Configurare il server SnapCenter

SnapCenter software

NetApp
November 06, 2025

Sommario

Configurare il server SnapCenter

Aggiungere e predisporre il sistema di archiviazione

Aggiungere sistemi di archiviazione

È necessario configurare il sistema di archiviazione che consente a SnapCenter di accedere all'archiviazione ONTAP , ai sistemi ASA r2 o Amazon FSx for NetApp ONTAP per eseguire operazioni di protezione dei dati e provisioning.

È possibile aggiungere una SVM autonoma oppure un cluster composto da più SVM. Se si utilizza Amazon FSx for NetApp ONTAP, è possibile aggiungere un LIF di amministrazione FSx composto da più SVM utilizzando l'account fsxadmin oppure aggiungere un SVM FSx in SnapCenter.

Prima di iniziare

- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

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

Informazioni su questo compito

- Quando si configurano i sistemi di archiviazione, è anche possibile abilitare le funzionalità Event Management System (EMS) e AutoSupport . Lo strumento AutoSupport raccoglie dati sullo stato del sistema e li invia automaticamente al supporto tecnico NetApp , consentendogli di risolvere i problemi del sistema.

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

- Se si prevede di replicare gli snapshot su una destinazione SnapMirror o SnapVault , è necessario configurare le connessioni del sistema di archiviazione per l'SVM o il cluster di destinazione, nonché per l'SVM o il cluster di origine.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, fare clic su **Nuovo**.
3. Nella pagina Aggiungi sistema di archiviazione, fornire le seguenti informazioni:

Per questo campo…	Fai questo…
Sistema di archiviazione	Immettere il nome del sistema di archiviazione o l'indirizzo IP. I nomi dei sistemi di archiviazione, escluso il nome di dominio, devono contenere al massimo 15 caratteri e devono essere risolvibili. Per creare connessioni al sistema di archiviazione con nomi composti da più di 15 caratteri, è possibile utilizzare il cmdlet Add-SmStorageConnectionPowerShell. Per i sistemi di storage con configurazione MetroCluster (MCC), si consiglia di registrare sia i cluster locali che quelli peer per operazioni non disruptive. SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportato da SnapCenter deve avere un nome univoco. Dopo aver aggiunto la connessione di archiviazione a SnapCenter, non dovresti rinominare l'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	Immettere le credenziali dell'utente di archiviazione che dispone dei privilegi richiesti per accedere al sistema di archiviazione.

Per questo campo…	Fai questo…
Impostazioni del sistema di gestione degli eventi (EMS) e AutoSupport	Se si desidera inviare messaggi EMS al syslog del sistema di archiviazione o se si desidera che i messaggi AutoSupport vengano inviati al sistema di archiviazione 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 archiviazione**, viene selezionata anche la casella di controllo **Registra eventi del server SnapCenter su syslog** perché è necessaria la messaggistica EMS per abilitare le notifiche AutoSupport .

4. Fare clic su **Altre opzioni** se si desidera modificare i valori predefiniti assegnati a piattaforma, protocollo, porta e timeout.

   a. In Piattaforma, seleziona una delle opzioni dall'elenco a discesa.

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

   Se hai aggiunto SVM in SnapCenter , l'utente dovrà selezionare manualmente il tipo di piattaforma dal menu a discesa.

   a. In Protocollo, seleziona il protocollo configurato durante la configurazione di SVM o Cluster, in genere HTTPS.
   b. Immettere la porta accettata dal sistema di archiviazione.

      In genere funziona la porta predefinita 443.

   c. Inserire il tempo in secondi che deve trascorrere prima che i tentativi di comunicazione vengano interrotti.

      Il valore predefinito è 60 secondi.

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

Risultato

Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, eseguire una delle seguenti azioni:

- Selezionare * ONTAP SVM* se si desidera visualizzare tutti gli SVM aggiunti.

  Se hai aggiunto SVM FSx, questi vengono elencati qui.

- Selezionare *Cluster ONTAP * se si desidera visualizzare tutti i cluster aggiunti.

  Se hai aggiunto cluster FSx utilizzando fsxadmin, i cluster FSx sono elencati qui.

  Facendo clic sul nome del cluster, tutte le SVM che ne fanno parte vengono visualizzate nella sezione Macchine virtuali di archiviazione.

  Se si aggiunge un nuovo SVM al cluster ONTAP tramite l'interfaccia utente grafica ONTAP , fare clic su **Riscopri** per visualizzare il nuovo SVM aggiunto.

Dopo aver finito

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

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

L'amministratore della macchina virtuale di archiviazione (SVM) non ha accesso ad AutoSupport.

Connessioni di archiviazione e credenziali

Prima di eseguire operazioni di protezione dei dati, è necessario configurare le connessioni di archiviazione e aggiungere le credenziali che verranno utilizzate da SnapCenter Server e dai plug-in SnapCenter .

Connessioni di archiviazione

Le connessioni di archiviazione consentono al server SnapCenter e ai plug-in SnapCenter di accedere all'archiviazione ONTAP . L'impostazione di queste connessioni comporta anche la configurazione delle funzionalità AutoSupport ed Event Management System (EMS).

Credenziali

- Amministratore di dominio o qualsiasi membro del gruppo di amministratori

  Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:

  - *NetBIOS\NomeUtente*
  - *FQDN dominio\Nome utente*
  - *NomeUtente@upn*
- Amministratore locale (solo per gruppi di lavoro)

  Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host.

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

- 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 al nome utente almeno i privilegi di gruppo di risorse e di backup.

Fornire spazio di archiviazione su host Windows

Creare e gestire igroup

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

Crea un igroup

È possibile utilizzare SnapCenter per creare un igroup su un host Windows. L'igroup sarà disponibile nella procedura guidata Crea disco o Connetti disco quando si esegue il mapping dell'igroup a un LUN.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic su **Nuovo**.
4. Nella finestra di dialogo Crea igroup, definire l'igroup:

In questo campo…	Fai questo…
Sistema di archiviazione	Selezionare l'SVM per la LUN che si desidera mappare all'igroup.
Ospite	Selezionare l'host su cui si desidera creare l'igroup.
Nome del gruppo	Inserisci il nome dell'igroup.
Iniziatori	Selezionare l'iniziatore.
Tipo	Selezionare il tipo di iniziatore: iSCSI, FCP o misto (FCP e iSCSI).

5. Quando sei soddisfatto dei tuoi dati, clicca su **OK**.

   SnapCenter crea l'igroup sul sistema di archiviazione.

Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera rinominare.
4. Nell'elenco degli igroup per l'SVM, seleziona l'igroup che vuoi rinominare e fai clic su **Rinomina**.
5. Nella finestra di dialogo Rinomina igroup, immettere il nuovo nome per l'igroup e fare clic su **Rinomina**.

Modificare un igroup

È possibile utilizzare SnapCenter per aggiungere 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 modificarlo per aggiungere altri nodi a tale igroup.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera modificare.
4. Nell'elenco degli igroup, seleziona un igroup e fai clic su **Aggiungi iniziatore all'igroup**.
5. Seleziona un host.
6. Selezionare gli iniziatori e fare clic su **OK**.

Elimina un igroup

È possibile utilizzare SnapCenter per eliminare un igroup quando non ne hai più bisogno.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera eliminare.
4. Nell'elenco degli igroup per l'SVM, seleziona l'igroup che desideri eliminare e fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina igroup, fare clic su **OK**.

   SnapCenter elimina l'igroup.

Creare e gestire dischi

L'host Windows vede i LUN sul sistema di archiviazione come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare una LUN connessa tramite FC o tramite iSCSI.

- SnapCenter supporta solo dischi di base. I dischi dinamici non sono supportati.

- Per GPT è consentita solo una partizione dati e per MBR è consentita solo una partizione primaria con un volume formattato con NTFS o CSVFS e un percorso di montaggio.
- Stili di partizione supportati: GPT, MBR; in una VM 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 riusciranno.

Visualizza i dischi su un host

Puoi visualizzare i dischi su ogni host Windows che gestisci con SnapCenter.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.

   I dischi sono elencati.

Visualizza i dischi in cluster

È possibile visualizzare i dischi in cluster sul cluster gestito con SnapCenter. I dischi in cluster vengono visualizzati solo quando si seleziona il cluster dal menu a discesa Host.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
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 archiviazione come destinazione iSCSI.
- È necessario aver avviato il servizio iSCSI sul sistema di archiviazione. "Saperne di più"

Informazioni su questo compito

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 delle sessioni 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 iniziatore iSCSI, l'accesso alle destinazioni iSCSI ne risente. Dopo aver modificato il nome, potrebbe essere necessario riconfigurare i target a cui accede l'iniziatore in modo che possano

riconoscere il nuovo nome. Dopo aver modificato il nome di un iniziatore iSCSI, è necessario assicurarsi di riavviare l'host.

Se l'host dispone di più di un'interfaccia 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Sessione iSCSI**.
3. Dall'elenco a discesa **Macchina virtuale di archiviazione**, selezionare la macchina virtuale di archiviazione (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **Host**, seleziona l'host per la sessione.
5. Fare clic su **Stabilisci sessione**.

   Viene visualizzata la procedura guidata Crea sessione.

6. Nella procedura guidata Stabilisci sessione, identifica la destinazione:

In questo campo…	Entra…
Nome del nodo di destinazione	Il nome del nodo della destinazione iSCSI Se esiste già 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
Portale di destinazione	La porta TCP del portale di rete di destinazione
Indirizzo del portale dell'iniziatore	L'indirizzo IP del portale di rete dell'iniziatore

7. Quando sei soddisfatto dei tuoi dati, clicca su **Connetti**.

   SnapCenter stabilisce la sessione iSCSI.

8. Ripetere questa procedura per stabilire una sessione per ciascun target.

Creare LUN o dischi connessi tramite FC o tramite iSCSI

L'host Windows vede i LUN sul sistema di archiviazione come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare una LUN connessa tramite FC o tramite 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 la LUN sul sistema di archiviazione.

  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 suddiviso.

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

Informazioni su questo compito

- Non è possibile connettere una LUN a più di un host, a meno che la LUN non sia condivisa dagli host in un cluster di failover di Windows Server.
- Se un LUN è condiviso da 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.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.
4. Fare clic su **Nuovo**.

   Si apre la procedura guidata Crea disco.

5. Nella pagina Nome LUN, identificare la LUN:

In questo campo…	Fai questo…
Sistema di archiviazione	Selezionare l'SVM per la LUN.
Percorso LUN	Fare clic su **Sfoglia** per selezionare il percorso completo della cartella contenente il LUN.
Nome LUN	Immettere il nome del LUN.
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. La dimensione del cluster dipende dal sistema operativo e dalle applicazioni.
Etichetta LUN	Facoltativamente, immettere un testo descrittivo per il LUN.

6. Nella pagina Tipo di disco, seleziona il tipo di disco:

Selezionare…	Se…
Disco dedicato	L'accesso alla LUN è consentito solo a un host. Ignora il campo **Gruppo di risorse**.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. Immettere 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 in un cluster di failover di Windows Server che utilizza CSV. Immettere 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 cluster.

7. Nella pagina Proprietà unità, specificare le proprietà dell'unità:

Proprietà	Descrizione
Assegnazione automatica del punto di montaggio	SnapCenter assegna automaticamente un punto di montaggio del volume in base all'unità di sistema. Ad esempio, se l'unità di sistema è C:, l'assegnazione automatica crea un punto di montaggio del volume nell'unità C: (C:\scmnpt\). L'assegnazione automatica non è supportata per i dischi condivisi.
Assegna lettera di unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.
Utilizza il punto di montaggio del volume	Montare il disco sul percorso dell'unità specificato nel campo adiacente. La radice del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.
Non assegnare la lettera dell'unità o il punto di montaggio del volume	Selezionare questa opzione se si preferisce montare manualmente il disco in Windows.
dimensione LUN	Specificare la dimensione LUN; minimo 150 MB. Selezionare MB, GB o TB nell'elenco a discesa adiacente.

Proprietà	Descrizione
Utilizzare il thin provisioning per il volume che ospita questa LUN	Fornire una disposizione sottile della LUN. Il thin provisioning alloca solo lo spazio di archiviazione necessario in un dato momento, consentendo alla LUN di crescere in modo efficiente fino alla massima capacità disponibile. Assicurati che ci sia abbastanza spazio disponibile sul volume per contenere tutto lo spazio di archiviazione LUN che ritieni necessario.
Scegli il tipo di partizione	Selezionare la partizione GPT per una tabella delle partizioni GUID o la partizione MBR per un Master Boot Record. 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 Mappa LUN, selezionare l'iniziatore iSCSI o FC sull'host:

In questo campo…	Fai questo…
Ospite	Fare doppio clic sul nome del gruppo 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.
Scegli 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 I/O multipath (MPIO).

9. Nella pagina Tipo di gruppo, specificare se si desidera mappare un igroup esistente al LUN o crearne uno nuovo:

Selezionare…	Se…
Crea un nuovo igroup per gli iniziatori selezionati	Si desidera creare un nuovo igroup per gli iniziatori selezionati.

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

10. Nella pagina Riepilogo, rivedi le tue selezioni e poi fai clic su **Fine**.

    SnapCenter crea il LUN e lo collega all'unità o al percorso dell'unità specificato sull'host.

Ridimensionare un disco

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

Informazioni su questo compito

- Per le LUN con provisioning sottile, la dimensione della geometria LUN ONTAP è indicata come dimensione massima.
- Per le LUN con provisioning spesso, la dimensione espandibile (dimensione disponibile nel volume) viene visualizzata come dimensione massima.
- Le LUN con partizioni di tipo MBR hanno un limite di dimensione di 2 TB.
- Le LUN con partizioni di tipo GPT hanno un limite di dimensione del sistema di archiviazione di 16 TB.
- È consigliabile creare uno snapshot prima di ridimensionare una LUN.
- Se è necessario ripristinare una LUN da uno Snapshot creato prima del ridimensionamento della LUN, SnapCenter ridimensiona automaticamente la LUN in base alle dimensioni dello Snapshot.

  Dopo l'operazione di ripristino, i dati aggiunti al LUN dopo il ridimensionamento devono essere ripristinati da uno snapshot creato dopo il ridimensionamento.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa Host.

   I dischi sono elencati.

4. Seleziona il disco che vuoi ridimensionare e poi clicca su **Ridimensiona**.
5. Nella finestra di dialogo Ridimensiona disco, utilizzare lo strumento cursore per specificare la nuova dimensione del disco oppure immettere la nuova dimensione nel campo Dimensione.

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

6. Quando sei soddisfatto dei dati inseriti, clicca su **Riduci** o **Espandi**, a seconda dei casi.

   SnapCenter ridimensiona il disco.

Collegare un disco

È possibile utilizzare la procedura guidata Connetti disco per connettere un LUN esistente a un host o per riconnettere un LUN che è stato disconnesso.

Prima di iniziare

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.
4. Fare clic su **Connetti**.

   Si apre la procedura guidata Connetti disco.

5. Nella pagina Nome LUN, identifica la LUN a cui connettersi:

In questo campo…	Fai questo…
Sistema di archiviazione	Selezionare l'SVM per la LUN.
Percorso LUN	Fare clic su **Sfoglia** per selezionare il percorso completo del volume contenente il LUN.
Nome LUN	Immettere il nome del LUN.
Dimensione del cluster	Selezionare la dimensione di allocazione del blocco LUN per il cluster. La dimensione del cluster dipende dal sistema operativo e dalle applicazioni.
Etichetta LUN	Facoltativamente, immettere un testo descrittivo per il LUN.

6. Nella pagina Tipo di disco, seleziona il tipo di disco:

Selezionare…	Se…
Disco dedicato	L'accesso alla LUN è consentito solo a un host.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. È sufficiente collegare il disco a un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host in 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 cluster.

7. Nella pagina Proprietà unità, specificare le proprietà dell'unità:

Proprietà	Descrizione
Assegnazione automatica	Consenti a SnapCenter di assegnare automaticamente un punto di montaggio del volume in base all'unità di sistema. Ad esempio, se l'unità di sistema è C:, la proprietà di assegnazione automatica crea un punto di montaggio del volume nell'unità C: (C:\scmnpt\). La proprietà di assegnazione automatica non è supportata per i dischi condivisi.
Assegna lettera di unità	Montare il disco sull'unità selezionata nell'elenco a discesa adiacente.
Utilizza il punto di montaggio del volume	Montare il disco sul percorso dell'unità specificato nel campo adiacente. La radice del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco.
Non assegnare la lettera dell'unità o il punto di montaggio del volume	Selezionare questa opzione se si preferisce montare manualmente il disco in Windows.

8. Nella pagina Mappa LUN, selezionare l'iniziatore iSCSI o FC sull'host:

In questo campo…	Fai questo…
Ospite	Fare doppio clic sul nome del gruppo 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.
Scegli l'iniziatore host	Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host. Se si utilizza FC con MPIO, è possibile selezionare più iniziatori FC.

9. Nella pagina Tipo di gruppo, specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

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

10. Nella pagina Riepilogo, rivedi le tue selezioni e fai clic su **Fine**.

    SnapCenter collega la LUN all'unità o al percorso dell'unità specificato sull'host.

Disconnettere un disco

È possibile disconnettere una LUN da un host senza alterarne il contenuto, con un'eccezione: se si disconnette un clone prima che sia stato suddiviso, si perde il contenuto del clone.

Prima di iniziare

- Assicurarsi che la LUN non sia utilizzata da alcuna applicazione.
- Assicurarsi che la LUN non sia monitorata tramite software di monitoraggio.
- Se la LUN è condivisa, assicurarsi di rimuovere le dipendenze delle risorse del cluster dalla LUN e verificare che tutti i nodi del cluster siano accesi, funzionino correttamente e siano disponibili per SnapCenter.

Informazioni su questo compito

Se si disconnette un LUN in un volume FlexClone creato 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 eliminato.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
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.

Elimina un disco

È possibile eliminare un disco quando non ne hai più bisogno. Dopo aver eliminato un disco, non è più possibile ripristinarlo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.

   I dischi sono elencati.
4. Seleziona il disco che vuoi eliminare, quindi fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina disco, fare clic su **OK**.

   SnapCenter elimina il disco.

Creare e gestire condivisioni SMB

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

Procedura consigliata: si consiglia di utilizzare i cmdlet perché consentono di sfruttare i modelli forniti con SnapCenter per automatizzare la configurazione delle condivisioni.

I modelli racchiudono le best practice per la configurazione del volume e della condivisione. È possibile trovare i modelli nella cartella Modelli nella cartella di installazione del pacchetto plug-in SnapCenter per Windows.

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

Crea una condivisione SMB

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Condivisioni**.
3. Selezionare la SVM dall'elenco a discesa **Macchina virtuale di archiviazione**.
4. Fare clic su **Nuovo**.

   Si apre la finestra di dialogo Nuova condivisione.

5. Nella finestra di dialogo Nuova condivisione, definire la condivisione:

In questo campo…	Fai questo…
Descrizione	Inserisci un testo descrittivo per la condivisione.
Condividi il nome	Immettere 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 caratteri speciali `\ / [ ] : (vertical bar) < > + = ; , ?`
Condividi percorso	• 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 di file system esistenti.

6. Quando sei soddisfatto dei tuoi dati, clicca su **OK**.

   SnapCenter crea la condivisione SMB sulla SVM.

Elimina una condivisione SMB

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Condivisioni**.
3. Nella pagina Condivisioni, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un menu a discesa con un elenco delle macchine virtuali di archiviazione (SVM) disponibili, quindi selezionare la SVM per la condivisione che si desidera eliminare.
4. Dall'elenco delle condivisioni sull'SVM, seleziona la condivisione che desideri eliminare e fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina condivisione, fare clic su **OK**.

   SnapCenter elimina la condivisione SMB dall'SVM.

Recuperare spazio sul sistema di archiviazione

Sebbene NTFS tenga traccia dello spazio disponibile su una LUN quando i file vengono eliminati o modificati, non segnala le nuove informazioni al sistema di archiviazione. È possibile eseguire il cmdlet PowerShell per il recupero dello spazio sull'host Plug-in per Windows per garantire che i blocchi appena liberati vengano contrassegnati come disponibili nell'archiviazione.

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

Prima di iniziare

- Prima di eseguire un'operazione di ripristino, è necessario assicurarsi che il processo di recupero dello spazio sia stato completato.
- Se il LUN è condiviso dagli host in un cluster di failover di Windows Server, è necessario eseguire il recupero dello spazio sull'host proprietario del gruppo di cluster.
- Per prestazioni di archiviazione ottimali, è opportuno effettuare il recupero dello spazio il più spesso possibile.

  È necessario assicurarsi che l'intero file system NTFS sia stato scansionato.

Informazioni su questo compito

- Il recupero dello spazio è un'operazione che richiede molto tempo e impegna molta CPU, quindi in genere è meglio eseguirla quando l'utilizzo del sistema di archiviazione e dell'host Windows è basso.
- Il recupero dello spazio recupera quasi tutto lo spazio disponibile, ma non il 100%.
- Non eseguire la deframmentazione del disco contemporaneamente al recupero dello spazio.

  Ciò potrebbe rallentare il processo di bonifica.

Fare un passo

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

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

drive_path è il percorso dell'unità mappato al LUN.

Fornire l'archiviazione utilizzando i cmdlet di PowerShell

Se non si desidera utilizzare l'interfaccia utente grafica SnapCenter per eseguire attività di provisioning host e recupero spazio, è possibile utilizzare i cmdlet di PowerShell. È possibile utilizzare i cmdlet direttamente oppure 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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Se i cmdlet di SnapCenter PowerShell non funzionano correttamente a causa della rimozione di SnapDrive per Windows dal server, fare riferimento a "I cmdlet SnapCenter non funzionano quando SnapDrive per Windows viene disinstallato" .

Fornire storage in ambienti VMware

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

Piattaforme di sistemi operativi guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni del 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 RDM LUN con quattro controller LSI Logic SCSI per RDMS normale o 42 RDM LUN con tre controller LSI Logic SCSI su un plug-in box-to-box VMware VM MSCS per la configurazione Windows

  Supporta il controller VMware ParaVirtual SCSI. Sui dischi RDM possono essere supportati 256 dischi.

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

Limitazioni relative al server VMware ESXi

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

  Quando si installa il plug-in per Windows su macchine virtuali in cluster, è necessario utilizzare le credenziali vCenter.

- Tutti i nodi del cluster devono utilizzare lo stesso ID di destinazione (sulla scheda SCSI virtuale) per lo stesso disco del cluster.
- Quando si crea un LUN RDM al di fuori del plug-in per Windows, è necessario riavviare il servizio plug-in per consentirgli di riconoscere il disco appena creato.
- Non è possibile utilizzare contemporaneamente gli iniziatori iSCSI e FC su un sistema operativo guest VMware.

Privilegi minimi vCenter richiesti per le operazioni SnapCenter RDM

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

- Datastore: Rimuovi file
- Host: Configurazione > Configurazione partizione di archiviazione
- Macchina virtuale: configurazione

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

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

Gestire le LUN FC RDM in un cluster Microsoft

È possibile utilizzare il plug-in per Windows per gestire un cluster Microsoft mediante LUN FC RDM, ma è necessario prima creare il quorum RDM condiviso e l'archiviazione condivisa all'esterno del plug-in, quindi aggiungere i dischi alle macchine virtuali nel cluster.

A partire da ESXi 5.5, è possibile utilizzare anche 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 supporto per cluster Microsoft che utilizzano LUN FC RDM su due diverse macchine virtuali appartenenti a due diversi server ESX o ESXi, noti anche come cluster across box, quando si soddisfano requisiti di configurazione specifici.

- Le macchine virtuali (VM) devono eseguire la stessa versione di Windows Server.
- Le versioni del server ESX o ESXi devono essere le stesse per ogni host padre VMware.
- Ogni host padre deve disporre di almeno due schede 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 tramite iSCSI.

- La LUN RDM condivisa 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 l'archiviazione condivisa.

- Su ogni macchina virtuale del cluster deve essere configurato un controller SCSI in modalità di

compatibilità fisica:

Windows Server 2008 R2 richiede di configurare il controller SCSI LSI Logic SAS su ogni macchina virtuale. Le LUN condivise non possono utilizzare il controller LSI Logic SAS esistente se ne esiste solo uno del suo tipo ed è già collegato all'unità C:.

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

Quando si aggiunge un controller SCSI a una LUN condivisa su una macchina virtuale in modalità di compatibilità fisica, è necessario selezionare l'opzione **Raw Device Mappings** (RDM) e non l'opzione **Crea un 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 quelle ESX o ESXi.
- Il plug-in per Windows non può creare un singolo igroup con iniziatori provenienti da più host.

  L'igroup contenente gli iniziatori di tutti gli host ESXi deve essere creato sul controller di archiviazione prima di creare i LUN RDM che verranno utilizzati 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 di iniziatori con ALUA.

Limitazioni

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

Questa funzionalità 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 iniziatori misti in un ambiente cluster.

  Gli iniziatori devono essere FC o Microsoft iSCSI, ma non entrambi.

- Gli iniziatori iSCSI e gli HBA ESX non sono supportati sui dischi condivisi in un cluster Microsoft.
- Il plug-in per Windows non supporta la migrazione di 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 FC RDM per condividere lo storage tra i nodi in un cluster Microsoft, è necessario creare il disco quorum condiviso e il disco di storage condiviso, quindi aggiungerli a entrambe le macchine virtuali nel cluster.

Il disco condiviso non viene creato utilizzando il plug-in per Windows. Dovresti creare e poi aggiungere la LUN condivisa a ciascuna macchina virtuale nel cluster. Per informazioni, vedere "Cluster di macchine virtuali su host fisici" .

Aggiungi licenze basate sul controller SnapCenter Standard

Se si utilizzano controller di archiviazione FAS, AFF o ASA , è necessaria una licenza basata sul controller SnapCenter Standard.

La licenza basata sul controller presenta le seguenti caratteristiche:

- Diritto a SnapCenter Standard incluso con l'acquisto di Premium o Flash Bundle (non con il pacchetto base)
- Utilizzo illimitato dello spazio di archiviazione
- 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" .

Passaggio 1: verificare se la licenza di SnapManager Suite è 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.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, seleziona se visualizzare tutti gli SVM o i cluster aggiunti:
   - Per visualizzare tutti gli SVM aggiunti, selezionare * ONTAP SVM*.
   - Per visualizzare tutti i cluster aggiunti, selezionare *Cluster ONTAP *.

     Quando si seleziona il nome del cluster, tutte le SVM che ne fanno parte vengono visualizzate nella sezione Macchine virtuali di archiviazione.
3. Nell'elenco Connessioni di archiviazione, individuare la colonna Licenza controller.

   La colonna Licenza controller visualizza il seguente stato:

   - ✔ indica che una licenza SnapManager Suite è installata su un sistema di archiviazione primario FAS, AFF o ASA .

-  indica che una licenza SnapManager Suite non è installata su un sistema di archiviazione primario FAS, AFF o ASA .
- Non applicabile indica che una licenza SnapManager Suite non è applicabile perché il controller di storage si trova su Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select o piattaforme di storage secondarie.

Passaggio 2: identificare le licenze installate sul controller

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

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

Passi

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

Esempio di output

```
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, è installata la licenza SnapManagerSuite, pertanto non è richiesta alcuna ulteriore azione di

licenza SnapCenter .

Passaggio 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 .

Passi

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

Esempio di output

```
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.

Passaggio 4: recuperare il numero di serie della licenza basata sul 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 valide al sito di supporto NetApp .

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

- Dovresti avere il numero di serie del controller.

Passi

1. Accedi al "Sito di supporto NetApp" .
2. Vai a **Sistemi** > **Licenze software**.
3. Nell'area Criteri di selezione, assicurati che sia selezionato Numero di serie (situato sul retro dell'unità), inserisci il numero di serie del controller e seleziona **Vai!**.

   Viene visualizzato un elenco delle licenze per il controller specificato.

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

Passaggio 5: aggiungere la licenza basata sul controller

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

Prima di iniziare

- Dovresti essere un amministratore del cluster sul sistema FAS, AFF o ASA .
- Dovresti avere la licenza SnapCenter Standard o SnapManagerSuite.

Informazioni su questo compito

Se desideri installare SnapCenter in prova con storage FAS, AFF o ASA , puoi ottenere una licenza di valutazione Premium Bundle da installare sul tuo controller.

Se desideri installare SnapCenter in prova, contatta il tuo rappresentante commerciale per ottenere una licenza di valutazione Premium Bundle da installare sul tuo controller.

Passi

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 amministratore.

3. Verificare che la licenza SnapManagerSuite sia installata:

```
license show
```

Passaggio 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 SnapCenter Standard.

Passi

1. Sul server SnapCenter , aprire una finestra di 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 ai cmdlet del software SnapCenter" .
2. Aprire il prompt dei comandi ed eseguire mysql -u root -p per accedere a MySQL.

   MySQL ti chiederà la password. Inserisci 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 l’alta disponibilità

Configurare i server SnapCenter per l’alta disponibilità

Per supportare l’alta disponibilità (HA) in SnapCenter in esecuzione su Windows o Linux, è possibile installare il bilanciatore del carico F5. F5 consente a SnapCenter Server di supportare configurazioni attive-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 configurare F5 Load Balancer.

È anche possibile configurare il bilanciamento del carico di rete (NLB) per impostare l’alta disponibilità SnapCenter . Per un’elevata disponibilità, è necessario configurare NLB manualmente al di fuori dell’installazione SnapCenter .

Per l’ambiente cloud, è possibile configurare l’elevata disponibilità utilizzando Amazon Web Services (AWS) Elastic Load Balancing (ELB) e Azure Load Balancer.

Configurare l'alta disponibilità utilizzando F5

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

È necessario essere membri del gruppo Amministratori locali sui server SnapCenter (oltre ad avere il ruolo SnapCenterAdmin) per utilizzare i seguenti cmdlet per aggiungere e rimuovere cluster F5:

- Aggiungi-SmServerCluster
- Aggiungi-SmServer
- Rimuovi-SmServerCluster

  Per ulteriori informazioni, consulta "Guida di riferimento ai cmdlet del software SnapCenter" .

Informazioni aggiuntive

- Dopo aver installato e configurato SnapCenter per l'elevata disponibilità, modificare il collegamento sul desktop SnapCenter in modo che punti all'IP del cluster F5.
- Se si verifica un failover tra i server SnapCenter e se è già presente una sessione SnapCenter , è necessario chiudere il browser e accedere nuovamente a SnapCenter .
- Nella configurazione del bilanciatore 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 dell'host SnapCenter passa frequentemente dallo stato di inattività a quello di esecuzione degli host. Per risolvere questo problema, è necessario assicurarsi che entrambi gli host SnapCenter siano in grado di risolvere l'host in NLB o nell'host F5.
- I comandi SnapCenter per le impostazioni MFA devono essere eseguiti su tutti gli host. La configurazione della relying party 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 host verrà bloccato dopo l'abilitazione dell'MFA.
- Durante il failover, le impostazioni del registro di controllo non verranno riflesse sul secondo host. Pertanto, è necessario ripetere manualmente le impostazioni del registro di controllo sull'host passivo F5 quando diventa attivo.

Configurare l'alta disponibilità utilizzando il bilanciamento del carico di rete (NLB)

È possibile configurare il bilanciamento del carico di rete (NLB) per impostare l'alta disponibilità SnapCenter . Per un'elevata disponibilità, è necessario configurare NLB manualmente al di fuori dell'installazione SnapCenter .

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

Configurare l'elevata disponibilità utilizzando AWS Elastic Load Balancing (ELB)

È possibile configurare un ambiente SnapCenter ad alta disponibilità in Amazon Web Services (AWS) impostando due server SnapCenter in zone di disponibilità (AZ) 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.

Passi

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

2. Prepara il tuo host Windows
    a. Forzare la priorità di IPv4 rispetto a IPv6:
        - Posizione: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
        - Chiave: DisabledComponents
        - Tipo: REG_DWORD
        - Valore: 0x20
    b. Assicurarsi che i nomi di dominio completi possano essere risolti tramite DNS o tramite la configurazione dell'host locale negli indirizzi IPv4.
    c. Assicurarsi di non aver configurato un proxy di sistema.
    d. Assicurarsi che la password dell'amministratore sia la stessa su entrambi i server Windows quando si utilizza una configurazione senza Active Directory e i server non si trovano nello stesso dominio.
    e. Aggiungere 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. Ottieni i dettagli sull'alta disponibilità. `Get-SmServerConfig`
4. Creare la funzione Lamda per adattare la tabella di routing nel caso in cui l'endpoint IP privato virtuale non sia più disponibile, monitorato da AWS CloudWatch. Per informazioni, fare riferimento a "Creare una funzione Lambda" .
5. Crea 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 a "Crea canarini sintetici" .
6. Implementare il flusso di lavoro utilizzando una funzione step come alternativa al monitoraggio CloudWatch, garantendo tempi di failover più brevi. Il flusso di lavoro include una funzione di sonda Lambda per testare l'URL SnapCenter , una tabella DynamoDB per memorizzare i conteggi degli errori e la funzione Step stessa.
    a. Utilizzare una funzione lambda per sondare l'URL SnapCenter . Per informazioni, fare riferimento a "Crea funzione Lambda" .
    b. Crea una tabella DynamoDB per memorizzare il conteggio degli errori tra due iterazioni di Step Function. Per informazioni, fare riferimento a "Inizia con la tabella DynamoDB" .
    c. Creare la funzione Step. Per informazioni, fare riferimento a "Documentazione della funzione Step" .
    d. Prova un singolo passaggio.
    e. Testare la funzione completa.
    f. Crea un ruolo IAM e modifica le autorizzazioni per poter eseguire la funzione Lambda.

g. Crea una pianificazione per attivare la funzione Step. Per informazioni, fare riferimento a "Utilizzo di Amazon EventBridge Scheduler per avviare Step Functions" .

Configurare l'alta disponibilità utilizzando il bilanciatore del carico di Azure

È possibile configurare un ambiente SnapCenter ad alta disponibilità utilizzando il bilanciamento del carico di Azure.

Passi

1. Crea macchine virtuali in un set di scalabilità tramite il portale di Azure. Il set di scalabilità delle macchine virtuali di 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 base alla domanda o a una pianificazione definita. Per informazioni, fare riferimento a "Crea macchine virtuali in un set di scalabilità utilizzando il portale di Azure" .
2. Dopo aver configurato le macchine virtuali, accedi a ciascuna macchina virtuale nel set di VM e installa SnapCenter Server 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. Ottieni i dettagli sull'alta disponibilità. `Get-SmServerConfig`
6. Se necessario, ricostruire l'host secondario. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Failover sul secondo host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Passa da NLB a F5 per un'elevata disponibilità

È possibile modificare la configurazione SnapCenter HA da Network Load Balancing (NLB) per utilizzare F5 Load Balancer.

Passi

1. Configurare i server SnapCenter per un'elevata disponibilità utilizzando F5. "Saperne 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 SnapCenter Server 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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Elevata disponibilità per il repository MySQL SnapCenter

La replicazione MySQL è una funzionalità di MySQL Server che consente di replicare i dati da un server di database MySQL (master) a un altro server di database MySQL

(slave). SnapCenter supporta la replica MySQL per un'elevata disponibilità solo su due nodi abilitati per il bilanciamento del carico di rete (NLB).

SnapCenter esegue operazioni di lettura o scrittura sul repository master e indirizza la sua connessione al repository slave quando si verifica un errore sul repository master. Il repository slave diventa quindi il repository master. SnapCenter supporta anche la replica inversa, che è abilitata solo durante il failover.

Se si desidera utilizzare la funzionalità di alta disponibilità (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 a F5 del primo nodo e creare una copia del repository MySQL sul secondo nodo.

SnapCenter fornisce i cmdlet PowerShell *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* per gestire la replica di 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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

È necessario essere consapevoli delle limitazioni relative alla funzionalità MySQL HA:

- NLB e MySQL HA non sono supportati oltre i due nodi.
- Il passaggio da un'installazione autonoma SnapCenter a un'installazione NLB o viceversa e il passaggio da una configurazione autonoma di 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 avviene perché MySQL Server o SnapCenter Server non è attivo, tutti i processi in esecuzione potrebbero non riuscire. Dopo il failover sul secondo nodo, tutti i processi successivi vengono eseguiti correttamente.

Per informazioni sulla configurazione dell'alta disponibilità, vedere "Come configurare NLB e ARR con SnapCenter" .

Configurare il controllo degli accessi basato sui ruoli (RBAC)

Crea un ruolo

Oltre a utilizzare i ruoli SnapCenter esistenti, puoi creare ruoli personalizzati e personalizzare le autorizzazioni.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Ruoli**.

3. Clic + .
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 vedere gli oggetti degli altri membri** per consentire agli altri membri del ruolo di vedere risorse quali volumi e host dopo aver aggiornato l'elenco delle risorse.

   Se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri, è necessario deselezionare questa opzione.

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

6. Nella pagina Autorizzazioni, seleziona le autorizzazioni che desideri assegnare al ruolo oppure fai clic su **Seleziona tutto** per concedere tutte le autorizzazioni al ruolo.
7. Fare clic su **Invia**.

Aggiungere un ruolo NetApp ONTAP RBAC utilizzando i comandi di accesso di sicurezza

È possibile utilizzare i comandi di accesso di sicurezza per aggiungere un ruolo NetApp ONTAP RBAC quando i sistemi di storage eseguono ONTAP in cluster.

Prima di iniziare

- Identifica l'attività (o le attività) che desideri eseguire e i privilegi richiesti per eseguirle.
- Concedi privilegi ai comandi e/o alle directory dei comandi.

  Per ogni comando/directory di comandi sono previsti due livelli di accesso: accesso completo e sola lettura.

  È sempre necessario assegnare prima i privilegi di accesso completo.

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

Informazioni su questo compito

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 RBAC User Creator per NetApp ONTAP aggiunge automaticamente i privilegi nell'ordine corretto, in modo che i privilegi di accesso completo vengano visualizzati per primi. 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 in seguito si aggiorna SnapCenter o ONTAP, è necessario eseguire nuovamente lo strumento RBAC User Creator 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 nuovamente lo strumento, l'aggiornamento viene gestito automaticamente. Non è necessario ricreare i ruoli.

Per ulteriori informazioni sulla configurazione dei ruoli ONTAP RBAC, vedere "Guida all'autenticazione dell'amministratore ONTAP 9 e all'alimentazione RBAC" .

Passi

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

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

   - svm_name è il nome dell'SVM. Se si lascia vuoto questo campo, il valore predefinito è amministratore del cluster.
   - role_name è il nome specificato per il ruolo.
   - il comando è la capacità ONTAP .

   È necessario ripetere questo comando per ogni autorizzazione. Ricorda che i comandi di accesso completo devono essere elencati prima dei comandi di sola lettura.

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

2. Crea 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 stai creando.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà una.
   - svm_name è il nome dell'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 nel passaggio 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome dell'SVM.
   - <role_name> è il nome del ruolo creato nel passaggio 1.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà 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 ONTAP CLI. Questo ruolo è obbligatorio se si configurano le SVM in ONTAP per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

Passi

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

Comandi CLI ONTAP per la creazione di ruoli SVM e l'assegnazione di autorizzazioni

Esistono diversi comandi ONTAP CLI che dovresti 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.

Passi

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

Comandi CLI ONTAP per la creazione di ruoli SVM e l'assegnazione di autorizzazioni

Esistono diversi comandi ONTAP CLI che dovresti 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 cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi ONTAP CLI per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

Passi

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

Comandi CLI ONTAP per la creazione di ruoli del cluster e l'assegnazione di autorizzazioni

Per creare ruoli del cluster e assegnare autorizzazioni, è necessario eseguire diversi comandi ONTAP CLI.

- 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 cluster ONTAP per sistemi ASA r2

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

Passi

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

Comandi CLI ONTAP per la creazione di ruoli del cluster e l'assegnazione di autorizzazioni

Per creare ruoli del cluster e assegnare autorizzazioni, è necessario eseguire diversi comandi ONTAP CLI.

- `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`

Aggiungi un utente o un gruppo e assegna ruoli e risorse

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

Prima di iniziare

- Devi aver effettuato l'accesso con il 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.

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

- SnapCenter include diversi ruoli predefiniti.

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

- Gli utenti AD e i gruppi AD aggiunti a SnapCenter RBAC devono disporre dell'autorizzazione READ sul contenitore Users e sul contenitore 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 , come host e connessioni di archiviazione.

  Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

- A un certo punto dovresti assegnare un ruolo all'utente o al gruppo per sfruttare i permessi e l'efficienza di RBAC.
- Durante la creazione dell'utente o del gruppo, è possibile assegnare risorse quali host, gruppi di risorse, policy, connessione di archiviazione, plug-in e credenziali all'utente.
- Le risorse minime che dovresti assegnare a un utente per eseguire determinate operazioni sono le seguenti:

Operazione	Assegnazione dei beni
Proteggere le risorse	ospite, politica

Operazione	Assegnazione dei beni
Backup	host, gruppo di risorse, policy
Ripristinare	host, gruppo di risorse
Clone	host, gruppo di risorse, policy
Ciclo di vita del clone	ospite
Crea un gruppo di risorse	ospite

- 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 nell'utente o nel gruppo.

  È necessario riassegnare l'utente o il gruppo RBAC al cluster o al DAG per includere il nuovo nodo nell'utente o nel gruppo RBAC. Ad esempio, si dispone di un cluster a due nodi e al cluster è stato assegnato un utente o un gruppo RBAC. 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 prevede di replicare gli snapshot, è necessario assegnare la connessione di archiviazione per il volume di origine e di destinazione all'utente che esegue l'operazione.

  È necessario aggiungere risorse prima di assegnare l'accesso agli utenti.

Se si utilizzano le funzioni SnapCenter Plug-in for VMware vSphere per proteggere VM, VMDK o datastore, è necessario utilizzare l'interfaccia utente grafica di VMware vSphere per aggiungere un utente vCenter a un ruolo SnapCenter Plug-in for VMware vSphere . Per informazioni sui ruoli VMware vSphere, vedere "Ruoli predefiniti forniti con il SnapCenter Plug-in for VMware vSphere" .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Utenti e accesso** > * *.
3. Nella pagina Aggiungi utenti/gruppi da Active Directory o gruppo di lavoro:

Per questo campo…	Fai questo…
Tipo di accesso	Seleziona Dominio o gruppo di lavoro Per il tipo di autenticazione Dominio, è necessario specificare il nome di dominio dell'utente o del gruppo a cui si desidera aggiungere l'utente a un ruolo. Per impostazione predefinita, è precompilato con il nome di dominio dell'utente registrato. È necessario registrare il dominio non attendibile nella pagina **Impostazioni** > **Impostazioni globali** > **Impostazioni dominio**.
Tipo	Seleziona Utente o 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 è sensibile alle maiuscole e alle minuscole. b. Selezionare il nome utente dall'elenco di ricerca. Quando aggiungi utenti da un dominio diverso o da un dominio non attendibile, dovresti digitare il nome utente per intero perché non esiste un elenco di ricerca per gli utenti di domini diversi. Ripetere questo passaggio per aggiungere altri utenti o gruppi al ruolo selezionato.
Ruoli	Seleziona il ruolo a cui vuoi 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, seleziona l'asset.

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

c. Ripetere questa procedura per tutte le risorse richieste.

d. Fare clic su **Salva**.

5. Fare clic su **Invia**.

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

Configurare le impostazioni del registro di controllo

I registri di controllo vengono generati per ogni singola attività del server SnapCenter . Per impostazione predefinita, i registri di controllo sono protetti nel percorso di installazione predefinito *C:\Programmi\ NetApp\ SnapCenter WebApp\audit*.

I registri di controllo sono protetti mediante la generazione di un digest firmato digitalmente per ogni singolo evento di controllo, per proteggerlo da modifiche non autorizzate. I digest generati vengono conservati in un file di checksum di controllo separato e sottoposti a controlli di integrità periodici per garantire l'integrità del contenuto.

Dovresti aver effettuato l'accesso con il ruolo "SnapCenterAdmin".

Informazioni su questo compito

- Gli avvisi vengono inviati nei seguenti scenari:
  - La pianificazione del controllo dell'integrità del registro di controllo o il server Syslog è abilitato o disabilitato
  - Controllo dell'integrità del registro di controllo, registro di controllo o errore del registro del server Syslog
  - Poco spazio su disco
- L'e-mail viene inviata solo quando il controllo di integrità fallisce.
- È necessario modificare contemporaneamente i percorsi della directory del registro di controllo e della directory del registro di checksum di controllo. Non è possibile modificarne solo uno.
- Quando vengono modificati i percorsi della directory del registro di controllo e della directory del registro di checksum di controllo, il controllo di integrità non può essere eseguito sui registri di controllo presenti nella posizione precedente.
- I percorsi della directory del registro di controllo e della directory del registro di checksum di controllo devono trovarsi sull'unità locale di SnapCenter Server.

  Le unità condivise o montate in rete non sono supportate.

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

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

Passi

1. Nella pagina **Impostazioni**, vai a **Impostazioni** > **Impostazioni globali** > **Impostazioni registro di controllo**.
2. Nella sezione Registro di controllo, immettere i dettagli.
3. Immettere la **directory del registro di controllo** e la **directory del registro di checksum di controllo**
   a. Inserisci la dimensione massima del file
   b. Inserisci il numero massimo di file di registro
   c. Inserisci la percentuale di utilizzo dello spazio su disco per inviare un avviso
4. (Facoltativo) Abilita **Registra ora UTC**.
5. (Facoltativo) Abilita **Pianificazione controllo integrità registro di controllo** e fai clic su **Avvia controllo integrità** per il controllo di integrità su richiesta.

   È anche possibile eseguire il comando **Start-SmAuditIntegrityCheck** per avviare il controllo di integrità su richiesta.

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

   È necessario importare il certificato dal server Syslog nella "radice attendibile" per il protocollo TLS 1.2.

   a. Inserisci l'host del server Syslog
   b. Inserisci la porta del server Syslog
   c. Inserisci il protocollo del server Syslog
   d. Inserisci il formato RFC
7. Fare clic su **Salva**.
8. È possibile visualizzare i controlli di integrità e di spazio su disco facendo clic su **Monitor** > **Jobs**.

Configurare connessioni MySQL protette con SnapCenter Server

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave se si desidera proteggere la comunicazione tra SnapCenter Server e MySQL Server in configurazioni autonome o configurazioni NLB (Network Load Balancing).

Configurare connessioni MySQL protette per configurazioni di SnapCenter Server autonome

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave se si desidera proteggere la comunicazione tra SnapCenter Server e MySQL Server. È necessario configurare i certificati e i file chiave in MySQL Server e SnapCenter Server.

Vengono generati i seguenti certificati:

- Certificato CA
- File del certificato pubblico e della chiave privata del server
- Certificato pubblico del client e file della chiave privata

Passi

1. Imposta i certificati SSL e i file chiave per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per informazioni, vedere "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

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

   Migliore pratica: dovresti usare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

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

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

3. Aggiornare i percorsi del certificato CA, del certificato pubblico del server, del certificato pubblico del client, della chiave privata del server e della chiave privata 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`.

   > È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file chiave 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 SnapCenter Server in Internet Information Server (IIS).
5. Riavviare il servizio MySQL.
6. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config.

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato 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 SnapCenter Server in IIS.

Configurare connessioni MySQL protette per configurazioni HA

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave per entrambi i nodi High Availability (HA) se si desidera proteggere la comunicazione tra SnapCenter Server e i server MySQL. È necessario configurare i certificati e i file chiave 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 sull'altro nodo HA.

- File del certificato pubblico del server e della chiave privata del server per entrambi i nodi HA
- File del certificato pubblico del client e della chiave privata del client per entrambi i nodi HA

Passi

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

   Per informazioni, vedere "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

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

   Migliore pratica: dovresti usare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

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

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

3. Aggiornare i percorsi del certificato CA, del certificato pubblico del server, del certificato pubblico del client, della chiave privata del server e della chiave privata 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.

   > È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file chiave 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 della chiave privata del server, il certificato pubblico del client e i file della chiave privata del client. Eseguire i seguenti passaggi:

   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. È necessario 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 chiave per i server e i client MySQL su Windows utilizzando il comando openssl.

      "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

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

      Si consiglia di utilizzare il nome di dominio completo del server come nome comune per il certificato del server.

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

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

È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

L'esempio seguente mostra i certificati e i file chiave 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 SnapCenter Server in Internet Information Server (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.

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato 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 SnapCenter Server in IIS su entrambi i nodi HA.
10. Utilizzare il cmdlet PowerShell Set-SmRepositoryConfig -RebuildSlave -Force con l'opzione -Force su uno dei nodi HA per stabilire una replica MySQL protetta su entrambi i nodi HA.

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

Informazioni sul copyright

Informazioni sul marchio commerciale