utilizzo futuro.
7. Fare clic su **Save** (Salva) per creare il Tier locale e aggiungerlo alla soluzione di storage.

**CLI**

Prima di creare gli aggregati manualmente, è necessario rivedere le opzioni di configurazione del disco e simulare la creazione.

A questo punto, è possibile eseguire il `storage aggregate create` controllare e verificare i risultati.

**Di cosa hai bisogno**

È necessario determinare il numero di dischi e il numero di dischi hot spare necessari nell'aggregato.

**A proposito di questa attività**

Se la partizione root-data-data è attivata e si dispone di 24 unità a stato solido (SSD) o meno nella configurazione, si consiglia di assegnare le partizioni dei dati a nodi diversi.

La procedura per la creazione di aggregati su sistemi con partizione dei dati root e partizione dei dati root abilitata è la stessa della procedura per la creazione di aggregati su sistemi che utilizzano dischi non partizionati. Se la partizione dei dati root è abilitata sul sistema, utilizzare il numero di partizioni del disco per `-diskcount` opzione. Per la partizione root-data-data, il `-diskcount` l'opzione specifica il numero di dischi da utilizzare.

> Quando si creano più aggregati per l'utilizzo con FlexGroups, gli aggregati devono avere dimensioni il più possibile vicine.

Il `storage aggregate create` la pagina man contiene ulteriori informazioni sulle opzioni e sui requisiti di creazione degli aggregati.

**Fasi**

1. Visualizzare l'elenco delle partizioni dei dischi di riserva per verificare di disporre di una quantità sufficiente per creare l'aggregato:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Le partizioni dei dati sono visualizzate in `Local Data Usable`. Non è possibile utilizzare una partizione root come spare.

2. Simulare la creazione dell'aggregato:

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. Se dal comando simulato vengono visualizzate delle avvertenze, regolare il comando e ripetere la simulazione.
4. Creare l'aggregato:

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. Visualizzare l'aggregato per verificare che sia stato creato:

   ```
   storage aggregate show-status aggregate_name
   ```

**Informazioni correlate**

"Comandi di ONTAP 9"

## Gestire l'utilizzo di Tier locali (aggregati)

### Gestire l'utilizzo di Tier locali (aggregati)

Dopo aver creato i Tier locali (aggregati), è possibile gestire il modo in cui vengono utilizzati.

È possibile eseguire le seguenti operazioni:

- "Rinominare un Tier locale (aggregato)"
- "Impostare il costo dei supporti di un Tier locale (aggregato)"
- "Determinare le informazioni su unità e gruppi RAID per un Tier locale (aggregato)"
- "Assegnazione di Tier locali (aggregati) alle macchine virtuali storage (SVM)"
- "Determinare quali volumi risiedono su un Tier locale (aggregato)"
- "Determinare e controllare l'utilizzo dello spazio di un volume in un Tier locale (aggregato)"
- "Determinare l'utilizzo dello spazio in un Tier locale (aggregato)"
- "Spostare la proprietà del Tier locale (aggregato) all'interno di una coppia ha"
- "Eliminazione di un Tier locale (aggregato)"

#### Rinominare un Tier locale (aggregato)

## È possibile rinominare un Tier locale (aggregato). Il metodo che si segue dipende dall'interfaccia in uso - System Manager o CLI:

**System Manager**

**Utilizzare System Manager per rinominare un Tier locale (aggregato)**

A partire da ONTAP 9.10.1, è possibile modificare il nome di un Tier locale (aggregato).

**Fasi**

1. In System Manager, fare clic su **Storage > Tier**.
2. Fare clic su ⋮ accanto al nome del tier locale.
3. Selezionare **Rinomina**.
4. Specificare un nuovo nome per il Tier locale.

**CLI**

**Utilizzare la CLI per rinominare un Tier locale (aggregato)**

**Fase**

1. Utilizzando la CLI, rinominare il Tier locale (aggregato):

   ```
   storage aggregate rename -aggregate aggr-name -newname aggr-new-name
   ```

   Nell'esempio riportato di seguito un aggregato denominato "aggr5" viene rinomicato come "sales-aggr":

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

#### Impostare il costo dei supporti di un Tier locale (aggregato)

## A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per impostare il costo

dei supporti di un Tier locale (aggregato).

**Fasi**

1. In System Manager, fare clic su **Storage > Tier**, quindi fare clic su **Set Media Cost** (Imposta costo supporti) nelle sezioni Local Tier (aggregato) desiderate.
2. Selezionare **Tier attivi e inattivi** per attivare il confronto.
3. Inserire un tipo di valuta e un importo.

Quando si inserisce o si modifica il costo del supporto, la modifica viene apportata a tutti i tipi di supporto.

#### Azzeramento rapido manuale dei dischi

Sui sistemi appena installati con ONTAP 9.4 o versione successiva e sui sistemi reinizializzati con ONTAP 9.4 o versione successiva, viene utilizzato il *azzeramento rapido* per azzerare i dischi.

Con il *azzeramento rapido*, i dischi vengono azzerati in pochi secondi. Questa operazione viene eseguita automaticamente prima del provisioning e riduce notevolmente il tempo necessario per inizializzare il sistema, creare aggregati o espandere aggregati quando vengono aggiunti dischi di riserva.

*Azzeramento rapido* è supportato su SSD e HDD.

> *Azzeramento rapido* non è supportato sui sistemi aggiornati da ONTAP 9.3 o versioni precedenti. ONTAP 9.4 o versione successiva deve essere installato di recente o il sistema deve essere reinizializzato. In ONTAP 9.3 e versioni precedenti, anche i dischi vengono azzerati automaticamente da ONTAP, tuttavia il processo richiede più tempo.

Se è necessario azzerare manualmente un disco, è possibile utilizzare uno dei seguenti metodi. In ONTAP 9.4 e versioni successive, l'azzeramento manuale di un disco richiede solo pochi secondi.

**Comando CLI**

**Utilizzare un comando CLI per azzerare rapidamente i dischi**

**A proposito di questa attività**

Per utilizzare questo comando sono necessari privilegi di amministratore.

**Fasi**

1. Immettere il comando CLI:

```
storage disk zerospares
```

**Opzioni del menu di boot**

**Selezionare le opzioni dal menu di boot per azzerare i dischi fast-zero**

**A proposito di questa attività**

- La funzione di azzeramento rapido non supporta i sistemi aggiornati da una release precedente a ONTAP 9.4.
- Se un nodo del cluster contiene un Tier locale (aggregato) con dischi con azzeramento rapido, non è possibile ripristinare il cluster a ONTAP 9.2 o versione precedente.

**Fasi**

1. Dal menu di avvio, selezionare una delle seguenti opzioni:
    - (4) pulizia della configurazione e inizializzazione di tutti i dischi
    - (9a) dispartizione di tutti i dischi e rimozione delle informazioni di proprietà
    - (9b) pulizia della configurazione e inizializzazione del nodo con interi dischi

#### Assegnare manualmente la proprietà del disco

## I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).

**A proposito di questa attività**

- Se stai assegnando manualmente la proprietà a una coppia ha che non viene inizializzata e che non ha solo DS460C shelf, utilizza l'opzione 1.
- Se stai inizializzando una coppia ha con solo DS460C shelf, puoi utilizzare l'opzione 2 per assegnare manualmente la proprietà dei dischi root.

**Opzione 1: Maggior parte delle coppie ha**

Per una coppia ha non inizializzata e che non dispone solo di DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà.

**A proposito di questa attività**

- I dischi per i quali si assegna la proprietà devono trovarsi in uno shelf collegato fisicamente al nodo a cui si assegna la proprietà.
- Se si utilizzano dischi in un Tier locale (aggregato):
  - I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).
  - Non è possibile riassegnare la proprietà di un disco in uso in un Tier locale (aggregato).

**Fasi**

1. Utilizzare la CLI per visualizzare tutti i dischi non posseduti:

   ```
   storage disk show -container-type unassigned
   ```

2. Assegnare ciascun disco:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta. Se si sta riassegnando un disco spare già di proprietà di un nodo diverso, è necessario utilizzare l'opzione "-force".

**Opzione 2: Coppia ha con solo DS460C shelf**

Per una coppia ha in fase di inizializzazione e dotata di soli DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà dei dischi root.

**A proposito di questa attività**

- Quando esegui l'inizializzazione di una coppia ha con soli DS460C shelf, devi assegnare manualmente i dischi root in modo che siano conformi alla policy a mezzo cassetto.

  Dopo l'inizializzazione (boot up) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi root) e a tutti i dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, in risposta a un messaggio di "low spare", o aggiungere capacità.

  Scoprite la politica di metà cassetto nell'argomento "Informazioni sull'assegnazione automatica della proprietà del disco".

- RAID richiede un minimo di 10 dischi per ciascuna coppia ha (5 per ogni nodo) per ogni più grande di 8TB dischi NL-SAS in uno shelf DS460C.

**Fasi**

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

   a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

      L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

   b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

      Riempire le file dei cassetti dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

      L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.


2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Assegnare manualmente le unità principali in ciascun cassetto in modo che siano conformi al criterio del mezzo cassetto, attenendosi alla seguente procedura:

   Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

   a. Visualizza tutti i dischi non posseduti:
      `storage disk show -container-type unassigned`
   b. Assegnare i dischi principali:
      `storage disk assign -disk disk_name -owner owner_name`

      È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta.

#### Determinare le informazioni su unità e gruppi RAID per un Tier locale (aggregato)

Alcune attività di amministrazione del Tier locale (aggregato) richiedono di conoscere i tipi di dischi che compongono il Tier locale, le loro dimensioni, checksum e stato, se sono condivisi con altri Tier locali e le dimensioni e la composizione dei gruppi RAID.

**Fase**

1. Mostra i dischi per l'aggregato, in base al gruppo RAID:

   `storage aggregate show-status` *`aggr_name`*

   I dischi vengono visualizzati per ciascun gruppo RAID nell'aggregato.

   È possibile visualizzare il tipo RAID del disco (dati, parità, dparity) in `Position` colonna. Se il `Position` viene visualizzata la colonna `shared`, Quindi l'unità viene condivisa: Se si tratta di un disco HDD, si tratta di un disco partizionato; se si tratta di un disco SSD, fa parte di un pool di storage.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

#### Assegnazione di Tier locali (aggregati) alle macchine virtuali storage (SVM)

Se si assegnano uno o più Tier locali (aggregati) a una macchina virtuale di storage (VM di storage o SVM, precedentemente nota come Vserver), è possibile utilizzare solo questi Tier locali per contenere i volumi per la VM di storage (SVM).

**Di cosa hai bisogno**

La VM di storage e i Tier locali che si desidera assegnare a quella VM di storage devono già esistere.

**A proposito di questa attività**

L'assegnazione di Tier locali alle VM di storage consente di mantenere le VM di storage isolate l'una dall'altra; ciò è particolarmente importante in un ambiente multi-tenancy.

**Fasi**

1. Controllare l'elenco dei Tier locali (aggregati) già assegnati alla SVM:

   ```
   vserver show -fields aggr-list
   ```

   Vengono visualizzati gli aggregati attualmente assegnati alla SVM. Se non sono assegnati aggregati, viene

visualizzato “-”.

2. Aggiungere o rimuovere gli aggregati assegnati, a seconda dei requisiti:

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Assegnare aggregati aggiuntivi | `vserver add-aggregates` |
| Annullare l’assegnazione degli aggregati | `vserver remove-aggregates` |

Gli aggregati elencati vengono assegnati o rimossi dalla SVM. Se la SVM dispone già di volumi che utilizzano un aggregato non assegnato alla SVM, viene visualizzato un messaggio di avviso, ma il comando viene completato correttamente. Tutti gli aggregati già assegnati alla SVM e non denominati nel comando non sono interessati.

**Esempio**

Nell’esempio seguente, gli aggregati aggr1 e aggr2 sono assegnati a SVM svm1:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

#### Determinare quali volumi risiedono su un Tier locale (aggregato)

Potrebbe essere necessario determinare quali volumi risiedono su un Tier locale (aggregato) prima di eseguire operazioni sul Tier locale, ad esempio spostandolo o portandolo offline.

**Fasi**

1. Per visualizzare i volumi che risiedono su un aggregato, immettere

   ```
   volume show -aggregate aggregate_name
   ```

   Vengono visualizzati tutti i volumi che risiedono nell’aggregato specificato.

#### Determinare e controllare l’utilizzo dello spazio di un volume in un Tier locale (aggregato)

È possibile determinare quali volumi FlexVol utilizzano la maggior parte dello spazio in un Tier locale (aggregato) e in particolare quali funzionalità all’interno del volume.

Il `volume show-footprint` il comando fornisce informazioni sull’impatto di un volume o sull’utilizzo dello spazio all’interno dell’aggregato contenente.

Il `volume show-footprint` il comando mostra i dettagli sull’utilizzo dello spazio di ciascun volume in un aggregato, inclusi i volumi offline. Questo comando colma la distanza tra l’output di `volume show-space` e. `aggregate show-space` comandi. Tutte le percentuali sono calcolate come percentuale della dimensione dell’aggregato.

Nell’esempio riportato di seguito viene illustrato il `volume show-footprint` output di comando per un volume chiamato testvol:

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                   Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                   120.6MB       4%
      Volume Guarantee                         1.88GB      71%
      Flexible Volume Metadata                11.38MB       0%
      Delayed Frees                            1.36MB       0%
      Total Footprint                          2.01GB      76%
```

La seguente tabella illustra alcune delle righe principali dell'output di `volume show-footprint` e cosa si può fare per cercare di ridurre l'utilizzo dello spazio in base a tale funzione:

| Nome riga/funzione | Descrizione/contenuto della riga | Alcuni modi per diminuire |
|---|---|---|
| `Volume Data Footprint` | La quantità totale di spazio utilizzata nell'aggregato contenente dai dati di un volume nel file system attivo e lo spazio utilizzato dalle copie Snapshot del volume. Questa riga non include lo spazio riservato. | • Eliminazione dei dati dal volume.<br>• Eliminazione delle copie Snapshot dal volume. |
| `Volume Guarantee` | La quantità di spazio riservato dal volume nell'aggregato per le scritture future. La quantità di spazio riservato dipende dal tipo di garanzia del volume. | Modifica del tipo di garanzia per il volume in `none`. |
| `Flexible Volume Metadata` | La quantità totale di spazio utilizzata nell'aggregato dai file di metadati del volume. | Nessun metodo diretto di controllo. |
| `Delayed Frees` | Blocchi utilizzati da ONTAP per le performance e che non possono essere immediatamente liberati. Per le destinazioni SnapMirror, questa riga ha un valore di `0` e non vengono visualizzati. | Nessun metodo diretto di controllo. |
| `File Operation Metadata` | La quantità totale di spazio riservato ai metadati delle operazioni del file. | Nessun metodo diretto di controllo. |

| | | |
|---|---|---|
| `Total Footprint` | La quantità totale di spazio utilizzata dal volume nell'aggregato. È la somma di tutte le righe. | Uno dei metodi utilizzati per ridurre lo spazio utilizzato da un volume. |

**Informazioni correlate**

"Report tecnico di NetApp 3483: Thin provisioning in un ambiente NetApp SAN o IP SAN Enterprise"

#### Determinare l'utilizzo dello spazio in un Tier locale (aggregato)

## È possibile visualizzare la quantità di spazio utilizzata da tutti i volumi in uno o più Tier locali (aggregati) in modo da poter intraprendere azioni per liberare più spazio.

WAFL riserva il 10% dello spazio totale su disco per le performance e i metadati a livello aggregato. Lo spazio utilizzato per mantenere i volumi nell'aggregato esce dalla WAFL Reserve e non può essere modificato.

> A partire da ONTAP 9.12.1 e versioni successive, la riserva WAFL per gli aggregati superiori a 30TB si riduce dal 10% al 5% per le piattaforme AFF e FAS500f. A partire dal sistema ONTAP 9.14.1, questa stessa riduzione si applica agli aggregati su tutte le piattaforme FAS, producendo il 5% di spazio utilizzabile in più negli aggregati.

È possibile visualizzare l'utilizzo dello spazio da parte di tutti i volumi in uno o più aggregati con `aggregate show-space` comando. In questo modo, è possibile individuare i volumi che consumano più spazio nei relativi aggregati di contenimento, in modo da poter intraprendere azioni per liberare più spazio.

Lo spazio utilizzato in un aggregato è direttamente influenzato dallo spazio utilizzato nei volumi FlexVol in esso contenuti. Le misure adottate per aumentare lo spazio in un volume influiscono anche sullo spazio nell'aggregato.

Le seguenti righe sono incluse in `aggregate show-space` output del comando:

- **Volume Footprint**

  Il totale di tutte le impronte di volume all'interno dell'aggregato. Include tutto lo spazio utilizzato o riservato da tutti i dati e i metadati di tutti i volumi nell'aggregato contenente.

- **Metadati aggregati**

  I metadati totali del file system richiesti dall'aggregato, come ad esempio bitmap di allocazione e file inode.

- **Snapshot Reserve**

  La quantità di spazio riservato per le copie Snapshot aggregate, in base alle dimensioni del volume. Viene considerato spazio utilizzato e non è disponibile per il volume o l'aggregazione di dati o metadati.

- **Snapshot Reserve inutilizzabile**

  La quantità di spazio allocato originariamente per la riserva Snapshot aggregata che non è disponibile per le copie Snapshot aggregate perché viene utilizzata dai volumi associati all'aggregato. Può verificarsi solo per gli aggregati con una riserva Snapshot aggregata diversa da zero.

- **Totale utilizzato**

La somma di tutto lo spazio utilizzato o riservato nell'aggregato in base a volumi, metadati o copie Snapshot.

- **Totale fisico utilizzato**

  La quantità di spazio utilizzata per i dati ora (anziché essere riservata per uso futuro). Include lo spazio utilizzato dalle copie Snapshot aggregate.

Nell'esempio riportato di seguito viene illustrato il `aggregate show-space` Output di comando per un aggregato la cui riserva Snapshot è del 5%. Se la riserva Snapshot era 0, la riga non veniva visualizzata.

```
cluster1::> storage aggregate show-space

                        Aggregate : wqa_gx106_aggr1

      Feature                                   Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                       101.0MB         0%
      Aggregate Metadata                        300KB         0%
      Snapshot Reserve                         5.98GB         5%

      Total Used                               6.07GB         5%
      Total Physical Used                     34.82KB         0%
```

**Informazioni correlate**

- "Articolo della Knowledge base: Utilizzo dello spazio"
- "Liberate fino al 5% della vostra capacità di storage eseguendo l'upgrade a ONTAP 9.12.1"

#### Trasferire la proprietà di un Tier locale (aggregato) all'interno di una coppia ha

## È possibile modificare la proprietà dei Tier locali (aggregati) tra i nodi di una coppia ha senza interrompere il servizio dai Tier locali.

Entrambi i nodi di una coppia ha sono fisicamente collegati tra loro a dischi o LUN di array. Ogni LUN di dischi o array è di proprietà di uno dei nodi.

La proprietà di tutti i dischi o le LUN degli array all'interno di un Tier locale (aggregato) cambia temporaneamente da un nodo all'altro quando si verifica un Takeover. Tuttavia, le operazioni di trasferimento dei Tier locali possono anche modificare in modo permanente la proprietà (ad esempio, se eseguite per il bilanciamento del carico). La proprietà cambia senza alcun processo di copia dei dati o spostamento fisico dei dischi o delle LUN degli array.

**A proposito di questa attività**

- Poiché i limiti del numero di volumi vengono validati a livello di programmazione durante le operazioni di trasferimento dei livelli locali, non è necessario controllarli manualmente.

  Se il numero di volumi supera il limite supportato, l'operazione di trasferimento del Tier locale non riesce e viene visualizzato un messaggio di errore pertinente.

- Non è consigliabile avviare il trasferimento locale del Tier quando sono in corso operazioni a livello di sistema sul nodo di origine o di destinazione; allo stesso modo, non è necessario avviare queste operazioni durante il trasferimento locale del Tier.

  Queste operazioni possono includere quanto segue:

  - Takeover
  - Giveback
  - Spegnere
  - Un'altra operazione di trasferimento locale del Tier
  - Modifica della proprietà del disco
  - Operazioni di configurazione locale di livelli o volumi
  - Sostituzione del controller storage
  - Aggiornamento di ONTAP
  - Indirizzamento ONTAP
- Se si dispone di una configurazione MetroCluster, non è necessario avviare il trasferimento locale del Tier durante le operazioni di disaster recovery (*switchover*, *healing* o *switchback*).
- Se si dispone di una configurazione MetroCluster e si avvia il trasferimento locale del Tier su un Tier locale switchover, l'operazione potrebbe non riuscire perché supera il numero di limiti di volume del partner DR.
- Non è consigliabile avviare il trasferimento locale del Tier su aggregati corrotti o in fase di manutenzione.
- Prima di iniziare il trasferimento locale del Tier, salvare i core dump sui nodi di origine e di destinazione.

**Fasi**

1. Visualizzare gli aggregati sul nodo per confermare quali aggregati spostare e assicurarsi che siano online e in buone condizioni:

   `storage aggregate show -node` *`source-node`*

   Il comando seguente mostra sei aggregati sui quattro nodi del cluster. Tutti gli aggregati sono online. Node1 e node3 formano una coppia ha e Node2 e node4 formano una coppia ha.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. Emettere il comando per avviare il trasferimento dell'aggregato:

   `storage aggregate relocation start -aggregate-list` *`aggregate-1`*`,` *`aggregate-2`*`…`
   `-node` *`source-node`* `-destination` *`destination-node`*

   Il seguente comando sposta gli aggregati aggr_1 e aggr_2 da Node1 a node3. Node3 è il partner ha di Node1. Gli aggregati possono essere spostati solo all'interno della coppia ha.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Monitorare l'avanzamento del trasferimento degli aggregati con `storage aggregate relocation show` comando:

   `storage aggregate relocation show -node` *`source-node`*

   Il seguente comando mostra l'avanzamento degli aggregati che vengono spostati al nodo 3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Al termine del trasferimento, l'output di questo comando mostra ogni aggregato con uno stato di trasferimento di "Done".

#### Eliminazione di un Tier locale (aggregato)

## È possibile eliminare un Tier locale (aggregato) se non sono presenti volumi nel Tier locale.

Il `storage aggregate delete` il comando elimina un aggregato di storage. Il comando non riesce se sono presenti volumi nell'aggregato. Se all'aggregato è associato un archivio di oggetti, oltre all'eliminazione dell'aggregato, il comando elimina anche gli oggetti nell'archivio di oggetti. Non vengono apportate modifiche alla configurazione dell'archivio di oggetti come parte di questo comando.

Nell'esempio seguente viene eliminato un aggregato denominato "aggr1":

```
> storage aggregate delete -aggregate aggr1
```

#### Comandi per il trasferimento degli aggregati

## Esistono comandi ONTAP specifici per spostare la proprietà dell'aggregato all'interno di una coppia ha.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Avviare il processo di trasferimento degli aggregati | `storage aggregate relocation start` |
| Monitorare il processo di trasferimento degli aggregati | `storage aggregate relocation show` |

**Informazioni correlate**

"Comandi di ONTAP 9"

#### Comandi per la gestione degli aggregati

## Si utilizza `storage aggregate` comando per gestire gli aggregati.

| Se si desidera… | Utilizzare questo comando… |
| --- | --- |
| Visualizza le dimensioni della cache per tutti gli aggregati di Flash Pool | `storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0` |
| Visualizza le informazioni e lo stato del disco per un aggregato | `storage aggregate show-status` |
| Visualizza dischi spare per nodo | `storage aggregate show-spare-disks` |
| Visualizzare gli aggregati root nel cluster | `storage aggregate show -has-mroot true` |
| Visualizza le informazioni di base e lo stato degli aggregati | `storage aggregate show` |
| Visualizza il tipo di storage utilizzato in un aggregato | `storage aggregate show -fields storage-type` |
| Porta online un aggregato | `storage aggregate online` |
| Eliminare un aggregato | `storage aggregate delete` |
| Mettere un aggregato nello stato limitato | `storage aggregate restrict` |
| Rinominare un aggregato | `storage aggregate rename` |
| Portare un aggregato offline | `storage aggregate offline` |
| Modificare il tipo di RAID per un aggregato | `storage aggregate modify -raidtype` |

**Informazioni correlate**

"Comandi di ONTAP 9"

## Aggiunta di capacità (dischi) a un Tier locale (aggregato)

### Aggiunta di capacità (dischi) a un Tier locale (aggregato)

Utilizzando metodi diversi, si segue un workflow specifico per aggiungere capacità.

- "Workflow per aggiungere capacità a un Tier locale (aggregato)"
- "Metodi per creare spazio in un Tier locale (aggregato)"

È possibile aggiungere dischi a un Tier locale e dischi a un nodo o a uno shelf.

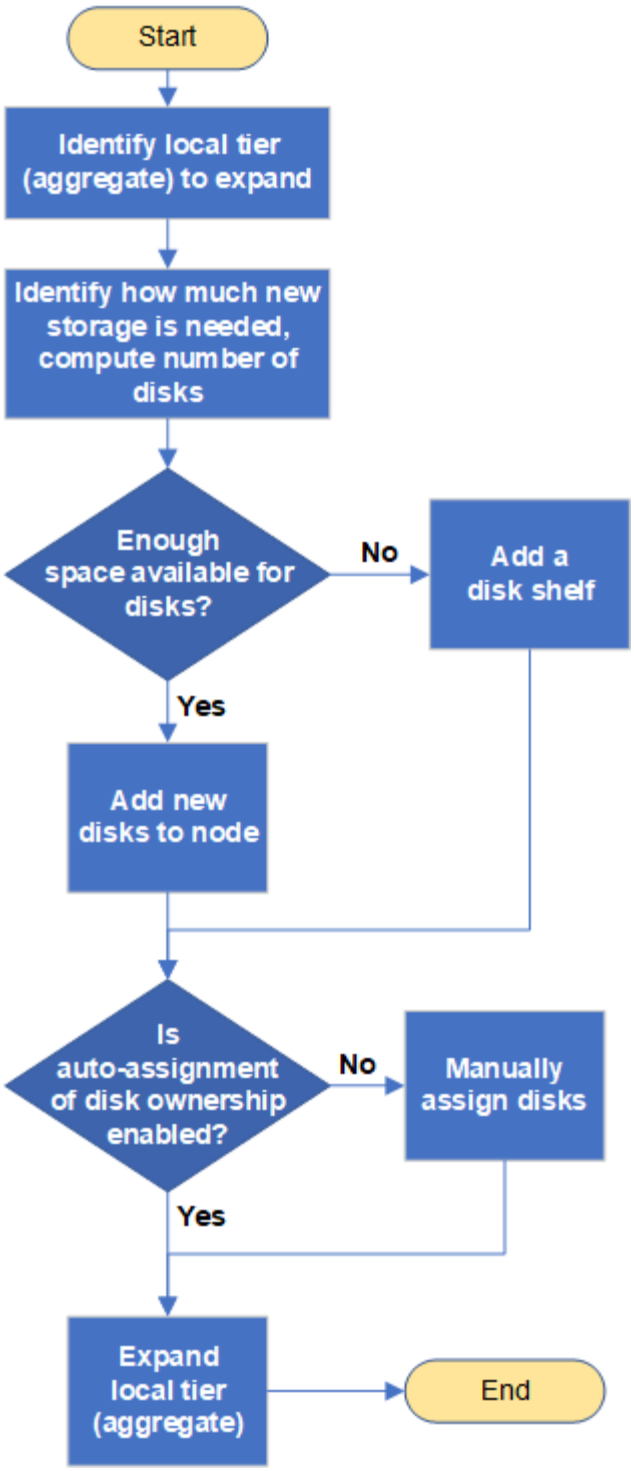
Se necessario, è possibile correggere le partizioni spare disallineate.

- "Aggiunta di dischi a un Tier locale (aggregato)"
- "Aggiungere dischi a un nodo o a uno shelf"
- "Correggere le partizioni spare disallineate"

#### Workflow per aggiungere capacità a un Tier locale (espansione di un aggregato)

Per aggiungere capacità a un Tier locale (espandere un aggregato), è necessario prima identificare il Tier locale a cui si desidera aggiungere, determinare la quantità di nuovo storage necessaria, installare nuovi dischi, assegnare la proprietà del disco e creare un nuovo gruppo RAID, se necessario.

È possibile utilizzare System Manager o CLI per aggiungere capacità.




**Metodi per creare spazio in un Tier locale (aggregato)**

Se un Tier locale (aggregato) esaurisce lo spazio libero, possono verificarsi diversi problemi, dalla perdita di dati alla disattivazione della garanzia di un volume. Esistono diversi modi per creare più spazio in un Tier locale.

Tutti i metodi hanno diverse conseguenze. Prima di intraprendere qualsiasi azione, leggere la relativa sezione della documentazione.

Di seguito sono riportati alcuni metodi comuni per creare spazio nel Tier locale, in ordine da minimo a maggior

parte delle conseguenze:

- Aggiungere dischi al Tier locale.
- Spostare alcuni volumi in un altro Tier locale con spazio disponibile.
- Ridurre le dimensioni dei volumi garantiti dal volume nel Tier locale.
- Eliminare le copie Snapshot del volume non necessarie se il tipo di garanzia del volume è “none”.
- Eliminare i volumi non necessari.
- Abilitare funzionalità per il risparmio di spazio, come deduplica o compressione.
- (Temporaneamente) disattivare le funzionalità che utilizzano una grande quantità di metadati .

#### Aggiunta di capacità a un Tier locale (aggiunta di dischi a un aggregato)

È possibile aggiungere dischi a un Tier locale (aggregato) in modo che possa fornire più storage ai volumi associati.

**Gestore di sistema (ONTAP 9.8 e versioni successive)**

**Utilizzare Gestione di sistema per aggiungere capacità (ONTAP 9.8 e versioni successive)**

È possibile aggiungere capacità a un Tier locale aggiungendo dischi di capacità.

> A partire da ONTAP 9.12.1, è possibile utilizzare Gestore di sistema per visualizzare la capacità impegnata di un Tier locale e determinare se è necessaria una capacità aggiuntiva per il Tier locale. Vedere "Monitorare la capacità in System Manager".

**A proposito di questa attività**

Questa operazione viene eseguita solo se è stato installato ONTAP 9.8 o versione successiva. Se è stata installata una versione precedente di ONTAP, fare riferimento alla scheda (o alla sezione) denominata "Gestore di sistema (ONTAP 9.7 e versioni precedenti)".

**Fasi**

1. Fare clic su **Storage > Tier**.
2. Fare clic su ⋮ accanto al nome del tier locale al quale si desidera aggiungere capacità.
3. Fare clic su **Add Capacity** (Aggiungi capacità).

> Se non sono presenti dischi di riserva che è possibile aggiungere, l'opzione **Add Capacity** (Aggiungi capacità) non viene visualizzata e non è possibile aumentare la capacità del Tier locale.

4. Attenersi alla seguente procedura, in base alla versione di ONTAP installata:

| Se questa versione di ONTAP è installata… | Eseguire questa procedura… |
|---|---|
| ONTAP 9.8, 9.9 o 9.10.1 | a. Se il nodo contiene più livelli di storage, selezionare il numero di dischi che si desidera aggiungere al livello locale. In caso contrario, se il nodo contiene solo un singolo Tier di storage, la capacità aggiunta viene stimata automaticamente.<br>b. Fare clic su **Aggiungi**. |
| A partire da ONTAP 9.11.1 | a. Selezionare il tipo di disco e il numero di dischi.<br>b. Se si desidera aggiungere dischi a un nuovo gruppo RAID, selezionare la casella di controllo. Viene visualizzata l'allocazione RAID.<br>c. Fare clic su **Save** (Salva). |

5. (Facoltativo) il completamento del processo richiede un po' di tempo. Se si desidera eseguire il processo in background, selezionare **Esegui in background**.
6. Al termine del processo, è possibile visualizzare l'aumento della capacità nelle informazioni del Tier locale in **Storage > Tier**.

**Gestore di sistema (ONTAP 9.7 e versioni precedenti)**

**Utilizzare Gestione di sistema per aggiungere capacità (ONTAP 9.7 e versioni precedenti)**

È possibile aggiungere capacità a un Tier locale (aggregato) aggiungendo dischi di capacità.

**A proposito di questa attività**

Questa operazione viene eseguita solo se è stato installato ONTAP 9.7 o una versione precedente. Se è stato installato ONTAP 9.8 o versione successiva, consultare la sezione Utilizzo di Gestione sistema per aggiungere capacità (ONTAP 9.8 o versione successiva).

**Fasi**

1. (Solo per ONTAP 9.7) fare clic su **(Torna alla versione classica)**.
2. Fare clic su **hardware e diagnostica > aggregati**.
3. Selezionare l'aggregato a cui si desidera aggiungere dischi di capacità, quindi fare clic su **azioni > Aggiungi capacità**.

   È necessario aggiungere dischi delle stesse dimensioni degli altri dischi dell'aggregato.

4. (Solo per ONTAP 9.7) fare clic su **passa alla nuova esperienza**.
5. Fare clic su **Storage > Tier** per verificare le dimensioni del nuovo aggregato.

**CLI**

**Utilizzare la CLI per aggiungere capacità**

La procedura per l'aggiunta di dischi partizionati a un aggregato è simile alla procedura per l'aggiunta di dischi non partizionati.

**Di cosa hai bisogno**

È necessario conoscere le dimensioni del gruppo RAID per l'aggregato a cui si aggiunge lo storage.

**A proposito di questa attività**

Quando si espande un aggregato, è necessario sapere se si stanno aggiungendo partizioni o dischi non partizionati all'aggregato. Quando si aggiungono unità non partizionate a un aggregato esistente, la dimensione dei gruppi RAID esistenti viene ereditata dal nuovo gruppo RAID, che può influire sul numero di dischi di parità richiesti. Se un disco non partizionato viene aggiunto a un gruppo RAID composto da dischi partizionati, il nuovo disco viene partizionato, lasciando una partizione spare inutilizzata.

Quando si effettua il provisioning delle partizioni, è necessario assicurarsi di non lasciare il nodo senza un disco con entrambe le partizioni come spare. In caso contrario, e il nodo subisce un'interruzione del controller, è possibile che non siano disponibili informazioni preziose sul problema (il file principale) da fornire al supporto tecnico.

Non utilizzare `disklist` per espandere gli aggregati. Ciò potrebbe causare un disallineamento delle partizioni.

**Fasi**

1. Mostrare lo storage di riserva disponibile sul sistema proprietario dell'aggregato:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   È possibile utilizzare `-is-disk-shared` parametro che mostra solo dischi partizionati o solo dischi non partizionati.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                             Local
Local
                                                              Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size Status
 --------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. Mostra i gruppi RAID correnti per l’aggregato:

   `storage aggregate show-status` *`aggr_name`*

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                   Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. Simulare l'aggiunta dello storage all'aggregato:

   `storage aggregate add-disks -aggregate` *`aggr_name`* `-diskcount` *`number_of_disks_or_partitions`* `-simulate true`

   È possibile vedere il risultato dell'aggiunta dello storage senza eseguire il provisioning effettivo dello storage. Se dal comando simulato vengono visualizzate delle avvertenze, è possibile regolare il comando e ripetere la simulazione.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. Aggiungere lo storage all'aggregato:

   `storage aggregate add-disks -aggregate` *`aggr_name`* `-raidgroup new -diskcount` *`number_of_disks_or_partitions`*

   Quando si crea un aggregato Flash Pool, se si aggiungono dischi con un checksum diverso dall'aggregato o se si aggiungono dischi a un aggregato di checksum misto, è necessario utilizzare `-checksumstyle` parametro.

   Se si aggiungono dischi a un aggregato di Flash Pool, è necessario utilizzare `-disktype` parametro per specificare il tipo di disco.

   È possibile utilizzare `-disksize` parametro per specificare la dimensione dei dischi da aggiungere. Per l'aggiunta all'aggregato vengono selezionati solo i dischi con dimensioni approssimativamente specificate.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Verificare che lo storage sia stato aggiunto correttamente:

   `storage aggregate show-status -aggregate` *`aggr_name`*

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                        0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Verificare che il nodo disponga ancora di almeno un disco con la partizione root e la partizione dati come spare:

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size Status
 --------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                      BSAS    7200 block               0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

#### Aggiungere dischi a un nodo o a uno shelf

## È possibile aggiungere dischi a un nodo o a uno shelf per aumentare il numero di hot spare o aggiungere spazio al Tier locale (aggregato).

#### Prima di iniziare

L'unità che si desidera aggiungere deve essere supportata dalla piattaforma. È possibile confermare utilizzando "NetApp Hardware Universe".

Il numero minimo di dischi da aggiungere in una singola procedura è sei. L'aggiunta di un singolo disco potrebbe ridurre le prestazioni.

#### Procedura per l'NetApp Hardware Universe

1. Nel menu a discesa **prodotti**, selezionare la configurazione hardware
2. Selezionare la piattaforma.
3. Selezionare la versione di ONTAP che si sta eseguendo quindi **Mostra risultati**.
4. Sotto l'immagine, selezionare **fare clic qui per visualizzare le viste alternative**. Scegliere la visualizzazione corrispondente alla configurazione.

**Procedura per l'installazione delle unità**

1. Controllare "Sito di supporto NetApp" Per firmware di dischi e shelf più recenti e file di Disk Qualification Package.

   Se il nodo o lo shelf non dispone delle versioni più recenti, aggiornarle prima di installare il nuovo disco.

   Il firmware del disco viene aggiornato automaticamente (senza interruzioni) sui nuovi dischi che non dispongono delle versioni firmware correnti.

2. Mettere a terra l'utente.
3. Rimuovere delicatamente il pannello frontale dalla parte anteriore della piattaforma.
4. Identificare lo slot corretto per il nuovo disco.

   > Gli slot corretti per l'aggiunta di dischi variano a seconda del modello di piattaforma e della versione di ONTAP. In alcuni casi è necessario aggiungere unità a slot specifici in sequenza. Ad esempio, in un AFF A800 si aggiungono i dischi a intervalli specifici lasciando cluster di slot vuoti. Mentre in un AFF A220 si aggiungono nuove unità ai successivi slot vuoti che vanno dall'esterno verso il centro dello shelf.

   Fare riferimento alla procedura descritta in **prima di iniziare** per identificare gli slot corretti per la configurazione in uso in "NetApp Hardware Universe".

5. Inserire il nuovo disco:
   a. Con la maniglia della camma in posizione aperta, inserire il nuovo disco con entrambe le mani.
   b. Premere fino all'arresto del disco.
   c. Chiudere la maniglia della camma in modo che l'unità sia completamente inserita nel piano intermedio e la maniglia scatti in posizione. Chiudere lentamente la maniglia della camma in modo che sia allineata correttamente con la superficie dell'unità.
6. Verificare che il LED di attività del disco (verde) sia acceso.

   Quando il LED di attività del disco è acceso, significa che il disco è alimentato. Quando il LED di attività del disco lampeggia, significa che il disco è alimentato e che l'i/o è in corso. Se il firmware del disco viene aggiornato automaticamente, il LED lampeggia.

7. Per aggiungere un'altra unità, ripetere i passaggi da 4 a 6.

   I nuovi dischi non vengono riconosciuti fino a quando non vengono assegnati a un nodo. È possibile assegnare i nuovi dischi manualmente oppure attendere che ONTAP assegni automaticamente i nuovi dischi se il nodo segue le regole per l'assegnazione automatica dei dischi.

8. Una volta riconosciuti tutti i nuovi dischi, verificare che siano stati aggiunti e che la proprietà sia specificata correttamente.

**Procedura per confermare l'installazione**

1. Visualizzare l'elenco dei dischi:

   ```
   storage aggregate show-spare-disks
   ```

   Dovrebbero essere visualizzati i nuovi dischi, di proprietà del nodo corretto.

2. **Facoltativamente (solo per ONTAP 9,3 e versioni precedenti),** azzerare le unità appena aggiunte:

```
storage disk zerospares
```

I dischi utilizzati in precedenza in un Tier locale (aggregato) ONTAP devono essere azzerati prima di poter essere aggiunti a un altro aggregato. In ONTAP 9.3 e versioni precedenti, il completamento dell'azzeramento può richiedere ore, a seconda delle dimensioni dei dischi non azzerati nel nodo. L'azzeramento dei dischi consente di evitare ritardi nel caso in cui sia necessario aumentare rapidamente le dimensioni di un Tier locale. Questo non è un problema in ONTAP 9.4 o versioni successive, in cui i dischi vengono azzerati utilizzando *l'azzeramento rapido* che richiede solo secondi.

**Risultati**

I nuovi dischi sono pronti. È possibile aggiungerli a un Tier locale (aggregato), inserirli nell'elenco delle hot spare o aggiungerli quando si crea un nuovo Tier locale.

#### Correggere le partizioni spare disallineate

Quando si aggiungono dischi partizionati a un Tier locale (aggregato), è necessario lasciare un disco con sia la partizione root che quella di dati disponibili come spare per ogni nodo. In caso contrario, ONTAP non è in grado di eseguire il dump del core nella partizione dei dati di riserva.

**Prima di iniziare**

È necessario disporre di una partizione di dati spare e di una partizione root spare sullo stesso tipo di disco di proprietà dello stesso nodo.

**Fasi**

1. Usando la CLI, visualizzare le partizioni spare per il nodo:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Si noti quale disco ha una partizione di dati spare (spare_data) e quale disco ha una partizione root spare (spare_root). La partizione spare mostra un valore diverso da zero sotto `Local Data Usable` oppure `Local Root Usable` colonna.

2. Sostituire il disco con una partizione di dati spare con il disco con la partizione root spare:

   ```
   storage disk replace -disk spare_data -replacement spare_root -action start
   ```

   È possibile copiare i dati in entrambe le direzioni; tuttavia, il completamento della copia della partizione root richiede meno tempo.

3. Monitorare l'avanzamento della sostituzione del disco:

   ```
   storage aggregate show-status -aggregate aggr_name
   ```

4. Una volta completata l'operazione di sostituzione, visualizzare nuovamente le parti di ricambio per confermare che si dispone di un disco libero completo:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   In "Local Data usable" (dati locali utilizzabili) e nella sezione viene visualizzato un disco spare con spazio utilizzabile `Local Root Usable`.

**Esempio**

Visualizzare le partizioni spare per il nodo c1-01 e verificare che le partizioni spare non siano allineate:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

Viene avviato il processo di sostituzione del disco:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Durante l'attesa del completamento dell'operazione di sostituzione, viene visualizzato il seguente stato di avanzamento:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                     Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

Una volta completata l'operazione di sostituzione, verificare di disporre di un disco libero completo:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

## Gestire i dischi

### Panoramica sulla gestione dei dischi

È possibile eseguire varie procedure per gestire i dischi nel sistema.

- **Aspetti della gestione dei dischi**
  - "Quando è necessario aggiornare il Disk Qualification Package"
  - "Funzionamento dei dischi hot spare"
  - "Gli avvisi di riserva bassi possono aiutarti a gestire i dischi spare"
  - "Opzioni aggiuntive di gestione della partizione dei dati root"
- **Proprietà di dischi e partizioni**
  - "Proprietà di dischi e partizioni"
- **Rimozione del disco non riuscita**
  - "Rimuovere un disco guasto"
- **Pulizia del disco**
  - "Pulizia dei dischi"

### Funzionamento dei dischi hot spare

Un disco hot spare è un disco assegnato a un sistema di storage ed è pronto per l'uso, ma non è in uso da un gruppo RAID e non conserva alcun dato.

Se si verifica un guasto al disco all'interno di un gruppo RAID, il disco hot spare viene assegnato automaticamente al gruppo RAID per sostituire i dischi guasti. I dati del disco guasto vengono ricostruiti sul disco sostitutivo hot spare in background dal disco di parità RAID. L'attività di ricostruzione viene registrata in `/etc/message` Viene inviato un file e un messaggio AutoSupport.

Se il disco hot spare disponibile non ha le stesse dimensioni del disco guasto, viene scelto un disco di dimensioni maggiori successive e quindi ridimensionato in modo da corrispondere alle dimensioni del disco che si sta sostituendo.

#### Requisiti di riserva per i dischi portanti multi-disco

Mantenere il numero corretto di dischi di riserva nei carrier multi-disco è fondamentale per ottimizzare la ridondanza dello storage e ridurre al minimo il tempo che ONTAP deve dedicare alla copia dei dischi per ottenere un layout ottimale dei dischi.

È necessario mantenere un minimo di due hot spare per i dischi portanti multi-disco in ogni momento. Per supportare l'utilizzo del Centro di manutenzione ed evitare problemi causati da guasti a più dischi simultanei, è necessario mantenere almeno quattro hot spare per il funzionamento a stato stazionario e sostituire tempestivamente i dischi guasti.

Se due dischi si guastano contemporaneamente con solo due hot spare disponibili, ONTAP potrebbe non essere in grado di scambiare il contenuto del disco guasto e del relativo carrier mate con i dischi spare. Questo scenario è chiamato stallo. In questo caso, viene inviata una notifica tramite messaggi EMS e messaggi AutoSupport. Quando i supporti sostitutivi diventano disponibili, è necessario seguire le istruzioni fornite dai messaggi EMS. Per ulteriori informazioni, consultare l'articolo della Knowledge base "Impossibile eseguire la calibrazione automatica del layout RAID - messaggio AutoSupport"

### Gli avvisi di riserva bassi possono aiutarti a gestire i dischi spare

Per impostazione predefinita, gli avvisi vengono inviati alla console e ai registri se si dispone di meno di un disco hot spare che corrisponde agli attributi di ciascun disco nel sistema di storage.

È possibile modificare il valore di soglia per questi messaggi di avviso per garantire che il sistema rispetti le Best practice.

#### A proposito di questa attività

Impostare l'opzione RAID "min_spare_count" su "2" per assicurarsi di disporre sempre del numero minimo di dischi di riserva consigliato.

#### Fase

1. Impostare l'opzione su "2":

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

### Opzioni aggiuntive di gestione della partizione dei dati root

A partire da ONTAP 9.2, dal menu di avvio è disponibile una nuova opzione di partizione dei dati root, che offre funzionalità di gestione aggiuntive per i dischi configurati per la partizione dei dati root.

Le seguenti funzionalità di gestione sono disponibili nell'opzione del menu di avvio 9.

- **Dispartizione di tutti i dischi e rimozione delle informazioni di proprietà**

  Questa opzione è utile se il sistema è configurato per la partizione dei dati root ed è necessario reinizializzarlo con una configurazione diversa.

- **Pulizia della configurazione e inizializzazione del nodo con dischi partizionati**

  Questa opzione è utile per:

- Il sistema non è configurato per la partizione dei dati root e si desidera configurarlo per la partizione dei dati root
- Il sistema non è configurato correttamente per la partizione dei dati root ed è necessario correggerla
- Si dispone di una piattaforma AFF o FAS con solo SSD collegati e configurati per la versione precedente della partizione dei dati root e si desidera aggiornarla alla versione più recente della partizione dei dati root per aumentare l'efficienza dello storage

- **Pulizia della configurazione e inizializzazione del nodo con interi dischi**

  Questa opzione è utile per:

  - Dispartizione delle partizioni esistenti
  - Rimuovere la proprietà del disco locale
  - Reinizializzare il sistema con interi dischi utilizzando RAID-DP

#### Quando è necessario aggiornare il Disk Qualification Package

Il Disk Qualification Package (DQP) aggiunge il supporto completo per i dischi appena qualificati. Prima di aggiornare il firmware del disco o aggiungere nuovi tipi o dimensioni di disco a un cluster, è necessario aggiornare il DQP. Una Best practice consiste nell'aggiornare regolarmente il DQP, ad esempio ogni trimestre o semestrale.

È necessario scaricare e installare DQP nelle seguenti situazioni:

- Ogni volta che si aggiunge un nuovo tipo di disco o una nuova dimensione al nodo

  Ad esempio, se si dispone già di dischi da 1 TB e si aggiungono dischi da 2 TB, è necessario verificare la disponibilità dell'aggiornamento DQP più recente.

- Ogni volta che si aggiorna il firmware del disco
- Ogni volta che sono disponibili firmware del disco o file DQP più recenti
- Ogni volta che si esegue l'aggiornamento a una nuova versione di ONTAP.

  Il DQP non viene aggiornato come parte di un aggiornamento del ONTAP.

#### Informazioni correlate

"Download NetApp: Pacchetto di qualificazione dei dischi"

"Download NetApp: Firmware del disco"

### Proprietà di dischi e partizioni

#### Proprietà di dischi e partizioni

È possibile gestire la proprietà di dischi e partizioni.

È possibile eseguire le seguenti operazioni:

- **"Visualizzare la proprietà di dischi e partizioni"**

  È possibile visualizzare la proprietà del disco per determinare quale nodo controlla lo storage. È inoltre

possibile visualizzare la proprietà della partizione sui sistemi che utilizzano dischi condivisi.

- **"Modificare le impostazioni per l'assegnazione automatica della proprietà del disco"**

  È possibile selezionare un criterio non predefinito per assegnare automaticamente la proprietà del disco o disattivare l'assegnazione automatica della proprietà del disco.

- **"Assegnare manualmente la proprietà dei dischi non partizionati"**

  Se il cluster non è configurato per utilizzare l'assegnazione automatica della proprietà del disco, è necessario assegnare la proprietà manualmente.

- **"Assegnare manualmente la proprietà dei dischi partizionati"**

  È possibile impostare la proprietà del disco container o delle partizioni manualmente o utilizzando l'assegnazione automatica, proprio come avviene per i dischi non partizionati.

- **"Rimuovere un disco guasto"**

  Un disco che si è guastato completamente non è più considerato da ONTAP come un disco utilizzabile ed è possibile scollegare immediatamente il disco dallo shelf.

- **"Rimuovere la proprietà da un disco"**

  ONTAP scrive le informazioni sulla proprietà del disco sul disco. Prima di rimuovere un disco spare o il relativo shelf da un nodo, è necessario rimuovere le relative informazioni di proprietà in modo che possano essere correttamente integrate in un altro nodo.

#### Informazioni sull'assegnazione automatica della proprietà del disco

L'assegnazione automatica dei dischi non proprietari è attivata per impostazione predefinita. L'assegnazione automatica della proprietà del disco avviene 10 minuti dopo l'inizializzazione della coppia ha e ogni cinque minuti durante il normale funzionamento del sistema.

Quando Aggiungi un nuovo disco a una coppia ha, ad esempio quando si sostituisce un disco guasto, si risponde a un messaggio di "low spare" o si aggiunge capacità, la policy predefinita di assegnazione automatica assegna la proprietà del disco a un nodo come spare.

La policy di assegnazione automatica predefinita si basa su caratteristiche specifiche della piattaforma o sullo shelf DS460C, se la coppia ha dispone solo di questi shelf, e utilizza uno dei seguenti metodi (policy) per assegnare la proprietà dei dischi:

| Metodo di assegnazione | Effetto sulle assegnazioni dei nodi | Configurazioni di piattaforma predefinite per il metodo di assegnazione |
|---|---|---|
| baia | Gli alloggiamenti con numero pari sono assegnati al nodo A e quelli con numero dispari al nodo B. | Sistemi entry-level in una configurazione ha Pair con un singolo shelf condiviso. |

| | | |
|---|---|---|
| shelf | Tutti i dischi nello shelf sono assegnati al nodo A. | Sistemi entry-level in configurazione con coppia ha con uno stack di due o più shelf e configurazioni MetroCluster con uno stack per nodo, due o più shelf. |
| shelf separato<br><br>Questa politica rientra nel valore "default" per il `-autoassign -policy` del parametro `storage disk option` comando per le configurazioni di piattaforma e shelf applicabili. | I dischi sul lato sinistro dello shelf sono assegnati al nodo A e sul lato destro al nodo B. Gli shelf parziali sulle coppie ha vengono spediti dalla fabbrica con dischi popolati dal bordo dello shelf verso il centro. | La maggior parte delle piattaforme AFF e alcune configurazioni MetroCluster. |
| impilare | Tutti i dischi nello stack vengono assegnati al nodo A. | Sistemi entry-level autonomi e tutte le altre configurazioni. |
| mezzo cassetto<br><br>Questa politica rientra nel valore "default" per il `-autoassign -policy` del parametro `storage disk option` comando per le configurazioni di piattaforma e shelf applicabili. | Tutti i dischi nella metà sinistra di un cassetto da DS460C GB (alloggiamenti per unità da 0 a 5) sono assegnati al nodo A; tutti i dischi nella metà destra di un cassetto (alloggiamenti per unità da 6 a 11) sono assegnati al nodo B.<br><br>Quando si inizializza una coppia ha con solo DS460C shelf, l'assegnazione automatica della proprietà del disco non è supportata. È necessario assegnare manualmente la proprietà per le unità contenenti unità root/container che hanno la partizione root in base al criterio half-cassetti. | Coppie HA con solo DS460C shelf, dopo l'inizializzazione della coppia ha (avvio).<br><br>Dopo l'avvio di una coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (ad eccezione dei dischi root/container che hanno la partizione root) e a eventuali dischi aggiunti in futuro.<br><br>Se la coppia ha ha ha DS460C shelf oltre agli altri modelli, non verrà utilizzata la policy a mezzo cassetto. Il criterio predefinito utilizzato è dettato dalle caratteristiche specifiche della piattaforma. |

Impostazioni e modifiche dell'assegnazione automatica:

- È possibile visualizzare le impostazioni di assegnazione automatica correnti (on/off) con `storage disk option show` comando.
- È possibile disattivare l'assegnazione automatica utilizzando `storage disk option modify` comando.
- Se il criterio di assegnazione automatica predefinito non è consigliabile nell'ambiente in uso, è possibile specificare (modificare) il metodo di assegnazione alloggiamento, shelf o stack utilizzando `-autoassign -policy` nel `storage disk option modify` comando.

  Scopri come "Modificare le impostazioni per l'assegnazione automatica della proprietà del disco".

> I criteri di assegnazione automatica predefiniti a mezzo cassetto e a scaffale diviso sono univoci perché non possono essere impostati dagli utenti come i criteri di alloggiamento, scaffale e stack.

Nei sistemi ADP (Advanced Drive Partitioning), per eseguire l'assegnazione automatica di shelf half-popled, i dischi devono essere installati negli alloggiamenti corretti in base al tipo di shelf di cui si dispone:

- Se il tuo shelf non è uno shelf da DS460C, installa i dischi in maniera equilibrata sul lato sinistro e sul lato destro, spostandoti al centro. Ad esempio, sei dischi negli alloggiamenti 0-5 e sei dischi negli alloggiamenti 18-23 di uno shelf DS224C.
- Se lo shelf è DS460C, installare i dischi della prima fila (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto. Per le unità rimanenti, distribuirle uniformemente su ciascun cassetto riempiendo le file dei cassetti dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

  L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

> Se i dischi non sono installati negli alloggiamenti corretti sugli shelf popolati a metà, in caso di guasto e sostituzione del disco di un container, ONTAP non assegna automaticamente la proprietà. In questo caso, l'assegnazione della nuova unità contenitore deve essere eseguita manualmente. Dopo aver assegnato la proprietà ai dischi del container, ONTAP gestisce automaticamente tutte le assegnazioni necessarie per le partizioni e il partizionamento dei dischi.

In alcune situazioni in cui l'assegnazione automatica non funziona, è necessario assegnare manualmente la proprietà del disco tramite `storage disk assign` comando:

- Se si disattiva l'assegnazione automatica, i nuovi dischi non sono disponibili come spare fino a quando non verranno assegnati manualmente a un nodo.
- Se si desidera che i dischi vengano assegnati automaticamente e si dispone di più stack o shelf che devono avere proprietà diverse, un disco deve essere stato assegnato manualmente su ogni stack o shelf in modo che l'assegnazione automatica della proprietà funzioni su ogni stack o shelf.
- Se l'assegnazione automatica è attivata e si assegna manualmente un singolo disco a un nodo non specificato nel criterio attivo, l'assegnazione automatica smette di funzionare e viene visualizzato un messaggio EMS.

Scopri come "Assegnare manualmente la proprietà dei dischi non partizionati".

Scopri come "Assegnare manualmente la proprietà dei dischi partizionati".

#### Visualizzare la proprietà di dischi e partizioni

È possibile visualizzare la proprietà del disco per determinare quale nodo controlla lo storage. È inoltre possibile visualizzare la proprietà della partizione sui sistemi che utilizzano dischi condivisi.

**Fasi**

1. Visualizzare la proprietà dei dischi fisici:

```
storage disk show -ownership
```

```
cluster::> storage disk show -ownership
Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
Home ID  Reserver    Pool
-------- --------- -------- -------- -------- ---------- -----------
----------- ----------- ------
1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
1.0.3    -         node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
```

2. Se si dispone di un sistema che utilizza dischi condivisi, è possibile visualizzare la proprietà della partizione:

```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
                              Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

#### Modificare le impostazioni per l'assegnazione automatica della proprietà del disco

È possibile utilizzare `storage disk option modify` per selezionare una policy non predefinita per l'assegnazione automatica della proprietà del disco o per la disattivazione dell'assegnazione automatica della proprietà del disco.

Scopri di più "assegnazione automatica della proprietà del disco".

**A proposito di questa attività**

Se disponi di una coppia ha con solo DS460C shelf, il criterio di assegnazione automatica predefinito è a metà cassetto. Non è possibile passare a un criterio non predefinito (alloggiamento, shelf, stack).

**Fasi**

1. Modificare l'assegnazione automatica dei dischi:
   a. Se si desidera selezionare un criterio non predefinito, immettere:

      `storage disk option modify -autoassign-policy` *`autoassign_policy`* `-node` *`node_name`*

      - Utilizzare `stack` come *`autoassign_policy`* per configurare la proprietà automatica a livello di stack o loop.
      - Utilizzare `shelf` come *`autoassign_policy`* per configurare la proprietà automatica a livello di shelf.
      - Utilizzare `bay` come *`autoassign_policy`* per configurare la proprietà automatica a livello di alloggiamento.

   b. Se si desidera disattivare l'assegnazione automatica della proprietà del disco, immettere:

      `storage disk option modify -autoassign off -node` *`node_name`*

2. Verificare le impostazioni di assegnazione automatica dei dischi:

   `storage disk option show`

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                          Assign Policy
-------------  -------------  ------------  -------------  --------
cluster1-1     on             on            on             default
cluster1-2     on             on            on             default
```

#### Assegnare manualmente la proprietà dei dischi non partizionati

Se la coppia ha non è configurata per l'utilizzo dell'assegnazione automatica della proprietà del disco, devi assegnare manualmente la proprietà. Se stai inizializzando una coppia ha con solo DS460C shelf, devi assegnare manualmente la proprietà dei dischi root.

**A proposito di questa attività**

- Se stai assegnando manualmente la proprietà a una coppia ha che non viene inizializzata e che non ha solo DS460C shelf, utilizza l'opzione 1.
- Se stai inizializzando una coppia ha con solo DS460C shelf, puoi utilizzare l'opzione 2 per assegnare manualmente la proprietà dei dischi root.

**Opzione 1: Maggior parte delle coppie ha**

Per una coppia ha non inizializzata e che non dispone solo di DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà.

**A proposito di questa attività**

- I dischi per i quali si assegna la proprietà devono trovarsi in uno shelf collegato fisicamente al nodo a cui si assegna la proprietà.
- Se si utilizzano dischi in un Tier locale (aggregato):
  - I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).
  - Non è possibile riassegnare la proprietà di un disco in uso in un Tier locale (aggregato).

**Fasi**

1. Utilizzare la CLI per visualizzare tutti i dischi non posseduti:

   ```
   storage disk show -container-type unassigned
   ```

2. Assegnare ciascun disco:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta. Se si sta riassegnando un disco spare già di proprietà di un nodo diverso, è necessario utilizzare l'opzione "-force".

**Opzione 2: Coppia ha con solo DS460C shelf**

Per una coppia ha in fase di inizializzazione e dotata di soli DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà dei dischi root.

**A proposito di questa attività**

- Quando esegui l'inizializzazione di una coppia ha con soli DS460C shelf, devi assegnare manualmente i dischi root in modo che siano conformi alla policy a mezzo cassetto.

  Dopo l'inizializzazione (boot up) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi root) e a tutti i dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, in risposta a un messaggio di "low spare", o aggiungere capacità.

  Scoprite la politica di metà cassetto nell'argomento "Informazioni sull'assegnazione automatica della proprietà del disco".

- RAID richiede un minimo di 10 dischi per ciascuna coppia ha (5 per ogni nodo) per ogni più grande di 8TB dischi NL-SAS in uno shelf DS460C.

**Fasi**

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

   a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

      L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

   b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

      Riempire le file dei cassetti dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

      L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.


2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Assegnare manualmente le unità principali in ciascun cassetto in modo che siano conformi al criterio del mezzo cassetto, attenendosi alla seguente procedura:

   Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

   a. Visualizza tutti i dischi non posseduti:
      `storage disk show -container-type unassigned`
   b. Assegnare i dischi principali:
      `storage disk assign -disk disk_name -owner owner_name`

      È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta.

#### Assegnare manualmente la proprietà dei dischi partizionati

Puoi assegnare manualmente la proprietà del disco del container o delle partizioni sui sistemi ADP (Advanced Disk Partitioning). Se si sta inizializzando una coppia ha con solo DS460C shelf, è necessario assegnare manualmente la proprietà per i dischi dei container che includeranno le partizioni root.

**A proposito di questa attività**

- Il tipo di sistema di storage stabilito determina il metodo di ADP supportato, root-data (RD) o root-data-data (RD2).

  I sistemi storage FAS utilizzano la RD e i sistemi storage AFF RD2.

- Se si assegna manualmente la proprietà in una coppia ha che non viene inizializzata e non ha solo DS460C shelf, utilizzare l'opzione 1 per assegnare manualmente i dischi con partizione root-data (RD) oppure utilizzare l'opzione 2 per assegnare manualmente i dischi con partizione root-data-data (RD2).
- Se si sta inizializzando una coppia ha con solo DS460C shelf, utilizzare l'opzione 3 per assegnare

manualmente la proprietà ai dischi dei container che hanno la partizione root.

**Opzione 1: Assegnazione manuale dei dischi con partizione root-data (RD)**

Per la partizione dei dati root, esistono tre entità possedute (il disco container e le due partizioni) collettivamente di proprietà della coppia ha.

**A proposito di questa attività**

- Il disco container e le due partizioni non devono essere tutte di proprietà dello stesso nodo della coppia ha, purché siano tutte di proprietà di uno dei nodi della coppia ha. Tuttavia, quando si utilizza una partizione in un Tier locale (aggregato), questa deve essere di proprietà dello stesso nodo proprietario del Tier locale.
- Se un disco contenitore si guasta in uno shelf mezzo popolato e viene sostituito, potrebbe essere necessario assegnare manualmente la proprietà del disco perché in questo caso ONTAP non sempre assegna automaticamente la proprietà.
- Una volta assegnato il disco del container, il software ONTAP gestisce automaticamente tutte le partizioni e le assegnazioni necessarie.

**Fasi**

1. Utilizzare la CLI per visualizzare la proprietà corrente del disco partizionato:

   `storage disk show -disk disk_name -partition-ownership`

2. Impostare il livello di privilegio CLI su Advanced (avanzato):

   `set -privilege advanced`

3. Immettere il comando appropriato, a seconda dell'entità di proprietà per cui si desidera assegnare la proprietà:

   Se una delle entità di proprietà è già di proprietà, devi includere l'opzione "-force".

| Se si desidera assegnare la proprietà per… | Utilizzare questo comando… |
|---|---|
| Disco container | `storage disk assign -disk disk_name -owner owner_name` |
| Partizione dei dati | `storage disk assign -disk disk_name -owner owner_name -data true` |
| Partizione root | `storage disk assign -disk disk_name -owner owner_name -root true` |

**Opzione 2: Assegnazione manuale dei dischi con partizione root-data-data (RD2)**

Per la partizione root-data-data, esistono quattro entità possedute (il disco container e le tre partizioni) collettivamente di proprietà della coppia ha. La partizione root-data-data crea una partizione piccola come partizione root e due partizioni più grandi e di pari dimensioni per i dati.

**A proposito di questa attività**

- I parametri devono essere utilizzati con `disk assign` comando per assegnare la partizione corretta di un disco partizionato root-data-data. Non è possibile utilizzare questi parametri con dischi che fanno parte di un pool di storage. Il valore predefinito è “false”.
  - Il `-data1 true` il parametro assegna la partizione “data1” di un disco partizionato root-data1-data2.
  - Il `-data2 true` il parametro assegna la partizione “data2” di un disco partizionato root-data1-data2.
- Se un disco contenitore si guasta in uno shelf mezzo popolato e viene sostituito, potrebbe essere necessario assegnare manualmente la proprietà del disco perché in questo caso ONTAP non sempre assegna automaticamente la proprietà.
- Una volta assegnato il disco del container, il software ONTAP gestisce automaticamente tutte le partizioni e le assegnazioni necessarie.

**Fasi**

1. Utilizzare la CLI per visualizzare la proprietà corrente del disco partizionato:

   ```
   storage disk show -disk disk_name -partition-ownership
   ```

2. Impostare il livello di privilegio CLI su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

3. Immettere il comando appropriato, a seconda dell’entità di proprietà per cui si desidera assegnare la proprietà:

   Se una delle entità di proprietà è già di proprietà, devi includere l’opzione “-force”.

| Se si desidera assegnare la proprietà per… | Utilizzare questo comando… |
|---|---|
| Disco container | `storage disk assign -disk disk_name -owner owner_name` |
| Partizione Data1 | `storage disk assign -disk disk_name -owner owner_name -data1 true` |
| Partizione Data2 | `storage disk assign -disk disk_name -owner owner_name -data2 true` |
| Partizione root | `storage disk assign -disk disk_name -owner owner_name -root true` |

**Opzione 3: Assegnare manualmente DS460C unità contenitore che hanno la partizione root**

Se si sta inizializzando una coppia ha con solo DS460C shelf, occorre assegnare manualmente la proprietà per i dischi dei container che hanno la partizione root, conformemente al criterio half-cassetto.

**A proposito di questa attività**

- Quando si inizializza una coppia ha con solo DS460C shelf, le opzioni 9a e 9b del menu di boot ADP (disponibile con ONTAP 9,2 e versioni successive) non supportano l'assegnazione automatica della proprietà dei dischi. È necessario assegnare manualmente le unità contenitore che hanno la partizione root in base al criterio half-cassetti.

  Dopo l'inizializzazione (avvio) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi dei container che hanno la partizione root) e a eventuali dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, risposta a un messaggio di "riserva insufficiente" o aggiunta di capacità.

- Scoprite la politica di metà cassetto nell'argomento "Informazioni sull'assegnazione automatica della proprietà del disco".

**Fasi**

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

   a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

      L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

   b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

      Riempire le file dei cassetti dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

      L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.


2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Per ogni cassetto, assegnare manualmente le unità contenitore che hanno la partizione root in base al criterio Half-Drawer utilizzando i seguenti passaggi secondari:

   Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

   a. Visualizza tutti i dischi non posseduti:
      `storage disk show -container-type unassigned`
   b. Assegnare le unità contenitore che hanno la partizione root:
      `storage disk assign -disk disk_name -owner owner_name`

      È possibile utilizzare il carattere jolly per assegnare più unità alla volta.

#### Impostare una configurazione Active-passive sui nodi utilizzando la partizione dei dati root

Quando una coppia ha viene configurata in fabbrica per utilizzare la partizione dei dati root, la proprietà delle partizioni dei dati viene divisa tra entrambi i nodi della coppia per essere utilizzata in una configurazione Active-Active. Se si desidera utilizzare la coppia ha in una configurazione Active-passive, è necessario aggiornare la proprietà della partizione prima di creare il livello locale dei dati (aggregato).

**Di cosa hai bisogno**

- Si dovrebbe aver deciso quale nodo sarà il nodo attivo e quale nodo sarà il nodo passivo.
- Il failover dello storage deve essere configurato sulla coppia ha.

**A proposito di questa attività**

Questa attività viene eseguita su due nodi: Il nodo A e il nodo B.

Questa procedura è progettata per i nodi per i quali non è stato creato alcun Tier locale di dati (aggregato) dai dischi partizionati.

Scopri di più "partizione avanzata dei dischi".

**Fasi**

Tutti i comandi vengono immessi nella shell del cluster.

1. Visualizzare la proprietà corrente delle partizioni dei dati:

   ```
   storage aggregate show-spare-disks
   ```

   L'output mostra che metà delle partizioni di dati appartiene a un nodo e metà all'altro. Tutte le partizioni dei dati devono essere spare.

   ```
   cluster1::> storage aggregate show-spare-disks

   Original Owner: cluster1-01
    Pool0
     Partitioned Spares
                                                                Local
   Local
                                                                 Data
   Root Physical
    Disk                        Type     RPM Checksum         Usable
   Usable     Size
    --------------------------- ----- ------ -------------- --------
   -------- --------
    1.0.0                       BSAS    7200 block           753.8GB
   0B  828.0GB
    1.0.1                       BSAS    7200 block           753.8GB
   73.89GB  828.0GB
    1.0.5                       BSAS    7200 block           753.8GB
   0B  828.0GB
    1.0.6                       BSAS    7200 block           753.8GB
   0B  828.0GB
    1.0.10                      BSAS    7200 block           753.8GB
   0B  828.0GB
    1.0.11                      BSAS    7200 block           753.8GB
   0B  828.0GB

   Original Owner: cluster1-02
    Pool0
     Partitioned Spares
                                                                Local
   Local
                                                                 Data
   Root Physical
    Disk                        Type     RPM Checksum         Usable
   Usable     Size
   ```

```
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. Immettere il livello di privilegio avanzato:

   `set advanced`

3. Per ciascuna partizione di dati di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

   `storage disk assign -force -data true -owner` *`active_node_name`* `-disk` *`disk_name`*

   Non è necessario includere la partizione come parte del nome del disco.

   Immettere un comando simile all'esempio seguente per ciascuna partizione di dati da riassegnare:

   `storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3`

4. Verificare che tutte le partizioni siano assegnate al nodo attivo.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
```

```
 1.0.1                        BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                         Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                        BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Si noti che il cluster1-02 possiede ancora una partizione root spare.

5. Tornare al privilegio amministrativo:

   ```
   set admin
   ```

6. Crea il tuo aggregato di dati, lasciando almeno una partizione di dati come spare:

   ```
   storage aggregate create new_aggr_name -diskcount number_of_partitions -node
   ```

*active_node_name*

L'aggregato di dati viene creato e appartiene al nodo attivo.

#### Impostare una configurazione Active-passive sui nodi utilizzando la partizione root-data-data

Quando una coppia ha viene configurata per utilizzare la partizione dei dati root in fabbrica, la proprietà delle partizioni dei dati viene divisa tra entrambi i nodi della coppia per essere utilizzata in una configurazione Active-Active. Se si desidera utilizzare la coppia ha in una configurazione Active-passive, è necessario aggiornare la proprietà della partizione prima di creare il livello locale dei dati (aggregato).

**Di cosa hai bisogno**

- Si dovrebbe aver deciso quale nodo sarà il nodo attivo e quale nodo sarà il nodo passivo.
- Il failover dello storage deve essere configurato sulla coppia ha.

**A proposito di questa attività**

Questa attività viene eseguita su due nodi: Il nodo A e il nodo B.

Questa procedura è progettata per i nodi per i quali non è stato creato alcun Tier locale di dati (aggregato) dai dischi partizionati.

Scopri di più "partizione avanzata dei dischi".

**Fasi**

Tutti i comandi vengono immessi nella shell del cluster.

1. Visualizzare la proprietà corrente delle partizioni dei dati:

   ```
   storage aggregate show-spare-disks -original-owner passive_node_name -fields
   local-usable-data1-size, local-usable-data2-size
   ```

   L'output mostra che metà delle partizioni di dati appartiene a un nodo e metà all'altro. Tutte le partizioni dei dati devono essere spare.

2. Immettere il livello di privilegio avanzato:

   ```
   set advanced
   ```

3. Per ogni partizione data1 di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

   ```
   storage disk assign -force -data1 -owner active_node_name -disk disk_name
   ```

   Non è necessario includere la partizione come parte del nome del disco

4. Per ogni partizione data2 di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

   ```
   storage disk assign -force -data2 -owner active_node_name -disk disk_name
   ```

   Non è necessario includere la partizione come parte del nome del disco

5. Verificare che tutte le partizioni siano assegnate al nodo attivo:

```
storage aggregate show-spare-disks
```

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
```

```
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Si noti che il cluster1-02 possiede ancora una partizione root spare.

6. Tornare al privilegio amministrativo:

   `set admin`

7. Crea il tuo aggregato di dati, lasciando almeno una partizione di dati come spare:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node` *`active_node_name`*

   L'aggregato di dati viene creato e appartiene al nodo attivo.

8. In alternativa, è possibile utilizzare il layout aggregato consigliato da ONTAP, che include Best practice per il layout dei gruppi RAID e il numero di spare:

   `storage aggregate auto-provision`

#### Rimuovere la proprietà da un disco

ONTAP scrive le informazioni sulla proprietà del disco sul disco. Prima di rimuovere un disco spare o il relativo shelf da un nodo, è necessario rimuovere le relative informazioni di proprietà in modo che possano essere correttamente integrate in un altro nodo.

> Se il disco è partizionato per la partizione root-dati e si sta eseguendo ONTAP 9.10.1 o versioni successive, contattare il supporto tecnico di NetApp per assistenza nella rimozione della proprietà. Per ulteriori informazioni, consultare "Articolo della Knowledge base: Impossibile rimuovere il proprietario del disco".

**Di cosa hai bisogno**

Il disco da cui si desidera rimuovere la proprietà deve soddisfare i seguenti requisiti:

- Deve essere un disco spare.

  Non è possibile rimuovere la proprietà da un disco utilizzato in un Tier locale (aggregato).

- Non può trovarsi nel centro di manutenzione.
- Non può essere sottoposto a sanificazione.
- Non è possibile eseguire il guasto.

  Non è necessario rimuovere la proprietà da un disco guasto.

#### A proposito di questa attività

Se l'assegnazione automatica dei dischi è attivata, ONTAP potrebbe riassegnare automaticamente la proprietà prima di rimuovere il disco dal nodo. Per questo motivo, si disattiva l'assegnazione automatica della proprietà fino a quando il disco non viene rimosso, quindi si riattiva.

#### Fasi

1. Se l'assegnazione automatica della proprietà del disco è attivata, utilizzare la CLI per disattivarla:

   `storage disk option modify -node node_name -autoassign off`

2. Se necessario, ripetere il passaggio precedente per il partner ha del nodo.
3. Rimuovere le informazioni di proprietà del software dal disco:

   `storage disk removeowner disk_name`

   Per rimuovere le informazioni di proprietà da più dischi, utilizzare un elenco separato da virgole.

   Esempio:

   ```
   storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
   ```

4. Se il disco è partizionato per la partizione root-dati e si esegue ONTAP 9.9.1 o versioni precedenti, rimuovere la proprietà dalle partizioni:

   `storage disk removeowner -disk disk_name -root true`

   `storage disk removeowner -disk disk_name -data true`

   Entrambe le partizioni non sono più di proprietà di alcun nodo.

5. Se in precedenza è stata disattivata l'assegnazione automatica della proprietà del disco, attivarla dopo la rimozione o la riassegnazione del disco:

   `storage disk option modify -node node_name -autoassign on`

6. Se necessario, ripetere il passaggio precedente per il partner ha del nodo.

### Rimuovere un disco guasto

Un disco completamente guasto non viene più conteggiato da ONTAP come disco utilizzabile ed è possibile scollegare immediatamente il disco dallo shelf. Tuttavia, si consiglia di lasciare un disco parzialmente guasto collegato abbastanza a lungo per il completamento del processo di ripristino RAID rapido.

#### A proposito di questa attività

Se si rimuove un disco perché si è verificato un errore o perché genera messaggi di errore eccessivi, non utilizzare nuovamente il disco in questo o in qualsiasi altro sistema di storage.

#### Fasi

1. Utilizzare l'interfaccia CLI per individuare l'ID del disco guasto:

```
storage disk show -broken
```

Se il disco non compare nell'elenco dei dischi guasti, potrebbe essersi verificato un errore parziale, con un ripristino RAID rapido in corso. In questo caso, prima di rimuovere il disco, è necessario attendere che il disco sia presente nell'elenco dei dischi guasti (il che significa che il processo di ripristino RAID rapido è completo).

2. Determinare la posizione fisica del disco che si desidera rimuovere:

   ```
   storage disk set-led -action on -disk disk_name 2
   ```

   Il LED di errore sulla parte anteriore del disco è acceso.

3. Rimuovere il disco dallo shelf seguendo le istruzioni riportate nella guida hardware del modello di shelf.

## Pulizia dei dischi

### Panoramica sulla disinfezione dei dischi

La sanificazione del disco è il processo di cancellazione fisica dei dati mediante la sovrascrittura di dischi o SSD con modelli di byte specifici o dati casuali, in modo che il ripristino dei dati originali diventi impossibile. L'utilizzo del processo di sanificazione garantisce che nessuno possa ripristinare i dati sui dischi.

Questa funzionalità è disponibile attraverso il nodeshell in tutte le release di ONTAP 9 e a partire da ONTAP 9.6 in modalità di manutenzione.

Il processo di sanificazione del disco utilizza tre modelli di sovrascrittura dei byte predefiniti o specificati dall'utente per un massimo di sette cicli per operazione. Il modello di sovrascrittura casuale viene ripetuto per ogni ciclo.

A seconda della capacità del disco, dei modelli e del numero di cicli, il processo può richiedere diverse ore. La sanitizzazione viene eseguita in background. È possibile avviare, arrestare e visualizzare lo stato del processo di disinfezione. Il processo di sanificazione contiene due fasi: La "fase di formattazione" e la "fase di sovrascrittura del modello".

#### Fase di formattazione

L'operazione eseguita per la fase di formattazione dipende dalla classe di dischi da sanificare, come mostrato nella tabella seguente:

| Classe di dischi | Operazione della fase di formattazione |
|---|---|
| Capacità HDD | Ignorato |
| HDD dalle performance elevate | Funzionamento in formato SCSI |
| SSD | Operazione di sanificazione SCSI |

#### Fase di sovrascrittura del modello

I modelli di sovrascrittura specificati vengono ripetuti per il numero di cicli specificato.

Una volta completato il processo di sanificazione, i dischi specificati si trovano in uno stato di sanificazione. Non vengono ripristinati automaticamente lo stato spare. È necessario restituire i dischi sanitizzati al pool di spare prima che i dischi appena sanitizzati siano disponibili per essere aggiunti a un altro aggregato.

#### Quando non è possibile eseguire la sanificazione del disco

La pulizia dei dischi non è supportata per tutti i tipi di dischi. Inoltre, in alcuni casi non è possibile eseguire la sanificazione del disco.

- Non è supportato su tutti i codici prodotto SSD.

  Per informazioni sui codici prodotto SSD che supportano la disinfezione dei dischi, consultare "Hardware Universe".

- Non è supportato in modalità Takeover per i sistemi in una coppia ha.
- Non può essere eseguito su dischi che si sono guastati a causa di problemi di leggibilità o di scrivibilità.
- Non esegue la relativa fase di formattazione sui dischi ATA.
- Se si utilizza il modello random, non è possibile eseguirlo su più di 100 dischi alla volta.
- Non è supportato sui LUN degli array.
- Se si disigienizzano entrambi i dischi SES nello stesso shelf ESH contemporaneamente, vengono visualizzati errori sulla console relativi all'accesso a tale shelf e gli avvisi sullo shelf non vengono segnalati per la durata della sanitizzazione.

  Tuttavia, l'accesso ai dati a tale shelf non viene interrotto.

#### Cosa succede se la pulizia del disco viene interrotta

Se la sanificazione del disco viene interrotta da un intervento dell'utente o da un evento imprevisto, ad esempio un'interruzione dell'alimentazione, ONTAP esegue un'azione per riportare i dischi sottoposti a sanitizzazione a uno stato noto, ma è necessario eseguire un'azione prima che il processo di sanitizzazione possa terminare.

La sanificazione dei dischi è un'operazione a esecuzione prolungata. Se il processo di sanificazione viene interrotto da un'interruzione dell'alimentazione, dal panico del sistema o da un intervento manuale, il processo di sanificazione deve essere ripetuto dall'inizio. Il disco non è stato progettato come sanitizzato.

Se la fase di formattazione della disinfezione del disco viene interrotta, ONTAP deve ripristinare i dischi danneggiati dall'interruzione. Dopo un riavvio del sistema e una volta ogni ora, ONTAP verifica la presenza di eventuali dischi di destinazione per la sanificazione che non hanno completato la fase di formattazione della relativa sanificazione. Se vengono rilevati dischi di questo tipo, ONTAP li ripristina. Il metodo di ripristino dipende dal tipo di disco. Una volta ripristinato un disco, è possibile rieseguire il processo di pulizia su tale disco; per gli HDD, è possibile utilizzare `-s` opzione per specificare che la fase di formattazione non viene ripetuta.

#### Suggerimenti per la creazione e il backup di Tier locali (aggregati) contenenti dati da sanificare

Se si creano o eseguono il backup di Tier locali (aggregati) per contenere dati che potrebbero dover essere sanificati, seguire alcune semplici linee guida ridurrà il tempo necessario per la sanificazione dei dati.

- Assicurati che i livelli locali contenenti dati sensibili non siano più grandi di quanto sia necessario.

  Se sono più grandi del necessario, la sanitizzazione richiede più tempo, spazio su disco e larghezza di banda.

- Quando si esegue il backup dei Tier locali contenenti dati sensibili, evitare di eseguirne il backup su Tier locale che contenga anche grandi quantità di dati non sensibili.

  In questo modo si riducono le risorse necessarie per spostare i dati non sensibili prima di procedere alla pulizia dei dati sensibili.

#### Igienizzare un disco

La sanificazione di un disco consente di rimuovere i dati da un disco o da un set di dischi su sistemi decommissionati o inutilizzabili, in modo che i dati non possano mai essere ripristinati.

Sono disponibili due metodi per la sanificazione dei dischi mediante l'interfaccia CLI:

**Sanificazione di un disco con & 8220;modalità di manutenzione& 8221; comandi (ONTAP 9.6 e versioni successive)**

A partire da ONTAP 9.6, è possibile eseguire la pulizia del disco in modalità di manutenzione.

**Prima di iniziare**

- I dischi non possono essere dischi con crittografia automatica (SED).

  È necessario utilizzare `storage encryption disk sanitize` Comando per sanificare un SED.

  "Crittografia dei dati inattivi"

**Fasi**

1. Avviare in modalità di manutenzione.
   a. Uscire dalla shell corrente immettendo `halt`.

      Viene visualizzato il prompt DEL CARICATORE.

   b. Accedere alla modalità di manutenzione immettendo `boot_ontap maint`.

      Una volta visualizzate alcune informazioni, viene visualizzato il prompt della modalità di manutenzione.

2. Se i dischi da sanificare sono partizionati, dispartizionare ciascun disco:

   > Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. Si consiglia vivamente di contattare il supporto NetApp prima di procedere. Consultare anche l'articolo della Knowledge base "Come dispartizionare un disco spare in ONTAP"

   `disk unpartition` *`disk_name`*

3. Igienizzare i dischi specificati:

   `disk sanitize start [-p` *`pattern1`*`|-r [-p` *`pattern2`*`|-r [-p` *`pattern3`*`|-r]]] [-c` *`cycle_count`*`] ` *`disk_list`*

   > Non spegnere il nodo, interrompere la connettività dello storage o rimuovere i dischi di destinazione durante la pulizia. Se la pulizia viene interrotta durante la fase di formattazione, la fase di formattazione deve essere riavviata e completata prima che i dischi siano stati sanitizzati e pronti per essere restituiti al pool di riserva. Se è necessario interrompere il processo di sanificazione, è possibile farlo utilizzando `disk sanitize abort` comando. Se i dischi specificati sono sottoposti alla fase di formattazione della disinfezione, l'interruzione non avviene fino al completamento della fase.

```
`-p` `_pattern1_` `-p` `_pattern2_` `-p` `_pattern3_` specifica un
ciclo di uno o tre modelli di sovrascrittura di byte esadecimali
definiti dall'utente che possono essere applicati in successione ai
dischi da sanificare. Il modello predefinito è tre passaggi,
utilizzando 0x55 per il primo passaggio, 0xaa per il secondo
passaggio e 0x3c per il terzo passaggio.
```

`-r` sostituisce una sovrascrittura ripetuta con una sovrascrittura casuale per uno o tutti i passaggi.

`-c` *`cycle_count`* specifica il numero di volte in cui vengono applicati i modelli di sovrascrittura specificati. Il valore predefinito è un ciclo. Il valore massimo è di sette cicli.

*`disk_list`* Specifica un elenco degli ID dei dischi spare da sanificare, separati da spazio.

4. Se lo si desidera, controllare lo stato del processo di pulizia del disco:

   `disk sanitize status [`*`disk_list`*`]`

5. Una volta completato il processo di sanificazione, riportare i dischi allo stato spare per ciascun disco:

   `disk sanitize release` *`disk_name`*

6. Uscire dalla modalità di manutenzione.

**Sanificazione di un disco con i comandi 8220; nodeshel 8221; (tutte le release di ONTAP 9)**

Per tutte le versioni di ONTAP 9, quando la disinfezione del disco viene attivata utilizzando comandi nodeshell, alcuni comandi ONTAP di basso livello sono disattivati. Una volta attivata la sanificazione del disco su un nodo, non è possibile disattivarla.

**Prima di iniziare**

- I dischi devono essere dischi spare; devono essere di proprietà di un nodo, ma non devono essere utilizzati in un Tier locale (aggregato).

  Se i dischi sono partizionati, nessuna partizione può essere utilizzata in un Tier locale (aggregato).

- I dischi non possono essere dischi con crittografia automatica (SED).

  È necessario utilizzare `storage encryption disk sanitize` Comando per sanificare un SED.

  "Crittografia dei dati inattivi"

- I dischi non possono far parte di un pool di storage.

**Fasi**

1. Se i dischi da sanificare sono partizionati, dispartizionare ciascun disco:

   > Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. **Si consiglia vivamente di contattare il supporto NetApp prima di procedere.** è inoltre possibile consultare l'articolo della Knowledge base "Come dispartizionare un disco spare in ONTAP".

   ```
   disk unpartition disk_name
   ```

2. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:

   ```
   system node run -node node_name
   ```

3. Abilitare la sanificazione del disco:

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   Viene richiesto di confermare il comando perché è irreversibile.

4. Passa al livello avanzato di privilegi più avanzato:

   ```
   priv set advanced
   ```

5. Igienizzare i dischi specificati:

   ```
   disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c
   cycle_count] disk_list
   ```

> Non spegnere il nodo, interrompere la connettività dello storage o rimuovere i dischi di destinazione durante la pulizia. Se la pulizia viene interrotta durante la fase di formattazione, la fase di formattazione deve essere riavviata e completata prima che i dischi siano stati sanitizzati e pronti per essere restituiti al pool di riserva. Se è necessario interrompere il processo di sanificazione, è possibile farlo utilizzando il comando disk sanitize abortor. Se i dischi specificati sono sottoposti alla fase di formattazione della disinfezione, l'interruzione non avviene fino al completamento della fase.

`-p pattern1 -p pattern2 -p pattern3` specifica un ciclo di uno o tre modelli di sovrascrittura di byte esadecimali definiti dall'utente che possono essere applicati in successione ai dischi da sanificare. Il modello predefinito è tre passaggi, utilizzando 0x55 per il primo passaggio, 0xaa per il secondo passaggio e 0x3c per il terzo passaggio.

`-r` sostituisce una sovrascrittura ripetuta con una sovrascrittura casuale per uno o tutti i passaggi.

`-c cycle_count` specifica il numero di volte in cui vengono applicati i modelli di sovrascrittura specificati.

Il valore predefinito è un ciclo. Il valore massimo è di sette cicli.

`disk_list` Specifica un elenco degli ID dei dischi spare da sanificare, separati da spazio.

6. Se si desidera controllare lo stato del processo di pulizia del disco:

   ```
   disk sanitize status [disk_list]
   ```

7. Una volta completato il processo di sanificazione, riportare i dischi allo stato spare:

   ```
   disk sanitize release disk_name
   ```

8. Torna al livello di privilegio admin nodeshell:

   ```
   priv set admin
   ```

9. Tornare all'interfaccia utente di ONTAP:

   ```
   exit
   ```

10. Determinare se tutti i dischi sono stati riportati allo stato spare:

    ```
    storage aggregate show-spare-disks
    ```

| Se… | Quindi… |
|---|---|
| Tutti i dischi sanitizzati sono elencati come spare | Hai finito. I dischi sono stati sanitizzati e in stato spare. |

| | |
|---|---|
| Alcuni dischi sanitizzati non sono elencati come dischi di riserva | Attenersi alla seguente procedura:<br>a. Accedere alla modalità avanzata dei privilegi:<br>`set -privilege advanced`<br>b. Assegnare i dischi sanitizzati non assegnati al nodo appropriato per ciascun disco:<br>`storage disk assign -disk` *`disk_name`* `-owner` *`node_name`*<br>c. Riportare i dischi allo stato spare per ciascun disco:<br>`storage disk unfail -disk` *`disk_name`* `-s -q`<br>d. Tornare alla modalità amministrativa:<br>`set -privilege admin` |

**Risultato**

I dischi specificati vengono sanitizzati e designati come hot spare. I numeri di serie dei dischi sanitizzati vengono scritti in `/etc/log/sanitized_disks`.

Vengono scritti i log di disk sanitization che mostrano gli elementi completati su ogni disco `/mroot/etc/log/sanitization.log`.

**Comandi per la gestione dei dischi**

## È possibile utilizzare `storage disk` e. `storage aggregate` comandi per gestire i dischi.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Visualizza un elenco di dischi di riserva, inclusi i dischi partizionati, per proprietario | `storage aggregate show-spare-disks` |
| Visualizza il tipo di RAID del disco, l'utilizzo corrente e il gruppo RAID per aggregato | `storage aggregate show-status` |
| Visualizzare il tipo di RAID, l'utilizzo corrente, l'aggregato e il gruppo RAID, inclusi i ricambi, per i dischi fisici | `storage disk show -raid` |
| Visualizza un elenco di dischi guasti | `storage disk show -broken` |

| | |
|---|---|
| Visualizzare il nome del disco pre-cluster (nodescope) per un disco | `storage disk show -primary-paths` (avanzato) |
| Accendere il LED di un disco o di uno shelf specifico | `storage disk set-led` |
| Visualizza il tipo di checksum per un disco specifico | `storage disk show -fields checksum-compatibility` |
| Visualizza il tipo di checksum per tutti i dischi spare | `storage disk show -fields checksum-compatibility -container-type spare` |
| Visualizzazione delle informazioni sulla connettività e sul posizionamento dei dischi | `storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay` |
| Visualizzare i nomi dei dischi pre-cluster per dischi specifici | `storage disk show -disk diskname -fields diskpathnames` |
| Visualizzare l'elenco dei dischi nel centro di manutenzione | `storage disk show -maintenance` |
| Mostra la durata dell'unità SSD | `storage disk show -ssd-wear` |
| Dispartizione di un disco condiviso | `storage disk unpartition` (disponibile a livello diagnostico) |
| Azzerare tutti i dischi non azzerati | `storage disk zerospares` |
| Interrompere un processo di sanificazione in corso su uno o più dischi specificati | `system node run -node nodename -command disk sanitize` |
| Visualizzare le informazioni sul disco di crittografia dello storage | `storage encryption disk show` |
| Recuperare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati | `security key-manager restore` |

**Informazioni correlate**

"Comandi di ONTAP 9"

**Comandi per la visualizzazione delle informazioni sull'utilizzo dello spazio**

Si utilizza `storage aggregate` e. `volume` Comandi per vedere come viene utilizzato lo spazio negli aggregati, nei volumi e nelle relative copie Snapshot.

| Per visualizzare informazioni su… | Utilizzare questo comando… |
| --- | --- |
| Aggregati, inclusi i dettagli sulle percentuali di spazio utilizzate e disponibili, le dimensioni della riserva Snapshot e altre informazioni sull'utilizzo dello spazio | `storage aggregate show`<br>`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve` |
| Modalità di utilizzo dei dischi e dei gruppi RAID in un aggregato e nello stato RAID | `storage aggregate show-status` |
| La quantità di spazio su disco che verrebbe recuperata se si elimina una copia Snapshot specifica | `volume snapshot compute-reclaimable` |
| La quantità di spazio utilizzata da un volume | `volume show -fields size,used,available,percent-used`<br>`volume show-space` |
| La quantità di spazio utilizzata da un volume nell'aggregato contenente | `volume show-footprint` |

**Informazioni correlate**

"Comandi di ONTAP 9"

**Comandi per visualizzare informazioni sugli shelf di storage**

Si utilizza `storage shelf show` comando per visualizzare le informazioni di configurazione e di errore per gli shelf di dischi.

| **Se si desidera visualizzare…** | **Utilizzare questo comando…** |
| --- | --- |
| Informazioni generali sulla configurazione dello shelf e sullo stato dell'hardware | `storage shelf show` |
| Informazioni dettagliate per uno shelf specifico, incluso l'ID dello stack | `storage shelf show -shelf` |
| Errori irrisolti, gestibili dal cliente, per shelf | `storage shelf show -errors` |
| Informazioni sugli alloggiamenti | `storage shelf show -bay` |
| Informazioni sulla connettività | `storage shelf show -connectivity` |
| Informazioni sul raffreddamento, tra cui sensori di temperatura e ventole di raffreddamento | `storage shelf show -cooling` |
| Informazioni sui moduli i/O. | `storage shelf show -module` |

| Se si desidera visualizzare… | Utilizzare questo comando… |
| --- | --- |
| Informazioni sulla porta | `storage shelf show -port` |
| Informazioni sull'alimentazione, inclusi PSU (alimentatori), sensori di corrente e sensori di tensione | `storage shelf show -power` |

**Informazioni correlate**

"Comandi di ONTAP 9"

## Gestire le configurazioni RAID

### Panoramica sulla gestione delle configurazioni RAID

È possibile eseguire varie procedure per gestire le configurazioni RAID nel sistema.

- **Aspetti della gestione delle configurazioni RAID**:
  - "Policy RAID predefinite per Tier locali (aggregati)"
  - "Livelli di protezione RAID per i dischi"
- **Informazioni su unità e gruppi RAID per un Tier locale (aggregato)**
  - "Determinare le informazioni su unità e gruppi RAID per un Tier locale (aggregato)"
- **Conversioni della configurazione RAID**
  - "Conversione da RAID-DP a RAID-TEC"
  - "Conversione da RAID-TEC a RAID-DP"
- **Dimensionamento del gruppo RAID**
  - "Considerazioni per il dimensionamento dei gruppi RAID"
  - "Personalizzare le dimensioni del gruppo RAID"

### Policy RAID predefinite per Tier locali (aggregati)

RAID-DP o RAID-TEC è il criterio RAID predefinito per tutti i nuovi Tier locali (aggregati). Il criterio RAID determina la protezione di parità in caso di guasto del disco.

RAID-DP offre una protezione a doppia parità in caso di guasto di un disco singolo o doppio. RAID-DP è il criterio RAID predefinito per i seguenti tipi di Tier locale (aggregato):

- Tier locali All Flash
- Tier locali di Flash Pool
- Tier locali dei dischi rigidi (HDD) dalle performance elevate

RAID-TEC è supportato su tutti i tipi di dischi e su tutte le piattaforme, incluso AFF. I Tier locali che contengono dischi più grandi hanno una maggiore possibilità di guasti simultanei dei dischi. RAID-TEC aiuta a mitigare questo rischio fornendo una protezione a tripla parità in modo che i dati possano sopravvivere fino a tre guasti simultanei del disco. RAID-TEC è il criterio RAID predefinito per i Tier locali di capacità dei dischi rigidi con dischi di 6 TB o superiori.

Ogni tipo di policy RAID richiede un numero minimo di dischi:

- RAID-DP: Minimo 5 dischi
- RAID-TEC: Minimo 7 dischi

#### Livelli di protezione RAID per i dischi

ONTAP supporta tre livelli di protezione RAID per Tier locali (aggregati). Il livello di protezione RAID determina il numero di dischi di parità disponibili per il ripristino dei dati in caso di guasti al disco.

Con la protezione RAID, se si verifica un guasto al disco dati in un gruppo RAID, ONTAP può sostituire il disco guasto con un disco spare e utilizzare i dati di parità per ricostruire i dati del disco guasto.

- **RAID4**

  Con la protezione RAID4, ONTAP può utilizzare un disco spare per sostituire e ricostruire i dati da un disco guasto all'interno del gruppo RAID.

- **RAID-DP**

  Con la protezione RAID-DP, ONTAP può utilizzare fino a due dischi di riserva per sostituire e ricostruire i dati da un massimo di due dischi guasti contemporaneamente all'interno del gruppo RAID.

- **RAID-TEC**

  Con la protezione RAID-TEC, ONTAP può utilizzare fino a tre dischi di riserva per sostituire e ricostruire i dati da un massimo di tre dischi guasti contemporaneamente all'interno del gruppo RAID.

#### Informazioni su unità e gruppi RAID per un Tier locale (aggregato)

Alcune attività di amministrazione del Tier locale (aggregato) richiedono di conoscere i tipi di dischi che compongono il Tier locale, le loro dimensioni, checksum e stato, se sono condivisi con altri Tier locali e le dimensioni e la composizione dei gruppi RAID.

**Fase**

1. Mostra i dischi per l'aggregato, in base al gruppo RAID:

   `storage aggregate show-status` *`aggr_name`*

   I dischi vengono visualizzati per ciascun gruppo RAID nell'aggregato.

   È possibile visualizzare il tipo RAID del disco (dati, parità, dparity) in `Position` colonna. Se il `Position` viene visualizzata la colonna `shared`, Quindi l'unità viene condivisa: Se si tratta di un disco HDD, si tratta di un disco partizionato; se si tratta di un disco SSD, fa parte di un pool di storage.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

#### Conversione da RAID-DP a RAID-TEC

Se si desidera una protezione aggiuntiva della tripla parità, è possibile convertire da RAID-DP a RAID-TEC. RAID-TEC è consigliato se le dimensioni dei dischi utilizzati nel Tier locale (aggregato) sono superiori a 4 TIB.

##### Di cosa hai bisogno

Il Tier locale (aggregato) da convertire deve avere un minimo di sette dischi.

##### A proposito di questa attività

I Tier locali dei dischi rigidi possono essere convertiti da RAID-DP a RAID-TEC. Sono inclusi i Tier HDD nei Tier locali di Flash Pool.

##### Fasi

1. Verificare che l'aggregato sia online e disponga di almeno sei dischi:

   ```
   storage aggregate show-status -aggregate aggregate_name
   ```

2. Convertire l'aggregato da RAID-DP a RAID-TEC:

   ```
   storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
   ```

3. Verificare che il criterio RAID aggregato sia RAID-TEC:

   ```
   storage aggregate show aggregate_name
   ```

#### Conversione da RAID-TEC a RAID-DP

Se si riducono le dimensioni del Tier locale (aggregato) e non è più necessaria la tripla parità, è possibile convertire la policy RAID da RAID-TEC a RAID-DP e ridurre il numero di dischi necessari per la parità RAID.

##### Di cosa hai bisogno

La dimensione massima del gruppo RAID per RAID-TEC è superiore alla dimensione massima del gruppo RAID per RAID-DP. Se la dimensione massima del gruppo RAID-TEC non rientra nei limiti RAID-DP, non è possibile eseguire la conversione in RAID-DP.

##### Fasi

1. Verificare che l'aggregato sia online e disponga di almeno sei dischi:

   ```
   storage aggregate show-status -aggregate aggregate_name
   ```

2. Convertire l'aggregato da RAID-TEC a RAID-DP:

   ```
   storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
   ```

3. Verificare che il criterio RAID aggregato sia RAID-DP:

   ```
   storage aggregate show aggregate_name
   ```

#### Considerazioni per il dimensionamento dei gruppi RAID

La configurazione di una dimensione ottimale del gruppo RAID richiede un compromesso di fattori. È necessario decidere quali fattori: Velocità di ricostruzione RAID, garanzia contro il rischio di perdita di dati dovuta a guasti del disco, ottimizzazione delle performance i/o e massimizzazione dello spazio di storage dei dati, sono i fattori più importanti per l'aggregato (Tier locale) che si sta configurando.

Quando si creano gruppi RAID più grandi, si massimizza lo spazio disponibile per lo storage dei dati per la stessa quantità di storage utilizzata per la parità (nota anche come "parità fiscale"). D'altra parte, quando un disco si guasta in un gruppo RAID più grande, il tempo di ricostruzione aumenta, influenzando le prestazioni per un periodo di tempo più lungo. Inoltre, la presenza di più dischi in un gruppo RAID aumenta la probabilità di guasti a più dischi all'interno dello stesso gruppo RAID.

##### Gruppi RAID HDD o LUN array

Attenersi alle seguenti linee guida per il dimensionamento dei gruppi RAID composti da HDD o LUN di array:

- Tutti i gruppi RAID in un Tier locale (aggregato) devono avere lo stesso numero di dischi.

Anche se è possibile avere fino al 50% in meno o più del numero di dischi in diversi gruppi raid su un unico livello locale, in alcuni casi ciò potrebbe causare colli di bottiglia nelle performance, per cui è meglio evitarlo.

- L'intervallo consigliato di numeri di dischi del gruppo RAID è compreso tra 12 e 20.

  L'affidabilità dei dischi dalle performance può supportare un gruppo RAID di dimensioni fino a 28, se necessario.

- Se è possibile soddisfare le prime due linee guida con più numeri di dischi di gruppo RAID, è necessario scegliere il numero maggiore di dischi.

#### Gruppi RAID SSD nei Tier locali di Flash Pool (aggregati)

Le dimensioni del gruppo RAID SSD possono essere diverse dalle dimensioni del gruppo RAID per i gruppi RAID HDD in un Tier locale di Flash Pool (aggregato). In genere, è necessario assicurarsi di disporre di un solo gruppo RAID SSD per un livello locale di Flash Pool, per ridurre al minimo il numero di SSD necessari per la parità.

#### Gruppi RAID SSD in Tier locali SSD (aggregati)

Attenersi alle seguenti linee guida per il dimensionamento dei gruppi RAID composti da SSD:

- Tutti i gruppi RAID in un Tier locale (aggregato) devono avere un numero di dischi simile.

  I gruppi RAID non devono avere esattamente le stesse dimensioni, ma si consiglia di evitare di avere gruppi RAID di dimensioni inferiori alla metà di altri gruppi RAID nello stesso livello locale, se possibile.

- Per RAID-DP, l'intervallo consigliato per le dimensioni del gruppo RAID è compreso tra 20 e 28.

### Personalizzare le dimensioni dei gruppi RAID

È possibile personalizzare le dimensioni dei gruppi RAID per garantire che le dimensioni dei gruppi RAID siano appropriate per la quantità di storage che si intende includere per un Tier locale (aggregato).

#### A proposito di questa attività

Per i Tier locali standard (aggregati), è possibile modificare separatamente la dimensione dei gruppi RAID per ciascun Tier locale. Per i Tier locali di Flash Pool, è possibile modificare le dimensioni del gruppo RAID per i gruppi RAID SSD e i gruppi RAID HDD in modo indipendente.

Il seguente elenco descrive alcuni fatti relativi alla modifica delle dimensioni del gruppo RAID:

- Per impostazione predefinita, se il numero di dischi o LUN degli array nel gruppo RAID creato più di recente è inferiore alla dimensione del nuovo gruppo RAID, i dischi o le LUN degli array verranno aggiunti al gruppo RAID creato più di recente fino a raggiungere la nuova dimensione.
- Tutti gli altri gruppi RAID esistenti in tale Tier locale rimangono delle stesse dimensioni, a meno che non si aggiungano esplicitamente dischi.
- Non è mai possibile fare in modo che un gruppo RAID diventi più grande della dimensione massima corrente del gruppo RAID per il Tier locale.
- Non è possibile ridurre le dimensioni dei gruppi RAID già creati.
- La nuova dimensione si applica a tutti i gruppi RAID in quel Tier locale (o, nel caso di un Tier locale di

Flash Pool, a tutti i gruppi RAID per il tipo di gruppo RAID interessato, ovvero SSD o HDD).

**Fasi**

1. Utilizzare il comando applicabile:

| Se si desidera… | Immettere il seguente comando… |
|---|---|
| Modificare la dimensione massima del gruppo RAID per i gruppi RAID SSD di un aggregato Flash Pool | `storage aggregate modify -aggregate aggr_name -cache-raid-group-size size` |
| Modificare la dimensione massima di qualsiasi altro gruppo RAID | `storage aggregate modify -aggregate aggr_name -maxraidsize size` |

**Esempi**

Il seguente comando modifica la dimensione massima del gruppo RAID dell'aggregato n1_a4 in 20 dischi o LUN di array:

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

Il seguente comando modifica la dimensione massima del gruppo RAID dei gruppi RAID della cache SSD dell'aggregato di Flash Pool n1_cache_a2 in 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Gestire i Tier locali di Flash Pool (aggregati)

### Gestire i Tier di Flash Pool (aggregati)

È possibile eseguire varie procedure per gestire i Tier (aggregati) di Flash Pool nel sistema.

- **Criteri di caching**
  - "Policy di caching del Tier locale (aggregato) di Flash Pool"
  - "Gestire le policy di caching di Flash Pool"
- **Partizione SSD**
  - "Partizione SSD di Flash Pool per Tier locali (aggregati) di Flash Pool utilizzando pool di storage"
- **Candidature e dimensione della cache**
  - "Determinare la candidatura di Flash Pool e le dimensioni ottimali della cache"
- **Creazione di Flash Pool**
  - "Creare un Tier locale (aggregato) di Flash Pool utilizzando SSD fisici"
  - "Creare un Tier locale Flash Pool (aggregato) utilizzando i pool di storage SSD"

### Policy di caching del Tier locale (aggregato) di Flash Pool

Le policy di caching per i volumi in un Tier locale (aggregato) di Flash Pool consentono di implementare la Flash come cache dalle performance elevate per il set di dati di lavoro,

utilizzando al contempo HDD a basso costo per i dati ad accesso meno frequente. Se si fornisce la cache a due o più Tier locali di Flash Pool, è necessario utilizzare la partizione SSD di Flash Pool per condividere gli SSD tra i Tier locali di Flash Pool.

I criteri di caching vengono applicati ai volumi che risiedono nei Tier locali di Flash Pool. Prima di modificarle, è necessario comprendere il funzionamento delle policy di caching.

Nella maggior parte dei casi, il criterio di caching predefinito “auto” è il miglior criterio di caching da utilizzare. La policy di caching deve essere modificata solo se una policy diversa offre performance migliori per il carico di lavoro. La configurazione di una policy di caching errata può degradare notevolmente le performance dei volumi; il degrado delle performance potrebbe aumentare gradualmente nel tempo.

Le policy di caching combinano una policy di caching in lettura e una policy di caching in scrittura. Il nome del criterio concatena i nomi del criterio di caching in lettura e del criterio di caching in scrittura, separati da un trattino. Se non è presente un trattino nel nome del criterio, il criterio di caching in scrittura è “none”, ad eccezione del criterio “auto”.

Le policy di caching in lettura ottimizzano le performance di lettura future inserendo una copia dei dati nella cache oltre ai dati memorizzati sugli HDD. Per le policy di caching in lettura che inseriscono i dati nella cache per le operazioni di scrittura, la cache funziona come una cache *write-through*.

I dati inseriti nella cache utilizzando il criterio di caching in scrittura esistono solo nella cache; non è presente alcuna copia negli HDD. La cache di Flash Pool è protetta da RAID. L’attivazione del caching in scrittura rende immediatamente disponibili i dati delle operazioni di scrittura per le letture dalla cache, mentre rinviando la scrittura dei dati sugli HDD fino a quando non esaurisce la cache.

Se si sposta un volume da un livello locale di Flash Pool a un livello locale a livello singolo, il criterio di caching viene perso; se successivamente lo si sposta di nuovo su un livello locale di Flash Pool, viene assegnato il criterio di caching predefinito “auto”. Se si sposta un volume tra due livelli locali di Flash Pool, il criterio di caching viene mantenuto.

#### Modificare un criterio di caching

È possibile utilizzare la CLI per modificare il criterio di caching per un volume che risiede su un livello locale di Flash Pool utilizzando `-caching-policy` con il `volume create` comando.

Quando si crea un volume su un Tier locale di Flash Pool, per impostazione predefinita, al volume viene assegnato il criterio di caching “auto”.

### Gestire le policy di caching di Flash Pool

#### Panoramica sulla gestione delle policy di caching di Flash Pool

Utilizzando la CLI, è possibile eseguire varie procedure per gestire le policy di caching di Flash Pool nel sistema.

- **Preparazione**
  - "Determinare se modificare la policy di caching dei Tier locali (aggregati) di Flash Pool"
- **Modifica delle policy di caching**
  - "Modificare le policy di caching dei Tier locali di Flash Pool (aggregati)"
  - "Impostare il criterio di conservazione della cache per i Tier locali (aggregati) di Flash Pool"

#### Determinare se modificare la policy di caching dei Tier locali (aggregati) di Flash Pool

È possibile assegnare criteri di conservazione della cache ai volumi nei Tier locali (aggregati) di Flash Pool per determinare la durata dei dati del volume nella cache di Flash Pool. Tuttavia, in alcuni casi, la modifica del criterio di conservazione della cache potrebbe non influire sul tempo in cui i dati del volume rimangono nella cache.

**A proposito di questa attività**

Se i dati soddisfano una delle seguenti condizioni, la modifica della policy di conservazione della cache potrebbe non avere alcun impatto:

- Il carico di lavoro è sequenziale.
- Il carico di lavoro non rileggerà i blocchi casuali memorizzati nella cache dei dischi a stato solido (SSD).
- La dimensione della cache del volume è troppo piccola.

**Fasi**

I seguenti passaggi verificano le condizioni che devono essere soddisfatte dai dati. L'attività deve essere eseguita utilizzando la CLI in modalità avanzata con privilegi.

1. Utilizzare la CLI per visualizzare il volume del carico di lavoro:

   ```
   statistics start -object workload_volume
   ```

2. Determinare il modello di carico di lavoro del volume:

   ```
   statistics show -object workload_volume -instance volume-workload -counter
   sequential_reads
   ```

3. Determinare la percentuale di hit del volume:

   ```
   statistics show -object wafl_hya_vvol -instance volume -counter
   read_ops_replaced_pwercent|wc_write_blks_overwritten_percent
   ```

4. Determinare il `Cacheable Read` e. `Project Cache Alloc` del volume:

   ```
   system node run -node node_name wafl awa start aggr_name
   ```

5. Visualizzare il riepilogo AWA:

   ```
   system node run -node node_name wafl awa print aggr_name
   ```

6. Confronta la percentuale di hit del volume con `Cacheable Read`.

   Se la percentuale di hit del volume è maggiore di `Cacheable Read`, Quindi, il carico di lavoro non rileggerà i blocchi casuali memorizzati nella cache degli SSD.

7. Confrontare le dimensioni correnti della cache del volume con `Project Cache Alloc`.

   Se la dimensione corrente della cache del volume è maggiore di `Project Cache Alloc`, quindi la dimensione della cache del volume è troppo piccola.

#### Modificare le policy di caching dei Tier locali di Flash Pool (aggregati)

È necessario modificare il criterio di caching di un volume solo se si prevede che un diverso criterio di caching fornisca prestazioni migliori. È possibile modificare il criterio di caching di un volume su un Tier locale di Flash Pool (aggregato).

**Di cosa hai bisogno**

È necessario determinare se si desidera modificare il criterio di caching.

**A proposito di questa attività**

Nella maggior parte dei casi, il criterio di caching predefinito “auto” è il miglior criterio di caching che sia possibile utilizzare. La policy di caching deve essere modificata solo se una policy diversa offre performance migliori per il carico di lavoro. La configurazione di una policy di caching errata può degradare notevolmente le performance dei volumi; il degrado delle performance potrebbe aumentare gradualmente nel tempo. Prestare attenzione quando si modificano i criteri di caching. In caso di problemi di performance con un volume per il quale è stato modificato il criterio di caching, riportare il criterio di caching su “auto”.

**Fase**

1. Utilizzare la CLI per modificare il criterio di caching del volume:

   ```
   volume modify -volume volume_name -caching-policy policy_name
   ```

**Esempio**

Nell’esempio riportato di seguito viene modificata la policy di caching di un volume denominato “vol2” nella policy “none”:

```
volume modify -volume vol2 -caching-policy none
```

#### Impostare il criterio di conservazione della cache per i Tier locali (aggregati) di Flash Pool

È possibile assegnare criteri di conservazione della cache ai volumi nei Tier locali di Flash Pool (aggregati). I dati nei volumi con una policy di conservazione della cache elevata rimangono nella cache più a lungo e i dati nei volumi con una policy di conservazione della cache bassa vengono rimossi prima. Ciò aumenta le performance dei carichi di lavoro critici rendendo accessibili le informazioni ad alta priorità a una velocità più rapida per un periodo di tempo più lungo.

**Di cosa hai bisogno**

È necessario sapere se il sistema presenta condizioni che potrebbero impedire al criterio di conservazione della cache di avere un impatto sulla durata dei dati nella cache.

**Fasi**

Utilizzare la CLI in modalità avanzata dei privilegi per eseguire le seguenti operazioni:

1. Impostare i privilegi su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Verificare il criterio di conservazione della cache del volume:

   Per impostazione predefinita, il criterio di conservazione della cache è “normal”.

3. Impostare il criterio di conservazione della cache:

| Versione di ONTAP | Comando |
|---|---|
| ONTAP 9.0, 9.1 | `priority hybrid-cache set volume_name read-cache=read_cache_value write-cache=write_cache_value cache-retention-priority=cache_retention_policy`<br><br>Impostare `cache_retention_policy` a. `high` per i dati che si desidera conservare nella cache più a lungo. Impostare `cache_retention_policy` a. `low` per i dati che si desidera rimuovere prima dalla cache. |
| ONTAP 9.2 o versione successiva | `volume modify -volume volume_name -vserver vserver_name -caching-policy policy_name.` |

4. Verificare che il criterio di conservazione della cache del volume sia stato modificato nell'opzione selezionata.
5. Restituire l'impostazione dei privilegi ad admin:

```
set -privilege admin
```

**Partizione SSD di Flash Pool per Tier locali (aggregati) di Flash Pool utilizzando pool di storage**

Se si fornisce la cache a due o più Tier locali di Flash Pool (aggregati), è necessario utilizzare la partizione SSD (Solid state Drive) di Flash Pool. Il partizionamento degli SSD Flash Pool consente di condividere gli SSD con tutti i Tier locali che utilizzano Flash Pool. In questo modo, il costo di parità viene diffuso su più Tier locali, la flessibilità di allocazione della cache SSD aumenta e le performance SSD massimizzano.

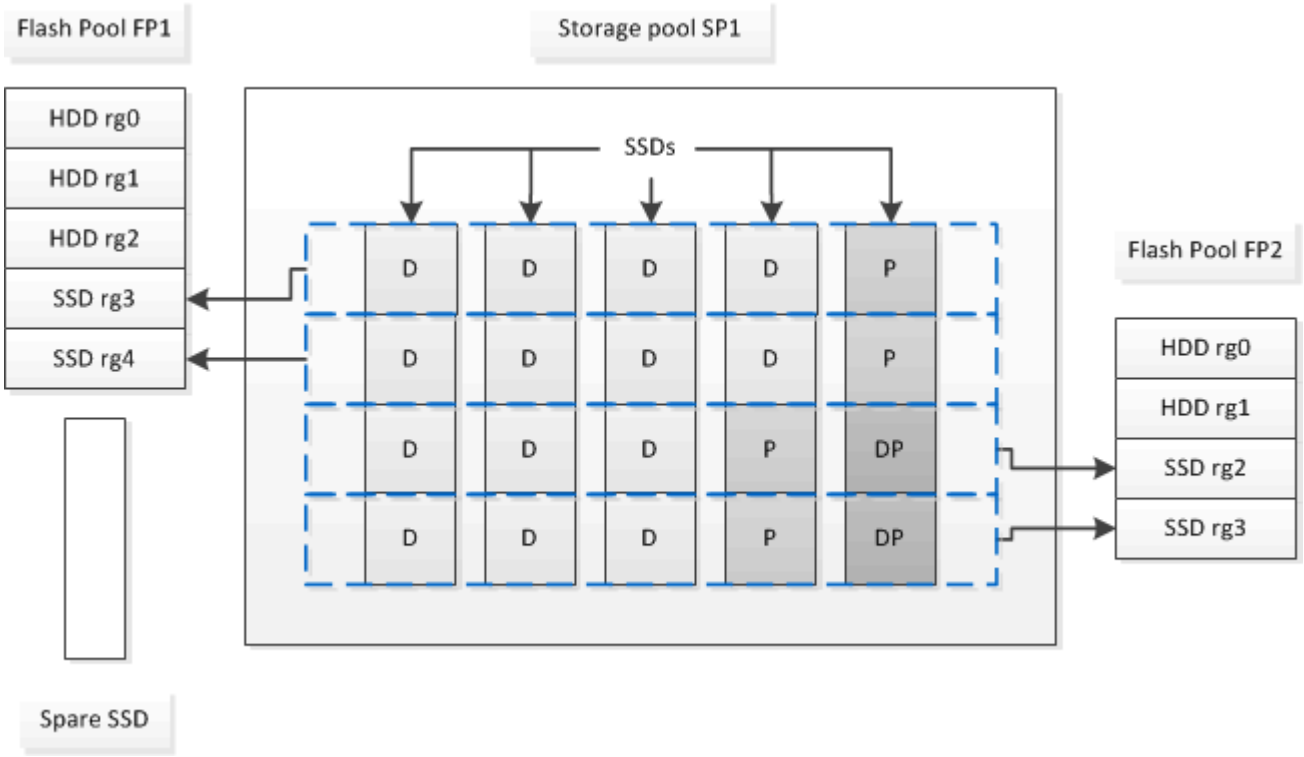
Affinché un SSD possa essere utilizzato in un Tier locale di Flash Pool, l'SSD deve essere collocato in un pool di storage. Non è possibile utilizzare SSD partizionati per la partizione dei dati root in un pool di storage. Una volta inserito l'SSD nel pool di storage, l'SSD non può più essere gestito come disco standalone e non può essere rimosso dal pool di storage a meno che non si distruggano i Tier locali associati a Flash Pool e si distrugga il pool di storage.

I pool di storage SSD sono suddivisi in quattro unità di allocazione uguali. Gli SSD aggiunti al pool di storage sono suddivisi in quattro partizioni e una partizione viene assegnata a ciascuna delle quattro unità di allocazione. Gli SSD nel pool di storage devono essere di proprietà della stessa coppia ha. Per impostazione predefinita, a ciascun nodo della coppia ha vengono assegnate due unità di allocazione. Le unità di allocazione devono essere di proprietà del nodo proprietario del Tier locale che sta servendo. Se per i Tier locali su uno dei nodi è necessaria una maggiore cache Flash, è possibile spostare il numero predefinito di unità di allocazione per diminuire il numero su un nodo e aumentare il numero sul nodo partner.

Si utilizzano SSD di riserva per aggiungerli a un pool di storage SSD. Se il pool di storage fornisce unità di allocazione ai Tier locali di Flash Pool di proprietà di entrambi i nodi della coppia ha, allora gli SSD spare

possono essere di proprietà di entrambi i nodi. Tuttavia, se il pool di storage fornisce unità di allocazione solo ai Tier locali di Flash Pool di proprietà di uno dei nodi della coppia ha, le unità di riserva SSD devono essere di proprietà dello stesso nodo.

La figura seguente mostra un esempio di partizione SSD Flash Pool. Il pool di storage SSD fornisce cache a due livelli locali di Flash Pool:




Lo Storage Pool SP1 è composto da cinque SSD e un SSD hot spare. Due delle unità di allocazione del pool di storage vengono allocate a Flash Pool FP1 e due a Flash Pool FP2. FP1 ha un tipo RAID cache di RAID4. Pertanto, le unità di allocazione fornite a FP1 contengono una sola partizione designata per la parità. FP2 ha un tipo di RAID-DP per la cache. Pertanto, le unità di allocazione fornite a FP2 includono una partizione di parità e una partizione di doppia parità.

In questo esempio, due unità di allocazione vengono allocate a ciascun Tier locale di Flash Pool. Tuttavia, se un livello locale di Flash Pool richiedeva una cache più grande, è possibile allocare tre unità di allocazione a quel livello locale di Flash Pool e una sola all'altra.

### Determinare la candidatura di Flash Pool e le dimensioni ottimali della cache

Prima di convertire un Tier locale (aggregato) esistente in un Tier locale di Flash Pool, è possibile determinare se il Tier locale è associato all'i/o e le migliori dimensioni della cache di Flash Pool per il carico di lavoro e il budget. È inoltre possibile controllare se la cache di un Tier locale di Flash Pool esistente è dimensionata correttamente.

#### Di cosa hai bisogno

Dovresti sapere approssimativamente quando il Tier locale che stai analizzando sperimenta il suo carico di picco.

#### Fasi

1. Accedere alla modalità avanzata:

```
set advanced
```

2. Se è necessario determinare se un Tier locale (aggregato) esistente sia un buon candidato per la conversione in un aggregato di Flash Pool, determinare la disponibilità dei dischi nell'aggregato durante un periodo di carico di picco e in che modo ciò influisce sulla latenza:

   ```
   statistics show-periodic -object disk:raid_group -instance raid_group_name
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

   Puoi decidere se ridurre la latenza aggiungendo la cache di Flash Pool è utile per questo aggregato.

   Il comando seguente mostra le statistiche per il primo gruppo RAID dell'aggregato "aggr1":

   ```
   statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

3. Avviare Automated workload Analyzer (AWA):

   ```
   storage automated-working-set-analyzer start -node node_name -aggregate
   aggr_name
   ```

   AWA inizia a raccogliere i dati del carico di lavoro per i volumi associati all'aggregato specificato.

4. Uscire dalla modalità avanzata:

   ```
   set admin
   ```

   Consentire l'esecuzione di AWA fino a quando non si sono verificati uno o più intervalli di carico di picco. AWA raccoglie le statistiche dei carichi di lavoro per i volumi associati all'aggregato specificato e analizza i dati per una durata massima di una settimana. L'esecuzione di AWA per più di una settimana riporta solo i dati raccolti dalla settimana più recente. Le stime delle dimensioni della cache si basano sui carichi più elevati rilevati durante il periodo di raccolta dei dati; non è necessario che il carico sia elevato per l'intero periodo di raccolta dei dati.

5. Accedere alla modalità avanzata:

   ```
   set advanced
   ```

6. Visualizzare l'analisi del carico di lavoro:

   ```
   storage automated-working-set-analyzer show -node node_name -instance
   ```

7. Arrestare AWA:

   ```
   storage automated-working-set-analyzer stop node_name
   ```

   Tutti i dati dei workload vengono eliminati e non sono più disponibili per l'analisi.

8. Uscire dalla modalità avanzata:

   ```
   set admin
   ```

### Creare un Tier locale (aggregato) di Flash Pool utilizzando SSD fisici

È possibile creare un Tier locale (aggregato) di Flash Pool abilitando la funzionalità su un Tier locale esistente composto da gruppi RAID HDD e aggiungendo uno o più gruppi RAID SSD a tale Tier locale. Ciò comporta due set di gruppi RAID per quel livello locale: Gruppi RAID SSD (la cache SSD) e gruppi RAID HDD.

#### A proposito di questa attività

Dopo aver aggiunto una cache SSD a un Tier locale per creare un Tier locale di Flash Pool, non è possibile rimuovere la cache SSD per convertire di nuovo il Tier locale nella configurazione originale.

Per impostazione predefinita, il livello RAID della cache SSD è lo stesso del livello RAID dei gruppi RAID HDD. È possibile ignorare questa selezione predefinita specificando l'opzione "raidtype" quando si aggiungono i primi gruppi RAID SSD.

#### Prima di iniziare

- È necessario aver identificato un Tier locale valido composto da HDD per la conversione in un Tier locale di Flash Pool.
- È necessario aver determinato l'idoneità del caching in scrittura dei volumi associati al Tier locale e aver completato tutte le procedure necessarie per risolvere i problemi di idoneità.
- È necessario aver determinato gli SSD da aggiungere e questi SSD devono essere di proprietà del nodo su cui si sta creando il Tier locale di Flash Pool.
- È necessario aver determinato i tipi di checksum sia degli SSD che si stanno aggiungendo che degli HDD già nel Tier locale.
- È necessario determinare il numero di SSD da aggiungere e la dimensione ottimale del gruppo RAID per i gruppi RAID SSD.

  L'utilizzo di un numero inferiore di gruppi RAID nella cache SSD riduce il numero di dischi di parità richiesti, ma i gruppi RAID più grandi richiedono RAID-DP.

- È necessario determinare il livello RAID che si desidera utilizzare per la cache SSD.
- È necessario determinare le dimensioni massime della cache per il sistema e determinare che l'aggiunta della cache SSD al Tier locale non causerà il superamento di tale dimensione.
- È necessario aver acquisito dimestichezza con i requisiti di configurazione per i Tier locali di Flash Pool.

#### Fasi

Puoi creare un aggregato di FlashPool utilizzando System Manager o l'interfaccia a riga di comando di ONTAP.

**System Manager**

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per creare un Tier locale di Flash Pool utilizzando SSD fisici.

**Fasi**

1. Selezionare **Storage > Tiers**, quindi selezionare un livello di archiviazione HDD locale esistente.
2. Selezionare ⋮ Quindi **Aggiungi Flash Pool cache**.
3. Selezionare **Usa SSD dedicati come cache**.
4. Selezionare un tipo di disco e il numero di dischi.
5. Scegliere un tipo di RAID.
6. Selezionare **Salva**.
7. Individuare il Tier di storage e selezionare ⋮.
8. Selezionare **altri dettagli**. Verificare che Flash Pool sia **abilitato**.

**CLI**

**Fasi**

1. Contrassegna il Tier locale (aggregato) come idoneo per diventare un aggregato di Flash Pool:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   Se questo passaggio non riesce, determinare l'idoneità del caching in scrittura per l'aggregato di destinazione.

2. Aggiungere gli SSD all'aggregato utilizzando `storage aggregate add` comando.
   - È possibile specificare gli SSD in base all'ID o utilizzando `diskcount` e. `disktype` parametri.
   - Se gli HDD e gli SSD non hanno lo stesso tipo di checksum o se l'aggregato è un aggregato di checksum misto, è necessario utilizzare `checksumstyle` parametro per specificare il tipo di checksum dei dischi da aggiungere all'aggregato.
   - È possibile specificare un tipo RAID diverso per la cache SSD utilizzando `raidtype` parametro.
   - Se si desidera che la dimensione del gruppo RAID della cache sia diversa da quella predefinita per il tipo RAID in uso, è necessario modificarla ora utilizzando `-cache-raid-group-size` parametro.

### Creare un Tier locale Flash Pool (aggregato) utilizzando i pool di storage SSD

#### Panoramica sulla creazione di un Tier locale (aggregato) di Flash Pool utilizzando i pool di storage SSD

È possibile eseguire varie procedure per creare un Tier locale (aggregato) di Flash Pool utilizzando i pool di storage SSD:

- **Preparazione**
  - "Determinare se un Tier locale (aggregato) di Flash Pool utilizza un pool di storage SSD"
- **Creazione del pool di storage SSD**
  - "Creare un pool di storage SSD"

- "Aggiungi SSD a un pool di storage SSD"

- **Creazione di Flash Pool con pool di storage SSD**
  - "Creare un Tier locale Flash Pool (aggregato) utilizzando le unità di allocazione del pool di storage SSD"
  - "Determinare l'impatto delle dimensioni della cache dell'aggiunta di SSD a un pool di storage SSD"

#### Determinare se un Tier locale (aggregato) di Flash Pool utilizza un pool di storage SSD

## È possibile configurare un aggregato Flash Pool (Tier locale) aggiungendo una o più unità di allocazione da un pool di storage SSD a un Tier locale HDD esistente.

I Tier locali di Flash Pool vengono gestiti in modo diverso quando utilizzano pool di storage SSD per fornire la cache rispetto a quando utilizzano SSD discreti.

**Fase**

1. Visualizzare i dischi dell'aggregato in base al gruppo RAID:

   `storage aggregate show-status` *`aggr_name`*

   Se l'aggregato utilizza uno o più pool di storage SSD, il valore per `Position` La colonna per i gruppi RAID SSD viene visualizzata come `Shared`E il nome del pool di storage viene visualizzato accanto al nome del gruppo RAID.

#### Aggiungere cache a un Tier locale (aggregato) creando un pool di storage SSD

## È possibile eseguire il provisioning della cache convertendo un Tier locale (aggregato) esistente in un Tier locale (aggregato) Flash Pool aggiungendo unità a stato solido (SSD).

È possibile creare pool di storage con unità a stato solido (SSD) per fornire cache SSD per due o quattro Tier locali di Flash Pool (aggregati). Gli aggregati di Flash Pool consentono di implementare la flash come cache dalle performance elevate per il set di dati di lavoro, utilizzando al contempo HDD a basso costo per i dati ad accesso meno frequente.

**A proposito di questa attività**

- Quando si creano o si aggiungono dischi a un pool di storage, è necessario fornire un elenco di dischi.

  I pool di storage non supportano un `diskcount` parametro.

- Gli SSD utilizzati nel pool di storage devono avere le stesse dimensioni.

**System Manager**

**Utilizzare Gestione sistema per aggiungere una cache SSD (ONTAP 9.12.1 e versioni successive)**

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per aggiungere una cache SSD.

> Le opzioni del pool di storage non sono disponibili sui sistemi AFF.

**Fasi**

1. Fare clic su **Cluster > Disks**, quindi su **Show/Hide** (Mostra/Nascondi).
2. Selezionare **Type** (tipo) e verificare che sul cluster siano presenti SSD di riserva.
3. Fare clic su **Storage > Tier** e fare clic su **Add Storage Pool**.
4. Selezionare il tipo di disco.
5. Inserire una dimensione del disco.
6. Selezionare il numero di dischi da aggiungere al pool di storage.
7. Esaminare le dimensioni stimate della cache.

**Utilizzare Gestione sistema per aggiungere una cache SSD (solo ONTAP 9.7)**

> Utilizzare la procedura CLI se si utilizza una versione di ONTAP successiva a ONTAP 9.7 o precedente a ONTAP 9.12.1.

**Fasi**

1. Fare clic su **(Torna alla versione classica)**.
2. Fare clic su **Storage > Aggregates & Disks > Aggregates**.
3. Selezionare il Tier locale (aggregato), quindi fare clic su **Actions > Add cache** (azioni > Aggiungi cache).
4. Selezionare l'origine della cache come "pool di storage" o "SSD dedicati".
5. Fare clic su **(passa alla nuova esperienza)**.
6. Fare clic su **Storage > Tier** per verificare le dimensioni del nuovo aggregato.

**CLI**

**Utilizzare la CLI per creare un pool di storage SSD**

**Fasi**

1. Determinare i nomi degli SSD spare disponibili:

   ```
   storage aggregate show-spare-disks -disk-type SSD
   ```

   Gli SSD utilizzati in un pool di storage possono essere di proprietà di entrambi i nodi di una coppia ha.

2. Creare il pool di storage:

   ```
   storage pool create -storage-pool sp_name -disk-list disk1,disk2,…
   ```

3. **Opzionale:** verificare il pool di storage appena creato:

   ```
   storage pool show -storage-pool sp_name
   ```

**Risultati**

Una volta inseriti nel pool di storage, gli SSD non vengono più visualizzati come parti di ricambio nel cluster, anche se lo storage fornito dal pool di storage non è ancora stato allocato alle cache di Flash Pool. Non è possibile aggiungere SSD a un gruppo RAID come dischi discreti; il relativo storage può essere fornito solo utilizzando le unità di allocazione del pool di storage a cui appartengono.

#### Creare un Tier locale Flash Pool (aggregato) utilizzando le unità di allocazione del pool di storage SSD

## È possibile configurare un Tier locale (aggregato) di Flash Pool aggiungendo una o più unità di allocazione da un pool di storage SSD a un Tier locale HDD esistente.

A partire da ONTAP 9.12.1, è possibile utilizzare il nuovo Gestore di sistema per creare un Tier locale di Flash Pool utilizzando le unità di allocazione del pool di storage.

**Di cosa hai bisogno**

- È necessario aver identificato un Tier locale valido composto da HDD per la conversione in un Tier locale di Flash Pool.
- È necessario aver determinato l'idoneità del caching in scrittura dei volumi associati al Tier locale e aver completato tutte le procedure necessarie per risolvere i problemi di idoneità.
- È necessario aver creato un pool di storage SSD per fornire la cache SSD a questo Tier locale di Flash Pool.

  Tutte le unità di allocazione del pool di storage che si desidera utilizzare devono essere di proprietà dello stesso nodo proprietario del Tier locale di Flash Pool.

- È necessario determinare la quantità di cache che si desidera aggiungere al Tier locale.

  La cache viene aggiunta al Tier locale in base alle unità di allocazione. È possibile aumentare le dimensioni delle unità di allocazione in un secondo momento aggiungendo SSD al pool di storage se c'è spazio.

- È necessario determinare il tipo di RAID che si desidera utilizzare per la cache SSD.

  Dopo aver aggiunto una cache al Tier locale dai pool di storage SSD, non è possibile modificare il tipo RAID dei gruppi RAID della cache.

- È necessario determinare le dimensioni massime della cache per il sistema e determinare che l'aggiunta della cache SSD al Tier locale non causerà il superamento di tale dimensione.

  È possibile visualizzare la quantità di cache che verrà aggiunta alle dimensioni totali della cache utilizzando `storage pool show` comando.

- È necessario aver acquisito dimestichezza con i requisiti di configurazione del Tier locale di Flash Pool.

**A proposito di questa attività**

Se si desidera che il tipo RAID della cache sia diverso da quello dei gruppi RAID HDD, è necessario specificare il tipo di cache RAID quando si aggiunge la capacità SSD. Dopo aver aggiunto la capacità SSD al Tier locale, non è più possibile modificare il tipo RAID della cache.

Dopo aver aggiunto una cache SSD a un Tier locale per creare un Tier locale di Flash Pool, non è possibile rimuovere la cache SSD per convertire di nuovo il Tier locale nella configurazione originale.

**System Manager**

A partire da ONTAP 9.12.1, puoi utilizzare Gestione sistema per aggiungere SSD a un pool di storage SSD.

**Fasi**

1. Fare clic su **Storage > Tier** e selezionare un Tier di storage HDD locale esistente.
2. Fare clic su ⋮ E selezionare **Add Flash Pool cache**.
3. Selezionare **Usa pool di storage**.
4. Selezionare un pool di storage.
5. Selezionare una dimensione della cache e una configurazione RAID.
6. Fare clic su **Save** (Salva).
7. Individuare nuovamente il Tier di storage e fare clic su ⋮.
8. Selezionare **More Details** (ulteriori dettagli) e verificare che Flash Pool sia visualizzato come **Enabled** (attivato).

**CLI**

**Fasi**

1. Contrassegna l'aggregato come idoneo per diventare un aggregato di Flash Pool:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   Se questo passaggio non riesce, determinare l'idoneità del caching in scrittura per l'aggregato di destinazione.

2. Mostrare le unità di allocazione del pool di storage SSD disponibili:

   ```
   storage pool show-available-capacity
   ```

3. Aggiungere la capacità SSD all'aggregato:

   ```
   storage aggregate add aggr_name -storage-pool sp_name -allocation-units
   number_of_units
   ```

   Se si desidera che il tipo RAID della cache sia diverso da quello dei gruppi RAID HDD, è necessario modificarlo quando si inserisce questo comando utilizzando `raidtype` parametro.

   Non è necessario specificare un nuovo gruppo RAID; ONTAP inserisce automaticamente la cache SSD in gruppi RAID separati dai gruppi RAID HDD.

   Non è possibile impostare la dimensione del gruppo RAID della cache, in quanto è determinata dal numero di SSD nel pool di storage.

   La cache viene aggiunta all'aggregato e l'aggregato è ora un aggregato di Flash Pool. Ogni unità di allocazione aggiunta all'aggregato diventa il proprio gruppo RAID.

4. Verificare la presenza e le dimensioni della cache SSD:

   ```
   storage aggregate show aggregate_name
   ```

Le dimensioni della cache sono elencate in `Total Hybrid Cache Size`.

**Informazioni correlate**

"Report tecnico di NetApp 4070: Guida alla progettazione e all'implementazione di Flash Pool"

#### Determinare l'impatto delle dimensioni della cache dell'aggiunta di SSD a un pool di storage SSD

Se l'aggiunta di SSD a un pool di storage causa il superamento del limite di cache del modello di piattaforma, ONTAP non assegna la capacità aggiunta di recente a alcun Tier locale di Flash Pool (aggregati). In questo modo, alcune o tutte le nuove capacità aggiunte potrebbero non essere disponibili per l'utilizzo.

**A proposito di questa attività**

Quando si aggiungono SSD a un pool di storage SSD con unità di allocazione già allocate ai Tier locali (aggregati) di Flash Pool, si aumentano le dimensioni della cache di ciascuno di questi Tier locali e la cache totale sul sistema. Se nessuna delle unità di allocazione del pool di storage è stata allocata, l'aggiunta di SSD a tale pool di storage non influisce sulle dimensioni della cache SSD fino a quando una o più unità di allocazione non vengono allocate in una cache.

**Fasi**

1. Determinare le dimensioni utilizzabili degli SSD che si stanno aggiungendo al pool di storage:

   ```
   storage disk show disk_name -fields usable-size
   ```

2. Determinare quante unità di allocazione rimangono non allocate per il pool di storage:

   ```
   storage pool show-available-capacity sp_name
   ```

   Vengono visualizzate tutte le unità di allocazione non allocate nel pool di storage.

3. Calcolare la quantità di cache che verrà aggiunta applicando la seguente formula:

   (4 — numero di unità di allocazione non allocate) × 25% × dimensione utilizzabile × numero di SSD

#### Aggiungi SSD a un pool di storage SSD

Quando si aggiungono dischi a stato solido (SSD) a un pool di storage SSD, si aumentano le dimensioni fisiche e utilizzabili del pool di storage e le dimensioni dell'unità di allocazione. La dimensione dell'unità di allocazione maggiore influisce anche sulle unità di allocazione che sono già state allocate ai Tier locali (aggregati).

**Di cosa hai bisogno**

È necessario determinare che questa operazione non causerà il superamento del limite di cache per la coppia ha. ONTAP non impedisce di superare il limite di cache quando si aggiungono SSD a un pool di storage SSD, rendendo la capacità di storage aggiunta di recente non disponibile per l'utilizzo.

**A proposito di questa attività**

Quando si aggiungono SSD a un pool di storage SSD esistente, gli SSD devono essere di proprietà di un nodo o dell'altro della stessa coppia ha che possedeva già gli SSD esistenti nel pool di storage. È possibile aggiungere SSD di proprietà di entrambi i nodi della coppia ha.

L'SSD aggiunto al pool di storage deve avere le stesse dimensioni del disco attualmente utilizzato nel pool di storage.

**System Manager**

A partire da ONTAP 9.12.1, puoi utilizzare Gestione sistema per aggiungere SSD a un pool di storage SSD.

**Fasi**

1. Fare clic su **Storage > Tier** e individuare la sezione **Storage Pools**.
2. Individuare il pool di storage, fare clic su ⋮ E selezionare **Aggiungi dischi**.
3. Scegliere il tipo di disco e selezionare il numero di dischi.
4. Esaminare la dimensione stimata della cache.

**CLI**

**Fasi**

1. **Opzionale:** Visualizza le dimensioni correnti dell'unità di allocazione e lo storage disponibile per il pool di storage:

   ```
   storage pool show -instance sp_name
   ```

2. Trova gli SSD disponibili:

   ```
   storage disk show -container-type spare -type SSD
   ```

3. Aggiungere gli SSD al pool di storage:

   ```
   storage pool add -storage-pool sp_name -disk-list disk1,disk2…
   ```

   Il sistema visualizza le dimensioni degli aggregati di Flash Pool aumentate in base a questa operazione e alla quantità di dati e richiede di confermare l'operazione.

#### Comandi per la gestione dei pool di storage SSD

### ONTAP offre `storage pool` Comando per la gestione dei pool di storage SSD.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Visualizzare la quantità di storage che un pool di storage fornisce a quali aggregati | `storage pool show-aggregate` |
| Visualizza la quantità di cache che verrà aggiunta alla capacità cache complessiva per entrambi i tipi RAID (dimensione dei dati dell'unità di allocazione) | `storage pool show -instance` |
| Visualizzare i dischi in un pool di storage | `storage pool show-disks` |

| | |
|---|---|
| Visualizzare le unità di allocazione non allocate per un pool di storage | `storage pool show-available-capacity` |
| Modificare la proprietà di una o più unità di allocazione di un pool di storage da un partner ha all'altro | `storage pool reassign` |

**Informazioni correlate**

"Comandi di ONTAP 9"

# Gestione dei livelli FabricPool

## Panoramica sulla gestione dei Tier FabricPool

È possibile utilizzare FabricPool per tierare automaticamente i dati in base alla frequenza di accesso.

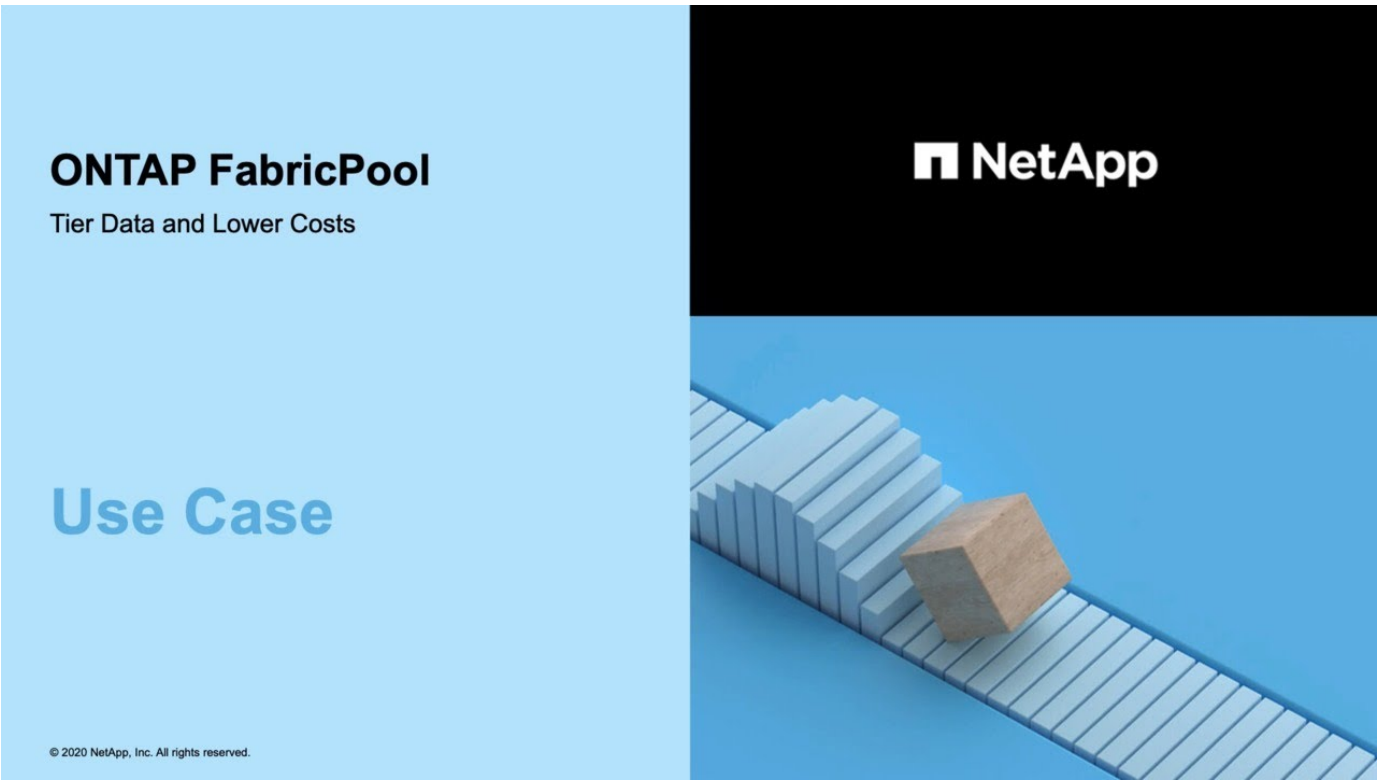
FabricPool è una soluzione di storage ibrido che utilizza un aggregato all flash (all SSD) come Tier di performance e un archivio di oggetti come Tier di cloud. L'utilizzo di un FabricPool consente di ridurre i costi dello storage senza compromettere le performance, l'efficienza o la protezione.

Il livello cloud può essere localizzato su NetApp StorageGRID o ONTAP S3 (a partire da ONTAP 9.8) o su uno dei seguenti service provider:

- Cloud di Alibaba
- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- Cloud IBM
- Storage Blob Microsoft Azure

A partire da ONTAP 9,7, è possibile utilizzare altri provider di archivi di oggetti che supportano API S3 generiche selezionando il provider di archivi di oggetti S3_Compatible.

**Video sul caso di utilizzo di dati Tier e costi inferiori**




**Informazioni correlate**

Vedere anche la "Tiering cloud di NetApp" documentazione.

## Vantaggi dei Tier di storage grazie a FabricPool

La configurazione di un aggregato per l'utilizzo di FabricPool consente di utilizzare i Tier di storage. Puoi bilanciare in modo efficiente le performance e i costi del tuo sistema storage, monitorare e ottimizzare l'utilizzo dello spazio ed eseguire lo spostamento dei dati basato su policy tra i Tier di storage.

- È possibile ottimizzare le performance dello storage e ridurre i costi dello storage memorizzando i dati in un Tier in base alla frequenza di accesso ai dati.
  - I dati ad accesso frequente ("hot") vengono memorizzati nel *Tier di performance*.

    Il Tier di performance utilizza uno storage primario dalle performance elevate, come un aggregato all flash (all SSD) del sistema storage.

  - I dati ad accesso non frequente ("cold") vengono memorizzati nel *Tier cloud*, noto anche come *Tier di capacità*.

    Il Tier cloud utilizza un archivio di oggetti meno costoso e che non richiede performance elevate.

- Hai la flessibilità di specificare il Tier in cui archiviare i dati.

  È possibile specificare una delle opzioni dei criteri di tiering supportate a livello di volume. Le opzioni consentono di spostare in modo efficiente i dati tra i vari Tier man mano che i dati diventano caldi o freddi.

  "Tipi di policy di tiering FabricPool"

- Puoi scegliere uno degli archivi di oggetti supportati da utilizzare come Tier cloud per FabricPool.
- È possibile monitorare l'utilizzo dello spazio in un aggregato abilitato a FabricPool.
- È possibile visualizzare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi.
- È possibile ridurre l'impatto on-premise del sistema storage.

  È possibile risparmiare spazio fisico quando si utilizza un archivio di oggetti basato sul cloud per il Tier cloud.

## Considerazioni e requisiti per l'utilizzo di FabricPool

È necessario acquisire familiarità con alcune considerazioni e requisiti relativi all'utilizzo di FabricPool.

### Considerazioni e requisiti generali

- Per utilizzare FabricPool, è necessario che ONTAP 9.2 sia in esecuzione almeno.
- È necessario eseguire ONTAP 9.4 o versioni successive per le seguenti funzionalità di FabricPool:
  - Il `auto` "policy di tiering"
  - Specifica del periodo di raffreddamento minimo di tiering
  - Report dei dati inattivi (IDR)
  - Utilizzo dello storage blob Microsoft Azure per il cloud come Tier cloud per FabricPool
  - Utilizzo di FabricPool con ONTAP Select
- È necessario eseguire ONTAP 9.5 o versioni successive per le seguenti funzionalità di FabricPool:
  - Specifica della soglia di tiering fullness
  - Utilizzo dello storage a oggetti cloud IBM come Tier cloud per FabricPool
  - NetApp Volume Encryption (NVE) del livello cloud, attivato per impostazione predefinita.
- È necessario eseguire ONTAP 9.6 o versioni successive per le seguenti funzionalità di FabricPool:
  - Il `all` policy di tiering
  - Report dei dati inattivi attivati manualmente sugli aggregati HDD
  - Report dei dati inattivi attivati automaticamente per gli aggregati SSD quando si esegue l'aggiornamento a ONTAP 9.6 e al momento della creazione dell'aggregato, ad eccezione dei sistemi di fascia bassa con meno di 4 CPU, meno di 6 GB di RAM o quando la dimensione della cache del buffer WAFL è inferiore a 3 GB.

    ONTAP monitora il carico del sistema e, se il carico rimane elevato per 4 minuti continui, l'IDR viene disattivato e non viene attivato automaticamente. È possibile riabilitare l'IDR manualmente, tuttavia l'IDR abilitato manualmente non viene disattivato automaticamente.
  - Utilizzo dello storage a oggetti cloud di Alibaba come livello cloud per FabricPool
  - Utilizzo della piattaforma cloud di Google come Tier cloud per FabricPool
  - Spostamento del volume senza copia dei dati del Tier cloud
- È necessario eseguire ONTAP 9.7 o versioni successive per le seguenti funzionalità di FabricPool:
  - Proxy HTTP e HTTPS non trasparente per fornire l'accesso solo ai punti di accesso whitelist e per

fornire funzionalità di auditing e reporting.

- Mirroring FabricPool per il tiering dei dati cold in due archivi di oggetti contemporaneamente
- Mirroring di FabricPool sulle configurazioni MetroCluster
- Dump e ripristino NDMP attivati per impostazione predefinita negli aggregati FabricPool Attached.

> Se l'applicazione di backup utilizza un protocollo diverso da NDMP, come NFS o SMB, tutti i dati di cui viene eseguito il backup nel Tier di performance diventano hot e possono influire sul tiering di tali dati nel Tier cloud. Le letture non NDMP possono causare la migrazione dei dati dal livello cloud al livello di performance.

"Supporto backup e ripristino NDMP per FabricPool"

- È necessario eseguire ONTAP 9.8 o versione successiva per le seguenti funzionalità di FabricPool:
  - Controllo della migrazione nel cloud per consentire l'override della policy di tiering predefinita
  - Promozione dei dati al Tier di performance
  - FabricPool con SnapLock Enterprise. FabricPool con SnapLock Enterprise richiede una richiesta di variazione del prodotto (FPVR). Per creare un FPVR, contatta il tuo team di vendita.
  - Periodo minimo di raffreddamento massimo di 183 giorni
  - Tagging degli oggetti mediante tag personalizzati creati dall'utente
  - FabricPools su piattaforme HDD e aggregati

    I dischi HDD FabricPool sono supportati con dischi SAS, FSAS, BSAS e MSATA solo su sistemi con 6 o più core CPU, inclusi i seguenti modelli:

    - FAS9000
    - FAS8700
    - FAS8300
    - FAS8200
    - FAS8080
    - FAS8060
    - FAS8040
    - FAS2750
    - FAS2720
    - FAS2650
    - FAS2620

      Controllare "Hardware Universe" per i modelli più recenti supportati.

- FabricPool è supportato su tutte le piattaforme in grado di eseguire ONTAP 9.2, ad eccezione di:
  - FAS8020
  - FAS2554
  - FAS2552
  - FAS2520

- FabricPool supporta i seguenti tipi di aggregato:
  - Sui sistemi AFF, è possibile utilizzare solo tutti gli aggregati flash (tutti gli SSD) per FabricPool.
  - Sui sistemi FAS, è possibile utilizzare aggregati all-flash (all-SSD) o HDD per FabricPool.

    Non è possibile utilizzare gli aggregati di Flash Pool, che contengono sia SSD che HDD.
  - Su Cloud Volumes ONTAP e ONTAP Select, è possibile utilizzare aggregati SSD o HDD per FabricPool.

    Tuttavia, si consiglia di utilizzare aggregati SSD.
- FabricPool supporta l'utilizzo dei seguenti archivi di oggetti come livello cloud:
  - NetApp StorageGRID 10.3 o versione successiva
  - NetApp ONTAP S3 (ONTAP 9.8 e versioni successive)
  - Alibaba Cloud Object Storage
  - Amazon Web Services Simple Storage Service (AWS S3)
  - Storage Google Cloud
  - Storage a oggetti IBM Cloud
  - Microsoft Azure Blob Storage per il cloud
- L'archivio di oggetti "bucket" (container) che intendi utilizzare deve essere già stato configurato, avere almeno 10 GB di spazio di storage e non deve essere rinominato.
- Le coppie HA che utilizzano FabricPool richiedono le LIF intercluster per comunicare con l'archivio di oggetti.
- Non è possibile scollegare un Tier cloud da un Tier locale dopo il collegamento; tuttavia, è possibile utilizzarlo "Specchio FabricPool" per collegare un tier locale a un tier cloud diverso.
- Se si utilizza il throughput floors (QoS min), la policy di tiering sui volumi deve essere impostata su `none` Prima che l'aggregato possa essere collegato a FabricPool.

  Altri criteri di tiering impediscono l'associazione dell'aggregato a FabricPool. Una policy di QoS non applicherà i piani di throughput quando FabricPool è attivato.
- Seguire le linee guida delle Best practice per l'utilizzo di FabricPool in scenari specifici.

  "Report tecnico di NetApp 4598: Best Practice FabricPool in ONTAP 9"

### Considerazioni aggiuntive sull'utilizzo di Cloud Volumes ONTAP

Cloud Volumes ONTAP non richiede una licenza FabricPool, indipendentemente dal provider dell'archivio di oggetti in uso.

### Considerazioni aggiuntive per il tiering dei dati a cui accedono i protocolli SAN

Quando si esegue il tiering dei dati a cui accedono i protocolli SAN, NetApp consiglia di utilizzare cloud privati, come StorageGRID, a causa di considerazioni sulla connettività.

**Importante**

Quando si utilizza FabricPool in un ambiente SAN con un host Windows, se lo storage a oggetti non è più disponibile per un periodo di tempo prolungato durante il tiering dei dati nel cloud, i file sul LUN NetApp

sull'host Windows potrebbero diventare inaccessibili o scomparire. Consultare l'articolo della Knowledge base "Durante l'archiviazione di oggetti FabricPool S3 non disponibile, l'host SAN di Windows ha segnalato un danneggiamento del file system".

#### Funzionalità o funzionalità non supportate da FabricPool

- Archivi di oggetti con WORM abilitato e versione degli oggetti abilitata.
- Policy ILM (Information Lifecycle Management) applicate ai bucket degli archivi di oggetti

  FabricPool supporta le policy di gestione del ciclo di vita delle informazioni di StorageGRID solo per la replica dei dati e l'erasure coding per proteggere i dati del Tier cloud dai guasti. Tuttavia, FabricPool *non* supporta le regole ILM avanzate, come il filtraggio basato su tag o metadati dell'utente. ILM include in genere varie policy di spostamento ed eliminazione. Queste policy possono interrompere i dati nel livello cloud di FabricPool. L'utilizzo di FabricPool con policy ILM configurate sugli archivi di oggetti può causare la perdita di dati.

- Transizione dei dati in 7 modalità utilizzando i comandi CLI di ONTAP o lo strumento di transizione in 7 modalità
- Virtualizzazione FlexArray
- RAID SyncMirror, tranne in una configurazione MetroCluster
- Volumi SnapLock quando si utilizza ONTAP 9.7 e versioni precedenti
- Backup su nastro con SMTape per aggregati abilitati FabricPool
- La funzionalità di bilanciamento automatico
- Volumi che utilizzano una garanzia di spazio diversa da `none`

  Ad eccezione dei volumi SVM root e dei volumi di staging dell'audit CIFS, FabricPool non supporta l'associazione di un Tier cloud a un aggregato che contiene volumi che utilizzano una garanzia di spazio diversa da `none`. Ad esempio, un volume che utilizza una garanzia di spazio di `volume` (`-space -guarantee volume`) non è supportato.

- Cluster con "Licenza DP_Optimized"
- Aggregati di Flash Pool

## Informazioni sulle policy di tiering FabricPool

Le policy di tiering di FabricPool ti consentono di spostare i dati in modo efficiente tra i vari livelli quando i dati diventano caldi o freddi. La comprensione delle policy di tiering ti aiuta a scegliere la policy più adatta alle tue esigenze di gestione dello storage.

#### Tipi di policy di tiering FabricPool

Le policy di tiering FabricPool determinano quando o se i blocchi di dati utente di un volume in FabricPool vengono spostati nel Tier cloud, in base al volume "temperature" di hot (attivo) o cold (inattivo). Il volume "temperature" aumenta quando si accede frequentemente e diminuisce quando non lo è. Alcune policy di tiering prevedono un periodo di raffreddamento minimo di tiering, che imposta il tempo in cui i dati utente in un volume di FabricPool devono rimanere inattivi affinché i dati vengano considerati "cold" e spostati al livello cloud.

Dopo che un blocco è stato identificato come cold, viene contrassegnato come idoneo per essere tiered. Una scansione giornaliera di tiering in background cerca i blocchi freddi. Una volta raccolti un numero sufficiente di

blocchi da 4 KB dallo stesso volume, questi vengono concatenati in un oggetto da 4 MB e spostati nel Tier cloud in base alla policy di tiering del volume.

> Dati nei volumi utilizzando `all` la policy di tiering viene immediatamente contrassegnata come cold e inizia il tiering al livello cloud il prima possibile. Non è necessario attendere l'esecuzione della scansione di tiering giornaliera.

È possibile utilizzare `volume object-store tiering show` Per visualizzare lo stato di tiering di un volume FabricPool. Per ulteriori informazioni, consultare "Riferimento comando".

Il criterio di tiering FabricPool viene specificato a livello di volume. Sono disponibili quattro opzioni:

- Il `snapshot-only` La policy di tiering (impostazione predefinita) sposta i blocchi di dati utente delle copie Snapshot del volume non associate al file system attivo nel Tier cloud.

  Il periodo di raffreddamento minimo per il tiering è di 2 giorni. È possibile modificare l'impostazione predefinita per il periodo di raffreddamento minimo di tiering con `-tiering-minimum-cooling-days` nel livello di privilegio avanzato di `volume create` e. `volume modify` comandi. I valori validi vanno da 2 a 183 giorni utilizzando ONTAP 9.8 e versioni successive. Se si utilizza una versione di ONTAP precedente alla 9.8, i valori validi sono compresi tra 2 e 63 giorni.

- Il `auto` La policy di tiering, supportata solo su ONTAP 9.4 e versioni successive, sposta i blocchi di dati utente cold nelle copie Snapshot e nel file system attivo nel Tier cloud.

  Il periodo di raffreddamento minimo di tiering predefinito è di 31 giorni e si applica all'intero volume, sia per il file system attivo che per le copie Snapshot.

  È possibile modificare l'impostazione predefinita per il periodo di raffreddamento minimo di tiering con `-tiering-minimum-cooling-days` nel livello di privilegio avanzato di `volume create` e. `volume modify` comandi. I valori validi vanno da 2 a 183 giorni.

- Il `all` La policy di tiering, supportata solo con ONTAP 9.6 e versioni successive, sposta tutti i blocchi di dati utente nel file system attivo e nelle copie Snapshot nel Tier cloud. Sostituisce il `backup` policy di tiering.

  Il `all` i criteri di tiering dei volumi non devono essere utilizzati su volumi di lettura/scrittura con traffico client normale.

  Il periodo di raffreddamento minimo del tiering non si applica perché i dati si spostano al livello cloud non appena viene eseguita la scansione del tiering e non è possibile modificare l'impostazione.

- Il `none` la policy di tiering mantiene i dati di un volume nel tier di performance e non passa al tier cloud.

  Impostazione del criterio di tiering su `none` impedisce il nuovo tiering. I dati del volume precedentemente spostati nel Tier cloud rimangono nel Tier cloud fino a quando non diventano hot e vengono automaticamente spostati di nuovo nel Tier locale.

  Il periodo di raffreddamento minimo del tiering non si applica perché i dati non si spostano mai al livello cloud e non è possibile modificare l'impostazione.

  Quando si blocca a freddo in un volume con una policy di tiering impostata su `none` vengono letti, vengono resi a caldo e scritti nel tier locale.

Il `volume show` l'output del comando mostra la policy di tiering di un volume. Un volume che non è mai stato

utilizzato con FabricPool mostra `none` policy di tiering nell'output.

### Cosa accade quando si modifica il criterio di tiering di un volume in FabricPool

È possibile modificare la policy di tiering di un volume eseguendo una `volume modify` operazione. Devi comprendere come la modifica della policy di tiering possa influire sul tempo necessario per far diventare i dati più freddi e spostarli nel Tier cloud.

- Modifica della policy di tiering da `snapshot-only` oppure `none` a. `auto` Fa sì che ONTAP invii blocchi di dati utente nel file system attivo che sono già cold al livello cloud, anche se tali blocchi di dati utente non erano precedentemente idonei per il livello cloud.
- Modifica della policy di tiering in `all` Da un'altra policy deriva che ONTAP sposta al più presto nel cloud tutti i blocchi utente nel file system attivo e nelle copie Snapshot. Prima di ONTAP 9,8, i blocchi necessitavano di attendere l'esecuzione della scansione di tiering successiva.

  Non è consentito spostare nuovamente i blocchi nel Tier di performance.

- Modifica della policy di tiering da `auto` a. `snapshot-only` oppure `none` non fa sì che i blocchi di file system attivi già spostati nel tier cloud vengano spostati di nuovo nel tier di performance.

  Le letture dei volumi sono necessarie per riportare i dati al Tier di performance.

- Ogni volta che si modifica il criterio di tiering su un volume, il periodo minimo di raffreddamento del tiering viene ripristinato al valore predefinito per il criterio.

### Cosa accade alla policy di tiering quando si sposta un volume

- A meno che non si specifichi esplicitamente un criterio di tiering diverso, un volume conserva la propria policy di tiering originale quando viene spostato all'interno e all'esterno di un aggregato abilitato a FabricPool.

  Tuttavia, la policy di tiering ha effetto solo quando il volume si trova in un aggregato abilitato a FabricPool.

- Il valore esistente di `-tiering-minimum-cooling-days` parametro per lo spostamento di un volume con il volume a meno che non si specifichi un criterio di tiering diverso per la destinazione.

  Se si specifica un criterio di tiering diverso, il volume utilizza il periodo di raffreddamento minimo di tiering predefinito per tale criterio. Questo è il caso se la destinazione è FabricPool o meno.

- È possibile spostare un volume tra gli aggregati e contemporaneamente modificare la policy di tiering.
- Prestare particolare attenzione quando un `volume move` l'operazione comprende `auto` policy di tiering.

  Supponendo che sia l'origine che la destinazione siano aggregati abilitati per FabricPool, la seguente tabella riassume il risultato di a. `volume move` operazione che comporta modifiche dei criteri correlate a. `auto`:

| Quando si sposta un volume con una policy di tiering di… | Inoltre, è possibile modificare la policy di tiering passando a… | Quindi, dopo lo spostamento del volume… |
|---|---|---|
| `all` | `auto` | Tutti i dati vengono spostati nel Tier di performance. |

| | | |
|---|---|---|
| `snapshot-only`, `none`, o. `auto` | `auto` | I blocchi di dati vengono spostati nello stesso livello della destinazione in cui si trovavano in precedenza nell'origine. |
| `auto` oppure `all` | `snapshot-only` | Tutti i dati vengono spostati nel Tier di performance. |
| `auto` | `all` | Tutti i dati degli utenti vengono spostati nel livello cloud. |
| `snapshot-only`,`auto` oppure `all` | `none` | Tutti i dati vengono conservati al livello di performance. |

### Cosa accade alla policy di tiering quando si clonano volumi

- A partire da ONTAP 9.8, un volume clone eredita sempre sia la policy di tiering che la policy di recupero del cloud dal volume padre.

  Nelle release precedenti a ONTAP 9.8, un clone eredita la policy di tiering dall'origine, tranne quando l'origine dispone di `all` policy di tiering.

- Se il volume padre dispone di `never` cloud retrieval policy, il suo volume clone deve disporre di `never` policy di recupero del cloud o di `all` policy di tiering e policy di recupero del cloud corrispondenti `default`.
- Impossibile modificare la policy di recupero cloud del volume padre in `never` a meno che tutti i volumi cloni non dispongano di una policy di recupero cloud `never`.

Quando si clonano i volumi, tenere presenti le seguenti Best practice:

- Il `-tiering-policy` opzione e. `tiering-minimum-cooling-days` l'opzione del clone controlla solo il comportamento di tiering dei blocchi unici per il clone. Pertanto, si consiglia di utilizzare le impostazioni di tiering sul FlexVol padre che spostano la stessa quantità di dati o spostano una quantità inferiore di dati rispetto a uno qualsiasi dei cloni
- La policy di recupero del cloud sul FlexVol padre deve spostare la stessa quantità di dati o spostare più dati rispetto alla policy di recupero di uno qualsiasi dei cloni

### Come funzionano le policy di tiering con la migrazione del cloud

Il recupero dei dati nel cloud di FabricPool è controllato da policy di tiering che determinano il recupero dei dati dal Tier cloud al Tier di performance in base al modello di lettura. I modelli di lettura possono essere sequenziali o casuali.

La tabella seguente elenca le policy di tiering e le regole di recupero dei dati cloud per ogni policy.

| Policy di tiering | Comportamento di recupero |
|---|---|
| nessuno | Letture sequenziali e casuali |

| | |
|---|---|
| solo snapshot | Letture sequenziali e casuali |
| automatico | Letture casuali |
| tutto | Nessun recupero dei dati |

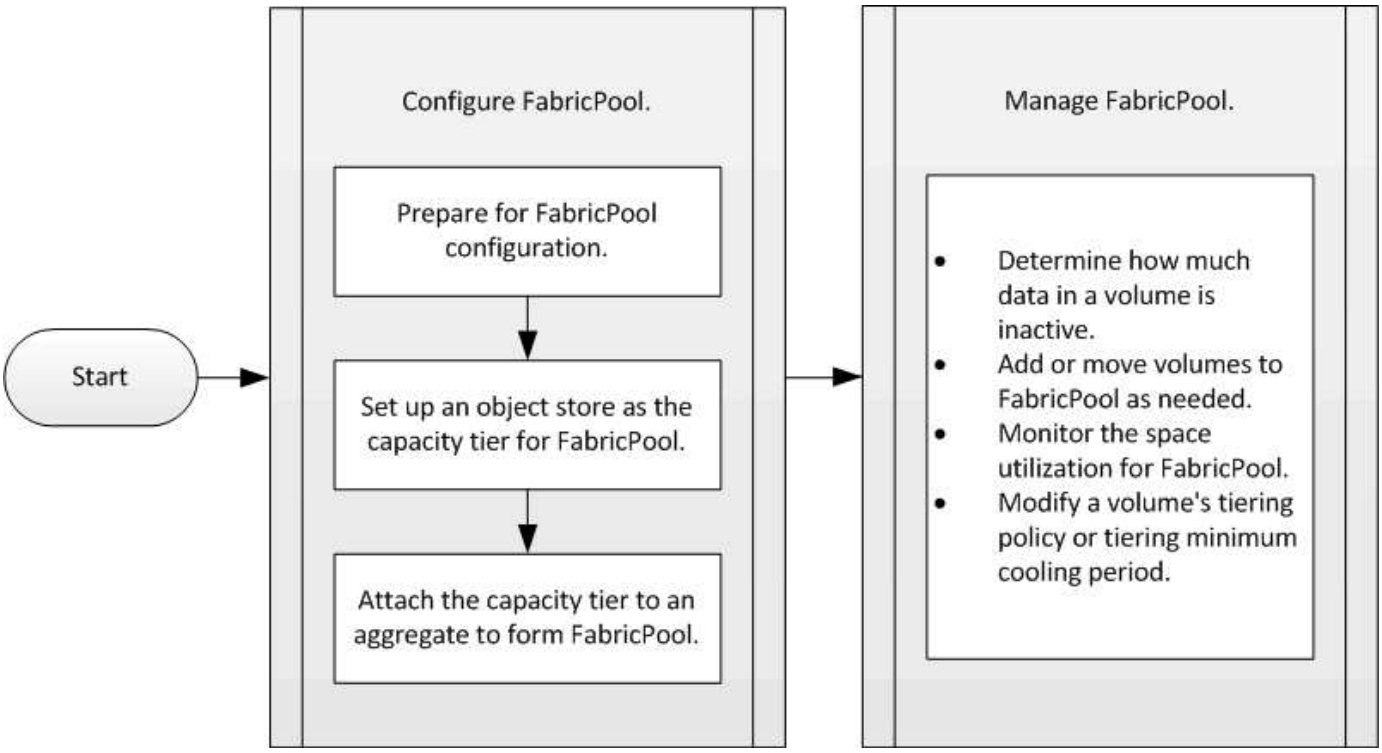
A partire da ONTAP 9.8, il controllo della migrazione nel cloud `cloud-retrieval-policy` l'opzione sovrascrive il comportamento predefinito di migrazione o recupero del cloud controllato dalla policy di tiering.

La seguente tabella elenca le policy di recupero cloud supportate e il loro comportamento di recupero.

| Policy di recupero del cloud | Comportamento di recupero |
|---|---|
| predefinito | La policy di tiering decide quali dati devono essere ritirati, quindi non vi è alcuna modifica al recupero dei dati nel cloud con "default," `cloud-retrieval-policy`. Questo criterio è il valore predefinito per qualsiasi volume, indipendentemente dal tipo di aggregato ospitato. |
| a lettura | Tutti i dati letti dal client vengono estratti dal Tier cloud al Tier di performance. |
| mai | Nessun dato client-driven viene estratto dal Tier cloud al Tier di performance |
| promuovi | • Per la policy di tiering "none", tutti i dati cloud vengono estratti dal Tier cloud al Tier di performance<br>• Per la policy di tiering "snapshot-only," vengono estratti i dati AFS. |

## Workflow di gestione di FabricPool

È possibile utilizzare il diagramma del flusso di lavoro di FabricPool per pianificare le attività di configurazione e gestione.




## Configurare FabricPool

### Preparazione per la configurazione FabricPool

#### Preparazione per la panoramica della configurazione di FabricPool

La configurazione di FabricPool consente di gestire i dati del Tier di storage (il Tier di performance locale o il Tier cloud) da memorizzare in base all'accesso frequente ai dati.

La preparazione richiesta per la configurazione FabricPool dipende dall'archivio di oggetti utilizzato come livello cloud.

#### Aggiungi una connessione al cloud

A partire da ONTAP 9.9.0, è possibile utilizzare Gestione sistema per aggiungere una connessione al cloud.

Per iniziare, utilizza NetApp Cloud Insights per configurare un collector. Durante il processo di configurazione, si copia un codice di accoppiamento generato da Cloud Insights, quindi si accede a un cluster utilizzando Gestione sistema. In questo caso, è possibile aggiungere una connessione cloud utilizzando il codice di accoppiamento. Il resto del processo viene completato in Cloud Insights.

> Se si sceglie l'opzione per utilizzare un server proxy quando si aggiunge una connessione da Cloud Volumes ONTAP al servizio Cloud Insights, è necessario assicurarsi che l'URL sia https://example.com è accessibile dal server proxy. Quando viene visualizzato il messaggio "la configurazione del proxy HTTP non è valida" https://example.com non è accessibile.

**Fasi**

1. In Cloud Insights, durante il processo di configurazione di un collector, copiare il codice di accoppiamento generato.

2. Utilizzando Gestione sistema con ONTAP 9.9.0 o versione successiva, accedere al cluster.
3. Selezionare **Cluster > Settings** (Cluster > Impostazioni).
4. Nella sezione connessioni cloud, selezionare **Aggiungi** per aggiungere una connessione.
5. Inserire un nome per la connessione e incollare il codice di accoppiamento nell'apposito spazio.
6. Selezionare **Aggiungi**.
7. Tornare a Cloud Insights per completare la configurazione del collector.

Per ulteriori informazioni su Cloud Insights, fare riferimento a. "Documentazione Cloud Insights".

#### Installare una licenza FabricPool

La licenza FabricPool utilizzata in passato sta cambiando e viene conservata solo per le configurazioni non supportate da BlueXP. A partire dal 21 agosto 2021, la licenza BYOL di Cloud Tiering è stata introdotta per le configurazioni di tiering che sono supportate in BlueXP utilizzando il servizio Cloud Tiering.

"Scopri di più sulla nuova licenza BYOL Cloud Tiering".

Le configurazioni supportate da BlueXP devono utilizzare la pagina del portafoglio digitale in BlueXP per il tiering delle licenze per i cluster ONTAP. Ciò richiede la configurazione di un account BlueXP e la configurazione del tiering per il provider di storage a oggetti che si intende utilizzare. Attualmente BlueXP supporta il tiering per i seguenti storage a oggetti: Amazon S3, Azure Blob, Google Cloud Storage, S3-compatibile e StorageGRID.

"Scopri di più sul servizio di tiering cloud".

È possibile scaricare e attivare una licenza FabricPool utilizzando Gestione sistema se si dispone di una delle configurazioni non supportate da BlueXP:

- Installazioni ONTAP in siti oscuri
- Cluster ONTAP che eseguono il tiering dei dati per lo storage a oggetti cloud IBM o Alibaba

La licenza FabricPool è una licenza a livello di cluster. Include un limite di utilizzo autorizzato acquistato per lo storage a oggetti associato a FabricPool nel cluster. L'utilizzo nel cluster non deve superare la capacità del limite di utilizzo autorizzato. Per aumentare il limite di utilizzo della licenza, contattare il rappresentante commerciale.

Le licenze FabricPool sono disponibili in formati perpetui o a termine, di 1 o 3 anni.

Una licenza FabricPool basata su termini con 10 TB di capacità libera è disponibile per i primi ordini FabricPool per le configurazioni di cluster esistenti non supportate in BlueXP. La capacità libera non è disponibile con licenze perpetue. Non è richiesta una licenza se si utilizza NetApp StorageGRID o ONTAP S3 per il livello cloud. Cloud Volumes ONTAP non richiede una licenza FabricPool, indipendentemente dal provider in uso.

Questa attività è supportata solo caricando il file di licenza nel cluster utilizzando System Manager.

**Fasi**

1. Scaricare il file di licenza NetApp (NLF) per la licenza FabricPool dal "Sito di supporto NetApp".
2. Eseguire le seguenti operazioni utilizzando Gestione di sistema per caricare la licenza FabricPool nel cluster:

a. Nel riquadro **Cluster > Settings** (Cluster > Impostazioni), nella scheda **Licenses** (licenze), fare clic su →.

b. Nella pagina **License**, fare clic su + Add .

c. Nella finestra di dialogo **Aggiungi licenza**, fare clic su **Sfoglia** per selezionare l'NLF scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

**Informazioni correlate**

"Panoramica sulle licenze ONTAP FabricPool (FP)"

"Ricerca licenze software NetApp"

"TechComm TV di NetApp: Elenco di riproduzione FabricPool"

#### Installare un certificato CA se si utilizza StorageGRID

A meno che non si preveda di disattivare il controllo dei certificati per StorageGRID, è necessario installare un certificato CA StorageGRID sul cluster in modo che ONTAP possa autenticare con StorageGRID come archivio di oggetti per FabricPool.

**A proposito di questa attività**

ONTAP 9.4 e versioni successive consentono di disattivare il controllo dei certificati per StorageGRID.

**Fasi**

1. Contattare l'amministratore di StorageGRID per ottenere il certificato CA del sistema StorageGRID.
2. Utilizzare `security certificate install` con il `-type server-ca` Parametro per installare il certificato CA StorageGRID sul cluster.

   Il nome di dominio completo (FQDN) immesso deve corrispondere al nome comune personalizzato sul certificato CA di StorageGRID.

### Aggiornare un certificato scaduto

Per aggiornare un certificato scaduto, è consigliabile utilizzare una CA attendibile per generare il nuovo certificato del server. Inoltre, è necessario assicurarsi che il certificato venga aggiornato contemporaneamente sul server StorageGRID e sul cluster ONTAP per ridurre al minimo i tempi di inattività.

**Informazioni correlate**

"Risorse StorageGRID"

#### Installare un certificato CA se si utilizza ONTAP S3

A meno che non si preveda di disattivare il controllo dei certificati per ONTAP S3, è necessario installare un certificato CA ONTAP S3 sul cluster in modo che ONTAP possa autenticare con ONTAP S3 come archivio di oggetti per FabricPool.

**Fasi**

1. Ottenere il certificato CA del sistema ONTAP S3.
2. Utilizzare `security certificate install` con il `-type server-ca` Parametro per installare il certificato CA ONTAP S3 sul cluster.

Il nome di dominio completo (FQDN) immesso deve corrispondere al nome comune personalizzato sul certificato CA di ONTAP S3.

### Aggiornare un certificato scaduto

Per aggiornare un certificato scaduto, è consigliabile utilizzare una CA attendibile per generare il nuovo certificato del server. Inoltre, è necessario assicurarsi che il certificato venga aggiornato contemporaneamente sul server ONTAP S3 e sul cluster ONTAP per ridurre al minimo i tempi di inattività.

#### Informazioni correlate

"Configurazione S3"

## Impostare un archivio di oggetti come livello cloud per FabricPool

### Imposta un archivio di oggetti come livello cloud per la panoramica di FabricPool

La configurazione di FabricPool implica la specifica delle informazioni di configurazione dell'archivio di oggetti (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage o Microsoft Azure Blob Storage per il cloud) che si intende utilizzare come livello cloud per FabricPool.

### Configura StorageGRID come Tier cloud

Se utilizzi ONTAP 9.2 o versioni successive, puoi impostare StorageGRID come livello cloud per FabricPool. Quando si esegue il tiering dei dati a cui accedono i protocolli SAN, NetApp consiglia di utilizzare cloud privati, come StorageGRID, a causa di considerazioni sulla connettività.

#### Considerazioni sull'utilizzo di StorageGRID con FabricPool

- È necessario installare un certificato CA per StorageGRID, a meno che non si disabiliti esplicitamente il controllo dei certificati.
- Non è necessario attivare la versione degli oggetti StorageGRID nel bucket dell'archivio di oggetti.
- Non è richiesta una licenza FabricPool.
- Se un nodo StorageGRID viene implementato in una macchina virtuale con storage assegnato da un sistema NetApp AFF, verificare che il volume non abbia una policy di tiering FabricPool attivata.

  La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.

> Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

#### A proposito di questa attività

Il bilanciamento del carico è abilitato per StorageGRID in ONTAP 9.8 e versioni successive. Quando il nome host del server viene risolto in più indirizzi IP, ONTAP stabilisce connessioni client con tutti gli indirizzi IP restituiti (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

**Procedure**

Puoi impostare StorageGRID come livello cloud per FabricPool con Gestione di sistema ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Fare clic su **Storage > Tier > Add Cloud Tier** e selezionare StorageGRID come provider dell'archivio di oggetti.
2. Completare le informazioni richieste.
3. Se si desidera creare un mirror cloud, fare clic su **Aggiungi come mirror FabricPool**.

Un mirror FabricPool offre un metodo per sostituire perfettamente un archivio di dati e garantisce che i dati siano disponibili in caso di disastro.

**CLI**

1. Specificare le informazioni di configurazione StorageGRID utilizzando `storage aggregate object-store config create` con il `-provider-type SGWS` parametro.

   - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere a StorageGRID con le informazioni fornite.
   - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti StorageGRID.
   - Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti StorageGRID.
   - Se la password StorageGRID viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

     In questo modo, ONTAP può accedere ai dati in StorageGRID senza interruzioni.
   - Impostazione di `-is-certificate-validation-enabled` parametro a. `false` Disattiva il controllo dei certificati per StorageGRID.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name mySGWS -provider-type SGWS -server mySGWSserver
   -container-name mySGWScontainer -access-key mySGWSkey
   -secret-password mySGWSpass
   ```

2. Visualizzare e verificare le informazioni di configurazione StorageGRID utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione StorageGRID per FabricPool.

**Imposta ONTAP S3 come Tier cloud**

Se utilizzi ONTAP 9.8 o versioni successive, puoi impostare ONTAP S3 come livello cloud per FabricPool.

### Di cosa hai bisogno

È necessario disporre del nome del server ONTAP S3 e dell'indirizzo IP dei relativi LIF associati sul cluster remoto.

Sul cluster locale devono essere presenti LIF intercluster.

"Creazione di LIF intercluster per tiering FabricPool remoto"

### A proposito di questa attività

Il bilanciamento del carico è abilitato per i server ONTAP S3 in ONTAP 9.8 e versioni successive. Quando il nome host del server viene risolto in più indirizzi IP, ONTAP stabilisce connessioni client con tutti gli indirizzi IP restituiti (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

### Procedure

Puoi impostare ONTAP S3 come livello cloud per FabricPool con Gestione di sistema ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Fare clic su **Storage > Tier > Add Cloud Tier** e selezionare ONTAP S3 come provider dell'archivio di oggetti.
2. Completare le informazioni richieste.
3. Se si desidera creare un mirror cloud, fare clic su **Aggiungi come mirror FabricPool**.

Un mirror FabricPool offre un metodo per sostituire perfettamente un archivio di dati e garantisce che i dati siano disponibili in caso di disastro.

**CLI**

1. Aggiungere voci per il server S3 e i LIF al server DNS.

| Opzione | Descrizione |
|---|---|
| **Se si utilizza un server DNS esterno** | Assegnare il nome del server S3 e gli indirizzi IP all'amministratore del server DNS. |
| **Se si utilizza la tabella degli host DNS del sistema locale** | Immettere il seguente comando:<br><br>`dns host create -vserver svm_name -address ip_address -hostname s3_server_name` |

2. Specificare le informazioni di configurazione di ONTAP S3 utilizzando `storage aggregate object-store config create` con il `-provider-type` `ONTAP_S3` parametro.
   - Il `storage aggregate object-store config create` Il comando non riesce se il sistema ONTAP locale non riesce ad accedere al server ONTAP S3 con le informazioni fornite.
   - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per l'autorizzazione delle richieste al server ONTAP S3.
   - Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste al server ONTAP S3.
   - Se la password del server ONTAP S3 viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata nel sistema ONTAP locale.

     In questo modo è possibile accedere ai dati nell'archivio di oggetti di ONTAP S3 senza interruzioni.
   - Impostazione di `-is-certificate-validation-enabled` parametro a. `false` Disattiva il controllo dei certificati per ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Visualizzare e verificare le informazioni di configurazione di ONTAP_S3 utilizzando `storage`

`aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` consente di modificare `ONTAP_S3` Informazioni di configurazione per FabricPool.

### Impostare Alibaba Cloud Object Storage come livello cloud

Se utilizzi ONTAP 9.6 o versioni successive, puoi impostare Alibaba Cloud Object Storage come livello cloud per FabricPool.

#### Considerazioni sull'utilizzo dello storage a oggetti cloud di Alibaba con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

  I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva su un sistema AFF, se utilizzi Alibaba Cloud Object Storage su un sistema non AFF, o se esegui l'upgrade da un cluster esistente, ti serve un "Licenza FabricPool".

- Nei sistemi AFF e FAS e in ONTAP Select, FabricPool supporta le seguenti classi di servizi di storage a oggetti Alibaba:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service - accesso non frequente

    "Alibaba Cloud: Introduzione alle classi di storage"

Per informazioni sulle classi di storage non elencate, contattare il rappresentante commerciale NetApp.

#### Fasi

1. Specificare le informazioni di configurazione di Alibaba Cloud Object Storage utilizzando `storage aggregate object-store config create` con il `-provider-type AliCloud` parametro.

   - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere all'archivio di oggetti cloud Alibaba con le informazioni fornite.
   - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di Alibaba Cloud Object Storage.
   - Se la password di Alibaba Cloud Object Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

     In questo modo, ONTAP può accedere ai dati nello storage a oggetti cloud di Alibaba senza interruzioni.

   ```
   storage aggregate object-store config create my_ali_oss_store_1
   -provider-type AliCloud -server oss-us-east-1.aliyuncs.com
   -container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
   ```

2. Visualizzare e verificare le informazioni di configurazione di Alibaba Cloud Object Storage utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Il comando consente di modificare le

informazioni di configurazione di Alibaba Cloud Object Storage per FabricPool.

### Imposta Amazon S3 come Tier cloud

Se utilizzi ONTAP 9.2 o versioni successive, puoi impostare Amazon S3 come livello cloud per FabricPool. Se utilizzi ONTAP 9.5 o versioni successive, puoi configurare i servizi cloud commerciali Amazon (C2S) per FabricPool.

#### Considerazioni sull'utilizzo di Amazon S3 con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.
  - I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool.

    Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi Amazon S3 su un sistema non AFF o se esegui l'upgrade da un cluster esistente, ti serve un "Licenza FabricPool".

  Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti Amazon S3 su una porta a 10 Gbps.
- Nei sistemi AFF e FAS e in ONTAP Select, FabricPool supporta le seguenti classi di storage Amazon S3:
  - Standard Amazon S3
  - Amazon S3 Standard - accesso non frequente (Standard - IA)
  - Amazon S3 One zone - accesso non frequente (una zona - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services
  - A partire da ONTAP 9.11.1, recupero immediato del ghiacciaio Amazon S3 (FabricPool non supporta il recupero flessibile del ghiacciaio o l'archiviazione profonda del ghiacciaio)

    "Documentazione Amazon Web Services: Classi di storage Amazon S3"

  Per informazioni sulle classi di storage non elencate, contattare il rappresentante commerciale.

- Su Cloud Volumes ONTAP, FabricPool supporta il tiering da SSD General Purpose (gp2) e volumi HDD ottimizzati per il throughput (st1) di Amazon Elastic Block Store (EBS).

#### Fasi

1. Specificare le informazioni di configurazione di Amazon S3 utilizzando `storage aggregate object-store config create` con il `-provider-type AWS_S3` parametro.
   - Si utilizza `-auth-type CAP` Parametro per ottenere le credenziali per l'accesso a C2S.

     Quando si utilizza `-auth-type CAP` è necessario utilizzare il `-cap-url` Parametro per specificare l'URL completo per richiedere credenziali temporanee per l'accesso a C2S.

   - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere ad Amazon S3 con le informazioni fornite.
   - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste

all'archivio di oggetti Amazon S3.

- Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti Amazon S3.
- Se la password Amazon S3 viene modificata, devi aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

  In questo modo, ONTAP può accedere ai dati in Amazon S3 senza interruzioni.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Visualizzare e verificare le informazioni di configurazione di Amazon S3 utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Comando consente di modificare le informazioni di configurazione di Amazon S3 per FabricPool.

#### Configura Google Cloud Storage come Tier cloud

Se utilizzi ONTAP 9.6 o versioni successive, puoi impostare Google Cloud Storage come livello cloud per FabricPool.

#### Considerazioni aggiuntive sull'utilizzo dello storage cloud Google con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

  I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi Google Cloud Storage su un sistema non AFF, o se esegui l'upgrade da un cluster esistente, ti serve un xref:./fabricpool/"Licenza FabricPool".

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per connettersi al server a oggetti di storage su Google Cloud su una porta a 10 Gbps.
- Sui sistemi AFF e FAS e su ONTAP Select, FabricPool supporta le seguenti classi di storage a oggetti di Google Cloud:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline

- Google Cloud Coldline

  "Google Cloud: Classi di storage"

**Fasi**

1. Specificare le informazioni di configurazione di Google Cloud Storage utilizzando `storage aggregate object-store config create` con il `-provider-type GoogleCloud` parametro.

   - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere a Google Cloud Storage con le informazioni fornite.
   - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di Google Cloud Storage.
   - Se la password di Google Cloud Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

     In questo modo, ONTAP può accedere ai dati in Google Cloud Storage senza interruzioni.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud  -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Visualizzare e verificare le informazioni di configurazione di Google Cloud Storage utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione di Google Cloud Storage per FabricPool.

### Configurare IBM Cloud Object Storage come Tier cloud

Se si utilizza ONTAP 9.5 o versione successiva, è possibile impostare lo storage a oggetti cloud IBM come livello cloud per FabricPool.

#### Considerazioni sull'utilizzo dello storage a oggetti cloud IBM con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

  I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva su un sistema AFF, se utilizzi IBM Cloud Object Storage su un sistema non AFF o se esegui l'upgrade da un cluster esistente, ti serve un "Licenza FabricPool".

  Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti cloud IBM su una porta a 10 Gbps.

**Fasi**

1. Specificare le informazioni di configurazione di IBM Cloud Object Storage utilizzando `storage aggregate object-store config create` con il `-provider-type IBM_COS` parametro.

- Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere all'archivio di oggetti cloud IBM con le informazioni fornite.
- Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di IBM Cloud Object Storage.
- Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti di IBM Cloud Object Storage.
- Se la password di IBM Cloud Object Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

  In questo modo, ONTAP può accedere ai dati nello storage a oggetti cloud IBM senza interruzioni.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Visualizzare e verificare le informazioni di configurazione di IBM Cloud Object Storage utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione di IBM Cloud Object Storage per FabricPool.

### Configura Azure Blob Storage per il cloud come Tier cloud

Se utilizzi ONTAP 9.4 o versioni successive, puoi configurare Azure Blob Storage per il cloud come Tier cloud per FabricPool.

#### Considerazioni sull'utilizzo dello storage Blob di Microsoft Azure con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

  I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi l'archiviazione BLOB di Azure su un sistema non AFF o se esegui l'upgrade da un cluster esistente, hai bisogno di un xref:./fabricpool/"Licenza FabricPool".

  Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Non è richiesta una licenza FabricPool se si utilizza Azure Blob Storage con Cloud Volumes ONTAP.
- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti dello storage Blob Azure su una porta a 10 Gbps.
- FabricPool attualmente non supporta Azure Stack, ovvero servizi Azure on-premise.
- A livello di account in Microsoft Azure Blob Storage, FabricPool supporta solo livelli di storage hot e cool.

  FabricPool non supporta il tiering a livello di blob. Inoltre, non supporta il tiering del Tier di storage di archivio di Azure.

#### A proposito di questa attività

FabricPool attualmente non supporta Azure Stack, ovvero servizi Azure on-premise.

**Fasi**

1. Specificare le informazioni di configurazione di Azure Blob Storage utilizzando `storage aggregate object-store config create` con il `-provider-type Azure_Cloud` parametro.

   - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere all'archivio Azure Blob con le informazioni fornite.
   - Si utilizza `-azure-account` Parametro per specificare l'account Azure Blob Storage.
   - Si utilizza `-azure-private-key` Parametro per specificare la chiave di accesso per l'autenticazione delle richieste a Azure Blob Storage.
   - Se la password di Azure Blob Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

     In questo modo, ONTAP può accedere ai dati nello storage di Azure Blob senza interruzioni.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Visualizzare e verificare le informazioni di configurazione di Azure Blob Storage utilizzando `storage aggregate object-store config show` comando.

   Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione dello storage di Azure Blob per FabricPool.

### Impostare gli archivi di oggetti per FabricPool in una configurazione MetroCluster

Se si esegue ONTAP 9.7 o versione successiva, è possibile impostare un FabricPool mirrorato su una configurazione MetroCluster per eseguire il Tier dei dati cold in archivi di oggetti in due diverse zone di errore.

**A proposito di questa attività**

- FabricPool in MetroCluster richiede che l'aggregato mirrorato sottostante e la configurazione dell'archivio di oggetti associata siano di proprietà della stessa configurazione di MetroCluster.
- Non è possibile associare un aggregato a un archivio di oggetti creato nel sito MetroCluster remoto.
- È necessario creare configurazioni dell'archivio di oggetti sulla configurazione MetroCluster proprietaria dell'aggregato.

**Prima di iniziare**

- La configurazione di MetroCluster è impostata e configurata correttamente.
- Nei siti MetroCluster appropriati vengono impostati due archivi di oggetti.
- I container sono configurati su ciascuno degli archivi di oggetti.
- Gli spazi IP vengono creati o identificati nelle due configurazioni MetroCluster e i relativi nomi corrispondono.

**Fase**

1. Specificare le informazioni di configurazione dell'archivio di oggetti su ciascun sito MetroCluster utilizzando `storage object-store config create` comando.

   In questo esempio, FabricPool è richiesto su un solo cluster nella configurazione MetroCluster. Per quel cluster vengono create due configurazioni di archivio di oggetti, una per ogni bucket di archivio di oggetti.

```
storage aggregate
    object-store config create -object-store-name mcc1-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
    -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
    -is-ssl-enabled <true|false> ipspace <IPSpace>
```

   Questo esempio imposta FabricPool sul secondo cluster nella configurazione MetroCluster.

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

#### Verificare le performance di throughput dell'archivio di oggetti prima di collegarlo a un Tier locale

Prima di collegare un archivio di oggetti a un livello locale, è possibile verificare le prestazioni di latenza e throughput dell'archivio di oggetti utilizzando il profiler dell'archivio di oggetti.

**Prima di essere**

- È necessario aggiungere il livello cloud a ONTAP prima di poterlo utilizzare con il profiler dell'archivio di oggetti.
- È necessario essere in modalità privilegio avanzato CLI ONTAP.

**Fasi**

1. Avviare il profiler dell'archivio oggetti:

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. Visualizzare i risultati:

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

#### Collegare il Tier cloud a un Tier locale (aggregato)

Dopo aver configurato un archivio di oggetti come Tier cloud, specificare il Tier locale (aggregato) da utilizzare allegandolo a FabricPool. In ONTAP 9.5 e versioni successive, è anche possibile collegare Tier locali (aggregati) che contengono componenti di volume FlexGroup qualificati.

**A proposito di questa attività**

Allegare un Tier cloud a un Tier locale è un'azione permanente. Non è possibile scollegare un Tier cloud da un Tier locale dopo il collegamento. Tuttavia, è possibile utilizzare "Specchio FabricPool" per collegare un tier locale a un tier cloud diverso.

**Prima di iniziare**

Quando si utilizza l'interfaccia utente di ONTAP per impostare un aggregato per FabricPool, l'aggregato deve già esistere.

> Quando si utilizza Gestione sistema per impostare un livello locale per FabricPool, è possibile creare il livello locale e configurarlo per l'utilizzo di FabricPool contemporaneamente.

**Fasi**

È possibile collegare un Tier locale (aggregato) a un archivio di oggetti FabricPool con Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Accedere a **Storage > Tier**, selezionare un livello cloud, quindi fare clic su ⋮.
2. Selezionare **Allega livelli locali**.
3. In **Add as Primary** (Aggiungi come principale), verificare che i volumi siano idonei per il collegamento.
4. Se necessario, selezionare **Converti volumi in thin provisioning**.
5. Fare clic su **Save** (Salva).

**CLI**

**Per associare un archivio di oggetti a un aggregato con la CLI:**

1. **Opzionale**: Per verificare la quantità di dati inattivi in un volume, seguire la procedura descritta in "Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi".

   La visualizzazione della quantità di dati inattivi in un volume può aiutare a decidere quale aggregato utilizzare per FabricPool.

2. Collegare l'archivio di oggetti a un aggregato utilizzando `storage aggregate object-store attach` comando.

   Se l'aggregato non è mai stato utilizzato con FabricPool e contiene volumi esistenti, ai volumi viene assegnato il valore predefinito `snapshot-only` policy di tiering.

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

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

3. Visualizzare le informazioni sull'archivio di oggetti e verificare che l'archivio di oggetti collegato sia disponibile utilizzando `storage aggregate object-store show` comando.

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

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

#### Dati di Tier al bucket locale

## A partire da ONTAP 9.8, è possibile eseguire il tiering dei dati sullo storage a oggetti locale utilizzando ONTAP S3.

Il tiering dei dati in un bucket locale offre una semplice alternativa allo spostamento dei dati in un altro Tier locale. Questa procedura utilizza un bucket esistente sul cluster locale oppure è possibile consentire a ONTAP di creare automaticamente una nuova VM di storage e un nuovo bucket.

Tenere presente che una volta collegato a un Tier locale (aggregato), il Tier cloud non può essere disconnesso.

Per questo flusso di lavoro è necessaria una licenza S3, che crea un nuovo server S3 e un nuovo bucket, oppure utilizza quelli esistenti. Questa licenza è inclusa in "ONTAP uno". Per questo flusso di lavoro non è richiesta una licenza FabricPool.

#### Fase

1. Tier data to a local bucket: Fare clic su **Tier**, selezionare un Tier, quindi fare clic su ⋮.
2. Se necessario, abilitare il thin provisioning.
3. Scegliere un livello esistente o crearne uno nuovo.
4. Se necessario, modificare il criterio di tiering esistente.

## Gestire FabricPool

#### Panoramica di Manage FabricPool

Per soddisfare le esigenze di tiering dello storage, ONTAP consente di visualizzare la quantità di dati inattivi in un volume, aggiungere o spostare volumi in FabricPool, monitorare l'utilizzo dello spazio per FabricPool o modificare la policy di tiering di un volume o il periodo di raffreddamento minimo di tiering.

#### Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi

La visualizzazione della quantità di dati inattivi in un volume consente di utilizzare correttamente i Tier di storage. Le informazioni nel reporting dei dati inattivi consentono di decidere quale aggregato utilizzare per FabricPool, se spostare un volume in FabricPool o da esso o se modificare il criterio di tiering di un volume.

#### Di cosa hai bisogno

Per utilizzare la funzionalità di reporting dei dati inattivi, è necessario eseguire ONTAP 9.4 o versioni successive.

#### A proposito di questa attività

- Alcuni aggregati non supportano il reporting dei dati inattivi.

  Non è possibile attivare la funzione di reporting dei dati inattivi quando non è possibile attivare FabricPool, incluse le seguenti istanze:

  - Aggregati root
  - Aggregati MetroCluster con versioni di ONTAP precedenti alla 9.7
  - Flash Pool (aggregati ibridi o aggregati SnapLock)
- Il reporting dei dati inattivi è attivato per impostazione predefinita sugli aggregati in cui è attivata la compressione adattiva per tutti i volumi.
- Per impostazione predefinita, il reporting dei dati inattivi è attivato su tutti gli aggregati SSD in ONTAP 9.6.
- Per impostazione predefinita, la funzione di reporting dei dati inattivi è attivata nell'aggregato FabricPool in ONTAP 9.4 e ONTAP 9.5.

- È possibile abilitare la creazione di report dei dati inattivi su aggregati non FabricPool utilizzando l'interfaccia CLI di ONTAP, inclusi gli aggregati di dischi rigidi, a partire da ONTAP 9.6.

**Procedura**

È possibile determinare la quantità di dati inattivi con Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Scegliere una delle seguenti opzioni:
   - Una volta esistenti aggregati HDD, selezionare **Storage > Tier** e fare clic su ⋮ per l'aggregato su cui si desidera attivare il reporting dei dati inattivi.
   - Se non sono configurati Tier cloud, accedere a **Dashboard** e fare clic sul collegamento **Enable inactive data reporting** sotto **Capacity**.

**CLI**

**Per attivare la creazione di report dei dati inattivi con la CLI:**

1. Se l'aggregato per il quale si desidera visualizzare il reporting dei dati inattivi non viene utilizzato in FabricPool, attivare il reporting dei dati inattivi per l'aggregato utilizzando `storage aggregate modify` con il `-is-inactive-data-reporting-enabled true` parametro.

   ```
   cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
   -data-reporting-enabled true
   ```

   È necessario attivare esplicitamente la funzionalità di reporting dei dati inattivi su un aggregato non utilizzato per FabricPool.

   Non è possibile e non è necessario attivare il reporting dei dati inattivi su un aggregato abilitato a FabricPool perché l'aggregato è già dotato di report dei dati inattivi. Il `-is-inactive-data -reporting-enabled` Il parametro non funziona sugli aggregati abilitati per FabricPool.

   Il `-fields is-inactive-data-reporting-enabled` del parametro `storage aggregate show` il comando indica se il reporting dei dati inattivi è attivato su un aggregato.

2. Per visualizzare la quantità di dati inattivi su un volume, utilizzare `volume show` con il `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parametro.

   ```
   cluster1::> volume show -fields performance-tier-inactive-user-
   data,performance-tier-inactive-user-data-percent

   vserver volume performance-tier-inactive-user-data performance-tier-
   inactive-user-data-percent
   ------- ------ ----------------------------------
   -------------------------------------------
   vsim1   vol0   0B                                  0%
   vs1     vs1rv1 0B                                  0%
   vs1     vv1    10.34MB                             0%
   vs1     vv2    10.38MB                             0%
   4 entries were displayed.
   ```

   - Il `performance-tier-inactive-user-data` campo visualizza la quantità di dati utente memorizzati nell'aggregato non attivi.

- Il `performance-tier-inactive-user-data-percent` Visualizza la percentuale di dati inattivi nel file system attivo e nelle copie Snapshot.
- Per un aggregato non utilizzato per FabricPool, il reporting dei dati inattivi utilizza la policy di tiering per stabilire la quantità di dati da riportare come cold.
  - Per `none` policy di tiering, 31 giorni.
  - Per `snapshot-only` e. `auto`, utilizza il reporting dei dati inattivi `tiering-minimum-cooling-days`.
  - Per `ALL` policy, il reporting dei dati inattivi presuppone che i dati verranno tier entro un giorno.

    Fino al raggiungimento del punto, l'output mostra "-" per la quantità di dati inattivi invece di un valore.
- Su un volume che fa parte di FabricPool, i report di ONTAP come inattivi dipendono dal criterio di tiering impostato su un volume.
  - Per `none` Policy di tiering, ONTAP riporta la quantità di volume intero che è inattivo per almeno 31 giorni. Non è possibile utilizzare `-tiering-minimum-cooling-days` con il `none` policy di tiering.
  - Per `ALL`, `snapshot-only`, e. `auto` policy di tiering, il reporting dei dati inattivi non è supportato.

## Gestire i volumi per FabricPool

### Creare un volume per FabricPool

È possibile aggiungere volumi a FabricPool creando nuovi volumi direttamente nell'aggregato abilitato a FabricPool o spostando i volumi esistenti da un altro aggregato all'aggregato abilitato a FabricPool.

Quando si crea un volume per FabricPool, è possibile specificare un criterio di tiering. Se non viene specificato alcun criterio di tiering, il volume creato utilizza l'impostazione predefinita `snapshot-only` policy di tiering. Per un volume con `snapshot-only` oppure `auto` policy di tiering, è anche possibile specificare il periodo minimo di raffreddamento del tiering.

#### Di cosa hai bisogno

- Impostazione di un volume per l'utilizzo di `auto` La policy di tiering o la specifica del periodo di raffreddamento minimo di tiering richiede ONTAP 9.4 o versione successiva.
- L'utilizzo di FlexGroup Volumes richiede ONTAP 9.5 o versione successiva.
- Impostazione di un volume per l'utilizzo di `all` I criteri di tiering richiedono ONTAP 9.6 o versione successiva.
- Impostazione di un volume per l'utilizzo di `-cloud-retrieval-policy` Il parametro richiede ONTAP 9.8 o versione successiva.

#### Fasi

1. Creare un nuovo volume per FabricPool utilizzando `volume create` comando.
   - Il `-tiering-policy` il parametro opzionale consente di specificare il criterio di tiering per il volume.

È possibile specificare uno dei seguenti criteri di tiering:

- `snapshot-only` (impostazione predefinita)
- `auto`
- `all`
- `backup` (obsoleto)
- `none`

  "Tipi di policy di tiering FabricPool"

- Il `-cloud-retrieval-policy` il parametro opzionale consente agli amministratori del cluster con il livello di privilegio avanzato di eseguire l'override del comportamento predefinito di recupero o migrazione del cloud controllato dalla policy di tiering.

  È possibile specificare una delle seguenti policy di recupero del cloud:

  - `default`

    La policy di tiering determina quali dati vengono recuperati, quindi non vi è alcuna modifica al recupero dei dati nel cloud `default` policy-recupero-cloud. Questo significa che il comportamento è lo stesso delle release precedenti a ONTAP 9.8:

    - Se la policy di tiering è `none` oppure `snapshot-only`, quindi "default" significa che qualsiasi lettura dei dati basata su client viene estratta dal tier cloud al tier di performance.
    - Se la policy di tiering è `auto`, quindi viene estratta qualsiasi lettura casuale basata su client, ma non letture sequenziali.
    - Se la policy di tiering è `all` quindi, nessun dato client-driven viene estratto dal tier cloud.

  - `on-read`

    Tutte le letture dei dati basate su client vengono estratte dal Tier cloud al Tier di performance.

  - `never`

    Nessun dato client-driven viene estratto dal Tier cloud al Tier di performance

  - `promote`

    - Per la policy di tiering `none`, tutti i dati del cloud vengono estratti dal livello cloud al livello di performance
    - Per la policy di tiering `snapshot-only`, tutti i dati del file system attivi vengono estratti dal livello cloud al livello di performance.

- Il `-tiering-minimum-cooling-days` il parametro opzionale nel livello di privilegio avanzato consente di specificare il periodo minimo di raffreddamento del tiering per un volume che utilizza `snapshot-only` oppure `auto` policy di tiering.

  A partire da ONTAP 9.8, è possibile specificare un valore compreso tra 2 e 183 per i giorni di raffreddamento minimi di tiering. Se si utilizza una versione di ONTAP precedente alla 9.8, è possibile specificare un valore compreso tra 2 e 63 per i giorni di raffreddamento minimi di tiering.

#### Esempio di creazione di un volume per FabricPool

Nell'esempio seguente viene creato un volume denominato "myvol1" nell'aggregato abilitato a FabricPool "myFabricPool". La policy di tiering è impostata su `auto` e il periodo minimo di raffreddamento del tiering è impostato su 45 giorni:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

#### Informazioni correlate

"Gestione dei volumi FlexGroup"

### Spostare un volume su FabricPool

Quando si sposta un volume in FabricPool, è possibile specificare o modificare il criterio di tiering per il volume durante lo spostamento. A partire da ONTAP 9.8, quando si sposta un volume non FabricPool con la funzione di reporting dei dati inattivi attivata, FabricPool utilizza una mappa termica per leggere i blocchi tierable e sposta i dati cold nel Tier di capacità sulla destinazione FabricPool.

#### Di cosa hai bisogno

Devi comprendere come la modifica della policy di tiering possa influire sul tempo necessario per far diventare i dati più freddi e spostarli nel Tier cloud.

"Cosa accade alla policy di tiering quando si sposta un volume"

#### A proposito di questa attività

Se un volume non FabricPool ha attivato la funzione di reporting dei dati inattivi, quando si sposta un volume con policy di tiering `auto` oppure `snapshot-only` In un FabricPool, FabricPool legge i blocchi di temperatura da un file di mappa termica e utilizza tale temperatura per spostare i dati Cold direttamente nel Tier di capacità sulla destinazione FabricPool.

Non utilizzare `-tiering-policy` Opzione di spostamento del volume se si utilizza ONTAP 9.8 e si desidera che FabricPools utilizzi le informazioni di reporting dei dati inattive per spostare i dati direttamente nel livello di capacità. L'utilizzo di questa opzione fa sì che FabricPools ignori i dati relativi alla temperatura e segua invece il comportamento di spostamento delle release precedenti a ONTAP 9.8.

#### Fase

1. Utilizzare `volume move start` Comando per spostare un volume in FabricPool.

   Il `-tiering-policy` il parametro opzionale consente di specificare il criterio di tiering per il volume.

   È possibile specificare uno dei seguenti criteri di tiering:

   - `snapshot-only` (impostazione predefinita)
   - `auto`
   - `all`
   - `none`+"Tipi di policy di tiering FabricPool"

#### Esempio di spostamento di un volume in FabricPool

Nell'esempio riportato di seguito viene spostato un volume denominato "myvol2" della SVM "vs1" nell'aggregato abilitato a FabricPool "dest_FabricPool". Il volume viene esplicitamente impostato per l'utilizzo di `none` policy di tiering:

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool -tiering-policy none
```

#### Attiva e disattiva i volumi da scrivere direttamente nel cloud

A partire da ONTAP 9.14.1, puoi abilitare e disabilitare la scrittura direttamente nel cloud su un volume nuovo o esistente in una FabricPool, per consentire ai client NFS di scrivere dati direttamente nel cloud senza attendere le scansioni di tiering. I client SMB continuano a scrivere nel Tier di performance in un volume abilitato per la scrittura nel cloud. La modalità cloud-write è disattivata per impostazione predefinita.

Avere la possibilità di scrivere direttamente nel cloud è utile per casi come le migrazioni, ad esempio, dove grandi quantità di dati vengono trasferite in un cluster rispetto a quanto il cluster può supportare nel Tier locale. Senza la modalità cloud-write, durante la migrazione, vengono trasferite piccole quantità di dati, quindi trasferite e di nuovo in tiering, fino al completamento della migrazione. Utilizzando la modalità cloud-write, questo tipo di gestione non è più necessario, perché i dati non vengono mai trasferiti nel Tier locale.

**Prima di iniziare**

- Dovresti essere un amministratore di cluster o SVM.
- È necessario essere al livello di privilegi avanzati.
- Il volume deve essere di tipo lettura-scrittura.
- Il volume deve disporre di TUTTA LA policy di tiering.

**Attiva la scrittura direttamente nel cloud durante la creazione del volume**

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Creazione di un volume e abilitazione della modalità cloud-write:

   ```
   volume create -volume <volume name> -is-cloud-write-enabled <true|false>
   -aggregate <local tier name>
   ```

   L'esempio seguente crea un volume denominato vol1 con Cloud Write abilitato nel Tier locale FabricPool (aggr1):

   ```
   volume create -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
   ```

#### Consenti la scrittura diretta nel cloud di un volume esistente

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modifica di un volume per abilitare la modalità cloud-write:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

Il seguente esempio modifica un volume chiamato vol1 con scrittura cloud abilitata nel Tier locale FabricPool (aggr1):

```
volume modify -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

#### Disattivare la scrittura direttamente nel cloud su un volume

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Disattiva modalità cloud-write:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <aggregate name>
```

L'esempio seguente crea un volume denominato vol1 con Cloud Write abilitato:

```
volume modify -volume vol1 -is-cloud-write-enabled false -aggregate
aggr1
```

#### Attiva e disattiva la modalità aggressiva di Read-ahead

A partire da ONTAP 9.14.1, puoi abilitare e disabilitare la modalità aggressiva Read-ahead sui volumi in FabricPool che offrono supporto per media e intrattenimento, come ad esempio i workload in streaming dei film. Una aggressiva modalità di Read-ahead è disponibile in ONTAP 9.14.1 su tutte le piattaforme on-premise che supportano FabricPool. La funzione è disattivata per impostazione predefinita.

### A proposito di questa attività

Il `aggressive-readahead-mode` il comando ha due opzioni:

- `none`: la funzione read-ahead è disattivata.
- `file_prefetch`: il sistema legge l'intero file in memoria prima dell'applicazione client.

### Prima di iniziare

- Dovresti essere un amministratore di cluster o SVM.
- È necessario essere al livello di privilegi avanzati.

### Attiva la modalità Read-ahead aggressiva durante la creazione del volume

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Creazione di un volume e abilitazione della modalità aggressiva di Read-ahead:

   ```
   volume create -volume <volume name>  -aggressive-readahead-mode
   <none|file_prefetch>
   ```

   Nell'esempio seguente viene creato un volume denominato vol1 con la funzione di Read-ahead aggressiva abilitata con l'opzione file_prefetch:

   ```
   volume create -volume vol1 -aggressive-readahead-mode file_prefetch
   ```

### Disattiva la modalità aggressiva di lettura anticipata

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Disattivare la modalità aggressiva di Read-ahead:

   ```
   volume modify -volume <volume name>  -aggressive-readahead-mode none
   ```

   Nell'esempio seguente viene modificato un volume denominato vol1 per disattivare la modalità aggressiva di Read-ahead:

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

### Visualizzazione di una modalità di Read-ahead aggressiva su un volume

**Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Visualizza la modalità di lettura aggressiva:

```
volume show -fields aggressive-readahead-mode
```

### Tagging degli oggetti mediante tag personalizzati creati dall'utente

#### Tagging degli oggetti mediante panoramica dei tag personalizzati creati dall'utente

A partire da ONTAP 9.8, FabricPool supporta il tagging degli oggetti utilizzando tag personalizzati creati dall'utente per consentire la classificazione e l'ordinamento degli oggetti per una gestione più semplice. Se si è un utente con il livello di privilegio admin, è possibile creare nuovi tag di oggetto e modificare, eliminare e visualizzare i tag esistenti.

#### Assegnare un nuovo tag durante la creazione del volume

È possibile creare un nuovo tag di oggetto quando si desidera assegnare uno o più tag a nuovi oggetti a più livelli da un nuovo volume creato. È possibile utilizzare i tag per classificare e ordinare gli oggetti di tiering per semplificare la gestione dei dati. A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per creare tag di oggetto.

**A proposito di questa attività**

È possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Questi tag vengono conservati durante lo spostamento di un volume.

- È consentito un massimo di 4 tag per volume
- Nella CLI, ogni tag di oggetto deve essere una coppia chiave-valore separata da un segno uguale (`""`)
- Nella CLI, più tag devono essere separati da una virgola (`""`)
- Ogni valore di tag può contenere un massimo di 127 caratteri
- Ogni tasto tag deve iniziare con un carattere alfabetico o con un carattere di sottolineatura.

  Le chiavi devono contenere solo caratteri alfanumerici e caratteri di sottolineatura, mentre il numero massimo consentito è 127.

### Procedura

È possibile assegnare tag di oggetto con Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con i volumi che si desidera etichettare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume da contrassegnare e nella colonna **Tag oggetto** selezionare **fare clic per inserire i tag**.
5. Inserire una chiave e un valore.
6. Fare clic su **Apply** (Applica).

**CLI**

1. Utilizzare `volume create` con il `-tiering-object-tags` opzione per creare un nuovo volume con i tag specificati. È possibile specificare più tag in coppie separate da virgole:

   ```
   volume create [ -vserver <vserver name> ] -volume <volume_name>
   -tiering-object-tags <key1=value1> [
       ,<key2=value2>,<key3=value3>,<key4=value4> ]
   ```

   Nell'esempio seguente viene creato un volume denominato fp_volume1 con tre tag di oggetto.

   ```
   vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
   project=fabricpool,type=abc,content=data
   ```

#### Modificare un tag esistente

È possibile modificare il nome di un tag, sostituire tag su oggetti esistenti nell'archivio di oggetti o aggiungere un tag diverso a nuovi oggetti che si intende aggiungere in seguito.

### A proposito di questa attività

Utilizzando il `volume modify` con il `-tiering-object-tags` l'opzione sostituisce i tag esistenti con il nuovo valore fornito.

### Procedura

**System Manager**

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con volumi contenenti tag che si desidera modificare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume con i tag che si desidera modificare e nella colonna **Tag oggetto** fare clic sul nome del tag.
5. Modificare il tag.
6. Fare clic su **Apply** (Applica).

**CLI**

1. Utilizzare `volume modify` con il `-tiering-object-tags` opzione per modificare un tag esistente.

   ```
   volume modify [ -vserver <vserver name> ] -volume <volume_name>
   -tiering-object-tags <key1=value1> [ ,<key2=value2>,
   <key3=value3>,<key4=value4> ]
   ```

   Nell'esempio seguente viene modificato il nome del tag esistente type=abc in type=xyz.

   ```
   vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
   project=fabricpool,type=xyz,content=data
   ```

#### Eliminare un tag

È possibile eliminare i tag di oggetto quando non si desidera che vengano impostati su un volume o su oggetti nell'archivio di oggetti.

### Procedura

È possibile eliminare i tag degli oggetti con Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

**System Manager**

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con volumi contenenti tag che si desidera eliminare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume con i tag che si desidera eliminare e nella colonna **Tag oggetto** fare clic sul nome del tag.
5. Per eliminare il tag, fare clic sull'icona del cestino.
6. Fare clic su **Apply** (Applica).

**CLI**

1. Utilizzare `volume modify` con il `-tiering-object-tags` seguito da un valore vuoto (`""`) per eliminare un tag esistente.

   Nell'esempio seguente vengono cancellati i tag esistenti su fp_volume1.

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

#### Visualizzare i tag esistenti su un volume

È possibile visualizzare i tag esistenti su un volume per visualizzare i tag disponibili prima di aggiungere nuovi tag all'elenco.

**Fase**

1. Utilizzare `volume show` con il `-tiering-object-tags` opzione per visualizzare i tag esistenti su un volume.

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   -tiering-object-tags
   ```

#### Controllare lo stato di tagging degli oggetti sui volumi FabricPool

È possibile verificare se il tagging è completo su uno o più volumi FabricPool.

**Fase**

1. Utilizzare `vol show` con il `-fieldsneeds-object-retagging` opzione per verificare se l'etichettatura è in corso, se è stata completata o se l'etichettatura non è stata impostata.

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   name>]
   ```

   Viene visualizzato uno dei seguenti valori:

- `true` — lo scanner di tag degli oggetti non deve ancora essere eseguito o deve essere eseguito nuovamente per questo volume
- `false` — lo scanner di tagging degli oggetti ha completato la tagging per questo volume
- `<->` — lo scanner di tag degli oggetti non è applicabile a questo volume. Questo accade per i volumi che non risiedono su FabricPools.

**Monitorare l'utilizzo dello spazio per FabricPool**

Devi sapere quanti dati sono memorizzati nei livelli di performance e cloud per FabricPool. Tali informazioni consentono di determinare se è necessario modificare la policy di tiering di un volume, aumentare il limite di utilizzo della licenza FabricPool o aumentare lo spazio di storage del Tier cloud.

**Fasi**

1. Monitorare l'utilizzo dello spazio per gli aggregati abilitati a FabricPool utilizzando uno dei seguenti comandi per visualizzare le informazioni:

| Se si desidera visualizzare… | Quindi utilizzare questo comando: |
|---|---|
| La dimensione utilizzata del Tier cloud in un aggregato | `storage aggregate show` con `-instance` parametro |
| Dettagli sull'utilizzo dello spazio all'interno di un aggregato, inclusa la capacità di riferimento dell'archivio di oggetti | `storage aggregate show-space` con `-instance` parametro |
| Utilizzo dello spazio degli archivi di oggetti collegati agli aggregati, inclusa la quantità di spazio di licenza utilizzata | `storage aggregate object-store show-space` |
| Un elenco di volumi in un aggregato e le impronte dei dati e dei metadati | `volume show-footprint` |

Oltre a utilizzare i comandi CLI, è possibile utilizzare Active IQ Unified Manager (precedentemente noto come gestore unificato di OnCommand), insieme a FabricPool Advisor, supportato su cluster ONTAP 9.4 e versioni successive, o System Manager per monitorare l'utilizzo dello spazio.

Nell'esempio seguente vengono illustrati i modi per visualizzare l'utilizzo dello spazio e le informazioni correlate per FabricPool:

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                    ...
                                                Aggregate Display Name:
MyFabricPool
                                                                    ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                    ...
                                                         Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                    Total Logical Used
Size: -
                                                    Logical Used
Percentage: -
                                              Logical Unreferenced
Capacity: -
                                            Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Volume Guarantee                 MB          %
Flexible Volume Metadata         KB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %

Vserver : vs1
Volume : vol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Footprint in Performance Tier    KB          %
Footprint in Amazon01            KB          %
Flexible Volume Metadata         MB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %
...
```

2. Eseguire una delle seguenti operazioni in base alle necessità:

| Se si desidera… | Quindi… |
|---|---|
| Modificare la policy di tiering di un volume | Seguire la procedura descritta in "Gestione del tiering dello storage modificando la policy di tiering di un volume o il periodo minimo di raffreddamento del tiering". |
| Aumentare il limite di utilizzo della licenza FabricPool | Contattare il rappresentante commerciale NetApp o del partner.<br><br>"Supporto NetApp" |
| Aumentare lo spazio di storage del Tier cloud | Contattare il provider dell'archivio di oggetti utilizzato per il livello cloud. |

### Gestire il tiering dello storage modificando la policy di tiering di un volume o il periodo minimo di raffreddamento del tiering

È possibile modificare la policy di tiering di un volume per controllare se i dati vengono spostati nel Tier cloud quando diventano inattivi (*cold*). Per un volume con `snapshot-only` oppure `auto` policy di tiering, puoi anche specificare il periodo minimo di raffreddamento del tiering in base al quale i dati dell'utente devono rimanere inattivi prima di essere spostati nel tier cloud.

#### Di cosa hai bisogno

Modifica di un volume in `auto` La policy di tiering o la modifica del periodo di raffreddamento minimo di tiering richiede ONTAP 9.4 o versione successiva.

#### A proposito di questa attività

La modifica della policy di tiering di un volume modifica solo il successivo comportamento di tiering del volume. Non sposta retroattivamente i dati nel Tier cloud.

La modifica della policy di tiering potrebbe influire sul tempo necessario affinché i dati diventino freddi e vengano spostati al livello cloud.

"Cosa accade quando si modifica il criterio di tiering di un volume in FabricPool"

#### Fasi

1. Modificare il criterio di tiering per un volume esistente utilizzando `volume modify` con il `-tiering -policy` parametro:

   È possibile specificare uno dei seguenti criteri di tiering:

   - `snapshot-only` (impostazione predefinita)
   - `auto`
   - `all`
   - `none`

     "Tipi di policy di tiering FabricPool"

2. Se il volume utilizza `snapshot-only` oppure `auto` policy di tiering e si desidera modificare il periodo di raffreddamento minimo di tiering, utilizzare `volume modify` con il `-tiering-minimum-cooling-days` parametro facoltativo nel livello di privilegio avanzato.

   È possibile specificare un valore compreso tra 2 e 183 per i giorni di raffreddamento minimi di tiering. Se si utilizza una versione di ONTAP precedente alla 9.8, è possibile specificare un valore compreso tra 2 e 63 per i giorni di raffreddamento minimi di tiering.

#### Esempio di modifica della policy di tiering e del periodo minimo di raffreddamento di tiering di un volume

Nell'esempio seguente viene modificata la policy di tiering del volume "myvol" in SVM "vs1" in `auto` e il periodo di raffreddamento minimo di tiering fino a 45 giorni:

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

#### Archiviazione di volumi con FabricPool (video)

Questo video mostra una rapida panoramica sull'utilizzo di Gestione sistema per archiviare un volume su un livello cloud con FabricPool.

"Video NetApp: Archiviazione dei volumi con FabricPool (backup + spostamento del volume)"

#### Informazioni correlate

"TechComm TV di NetApp: Elenco di riproduzione FabricPool"

#### Utilizza i controlli di migrazione del cloud per ignorare la policy di tiering predefinita di un volume

È possibile modificare la policy di tiering predefinita di un volume per controllare il recupero dei dati utente dal livello cloud al livello di performance utilizzando `-cloud-retrieval-policy` Opzione introdotta in ONTAP 9.8.

#### Di cosa hai bisogno

- Modifica di un volume mediante `-cloud-retrieval-policy` L'opzione richiede ONTAP 9.8 o versione successiva.
- Per eseguire questa operazione, è necessario disporre del livello di privilegio avanzato.
- È necessario comprendere il comportamento delle policy di tiering con `-cloud-retrieval-policy`.

  "Come funzionano le policy di tiering con la migrazione del cloud"

#### Fase

1. Modificare il comportamento dei criteri di tiering per un volume esistente utilizzando `volume modify` con il `-cloud-retrieval-policy` opzione:

   ```
   volume create -volume <volume_name> -vserver <vserver_name> - tiering-
   policy <policy_name> -cloud-retrieval-policy
   ```

   ```
   vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
   promote
   ```

### Promuovi i dati al Tier di performance

#### Promuovi i dati nella panoramica del Tier di performance

A partire da ONTAP 9.8, se sei un amministratore del cluster a livello di privilegi avanzati, puoi promuovere in modo proattivo i dati al livello di performance dal livello cloud

utilizzando una combinazione di `tiering-policy` e a. `cloud-retrieval-policy` impostazione.

### A proposito di questa attività

Questa operazione può essere eseguita se si desidera interrompere l'utilizzo di FabricPool su un volume o se si dispone di `snapshot-only` Tiering policy e vuoi riportare i dati di copia Snapshot ripristinati al Tier di performance.

#### Promuovi tutti i dati da un volume FabricPool al Tier di performance

Puoi recuperare in modo proattivo tutti i dati su un volume FabricPool nel cloud e promuoverli al livello di performance.

### Fase

1. Utilizzare `volume modify` comando da impostare `tiering-policy` a. `none` e. `cloud-retrieval-policy` a. `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

#### Promuovere i dati del file system al livello di performance

È possibile recuperare in modo proattivo i dati del file system attivi da una copia Snapshot ripristinata nel Tier cloud e promuoverli nel Tier di performance.

### Fase

1. Utilizzare `volume modify` comando da impostare `tiering-policy` a. `snapshot-only` e. `cloud-retrieval-policy` a. `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

#### Verifica lo stato di una promozione per i Tier di performance

È possibile controllare lo stato della promozione del Tier di performance per determinare quando l'operazione è completa.

### Fase

1. Utilizzare il volume `object-store` con il `tiering` opzione per controllare lo stato della promozione del tier di performance.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                 Vserver: vs1
                                  Volume: v1
                               Node Name: node1
                             Volume DSID: 1023
                          Aggregate Name: a1
                                   State: ready
                      Previous Run Status: completed
                 Aborted Exception Status: -
               Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                 Scanner Percent Complete: -
                      Scanner Current VBN: -
                         Scanner Max VBNs: -
      Time Waiting Scan will be scheduled: -
                          Tiering Policy: snapshot-only
     Estimated Space Needed for Promotion: -
                        Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                   Cloud Retrieve Policy: promote
```

#### Attivare la migrazione pianificata e il tiering

A partire da ONTAP 9.8, è possibile attivare una richiesta di scansione a più livelli in qualsiasi momento quando si preferisce non attendere la scansione a più livelli predefinita.

**Fase**

1. Utilizzare `volume object-store` con il `trigger` opzione per richiedere migrazione e tiering.

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

## Gestire i mirror FabricPool

### Panoramica di Manage FabricPool Mirrors

Per garantire che i dati siano accessibili negli archivi dati in caso di disastro e per consentire la sostituzione di un archivio dati, è possibile configurare un mirror FabricPool aggiungendo un secondo archivio dati per il Tier sincrono dei dati a due archivi dati . È possibile aggiungere un secondo archivio dati a configurazioni FabricPool nuove o esistenti, monitorare lo stato del mirror, visualizzare i dettagli del mirror FabricPool, promuovere un mirror e rimuovere un mirror. È necessario eseguire ONTAP 9.7 o versione successiva.

### Creare un mirror FabricPool

Per creare un mirror FabricPool, si allegano due archivi di oggetti a un singolo FabricPool. È possibile creare un mirror FabricPool allegando un secondo archivio di oggetti a una configurazione FabricPool esistente di un singolo archivio di oggetti oppure creare una nuova configurazione FabricPool di un singolo archivio di oggetti e quindi allegarvi un secondo archivio di oggetti. È inoltre possibile creare mirror FabricPool sulle configurazioni MetroCluster.

#### Di cosa hai bisogno

- È necessario aver già creato i due archivi di oggetti utilizzando `storage aggregate object-store config` comando.
- Se si creano mirror FabricPool su configurazioni MetroCluster:
  - È necessario aver già configurato e configurato MetroCluster
  - È necessario aver creato le configurazioni dell'archivio di oggetti sul cluster selezionato.

    Se si creano mirror FabricPool su entrambi i cluster in una configurazione MetroCluster, è necessario aver creato le configurazioni dell'archivio di oggetti su entrambi i cluster.

  - Se non si utilizzano archivi di oggetti on-premise per le configurazioni MetroCluster, è necessario verificare che esista uno dei seguenti scenari:
    - Gli archivi di oggetti si trovano in diverse zone di disponibilità
    - Gli archivi di oggetti sono configurati per conservare copie di oggetti in più zone di disponibilità

      "Impostazione degli archivi di oggetti per FabricPool in una configurazione MetroCluster"

#### A proposito di questa attività

L'archivio di oggetti utilizzato per il mirror FabricPool deve essere diverso dall'archivio di oggetti primario.

La procedura per la creazione di un mirror FabricPool è la stessa per le configurazioni MetroCluster e non MetroCluster.

#### Fasi

1. Se non si utilizza una configurazione FabricPool esistente, crearne una nuova allegando un archivio di oggetti a un aggregato utilizzando `storage aggregate object-store attach` comando.

   Questo esempio crea un nuovo FabricPool allegando un archivio di oggetti a un aggregato.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
my-store-1
```

2. Collegare un secondo archivio di oggetti all'aggregato utilizzando `storage aggregate object-store mirror` comando.

   In questo esempio viene collegato un secondo archivio di oggetti a un aggregato per creare un mirror FabricPool.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

#### Monitorare lo stato di risincronizzazione del mirror FabricPool

Quando si sostituisce un archivio di oggetti primario con un mirror, potrebbe essere necessario attendere la risincronizzazione del mirror con l'archivio di dati primario.

**A proposito di questa attività**

Se il mirror FabricPool è sincronizzato, non viene visualizzata alcuna voce.

**Fase**

1. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
      Aggregate    Primary       Mirror        Percentage
      ---------    -----------   ----------    ----------
      aggr1        my-store-1     my-store-2     40%
```

#### Visualizza i dettagli del mirror FabricPool

È possibile visualizzare i dettagli di un mirror FabricPool per visualizzare gli archivi di oggetti presenti nella configurazione e se il mirror dell'archivio di oggetti è sincronizzato con l'archivio di oggetti primario.

**Fase**

1. Visualizzare le informazioni su un mirror FabricPool utilizzando `storage aggregate object-store show` comando.

   In questo esempio vengono visualizzati i dettagli relativi agli archivi di oggetti primari e mirror in un mirror

FabricPool.

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

```
Aggregate      Object Store Name Availability    Mirror Type
-------------- ----------------- -------------   ----------
aggr1          my-store-1        available       primary
               my-store-2        available       mirror
```

Questo esempio mostra i dettagli sul mirror FabricPool, incluso se il mirror è degradato a causa di un'operazione di risincronizzazione.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

#### Promuovere un mirror FabricPool

È possibile riassegnare il mirror dell'archivio di oggetti come archivio di oggetti primario promuovendolo. Quando il mirror dell'archivio di oggetti diventa il principale, il principale originale diventa automaticamente il mirror.

##### Di cosa hai bisogno

- Il mirror FabricPool deve essere sincronizzato
- L'archivio di oggetti deve essere operativo

##### A proposito di questa attività

È possibile sostituire l'archivio di oggetti originale con un archivio di oggetti di un altro provider cloud. Ad esempio, il mirror originale potrebbe essere un archivio di oggetti AWS, ma è possibile sostituirlo con un archivio di oggetti Azure.

##### Fase

1. Promuovere un mirror dell'archivio di oggetti utilizzando `storage aggregate object-store modify -aggregate` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

### Rimuovere un mirror FabricPool

È possibile rimuovere un mirror FabricPool se non è più necessario replicare un archivio di oggetti.

#### Di cosa hai bisogno

L'archivio di oggetti primario deve essere operativo, altrimenti il comando non riesce.

#### Fase

1. Rimuovere un mirror dell'archivio di oggetti in un FabricPool utilizzando `storage aggregate object-store unmirror -aggregate` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

### Sostituire un archivio di oggetti esistente utilizzando un mirror FabricPool

È possibile utilizzare la tecnologia mirror FabricPool per sostituire un archivio di oggetti con un altro. Il nuovo archivio di oggetti non deve utilizzare lo stesso provider cloud dell'archivio di oggetti originale.

#### A proposito di questa attività

È possibile sostituire l'archivio di oggetti originale con un archivio di oggetti che utilizza un provider cloud diverso. Ad esempio, l'archivio di oggetti originale potrebbe utilizzare AWS come provider cloud, ma è possibile sostituirlo con un archivio di oggetti che utilizza Azure come provider cloud e viceversa. Tuttavia, il nuovo archivio di oggetti deve conservare le stesse dimensioni dell'oggetto originale.

#### Fasi

1. Creare un mirror FabricPool aggiungendo un nuovo archivio di oggetti a un FabricPool esistente utilizzando `storage aggregate object-store mirror` comando.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-AZURE-store
```

2. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                Complete
      Aggregate    Primary          Mirror        Percentage
      ---------    -----------      ----------    ----------
      aggr1        my-AWS-store     my-AZURE-store     40%
```

3. Verificare che il mirror sia sincronizzato utilizzando `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. Sostituire l'archivio di oggetti primario con l'archivio di oggetti mirror utilizzando `storage aggregate object-store modify` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-AZURE-store -mirror-type primary
```

5. Visualizzare i dettagli relativi al mirror FabricPool utilizzando `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

   In questo esempio vengono visualizzate le informazioni relative al mirror FabricPool, incluso se il mirror è danneggiato (non sincronizzato).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. Rimuovere il mirror FabricPool utilizzando `storage aggregate object-store unmirror` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Verificare che FabricPool sia di nuovo in una configurazione di archivio oggetti singolo utilizzando `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

#### Sostituire un mirror FabricPool in una configurazione MetroCluster

Se uno degli archivi di oggetti in un mirror FabricPool viene distrutto o diventa permanentemente non disponibile in una configurazione MetroCluster, è possibile rendere l'archivio di oggetti il mirror se non è già il mirror, rimuovere l'archivio di oggetti danneggiato dal mirror FabricPool, Quindi aggiungere un nuovo mirror dell'archivio di oggetti a FabricPool.

**Fasi**

1. Se l'archivio di oggetti danneggiato non è già il mirror, fare in modo che l'oggetto memorizzi il mirror con `storage aggregate object-store modify` comando.

   ```
   storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
   -name mcc1_ostore1 -mirror-type mirror
   ```

2. Rimuovere il mirror dell'archivio di oggetti da FabricPool utilizzando `storage aggregate object-store unmirror` comando.

   ```
   storage aggregate object-store unmirror -aggregate <aggregate name>
   -name mcc1_ostore1
   ```

3. È possibile forzare il ripristino del tiering nell'archivio dati principale dopo aver rimosso l'archivio dati mirror utilizzando `storage aggregate object-store modify` con `-force-tiering-on-metrocluster true` opzione.

   L'assenza di un mirror interferisce con i requisiti di replica di una configurazione MetroCluster.

   ```
   storage aggregate object-store modify -aggregate <aggregate name> -name
   mcc1_ostore1 -force-tiering-on-metrocluster true
   ```

4. Creare un archivio di oggetti sostitutivo utilizzando `storage aggregate object-store config create` comando.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Aggiungere il mirror dell'archivio di oggetti al mirror FabricPool utilizzando `storage aggregate object-store mirror` comando.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Visualizzare le informazioni sull'archivio di oggetti utilizzando `storage aggregate object-store show` comando.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary           -
               mcc1_ostore3-mc    mirror          true
```

7. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                                Complete
      Aggregate    Primary        Mirror         Percentage
      ---------    -----------    ----------     ----------
      aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

## Comandi per la gestione degli aggregati con FabricPool

Si utilizza `storage aggregate object-store` Comandi per gestire gli archivi di oggetti per FabricPool. Si utilizza `storage aggregate` Comandi per gestire gli aggregati per FabricPool. Si utilizza `volume` Comandi per gestire i volumi per FabricPool.

| Se si desidera… | Utilizzare questo comando: |
| --- | --- |
| Definire la configurazione per un archivio di oggetti in modo che ONTAP possa accedervi | `storage aggregate object-store config create` |
| Modificare gli attributi di configurazione dell'archivio di oggetti | `storage aggregate object-store config modify` |
| Rinominare una configurazione dell'archivio di oggetti esistente | `storage aggregate object-store config rename` |
| Eliminare la configurazione di un archivio di oggetti | `storage aggregate object-store config delete` |
| Visualizzare un elenco di configurazioni dell'archivio di oggetti | `storage aggregate object-store config show` |
| Collegare un secondo archivio di oggetti a un FabricPool nuovo o esistente come mirror | `storage aggregate object-store mirror` con `-aggregate` e. `-name` nel livello di privilegio admin |
| Rimuovere un mirror dell'archivio di oggetti da un mirror FabricPool esistente | `storage aggregate object-store unmirror` con `-aggregate` e. `-name` nel livello di privilegio admin |
| Monitorare lo stato di risincronizzazione del mirror FabricPool | `storage aggregate object-store show-resync-status` |
| Visualizza i dettagli del mirror FabricPool | `storage aggregate object-store show` |
| Promuovere un mirror dell'archivio di oggetti per sostituire un archivio di oggetti primario in una configurazione mirror FabricPool | `storage aggregate object-store modify` con `-aggregate` nel livello di privilegio admin |
| Verificare la latenza e le performance di un archivio di oggetti senza collegare l'archivio di oggetti a un aggregato | `storage aggregate object-store profiler start` con `-object-store-name` e. `-node` nel livello di privilegio avanzato |
| Monitorare lo stato del profiler dell'archivio di oggetti | `storage aggregate object-store profiler show` con `-object-store-name` e. `-node` nel livello di privilegio avanzato |
| Interrompere il profiler dell'archivio di oggetti quando è in esecuzione | `storage aggregate object-store profiler abort` con `-object-store-name` e. `-node` nel livello di privilegio avanzato |

| | |
|---|---|
| Collegare un archivio di oggetti a un aggregato per utilizzare FabricPool | `storage aggregate object-store attach` |
| Collegare un archivio di oggetti a un aggregato che contiene un volume FlexGroup per l'utilizzo di FabricPool | `storage aggregate object-store attach` con `allow-flexgroup true` |
| Visualizza i dettagli degli archivi di oggetti collegati agli aggregati abilitati per FabricPool | `storage aggregate object-store show` |
| Visualizza la soglia di fullness aggregata utilizzata dalla scansione di tiering | `storage aggregate object-store show` con `-fields tiering-fullness-threshold` nel livello di privilegio avanzato |
| Visualizza l'utilizzo dello spazio degli archivi di oggetti collegati agli aggregati abilitati per FabricPool | `storage aggregate object-store show-space` |
| Attiva la creazione di report dei dati inattivi su un aggregato non utilizzato per FabricPool | `storage aggregate modify` con `-is-inactive-data-reporting-enabled true` parametro |
| Visualizza se il reporting dei dati inattivi è attivato su un aggregato | `storage aggregate show` con `-fields is-inactive-data-reporting-enabled` parametro |
| Visualizza le informazioni sulla quantità di dati utente a freddo all'interno di un aggregato | `storage aggregate show-space` con `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parametro |
| Creare un volume per FabricPool, specificando quanto segue:<br>• La policy di tiering<br>• Il periodo di raffreddamento minimo di tiering (per `snapshot-only` oppure `auto` policy di tiering) | `volume create`<br>• Si utilizza `-tiering-policy` parametro per specificare il criterio di tiering.<br>• Si utilizza `-tiering-minimum-cooling-days` nel livello di privilegio avanzato per specificare il periodo minimo di raffreddamento del tiering. |
| Modificare un volume per FabricPool, modificando quanto segue:<br>• La policy di tiering<br>• Il periodo di raffreddamento minimo di tiering (per `snapshot-only` oppure `auto` policy di tiering) | `volume modify`<br>• Si utilizza `-tiering-policy` parametro per specificare il criterio di tiering.<br>• Si utilizza `-tiering-minimum-cooling-days` nel livello di privilegio avanzato per specificare il periodo minimo di raffreddamento del tiering. |

| | |
|---|---|
| Visualizzare le informazioni FabricPool relative a un volume, tra cui:<br>• Il periodo di raffreddamento minimo di tiering<br>• Quanti dati utente sono cold | `volume show`<br>• Si utilizza `-fields tiering-minimum-cooling-days` nel livello di privilegio avanzato per visualizzare il periodo minimo di raffreddamento del tiering.<br>• Si utilizza `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parametro per visualizzare la quantità di dati utente a freddo. |
| Consente di spostare un volume in entrata o in uscita da FabricPool | `volume move start` Si utilizza `-tiering-policy` parametro facoltativo per specificare il criterio di tiering per il volume. |
| Modificare la soglia per recuperare lo spazio senza riferimento (la soglia di deframmentazione) per FabricPool | `storage aggregate object-store modify` con `-unreclaimed-space-threshold` nel livello di privilegio avanzato |
| Modificare la soglia per la percentuale di pieno che l'aggregato diventa prima che la scansione del tiering inizi a tiering dei dati per FabricPool<br><br>FabricPool continua a eseguire il tiering dei dati cold su un Tier cloud fino a quando il Tier locale non raggiunge il 98% della capacità. | `storage aggregate object-store modify` con `-tiering-fullness-threshold` nel livello di privilegio avanzato |
| Visualizza la soglia per il recupero dello spazio senza riferimento per FabricPool | `storage aggregate object-store show` oppure `storage aggregate object-store show-space` con il `-unreclaimed-space -threshold` nel livello di privilegio avanzato |

# Mobilità dei dati SVM

## Panoramica sulla mobilità dei dati SVM

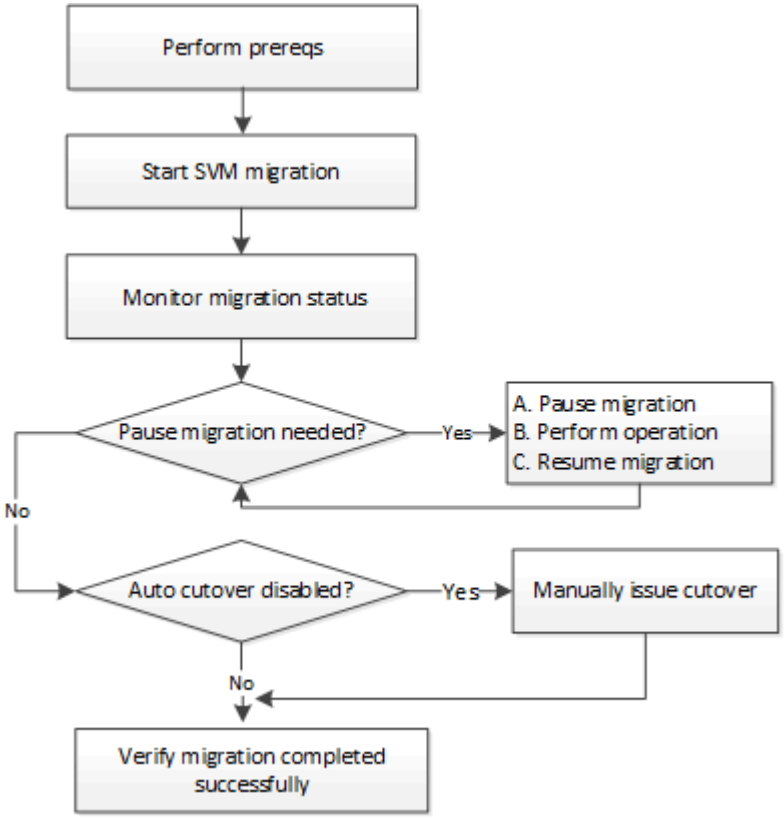
A partire da ONTAP 9.10.1, gli amministratori del cluster possono spostare senza interruzioni una SVM da un cluster di origine a un cluster di destinazione per gestire il bilanciamento della capacità e del carico, oppure per abilitare gli aggiornamenti delle apparecchiature o il consolidamento del data center utilizzando la CLI ONTAP.

Questa funzionalità di trasferimento SVM senza interruzioni è supportata sulle piattaforme AFF in ONTAP 9.10.1 e 9.11.1. A partire da ONTAP 9.12.1, questa funzionalità è supportata su piattaforme FAS e AFF e su aggregati ibridi.

Il nome e l'UUID di SVM rimangono invariati dopo la migrazione, oltre al nome LIF dei dati, all'indirizzo IP e ai nomi degli oggetti, come il nome del volume. L'UUID degli oggetti nella SVM sarà diverso.

### Workflow di migrazione SVM

Il diagramma illustra il tipico flusso di lavoro per una migrazione SVM. Viene avviata una migrazione SVM dal cluster di destinazione. È possibile monitorare la migrazione dall'origine o dalla destinazione. È possibile eseguire un cutover manuale o automatico. Per impostazione predefinita viene eseguito un cutover automatico.




### Supporto della piattaforma di migrazione SVM

| Famiglia di controller | Versioni di ONTAP supportate |
|---|---|
| AFF serie A. | ONTAP 9.10.1 e versioni successive |
| AFF serie C. | ONTAP 9.12.1 patch 4 e versioni successive |
| FAS | ONTAP 9.12.1 e versioni successive |

> Durante la migrazione da un cluster AFF a un cluster FAS con aggregati ibridi, il posizionamento automatico del volume tenterà di eseguire una corrispondenza simile a quella degli aggregati. Ad esempio, se il cluster di origine ha 60 volumi, il posizionamento del volume tenterà di trovare un aggregato AFF sulla destinazione per posizionare i volumi. In mancanza di spazio sufficiente sugli aggregati AFF, i volumi verranno collocati negli aggregati con dischi non flash.

### Supporto della scalabilità tramite la versione di ONTAP

| Versione di ONTAP | COPPIE HA in origine e destinazione |
|---|---|
| ONTAP 9.14.1 | 12 |
| ONTAP 9.13.1 | 6 |

| | |
|---|---|
| ONTAP 9.11.1 | 3 |
| ONTAP 9.10.1 | 1 |

### Requisiti di performance dell'infrastruttura di rete per il tempo di round trip TCP (RTT) tra il cluster di origine e di destinazione

A seconda della versione di ONTAP installata sul cluster, la rete che collega i cluster di origine e di destinazione deve avere un tempo massimo di andata e ritorno, come indicato di seguito:

| Versione di ONTAP | RTT massimo |
|---|---|
| ONTAP 9.12.1 e versioni successive | 10 ms. |
| ONTAP 9.11.1 e versioni precedenti | 2 ms. |

### Volumi massimi supportati per SVM

| Origine | Destinazione | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 e versioni precedenti |
|---|---|---|---|---|---|
| AFF | AFF | 400 | 200 | 100 | 100 |
| FAS | FAS | 80 | 80 | 80 | N/A. |
| FAS | AFF | 80 | 80 | 80 | N/A. |
| AFF | FAS | 80 | 80 | 80 | N/A. |

### Prerequisiti

Prima di iniziare una migrazione SVM, è necessario soddisfare i seguenti prerequisiti:

- Devi essere un amministratore del cluster.
- "I cluster di origine e di destinazione devono essere connessi in peering l'uno all'altro".
- I cluster di destinazione e di origine devono avere SnapMirror sincrono "licenza installata". Questa licenza è inclusa con "ONTAP uno".
- Tutti i nodi nel cluster di origine devono eseguire ONTAP 9.10.1 o versione successiva. Per informazioni sul supporto specifico dei controller di array ONTAP, vedere "Hardware Universe".
- Tutti i nodi nel cluster di origine devono eseguire la stessa versione di ONTAP.
- Tutti i nodi nel cluster di destinazione devono eseguire la stessa versione di ONTAP.
- Il cluster di destinazione deve essere uguale o non più di due importanti versioni effettive del cluster (ECV) del cluster di origine.
- I cluster di origine e di destinazione devono supportare la stessa subnet IP per l'accesso ai dati LIF.
- La SVM di origine deve contenere meno di numero massimo di volumi di dati supportati per la release.
- Sulla destinazione deve essere disponibile uno spazio sufficiente per il posizionamento del volume
- Onboard Key Manager deve essere configurato sulla destinazione se la SVM di origine ha volumi crittografati

### Best practice

Durante la migrazione delle SVM, è consigliabile lasciare il 30% di spazio a disposizione della CPU sia sul cluster di origine che su quello di destinazione per consentire l'esecuzione del workload della CPU.

### Operazioni SVM

È necessario controllare le operazioni che possono entrare in conflitto con una migrazione SVM:

- Non sono in corso operazioni di failover
- WAFLIRON non può essere in esecuzione
- Impronta digitale non in corso
- Vol move, rehosting, cloning, create, convert o analytics non sono in esecuzione

### Funzioni supportate e non supportate

La tabella indica le funzionalità di ONTAP supportate dalla mobilità dei dati SVM e le release di ONTAP in cui è disponibile il supporto.

| Funzione | Release supportata per la prima volta | Commenti |
|---|---|---|
| Protezione ransomware autonoma | ONTAP 9.12.1 | |
| Cloud Volumes ONTAP | Non supportato | |
| Gestore delle chiavi esterno | ONTAP 9.11.1 | |
| FabricPool | ONTAP 9.11.1 | Scopri di più Supporto FabricPool. |
| Relazione fanout (l'origine della migrazione ha un volume di origine SnapMirror con più di una destinazione) | ONTAP 9.11.1 | |
| SAN FC | Non supportato | |
| Flash Pool | ONTAP 9.12.1 | |
| Volumi FlexCache | Non supportato | |
| FlexGroup | Non supportato | |
| Criteri IPsec | Non supportato | |
| LIF IPv6 | Non supportato | |

| | | |
|---|---|---|
| SAN iSCSI | Non supportato | |
| Replica della pianificazione del processo | ONTAP 9.11.1 | In ONTAP 9.10.1, le pianificazioni dei processi non vengono replicate durante la migrazione e devono essere create manualmente sulla destinazione. A partire da ONTAP 9.11.1, le pianificazioni dei processi utilizzate dall'origine vengono replicate automaticamente durante la migrazione. |
| Mirror per la condivisione del carico | Non supportato | |
| SVM MetroCluster | Non supportato | Sebbene la migrazione SVM non supporti la migrazione MetroCluster SVM, potrebbe essere possibile utilizzare la replica asincrona SnapMirror in "Migrare una SVM in una configurazione MetroCluster". Tenere presente che il processo descritto per la migrazione di una SVM in una configurazione MetroCluster è *non* un metodo senza interruzioni. |
| NetApp aggregate Encryption (NAE) | Non supportato | La migrazione non è supportata da un'origine non crittografata a una destinazione crittografata. |
| Configurazioni NDMP | Non supportato | |
| NetApp Volume Encryption (NVE) | ONTAP 9.10.1 | |
| Registri di audit NFS e SMB | ONTAP 9.13.1 | Il reindirizzamento dei log di audit è disponibile solo in modalità cloud. Per la migrazione delle SVM on-premise con audit abilitato, devi disabilitare l'audit sulla SVM di origine ed eseguire la migrazione.<br><br>Prima della migrazione SVM:<br><br>• "Il reindirizzamento del log di audit deve essere abilitato sul cluster di destinazione".<br>• "Occorre creare il percorso di destinazione dell'audit log dalla SVM di origine nel cluster di destinazione". |
| NFS v3, NFS v4.1 e NFS v4.2 | ONTAP 9.10.1 | |
| NFS v4.0 | ONTAP 9.12.1 | |
| NFSv4,1 con pNFS | ONTAP 9.14.1 | |
| NVMe su fabric | Non supportato | |

| | | |
|---|---|---|
| Onboard Key Manager (OKM) con la modalità Common Criteria attivata sul cluster di origine | Non supportato | |
| Qtree | ONTAP 9.14.1 | |
| Quote | ONTAP 9.14.1 | |
| S3 | Non supportato | |
| Protocollo SMB | ONTAP 9.12.1 | Le migrazioni SMB sono un'interruzione e richiedono un refresh del client dopo la migrazione. |
| Relazioni di SnapMirror Cloud | ONTAP 9.12.1 | A partire da ONTAP 9.12.1, per migrare una SVM con relazioni SnapMirror Cloud, il cluster di destinazione deve disporre di "Licenza SnapMirror Cloud" installato e deve avere sufficiente capacità a disposizione per supportare lo spostamento della capacità nei volumi su cui viene eseguito il mirroring nel cloud. |
| Destinazione asincrona di SnapMirror | ONTAP 9.12.1 | |
| Fonte asincrona di SnapMirror | ONTAP 9.11.1 | • I trasferimenti possono continuare normalmente sulle relazioni di FlexVol SnapMirror durante la maggior parte della migrazione.<br>• Eventuali trasferimenti in corso vengono annullati durante il cutover e i nuovi trasferimenti falliscono durante il cutover e non possono essere riavviati fino al completamento della migrazione.<br>• I trasferimenti pianificati che sono stati annullati o persi durante la migrazione non vengono avviati automaticamente al termine della migrazione.<br>Al momento della migrazione di un'origine SnapMirror, ONTAP non impedisce la cancellazione del volume dopo la migrazione fino all'esecuzione dell'aggiornamento di SnapMirror. Questo si verifica perché le informazioni relative a SnapMirror per i volumi di origine di SnapMirror migrati sono disponibili solo al termine della migrazione e dopo il primo aggiornamento. |
| Impostazioni SMTape | Non supportato | |
| SnapLock | Non supportato | |

| | | |
|---|---|---|
| Continuità aziendale di SnapMirror | Non supportato | |
| Relazioni peer di SnapMirror SVM | ONTAP 9.12.1 | |
| Disaster recovery di SnapMirror SVM | Non supportato | |
| SnapMirror sincrono | Non supportato | |
| Copia Snapshot | ONTAP 9.10.1 | |
| Blocco delle copie Snapshot a prova di manomissione | ONTAP 9.14.1 | Il blocco delle copie Snapshot a prova di manomissione non è equivalente a SnapLock. SnapLock rimane non supportato. |
| LIF IP/BGP virtuali | Non supportato | |
| Virtual Storage Console 7.0 e versioni successive | Non supportato | VSC fa parte di "Strumenti ONTAP per appliance virtuali VMware vSphere" A partire da VSC 7.0. |
| Cloni di volume | Non supportato | |
| VStorage | Non supportato | |

#### Supporto FabricPool

La migrazione SVM è supportata con i volumi su FabricPools per le seguenti piattaforme:

- Piattaforma Azure NetApp Files. Sono supportati tutti i criteri di tiering (solo snapshot, automatico, tutti e nessuno).
- Piattaforma on-premise. È supportato solo il criterio di tiering del volume "nessuno".

### Operazioni supportate durante la migrazione

La seguente tabella indica le operazioni di volume supportate nella SVM in migrazione in base allo stato di migrazione:

| Funzionamento del volume | Stato di migrazione SVM | | |
|---|---|---|---|
| | **In corso** | **In pausa** | **Cutover** |
| Creare | Non consentito | Consentito | Non supportato |
| Eliminare | Non consentito | Consentito | Non supportato |
| Disattivazione di file System Analytics | Consentito | Consentito | Non supportato |
| Attivazione di file System Analytics | Non consentito | Consentito | Non supportato |
| Modificare | Consentito | Consentito | Non supportato |
| Offline/Online | Non consentito | Consentito | Non supportato |

| | | | |
|---|---|---|---|
| Spostare/eseguire nuovamente l'host | Non consentito | Consentito | Non supportato |
| Creazione/modifica qtree | Non consentito | Consentito | Non supportato |
| Creazione/modifica quota | Non consentito | Consentito | Non supportato |
| Rinominare | Non consentito | Consentito | Non supportato |
| Ridimensionare | Consentito | Consentito | Non supportato |
| Limitare | Non consentito | Consentito | Non supportato |
| Modifica degli attributi della copia Snapshot | Consentito | Consentito | Non supportato |
| Modifica dell'eliminazione automatica della copia Snapshot | Consentito | Consentito | Non supportato |
| Creazione della copia Snapshot | Consentito | Consentito | Non supportato |
| Eliminazione della copia Snapshot | Consentito | Consentito | Non supportato |
| Ripristinare il file dalla copia Snapshot | Consentito | Consentito | Non supportato |

## Migrare una SVM

Al termine di una migrazione SVM, i client vengono tagliati automaticamente nel cluster di destinazione e la SVM non necessaria viene rimossa dal cluster di origine. Il cutover automatico e il cleanup automatico della sorgente sono attivati per impostazione predefinita. Se necessario, è possibile disattivare il cutover automatico del client per sospendere la migrazione prima che si verifichi il cutover ed è anche possibile disattivare il cleanup SVM di origine automatico.

- È possibile utilizzare `-auto-cutover false` opzione per sospendere la migrazione quando normalmente si verifica il cutover automatico del client e quindi eseguire manualmente il cutover in un secondo momento.

  Cutover manuale dei client dopo la migrazione SVM

- È possibile utilizzare il privilegio Advance `-auto-source-cleanup false` Opzione per disattivare la rimozione della SVM di origine dopo il cutover e quindi attivare manualmente la pulitura della sorgente in un secondo momento, dopo il cutover.

  Rimuovere manualmente la SVM di origine dopo il cutover

### Migrare una SVM con il cutover automatico attivato

Per impostazione predefinita, i client vengono tagliati automaticamente nel cluster di destinazione al termine della migrazione e la SVM non necessaria viene rimossa dal cluster di origine.

#### Fasi

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. Dal cluster di destinazione, avviare la migrazione SVM:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name
   ```

3. Controllare lo stato della migrazione:

   ```
   dest_cluster> vserver migrate show
   ```

   Lo stato visualizza Migrate-complete (migrazione completata) al termine della migrazione SVM.

### Migrare una SVM con il cutover automatico del client disattivato

È possibile utilizzare l'opzione -auto-cutover false per sospendere la migrazione quando si verifica normalmente un cutover automatico del client e quindi eseguire manualmente il cutover in un secondo momento. Vedere Cutover manuale dei client dopo la migrazione SVM.

**Fasi**

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. Dal cluster di destinazione, avviare la migrazione SVM:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-cutover false
   ```

3. Controllare lo stato della migrazione:

   `dest_cluster> vserver migrate show`Lo stato visualizza Ready-for-cutover quando la migrazione SVM completa i trasferimenti di dati asincroni ed è pronta per l'operazione di cutover.

### Migrazione di una SVM con pulitura origine disattivata

È possibile utilizzare l'opzione Advance Privilege -auto-source-cleanup false per disattivare la rimozione della SVM di origine dopo il cutover e quindi attivare manualmente la pulitura della sorgente in un secondo momento, dopo il cutover. Vedere Rimuovere manualmente SVM di origine.

**Fasi**

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. Dal cluster di destinazione, avviare la migrazione SVM:

   ```
   dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-source-cleanup false
   ```

3. Controllare lo stato della migrazione:

   ```
   dest_cluster*> vserver migrate show
   ```

Lo stato visualizza Ready-for-source-cleanup quando la migrazione SVM è completa ed è pronto per rimuovere SVM sul cluster di origine.

## Monitorare la migrazione dei volumi

Oltre a monitorare la migrazione SVM complessiva con `vserver migrate show` È possibile monitorare lo stato di migrazione dei volumi contenuti nella SVM.

**Fasi**

1. Controllare lo stato della migrazione del volume:

```
dest_clust> vserver migrate show-volume
```

## Sospendere e riprendere la migrazione SVM

Potrebbe essere necessario sospendere una migrazione SVM prima dell'inizio del cutover della migrazione. È possibile sospendere una migrazione SVM utilizzando `vserver migrate pause` comando.

### Sospendere la migrazione

È possibile sospendere una migrazione SVM prima dell'avvio del cutover del client utilizzando `vserver migrate pause` comando.

Alcune modifiche alla configurazione sono limitate quando è in corso un'operazione di migrazione; tuttavia, a partire da ONTAP 9.12.1, è possibile sospendere una migrazione per correggere alcune configurazioni limitate e alcuni stati non riusciti, in modo da risolvere i problemi di configurazione che potrebbero aver causato l'errore. Alcuni degli stati di errore che è possibile correggere quando si interrompe la migrazione SVM includono:

- setup-configuration-failed. (configurazione non riuscita.
- migrazione non riuscita

**Fasi**

1. Dal cluster di destinazione, sospendere la migrazione:

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

### Riprendere le migrazioni

Quando si è pronti a riprendere una migrazione SVM in pausa o quando una migrazione SVM non è riuscita, è possibile utilizzare `vserver migrate resume` comando.

**Fase**

1. Riprendere la migrazione SVM:

```
dest_cluster> vserver migrate resume
```

2. Verificare che la migrazione SVM sia stata ripresa e monitorare l'avanzamento:

```
dest_cluster> vserver migrate show
```

## Annullare una migrazione SVM

Se è necessario annullare una migrazione SVM prima del completamento, è possibile utilizzare `vserver migrate abort` comando. È possibile annullare una migrazione SVM solo quando l'operazione è in stato di pausa o non riuscita. Non è possibile annullare una migrazione SVM quando lo stato è "cutover-started" (cutover avviato) o dopo il completamento del cutover. Non è possibile utilizzare `abort` Opzione quando è in corso una migrazione SVM.

**Fasi**

1. Controllare lo stato della migrazione:

   ```
   dest_cluster> vserver migrate show -vserver <vserver name>
   ```

2. Annullare la migrazione:

   ```
   dest_cluster> vserver migrate abort -vserver <vserver name>
   ```

3. Verificare l'avanzamento dell'operazione di annullamento:

   ```
   dest_cluster> vserver migrate show
   ```

   Lo stato della migrazione mostra l'interruzione della migrazione mentre l'operazione di annullamento è in corso. Al termine dell'operazione di annullamento, lo stato della migrazione non mostra nulla.

## Tagliare manualmente i client

Per impostazione predefinita, il cutover del client al cluster di destinazione viene eseguito automaticamente quando la migrazione SVM raggiunge lo stato "ready-for-cutover". Se si sceglie di disattivare il cutover automatico del client, è necessario eseguire manualmente il cutover del client.

**Fasi**

1. Eseguire manualmente il cutover del client:

   ```
   dest_cluster> vserver migrate cutover -vserver <vserver name>
   ```

2. Controllare lo stato dell'operazione di cutover:

   ```
   dest_cluster> vserver migrate show
   ```

## Rimuovere manualmente la SVM di origine dopo il cutover del client

Se è stata eseguita la migrazione SVM con la pulitura del codice sorgente disattivata, è possibile rimuovere manualmente la SVM di origine al termine del cutover del client.

**Fasi**

1. Verificare che lo stato sia pronto per la pulizia della sorgente:

   ```
   dest_cluster> vserver migrate show
   ```

2. Pulire la fonte:

   ```
   dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
   ```

# Gestione delle coppie HA

## Panoramica sulla gestione delle coppie HA

I nodi del cluster sono configurati in coppie ad alta disponibilità (ha) per la fault tolerance e le operazioni senza interruzioni. Se un nodo si guasta o se è necessario interrompere un nodo per la manutenzione ordinaria, il partner può assumere il controllo dello storage e continuare a fornire i dati da esso. Il partner restituisce lo storage quando il nodo viene riportato on-line.

La configurazione del Pair Controller ha è costituita da una coppia di storage controller FAS/AFF corrispondenti (nodo locale e nodo partner). Ciascuno di questi nodi è collegato agli shelf di dischi dell'altro. Quando un nodo di una coppia ha rileva un errore e interrompe l'elaborazione dei dati, il partner rileva lo stato di errore del partner e rileva tutte le elaborazioni dei dati da quel controller.

*Takeover* è il processo in cui un nodo assume il controllo dello storage del partner.

*Giveback* è il processo in cui lo storage viene restituito al partner.

Per impostazione predefinita, i takeover si verificano automaticamente in una delle seguenti situazioni:

- Si verifica un errore di software o di sistema su un nodo che porta a un panico. I controller di coppia ha eseguono automaticamente il failover nel nodo partner. Una volta che il partner si è ripristinato dal panico e si è avviato, il nodo esegue automaticamente un giveback, riportando il partner al normale funzionamento.
- Si verifica un errore di sistema su un nodo e il nodo non può essere riavviato. Ad esempio, quando un nodo si guasta a causa di una perdita di alimentazione, i controller di coppia ha eseguono automaticamente il failover nel nodo partner e distribuiscono i dati dal controller di storage sopravvissuto.

> Se anche lo storage di un nodo perde alimentazione contemporaneamente, non è possibile eseguire un takeover standard.

- I messaggi heartbeat non vengono ricevuti dal partner del nodo. Ciò potrebbe verificarsi se il partner ha riscontrato un errore hardware o software (ad esempio, un errore di interconnessione) che non ha causato panico ma ha comunque impedito il corretto funzionamento.
- Arrestare uno dei nodi senza utilizzare `-f` oppure `-inhibit-takeover true` parametro.

> In un cluster a due nodi con cluster ha attivato, arrestare o riavviare un nodo utilizzando `-inhibit-takeover true` Il parametro causa l'interruzione della fornitura dei dati da parte di entrambi i nodi, a meno che non venga prima disattivata la disponibilità del cluster e quindi assegnata l'epsilon al nodo che si desidera mantenere in linea.

- Riavviare uno dei nodi senza utilizzare `-inhibit-takeover true` parametro. (Il `-onboot` del parametro

`storage failover` il comando è attivato per impostazione predefinita).

- Il dispositivo di gestione remota (Service Processor) rileva un errore del nodo partner. Questa opzione non è applicabile se si disattiva il Takeover assistito dall'hardware.

È inoltre possibile avviare manualmente le operazioni di takeover con `storage failover takeover` comando.

#### Resilienza del cluster e miglioramenti diagnostici

A partire da ONTAP 9,9.1, le seguenti aggiunte di resilienza e diagnostica migliorano il funzionamento del cluster:

- **Monitoraggio ed esclusione delle porte**: Nelle configurazioni cluster senza switch a due nodi, il sistema evita le porte che subiscono la perdita totale dei pacchetti (perdita di connettività). In ONTAP 9.8.1 e versioni precedenti, questa funzionalità era disponibile solo nelle configurazioni con switch.
- **Failover automatico dei nodi**: Se un nodo non è in grado di fornire dati attraverso la rete cluster, tale nodo non deve possedere alcun disco. Il partner ha dovrebbe invece assumere il controllo, se il partner è in buona salute.
- **Comandi per analizzare i problemi di connettività**: Utilizzare il seguente comando per visualizzare i percorsi del cluster in cui si verificano perdite di pacchetti: `network interface check cluster-connectivity show`

## Come funziona il Takeover assistito dall'hardware

Attivata per impostazione predefinita, la funzione di Takeover assistita dall'hardware può accelerare il processo di Takeover utilizzando il dispositivo di gestione remota di un nodo (Service Processor).

Quando il dispositivo di gestione remota rileva un guasto, avvia rapidamente il rilevamento piuttosto che attendere che ONTAP riconosca che il battito cardiaco del partner si è arrestato. Se si verifica un errore senza che questa funzione sia attivata, il partner attende fino a quando non rileva che il nodo non sta più dando un heartbeat, conferma la perdita di heartbeat, quindi avvia il takeover.

La funzionalità di Takeover assistita dall'hardware utilizza il seguente processo per evitare tale attesa:

1. Il dispositivo di gestione remota monitora il sistema locale per rilevare determinati tipi di guasti.
2. Se viene rilevato un errore, il dispositivo di gestione remota invia immediatamente un avviso al nodo partner.
3. Una volta ricevuto l'avviso, il partner avvia la presa in consegna.

#### Eventi di sistema che attivano il Takeover assistito dall'hardware

Il nodo partner potrebbe generare un Takeover a seconda del tipo di avviso ricevuto dal dispositivo di gestione remota (Service Processor).

| Avviso | Acquisizione avviata al ricevimento? | Descrizione |
|---|---|---|
| abnormal_reboot | No | Si è verificato un riavvio anomalo del nodo. |

| | | |
|---|---|---|
| l2_watchdog_reset | Sì | L'hardware del watchdog di sistema ha rilevato un ripristino L2. Il dispositivo di gestione remota ha rilevato una mancanza di risposta dalla CPU di sistema e ha ripristinato il sistema. |
| perdita di heartbeat | No | Il dispositivo di gestione remota non riceve più il messaggio heartbeat dal nodo. Questo avviso non fa riferimento ai messaggi heartbeat tra i nodi della coppia ha; si riferisce al heartbeat tra il nodo e il dispositivo di gestione remota locale. |
| messaggio_periodico | No | Viene inviato un messaggio periodico durante una normale operazione di Takeover assistita dall'hardware. |
| power_cycle_via_sp | Sì | Il dispositivo di gestione remota ha spento e riacceso il sistema. |
| power_loss | Sì | Si è verificata una perdita di alimentazione nel nodo. Il dispositivo di gestione remota dispone di un alimentatore che mantiene l'alimentazione per un breve periodo dopo un'interruzione dell'alimentazione, consentendo di segnalare al partner l'interruzione dell'alimentazione. |
| power_off_via_sp | Sì | Il dispositivo di gestione remota ha spento il sistema. |
| reset_via_sp | Sì | Il dispositivo di gestione remota ripristina il sistema. |
| test | No | Viene inviato un messaggio di test per verificare un'operazione di Takeover assistita dall'hardware. |

## Come funziona il Takeover e il giveback automatico

Le operazioni automatiche di Takeover e giveback possono lavorare insieme per ridurre ed evitare le interruzioni dei client.

Per impostazione predefinita, se un nodo della coppia ha esegue il panic, il riavvio o l'arresto, il nodo partner assume automaticamente il controllo e restituisce lo storage al riavvio del nodo interessato. La coppia ha riprende quindi uno stato operativo normale.

Le acquisizioni automatiche possono verificarsi anche se uno dei nodi non risponde.

Il giveback automatico viene eseguito per impostazione predefinita. Se si desidera controllare l'impatto del giveback sui client, è possibile disattivare il giveback automatico e utilizzare `storage failover modify -auto-giveback false -node <node>` comando. Prima di eseguire il giveback automatico (indipendentemente da ciò che lo ha attivato), il nodo partner attende un periodo di tempo fisso, come controllato da `-delay- seconds` del parametro `storage failover modify` comando. Il ritardo predefinito è di 600 secondi. Ritardando il giveback, il processo si traduce in due brevi interruzioni: Una durante il takeover e una durante il giveback.

Questo processo evita un singolo e prolungato disservizio che include il tempo necessario per:

- Operazione di Takeover
- Il nodo preso in consegna per l'avvio fino al punto in cui è pronto per il giveback

- L'operazione di giveback

Se il giveback automatico non riesce per uno qualsiasi degli aggregati non root, il sistema effettua automaticamente due tentativi aggiuntivi per completare il giveback.

> Durante il processo di takeover, il processo di giveback automatico inizia prima che il nodo partner sia pronto per il giveback. Quando il limite di tempo del processo di giveback automatico scade e il nodo partner non è ancora pronto, il timer viene riavviato. Di conseguenza, il tempo che intercorre tra il nodo partner pronto e l'effettivo giveback eseguito potrebbe essere inferiore al tempo di giveback automatico.

**Cosa succede durante il takeover**

Quando un nodo assume il controllo del proprio partner, continua a fornire e aggiornare i dati negli aggregati e nei volumi del partner.

Durante il processo di Takeover si verificano le seguenti fasi:

1. Se il Takeover negoziato è avviato dall'utente, i dati aggregati vengono spostati dal nodo partner al nodo che sta eseguendo il Takeover. Una breve interruzione si verifica quando il proprietario corrente di ciascun aggregato (ad eccezione dell'aggregato root) passa al nodo di Takeover. Questa interruzione è più breve di un'interruzione che si verifica durante un'acquisizione senza ricollocazione aggregata.

   > Un takover negoziato durante il panico non può verificarsi in caso di panico. Un takeover può derivare da un errore non associato a un panico. Si verifica un errore quando la comunicazione tra un nodo e il suo partner viene persa, chiamata anche perdita heartbeat. In caso di takeover a causa di un guasto, l'interruzione potrebbe essere più lunga poiché il nodo partner ha bisogno di tempo per rilevare la perdita di heartbeat.

   - È possibile monitorare l'avanzamento utilizzando `storage failover show-takeover` comando.
   - È possibile evitare il trasferimento dell'aggregato durante questa istanza di Takeover utilizzando `-bypass-optimization` con il `storage failover takeover` comando.

     Gli aggregati vengono ricollocati in modo seriale durante le operazioni di Takeover pianificate per ridurre l'interruzione del servizio del client. Se il trasferimento aggregato viene ignorato, si verifica un'interruzione più lunga del client durante gli eventi di acquisizione pianificati.

2. Se il Takeover avviato dall'utente è un Takeover negoziato, il nodo di destinazione si spegne senza problemi, seguito dal Takeover dell'aggregato root del nodo di destinazione e degli aggregati che non sono stati ricollocati nella fase 1.
3. Le interfacce logiche (LIF) dei dati migrano dal nodo di destinazione al nodo di takeover o a qualsiasi altro nodo del cluster in base alle regole di failover della LIF. È possibile evitare la migrazione LIF utilizzando `-skip-lif-migration` con il `storage failover takeover` comando. In caso di takeover avviato dall'utente, le LIF dati vengono migrate prima dell'inizio del takeover dello storage. In caso di panico o guasto, le LIF dati e lo storage vengono migrati insieme.
4. Le sessioni SMB esistenti vengono disconnesse quando si verifica il takeover.

> A causa della natura del protocollo SMB, tutte le sessioni SMB vengono interrotte (ad eccezione delle sessioni SMB 3.0 connesse alle condivisioni con il set di proprietà Continuous Availability). Le sessioni SMB 1.0 e SMB 2.x non possono riconnettersi dopo un evento di Takeover; pertanto, il Takeover è un'interruzione e potrebbe verificarsi una perdita di dati.

5. Le sessioni SMB 3.0 stabilite per le condivisioni con la proprietà disponibilità continua attivata possono riconnettersi alle condivisioni disconnesse dopo un evento di Takeover. Se il sito utilizza connessioni SMB 3.0 a Microsoft Hyper-V e la proprietà disponibilità continua è attivata sulle condivisioni associate, le acquisizioni non sono disruptive per tali sessioni.

#### Cosa succede se un nodo che esegue una panoramica di Takeover

Se il nodo che esegue il takeover esegue il panic entro 60 secondi dall'inizio del takeover, si verificano i seguenti eventi:

- Il nodo che ha avviato il panico si riavvia.
- Dopo il riavvio, il nodo esegue le operazioni di ripristino automatico e non è più in modalità Takeover.
- Il failover è disattivato.
- Se il nodo possiede ancora alcuni aggregati del partner, dopo aver attivato il failover dello storage, restituire questi aggregati al partner utilizzando `storage failover giveback` comando.

### Cosa succede durante il giveback

Il nodo locale restituisce la proprietà al nodo partner quando i problemi vengono risolti, quando il nodo partner si avvia o quando viene avviato il giveback.

Il seguente processo viene eseguito in una normale operazione di giveback. In questa discussione, il nodo A ha assunto il controllo del nodo B. Tutti i problemi sul nodo B sono stati risolti ed è pronto per riprendere la fornitura dei dati.

1. Tutti i problemi sul nodo B vengono risolti e viene visualizzato il seguente messaggio: `Waiting for giveback`
2. Il giveback viene avviato da `storage failover giveback` o tramite giveback automatico se il sistema è configurato per esso. Questo avvia il processo di restituzione della proprietà degli aggregati e dei volumi del nodo B dal nodo A al nodo B.
3. Il nodo A restituisce prima il controllo dell'aggregato root.
4. Il nodo B completa il processo di avvio fino al suo normale stato operativo.
5. Non appena il nodo B raggiunge il punto del processo di boot in cui può accettare gli aggregati non root, il nodo A restituisce la proprietà degli altri aggregati, uno alla volta, fino al completamento del giveback. È possibile monitorare l'avanzamento del giveback utilizzando `storage failover show-giveback` comando.

> Il `storage failover show-giveback` command non visualizza (né intende) informazioni su tutte le operazioni che si verificano durante l'operazione di giveback di failover dello storage. È possibile utilizzare `storage failover show` per visualizzare ulteriori dettagli sullo stato di failover corrente del nodo, ad esempio se il nodo è completamente funzionante, è possibile eseguire il takeover e il giveback è completo.

I/o riprende per ciascun aggregato dopo il completamento del giveback per quell'aggregato, riducendo così

la finestra generale di interruzione.

### Ha e il suo effetto sull'acquisizione e sul giveback

ONTAP assegna automaticamente a un aggregato una policy ha di CFO (failover del controller) e SFO (failover dello storage). Questo criterio determina il modo in cui avvengono le operazioni di failover dello storage per l'aggregato e i suoi volumi.

Le due opzioni, CFO e SFO, determinano la sequenza di controllo aggregata utilizzata da ONTAP durante le operazioni di giveback e failover dello storage.

Sebbene i termini CFO e SFO siano talvolta utilizzati in modo informale per fare riferimento alle operazioni di failover dello storage (takeover e giveback), essi rappresentano effettivamente la policy ha assegnata agli aggregati. Ad esempio, i termini aggregato SFO o aggregato CFO si riferiscono semplicemente all'assegnazione dei criteri ha dell'aggregato.

Le policy DI HA influiscono sulle operazioni di takeover e giveback come segue:

- Gli aggregati creati sui sistemi ONTAP (ad eccezione dell'aggregato root contenente il volume root) hanno una policy di ha di SFO. Il Takeover avviato manualmente è ottimizzato per le performance trasferendo gli aggregati SFO (non root) in modo seriale al partner prima del Takeover. Durante il processo di giveback, gli aggregati vengono restituiti in modo seriale dopo l'avvio del sistema acquisito e l'accesso alle applicazioni di gestione, consentendo al nodo di ricevere i propri aggregati.
- Poiché le operazioni di riposizionamento degli aggregati comportano la riassegnazione della proprietà dei dischi aggregati e lo spostamento del controllo da un nodo al suo partner, solo gli aggregati con una policy di ha di SFO sono idonei per il riposizionamento degli aggregati.
- L'aggregato root ha sempre una policy di ha di CFO e viene restituita all'inizio dell'operazione di giveback. Ciò è necessario per consentire l'avvio del sistema preso in consegna. Tutti gli altri aggregati vengono restituiti in modo seriale dopo che il sistema acquisito ha completato il processo di boot e le applicazioni di gestione sono online, consentendo al nodo di ricevere i propri aggregati.

> La modifica della policy ha di un aggregato da SFO a CFO è un'operazione in modalità Maintenance. Non modificare questa impostazione a meno che non sia richiesto da un rappresentante dell'assistenza clienti.

### In che modo gli aggiornamenti in background influiscono su Takeover e giveback

Gli aggiornamenti in background del firmware del disco influiscono in modo diverso sulle operazioni di takeover, giveback e trasferimento degli aggregati della coppia ha, a seconda di come vengono avviate tali operazioni.

Il seguente elenco descrive come gli aggiornamenti del firmware dei dischi in background influiscono su Takeover, giveback e trasferimento degli aggregati:

- Se si verifica un aggiornamento del firmware del disco in background su un disco su uno dei nodi, le operazioni di Takeover avviate manualmente vengono ritardate fino al completamento dell'aggiornamento del firmware del disco su tale disco. Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di Takeover vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco. Se l'acquisizione è stata avviata con `-bypass -optimization` del parametro `storage failover takeover` comando impostato su `true`, l'aggiornamento del firmware del disco in background che si verifica sul nodo di destinazione non influisce sul takeover.

- Se si verifica un aggiornamento del firmware del disco in background su un disco nel nodo di origine (o Takeover) e il Takeover è stato avviato manualmente con `-options` del parametro `storage failover takeover` comando impostato su `immediate`, le operazioni di takeover iniziano immediatamente.
- Se si verifica un aggiornamento del firmware del disco in background su un disco di un nodo e si verifica una situazione di panico, l'acquisizione del nodo in panello inizia immediatamente.
- Se si verifica un aggiornamento del firmware del disco in background su un disco su uno dei nodi, il giveback degli aggregati di dati viene ritardato fino al completamento dell'aggiornamento del firmware del disco su tale disco.
- Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di giveback vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco.
- Se si verifica un aggiornamento del firmware del disco in background su un disco di uno dei nodi, le operazioni di trasferimento aggregato vengono ritardate fino al completamento dell'aggiornamento del firmware del disco su tale disco. Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di trasferimento aggregato vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco. Se è stato avviato il trasferimento di aggregati con `-override-destination-checks` di `storage aggregate relocation` comando impostato su `true`, l'aggiornamento del firmware del disco in background che si verifica sul nodo di destinazione non influisce sul trasferimento dell'aggregato.

## Comandi di Takeover automatico

Il Takeover automatico è attivato per impostazione predefinita su tutte le piattaforme NetApp FAS, AFF e ASA supportate. Potrebbe essere necessario modificare il comportamento e il controllo predefiniti quando si verificano ripristini automatici quando il nodo partner si riavvia, esegue una panoramica o si arresta.

| Se si desidera che l'acquisizione avvenga automaticamente quando il nodo partner… | Utilizzare questo comando… |
|---|---|
| Si riavvia o si arresta | `storage failover modify -node nodename -onreboot true` |
| Panoramica | `storage failover modify -node nodename -onpanic true` |

#### Attivare la notifica via email se la funzionalità di Takeover è disattivata

Per ricevere una notifica rapida in caso di disattivazione della funzionalità di Takeover, configurare il sistema in modo da abilitare la notifica automatica via email per i messaggi EMS "Takeover impossible":

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`

- `ha.takeoverImpNotDef`

## Comandi di giveback automatici

Per impostazione predefinita, il nodo partner take-over restituisce automaticamente lo storage quando il nodo off-line viene riportato in linea, ripristinando così la relazione di coppia ad alta disponibilità. Nella maggior parte dei casi, questo è il comportamento desiderato. Se è necessario disattivare il giveback automatico, ad esempio se si desidera esaminare la causa del takeover prima di restituirgli, è necessario essere consapevoli dell'interazione delle impostazioni non predefinite.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Abilitare il giveback automatico in modo che il giveback avvenga non appena il nodo preso in consegna si avvia, raggiunga lo stato Waiting for Giveback (in attesa di giveback) e il periodo Delay before Auto Giveback (ritardo prima del giveback automatico) sia scaduto.<br><br>L'impostazione predefinita è true. | `storage failover modify -node` *`nodename`* `-auto-giveback true` |
| Disattiva il giveback automatico. L'impostazione predefinita è true.<br><br>**Nota:** l'impostazione di questo parametro su false non disattiva il giveback automatico dopo il takeover in panic; il giveback automatico dopo il takeover in panic deve essere disattivato impostando il `-auto -giveback-after-panic` parametro su false. | `storage failover modify -node` *`nodename`* `-auto-giveback false` |
| Disattiva il giveback automatico dopo il takeover in panic (questa impostazione è attivata per impostazione predefinita). | `storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false` |
| Ritarda il giveback automatico per un numero di secondi specificato (l'impostazione predefinita è 600). Questa opzione determina il tempo minimo in cui un nodo rimane in fase di Takeover prima di eseguire un giveback automatico. | `storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`* |

#### In che modo le variazioni del comando di modifica del failover dello storage influiscono sul giveback automatico

Il funzionamento del giveback automatico dipende dalla modalità di configurazione dei parametri del comando di modifica del failover dello storage.

La seguente tabella elenca le impostazioni predefinite per `storage failover modify` parametri di comando che si applicano agli eventi di takeover non causati da un panico.

| Parametro | Impostazione predefinita |
| --- | --- |
| `-auto-giveback *true* | *false*` |
| `*true*` | `-delay-seconds *integer* (seconds)` |
| 600 | `-onreboot *true* |
| *false*` | `*true*` |

La seguente tabella descrive le combinazioni di `-onreboot` e. `-auto-giveback` i parametri influiscono sul giveback automatico per gli eventi di takeover non causati da un panico.

| `storage failover modify` parametri utilizzati | Causa dell'acquisizione | Si verifica il giveback automatico? |
| --- | --- | --- |
| `-onreboot *true*`<br><br>`-auto-giveback *true*` | comando reboot | Sì |
| Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor | Sì | `-onreboot *true*`<br><br>`-auto-giveback *false*` |
| comando reboot | Sì | Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor |
| No | `-onreboot *false*`<br><br>`-auto-giveback *true*` | comando reboot |
| N/D in questo caso, l'acquisizione non avviene | Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor | Sì |
| `-onreboot *false*`<br><br>`-auto-giveback *false*` | comando reboot | No |

Il `-auto-giveback` i controlli dei parametri vengono ripristinati dopo il panic e tutti gli altri takover automatici. Se il `-onreboot` il parametro è impostato su `true` e un takeover si verifica a causa di un riavvio, quindi viene sempre eseguito il giveback automatico, indipendentemente dal fatto che il `-auto-giveback` il parametro è impostato su `true`.

Il `-onreboot` Il parametro si applica ai comandi di riavvio e arresto emessi da ONTAP. Quando il `-onreboot` il parametro è impostato su false, non si verifica un takeover in caso di riavvio di un nodo. Pertanto, non è

possibile eseguire il giveback automatico, indipendentemente dal fatto che il `-auto-giveback` il parametro è impostato su true. Si verifica un'interruzione del client.

**Gli effetti delle combinazioni di parametri di giveback automatico che si applicano alle situazioni di panico.**

La seguente tabella elenca `storage failover modify` parametri dei comandi applicabili alle situazioni di emergenza:

| Parametro | Impostazione predefinita |
|---|---|
| `-onpanic _true | false_` |
| *`true`* | `-auto-giveback-after-panic _true |
| false_`<br><br>(Privilegio: Avanzato) | *`true`* |
| `-auto-giveback _true | false_` |

La seguente tabella descrive le combinazioni di parametri di `storage failover modify` il comando influisce sul giveback automatico in situazioni di panico.

| `storage failover` parametri utilizzati | Il giveback automatico si verifica dopo il panico? |
|---|---|
| `-onpanic true`<br>`-auto-giveback true`<br>`-auto-giveback-after-panic true` | Sì |
| `-onpanic true`<br>`-auto-giveback true`<br>`-auto-giveback-after-panic false` | Sì |
| `-onpanic true`<br>`-auto-giveback false`<br>`-auto-giveback-after-panic true` | Sì |
| `-onpanic true`<br>`-auto-giveback false`<br>`-auto-giveback-after-panic false` | No |
| `-onpanic false`Se `-onpanic` è impostato su `false`, il takeover/giveback non si verifica, indipendentemente dal valore impostato per `-auto-giveback` oppure `-auto-giveback -after-panic` | No |

> Un takeover può derivare da un errore non associato a un panico. Si verifica un *guasto* quando la comunicazione tra un nodo e il suo partner viene persa, chiamata anche *perdita heartbeat*. Se si verifica un Takeover a causa di un guasto, il giveback viene controllato da `-onfailure` invece di `-auto-giveback-after-panic parameter`.

> Quando un nodo viene preso in panica, invia un pacchetto panic al nodo partner. Se per qualsiasi motivo il pacchetto panic non viene ricevuto dal nodo partner, il panic può essere interpretato erroneamente come un errore. Senza la ricezione del pacchetto panic, il nodo partner sa solo che la comunicazione è stata persa e non sa che si è verificato un panico. In questo caso, il nodo partner elabora la perdita di comunicazione come un errore invece di un panico e il giveback è controllato da `-onfailure` (e non da `-auto-giveback-after-panic parameter`).

Per ulteriori informazioni su tutti `storage failover modify` per i parametri, vedere "Pagine di manuale di ONTAP".

## Comandi manuali di Takeover

È possibile eseguire un takeover manualmente quando è necessaria la manutenzione del partner e in altre situazioni simili. A seconda dello stato del partner, il comando utilizzato per eseguire il takeover varia.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Assumere il controllo del nodo partner | `storage failover takeover` |
| Monitorare l'avanzamento dell'acquisizione man mano che gli aggregati del partner vengono spostati nel nodo che esegue l'acquisizione | `storage failover show-takeover` |
| Visualizzare lo stato di failover dello storage per tutti i nodi del cluster | `storage failover show` |
| Assumere il controllo del nodo partner senza migrare i LIF | `storage failover takeover -skip-lif -migration-before-takeover true` |
| Assumere il controllo del nodo partner anche in caso di mancata corrispondenza del disco | `storage failover takeover -skip-lif -migration-before-takeover true` |
| Assumere il controllo del nodo partner anche in caso di mancata corrispondenza della versione di ONTAP **Nota:** questa opzione viene utilizzata solo durante il processo di aggiornamento di ONTAP senza interruzioni. | `storage failover takeover -option allow -version-mismatch` |
| Assumere il controllo del nodo partner senza eseguire il trasferimento dell'aggregato | `storage failover takeover -bypass -optimization true` |
| Assumere il controllo del nodo partner prima che il partner abbia il tempo di chiudere correttamente le proprie risorse di storage | `storage failover takeover -option immediate` |

> Prima di eseguire il comando di failover dello storage con l'opzione immediate, è necessario migrare i file LIF dei dati in un altro nodo utilizzando il seguente comando: `network interface migrate-all -node` *`node`*
>
> Se si specifica `storage failover takeover -option immediate` Senza prima eseguire la migrazione dei dati LIF, la migrazione dei dati LIF dal nodo viene ritardata in modo significativo anche se `skip-lif-migration-before-takeover` opzione non specificata.
>
> Analogamente, se si specifica l'opzione immediata, l'ottimizzazione del Takeover negoziato viene ignorata anche se l'opzione di ottimizzazione bypass-è impostata su *false*.

### Spostamento di epsilon per alcuni takeover avviati manualmente

È consigliabile spostare epsilon se si prevede che eventuali operazioni di takeover avviate manualmente potrebbero causare un guasto inaspettato del nodo del sistema storage, lontano da una perdita di quorum a livello di cluster.

#### A proposito di questa attività

Per eseguire la manutenzione pianificata, è necessario assumere il controllo di uno dei nodi di una coppia ha. È necessario mantenere il quorum a livello di cluster per evitare interruzioni non pianificate dei dati dei client per i nodi rimanenti. In alcuni casi, l'esecuzione del takeover può causare un cluster che rappresenta un guasto inaspettato del nodo a causa della perdita di quorum a livello di cluster.

Questo può verificarsi se il nodo che viene sostituito contiene epsilon o se il nodo con epsilon non è integro. Per mantenere un cluster più resiliente, è possibile trasferire epsilon a un nodo integro che non viene sostituito. In genere, questo sarebbe il partner ha.

Solo i nodi sani e idonei partecipano al voto del quorum. Per mantenere il quorum a livello di cluster, sono richiesti più di N/2 voti (dove *N* rappresenta la somma dei nodi online sani e idonei). Nei cluster con un numero pari di nodi online, epsilon aggiunge ulteriore peso di voto per mantenere il quorum per il nodo a cui è assegnato.

> Sebbene il voto di formazione del cluster possa essere modificato utilizzando `cluster modify -eligibility false` evitare questo problema, ad eccezione di situazioni come il ripristino della configurazione del nodo o la manutenzione prolungata del nodo. Se si imposta un nodo come non idoneo, questo interrompe la fornitura dei dati SAN fino a quando il nodo non viene reimpostato su idoneo e riavviato. Anche l'accesso ai dati NAS al nodo potrebbe essere compromesso quando il nodo non è idoneo.

#### Fasi

1. Verificare lo stato del cluster e verificare che epsilon sia mantenuto da un nodo integro che non viene sostituito:

   a. Passare al livello di privilegio avanzato, confermando che si desidera continuare quando viene visualizzato il prompt della modalità avanzata (*>):

      ```
      set -privilege advanced
      ```

   b. Determinare quale nodo contiene epsilon:

      ```
      cluster show
      ```

      Nell'esempio seguente, Node1 contiene epsilon:

| Nodo | Salute | Idoneità | Epsilon |
|---|---|---|---|
| Node1 Node2 | vero vero | vero vero | vero falso |

+
Se il nodo che si desidera sostituire non include epsilon, passare alla fase 4.

2. Rimuovere epsilon dal nodo che si desidera sostituire:

   ```
   cluster modify -node Node1 -epsilon false
   ```

3. Assegnare epsilon al nodo partner (in questo esempio, Node2):

   ```
   cluster modify -node Node2 -epsilon true
   ```

4. Eseguire l'operazione di takeover:

   ```
   storage failover takeover -ofnode node_name
   ```

5. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

## Comandi manuali di giveback

È possibile eseguire un giveback normale, un giveback in cui si terminano i processi sul nodo partner o un giveback forzato.

> Prima di eseguire un giveback, è necessario rimuovere i dischi guasti nel sistema preso in consegna come descritto in "Gestione di dischi e aggregati".

### In caso di interruzione del giveback

Se durante il processo di giveback si verifica un guasto o un'interruzione dell'alimentazione del nodo di Takeover, tale processo si interrompe e il nodo di Takeover torna in modalità Takeover fino a quando l'errore non viene riparato o l'alimentazione non viene ripristinata.

Tuttavia, ciò dipende dalla fase di giveback in cui si è verificato il guasto. Se il nodo ha riscontrato un guasto o un'interruzione dell'alimentazione durante lo stato di giveback parziale (dopo aver restituito l'aggregato root), non tornerà alla modalità Takeover. Il nodo torna invece alla modalità di parziale giveback. In tal caso, completare il processo ripetendo l'operazione di giveback.

### Se il giveback è veto

Se il giveback è vetoed, è necessario controllare i messaggi EMS per determinare la causa. A seconda del motivo o dei motivi, è possibile decidere se è possibile eseguire l'override dei veti in modo sicuro.

Il `storage failover show-giveback` il comando visualizza l'avanzamento del giveback e indica quale sottosistema ha posto il veto del giveback, se presente. I veti morbidi possono essere ignorati, mentre i veti difficili non possono essere, anche se forzati. Le seguenti tabelle riepilogano i file soft vetoes che non devono essere sovrascritti, insieme alle soluzioni consigliate.

È possibile rivedere i dettagli EMS per qualsiasi veto di giveback utilizzando il seguente comando:

```
event log show -node * -event gb*
```

### Giveback dell'aggregato root

Questi veti non si applicano alle operazioni di trasferimento degli aggregati:

| Modulo del sottosistema di vetoing | Soluzione alternativa |
|---|---|
| vfiler_low_level | Terminare le sessioni SMB che causano il veto o chiudere l'applicazione SMB che ha stabilito le sessioni aperte.<br><br>L'override di questo veto potrebbe causare la disconnessione improvvisa dell'applicazione che utilizza SMB e la perdita di dati. |
| Controllo disco | Tutti i dischi guasti o bypassati devono essere rimossi prima di tentare il giveback. Se i dischi vengono disinfettati, attendere il completamento dell'operazione.<br><br>L'override di questo veto potrebbe causare un'interruzione causata da aggregati o volumi che vanno fuori linea a causa di conflitti di prenotazione o dischi inaccessibili. |

### Giveback degli aggregati SFO

Questi veti non si applicano alle operazioni di trasferimento degli aggregati:

| Modulo del sottosistema di vetoing | Soluzione alternativa |
|---|---|
| Gestione blocchi | Arrestare correttamente le applicazioni SMB che hanno file aperti o spostare tali volumi in un aggregato diverso.<br><br>L'override di questo veto comporta la perdita dello stato di blocco SMB, causando interruzioni e perdita di dati. |
| Gestione blocchi NDO | Attendere il mirroring dei blocchi.<br><br>L'override di questo veto causa interruzioni alle macchine virtuali Microsoft Hyper-V. |

| | |
|---|---|
| RAID | Controllare i messaggi EMS per determinare la causa del veto:<br><br>Se il veto è dovuto a nvfile, portare online i volumi offline e gli aggregati.<br><br>Se sono in corso operazioni di aggiunta o riassegnazione della proprietà del disco, attendere il completamento.<br><br>Se il veto è dovuto a un conflitto di nome aggregato o UUID, risolvere il problema.<br><br>Se il veto è dovuto alla risincronizzazione del mirror, alla verifica del mirror o ai dischi offline, il veto può essere ignorato e l'operazione viene riavviata dopo il giveback. |
| Inventario dei dischi | Risolvere i problemi per identificare e risolvere la causa del problema.<br><br>Il nodo di destinazione potrebbe non essere in grado di visualizzare i dischi appartenenti a un aggregato in fase di migrazione.<br><br>I dischi inaccessibili possono causare aggregati o volumi inaccessibili. |
| Operazione di spostamento del volume | Risolvere i problemi per identificare e risolvere la causa del problema.<br><br>Questo veto impedisce l'interruzione dell'operazione di spostamento del volume durante l'importante fase di cutover. Se il lavoro viene interrotto durante il cutover, il volume potrebbe diventare inaccessibile. |

#### Comandi per l'esecuzione di un giveback manuale

È possibile avviare manualmente un giveback su un nodo di una coppia ha per restituire lo storage al proprietario originale dopo aver completato la manutenzione o aver risolto eventuali problemi che hanno causato il takeover.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Restituire lo storage a un nodo partner | `storage failover giveback -ofnode` *`nodename`* |
| Restituire lo storage anche se il partner non è in attesa della modalità di giveback | `storage failover giveback -ofnode` *`nodename`*<br>`-require-partner-waiting false`<br><br>Non utilizzare questa opzione a meno che non sia accettabile un'interruzione più lunga del client. |

| | |
|---|---|
| Restituire lo storage anche se i processi stanno vetoing l'operazione di giveback (forzare il giveback) | `storage failover giveback -ofnode` *`nodename`* `-override-vetoes true`<br><br>L'utilizzo di questa opzione può potenzialmente causare un'interruzione più lunga del servizio client o la mancata disponibilità di aggregati e volumi dopo il giveback. |
| Restituire solo gli aggregati CFO (l'aggregato root) | `storage failover giveback -ofnode` *`nodename`*<br><br>`-only-cfo-aggregates true` |
| Monitorare l'avanzamento del giveback dopo aver eseguito il comando giveback | `storage failover show-giveback` |

## Test di Takeover e giveback

Dopo aver configurato tutti gli aspetti della coppia ha, è necessario verificare che funzioni come previsto per mantenere l'accesso ininterrotto allo storage di entrambi i nodi durante le operazioni di takeover e giveback. Durante il processo di acquisizione, il nodo locale (o Takeover) deve continuare a fornire i dati normalmente forniti dal nodo partner. Durante il giveback, il controllo e la consegna dello storage del partner dovrebbero tornare al nodo partner.

**Fasi**

1. Verificare che i cavi di interconnessione ha siano collegati correttamente.
2. Verificare che sia possibile creare e recuperare file su entrambi i nodi per ciascun protocollo concesso in licenza.
3. Immettere il seguente comando:

   ```
   storage failover takeover -ofnode partnernode
   ```

   Vedere la pagina man per i dettagli sui comandi.

4. Immettere uno dei seguenti comandi per confermare che si è verificato il Takeover:

   ```
   storage failover show-takeover
   ```

   ```
   storage failover show
   ```

   Se si dispone di `storage failover` del comando `-auto-giveback` opzione attivata:

   | Nodo | Partner | Possibilità di acquisizione | Descrizione dello stato |
   |---|---|---|---|
   | nodo 1 | nodo 2 | - | In attesa di un giveback |

| | | | |
|---|---|---|---|
| nodo 2 | nodo 1 | falso | In fase di acquisizione, il giveback automatico verrà avviato in pochi secondi |

Se si dispone di `storage failover` del comando `-auto-giveback` opzione disattivata:

| Nodo | Partner | Possibilità di acquisizione | Descrizione dello stato |
|---|---|---|---|
| nodo 1 | nodo 2 | - | In attesa di un giveback |
| nodo 2 | nodo 1 | falso | In fase di acquisizione |

5. Visualizzare tutti i dischi appartenenti al nodo partner (Node2) che il nodo di Takeover (Node1) può rilevare:

   ```
   storage disk show -home node2 -ownership
   ```

   Il seguente comando visualizza tutti i dischi appartenenti a Node2 che Node1 può rilevare:
   `cluster::> storage disk show -home node2 -ownership`

| Disco | Aggregato | A casa | Proprietario | Dr. Casa | ID casa | ID proprietario | ID casa DR | Riservatore | Piscina |
|---|---|---|---|---|---|---|---|---|---|
| 1.0.2 | - | node2 | node2 | - | 4078312453 | 4078312453 | - | 4078312452 | Pool0 |
| 1.0.3 | - | node2 | node2 | - | 4078312453 | 4078312453 | - | 4078312452 | Pool0 |

6. Verificare che il nodo di Takeover (Node1) controlli gli aggregati del nodo partner (Node2):

   ```
   aggr show -fields home-id,home-name,is-home
   ```

| aggregato | id abitazione | nome di casa | è a casa |
|---|---|---|---|
| aggr0_1 | 2014942045 | node1 | vero |
| aggr0_2 | 4078312453 | node2 | falso |
| aggr1_1 | 2014942045 | node1 | vero |
| aggr1_2 | 4078312453 | node2 | falso |

   Durante l'acquisizione, il valore "is-home" degli aggregati del nodo partner è falso.

7. Restituire il servizio dati del nodo partner dopo aver visualizzato il messaggio "Waiting for giveback":

   ```
   storage failover giveback -ofnode partnernode
   ```

8. Immettere uno dei seguenti comandi per osservare l'avanzamento dell'operazione di giveback:

```
storage failover show-giveback

storage failover show
```

9. Procedere, a seconda che sia stato visualizzato il messaggio che indica che il giveback è stato completato correttamente:

| In caso di acquisizione e giveback… | Quindi… |
|---|---|
| Sono stati completati correttamente | Ripetere i passaggi da 2 a 8 sul nodo partner. |
| Non riuscito | Correggere l'errore di takeover o giveback, quindi ripetere questa procedura. |

## Comandi per il monitoraggio di una coppia ha

È possibile utilizzare i comandi ONTAP per monitorare lo stato della coppia ha. Se si verifica un Takeover, è anche possibile determinare la causa del Takeover.

| Se si desidera controllare | Utilizzare questo comando |
|---|---|
| Se il failover è attivato o si è verificato, oppure perché il failover non è attualmente possibile | `storage failover show` |
| Consente di visualizzare i nodi su cui è abilitata l'impostazione ha-mode di failover dello storage Devi impostare il valore su ha perché il nodo partecipi a una configurazione di failover dello storage (coppia ha). | `storage failover show -fields mode` |
| Se il Takeover assistito dall'hardware è attivato | `storage failover hwassist show` |
| La cronologia degli eventi di Takeover assistiti dall'hardware che si sono verificati | `storage failover hwassist stats show` |
| Lo stato di avanzamento di un'operazione di Takeover mentre gli aggregati del partner vengono spostati nel nodo che esegue il Takeover | `storage failover show-takeover` |
| Lo stato di avanzamento di un'operazione di giveback nella restituzione degli aggregati al nodo partner | `storage failover show-giveback` |
| Se un aggregato è a casa durante le operazioni di acquisizione o di giveback | `aggregate show -fields home-id,owner -id,home-name,owner-name,is-home` |
| Se l'ha del cluster è attivato (si applica solo ai cluster a due nodi) | `cluster ha show` |
| Lo stato ha dei componenti di una coppia ha (sui sistemi che utilizzano lo stato ha) | `ha-config show`Si tratta di un comando della modalità di manutenzione. |

#### stati dei nodi visualizzati dai comandi di tipo show di failover dello storage

L'elenco seguente descrive gli stati dei nodi in cui si trova `storage failover show` viene visualizzato il comando.

| Stato del nodo | Descrizione |
| --- | --- |
| Connesso a partner_name, Takeover automatico disattivato. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. L'acquisizione automatica del partner è disattivata. |
| In attesa di nome_partner, giveback dei dischi di riserva del partner in sospeso. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il giveback degli aggregati SFO per il partner viene eseguito, ma i dischi di riserva del partner sono ancora di proprietà del nodo locale.<br><br>• Eseguire `storage failover show-giveback` per ulteriori informazioni. |
| In attesa di nome_partner. In attesa della sincronizzazione del blocco partner. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha e attende che venga eseguita la sincronizzazione del blocco del partner. |
| In attesa di nome_partner. In attesa che le applicazioni cluster siano online sul nodo locale. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha e attende che le applicazioni del cluster siano online. |
| Takeover pianificato. Nodo di destinazione spostamento dei propri aggregati SFO in preparazione del Takeover. | L'elaborazione del takeover è iniziata. Il nodo di destinazione sta trasferendo la proprietà dei propri aggregati SFO in preparazione del takeover. |
| Takeover pianificato. Il nodo di destinazione ha riallocato i propri aggregati SFO in preparazione del Takeover. | L'elaborazione del takeover è iniziata. Il nodo di destinazione ha riallocato la proprietà dei propri aggregati SFO in preparazione del takeover. |
| Takeover pianificato. In attesa di disattivare gli aggiornamenti del firmware del disco in background sul nodo locale. È in corso un aggiornamento del firmware sul nodo. | L'elaborazione del takeover è iniziata. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo locale. |
| Spostamento degli aggregati SFO nel nodo di acquisizione in preparazione del Takeover. | Il nodo locale sta trasferendo la proprietà dei propri aggregati SFO nel nodo di Taking-over in preparazione del Takeover. |
| Riallocare gli aggregati SFO per assumere il nodo. In attesa di acquisizione del nodo. | Il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione è stato completato. Il sistema è in attesa di essere assunto dal nodo di acquisizione. |

| | |
|---|---|
| Spostamento degli aggregati SFO in nome_partner. In attesa di disattivare gli aggiornamenti del firmware del disco in background sul nodo locale. È in corso un aggiornamento del firmware sul nodo. | È in corso il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo locale. |
| Spostamento degli aggregati SFO in nome_partner. In attesa di disattivare gli aggiornamenti del firmware del disco in background su partner_name. È in corso un aggiornamento del firmware sul nodo. | È in corso il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo partner. |
| Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto a causa del motivo. Il nodo locale possiede alcuni aggregati SFO del partner. Riemettere un'acquisizione del partner con `-bypass-optimization` parametro impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). Il nodo locale possiede alcuni aggregati SFO del partner.<br>• Riemettere un takeover del nodo partner, impostando il parametro di ottimizzazione -bypass-su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati. |
| Connesso a partner_name. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner. Riemettere un'acquisizione del partner con `-bypass-optimization` parametro impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner.<br>• Riemettere un takeover del nodo partner, impostando il parametro di ottimizzazione -bypass-su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati. |
| In attesa di nome_partner. Il precedente tentativo di takeover è stato interrotto a causa del motivo. Il nodo locale possiede alcuni aggregati SFO del partner. Riemettere un'acquisizione del partner con il parametro "-bypass-Optimization" impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). Il nodo locale possiede alcuni aggregati SFO del partner.<br>• Riemettere un takeover del nodo partner, impostando il parametro di ottimizzazione -bypass-su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati. |

| | |
|---|---|
| In attesa di nome_partner. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner. Riemettere un'acquisizione del partner con il parametro "-bypass-Optimization" impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner.<br><br>• Riemettere un takeover del nodo partner, impostando il parametro di ottimizzazione `-bypass-su` true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati. |
| Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto perché non è stato possibile disattivare l'aggiornamento del firmware del disco in background (BDFU) sul nodo locale. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di takeover precedente è stato interrotto perché l'aggiornamento del firmware del disco in background sul nodo locale non era stato disattivato. |
| Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto a causa del motivo. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). |
| In attesa di nome_partner. Il precedente tentativo di takeover è stato interrotto a causa del motivo. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). |
| Connesso a partner_name. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto a causa del motivo. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto a causa del motivo visualizzato sotto Reason. |
| Connesso a partner_name. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto. |
| In attesa di nome_partner. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto a causa del motivo. | Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto a causa del motivo visualizzato sotto Reason. |
| Giveback precedente non riuscito nel modulo: Nome modulo. Il giveback automatico verrà avviato in pochi secondi. | Il precedente tentativo di giveback non è riuscito nel modulo module_name. Il giveback automatico verrà avviato in pochi secondi.<br><br>• Eseguire `storage failover show-giveback` per ulteriori informazioni. |

| | |
|---|---|
| Node possiede gli aggregati del partner come parte della procedura di upgrade del controller senza interruzioni. | Il nodo possiede gli aggregati del partner a causa della procedura di aggiornamento del controller senza interruzioni attualmente in corso. |
| Connesso a partner_name. Il nodo possiede aggregati appartenenti a un altro nodo del cluster. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il nodo possiede aggregati appartenenti a un altro nodo del cluster. |
| Connesso a partner_name. In attesa della sincronizzazione del blocco partner. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il sistema è in attesa del completamento della sincronizzazione del blocco partner. |
| Connesso a partner_name. In attesa che le applicazioni cluster siano online sul nodo locale. | L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il sistema è in attesa che le applicazioni del cluster siano online sul nodo locale. |
| Modalità non ha, riavviare per utilizzare la NVRAM completa. | Il failover dello storage non è possibile. L'opzione ha mode è configurata come non_ha.<br>• Riavviare il nodo per utilizzare tutta la NVRAM. |
| Modalità non ha. Riavviare il nodo per attivare ha. | Il failover dello storage non è possibile.<br>• Il nodo deve essere riavviato per abilitare la funzionalità ha. |
| Modalità non ha. | Il failover dello storage non è possibile. L'opzione ha mode è configurata come non_ha.<br>• È necessario eseguire `storage failover modify -mode ha -node nodename` Su entrambi i nodi della coppia ha, quindi riavviare i nodi per abilitare la funzionalità ha. |

## Comandi per abilitare e disabilitare il failover dello storage

Utilizzare i seguenti comandi per attivare e disattivare la funzionalità di failover dello storage.

| Se si desidera… | Utilizzare questo comando… |
|---|---|
| Abilitare il Takeover | `storage failover modify -enabled true -node` *`nodename`* |
| Disattiva il Takeover | `storage failover modify -enabled false -node` *`nodename`* |

È necessario disattivare il failover dello storage solo se necessario come parte di una procedura di manutenzione.

## Arrestare o riavviare un nodo senza avviare il Takeover in un cluster a due nodi

Arrestare o riavviare un nodo in un cluster a due nodi senza avviare il Takeover quando si esegue una determinata manutenzione hardware su un nodo o uno shelf e si desidera limitare il tempo di inattività mantenendo il nodo partner attivo, oppure quando si verificano problemi che impediscono un takeover manuale e si desidera mantenere aggiornati gli aggregati del nodo partner e fornire i dati. Inoltre, se il supporto tecnico sta fornendo assistenza per la risoluzione dei problemi, potrebbe essere necessario eseguire questa procedura come parte di tali sforzi.

**A proposito di questa attività**

- Prima di inibire il Takeover (utilizzando il `-inhibit-takeover true` Parametro), si disattiva il cluster ha.

> - In un cluster a due nodi, il cluster ha garantisce che il guasto di un nodo non disabiliti il cluster. Tuttavia, se non si disattiva il cluster ha prima di utilizzare `-inhibit-takeover true` parametro, entrambi i nodi interrompono la fornitura dei dati.
> - Se si tenta di arrestare o riavviare un nodo prima di disattivare il cluster ha, ONTAP emette un avviso e richiede di disattivare il cluster ha.

- La migrazione delle LIF (interfacce logiche) al nodo partner che si desidera mantenere in linea.
- Se sul nodo che si sta arrestando o riavviando sono presenti aggregati che si desidera mantenere, spostarli nel nodo che si desidera mantenere in linea.

**Fasi**

1. Verificare che entrambi i nodi siano integri:
   `cluster show`

   Per entrambi i nodi, `true` viene visualizzato in `Health` colonna.

   ```
   cluster::> cluster show
   Node          Health  Eligibility
   ------------ ------- ------------
   node1         true     true
   node2         true     true
   ```

2. Migrare tutte le LIF dal nodo che si desidera arrestare o riavviare al nodo partner:
   `network interface migrate-all -node node_name`
3. Se sul nodo si arresta o si riavvia ci sono aggregati che si desidera mantenere in linea quando il nodo è inattivo, trasferirli sul nodo partner; in caso contrario, passare alla fase successiva.

   a. Mostrare gli aggregati sul nodo che si desidera arrestare o riavviare:
      `storage aggregates show -node node_name`

      Ad esempio, node1 è il nodo che verrà arrestato o riavviato:

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

b. Spostare gli aggregati nel nodo partner:
`storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

Ad esempio, gli aggregati aggr1, aggr2 e test2_aggr vengono spostati da node1 a node2:

`storage aggregate relocation start -node node1 -destination node2 -aggregate -list aggr1,aggr2,test2_aggr`

4. Disattiva cluster ha:
`cluster ha modify -configured false`

L'output di ritorno conferma che ha è disattivato: `Notice: HA is disabled`

> Questa operazione non disattiva il failover dello storage.

5. Arrestare o riavviare e inibire il takeover del nodo di destinazione, utilizzando il comando appropriato:
   - `system node halt -node node_name -inhibit-takeover true`
   - `system node reboot -node node_name -inhibit-takeover true`

> Nell'output del comando, viene visualizzato un avviso che chiede se si desidera procedere, digitare `y`.

6. Verificare che il nodo ancora in linea sia in buono stato (mentre il partner non è attivo):
`cluster show`

Per il nodo online, `true` viene visualizzato in `Health` colonna.

> Nell'output del comando, viene visualizzato un avviso che indica che il cluster ha non è configurato. È possibile ignorare l'avviso in questo momento.

7. Eseguire le azioni necessarie per arrestare o riavviare il nodo.
8. Avviare il nodo non allineato dal prompt DEL CARICATORE:
   `boot_ontap`
9. Verificare che entrambi i nodi siano integri:
   `cluster show`

   Per entrambi i nodi, `true` viene visualizzato in `Health` colonna.

   > Nell'output del comando, viene visualizzato un avviso che indica che il cluster ha non è configurato. È possibile ignorare l'avviso in questo momento.

10. Riabilitare il cluster ha:
    `cluster ha modify -configured true`
11. Se prima di questa procedura sono state spostate le aggregazioni nel nodo partner, spostarle di nuovo nel nodo principale; in caso contrario, passare alla fase successiva:
    `storage aggregate relocation start -node` *`node_name`* `-destination` *`node_name`* `-aggregate-list` *`aggregate_name`*

    Ad esempio, gli aggregati aggr1, aggr2 e test2_aggr vengono spostati dal nodo node2 al nodo node1:
    `storage aggregate relocation start -node` *`node2`* `-destination` *`node1`* `-aggregate -list` *`aggr1`*`,`*`aggr2`*`,`*`test2_aggr`*

12. Ripristinare le LIF alle porte home:
    a. Visualizza le LIF che non sono a casa:
       `network interface show -is-home false`
    b. Se esistono LIF non domestiche che non sono state migrate dal nodo DOWN, verificare che sia sicuro spostarle prima di eseguire il ripristino.
    c. In caso di sicurezza, ripristinare tutte le LIF a casa.
       `network interface revert *`

# Gestione delle API REST con System Manager

## Gestione delle API REST con System Manager

Il log delle API REST acquisisce le chiamate API che Gestione di sistema invia a ONTAP. È possibile utilizzare il log per comprendere la natura e la sequenza delle chiamate necessarie per eseguire le varie attività amministrative di ONTAP.

### Come System Manager utilizza l'API REST e il log API

Esistono diversi modi in cui le chiamate REST API vengono inviate da Gestore di sistema a ONTAP.

#### Quando System Manager effettua chiamate API

Di seguito sono riportati gli esempi più importanti di quando Gestione sistema esegue chiamate API REST ONTAP.

### Aggiornamento automatico della pagina

System Manager effettua automaticamente chiamate API in background per aggiornare le informazioni visualizzate, ad esempio nella pagina della dashboard.

### Azione di visualizzazione per utente

Una o più chiamate API vengono emesse quando si visualizza una risorsa di storage specifica o una raccolta di risorse dall'interfaccia utente di System Manager.

### Azione di aggiornamento da parte dell'utente

Una chiamata API viene eseguita quando si aggiunge, modifica o elimina una risorsa ONTAP dall'interfaccia utente di Gestione sistema.

#### Riemissione di una chiamata API

È inoltre possibile eseguire manualmente una chiamata API facendo clic su una voce di registro. Visualizza l'output JSON raw della chiamata.

### Ulteriori informazioni

- "Documentazione sull'automazione di ONTAP 9"

## Accesso al log API REST

È possibile accedere al registro contenente un record delle chiamate API REST ONTAP effettuate da Gestore di sistema. Quando si visualizza il log, è possibile anche emettere nuovamente le chiamate API e rivedere l'output.

#### Fasi

1. Nella parte superiore della pagina, fare clic su  Per visualizzare il log API REST.

   Le voci più recenti vengono visualizzate nella parte inferiore della pagina.

2. A sinistra, fare clic su **DASHBOARD** e osservare le nuove voci create per le chiamate API emesse per aggiornare la pagina.
3. Fare clic su **STORAGE**, quindi su **Qtree**.

   In questo modo System Manager esegue una chiamata API specifica per recuperare un elenco di Qtree.

4. Individuare la voce di registro che descrive la chiamata API che ha il modulo:

   ```
   GET /api/storage/qtrees
   ```

   Verranno visualizzati ulteriori parametri di query HTTP inclusi nella voce, ad esempio `max_records`.

5. Fare clic sulla voce di registro per emettere nuovamente la chiamata GET API e visualizzare l'output JSON raw.

   Esempio


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
```

```
        }
      },
      ],
      "num_records": 1,
      "_links": {
        "self": {
          "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
        }
      }
    }
```