Configurare il server SnapCenter

SnapCenter software

NetApp
January 09, 2026

Sommario

Configurare il server SnapCenter

Aggiungere e predisporre il sistema di archiviazione

Aggiungere sistemi storage

Per eseguire operazioni di provisioning e data Protection, devi configurare il sistema storage che offra accesso SnapCenter allo storage ONTAP, ai sistemi ASA R2 o ad Amazon FSX per NetApp ONTAP.

È possibile aggiungere una SVM standalone o un cluster composto da più SVM. Se si utilizza Amazon FSX per NetApp ONTAP, è possibile aggiungere FSX admin LIF composto da più SVM utilizzando l'account fsxadmin o aggiungere FSX SVM in SnapCenter.

Prima di iniziare

- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".

- I nomi dei sistemi di storage devono essere univoci.

  SnapCenter non supporta più sistemi storage con lo stesso nome su cluster diversi. Ogni sistema storage supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dei dati univoco.

A proposito di questa attività

- Quando si configurano i sistemi storage, è possibile attivare anche le funzioni del sistema di gestione degli eventi (EMS) e AutoSupport. Lo strumento AutoSupport raccoglie i dati sullo stato di salute del sistema e li invia automaticamente al supporto tecnico NetApp, consentendo loro di eseguire il troubleshooting del sistema.

  Se si abilitano queste funzioni, SnapCenter invia informazioni AutoSupport al sistema di storage e messaggi EMS al syslog del sistema di storage quando una risorsa viene protetta, un'operazione di ripristino o clonazione viene completata correttamente o un'operazione non riesce.

- Se hai intenzione di replicare Snapshot su una destinazione SnapMirror o su una destinazione SnapVault, devi impostare connessioni del sistema storage per la SVM o il cluster di destinazione così come la SVM o il cluster di origine.

> Se si modifica la password del sistema di storage, i processi pianificati, il backup su richiesta e le operazioni di ripristino potrebbero non riuscire. Dopo aver modificato la password del sistema di storage, è possibile aggiornarla facendo clic su **Modify** (Modifica) nella scheda Storage (archiviazione).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Systems**.
2. Nella pagina Storage Systems (sistemi storage), fare clic su **New** (nuovo).
3. Nella pagina Add Storage System (Aggiungi sistema di storage), fornire le seguenti informazioni:

Per questo campo…	Eseguire questa operazione…
Sistema storage	Inserire il nome del sistema di storage o l'indirizzo IP. I nomi dei sistemi di storage, che non includono il nome di dominio, devono contenere un massimo di 15 caratteri e devono essere risolutibili. Per creare connessioni al sistema di storage con nomi che hanno più di 15 caratteri, è possibile utilizzare il cmdlet Add-SmStorageConnectionPowerShell. Per i sistemi storage con configurazione MetroCluster (MCC), si consiglia di registrare cluster locali e peer per operazioni senza interruzioni. SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportata da SnapCenter deve avere un nome univoco. Dopo aver aggiunto la connessione allo storage a SnapCenter, non rinominare la SVM o il cluster utilizzando ONTAP. Se SVM viene aggiunto con un nome breve o FQDN, deve essere risolvibile sia da SnapCenter che dall'host del plug-in.
Nome utente/Password	Inserire le credenziali dell'utente dello storage che dispone dei privilegi necessari per accedere al sistema di storage.

Per questo campo…	Eseguire questa operazione…
Sistema di gestione degli eventi (EMS) e impostazioni AutoSupport	Se si desidera inviare messaggi EMS al syslog del sistema di storage o inviare messaggi AutoSupport al sistema di storage per la protezione applicata, le operazioni di ripristino completate o le operazioni non riuscite, selezionare la casella di controllo appropriata. Quando si seleziona la casella di controllo **Invia notifica AutoSupport per operazioni non riuscite al sistema di storage**, viene selezionata anche la casella di controllo **Registra eventi server SnapCenter su syslog**, in quanto è necessaria la messaggistica EMS per attivare le notifiche AutoSupport.

4. Fare clic su **altre opzioni** per modificare i valori predefiniti assegnati a piattaforma, protocollo, porta e timeout.

   a. In Platform (piattaforma), selezionare una delle opzioni dall'elenco a discesa.

      Se SVM è il sistema di storage secondario in una relazione di backup, selezionare la casella di controllo **secondario**. Quando si seleziona l'opzione **secondario**, SnapCenter non esegue immediatamente un controllo della licenza.

   Se è stata aggiunta una SVM in SnapCenter, l'utente deve selezionare manualmente il tipo di piattaforma dal menu a discesa.

   a. In Protocol (protocollo), selezionare il protocollo configurato durante l'installazione di SVM o Cluster, in genere HTTPS.
   b. Inserire la porta accettata dal sistema di storage.

      La porta predefinita 443 in genere funziona.

   c. Inserire il tempo, espresso in secondi, che deve trascorrere prima dell'arresto dei tentativi di comunicazione.

      Il valore predefinito è 60 secondi.

   d. Se SVM dispone di più interfacce di gestione, selezionare la casella di controllo **Preferred IP** (IP preferito), quindi immettere l'indirizzo IP preferito per le connessioni SVM.
   e. Fare clic su **Save** (Salva).
5. Fare clic su **Invia**.

Risultato

Nella pagina Storage Systems (sistemi storage), dal menu a discesa **Type** (tipo), eseguire una delle seguenti operazioni:

- Selezionare **ONTAP SVM** per visualizzare tutte le SVM aggiunte.

  Se sono state aggiunte le SVM FSX, le SVM FSX sono elencate qui.

- Selezionare **ONTAP Clusters** per visualizzare tutti i cluster aggiunti.

  Se sono stati aggiunti cluster FSX utilizzando fsxadmin, i cluster FSX sono elencati qui.

  Quando si fa clic sul nome del cluster, tutte le SVM che fanno parte del cluster vengono visualizzate nella sezione Storage Virtual Machines (macchine virtuali di storage).

  Se una nuova SVM viene aggiunta al cluster ONTAP utilizzando l'interfaccia grafica di ONTAP, fare clic su **riscopri** per visualizzare la nuova SVM aggiunta.

Al termine

Un amministratore del cluster deve abilitare AutoSupport su ciascun nodo del sistema di storage per inviare notifiche e-mail da tutti i sistemi di storage a cui SnapCenter ha accesso, eseguendo il seguente comando dalla riga di comando del sistema di storage:

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```

L'amministratore della macchina virtuale per lo storage (SVM) non ha accesso a AutoSupport.

Connessioni e credenziali dello storage

Prima di eseguire operazioni di protezione dei dati, è necessario configurare le connessioni di storage e aggiungere le credenziali utilizzate dal server SnapCenter e dai plug-in SnapCenter.

Connessioni di archiviazione

Le connessioni storage consentono al server SnapCenter e ai plug-in SnapCenter di accedere allo storage ONTAP. L'impostazione di queste connessioni comporta anche la configurazione delle funzionalità di AutoSupport e del sistema di gestione degli eventi (EMS).

Credenziali

- Amministratore di dominio o qualsiasi membro del gruppo di amministratori

  Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori nel sistema in cui si installa il plug-in SnapCenter. I formati validi per il campo Nome utente sono:

  - *NetBIOS/nome utente*
  - *Dominio FQDN/nome utente*
  - *Nome utente@upn*
- Amministratore locale (solo per gruppi di lavoro)

  Per i sistemi appartenenti a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si installa il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locali se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata sul sistema host.

  Il formato valido per il campo Nome utente è: *Nome utente*

- Credenziali per singoli gruppi di risorse

  Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Eseguire il provisioning dello storage su host Windows

Creare e gestire igroups

È possibile creare gruppi di iniziatori (igroups) per specificare gli host che possono accedere a una determinata LUN sul sistema di storage. È possibile utilizzare SnapCenter per creare, rinominare, modificare o eliminare un igroup su un host Windows.

Creare un igroup

È possibile utilizzare SnapCenter per creare un igroup su un host Windows. L'igroup sarà disponibile nella procedura guidata Create Disk (Crea disco) o Connect Disk (Connetti disco) quando si esegue la mappatura dell'igroup a un LUN.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic su **New** (nuovo).
4. Nella finestra di dialogo Create iGroup (Crea iGroup), definire il campo igroup:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN da mappare all'igroup.
Host	Selezionare l'host su cui si desidera creare l'igroup.
Nome iGroup	Immettere il nome dell'igroup.
Iniziatori	Selezionare l'iniziatore.
Tipo	Selezionare il tipo di iniziatore, iSCSI, FCP o misto (FCP e iSCSI).

5. Quando si è soddisfatti delle voci immesse, fare clic su **OK**.

   SnapCenter crea l'igroup sul sistema storage.

Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco di SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera rinominare.
4. Nell'elenco di igroups per SVM, selezionare l'igroup che si desidera rinominare e fare clic su **Rename** (Rinomina).
5. Nella finestra di dialogo Rinomina igroup, immettere il nuovo nome per igroup e fare clic su **Rinomina**.

Modificare un igroup

È possibile utilizzare SnapCenter per aggiungere gli iniziatori igroup a un igroup esistente. Durante la creazione di un igroup è possibile aggiungere un solo host. Se si desidera creare un igroup per un cluster, è possibile modificare il igroup per aggiungere altri nodi a tale igroup.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi di iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera modificare.
4. Nell'elenco di igroups, selezionare un igroup e fare clic su **Add Initiator to igroup**.
5. Selezionare un host.
6. Selezionare gli iniziatori e fare clic su **OK**.

Eliminare un igroup

È possibile utilizzare SnapCenter per eliminare un igroup quando non è più necessario.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iGroup**.
3. Nella pagina Initiator Groups (gruppi iniziatori), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera eliminare.
4. Nell'elenco di igroups per SVM, selezionare l'igroup che si desidera eliminare e fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Delete igroup (Elimina igroup), fare clic su **OK**.

   SnapCenter elimina l'igroup.

Creare e gestire i dischi

L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare un LUN connesso a FC o iSCSI.

- SnapCenter supporta solo dischi di base. I dischi dinamici non sono supportati.
- Per GPT è consentita una sola partizione di dati e per MBR una partizione primaria con un volume formattato con NTFS o CSVFS e un percorso di montaggio.
- Stili di partizione supportati: GPT, MBR; in una macchina virtuale VMware UEFI, sono supportati solo i dischi iSCSI

SnapCenter non supporta la ridenominazione di un disco. Se un disco gestito da SnapCenter viene rinominato, le operazioni SnapCenter non avranno esito positivo.

Visualizzare i dischi su un host

È possibile visualizzare i dischi su ciascun host Windows gestito con SnapCenter.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

Visualizzare i dischi in cluster

È possibile visualizzare i dischi in cluster nel cluster gestito con SnapCenter. I dischi in cluster vengono visualizzati solo quando si seleziona il cluster dall'elenco a discesa host.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare il cluster dall'elenco a discesa **host**.

   I dischi sono elencati.

Stabilire una sessione iSCSI

Se si utilizza iSCSI per connettersi a un LUN, è necessario stabilire una sessione iSCSI prima di creare il LUN per abilitare la comunicazione.

Prima di iniziare

- È necessario aver definito il nodo del sistema di storage come destinazione iSCSI.
- È necessario aver avviato il servizio iSCSI sul sistema di storage. "Scopri di più"

A proposito di questa attività

È possibile stabilire una sessione iSCSI solo tra le stesse versioni IP, da IPv6 a IPv6 o da IPv4 a IPv4.

È possibile utilizzare un indirizzo IPv6 link-local per la gestione della sessione iSCSI e per la comunicazione tra un host e una destinazione solo quando entrambi si trovano nella stessa subnet.

Se si modifica il nome di un iSCSI Initiator, l'accesso alle destinazioni iSCSI viene compromesso. Dopo aver modificato il nome, potrebbe essere necessario riconfigurare le destinazioni a cui ha accesso l'iniziatore in modo che possano riconoscere il nuovo nome. Dopo aver modificato il nome di un iSCSI Initiator, è necessario riavviare l'host.

Se l'host dispone di più interfacce iSCSI, una volta stabilita una sessione iSCSI su SnapCenter utilizzando un indirizzo IP sulla prima interfaccia, non è possibile stabilire una sessione iSCSI da un'altra interfaccia con un indirizzo IP diverso.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **iSCSI Session** (sessione iSCSI).
3. Dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage), selezionare la macchina virtuale di storage (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **host**, selezionare l'host per la sessione.
5. Fare clic su **Definisci sessione**.

   Viene visualizzata la procedura guidata per stabilire la sessione.

6. Nella procedura guidata per stabilire la sessione, identificare la destinazione:

In questo campo…	Inserisci…
Nome del nodo di destinazione	Il nome del nodo della destinazione iSCSI Se esiste un nome di nodo di destinazione, il nome viene visualizzato in formato di sola lettura.
Indirizzo del portale di destinazione	L'indirizzo IP del portale di rete di destinazione
Porta del portale di destinazione	La porta TCP del portale di rete di destinazione
Indirizzo del portale iniziatore	L'indirizzo IP del portale di rete dell'iniziatore

7. Quando si è soddisfatti delle voci immesse, fare clic su **Connect** (Connetti).

   SnapCenter stabilisce la sessione iSCSI.

8. Ripetere questa procedura per stabilire una sessione per ogni destinazione.

Creazione di LUN o dischi connessi a FC o iSCSI

L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare un LUN connesso a FC o iSCSI.

Se si desidera creare e formattare dischi al di fuori di SnapCenter, sono supportati solo i file system NTFS e CSVFS.

Prima di iniziare

- È necessario aver creato un volume per il LUN sul sistema storage.

  Il volume deve contenere solo LUN e solo LUN creati con SnapCenter.

  > Non è possibile creare un LUN su un volume clone creato da SnapCenter a meno che il clone non sia già stato diviso.

- È necessario aver avviato il servizio FC o iSCSI sul sistema di storage.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di storage.
- Il pacchetto di plug-in SnapCenter per Windows deve essere installato solo sull'host su cui si sta creando il disco.

A proposito di questa attività

- Non è possibile connettere un LUN a più di un host a meno che il LUN non sia condiviso dagli host in un cluster di failover di Windows Server.
- Se un LUN viene condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario creare il disco sull'host proprietario del gruppo di cluster.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.
4. Fare clic su **nuovo**.

   Viene visualizzata la procedura guidata Create Disk (Crea disco).

5. Nella pagina LUN Name (Nome LUN), identificare il LUN:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN.
Percorso LUN	Fare clic su **Browse** (Sfoglia) per selezionare il percorso completo della cartella contenente il LUN.
Nome del LUN	Immettere il nome del LUN.
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. Le dimensioni del cluster dipendono dal sistema operativo e dalle applicazioni.

In questo campo…	Eseguire questa operazione…
Etichetta LUN	Se si desidera, inserire un testo descrittivo per il LUN.

6. Nella pagina Disk Type (tipo di disco), selezionare il tipo di disco:

Selezionare…	Se…
Disco dedicato	È possibile accedere al LUN solo da un host. Ignorare il campo **Gruppo di risorse**.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. Inserire il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. È necessario creare il disco su un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host di un cluster di failover di Windows Server che utilizza CSV. Inserire il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. Assicurarsi che l'host su cui si sta creando il disco sia il proprietario del gruppo di cluster.

7. Nella pagina Drive Properties, specificare le proprietà del disco:

Proprietà	Descrizione
Assegnazione automatica del punto di montaggio	SnapCenter assegna automaticamente un punto di montaggio del volume in base al disco di sistema. Ad esempio, se il disco di sistema è C:, l'assegnazione automatica crea un punto di montaggio del volume sotto l'unità C:. L'assegnazione automatica non è supportata per i dischi condivisi.
Assegnare la lettera dell'unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.
Utilizzare il punto di montaggio del volume	Montare il disco sul percorso specificato nel campo adiacente. La directory principale del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.

Proprietà	Descrizione
Non assegnare la lettera del disco o il punto di montaggio del volume	Scegliere questa opzione se si preferisce montare il disco manualmente in Windows.
Dimensione del LUN	Specificare la dimensione del LUN; almeno 150 MB. Selezionare MB, GB o TB nell'elenco a discesa adiacente.
Utilizzare il thin provisioning per il volume che ospita questo LUN	Eseguire il thin provisioning del LUN. Il thin provisioning alloca solo lo spazio di storage necessario alla volta, consentendo al LUN di crescere in modo efficiente fino alla massima capacità disponibile. Assicurarsi che sul volume sia disponibile spazio sufficiente per ospitare tutto lo storage LUN che si ritiene necessario.
Scegliere il tipo di partizione	Selezionare la partizione GPT per una tabella di partizione GUID o la partizione MBR per un record di avvio principale. Le partizioni MBR potrebbero causare problemi di disallineamento nei cluster di failover di Windows Server. I dischi di partizione UEFI (Unified Extensible firmware Interface) non sono supportati.

8. Nella pagina Map LUN (LUN mappa), selezionare iSCSI o FC Initiator (iniziatore iSCSI o FC) sull'host:

In questo campo…	Eseguire questa operazione…
Host	Fare doppio clic sul nome del gruppo di cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore. Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server.
Scegliere l'iniziatore host	Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host. È possibile selezionare più iniziatori FC se si utilizza FC con multipath i/o (MPIO).

9. Nella pagina Group Type (tipo gruppo), specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

Selezionare…	Se…
Creare un nuovo igroup per gli iniziatori selezionati	Si desidera creare un nuovo igroup per gli iniziatori selezionati.
Scegliere un igroup esistente o specificare un nuovo igroup per gli iniziatori selezionati	Si desidera specificare un igroup esistente per gli iniziatori selezionati o creare un nuovo igroup con il nome specificato. Digitare il nome dell'igroup nel campo **igroup name**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo.

10. Nella pagina Summary (Riepilogo), rivedere le selezioni e fare clic su **Finish** (fine).

    SnapCenter crea il LUN e lo connette all'unità o al percorso del disco specificato sull'host.

Ridimensionare un disco

È possibile aumentare o ridurre le dimensioni di un disco in base alle esigenze del sistema di storage.

A proposito di questa attività

- Per i LUN con thin provisioning, la dimensione della geometria del lun ONTAP viene visualizzata come dimensione massima.
- Per i LUN con thick provisioning, la dimensione espandibile (dimensione disponibile nel volume) viene visualizzata come dimensione massima.
- Le LUN con partizioni di tipo MBR hanno una dimensione massima di 2 TB.
- Le LUN con partizioni di tipo GPT hanno un limite di dimensioni del sistema storage di 16 TB.
- È consigliabile creare un'istantanea prima di ridimensionare un LUN.
- Per ripristinare una LUN da una Snapshot creata prima del ridimensionamento della LUN, SnapCenter ridimensiona automaticamente il LUN alla dimensione della Snapshot.

  Dopo l'operazione di ripristino, i dati aggiunti al LUN dopo il ridimensionamento devono essere ripristinati da una Snapshot creata dopo il ridimensionamento.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa host.

   I dischi sono elencati.

4. Selezionare il disco che si desidera ridimensionare, quindi fare clic su **Ridimensiona**.

5. Nella finestra di dialogo Ridimensiona disco, utilizzare lo strumento a scorrimento per specificare le nuove dimensioni del disco oppure inserire le nuove dimensioni nel campo dimensione.

   Se si inserisce la dimensione manualmente, è necessario fare clic all'esterno del campo dimensione prima che il pulsante Riduci o Espandi sia attivato correttamente. Inoltre, è necessario fare clic su MB, GB o TB per specificare l'unità di misura.

6. Quando si è soddisfatti delle voci immesse, fare clic su **Riduci** o **Espandi**, a seconda dei casi.

   SnapCenter ridimensiona il disco.

Collegare un disco

È possibile utilizzare la procedura guidata Connect Disk per connettere un LUN esistente a un host o per riconnettere un LUN disconnesso.

Prima di iniziare

- È necessario aver avviato il servizio FC o iSCSI sul sistema di storage.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di storage.
- Non è possibile connettere un LUN a più di un host a meno che il LUN non sia condiviso dagli host in un cluster di failover di Windows Server.
- Se il LUN è condiviso da host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario collegare il disco all'host proprietario del gruppo di cluster.
- Il plug-in per Windows deve essere installato solo sull'host su cui si sta collegando il disco.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.
4. Fare clic su **Connect** (Connetti).

   Viene visualizzata la procedura guidata Connect Disk.

5. Nella pagina LUN Name (Nome LUN), identificare il LUN a cui connettersi:

In questo campo…	Eseguire questa operazione…
Sistema storage	Selezionare la SVM per il LUN.
Percorso LUN	Fare clic su **Browse** (Sfoglia) per selezionare il percorso completo del volume contenente il LUN.
Nome del LUN	Immettere il nome del LUN.

In questo campo…	Eseguire questa operazione…
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. Le dimensioni del cluster dipendono dal sistema operativo e dalle applicazioni.
Etichetta LUN	Se si desidera, inserire un testo descrittivo per il LUN.

6. Nella pagina Disk Type (tipo di disco), selezionare il tipo di disco:

Selezionare…	Se…
Disco dedicato	È possibile accedere al LUN solo da un host.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. È necessario connettere il disco a un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host di un cluster di failover di Windows Server che utilizza CSV. Assicurarsi che l'host su cui ci si connette al disco sia il proprietario del gruppo di cluster.

7. Nella pagina Drive Properties, specificare le proprietà del disco:

Proprietà	Descrizione
Assegnazione automatica	Consentire a SnapCenter di assegnare automaticamente un punto di montaggio del volume in base al disco di sistema. Ad esempio, se il disco di sistema è C:, la proprietà di assegnazione automatica crea un punto di montaggio del volume sotto l'unità C:. La proprietà di assegnazione automatica non è supportata per i dischi condivisi.
Assegnare la lettera dell'unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.

Proprietà	Descrizione
Utilizzare il punto di montaggio del volume	Montare il disco sul percorso specificato nel campo adiacente. La directory principale del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.
Non assegnare la lettera del disco o il punto di montaggio del volume	Scegliere questa opzione se si preferisce montare il disco manualmente in Windows.

8. Nella pagina Map LUN (LUN mappa), selezionare iSCSI o FC Initiator (iniziatore iSCSI o FC) sull'host:

In questo campo…	Eseguire questa operazione…
Host	Fare doppio clic sul nome del gruppo di cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore. Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server.
Scegliere l'iniziatore host	Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host. È possibile selezionare più iniziatori FC se si utilizza FC con MPIO.

9. Nella pagina Group Type (tipo di gruppo), specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

Selezionare…	Se…
Creare un nuovo igroup per gli iniziatori selezionati	Si desidera creare un nuovo igroup per gli iniziatori selezionati.
Scegliere un igroup esistente o specificare un nuovo igroup per gli iniziatori selezionati	Si desidera specificare un igroup esistente per gli iniziatori selezionati o creare un nuovo igroup con il nome specificato. Digitare il nome dell'igroup nel campo **igroup name**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo.

10. Nella pagina Summary (Riepilogo), rivedere le selezioni e fare clic su **Finish** (fine).

    SnapCenter connette il LUN all'unità o al percorso del disco specificato sull'host.

Scollegare un disco

È possibile disconnettere un LUN da un host senza influire sul contenuto del LUN, con un'eccezione: Se si disconnette un clone prima che sia stato separato, il contenuto del clone viene perso.

Prima di iniziare

- Assicurarsi che il LUN non sia in uso da nessuna applicazione.
- Assicurarsi che il LUN non venga monitorato con il software di monitoraggio.
- Se il LUN è condiviso, assicurarsi di rimuovere le dipendenze delle risorse del cluster dal LUN e verificare che tutti i nodi del cluster siano accesi, funzionino correttamente e disponibili per SnapCenter.

A proposito di questa attività

Se si disconnette un LUN in un volume FlexClone creato da SnapCenter e non sono connessi altri LUN sul volume, SnapCenter elimina il volume. Prima di disconnettere il LUN, SnapCenter visualizza un messaggio che avvisa che il volume FlexClone potrebbe essere stato eliminato.

Per evitare l'eliminazione automatica del volume FlexClone, rinominare il volume prima di disconnettere l'ultimo LUN. Quando si rinomina il volume, assicurarsi di modificare più caratteri rispetto all'ultimo carattere del nome.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

4. Selezionare il disco che si desidera disconnettere, quindi fare clic su **Disconnetti**.
5. Nella finestra di dialogo Disconnetti disco, fare clic su **OK**.

   SnapCenter disconnette il disco.

Eliminare un disco

È possibile eliminare un disco quando non è più necessario. Una volta eliminato un disco, non è possibile annullarlo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **dischi**.
3. Selezionare l'host dall'elenco a discesa **host**.

   I dischi sono elencati.

4. Selezionare il disco che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Delete Disk (Elimina disco), fare clic su **OK**.

   SnapCenter elimina il disco.

Creare e gestire le condivisioni SMB

Per configurare una condivisione SMB3 su una macchina virtuale di storage (SVM), è possibile utilizzare l'interfaccia utente di SnapCenter o i cmdlet PowerShell.

Procedura consigliata: l'utilizzo dei cmdlet è consigliato in quanto consente di sfruttare i modelli forniti con SnapCenter per automatizzare la configurazione delle condivisioni.

I modelli incapsulano le Best practice per la configurazione di volumi e condivisioni. I modelli sono disponibili nella cartella modelli della cartella di installazione del pacchetto di plug-in SnapCenter per Windows.

Se ti senti a tuo agio, puoi creare i tuoi modelli seguendo i modelli forniti. Prima di creare un modello personalizzato, esaminare i parametri contenuti nella documentazione del cmdlet.

Creare una condivisione SMB

È possibile utilizzare la pagina condivisioni SnapCenter per creare una condivisione SMB3 su una macchina virtuale di storage (SVM).

Non è possibile utilizzare SnapCenter per eseguire il backup dei database sulle condivisioni SMB. Il supporto SMB è limitato solo al provisioning.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **shares**.
3. Selezionare la SVM dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage).
4. Fare clic su **nuovo**.

   Viene visualizzata la finestra di dialogo Nuova condivisione.

5. Nella finestra di dialogo New Share (Nuova condivisione), definire la condivisione:

In questo campo…	Eseguire questa operazione…
Descrizione	Inserire un testo descrittivo per la condivisione.

In questo campo…	Eseguire questa operazione…
Nome di condivisione	Inserire il nome della condivisione, ad esempio test_share. Il nome immesso per la condivisione verrà utilizzato anche come nome del volume. Il nome della condivisione: • Deve essere una stringa UTF-8. • Non deve includere i seguenti caratteri: Caratteri di controllo da 0x00 a 0x1F (entrambi inclusi), 0x22 (virgolette doppie) e i caratteri speciali `\ / [ ] : (vertical bar) < > + = ; , ?`
Percorso di condivisione	• Fare clic nel campo per immettere un nuovo percorso del file system, ad esempio /. • Fare doppio clic nel campo per selezionare da un elenco di percorsi del file system esistenti.

6. Quando si è soddisfatti delle voci immesse, fare clic su **OK**.

   SnapCenter crea la condivisione SMB sulla SVM.

Eliminare una condivisione SMB

È possibile eliminare una condivisione SMB quando non è più necessaria.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina host, fare clic su **shares**.
3. Nella pagina Shares (condivisioni), fare clic nel campo **Storage Virtual Machine** (macchina virtuale di storage) per visualizzare un elenco a discesa con un elenco di macchine virtuali di storage disponibili (SVM), quindi selezionare la SVM per la condivisione che si desidera eliminare.
4. Dall'elenco delle condivisioni di SVM, selezionare la condivisione che si desidera eliminare e fare clic su **Delete** (Elimina).
5. Nella finestra di dialogo Elimina condivisione, fare clic su **OK**.

   SnapCenter elimina la condivisione SMB dalla SVM.

Recuperare spazio sul sistema storage

Sebbene NTFS rilevi lo spazio disponibile su un LUN quando i file vengono cancellati o modificati, non riporta le nuove informazioni al sistema di storage. È possibile eseguire il cmdlet PowerShell per la rigenerazione dello spazio nel plug-in per l'host Windows per assicurarsi che i blocchi appena liberati siano contrassegnati come disponibili nello

storage.

Se si esegue il cmdlet su un host plug-in remoto, è necessario eseguire il cmdlet SnapCenterOpen-SMConnection per aprire una connessione al server SnapCenter.

Prima di iniziare

- Prima di eseguire un'operazione di ripristino, assicurarsi che il processo di recupero dello spazio sia stato completato.
- Se il LUN è condiviso da host in un cluster di failover di Windows Server, è necessario eseguire la rigenerazione dello spazio sull'host proprietario del gruppo di cluster.
- Per ottenere performance di storage ottimali, è necessario eseguire il recupero dello spazio il più spesso possibile.

  Assicurarsi che sia stata eseguita la scansione dell'intero file system NTFS.

A proposito di questa attività

- Il recupero di spazio richiede tempo e richiede molta CPU, quindi è consigliabile eseguire l'operazione quando l'utilizzo del sistema storage e dell'host Windows è basso.
- La bonifica dello spazio recupera quasi tutto lo spazio disponibile, ma non il 100%.
- Non eseguire la deframmentazione del disco contemporaneamente alla rigenerazione dello spazio.

  In questo modo, il processo di recupero può rallentare.

Passo

Dal prompt dei comandi PowerShell del server applicativo, immettere il seguente comando:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

Drive_path è il percorso del disco mappato al LUN.

Eseguire il provisioning dello storage utilizzando i cmdlet PowerShell

Se non si desidera utilizzare l'interfaccia utente grafica di SnapCenter per eseguire attività di provisioning host e recupero spazio, è possibile utilizzare i cmdlet di PowerShell. È possibile utilizzare i cmdlet direttamente o aggiungerli agli script.

Se si eseguono i cmdlet su un host plug-in remoto, è necessario eseguire il cmdlet SnapCenter Open-SMConnection per aprire una connessione al server SnapCenter.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Se i cmdlet PowerShell di SnapCenter vengono danneggiati a causa della rimozione di SnapDrive per Windows dal server, fare riferimento a. "I cmdlet di SnapCenter sono guasti quando SnapDrive per Windows viene disinstallato".

Eseguire il provisioning dello storage in ambienti VMware

È possibile utilizzare il plug-in SnapCenter per Microsoft Windows in ambienti VMware per creare e gestire LUN e Snapshot.

Piattaforme del sistema operativo guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni cluster Microsoft

  Supporto per un massimo di 16 nodi supportati su VMware quando si utilizza Microsoft iSCSI Software Initiator o fino a due nodi utilizzando FC

- LUN RDM

  Supporto per un massimo di 56 LUN RDM con quattro controller LSI Logic SCSI per RDMS normale o 42 LUN RDM con tre controller LSI Logic SCSI su un plug-in box-to-box MSCS VMware per configurazione Windows

  Supporta il controller SCSI paravirtuale VMware. È possibile supportare 256 dischi sui dischi RDM.

Limitazioni relative al server VMware ESXi

- L'installazione del plug-in per Windows su un cluster Microsoft su macchine virtuali che utilizzano le credenziali ESXi non è supportata.

  Utilizzare le credenziali vCenter per installare il plug-in per Windows su macchine virtuali in cluster.

- Tutti i nodi in cluster devono utilizzare lo stesso ID di destinazione (sull'adattatore SCSI virtuale) per lo stesso disco in cluster.
- Quando si crea un LUN RDM all'esterno del plug-in per Windows, è necessario riavviare il servizio plug-in per consentire il riconoscimento del disco appena creato.
- Non è possibile utilizzare gli iniziatori iSCSI e FC contemporaneamente su un sistema operativo guest VMware.

Privilegi minimi vCenter richiesti per le operazioni RDM di SnapCenter

Per eseguire operazioni RDM in un sistema operativo guest, è necessario disporre dei seguenti privilegi vCenter sull'host:

- Datastore: Rimuovere il file
- Host: Configuration > Storage Partition Configuration (Configurazione > Configurazione partizione storage)
- Macchina virtuale: Configurazione

È necessario assegnare questi privilegi a un ruolo a livello di Virtual Center Server. Il ruolo a cui si assegnano questi privilegi non può essere assegnato a nessun utente senza privilegi root.

Dopo aver assegnato questi privilegi, è possibile installare il plug-in per Windows sul sistema operativo guest.

Gestire LUN RDM FC in un cluster Microsoft

È possibile utilizzare il plug-in per Windows per gestire un cluster Microsoft utilizzando LUN RDM FC, ma è

necessario prima creare il quorum RDM condiviso e lo storage condiviso all'esterno del plug-in, quindi aggiungere i dischi alle macchine virtuali del cluster.

A partire da ESXi 5.5, è possibile utilizzare anche l'hardware ESX iSCSI e FCoE per gestire un cluster Microsoft. Il plug-in per Windows include il supporto immediato per i cluster Microsoft.

Requisiti

Il plug-in per Windows fornisce il supporto per i cluster Microsoft che utilizzano LUN RDM FC su due macchine virtuali diverse che appartengono a due server ESX o ESXi diversi, noti anche come cluster tra le diverse caselle, quando si soddisfano requisiti di configurazione specifici.

- Le macchine virtuali (VM) devono eseguire la stessa versione di Windows Server.
- Le versioni dei server ESX o ESXi devono essere le stesse per ogni host VMware principale.
- Ogni host principale deve disporre di almeno due adattatori di rete.
- Deve essere presente almeno un datastore VMware Virtual Machine file System (VMFS) condiviso tra i due server ESX o ESXi.
- VMware consiglia di creare il datastore condiviso su una SAN FC.

  Se necessario, il datastore condiviso può essere creato anche su iSCSI.

- Il LUN RDM condiviso deve essere in modalità di compatibilità fisica.
- Il LUN RDM condiviso deve essere creato manualmente all'esterno del plug-in per Windows.

  Non è possibile utilizzare dischi virtuali per lo storage condiviso.

- È necessario configurare un controller SCSI su ciascuna macchina virtuale del cluster in modalità di compatibilità fisica:

  Windows Server 2008 R2 richiede la configurazione del controller SCSI SAS LSI Logic su ciascuna macchina virtuale. I LUN condivisi non possono utilizzare il controller SAS LSI Logic esistente se ne esiste uno solo e se è già collegato all'unità C.

  I controller SCSI di tipo paravirtuale non sono supportati dai cluster VMware Microsoft.

  > Quando si aggiunge un controller SCSI a un LUN condiviso su una macchina virtuale in modalità di compatibilità fisica, è necessario selezionare l'opzione **Raw Device Mapping** (RDM) e non l'opzione **Create a new disk** (Crea nuovo disco) in VMware Infrastructure Client.

- I cluster di macchine virtuali Microsoft non possono far parte di un cluster VMware.
- Quando si installa il plug-in per Windows su macchine virtuali appartenenti a un cluster Microsoft, è necessario utilizzare le credenziali vCenter e non le credenziali ESX o ESXi.
- Il plug-in per Windows non può creare un singolo igroup con iniziatori da più host.

  L'igroup contenente gli iniziatori di tutti gli host ESXi deve essere creato sul controller dello storage prima di creare le LUN RDM che verranno utilizzate come dischi del cluster condivisi.

- Assicurarsi di creare un LUN RDM su ESXi 5.0 utilizzando un iniziatore FC.

  Quando si crea un LUN RDM, viene creato un gruppo iniziatore con ALUA.

Limitazioni

Il plug-in per Windows supporta cluster Microsoft che utilizzano LUN RDM FC/iSCSI su macchine virtuali diverse appartenenti a server ESX o ESXi diversi.

Questa funzione non è supportata nelle versioni precedenti a ESX 5.5i.

- Il plug-in per Windows non supporta cluster su datastore ESX iSCSI e NFS.
- Il plug-in per Windows non supporta gli iniziatori misti in un ambiente cluster.

  Gli iniziatori devono essere FC o Microsoft iSCSI, ma non entrambi.
- Gli iniziatori iSCSI ESX e gli HBA non sono supportati sui dischi condivisi in un cluster Microsoft.
- Il plug-in per Windows non supporta la migrazione delle macchine virtuali con vMotion se la macchina virtuale fa parte di un cluster Microsoft.
- Il plug-in per Windows non supporta MPIO su macchine virtuali in un cluster Microsoft.

Creare un LUN FC RDM condiviso

Prima di poter utilizzare le LUN RDM FC per condividere lo storage tra i nodi di un cluster Microsoft, è necessario creare il disco di quorum condiviso e il disco di storage condiviso, quindi aggiungerli a entrambe le macchine virtuali del cluster.

Il disco condiviso non viene creato utilizzando il plug-in per Windows. Creare e aggiungere il LUN condiviso a ciascuna macchina virtuale del cluster. Per informazioni, vedere "Cluster di macchine virtuali tra host fisici".

Aggiunta di licenze SnapCenter basate su controller standard

Se si utilizzano i controller di storage FAS, AFF o ASA, è necessaria una licenza basata su controller standard SnapCenter.

La licenza basata su controller ha le seguenti caratteristiche:

- Diritto standard SnapCenter incluso con l'acquisto di bundle premium o flash (non con il pacchetto base)
- Utilizzo illimitato dello storage
- Aggiunto direttamente al controller di archiviazione FAS, AFF o ASA tramite ONTAP System Manager o ONTAP CLI.

  Per le licenze basate sul controller SnapCenter non è necessario immettere alcuna informazione sulla licenza nell'interfaccia utente SnapCenter .
- Bloccato sul numero di serie del controller

Per informazioni sulle licenze richieste, vedere "Licenze SnapCenter".

Fase 1: Verificare che la licenza della suite SnapManager sia installata

È possibile utilizzare l'interfaccia utente SnapCenter per verificare se una licenza SnapManager Suite è installata sui sistemi di archiviazione primari FAS, AFF o ASA e identificare quali sistemi necessitano di

licenze. Le licenze di SnapManager Suite si applicano solo a SVM o cluster FAS, AFF e ASA su sistemi di storage primari.

Se sul controller è già presente una licenza SnapManager Suite, SnapCenter fornisce automaticamente il diritto alla licenza Standard basata sul controller. I nomi licenza SnapManagerSuite e licenza basata su controller SnapCenter Standard vengono utilizzati in modo intercambiabile, ma si riferiscono alla stessa licenza.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Storage Systems**.
2. Nella pagina Storage Systems (sistemi storage), dal menu a discesa **Type** (tipo), selezionare se visualizzare tutte le SVM o i cluster aggiunti:
   - Per visualizzare tutte le SVM aggiunte, selezionare **ONTAP SVM**.
   - Per visualizzare tutti i cluster aggiunti, selezionare **ONTAP Clusters**.

     Quando si seleziona il nome del cluster, tutte le SVM che fanno parte del cluster vengono visualizzate nella sezione Storage Virtual Machines (macchine virtuali di storage).
3. Nell'elenco Storage Connections (connessioni storage), individuare la colonna Controller License (licenza controller).

   La colonna Controller License (licenza controller) visualizza il seguente stato:

   -  Indica che una licenza della suite SnapManager è installata su un sistema di storage primario FAS, AFF o ASA.
   -  Indica che la licenza della suite SnapManager non è installata su un sistema di storage primario FAS, AFF o ASA.
   - Non applicabile indica che una licenza della suite SnapManager non è applicabile perché lo storage controller è su Amazon FSX per piattaforme di storage NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select o secondarie.

Fase 2: Identificare le licenze installate sul controller

È possibile utilizzare la riga di comando ONTAP per visualizzare tutte le licenze installate sul controller. È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.

Il controller visualizza la licenza basata sul controller SnapCenter Standard come licenza SnapManagerSuite.

Fasi

1. Accedere al controller NetApp utilizzando la riga di comando ONTAP.
2. Immettere il comando license show, quindi visualizzare l'output per verificare se la licenza SnapManagerSuite è installata.

Output di esempio

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
Base              site     Cluster Base License     -

Serial Number: 1-81-0000000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

Nell'esempio, la licenza SnapManagerSuite è installata, pertanto non sono richieste ulteriori azioni di licenza SnapCenter.

Fase 3: Recuperare il numero di serie del controller

Ottenere il numero di serie del controller utilizzando la riga di comando ONTAP . Per ottenere il numero di serie della licenza basata sul controller, è necessario essere un amministratore del cluster sul sistema FAS, AFF o ASA .

Fasi

1. Accedere al controller utilizzando la riga di comando ONTAP.
2. Immettere il comando show -instance del sistema, quindi esaminare l'output per individuare il numero di serie del controller.

Output di esempio

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Annotare i numeri di serie.

Fase 4: Recuperare il numero di serie della licenza basata su controller

Se si utilizza un archivio FAS, ASA o AFF , è possibile recuperare la licenza basata sul controller SnapCenter dal sito di supporto NetApp prima di installarla utilizzando la riga di comando ONTAP .

Prima di iniziare

- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.

  Se non inserisci credenziali valide, il sistema non restituirà alcuna informazione per la tua ricerca.

- Il numero di serie del controller dovrebbe essere disponibile.

Fasi

1. Accedere a. "Sito di supporto NetApp".
2. Accedere a **sistemi** > **licenze software**.
3. Nell'area Selection Criteria (Criteri di selezione), assicurarsi che sia selezionato Serial Number (numero di serie) (situato sul retro dell'unità), inserire il numero di serie del controller, quindi selezionare **Go!** (Vai).

   Viene visualizzato un elenco di licenze per il controller specificato.

4. Individuare e registrare la licenza di SnapCenter o SnapManagerSuite.

Fase 5: Aggiungere una licenza basata su controller

È possibile utilizzare la riga di comando ONTAP per aggiungere una licenza basata su controller SnapCenter quando si utilizzano sistemi FAS, AFF o ASA e si dispone di una licenza SnapCenter o SnapManagerSuite.

Prima di iniziare

- È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.
- È necessario disporre della licenza standard o SnapManagerSuite di SnapCenter.

A proposito di questa attività

Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA, è possibile ottenere una licenza di valutazione Premium Bundle da installare sul controller.

Se si desidera installare SnapCenter in prova, contattare il rappresentante commerciale per ottenere una licenza di valutazione del bundle Premium da installare sul controller.

Fasi

1. Accedere al cluster NetApp utilizzando la riga di comando ONTAP.
2. Aggiungere la chiave di licenza SnapManagerSuite:

   ```
   system license add -license-code license_key
   ```

   Questo comando è disponibile a livello di privilegio admin.

3. Verificare che la licenza SnapManagerSuite sia installata:

   ```
   license show
   ```

Fase 6: Rimuovere la licenza di prova

Se si utilizza una licenza SnapCenter Standard basata su controller e si ha bisogno di rimuovere la licenza di prova basata sulla capacità (numero di serie che termina con “50”), è necessario utilizzare i comandi MySQL per rimuovere manualmente la licenza di prova. La licenza di prova non può essere eliminata tramite l’interfaccia utente SnapCenter .

La rimozione manuale di una licenza di prova è necessaria solo se si utilizza una licenza basata su controller standard SnapCenter.

Fasi

1. Sul server SnapCenter, aprire una finestra PowerShell per reimpostare la password MySQL.
   a. Eseguire il cmdlet Open-SmConnection per stabilire una connessione con SnapCenter Server per un account SnapCenterAdmin.
   b. Eseguire Set-SmRepositoryPassword per reimpostare la password MySQL.

      Per informazioni sui cmdlet, vedere "Guida di riferimento al cmdlet del software SnapCenter" .
2. Aprire il prompt dei comandi ed eseguire mysql -u root -p per accedere a MySQL.

   MySQL richiede la password. Immettere le credenziali fornite durante la reimpostazione della password.
3. Rimuovere la licenza di prova dal database:

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

Configurare la disponibilità elevata

Configurare i server SnapCenter per la disponibilità elevata

Per supportare l’alta disponibilità (ha) in SnapCenter in esecuzione su Windows o su Linux, è possibile installare il bilanciamento del carico F5. F5 consente al server SnapCenter di supportare configurazioni Active-passive in un massimo di due host che si trovano nella stessa posizione. Per utilizzare F5 Load Balancer in SnapCenter, è necessario configurare i server SnapCenter e il bilanciamento del carico F5.

È inoltre possibile configurare il bilanciamento del carico di rete (NLB) per impostare la disponibilità elevata di SnapCenter. È necessario configurare manualmente NLB al di fuori dell’installazione di SnapCenter per garantire la disponibilità elevata.

Per gli ambienti cloud, è possibile configurare l’high Availability utilizzando l’Elastic Load Balancing (ELB) di Amazon Web Services (AWS) e il bilanciamento del carico di Azure.

Configurare la disponibilità elevata utilizzando F5

Per istruzioni su come configurare i server SnapCenter per l'elevata disponibilità utilizzando il bilanciatore di carico F5, fare riferimento a "Come configurare i server SnapCenter per l'alta disponibilità utilizzando F5 Load Balancer" .

Per aggiungere e rimuovere i cluster F5, è necessario essere membri del gruppo amministratori locali sui server SnapCenter (oltre che essere assegnati al ruolo SnapCenterAdmin):

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

  Per ulteriori informazioni, fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Ulteriori informazioni

- Dopo aver installato e configurato SnapCenter per la disponibilità elevata, modificare il collegamento al desktop di SnapCenter in modo che punti all'IP del cluster F5.
- Se si verifica un failover tra i server SnapCenter e se esiste anche una sessione SnapCenter, chiudere il browser e accedere nuovamente a SnapCenter.
- Nell'impostazione del bilanciamento del carico (NLB o F5), se si aggiunge un host parzialmente risolto dall'host NLB o F5 e se l'host SnapCenter non è in grado di raggiungere questo host, la pagina host SnapCenter passa frequentemente dallo stato inattivo allo stato in esecuzione. Per risolvere questo problema, è necessario assicurarsi che entrambi gli host SnapCenter siano in grado di risolvere l'host in NLB o F5 host.
- I comandi SnapCenter per le impostazioni MFA devono essere eseguiti su tutti gli host. La configurazione della parte di base deve essere eseguita nel server Active Directory Federation Services (ad FS) utilizzando i dettagli del cluster F5. L'accesso all'interfaccia utente SnapCenter a livello di host viene bloccato dopo l'attivazione di MFA.
- Durante il failover, le impostazioni del registro di controllo non verranno applicate al secondo host. Pertanto, è necessario ripetere manualmente le impostazioni del registro di controllo sull'host passivo F5 quando diventa attivo.

Configurare la disponibilità elevata utilizzando il bilanciamento del carico di rete (NLB)

È possibile configurare il bilanciamento del carico di rete (NLB, Network Load Balancing) per impostare la disponibilità elevata di SnapCenter. È necessario configurare manualmente NLB al di fuori dell'installazione di SnapCenter per garantire la disponibilità elevata.

Per informazioni su come configurare il bilanciamento del carico di rete (NLB) con SnapCenter, fare riferimento a "Come configurare NLB con SnapCenter".

Configurare l'high Availability utilizzando il bilanciamento del carico elastico (ELB) di AWS

Puoi configurare un ambiente SnapCenter a disponibilità elevata in Amazon Web Services (AWS) configurando due server SnapCenter in zone di disponibilità separate e configurandoli per il failover automatico. L'architettura include indirizzi IP privati virtuali, tabelle di routing e sincronizzazione tra database MySQL attivi e in standby.

Fasi

1. Configurare l'IP overlay privato virtuale in AWS. Per informazioni, fare riferimento alla "Configurare l'IP overlay privato virtuale".

2. Preparare l'host Windows
    a. Forza IPv4 con priorità superiore a IPv6:
        - Posizione: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
        - Chiave: DisabledComponents
        - Digitare: REG_DWORD
        - Valore: 0x20
    b. Assicurarsi che i nomi di dominio completi possano essere risolti tramite DNS o tramite la configurazione dell'host locale agli indirizzi IPv4.
    c. Assicurarsi di non avere un proxy di sistema configurato.
    d. Assicurarsi che la password dell'amministratore sia la stessa su entrambi i server Windows quando si utilizza un'installazione senza Active Directory e che i server non si trovino in un dominio.
    e. Aggiungere un IP virtuale su entrambi i server Windows.
3. Creare il cluster SnapCenter.
    a. Avvia PowerShell e connettiti a SnapCenter. `Open-SmConnection`
    b. Creare il cluster. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
    c. Aggiungere il server secondario. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
    d. Scopri i dettagli sull'alta disponibilità. `Get-SmServerConfig`
4. Creare la funzione Lamda per regolare la tabella di routing nel caso in cui l'endpoint IP privato virtuale non sia disponibile, monitorato da AWS CloudWatch. Per informazioni, fare riferimento alla "Creare una funzione Lambda".
5. Creare un monitor in CloudWatch per monitorare la disponibilità dell'endpoint SnapCenter. Un allarme è configurato per attivare una funzione Lambda se l'endpoint non è raggiungibile. La funzione Lambda regola la tabella di routing per reindirizzare il traffico al server SnapCenter attivo. Per informazioni, fare riferimento alla "Creare canari sintetici".
6. Implementare il flusso di lavoro utilizzando una funzione STEP come alternativa al monitoraggio di CloudWatch, fornendo tempi di failover ridotti. Il flusso di lavoro include una funzione sonda lambda per verificare l'URL SnapCenter, una tabella DynamoDB per la memorizzazione dei conteggi degli errori e la funzione Step stessa.
    a. Utilizzare una funzione lambda per esaminare l'URL SnapCenter. Per informazioni, fare riferimento alla "Crea funzione Lambda".
    b. Creare una tabella DynamoDB per memorizzare il conteggio degli errori tra due iterazioni della funzione Step. Per informazioni, fare riferimento alla "Iniziate con la tabella DynamoDB".
    c. Creare la funzione Step. Per informazioni, fare riferimento alla "Documentazione della funzione STEP".
    d. Eseguire il test di una singola fase.
    e. Testare la funzione completa.
    f. Creare un ruolo IAM e regolare le autorizzazioni per eseguire la funzione Lambda.

g. Creare un programma per attivare la funzione Step (fase). Per informazioni, fare riferimento alla "Utilizzo di Amazon EventBridge Scheduler per avviare le funzioni Step".

Configurare la high Availability utilizzando il bilanciamento del carico di Azure

Puoi configurare un ambiente SnapCenter ad alta disponibilità usando il bilanciamento del carico Azure.

Fasi

1. Crea macchine virtuali in un set scale utilizzando il portale di Azure. Il set di scalabilità delle macchine virtuali Azure consente di creare e gestire un gruppo di macchine virtuali con bilanciamento del carico. Il numero di istanze di macchine virtuali può aumentare o diminuire automaticamente in risposta alla richiesta o a una pianificazione definita. Per informazioni, fare riferimento alla "Crea macchine virtuali in un set scale utilizzando il portale di Azure".
2. Dopo aver configurato le macchine virtuali, accedere a ciascuna macchina virtuale nel set di macchine virtuali e installare il server SnapCenter in entrambi i nodi.
3. Creare il cluster nell'host 1. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. Aggiungere il server secondario. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. Ottenere i dettagli sull'alta disponibilità. `Get-SmServerConfig`
6. Se necessario, ricostruire l'host secondario. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Eseguire il failover sul secondo host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== passare da NLB a F5 per l'alta disponibilità

È possibile modificare la configurazione SnapCenter ha da bilanciamento del carico di rete (NLB) per utilizzare bilanciamento del carico F5.

Fasi

1. Configurare i server SnapCenter per la disponibilità elevata utilizzando F5. "Scopri di più".
2. Sull'host del server SnapCenter, avviare PowerShell.
3. Avviare una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
4. Aggiornare il server SnapCenter in modo che punti all'indirizzo IP del cluster F5 utilizzando il cmdlet Update-SmServerCluster.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Alta disponibilità per il repository MySQL di SnapCenter

La replica MySQL è una funzionalità di MySQL Server che consente di replicare i dati da un server database MySQL (master) a un altro server database MySQL (slave). SnapCenter supporta la replica MySQL per l'alta disponibilità solo su due nodi abilitati per

il bilanciamento del carico di rete (abilitati per NLB).

SnapCenter esegue operazioni di lettura o scrittura sul repository master e instrada la connessione al repository slave in caso di errore nel repository master. Il repository slave diventa quindi il repository master. SnapCenter supporta inoltre la replica inversa, che viene attivata solo durante il failover.

Se si desidera utilizzare la funzionalità di disponibilità elevata (ha) di MySQL, è necessario configurare Network Load Balancer (NLB) sul primo nodo. Il repository MySQL viene installato su questo nodo come parte dell'installazione. Durante l'installazione di SnapCenter sul secondo nodo, è necessario unirsi alla F5 del primo nodo e creare una copia del repository MySQL sul secondo nodo.

SnapCenter fornisce i cmdlet *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* PowerShell per gestire la replica MySQL.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

È necessario conoscere le limitazioni relative alla funzionalità MySQL ha:

- NLB e MySQL ha non sono supportati oltre due nodi.
- Il passaggio da un'installazione standalone SnapCenter a un'installazione NLB o viceversa e il passaggio da un'installazione standalone MySQL a MySQL ha non sono supportati.
- Il failover automatico non è supportato se i dati del repository slave non sono sincronizzati con i dati del repository master.

  È possibile avviare un failover forzato utilizzando il cmdlet *set-SmRepositoryConfig*.

- Quando viene avviato il failover, i processi in esecuzione potrebbero non riuscire.

  Se il failover si verifica perché il server MySQL o SnapCenter non è attivo, i processi in esecuzione potrebbero non riuscire. Dopo aver eseguito il failover sul secondo nodo, tutti i processi successivi vengono eseguiti correttamente.

Per informazioni sulla configurazione della disponibilità elevata, vedere "Come configurare NLB e ARR con SnapCenter".

Configurare RBAC (role-based access control)

Creare un ruolo

Oltre a utilizzare i ruoli SnapCenter esistenti, è possibile creare i propri ruoli e personalizzare le autorizzazioni.

Per creare i propri ruoli, è necessario accedere con il ruolo "SnapCenterAdmin".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **ruoli**.
3. Fare clic su  .

4. Specificare un nome e una descrizione per il nuovo ruolo.

   Nei nomi utente e nei nomi di gruppo è possibile utilizzare solo i seguenti caratteri speciali: spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:).

5. Selezionare **tutti i membri di questo ruolo possono visualizzare gli oggetti degli altri membri** per consentire agli altri membri del ruolo di visualizzare risorse come volumi e host dopo l'aggiornamento dell'elenco delle risorse.

   Deselezionare questa opzione se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri.

   Quando questa opzione è attivata, l'assegnazione dell'accesso degli utenti agli oggetti o alle risorse non è necessaria se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

6. Nella pagina autorizzazioni, selezionare le autorizzazioni che si desidera assegnare al ruolo o fare clic su **Seleziona tutto** per concedere tutte le autorizzazioni al ruolo.
7. Fare clic su **Invia**.

Aggiungi un ruolo RBAC di NetApp ONTAP utilizzando i comandi di login e sicurezza

Puoi utilizzare i comandi di login alla sicurezza per aggiungere un ruolo RBAC di NetApp ONTAP quando i tuoi sistemi storage eseguono Clustered ONTAP.

Prima di iniziare

- Identifica l'attività (o le attività) che vuoi svolgere e i privilegi richiesti per eseguirle.
- Concedere privilegi alle directory dei comandi e/o dei comandi.

  Esistono due livelli di accesso per ogni directory di comando: All-access e Read-only.

  È sempre necessario assegnare prima i privilegi di accesso completo.

- Assegnare ruoli agli utenti.
- Identifica la tua configurazione a seconda che i plug-in SnapCenter siano connessi all'IP dell'amministratore del cluster per l'intero cluster o direttamente a una SVM all'interno del cluster.

A proposito di questa attività

Per semplificare la configurazione di questi ruoli sui sistemi di storage, è possibile utilizzare lo strumento RBAC User Creator per NetApp ONTAP, pubblicato sul NetApp Communities Forum.

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP. Ad esempio, lo strumento creazione utenti RBAC per NetApp ONTAP aggiunge automaticamente il Privileges nell'ordine corretto in modo che il Privileges ad accesso completo venga visualizzato per primo. Se si aggiungono prima i privilegi di sola lettura e poi i privilegi di accesso completo, ONTAP contrassegna i privilegi di accesso completo come duplicati e li ignora.

Se successivamente si aggiorna SnapCenter o ONTAP, è necessario eseguire nuovamente lo strumento creazione utenti RBAC per NetApp ONTAP per aggiornare i ruoli utente creati in precedenza. I ruoli utente creati per una versione precedente di SnapCenter o ONTAP non funzionano correttamente con le versioni aggiornate. Quando si esegue di nuovo, lo strumento gestisce automaticamente l'aggiornamento. Non è necessario ricreare i ruoli.

Per ulteriori informazioni sull'impostazione dei ruoli RBAC di ONTAP, vedere "Autenticazione amministratore di ONTAP 9 e guida all'alimentazione RBAC".

Fasi

1. Nel sistema di storage, creare un nuovo ruolo immettendo il seguente comando:

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - nome_svm è il nome della SVM. Se si lascia questo campo vuoto, per impostazione predefinita viene visualizzato l'amministratore del cluster.
   - role_name è il nome specificato per il ruolo.
   - Command è la funzionalità ONTAP.

     È necessario ripetere questo comando per ogni autorizzazione. Tenere presente che i comandi all-access devono essere elencati prima dei comandi di sola lettura.

   Per informazioni sull'elenco delle autorizzazioni, vedere "Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli e l'assegnazione delle autorizzazioni".

2. Creare un nome utente immettendo il seguente comando:

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name è il nome dell'utente che si sta creando.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.
   - nome_svm è il nome della SVM.

3. Assegnare il ruolo all'utente immettendo il seguente comando:

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <user_name> è il nome dell'utente creato al punto 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome della SVM.
   - <role_name> è il nome del ruolo creato nella fase 1.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.

4. Verificare che l'utente sia stato creato correttamente immettendo il seguente comando:

   ```
   security login show -vserver <svm_name\> -user-or-group-name <user_name\>
   ```

User_name è il nome dell'utente creato nel passaggio 3.

Creare ruoli SVM con privilegi minimi

Quando si crea un ruolo per un nuovo utente SVM in ONTAP, è necessario eseguire diversi comandi dell'interfaccia utente di ONTAP. Questo ruolo è necessario se si configurano le SVM in ONTAP per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

```
security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Liberare l'utente.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli SVM e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli SVM e assegnare autorizzazioni.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"snapmirror policy modify-rule" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"vserver export-policy delete" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

Creare ruoli SVM per i sistemi ASA R2

Per creare un ruolo per un nuovo utente SVM nei sistemi ASA r2 è necessario eseguire diversi comandi ONTAP CLI. Questo ruolo è obbligatorio se si configurano le SVM nei sistemi ASA r2 per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   http -authmethod password -role <SVM_Role_Name\>
   ```

3. Liberare l'utente.

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli SVM e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli SVM e assegnare autorizzazioni.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun igroup add" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume qtree modify" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"consistency-group" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all
- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

Creare ruoli cluster ONTAP con privilegi minimi

È necessario creare un ruolo di cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore di ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi dell'interfaccia utente di ONTAP per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi http -authmethod password -role <role_name\>
   ```

3. Liberare l'utente.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli cluster e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli cluster e assegnare autorizzazioni.

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun mapping show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"system license delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"vserver cifs share delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

Creare ruoli del cluster ONTAP per i sistemi ASA R2

È necessario creare un ruolo di cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore di ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi dell'interfaccia utente di ONTAP per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

```
security login role create –vserver <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```

Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

```
security login create -user <user_name\> -vserver <cluster_name\> -application
http -authmethod password -role <role_name\>
```

3. Liberare l'utente.

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli cluster e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli cluster e assegnare autorizzazioni.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"network interface modify" -access readonly

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"vserver export-policy show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

Aggiungere un utente o un gruppo e assegnare ruolo e risorse

Per configurare il controllo degli accessi basato sui ruoli per gli utenti SnapCenter, è possibile aggiungere utenti o gruppi e assegnare un ruolo. Il ruolo determina le opzioni a cui gli utenti SnapCenter possono accedere.

Prima di iniziare

- È necessario aver effettuato l'accesso come ruolo "SnapCenterAdmin".
- È necessario aver creato gli account utente o di gruppo in Active Directory nel sistema operativo o nel database. Non è possibile utilizzare SnapCenter per creare questi account.

  È possibile includere solo i seguenti caratteri speciali nei nomi degli utenti e dei gruppi: Spazio ( ), trattino (-), trattino basso (_) e due punti (:).

- SnapCenter include diversi ruoli predefiniti.

  È possibile assegnare questi ruoli all'utente o crearne di nuovi.

- Gli utenti AD e i gruppi ad aggiunti a RBAC SnapCenter devono disporre dell'autorizzazione DI LETTURA sul container utenti e sul container computer in Active Directory.
- Dopo aver assegnato un ruolo a un utente o a un gruppo che contiene le autorizzazioni appropriate, è necessario assegnare all'utente l'accesso alle risorse SnapCenter, ad esempio host e connessioni storage.

  In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

- È necessario assegnare un ruolo all'utente o al gruppo per sfruttare le autorizzazioni e le efficienze RBAC.
- È possibile assegnare risorse come host, gruppi di risorse, policy, connessione allo storage, plug-in, e all'utente durante la creazione dell'utente o del gruppo.
- Le risorse minime che è necessario assegnare a un utente per eseguire determinate operazioni sono le seguenti:

Operazione	Assegnazione delle risorse
Proteggere le risorse	host, policy
Backup	host, gruppo di risorse, policy
Ripristinare	host, gruppo di risorse
Clonare	host, gruppo di risorse, policy
Ciclo di vita dei cloni	host
Creare un gruppo di risorse	host

- Quando un nuovo nodo viene aggiunto a un cluster Windows o a una risorsa DAG (Exchange Server Database Availability Group) e se questo nuovo nodo viene assegnato a un utente, è necessario riassegnare la risorsa all'utente o al gruppo per includere il nuovo nodo all'utente o al gruppo.

  È necessario riassegnare l'utente o il gruppo RBAC al cluster o al DAG per includere il nuovo nodo all'utente o al gruppo RBAC. Ad esempio, si dispone di un cluster a due nodi ed è stato assegnato un utente o un gruppo RBAC al cluster. Quando si aggiunge un altro nodo al cluster, è necessario riassegnare l'utente o il gruppo RBAC al cluster per includere il nuovo nodo per l'utente o il gruppo RBAC.

- Se si intende replicare le istantanee, è necessario assegnare la connessione di archiviazione per il volume di origine e di destinazione all'utente che esegue l'operazione.

  Aggiungere le risorse prima di assegnare l'accesso agli utenti.

Se si utilizza il plug-in SnapCenter per le funzioni di VMware vSphere per proteggere macchine virtuali, VMDK o datastore, è necessario utilizzare l'interfaccia utente di VMware vSphere per aggiungere un utente vCenter a un plug-in SnapCenter per il ruolo di VMware vSphere. Per informazioni sui ruoli di VMware vSphere, vedere "Ruoli predefiniti in pacchetto con il plug-in SnapCenter per VMware vSphere".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **utenti e accesso** > .
3. Nella pagina Add Users/Groups from Active Directory or Workgroup (Aggiungi utenti/gruppi da Active Directory o Workgroup):

Per questo campo…	Eseguire questa operazione…
Tipo di accesso	Selezionare Domain (dominio) o Workgroup (gruppo di lavoro) Per il tipo di autenticazione dominio, specificare il nome di dominio dell'utente o del gruppo a cui si desidera aggiungere l'utente a un ruolo. Per impostazione predefinita, viene compilato con il nome di dominio connesso. È necessario registrare il dominio non attendibile nella pagina **Impostazioni** > **Impostazioni globali** > **Impostazioni dominio**.
Tipo	Selezionare User (utente) o Group (Gruppo) SnapCenter supporta solo il gruppo di sicurezza e non il gruppo di distribuzione.
Nome utente	a. Digitare il nome utente parziale, quindi fare clic su **Aggiungi**. Il nome utente fa distinzione tra maiuscole e minuscole. b. Selezionare il nome utente dall'elenco di ricerca. Quando si aggiungono utenti da un dominio diverso o da un dominio non attendibile, è necessario digitare completamente il nome utente, in quanto non esiste un elenco di ricerca per gli utenti di più domini. Ripetere questo passaggio per aggiungere altri utenti o gruppi al ruolo selezionato.
Ruoli	Selezionare il ruolo a cui si desidera aggiungere l'utente.

4. Fare clic su **Assegna**, quindi nella pagina Assegna risorse:
   a. Selezionare il tipo di risorsa dall'elenco a discesa **risorsa**.
   b. Nella tabella Asset, selezionare la risorsa.

      Le risorse vengono elencate solo se l'utente ha aggiunto le risorse a SnapCenter.

c. Ripetere questa procedura per tutte le risorse richieste.

d. Fare clic su **Save** (Salva).

5. Fare clic su **Invia**.

Dopo aver aggiunto utenti o gruppi e aver assegnato ruoli, aggiornare l'elenco delle risorse.

Configurare le impostazioni del registro di controllo

I registri di audit vengono generati per ogni attività del server SnapCenter. Per impostazione predefinita, i registri di controllo sono protetti nella posizione predefinita installata _C: File di programma/NetApp/SnapCenter WebApp/audit.

I registri di audit sono protetti mediante la generazione di digest con firma digitale per ogni evento di audit per proteggerlo da modifiche non autorizzate. I digest generati vengono mantenuti nel file checksum di audit separato e vengono sottoposti a controlli di integrità periodici per garantire l'integrità del contenuto.

Dovresti aver effettuato l'accesso come ruolo "SnapCenterAdmin".

A proposito di questa attività

- Gli avvisi vengono inviati nei seguenti scenari:
  - Il programma di controllo dell'integrità del registro di controllo o il server Syslog sono attivati o disattivati
  - Controllo dell'integrità del registro di controllo, registro di controllo o errore del registro del server Syslog
  - Spazio su disco insufficiente
- L'e-mail viene inviata solo quando il controllo dell'integrità non riesce.
- È necessario modificare insieme la directory del registro di controllo e i percorsi della directory del registro di controllo. Non è possibile modificarne solo uno.
- Quando vengono modificati i percorsi delle directory dei log di audit e dei log di checksum, non è possibile eseguire il controllo dell'integrità dei log di audit presenti nella posizione precedente.
- I percorsi delle directory dei log di audit e dei log di checksum devono trovarsi sul disco locale del server SnapCenter.

  I dischi condivisi o montati in rete non sono supportati.

- Se nelle impostazioni del server Syslog viene utilizzato il protocollo UDP, gli errori dovuti alla porta non sono attivi o non disponibili non possono essere acquisiti come errore o avviso in SnapCenter.
- È possibile utilizzare i comandi Set-SmAuditSettings e Get-SmAuditSettings per configurare i registri di controllo.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help command_name. In alternativa, è anche possibile fare riferimento a "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nella pagina **Impostazioni**, selezionare **Impostazioni** > **Impostazioni globali** > **Impostazioni registro di controllo**.

2. Nella sezione Registro di controllo, immettere i dettagli.
3. Inserire la directory **Registro audit** e la directory **Registro checksum audit**
   a. Inserire la dimensione massima del file
   b. Immettere il numero massimo di file di log
   c. Immettere la percentuale di utilizzo dello spazio su disco per inviare un avviso
4. (Facoltativo) attiva **Log UTC Time**.
5. (Facoltativo) attivare **Audit Log Integrity Check Schedule** e fare clic su **Start Integrity Check** per il controllo dell'integrità on-demand.

   È inoltre possibile eseguire il comando **Start-SmAuditIntegrityCheck** per avviare il controllo dell'integrità on-demand.

6. (Facoltativo) attivare i registri di controllo inoltrati al server syslog remoto e immettere i dettagli del server Syslog.

   È necessario importare il certificato dal server Syslog nel protocollo "Trusted Root" per TLS 1.2.

   a. Immettere Syslog Server host
   b. Immettere la porta del server Syslog
   c. Immettere il protocollo del server Syslog
   d. Inserire il formato RFC
7. Fare clic su **Save** (Salva).
8. È possibile visualizzare i controlli di integrità e lo spazio su disco facendo clic su **Monitor** > **Jobs**.

Configura connessioni MySQL protette con il server SnapCenter

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi se si desidera proteggere la comunicazione tra server SnapCenter e MySQL in configurazioni standalone o di bilanciamento del carico di rete (NLB).

Configurare connessioni MySQL protette per configurazioni standalone del server SnapCenter

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi, se si desidera proteggere la comunicazione tra il server SnapCenter e MySQL. È necessario configurare i certificati e i file delle chiavi nel server MySQL e nel server SnapCenter.

Vengono generati i seguenti certificati:

- Certificato CA
- Certificato pubblico del server e file di chiave privata
- Certificato pubblico del client e file di chiave privata

Fasi

1. Impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per ulteriori informazioni, vedere "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

   Procedura consigliata: utilizzare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

   Il percorso predefinito della cartella MySQL Data è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file delle chiavi copiati nella sezione [mysqld] del file my.ini nella cartella predefinita `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Arrestare l'applicazione Web del server SnapCenter nel server di informazioni Internet (IIS).
5. Riavviare il servizio MySQL.
6. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config.

   Nell'esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file SnapManager.Web.UI.dll.config.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Aggiornare il file SnapManager.Web.UI.dll.config con i percorsi forniti nella sezione [client] del file my.ini.

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Avviare l'applicazione Web del server SnapCenter in IIS.

Configurare connessioni MySQL protette per le configurazioni ha

È possibile generare certificati SSL (Secure Sockets Layer) e file di chiavi per i nodi ad alta disponibilità (ha) se si desidera proteggere la comunicazione tra server SnapCenter e server MySQL. È necessario configurare i certificati e i file delle chiavi nei server MySQL e nei nodi ha.

Vengono generati i seguenti certificati:

- Certificato CA

  Un certificato CA viene generato su uno dei nodi ha e questo certificato CA viene copiato nell'altro nodo ha.

- File di certificati pubblici e chiavi private del server per entrambi i nodi ha
- File di certificato pubblico del client e di chiave privata del client per entrambi i nodi ha

Fasi

1. Per il primo nodo ha, impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per ulteriori informazioni, vedere "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

   Procedura consigliata: utilizzare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

   Il percorso predefinito della cartella MySQL Data è C: ProgramData/NetApp/SnapCenter/MySQL Data/Data.

3. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è C: ProgramData/NetApp/SnapCenter/MySQL Data/my.ini.

   > Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file delle chiavi copiati nella sezione [mysqld] del file my.ini nella cartella predefinita C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

   ```
   ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
   ```

   ```
   ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
   ```

   ```
   ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
   ```

L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. Per il secondo nodo ha, copiare il certificato CA e generare il certificato pubblico del server, i file delle chiavi private del server, il certificato pubblico del client e i file delle chiavi private del client. attenersi alla seguente procedura:

   a. Copiare il certificato CA generato sul primo nodo ha nella cartella MySQL Data del secondo nodo NLB.

      Il percorso predefinito della cartella MySQL Data è C: ProgramData/NetApp/SnapCenter/MySQL Data/Data.

      > Non è necessario creare nuovamente un certificato CA. Creare solo il certificato pubblico del server, il certificato pubblico del client, il file della chiave privata del server e il file della chiave privata del client.

   b. Per il primo nodo ha, impostare i certificati SSL e i file delle chiavi per i server e i client MySQL su Windows utilizzando il comando openssl.

      "MySQL versione 5.7: Creazione di certificati e chiavi SSL con openssl"

      > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file delle chiavi deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file dei certificati e delle chiavi non funzionano per i server compilati utilizzando OpenSSL.

      Si consiglia di utilizzare l'FQDN del server come nome comune per il certificato del server.

   c. Copiare i certificati SSL e i file delle chiavi nella cartella MySQL Data.

   d. Aggiornare il certificato CA, il certificato pubblico del server, il certificato pubblico del client, la chiave privata del server e i percorsi delle chiavi private del client nel file di configurazione del server MySQL (my.ini).

      > Specificare il certificato CA, il certificato pubblico del server e i percorsi delle chiavi private del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

      Specificare il certificato CA, il certificato pubblico del client e i percorsi delle chiavi private del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

L’esempio seguente mostra i certificati e i file delle chiavi copiati nella sezione [mysqld] del file my.ini nella cartella predefinita C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L’esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. Arrestare l’applicazione Web del server SnapCenter in IIS su entrambi i nodi ha.
6. Riavviare il servizio MySQL su entrambi i nodi ha.
7. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config per entrambi i nodi ha.

   Nell’esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file SnapManager.Web.UI.dll.config.

   ```
   <add key="MySQLProtocol" value="SSL" />
   ```

8. Aggiornare il file SnapManager.Web.UI.dll.config con i percorsi specificati nella sezione [client] del file my.ini per entrambi i nodi ha.

   L’esempio seguente mostra i percorsi aggiornati nella sezione [client] dei file my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. Avviare l'applicazione Web del server SnapCenter in IIS su entrambi i nodi ha.
10. Utilizzare il cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell con l'opzione -Force su uno dei nodi ha per stabilire una replica MySQL sicura su entrambi i nodi ha.

    Anche se lo stato della replica è integro, l'opzione -Force consente di ricostruire il repository slave.