Installazione del server SnapCenter

SnapCenter Software 5.0

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-50/install/install_workflow.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommario

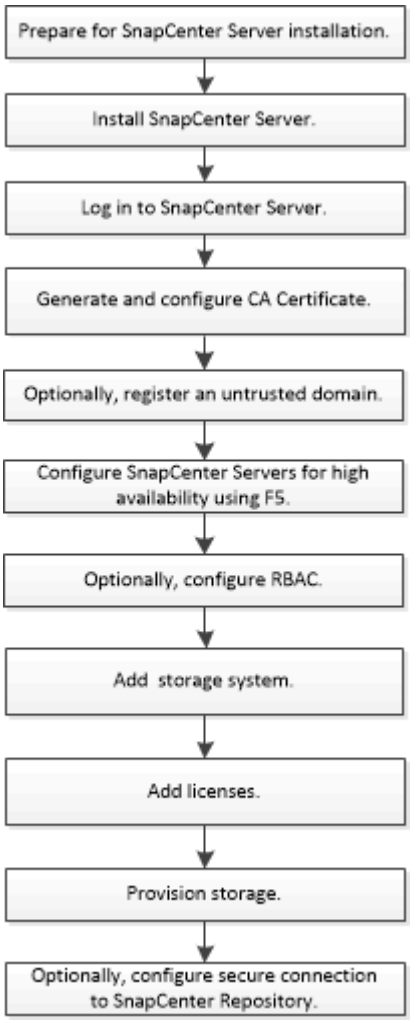
Installazione del server SnapCenter . . . 1
- Workflow di installazione . . . 1
- Preparazione per l'installazione del server SnapCenter . . . 1
  - Requisiti di dominio e gruppo di lavoro . . . 1
  - Requisiti di spazio e dimensionamento . . . 2
  - Requisiti degli host SAN . . . 3
  - Sistemi e applicazioni storage supportati . . . 3
  - Browser supportati . . . 4
  - Requisiti di connessione e porta . . . 4
  - Licenze SnapCenter . . . 7
  - Metodi di autenticazione per le credenziali . . . 10
  - Connessioni e credenziali dello storage . . . 11
  - Autenticazione a più fattori (MFA) . . . 12
- Installare il server SnapCenter . . . 22
- Accedere a SnapCenter utilizzando l'autorizzazione RBAC . . . 23
  - Accedere a SnapCenter utilizzando l'autenticazione multifattore (MFA) . . . 25
  - Modificare il timeout della sessione GUI predefinita di SnapCenter . . . 25
  - Proteggere il server Web SnapCenter disattivando SSL 3.0 . . . 25
- Configurare il certificato CA . . . 26
  - Generare il file CSR del certificato CA . . . 26
  - Importare i certificati CA . . . 26
  - Ottenere il thumbprint del certificato CA . . . 27
  - Configurare il certificato CA con i servizi plug-in dell'host Windows . . . 28
  - Configurare il certificato CA con il sito SnapCenter . . . 28
  - Abilitare i certificati CA per SnapCenter . . . 29
- Configurare e abilitare la comunicazione SSL bidirezionale . . . 30
  - Configurare la comunicazione SSL bidirezionale . . . 30
  - Abilitare la comunicazione SSL bidirezionale . . . 32
- Configurare l'autenticazione basata su certificato . . . 34
  - Esportare i certificati dell'autorità di certificazione (CA) dal server SnapCenter . . . 34
  - Importa certificato CA (Certificate Authority) negli host plug-in di Windows . . . 34
  - Importare il certificato CA nei plug-in host UNIX e configurare i certificati root o intermedi nell'archivio di fiducia SPL . . . 35
  - Abilitare l'autenticazione basata su certificato . . . 37
- Configurare Active Directory, LDAP e LDAPS . . . 37
  - Registrare domini Active Directory non attendibili . . . 37
  - Configurare il certificato del client CA per LDAPS . . . 39
- Configurare la disponibilità elevata . . . 39
  - Configurare i server SnapCenter per l'alta disponibilità utilizzando F5 . . . 39
  - Configurare Microsoft Network Load Balancer manualmente . . . 41
  - Passa da NLB a F5 per ottenere alta disponibilità . . . 41
  - Alta disponibilità per il repository MySQL di SnapCenter . . . 41
  - Esportare i certificati SnapCenter . . . 42

Configurare RBAC (role-based access control) . . . 43
Aggiungere un utente o un gruppo e assegnare ruolo e risorse . . . 43
Creare un ruolo . . . 46
Aggiungere un ruolo RBAC ONTAP utilizzando i comandi di accesso di sicurezza . . . 46
Creare ruoli SVM con privilegi minimi . . . 48
Creare ruoli cluster ONTAP con privilegi minimi . . . 53
Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory . . . 58
Configurare le impostazioni del registro di controllo . . . 59
Aggiungere sistemi storage . . . 60
Aggiunta di licenze SnapCenter basate su controller standard . . . 64
Fase 1: Verificare che la licenza della suite SnapManager sia installata . . . 64
Fase 2: Identificare le licenze installate sul controller . . . 65
Fase 3: Recuperare il numero di serie del controller . . . 66
Fase 4: Recuperare il numero di serie della licenza basata su controller . . . 67
Fase 5: Aggiungere una licenza basata su controller . . . 68
Fase 6: Rimuovere la licenza di prova . . . 69
Aggiunta di licenze SnapCenter basate sulla capacità standard . . . 69
Eseguire il provisioning del sistema storage . . . 73
Eseguire il provisioning dello storage su host Windows . . . 73
Eseguire il provisioning dello storage in ambienti VMware . . . 88
Configura connessioni MySQL protette con il server SnapCenter . . . 91
Configurare connessioni MySQL protette per configurazioni standalone del server SnapCenter . . . 91
Configurare connessioni MySQL protette per le configurazioni ha . . . 93
Funzionalità abilitate sull'host Windows durante l'installazione . . . 96

Installazione del server SnapCenter

Workflow di installazione

Il flusso di lavoro mostra le diverse attività necessarie per installare e configurare il server SnapCenter.



Preparazione per l'installazione del server SnapCenter

Requisiti di dominio e gruppo di lavoro

Il server SnapCenter può essere installato su sistemi che si trovano in un dominio o in un gruppo di lavoro. L'utente utilizzato per l'installazione deve disporre dei privilegi di amministratore sul computer in caso di gruppo di lavoro e dominio.

Per installare il server SnapCenter e i plug-in SnapCenter su host Windows, è necessario utilizzare uno dei seguenti elementi:

- **Dominio Active Directory**

  È necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente di dominio deve

essere membro del gruppo Administrator locale sull'host Windows.

- **Gruppi di lavoro**

  È necessario utilizzare un account locale con diritti di amministratore locale.

Sebbene siano supportati trust di dominio, foreste di domini multipli e trust tra domini, i domini tra foreste non sono supportati. La documentazione Microsoft sui domini e trust di Active Directory contiene ulteriori informazioni.

> Dopo aver installato il server SnapCenter, non modificare il dominio in cui si trova l'host SnapCenter. Se si rimuove l'host del server SnapCenter dal dominio in cui si trovava quando è stato installato il server SnapCenter e si tenta di disinstallare il server SnapCenter, l'operazione di disinstallazione non riesce.

Requisiti di spazio e dimensionamento

Prima di installare il server SnapCenter, è necessario conoscere i requisiti di spazio e dimensionamento. È inoltre necessario applicare gli aggiornamenti di sicurezza e di sistema disponibili.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
Numero minimo di CPU	4 core
RAM minima	8 GB Il pool di buffer di MySQL Server utilizza il 20% della RAM totale.
Spazio minimo su disco rigido per il software e i registri del server SnapCenter	4 GB Se il repository SnapCenter si trova nello stesso disco in cui è installato il server SnapCenter, si consiglia di utilizzare 10 GB.

Elemento	Requisiti
Spazio minimo su disco rigido per il repository SnapCenter	6 GB NOTA: Se il server SnapCenter si trova nello stesso disco in cui è installato il repository SnapCenter, si consiglia di utilizzare 10 GB.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet".

Requisiti degli host SAN

Se l'host SnapCenter fa parte di un ambiente FC/iSCSI, potrebbe essere necessario installare software aggiuntivo sul sistema per consentire l'accesso allo storage ONTAP.

SnapCenter non include le utility host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN, potrebbe essere necessario installare e configurare il seguente software:

- Utility host

  Le utility host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. Per informazioni, vedere "Documentazione delle utility host".

- Microsoft DSM per Windows MPIO

  Questo software funziona con i driver MPIO di Windows per gestire percorsi multipli tra i computer host NetApp e Windows.

  Per le configurazioni ad alta disponibilità è necessario un DSM.

  Se si utilizza ONTAP DSM, è necessario eseguire la migrazione a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM".

Sistemi e applicazioni storage supportati

È necessario conoscere il sistema di storage, le applicazioni e i database supportati.

- SnapCenter supporta ONTAP 9.8 e versioni successive per proteggere i dati.
- SnapCenter supporta Amazon FSX per NetApp ONTAP per proteggere i dati dalla versione della patch P1

del software SnapCenter 4.5.

Se si utilizza Amazon FSX per NetApp ONTAP, assicurarsi che i plug-in host del server SnapCenter siano aggiornati alla versione 4.5 P1 o successiva per eseguire le operazioni di protezione dei dati.

Per informazioni su Amazon FSX per NetApp ONTAP, vedere "Documentazione di Amazon FSX per NetApp ONTAP".

- SnapCenter supporta la protezione di diverse applicazioni e database.

  Per informazioni dettagliate sulle applicazioni e i database supportati, vedere "Tool di matrice di interoperabilità NetApp".

- SnapCenter 4,9 P1 e versioni successive supporta la protezione dei carichi di lavoro Oracle e Microsoft SQL in ambienti VMware Cloud su Amazon Web Services (AWS) Software-Defined Data Center (SDDC).

  Per ulteriori informazioni, vedere "Proteggi i carichi di lavoro Oracle e MS SQL utilizzando NetApp SnapCenter in VMware Cloud su ambienti SDDC AWS".

Browser supportati

Il software SnapCenter può essere utilizzato su più browser.

- Cromo

  Se si utilizza la versione 66, potrebbe non essere possibile avviare l'interfaccia grafica di SnapCenter.

- Microsoft Edge 110.0.1587.17 e versioni successive

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Requisiti di connessione e porta

Prima di installare il server SnapCenter e i plug-in dell'applicazione o del database, assicurarsi che i requisiti di connessione e porte siano soddisfatti.

- Le applicazioni non possono condividere una porta.

  Ciascuna porta deve essere dedicata all'applicazione appropriata.

- Per le porte personalizzabili, è possibile selezionare una porta personalizzata durante l'installazione se non si desidera utilizzare la porta predefinita.

  È possibile modificare una porta del plug-in dopo l'installazione utilizzando la procedura guidata Modify host (Modifica host).

- Per le porte fisse, accettare il numero di porta predefinito.
- Firewall
  - Firewall, proxy o altri dispositivi di rete non devono interferire con le connessioni.
  - Se si specifica una porta personalizzata quando si installa SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per tale porta per il caricatore plug-in SnapCenter.

La tabella seguente elenca le diverse porte e i relativi valori predefiniti.

Tipo di porta	Porta predefinita
Porta web SnapCenter	8146 (HTTPS), bidirezionale, personalizzabile, come nell'URL *https://server:8146* Utilizzato per la comunicazione tra il client SnapCenter (l'utente SnapCenter) e il server SnapCenter. Utilizzato anche per la comunicazione dagli host plug-in al server SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta di comunicazione SMCore SnapCenter	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra il server SnapCenter e gli host in cui sono installati i plug-in SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta MySQL	3306 (HTTPS), bidirezionale La porta viene utilizzata per la comunicazione tra SnapCenter e il database del repository MySQL. È possibile creare connessioni protette dal server SnapCenter al server MySQL. "Scopri di più" Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Host plug-in Windows	135, 445 (TCP) Oltre alle porte 135 e 445, dovrebbe essere aperto anche l'intervallo di porte dinamiche specificato da Microsoft. Le operazioni di installazione remota utilizzano il servizio WMI (Windows Management Instrumentation), che ricerca dinamicamente questo intervallo di porte. Per informazioni sull'intervallo di porte dinamiche supportato, consultare la sezione "Panoramica del servizio e requisiti della porta di rete per Windows" Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host su cui viene installato il plug-in. Per inviare i binari dei pacchetti plug-in agli host plug-in di Windows, le porte devono essere aperte solo sull'host plug-in e possono essere chiuse dopo l'installazione.

Tipo di porta	Porta predefinita
Host plug-in Linux o AIX	22 (SSH) Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host in cui viene installato il plug-in. Le porte vengono utilizzate da SnapCenter per copiare i binari dei pacchetti plug-in su host plug-in Linux o AIX e devono essere aperte o escluse dal firewall o da iptables.
Pacchetto plug-in SnapCenter per Windows, pacchetto plug-in SnapCenter per Linux o pacchetto plug-in SnapCenter per AIX	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Il percorso di comunicazione deve essere aperto anche tra la LIF di gestione SVM e il server SnapCenter. Per personalizzare la porta, vedere "Aggiungere host e installare il plug-in SnapCenter per Microsoft Windows" o. "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in SnapCenter per database Oracle	27216, personalizzabile La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle. Per personalizzare la porta, vedere "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in personalizzati per SnapCenter	9090 (HTTPS), fisso Si tratta di una porta interna che viene utilizzata solo sull'host plug-in personalizzato; non è richiesta alcuna eccezione firewall. La comunicazione tra il server SnapCenter e i plug-in personalizzati viene instradata attraverso la porta 8145.

Tipo di porta	Porta predefinita
Porta di comunicazione SVM o cluster ONTAP	443 (HTTPS), bidirezionale (HTTP), bidirezionale La porta viene utilizzata da SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue il server SnapCenter e SVM. La porta viene attualmente utilizzata anche dagli host plug-in SAL on SnapCenter per Windows per la comunicazione tra l'host plug-in SnapCenter e SVM.
Plug-in SnapCenter per database SAP HANA vCode controllo ortografico	3instance_number13 o 3instance_number15, HTTP o HTTPS, bidirezionale e personalizzabile Per un singolo tenant MDC (Multitenant Database Container), il numero di porta termina con 13; per i non MDC, il numero di porta termina con 15. Ad esempio, 32013 è il numero della porta, ad esempio 20 e 31015 è il numero della porta, ad esempio 10. Per personalizzare la porta, vedere "Aggiungere host e installare pacchetti plug-in su host remoti."
Porta di comunicazione del controller di dominio	Consultare la documentazione Microsoft per identificare le porte che devono essere aperte nel firewall di un controller di dominio affinché l'autenticazione funzioni correttamente. È necessario aprire le porte richieste da Microsoft sul controller di dominio in modo che il server SnapCenter, gli host plug-in o altri client Windows possano autenticare gli utenti.

Per modificare i dettagli della porta, vedere "Modificare gli host dei plug-in".

Licenze SnapCenter

SnapCenter richiede diverse licenze per consentire la protezione dei dati di applicazioni, database, file system e macchine virtuali. Il tipo di licenze SnapCenter installate dipende dall'ambiente di storage e dalle funzionalità che si desidera utilizzare.

Licenza	Dove richiesto
Basato su controller standard SnapCenter	Richiesto per FAS, AFF, All SAN Array (ASA) La licenza standard di SnapCenter è una licenza basata su controller ed è inclusa nel pacchetto premium. Se si dispone della licenza della suite SnapManager, si ottiene anche il diritto di licenza standard SnapCenter. Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA, è possibile ottenere una licenza di valutazione Premium Bundle contattando il rappresentante commerciale. SnapCenter è anche offerto come parte del bundle per la protezione dei dati. Se hai acquistato A400 o versioni successive, devi acquistare il bundle per la protezione dei dati.
SnapCenter basato sulla capacità standard	Richiesto con ONTAP Select e Cloud Volumes ONTAP Se sei un cliente Cloud Volumes ONTAP o ONTAP Select, devi procurarti una licenza per TB basata sulla capacità in base ai dati gestiti da SnapCenter. Per impostazione predefinita, SnapCenter fornisce una licenza di prova integrata per SnapCenter standard da 100 TB, valida 90 giorni. Per ulteriori informazioni, contattare il rappresentante commerciale.
SnapMirror o SnapVault	ONTAP Se la replica è attivata in SnapCenter, è necessario disporre di una licenza SnapMirror o SnapVault.
SnapRestore	Necessario per ripristinare e verificare i backup. Sui sistemi storage primari • Necessario sui sistemi di destinazione SnapVault per eseguire la verifica remota e il ripristino da un backup. • Necessario sui sistemi di destinazione SnapMirror per eseguire la verifica in remoto.

Licenza	Dove richiesto
FlexClone	Necessario per clonare i database e le operazioni di verifica. Sui sistemi di storage primario e secondario • Necessario sui sistemi di destinazione SnapVault per creare cloni dal backup del vault secondario. • Necessario sui sistemi di destinazione SnapMirror per creare cloni dal backup SnapMirror secondario.
Protocolli	• Licenza iSCSI o FC per LUN • Licenza CIFS per le condivisioni SMB • Licenza NFS per VMDK di tipo NFS • Licenza iSCSI o FC per VMFS tipo VMDK Necessario sui sistemi di destinazione SnapMirror per la distribuzione dei dati se un volume di origine non è disponibile.
Licenze standard SnapCenter (opzionali)	Destinazioni secondarie Si consiglia, ma non è necessario, di aggiungere le licenze standard di SnapCenter alle destinazioni secondarie. Se le licenze standard di SnapCenter non sono abilitate sulle destinazioni secondarie, non è possibile utilizzare SnapCenter per eseguire il backup delle risorse sulla destinazione secondaria dopo aver eseguito un'operazione di failover. Tuttavia, è necessaria una licenza FlexClone sulle destinazioni secondarie per eseguire operazioni di cloning e verifica.

Le licenze servizi file NAS SnapCenter e SnapCenter sono obsolete e non sono più disponibili.

Installare una o più licenze SnapCenter. Per informazioni su come aggiungere le licenze, vedere "Aggiunta di licenze SnapCenter basate su controller standard" o "Aggiunta di licenze SnapCenter basate sulla capacità standard".

Licenze SMBR (Single Mailbox Recovery)

Se si utilizza il plug-in SnapCenter per Exchange per gestire i database e il ripristino di una singola casella postale (SMBR), è necessaria una licenza aggiuntiva per SMBR che deve essere acquistata separatamente in base alla casella postale dell'utente.

Il ripristino di una singola casella postale di NetApp® è giunto alla fine della disponibilità (EOA) il 12 maggio 2023. Per ulteriori informazioni, fare riferimento a "CPC-00507". NetApp continuerà a supportare i clienti che hanno acquistato capacità, manutenzione e supporto della casella postale attraverso i codici marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.

Il servizio di ripristino di una singola casella postale di NetApp è un prodotto partner fornito da Ontrack. Ontrack PowerControl offre funzionalità simili a quelle del ripristino di una singola casella postale di NetApp. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di assistenza e manutenzione Ontrack PowerControls da Ontrack (fino al licensingteam@ontrack.com) per il ripristino granulare della mailbox dopo la data EOA del 12 maggio 2023.

Metodi di autenticazione per le credenziali

Le credenziali utilizzano metodi di autenticazione diversi a seconda dell'applicazione o dell'ambiente. Le credenziali autenticano gli utenti in modo che possano eseguire operazioni SnapCenter. È necessario creare un set di credenziali per l'installazione dei plug-in e un altro set per le operazioni di protezione dei dati.

Autenticazione di Windows

Il metodo di autenticazione di Windows esegue l'autenticazione con Active Directory. Per l'autenticazione di Windows, Active Directory viene configurato al di fuori di SnapCenter. SnapCenter esegue l'autenticazione senza alcuna configurazione aggiuntiva. È necessaria una credenziale Windows per eseguire attività come l'aggiunta di host, l'installazione di pacchetti plug-in e la pianificazione dei processi.

Autenticazione di dominio non attendibile

SnapCenter consente la creazione di credenziali Windows utilizzando utenti e gruppi appartenenti a domini non attendibili. Affinché l'autenticazione abbia esito positivo, è necessario registrare i domini non attendibili con SnapCenter.

Autenticazione del gruppo di lavoro locale

SnapCenter consente la creazione di credenziali Windows con utenti e gruppi di lavoro locali. L'autenticazione di Windows per gli utenti e i gruppi di lavoro locali non avviene al momento della creazione delle credenziali di Windows, ma viene posticipata fino a quando non vengono eseguite la registrazione dell'host e altre operazioni dell'host.

Autenticazione di SQL Server

Il metodo di autenticazione SQL esegue l'autenticazione con un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere rilevata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. È necessaria l'autenticazione di SQL Server per eseguire operazioni come la pianificazione su SQL Server o il rilevamento delle risorse.

Autenticazione Linux

Il metodo di autenticazione Linux esegue l'autenticazione su un host Linux. L'autenticazione Linux è necessaria durante la fase iniziale di aggiunta dell'host Linux e installazione del pacchetto di plug-in SnapCenter per Linux in remoto dall'interfaccia grafica di SnapCenter.

Autenticazione AIX

Il metodo di autenticazione AIX esegue l'autenticazione su un host AIX. È necessaria l'autenticazione AIX durante la fase iniziale di aggiunta dell'host AIX e installazione del pacchetto di plug-in SnapCenter per AIX in remoto dalla GUI di SnapCenter.

Autenticazione del database Oracle

Il metodo di autenticazione del database Oracle esegue l'autenticazione su un database Oracle. Se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione del database Oracle per eseguire operazioni sul database Oracle. Pertanto, prima di aggiungere una credenziale di database Oracle, è necessario creare un utente Oracle nel database Oracle con privilegi sysdba.

Autenticazione Oracle ASM

Il metodo di autenticazione Oracle ASM esegue l'autenticazione con un'istanza di Oracle Automatic Storage Management (ASM). Se viene richiesto di accedere all'istanza di Oracle ASM e se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione Oracle ASM. Pertanto, prima di aggiungere una credenziale Oracle ASM, è necessario creare un utente Oracle con privilegi sysasm nell'istanza di ASM.

Autenticazione del catalogo RMAN

Il metodo di autenticazione del catalogo RMAN viene autenticato nel database del catalogo Oracle Recovery Manager (RMAN). Se è stato configurato un meccanismo di catalogo esterno e il database è stato registrato nel database del catalogo, è necessario aggiungere l'autenticazione del catalogo RMAN.

Connessioni e credenziali dello storage

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

- **Connessioni storage**

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

- **Credenziali**

  - Amministratore di dominio o qualsiasi membro del gruppo di amministratori

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

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

    Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato

nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host.

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

- Credenziali per singoli gruppi di risorse

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

Autenticazione a più fattori (MFA)

Gestire l'autenticazione a più fattori (MFA)

È possibile gestire la funzionalità di autenticazione multifattore (MFA) nel server del servizio di federazione Active Directory (ad FS) e nel server SnapCenter.

Attiva autenticazione a più fattori (MFA)

È possibile attivare la funzionalità MFA per il server SnapCenter utilizzando i comandi PowerShell.

A proposito di questa attività

- SnapCenter supporta gli accessi basati su SSO quando altre applicazioni sono configurate nello stesso ad FS. In alcune configurazioni di ad FS, SnapCenter potrebbe richiedere l'autenticazione dell'utente per motivi di sicurezza, a seconda della persistenza della sessione di ad FS.
- Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, è anche possibile vedere "Guida di riferimento al cmdlet del software SnapCenter".

Prima di iniziare

- Windows Active Directory Federation Service (ad FS) deve essere attivo e in esecuzione nel rispettivo dominio.
- È necessario disporre di un servizio di autenticazione multifattore supportato da ad FS, ad esempio Azure MFA, Cisco Duo e così via.
- L'indicatore di data e ora del server SnapCenter e ad FS deve essere lo stesso indipendentemente dal fuso orario.
- Procurarsi e configurare il certificato CA autorizzato per il server SnapCenter.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non si interrangano perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l'upgrade, la riparazione o il disaster recovery (DR) in una configurazione standalone o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce risoluzioni IP-FQDN.

    Per informazioni sul certificato CA, vedere "Generare il file CSR del certificato CA".

Fasi

1. Connettersi all'host Active Directory Federation Services (ad FS).
2. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato sul server SnapCenter per attivare la funzione MFA.
4. Accedere al server SnapCenter come utente amministratore di SnapCenter tramite PowerShell.
5. Utilizzando la sessione PowerShell, generare il file di metadati MFA di SnapCenter utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   Il parametro path specifica il percorso per salvare il file di metadati MFA nell'host del server SnapCenter.
6. Copiare il file generato nell'host ad FS per configurare SnapCenter come entità client.
7. Attivare MFA per il server SnapCenter utilizzando il `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) controllare lo stato e le impostazioni della configurazione MFA utilizzando il `Get-SmMultiFactorAuthentication` cmdlet.
9. Accedere alla console di gestione Microsoft (MMC) ed effettuare le seguenti operazioni:
   a. Fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Fare clic con il pulsante destro del mouse sul certificato CA associato a SnapCenter, quindi selezionare **tutte le attività** > **Gestisci chiavi private**.
   f. Nella procedura guidata delle autorizzazioni, attenersi alla seguente procedura:
      i. Fare clic su **Aggiungi**.
      ii. Fare clic su **Locations** (posizioni) e selezionare l'host desiderato (in cima alla gerarchia).
      iii. Fare clic su **OK** nella finestra a comparsa **Locations**.
      iv. Nel campo Object name (Nome oggetto), immettere 'IIS_IUSRS', fare clic su **Check Names** (Controlla nomi) e fare clic su **OK**.

      Se il controllo ha esito positivo, fare clic su **OK**.
10. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:
    a. Fare clic con il pulsante destro del mouse su **Trust di parte affidabile** > **Aggiungi Trust di parte affidabile** > **Start**.
    b. Selezionare la seconda opzione, sfogliare il file di metadati MFA di SnapCenter e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Scegliere un criterio di controllo degli accessi come richiesto e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **fine**.

    SnapCenter si riflette ora come parte di base con il nome visualizzato fornito.
11. Selezionare il nome ed effettuare le seguenti operazioni:

a. Fare clic su **Edit Claim Issuance Policy** (Modifica policy di emissione richieste
b. Fare clic su **Add Rule** (Aggiungi regola) e fare clic su **Next** (Avanti).
c. Specificare un nome per la regola di richiesta di rimborso.
d. Selezionare **Active Directory** come archivio di attributi.
e. Selezionare l'attributo **User-Principal-Name** e il tipo di richiesta di rimborso in uscita come **Name-ID**.
f. Fare clic su **fine**.

12. Eseguire i seguenti comandi PowerShell sul server ADFS.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. Attenersi alla seguente procedura per confermare che i metadati sono stati importati correttamente.
    a. Fare clic con il pulsante destro del mouse sul trust della parte che si basa e selezionare **Proprietà**.
    b. Assicurarsi che i campi Endpoint, Identifier e Firma siano compilati.
14. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

La funzionalità MFA di SnapCenter può anche essere attivata utilizzando API REST.

Per informazioni sulla risoluzione dei problemi, fare riferimento alla "I tentativi di accesso simultanei in più schede mostrano un errore MFA".

Aggiornare i metadati di ad FS MFA

È necessario aggiornare i metadati MFA di ad FS in SnapCenter ogni volta che si verifica una modifica nel server di ad FS, ad esempio aggiornamento, rinnovo del certificato CA, DR e così via.

Fasi

1. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiare il file scaricato sul server SnapCenter per aggiornare la configurazione MFA.
3. Aggiornare i metadati di ad FS in SnapCenter eseguendo il seguente cmdlet:

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Aggiornare i metadati MFA di SnapCenter

È necessario aggiornare i metadati MFA di SnapCenter in ad FS ogni volta che si verifica una modifica nel server ADFS, ad esempio riparazione, rinnovo del certificato CA, DR e così via.

Fasi

1. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:

a. Fare clic su **Trust di parte**.
b. Fare clic con il pulsante destro del mouse sul trust della parte di base creato per SnapCenter e fare clic su **Elimina**.

   Viene visualizzato il nome definito dall'utente del trust della parte che si basa.

c. Attivare l'autenticazione a più fattori (MFA).

   Vedere "Abilitare l'autenticazione a più fattori".

2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Disattiva autenticazione a più fattori (MFA)

Fasi

1. Disattivare MFA e pulire i file di configurazione creati quando MFA è stato attivato utilizzando il `Set-SmMultiFactorAuthentication` cmdlet.
2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Gestisci l'autenticazione a più fattori (MFA) utilizzando REST API, PowerShell e SCCLI

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. MFA è supportato tramite un Identity manager di ad FS. È possibile attivare MFA, disattivare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

Impostare ad FS come OAuth/OIDC

Configurare ad FS utilizzando la GUI di Windows

1. Accedere a **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Accedere a **ADFS** > **gruppi di applicazioni**.
   a. Fare clic con il pulsante destro del mouse su **gruppi di applicazioni**.
   b. Selezionare **Add Application group** (Aggiungi gruppo di applicazioni) e immettere **Application Name** (Nome applicazione).
   c. Selezionare **applicazione server**.
   d. Fare clic su **Avanti**.
3. Copia **identificatore del client**.

   ID client. .. Aggiungere l'URL di richiamata (URL del server SnapCenter) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Selezionare **generate shared secret**.

   Copiare il valore segreto. Questo è il segreto del cliente. .. Fare clic su **Avanti**.

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.
   a. Nella pagina **complete**, fare clic su **Close** (Chiudi).

6. Fare clic con il pulsante destro del mouse sul nuovo **Application Group** e selezionare **Properties**.
7. Selezionare **Aggiungi applicazione** da Proprietà applicazione.
8. Fare clic su **Aggiungi applicazione**.

   Selezionare API Web e fare clic su **Avanti**.

9. Nella pagina Configura API web, inserire l'URL del server SnapCenter e l'identificativo client creati nel passaggio precedente nella sezione identificativo.
   a. Fare clic su **Aggiungi**.
   b. Fare clic su **Avanti**.
10. Nella pagina **Choose Access Control Policy** (Scegli policy di controllo dell'accesso), selezionare la policy di controllo in base ai requisiti (ad esempio, Permit Everyone and Request MFA) e fare clic su **Next** (Avanti).
11. Nella pagina **Configure Application Permission** (Configura autorizzazione applicazione), per impostazione predefinita openid è selezionato come ambito, fare clic su **Next** (Avanti).
12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

    Nella pagina **complete**, fare clic su **Close** (Chiudi).

13. Nella pagina **Proprietà applicazione di esempio**, fare clic su **OK**.
14. Token JWT emesso da un server di autorizzazione (ad FS) e destinato ad essere utilizzato dalla risorsa.

    La richiesta "aud" o di pubblico di questo token deve corrispondere all'identificatore della risorsa o dell'API Web.

15. Modificare l'API Web selezionata e verificare che l'URL di richiamata (URL del server SnapCenter) e l'identificatore del client siano stati aggiunti correttamente.

    Configurare OpenID Connect in modo da fornire un nome utente come rivendicato.

16. Aprire lo strumento **ad FS Management** situato nel menu **Tools** in alto a destra di Server Manager.
    a. Selezionare la cartella **Application Groups** dalla barra laterale sinistra.
    b. Selezionare l'API Web e fare clic su **EDIT**.
    c. Accedere alla scheda Issuance Transform Rules (regole di trasformazione emissione)
17. Fare clic su **Add Rule** (Aggiungi regola).
    a. Selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) nell'elenco a discesa Claim Rule template (
    b. Fare clic su **Avanti**.
18. Inserire il nome **Claim rule**.
    a. Selezionare **Active Directory** nell'elenco a discesa dell'archivio degli attributi.
    b. Selezionare **User-Principal-Name** nel menu a discesa **LDAP Attribute** e **UPN** nel menu a discesa o*utgoing Claim Type*.
    c. Fare clic su **fine**.

Creare un gruppo di applicazioni utilizzando i comandi PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per ulteriori informazioni, vedere <link to KB article>.

1. Creare il nuovo gruppo di applicazioni in ad FS utilizzando la seguente comand.

   ```
   New-AdfsApplicationGroup -Name $ClientRoleIdentifier
   -ApplicationGroupIdentifier $ClientRoleIdentifier
   ```

   `ClientRoleIdentifier` nome del gruppo di applicazioni

   `redirectURL` URL valido per il reindirizzamento dopo l'autorizzazione

2. Creare l'applicazione server di ad FS e generare il segreto del client.

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. Creare l'applicazione API Web ADFS e configurare il nome del criterio da utilizzare.

   ```
   $identifier = (New-Guid).Guid

   Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
   -Name "App Web API"

   -Identifier $identifier -AccessControlPolicyName "Permit everyone"
   ```

4. Ottenere l'ID client e il client secret dall'output dei seguenti comandi perché vengono visualizzati una sola volta.

   ```
   "client_id = $identifier"

   "client_secret: "$($ADFSApp.ClientSecret)
   ```

5. Concedere all'applicazione ad FS le autorizzazioni Allatclaims e openid.

   ```
   Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
   -ServerRoleIdentifier $identifier -ScopeNames @('openid')

   $transformrule = @"

   @RuleTemplate = "LdapClaims"

   @RuleName = "AD User properties and Groups"

   c:[Type ==
   "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
   Issuer ==

   "AD AUTHORITY"]
   ```

```
⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. Annotare il file di regole di trasformazione.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Assegnare un nome all'applicazione API Web e definirne le regole di conversione mediante un file esterno.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Aggiornare il tempo di scadenza del token di accesso

È possibile aggiornare il tempo di scadenza del token di accesso utilizzando il comando PowerShell.

A proposito di questa attività

- Un token di accesso può essere utilizzato solo per una combinazione specifica di utente, client e risorsa. I token di accesso non possono essere revocati e sono validi fino alla scadenza.
- Per impostazione predefinita, la scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e scalabile. Devi fornire un valore sufficiente per evitare qualsiasi lavoro business-critical in corso.

Passo

Per aggiornare il tempo di scadenza del token di accesso per un gruppo di applicazioni WebAPI, utilizzare il seguente comando nel server ad FS.

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

Ottenere il token del bearer da ad FS

Inserire i parametri indicati di seguito in qualsiasi client REST (come Postman) e richiedere di inserire le credenziali dell'utente. Inoltre, è necessario immettere l'autenticazione a secondo fattore (qualcosa che si ha e qualcosa che si è) per ottenere il token portante.

+ la validità del token portante è configurabile dal server ad FS per applicazione e il periodo di validità predefinito è di 60 minuti.

Campo	Valore
Tipo di concessione	Codice di autorizzazione

URL di richiamata	Se non si dispone di un URL di richiamata, immettere l'URL di base dell'applicazione.
URL di autenticazione	[adfs-domain-name]/adfs/oauth2/authorize
URL token di accesso	[adfs-domain-name]/adfs/oauth2/token
ID client	Inserire l'ID del client ad FS
Segreto del client	Inserire il segreto del client ad FS
Scopo	OpenID
Autenticazione del client	Invia come intestazione AUTH di base
Risorsa	Nella scheda **Opzioni avanzate**, aggiungere il campo risorsa con lo stesso valore dell'URL di richiamata, che viene fornito come valore "aud" nel token JWT.

Configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API

È possibile configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API.

Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) viene esteso con un altro campo chiamato "AccessToken" per utilizzare il token bearer per autenticare l'utente.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

Una volta eseguito il cmdlet sopra indicato, viene creata una sessione per consentire al rispettivo utente di eseguire ulteriori cmdlet SnapCenter.

Autenticazione API REST MFA SnapCenter

Utilizzare il token bearer nel formato *Authorization=bearer <access token>* nel client API REST (come Postman o swagger) e citare il nome del ruolo dell'utente nell'intestazione per ottenere una risposta corretta da SnapCenter.

Flusso di lavoro API REST MFA

Quando MFA è configurato con ad FS, è necessario eseguire l'autenticazione utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter da qualsiasi API REST.

A proposito di questa attività

- Puoi utilizzare qualsiasi client REST come Postman, Swagger UI o FireCamp.

- Ottenere un token di accesso e utilizzarlo per autenticare le richieste successive (API REST SnapCenter) per eseguire qualsiasi operazione.

Fasi

Per l'autenticazione tramite ad FS MFA

1. Configurare il client REST per chiamare l'endpoint ad FS per ottenere il token di accesso.

   Quando si preme il pulsante per ottenere un token di accesso per un'applicazione, si viene reindirizzati alla pagina SSO di ad FS, dove è necessario fornire le credenziali ad e autenticare con MFA. 1. Nella pagina SSO di ad FS, digitare il nome utente o l'indirizzo e-mail nella casella di testo Nome utente.

   + i nomi utente devono essere formattati come utente@dominio o dominio\utente.

2. Digitare la password nella casella di testo Password.
3. Fare clic su **Log in** (Accedi).
4. Nella sezione **Opzioni di accesso**, selezionare un'opzione di autenticazione e autenticare (a seconda della configurazione).
   - Push: Consente di approvare la notifica push inviata al telefono.
   - Codice QR: Utilizza l'app mobile AUTH Point per eseguire la scansione del codice QR, quindi digita il codice di verifica visualizzato nell'app
   - Password monouso: Digitare la password monouso per il token.
5. Una volta completata l'autenticazione, viene visualizzata una finestra a comparsa contenente Access, ID e Refresh Token.

   Copiare il token di accesso e utilizzarlo nell'API REST di SnapCenter per eseguire l'operazione.

6. Nell'API REST, passare il token di accesso e il nome del ruolo nella sezione dell'intestazione.
7. SnapCenter convalida questo token di accesso da ad FS.

   Se si tratta di un token valido, SnapCenter lo decodifica e ottiene il nome utente.

8. Utilizzando il nome utente e il nome ruolo, SnapCenter autentica l'utente per un'esecuzione API.

   Se l'autenticazione ha esito positivo, SnapCenter restituisce il risultato, altrimenti viene visualizzato un messaggio di errore.

Attivare o disattivare la funzionalità MFA di SnapCenter per API REST, CLI e GUI

GUI

Fasi

1. Accedere al server SnapCenter come amministratore SnapCenter.
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni MultiFactorAuthentication(MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per attivare o disattivare l'accesso MFA.

Interfaccia PowerShell

Fasi

1. Eseguire i comandi PowerShell o CLI per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

   ```
   Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
   -IsCliMFAEnabled -Path
   ```

   Il parametro path specifica la posizione del file xml di metadati di ad FS MFA.

   Abilita MFA per GUI SnapCenter, API REST, PowerShell e SCCLI configurati con il percorso file di metadati ad FS specificato.

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando il `Get-SmMultiFactorAuthentication` cmdlet.

INTERFACCIA SCCLI

Fasi

1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. `# sccli Get-SmMultiFactorAuthentication`

API REST

1. Eseguire la seguente API post per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale
Metodo HTTP	Post
Corpo della richiesta	{ "IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com" }

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando la seguente API.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale

Metodo HTTP	Ottieni
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com" }

Installare il server SnapCenter

È possibile eseguire il programma di installazione del server SnapCenter per installare il server SnapCenter.

È possibile eseguire diverse procedure di installazione e configurazione utilizzando i cmdlet PowerShell.

L'installazione automatica del server SnapCenter dalla riga di comando non è supportata.

Prima di iniziare

- L'host del server SnapCenter deve essere aggiornato con gli aggiornamenti di Windows senza riavvii di sistema in sospeso.
- È necessario assicurarsi che MySQL Server non sia installato sull'host in cui si intende installare il server SnapCenter.
- Dovrebbe essere stato attivato il debug del programma di installazione di Windows.

  Per informazioni sull'attivazione di , consultare il sito Web Microsoft "Registrazione del programma di installazione di Windows".

Non installare il server SnapCenter su un host che dispone di server Exchange, Active Directory o server dei nomi di dominio.

Fasi

1. Scaricare il pacchetto di installazione del server SnapCenter da "Sito di supporto NetApp".
2. Avviare l'installazione del server SnapCenter facendo doppio clic sul file .exe scaricato.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

3. Esaminare i valori precompilati richiesti per l'installazione del server SnapCenter e modificarli, se necessario.

   Non è necessario specificare la password per il database del repository MySQL Server. Durante l'installazione del server SnapCenter, la password viene generata automaticamente.

Il carattere speciale “%” is not supported in the custom path for the repository database. If you include "`%"" nel percorso, l’installazione non riesce.

4. Fare clic su **Installa ora**.

   Se sono stati specificati valori non validi, vengono visualizzati i messaggi di errore appropriati. Immettere nuovamente i valori e avviare l’installazione.

   Se si fa clic sul pulsante **Annulla**, la fase in corso di esecuzione viene completata e quindi viene avviata l’operazione di rollback. Il server SnapCenter verrà completamente rimosso dall’host.

   Tuttavia, se si fa clic su **Annulla** durante l’esecuzione delle operazioni "riavvio del server SnapCenter" o "in attesa dell’avvio del server SnapCenter", l’installazione proseguirà senza annullare l’operazione.

   I file di log sono sempre elencati (per primi quelli meno recenti) nella cartella %temp% dell’utente amministratore. Se si desidera reindirizzare le posizioni del registro, avviare l’installazione del server SnapCenter dal prompt dei comandi eseguendo:`C:\installer_location\installer_name.exe /log"C:\"`

Accedere a SnapCenter utilizzando l’autorizzazione RBAC

SnapCenter supporta il RBAC (role-based access control). L’amministratore di SnapCenter assegna ruoli e risorse tramite SnapCenter RBAC a un utente nel gruppo di lavoro o in Active Directory o a gruppi in Active Directory. L’utente RBAC può ora accedere a SnapCenter con i ruoli assegnati.

Prima di iniziare

- Attivare il servizio di attivazione del processo Windows (WAS) in Windows Server Manager.
- Se si desidera utilizzare Internet Explorer come browser per accedere al server SnapCenter, assicurarsi che la modalità protetta sia disattivata.

A proposito di questa attività

Durante l’installazione, l’installazione guidata del server SnapCenter crea un collegamento e lo posiziona sul desktop e nel menu Start dell’host in cui è installato SnapCenter. Inoltre, al termine dell’installazione, la procedura guidata di installazione visualizza l’URL SnapCenter in base alle informazioni fornite durante l’installazione, che è possibile copiare se si desidera effettuare l’accesso da un sistema remoto.

Se nel browser Web sono aperte più schede, la chiusura della scheda del browser SnapCenter non consente di disconnettersi da SnapCenter. Per terminare la connessione con SnapCenter, è necessario disconnettersi da SnapCenter facendo clic sul pulsante **Esci** o chiudendo l’intero browser Web.

Best practice: per motivi di sicurezza, si consiglia di non abilitare il browser per il salvataggio della password SnapCenter.

L’URL GUI predefinito è una connessione sicura alla porta predefinita 8146 sul server in cui è installato il server SnapCenter (*https://server:8146*). Se durante l’installazione di SnapCenter è stata fornita una porta server diversa, viene utilizzata tale porta.

Per l'implementazione ad alta disponibilità (ha), è necessario accedere a SnapCenter utilizzando l'IP *https://Virtual_Cluster_IP_or_FQDN:8146*. del cluster virtuale Se l'interfaccia utente di SnapCenter non viene visualizzata quando si seleziona *https://Virtual_Cluster_IP_or_FQDN:8146* in Internet Explorer (IE), è necessario aggiungere l'indirizzo IP del cluster virtuale o l'FQDN come sito attendibile in IE su ciascun host plug-in oppure disattivare la protezione avanzata di IE su ciascun host plug-in. Per ulteriori informazioni, vedere "Impossibile accedere all'indirizzo IP del cluster dall'esterno della rete".

Oltre a utilizzare l'interfaccia grafica di SnapCenter, è possibile utilizzare i cmdlet PowerShell per creare script per eseguire operazioni di configurazione, backup e ripristino. Alcuni cmdlet potrebbero essere stati modificati con ogni release di SnapCenter. La "Guida di riferimento al cmdlet del software SnapCenter" contiene i dettagli.

Se si effettua l'accesso a SnapCenter per la prima volta, è necessario effettuare l'accesso utilizzando le credenziali fornite durante il processo di installazione.

Fasi

1. Avviare SnapCenter dal collegamento situato sul desktop host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore di SnapCenter.
2. Immettere le credenziali dell'utente.

Per specificare quanto segue…	Utilizzare uno di questi formati…
Amministratore di dominio	• NetBIOS/nome utente • Nome utente@suffisso UPN Ad esempio, username@netapp.com • Nome utente FQDN del dominio
Amministratore locale	Nome utente

3. Se si dispone di più ruoli, selezionare il ruolo che si desidera utilizzare per questa sessione di accesso dalla casella ruolo.

   L'utente corrente e il ruolo associato vengono visualizzati nella parte superiore destra di SnapCenter dopo l'accesso.

Risultato

Viene visualizzata la pagina Dashboard.

Se la registrazione non riesce e viene visualizzato l'errore che indica che il sito non può essere raggiunto, è necessario mappare il certificato SSL a SnapCenter. "Scopri di più"

Al termine

Dopo aver effettuato l'accesso al server SnapCenter come utente RBAC per la prima volta, aggiornare l'elenco delle risorse.

Se si dispone di domini Active Directory non attendibili che si desidera supportare da SnapCenter, è necessario registrare tali domini con SnapCenter prima di configurare i ruoli per gli utenti in domini non

attendibili. "Scopri di più"

Accedere a SnapCenter utilizzando l'autenticazione multifattore (MFA)

Il server SnapCenter supporta MFA per l'account di dominio, che fa parte di Active Directory.

Prima di iniziare

- Dovrebbe essere stata attivata l'autenticazione MFA.

  Per informazioni su come attivare l'MFA, vedere "Abilitare l'autenticazione a più fattori"

A proposito di questa attività

- È supportato solo il nome FQDN
- Gli utenti di gruppi di lavoro e di più domini non possono accedere utilizzando MFA

Fasi

1. Avviare SnapCenter dal collegamento situato sul desktop host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore di SnapCenter.
2. Nella pagina di accesso ad FS, immettere il nome utente e la password.

   Quando il messaggio di errore nome utente o password non valida viene visualizzato nella pagina ad FS, verificare quanto segue:

   - Se il nome utente o la password sono validi

     L'account utente deve esistere in Active Directory (ad)

   - Se è stato superato il numero massimo di tentativi consentito impostato in ad
   - Se ad e ad FS sono attivi e in esecuzione

Modificare il timeout della sessione GUI predefinita di SnapCenter

È possibile modificare il periodo di timeout della sessione GUI di SnapCenter in modo che sia inferiore o superiore al periodo di timeout predefinito di 20 minuti.

Come funzione di sicurezza, dopo un periodo di inattività predefinito di 15 minuti, SnapCenter avvisa che la sessione della GUI verrà disconnessa in 5 minuti. Per impostazione predefinita, SnapCenter disconnette l'utente dalla sessione GUI dopo 20 minuti di inattività ed è necessario effettuare nuovamente l'accesso.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni** > **Impostazioni globali**.
2. Nella pagina Global Settings (Impostazioni globali), fare clic su **Configuration Settings** (Impostazioni di configurazione).
3. Nel campo Timeout sessione, immettere il timeout della nuova sessione in minuti, quindi fare clic su **Salva**.

Proteggere il server Web SnapCenter disattivando SSL 3.0

Per motivi di sicurezza, è necessario disattivare il protocollo SSL (Secure Socket Layer) 3.0 in Microsoft IIS, se attivato sul server Web SnapCenter.

Il protocollo SSL 3.0 presenta difetti che un utente malintenzionato può utilizzare per causare errori di connessione o per eseguire attacchi man-in-the-middle e osservare il traffico di crittografia tra il sito Web e i relativi visitatori.

Fasi

1. Per avviare l'editor del Registro di sistema sull'host del server Web di SnapCenter, fare clic su **Start** > **Esegui**, quindi digitare regedit.
2. Nell'Editor del Registro di sistema, accedere a HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SecurityProviders/SCHANNEL/Protocols/SSL 3.0.
   - Se la chiave Server esiste già:
     i. Selezionare il DWORD abilitato, quindi fare clic su **Modifica** > **Modifica**.
     ii. Impostare il valore su 0, quindi fare clic su **OK**.
   - Se la chiave Server non esiste:
     i. Fare clic su **Modifica** > **nuovo** > **chiave**, quindi assegnare un nome al server delle chiavi.
     ii. Con la nuova chiave Server selezionata, fare clic su **Edit** > **New** > **DWORD**.
     iii. Assegnare un nome al nuovo DWORD abilitato, quindi immettere 0 come valore.
3. Chiudere l'Editor del Registro di sistema.

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di

Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

> Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Ad esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurare il certificato CA con il sito SnapCenter

È necessario configurare il certificato CA con il sito SnapCenter sull'host Windows.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di navigazione a sinistra, fare clic su **connessioni**.
3. Espandere il nome del server e **Sites**.
4. Selezionare il sito Web di SnapCenter su cui si desidera installare il certificato SSL.
5. Accedere a **azioni** > **Modifica sito**, fare clic su **associazioni**.
6. Nella pagina binding, selezionare **binding for https**.
7. Fare clic su **Edit** (Modifica).
8. Dall'elenco a discesa SSL certificate (certificato SSL), selezionare il certificato SSL importato di recente.
9. Fare clic su **OK**.

Se il certificato CA distribuito di recente non è elencato nel menu a discesa, controllare se il certificato CA è associato alla chiave privata.

Assicurarsi che il certificato venga aggiunto utilizzando il seguente percorso: **Root console > certificati – computer locale > autorità di certificazione root attendibili > certificati**.

Abilitare i certificati CA per SnapCenter

È necessario configurare i certificati CA e attivare la convalida del certificato CA per il server SnapCenter.

Prima di iniziare

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Set-SmCertificateSettings.
- È possibile visualizzare lo stato del certificato per il server SnapCenter utilizzando il cmdlet Get-SmCertificateSettings.

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

Fasi

1. Nella pagina Settings (Impostazioni), selezionare **Settings** (Impostazioni) > **Global Settings** (Impostazioni globali) > **CA Certificate Settings** (Impostazioni certificato CA).
2. Selezionare **attiva convalida certificato**.
3. Fare clic su **Apply** (Applica).

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- * * Indica che non è stato attivato o assegnato alcun certificato CA all'host del plug-in.
- * * Indica che il certificato CA è stato convalidato correttamente.
- * * Indica che il certificato CA non può essere convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Configurare e abilitare la comunicazione SSL bidirezionale

Configurare la comunicazione SSL bidirezionale

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in.

Prima di iniziare

- Il file CSR del certificato CA dovrebbe essere stato generato con la lunghezza minima supportata della chiave di 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- È necessario disporre di un certificato CA con chiave privata e dettagli di identificazione personale.
- La configurazione SSL unidirezionale dovrebbe essere stata attivata.

  Per ulteriori informazioni, vedere "Sezione Configure CA certificate (Configura certificato CA)."

- È necessario attivare la comunicazione SSL bidirezionale su tutti gli host plug-in e sul server SnapCenter.

  L'ambiente con alcuni host o server non abilitati per la comunicazione SSL bidirezionale non è supportato.

Fasi

1. Per eseguire il binding della porta, attenersi alla seguente procedura sull'host del server SnapCenter per la porta 8146 del server Web IIS SnapCenter (impostazione predefinita) e ancora per la porta 8145 SMCore (impostazione predefinita) utilizzando i comandi PowerShell.

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      Ad esempio,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

   b. Associare il certificato CA appena procurato al server SnapCenter e alla porta SMCore.

      ```
      > $cert = "<CA_certificate thumbprint>"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
      certhash=$cert appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable
      ```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Ad esempio,

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Per accedere all'autorizzazione al certificato CA, aggiungere l'utente predefinito del server Web IIS di SnapCenter "**IIS AppPool/SnapCenter**" nell'elenco delle autorizzazioni del certificato eseguendo la procedura seguente per accedere al certificato CA appena procurato.
   a. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi SnapIn**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Selezionare il certificato SnapCenter.
   f. Per avviare l'aggiunta guidata autorizzazioni utente, fare clic con il pulsante destro del mouse sul certificato CA e selezionare **tutte le attività** > **Gestisci chiavi private**.
   g. Fare clic su **Aggiungi**, nella procedura guidata Seleziona utenti e gruppi modificare la posizione in Nome computer locale (in alto nella gerarchia)
   h. Aggiungere l'utente di IIS AppPool/SnapCenter, assegnare autorizzazioni di controllo complete.
3. Per l'autorizzazione IIS * del certificato CA, aggiungere la nuova voce delle chiavi di registro DWORD nel server SnapCenter dal seguente percorso:

   Nell'editor del Registro di sistema di Windows, passare al percorso indicato di seguito,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL
   ```

4. Creare una nuova voce della chiave del Registro di sistema DWORD nel contesto della configurazione DEL Registro DI sistema SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

Configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale

È necessario configurare il plug-in Windows di SnapCenter per la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

Prima di iniziare

Assicurarsi che il thumbprint del certificato CA sia disponibile.

Fasi

1. Per collegare la porta, eseguire le seguenti operazioni sull'host plug-in di Windows per la porta SMCore 8145 (impostazione predefinita).

   a. Rimuovere il binding della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      Ad esempio,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. Associare il certificato CA appena procurato alla porta SMCore.

      ```
      > $cert = "<CA_certificate thumbprint>"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
      appid="$guid" clientcertnegotiation=enable
      verifyclientcertrevocation=disable

      > netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
      ```

      Ad esempio,

      ```
      > $cert = "abc123abc123abc123abc123"

      > $guid = [guid]::NewGuid().ToString("B")

      > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
      clientcertnegotiation=enable verifyclientcertrevocation=disable

    > netsh http show sslcert ipport=0.0.0.0:8145
      ```

Abilitare la comunicazione SSL bidirezionale

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter e i plug-in utilizzando i comandi PowerShell.

Prima di iniziare

Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.

Fasi

1. Per attivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per i plug-in, il server e per ciascuno degli agenti per i quali è richiesta la comunicazione SSL bidirezionale.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Disattiva la comunicazione SSL bidirezionale

È possibile disattivare la comunicazione SSL bidirezionale utilizzando i comandi PowerShell.

A proposito di questa attività

- Eseguire i comandi per tutti i plug-in e l'agente SMCore prima e poi per il server.
- Quando si disattiva la comunicazione SSL bidirezionale, il certificato CA e la relativa configurazione non vengono rimossi.
- Per aggiungere un nuovo host al server SnapCenter, è necessario disattivare il protocollo SSL bidirezionale per tutti gli host plug-in.
- NLB e F5 non sono supportati.

Fasi

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per tutti gli host plug-in e l'host SnapCenter.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando. `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configurare l'autenticazione basata su certificato

Esportare i certificati dell'autorità di certificazione (CA) dal server SnapCenter

È necessario esportare i certificati CA dal server SnapCenter agli host plug-in utilizzando la console di gestione Microsoft.

Prima di iniziare

Il protocollo SSL bidirezionale dovrebbe essere stato configurato.

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra Snap-in certificati, selezionare l'opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato CA procurato, utilizzato per il server SnapCenter, quindi selezionare **tutte le attività** > **Esporta** per avviare l'esportazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Esporta chiave privata	Selezionare **No, non esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Fare clic su **Avanti**.
Nome file	Fare clic su **Browse** (Sfoglia) e specificare il percorso del file per il salvataggio del certificato, quindi fare clic su **Next** (Avanti).
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'esportazione.

L'autenticazione basata su certificato non è supportata per le configurazioni SnapCenter ha e il plug-in SnapCenter per VMware vSphere.

Importa certificato CA (Certificate Authority) negli host plug-in di Windows

Per utilizzare il certificato della CA del server SnapCenter esportato, è necessario importare il certificato correlato negli host dei plug-in di SnapCenter utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra Snap-in certificati, selezionare l'opzione **computer account**, quindi fare clic su **fine**.
4. Fare clic su **Console root** > **certificati - computer locale** > **personale** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Personal", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Eseguire le seguenti operazioni nella procedura guidata.

Per questa opzione…	Effettuare le seguenti operazioni…
Ubicazione del negozio	Fare clic su **Avanti**.
File da importare	Selezionare il certificato del server SnapCenter che termina con l'estensione .cer.
Archivio certificati	Fare clic su **Avanti**.
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Importare il certificato CA nei plug-in host UNIX e configurare i certificati root o intermedi nell'archivio di fiducia SPL

Importa certificato CA negli host plug-in UNIX

È necessario importare il certificato CA negli host plug-in UNIX.

A proposito di questa attività

- È possibile gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmate CA in uso.
- La password per l'archivio chiavi SPL e per tutte le password alias associate della chiave privata deve essere la stessa.

Fasi

1. È possibile recuperare la password predefinita del keystore SPL dal file di proprietà SPL. È il valore corrispondente alla chiave `SPL_KEYSTORE_PASS`.
2. Modificare la password dell'archivio chiavi: `$ keytool -storepasswd -keystore keystore.jks`
3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per l'archivio chiavi: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel `spl.properties` file.
5. Riavviare il servizio dopo aver modificato la password.

Configurare i certificati root o intermedi per l'archivio di trust SPL

È necessario configurare i certificati root o intermedi in SPL trust-store. Aggiungere il certificato CA principale e i certificati CA intermedi.

Fasi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere un certificato root o intermedio: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in SPL trust-store.

Configurare la coppia di chiavi con firma CA nell'archivio di trust SPL

È necessario configurare la coppia di chiavi firmate della CA in SPL trust-store.

Fasi

1. Passare alla cartella contenente il keystore di SPL `/var/opt/snapcenter/spl/etc`.
2. Individuare il file `keystore.jks`.
3. Elencare i certificati aggiunti nell'archivio chiavi: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere il certificato CA con chiave pubblica e privata. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Elencare i certificati aggiunti nel keystore. `$ keytool -list -v -keystore keystore.jks`
6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita dell'archivio chiavi SPL è il valore della chiave SPL_KEYSTORE_PASS nel `spl.properties` file.

   ```
   $ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
   ```

8. Se il nome dell'alias nel certificato CA è lungo e contiene spazi o caratteri speciali ("*",","), modificare il nome dell'alias con un nome semplice: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configurare il nome alias dall'archivio chiavi presente nel `spl.properties` file. Aggiornare questo valore con la chiave SPL_CERTIFICATE_ALIAS.
10. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA in SPL trust-store.

Abilitare l'autenticazione basata su certificato

Per abilitare l'autenticazione basata su certificato per il server SnapCenter e gli host plug-in Windows, eseguire il seguente cmdlet PowerShell. Per gli host plug-in Linux, l'autenticazione basata su certificato viene attivata quando si attiva il protocollo SSL bidirezionale.

- Per attivare l'autenticazione basata su certificati client:

  ```
  Set-SmConfigSettings -Agent -configSettings
  @{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
  ```

- Per disattivare l'autenticazione basata su certificato del client:

  ```
  Set-SmConfigSettings -Agent -configSettings
  @{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
  ```

Configurare Active Directory, LDAP e LDAPS

Registrare domini Active Directory non attendibili

È necessario registrare Active Directory con il server SnapCenter per gestire host, utenti e gruppi di più domini Active Directory non attendibili.

Prima di iniziare

Protocolli LDAP e LDAPS

- È possibile registrare i domini Active Directory non attendibili utilizzando il protocollo LDAP o LDAPS.
- La comunicazione bidirezionale tra gli host plug-in e il server SnapCenter dovrebbe essere stata attivata.
- La risoluzione DNS deve essere impostata dal server SnapCenter agli host plug-in e viceversa.

Protocollo LDAP

- Il nome di dominio completo (FQDN) deve essere risolvibile dal server SnapCenter.

  È possibile registrare un dominio non attendibile con l'FQDN. Se l'FQDN non è risolvibile dal server SnapCenter, è possibile registrarsi con un indirizzo IP del controller di dominio, che dovrebbe essere risolvibile dal server SnapCenter.

Protocollo LDAPS

- I certificati CA sono necessari affinché LDAPS fornisca la crittografia end-to-end durante la comunicazione Active Directory.

  "Configurare il certificato del client CA per LDAPS"

- I nomi host dei controller di dominio (nome host DC) devono essere raggiungibili dal server SnapCenter.

A proposito di questa attività

- È possibile utilizzare l'interfaccia utente di SnapCenter, i cmdlet PowerShell o l'API REST per registrare un dominio non attendibile.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Global Settings (Impostazioni globali), fare clic su **Domain Settings** (Impostazioni dominio).
4. Fare clic su per registrare un nuovo dominio.
5. Nella pagina Registra nuovo dominio, selezionare **LDAP** o **LDAPS**.
   a. Se si seleziona **LDAP**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAP:

Per questo campo…	Eseguire questa operazione…
Domain Name (Nome dominio)	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare l'FQDN e fare clic su **Resolve** (Risolvi).
Indirizzi IP dei controller di dominio	Se l'FQDN del dominio non è risolvibile dal server SnapCenter, specificare uno o più indirizzi IP del controller di dominio. Per ulteriori informazioni, vedere "Aggiungere l'IP del controller di dominio per il dominio non attendibile dalla GUI".

   b. Se si seleziona **LDAPS**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAPS:

Per questo campo…	Eseguire questa operazione…
Domain Name (Nome dominio)	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare l'FQDN.
Nomi dei controller di dominio	Specificare uno o più nomi di controller di dominio e fare clic su **Risolvi**.
Indirizzi IP dei controller di dominio	Se i nomi dei controller di dominio non sono risolvibili dal server SnapCenter, correggere le risoluzioni DNS.

6. Fare clic su **OK**.

Configurare il certificato del client CA per LDAPS

È necessario configurare il certificato del client CA per LDAPS sul server SnapCenter quando quest'ultimo è configurato con i certificati CA.

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Nella seconda pagina della procedura guidata	Fare clic su **Browse** (Sfoglia), selezionare *Root Certificate* (certificato principale) e fare clic su **Next** (Avanti).
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

7. Ripetere i passaggi 5 e 6 per i certificati intermedi.

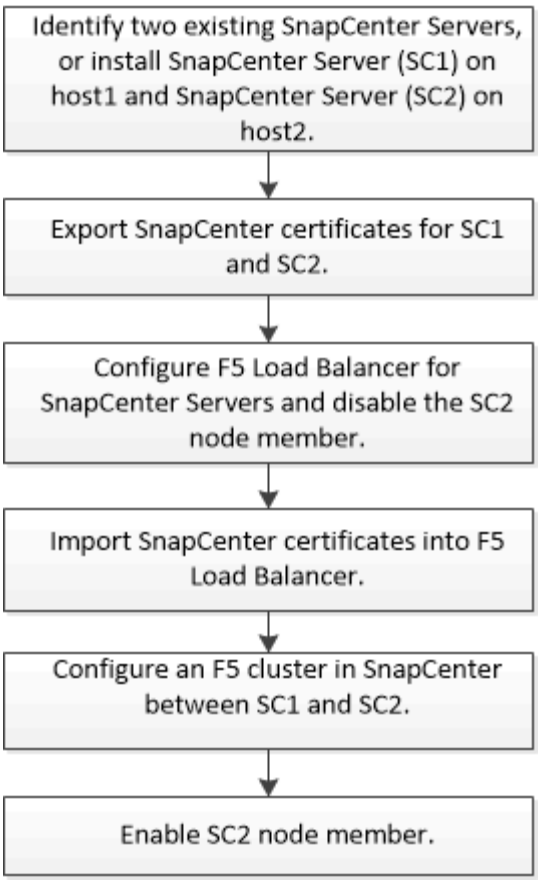
Configurare la disponibilità elevata

Configurare i server SnapCenter per l'alta disponibilità utilizzando F5

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

> Se è stato eseguito l'aggiornamento da SnapCenter 4.2.x e in precedenza si utilizzava il bilanciamento del carico di rete (NLB), è possibile continuare a utilizzare tale configurazione o passare a F5.

L'immagine del flusso di lavoro elenca i passaggi per configurare i server SnapCenter per l'alta disponibilità utilizzando il bilanciamento del carico F5. Per istruzioni dettagliate, vedere "Come configurare i server SnapCenter per l'alta disponibilità utilizzando F5 Load Balancer".



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

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

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

Ulteriori informazioni sulla configurazione di F5

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

diventa attivo.

Configurare Microsoft Network Load Balancer manualmente

È possibile configurare il bilanciamento del carico di rete Microsoft per impostare la disponibilità elevata SnapCenter. A partire da SnapCenter 4.2, è necessario configurare manualmente NLB al di fuori dell'installazione di SnapCenter per ottenere una disponibilità elevata.

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

SnapCenter 4.1.1 o versioni precedenti supportava la configurazione del bilanciamento del carico di rete (NLB) durante l'installazione di SnapCenter.

Passa da NLB a F5 per ottenere alta disponibilità

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

Fasi

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

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

Alta disponibilità per il repository MySQL di SnapCenter

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

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

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

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

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

È necessario conoscere le limitazioni relative alla funzionalità MySQL ha:

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

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

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

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

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

Esportare i certificati SnapCenter

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account utente**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.
5. Fare clic con il pulsante destro del mouse sul certificato con il nome descrittivo SnapCenter, quindi selezionare **tutte le attività** > **Esporta** per avviare l'esportazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Esporta chiave privata	Selezionare l'opzione **Sì, esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
File da esportare	Specificare un nome di file per il certificato esportato (è necessario utilizzare .pfx), quindi fare clic su **Avanti**.

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Completamento dell'esportazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'esportazione.

Risultato

I certificati vengono esportati in formato .pfx.

Configurare RBAC (role-based access control)

Aggiungere un utente o un gruppo e assegnare ruolo e risorse

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

Prima di iniziare

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

> Da SnapCenter 4.5, è possibile includere solo i seguenti caratteri speciali nei nomi utente e nei nomi dei gruppi: Spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:). Se si desidera utilizzare un ruolo creato in una release precedente di SnapCenter con questi caratteri speciali, è possibile disattivare la convalida del nome del ruolo modificando il valore del parametro "DisableSQLInjectionValidation" su true nel file web.config in cui è installata l'applicazione web di SnapCenter. Dopo aver modificato il valore, non è necessario riavviare il servizio.

- SnapCenter include diversi ruoli predefiniti.

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

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

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

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

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

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

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

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

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

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

Fasi

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

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

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

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

c. Ripetere questa procedura per tutte le risorse richieste.

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

5. Fare clic su **Invia**.

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

Creare un ruolo

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

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **ruoli**.
3. Fare clic su .
4. Nella pagina Add role (Aggiungi ruolo), specificare un nome e una descrizione per il nuovo ruolo.

> Da SnapCenter 4.5, è possibile includere solo i seguenti caratteri speciali nei nomi utente e nei nomi dei gruppi: Spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:). Se si desidera utilizzare un ruolo creato in una release precedente di SnapCenter con questi caratteri speciali, è possibile disattivare la convalida del nome del ruolo modificando il valore del parametro "DisableSQLInjectionValidation" su true nel file web.config in cui è installata l'applicazione web di SnapCenter. Dopo aver modificato il valore, non è necessario riavviare il servizio.

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

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

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

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

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

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

Prima di iniziare

- Prima di creare un ruolo RBAC ONTAP per i sistemi storage che eseguono Clustered ONTAP, è necessario identificare quanto segue:
  - L'attività (o le attività) che si desidera eseguire
  - I privilegi richiesti per eseguire queste attività
- La configurazione di un ruolo RBAC richiede l'esecuzione delle seguenti azioni:
  - Concedere privilegi alle directory dei comandi e/o dei comandi.

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

    È sempre necessario assegnare prima i privilegi di accesso completo.
  - Assegnare ruoli agli utenti.
  - Modificare la configurazione a seconda che i plug-in SnapCenter siano collegati all'IP dell'amministratore del cluster per l'intero cluster o direttamente a una SVM all'interno del cluster.

A proposito di questa attività

Per semplificare la configurazione di questi ruoli nei sistemi storage, è possibile utilizzare il tool RBAC User Creator for Data ONTAP, disponibile nel forum delle community NetApp.

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP. Ad esempio, lo strumento RBAC User Creator for Data 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, eseguire nuovamente lo strumento RBAC User Creator for Data ONTAP per aggiornare i ruoli utente creati in precedenza. I ruoli utente creati per una versione precedente di SnapCenter o ONTAP non funzionano correttamente con le versioni aggiornate. Quando si esegue di nuovo, lo strumento gestisce automaticamente l'aggiornamento. Non è necessario ricreare i ruoli.

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

Per coerenza, la documentazione di SnapCenter fa riferimento ai ruoli come all'utilizzo dei privilegi. L'interfaccia utente grafica di Gestore di sistema di OnCommand utilizza il termine *attribute* invece di *Privilege*. Quando si impostano i ruoli RBAC di ONTAP, entrambi questi termini significano la stessa cosa.

Fasi

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

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

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

- Command è la funzionalità ONTAP.

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

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

2. Creare un nome utente immettendo il seguente comando:

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

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

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

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

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

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

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

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

Creare ruoli SVM con privilegi minimi

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

Fasi

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

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

> Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

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

3. Liberare l'utente.

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

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

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

> A partire da SnapCenter 5,0, gli utenti amministratori dei vserver sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non vserver, è necessario utilizzare ZAPI.

- `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 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 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 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
```

Creare ruoli cluster ONTAP con privilegi minimi

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

Fasi

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

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

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

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

3. Liberare l'utente.

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

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

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

A partire da SnapCenter 5,0, gli utenti degli amministratori dei cluster sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non cluster, è necessario utilizzare ZAPI.

- `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 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 "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 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 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

Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory

È possibile configurare Internet Information Services (IIS) sul server Windows per creare

un account pool di applicazioni personalizzato quando è necessario attivare le autorizzazioni di lettura di Active Directory per SnapCenter.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di spostamento di sinistra, fare clic su **Application Pools**.
3. Selezionare SnapCenter nell'elenco Pool di applicazioni, quindi fare clic su **Impostazioni avanzate** nel riquadro delle azioni.
4. Selezionare identità, quindi fare clic su **…** per modificare l'identità del pool di applicazioni SnapCenter.
5. Nel campo Custom account (account personalizzato), immettere un nome utente di dominio o un nome account admin di dominio con l'autorizzazione di lettura di Active Directory.
6. Fare clic su OK.

   L'account personalizzato sostituisce l'account ApplicationPoolIdentity incorporato per il pool di applicazioni SnapCenter.

Configurare le impostazioni del registro di controllo

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

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

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

A proposito di questa attività

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

  I dischi condivisi o montati in rete non sono supportati.

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

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

Fasi

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

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

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

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

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

Aggiungere sistemi storage

È necessario configurare il sistema storage che consente a SnapCenter di accedere allo storage ONTAP o ad Amazon FSX per NetApp ONTAP per eseguire operazioni di provisioning e protezione dei dati.

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

Prima di iniziare

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

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

- I nomi dei sistemi di storage devono essere univoci.

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

A proposito di questa attività

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

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

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

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

Fasi

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

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

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

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

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

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

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

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

      La porta predefinita 443 in genere funziona.

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

      Il valore predefinito è 60 secondi.

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

Risultato

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

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

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

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

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

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

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

Se i sistemi di storage FAS o AFF sono stati aggiornati a tutti gli array SAN (ASA), è necessario aggiornare la connessione di storage nel server SnapCenter in modo che rifletta il nuovo tipo di storage in SnapCenter.

Al termine

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

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

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

Aggiunta di licenze SnapCenter basate su controller standard

È necessaria una licenza basata su controller standard SnapCenter se si utilizzano controller di storage FAS, AFF o All SAN Array (ASA).

La licenza basata su controller ha le seguenti caratteristiche:

- Diritto standard SnapCenter incluso con l'acquisto di bundle premium o flash (non con il pacchetto base)
- Utilizzo illimitato dello storage
- È possibile aggiungerlo direttamente al controller di storage FAS, AFF o ASA utilizzando Gestione di sistema di ONTAP o la riga di comando del cluster di storage

  Non inserire alcuna informazione di licenza nell'interfaccia grafica di SnapCenter per le licenze basate su controller SnapCenter.

- Bloccato sul numero di serie del controller

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

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

È possibile utilizzare l'interfaccia grafica di SnapCenter per verificare se una licenza della suite SnapManager è installata su sistemi di storage primari FAS, AFF o ASA e per identificare i sistemi di storage che potrebbero richiedere licenze della suite SnapManager. Le licenze della suite SnapManager sono valide solo per SVM

FAS, AFF e ASA o per cluster su sistemi storage primari.

> Se si dispone già di una licenza della suite SnapManager sul controller, il diritto alla licenza basata su controller standard SnapCenter viene fornito automaticamente. I nomi licenza SnapManagerSuite e licenza basata su controller standard SnapCenter vengono utilizzati in modo intercambiabile, ma si riferiscono alla stessa licenza.

Fasi

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

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

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

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

Fase 2: Identificare le licenze installate sul controller

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

> La licenza basata su controller standard SnapCenter viene visualizzata come licenza SnapManagerSuite sul controller.

Fasi

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

Output di esempio

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

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

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

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

Fase 3: Recuperare il numero di serie del controller

Per recuperare il numero di serie della licenza basata su controller, è necessario disporre del numero di serie del controller. È possibile recuperare il numero di serie del controller utilizzando la riga di comando ONTAP. È necessario essere un amministratore del cluster nel sistema FAS, AFF o ASA.

Fasi

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

Output di esempio

```
cluster1::> system show -instance

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

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

3. Annotare i numeri di serie.

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

Se si utilizza lo storage FAS o AFF, è possibile recuperare la licenza basata su controller SnapCenter dal sito di supporto NetApp prima di poterla installare utilizzando la riga di comando ONTAP.

Prima di iniziare

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

  Se non si inseriscono credenziali valide, non vengono restituite informazioni per la ricerca.

- Il numero di serie del controller dovrebbe essere disponibile.

Fasi

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

   Viene visualizzato un elenco di licenze per il controller specificato.

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

Fase 5: Aggiungere una licenza basata su controller

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

Prima di iniziare

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

A proposito di questa attività

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

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

Fasi

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

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

   Questo comando è disponibile a livello di privilegio admin.

3. Verificare che la licenza SnapManagerSuite sia installata:

   ```
   license show
   ```

Fase 6: Rimuovere la licenza di prova

Se si utilizza una licenza standard SnapCenter basata su controller e si deve rimuovere la licenza di prova basata su capacità (numero di serie che termina con “50”), utilizzare i comandi MySQL per rimuovere manualmente la licenza di prova. La licenza di prova non può essere eliminata utilizzando l’interfaccia grafica di SnapCenter.

> La rimozione manuale di una licenza di prova è necessaria solo se si utilizza una licenza basata su controller standard SnapCenter. Se si è acquistata una licenza basata sulla capacità standard di SnapCenter e la si è aggiunta nella GUI di SnapCenter, la licenza di prova viene sovrascritta automaticamente.

Fasi

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

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

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

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

Aggiunta di licenze SnapCenter basate sulla capacità standard

Si utilizza una licenza SnapCenter con capacità standard per proteggere i dati sulle piattaforme ONTAP Select e Cloud Volumes ONTAP.

Una licenza di capacità ha le seguenti caratteristiche:

- Composto da un numero di serie di nove cifre con il formato 51xxxxxxx

  Per attivare la licenza utilizzando l’interfaccia grafica di SnapCenter, utilizzare il numero di serie della licenza e le credenziali di accesso al sito di supporto NetApp valide.
- Disponibile come licenza perpetua separata, con il costo basato sulla capacità di storage utilizzata o sulla dimensione dei dati che si desidera proteggere, a seconda di quale sia inferiore, e i dati sono gestiti da SnapCenter
- Disponibile per terabyte

  Ad esempio, è possibile ottenere una licenza basata sulla capacità per 1 TB, 2 TB, 4 TB e così via.
- Disponibile come licenza di prova per 90 giorni con capacità di 100 TB

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

SnapCenter calcola automaticamente l'utilizzo della capacità una volta al giorno a mezzanotte sullo storage ONTAP Select e Cloud Volumes ONTAP gestito. Quando si utilizza una licenza con capacità standard, SnapCenter calcola la capacità inutilizzata deducendo la capacità utilizzata su tutti i volumi dalla capacità totale concessa in licenza. Se la capacità utilizzata supera la capacità concessa in licenza, viene visualizzato un avviso di utilizzo eccessivo nella dashboard di SnapCenter. Se sono state configurate soglie di capacità e notifiche in SnapCenter, viene inviata un'e-mail quando la capacità utilizzata raggiunge la soglia specificata.

Fase 1: Calcolo dei requisiti di capacità

Prima di ottenere una licenza SnapCenter basata sulla capacità, è necessario calcolare la capacità di un host che deve essere gestito da SnapCenter.

L'utente deve essere un amministratore del cluster nel sistema Cloud Volumes ONTAP o ONTAP Select.

A proposito di questa attività

SnapCenter calcola la capacità effettiva utilizzata. Se la dimensione del file system o del database è di 1 TB, ma vengono utilizzati solo 500 GB di spazio, SnapCenter calcola 500 GB di capacità utilizzata. La capacità del volume viene calcolata dopo la deduplica e la compressione e si basa sulla capacità utilizzata dell'intero volume.

Fasi

1. Accedere al controller NetApp utilizzando la riga di comando ONTAP.
2. Per visualizzare la capacità del volume utilizzata, immettere il comando.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

La capacità combinata utilizzata per i due volumi è inferiore a 5 TB; pertanto, se si desidera proteggere tutti i 5 TB di dati, il requisito minimo di licenza SnapCenter basato sulla capacità è di 5 TB.

Tuttavia, se si desidera proteggere solo 2 TB dei 5 TB di capacità totale utilizzata, è possibile acquistare una licenza basata sulla capacità da 2 TB.

Fase 2: Recuperare il numero di serie della licenza basata sulla capacità

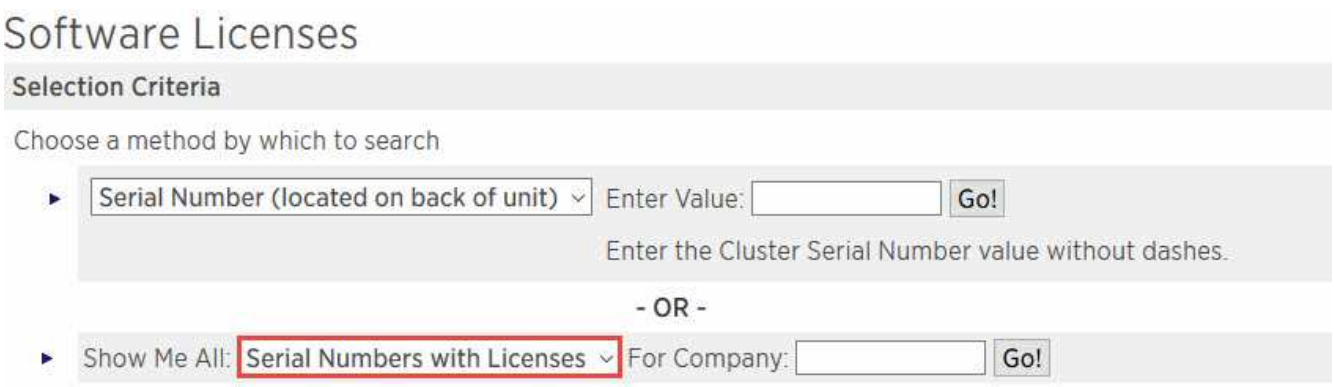
Il numero di serie della licenza SnapCenter basata sulla capacità è disponibile nella conferma dell'ordine o nella documentazione; tuttavia, se non si dispone di questo numero di serie, è possibile recuperarlo dal sito del supporto NetApp.

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

Fasi

1. Accedere a "Sito di supporto NetApp".
2. Accedere a **sistemi** > **licenze software**.

3. Nell'area Selection Criteria (Criteri di selezione), scegliere **SC_STANDARD** dal menu a discesa Show Me All: Serial Numbers and Licenses (Mostra tutti: Numeri di serie e licenze).



4. Digitare il nome della società, quindi selezionare **Go!**.

   Viene visualizzato il numero di serie di nove cifre della licenza SnapCenter, con il formato 51xxxxxxx.

5. Annotare il numero di serie.

Fase 3: Generare un file di licenza NetApp

Se non si desidera inserire le credenziali del sito di supporto NetApp e il numero di serie della licenza SnapCenter nell'interfaccia grafica di SnapCenter o se non si dispone dell'accesso a Internet al sito di supporto NetApp da SnapCenter, è possibile generare un file di licenza NetApp (NLF). È quindi possibile scaricare e memorizzare il file in una posizione accessibile dall'host SnapCenter.

Prima di iniziare

- SnapCenter deve essere utilizzato con ONTAP Select o Cloud Volumes ONTAP.
- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.
- Il numero seriale a nove cifre della licenza deve essere in formato 51xxxxxxx.

Fasi

1. Passare a "NetApp License file Generator".
2. Inserire le informazioni richieste.
3. Nel campo linea di prodotti, selezionare **SnapCenter standard (basato sulla capacità)** dal menu a discesa.
4. Nel campo Product Serial Number (numero di serie del prodotto), inserire il numero di serie della licenza SnapCenter
5. Leggere e accettare la direttiva sulla privacy dei dati di NetApp, quindi selezionare **Invia**.
6. Salvare il file di licenza, quindi registrare la posizione del file.

Fase 4: Aggiunta di una licenza basata sulla capacità

Se si utilizza SnapCenter con piattaforme ONTAP Select o Cloud Volumes ONTAP, è necessario installare una o più licenze SnapCenter basate sulla capacità.

Prima di iniziare

- Accedere come utente amministratore di SnapCenter.

- È necessario disporre di credenziali di accesso al sito di supporto NetApp valide.
- Il numero seriale a nove cifre della licenza deve essere in formato 51xxxxxxx.

  Se si utilizza un file di licenza NetApp (NLF) per aggiungere la licenza, è necessario conoscere la posizione del file di licenza.

A proposito di questa attività

Nella pagina Impostazioni è possibile eseguire le seguenti operazioni:

- Aggiungere una licenza.
- Visualizzare i dettagli della licenza per individuare rapidamente le informazioni relative a ciascuna licenza.
- Modificare una licenza quando si desidera sostituire la licenza esistente, ad esempio per aggiornare la capacità della licenza o per modificare le impostazioni di notifica della soglia.
- Eliminare una licenza quando si desidera sostituire una licenza esistente o quando la licenza non è più necessaria.

La licenza di prova (numero di serie che termina con 50) non può essere eliminata utilizzando l'interfaccia grafica di SnapCenter. La licenza di prova viene sovrascritta automaticamente quando si aggiunge una licenza basata sulla capacità dello standard SnapCenter procurato.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni**.
2. Nella pagina Impostazioni, selezionare **Software**.
3. Nella sezione licenza della pagina Software, selezionare **Aggiungi** (+).
4. Nella procedura guidata Aggiungi licenza SnapCenter, selezionare uno dei seguenti metodi per ottenere la licenza che si desidera aggiungere:

Per questo campo…	Eseguire questa operazione…
Immettere le credenziali di accesso al NetApp Support Site (NSS) per importare le licenze	a. Immettere il nome utente NSS. b. Inserire la password NSS. c. Inserire il numero di serie della licenza basata su controller.
File di licenza NetApp	a. Individuare il percorso del file di licenza, quindi selezionarlo. b. Selezionare **Apri**.

5. Nella pagina Notifiche, immettere la soglia di capacità alla quale SnapCenter invia le notifiche di posta elettronica, EMS e AutoSupport.

   La soglia predefinita è 90 percento.

6. Per configurare il server SMTP per le notifiche e-mail, selezionare **Impostazioni** > **Impostazioni globali** > **Impostazioni server di notifica**, quindi immettere i seguenti dettagli:

Per questo campo…	Eseguire questa operazione…
Preferenza e-mail	Scegliere **sempre** o **mai**.
Fornire le impostazioni e-mail	Se si seleziona **sempre**, specificare quanto segue: • Indirizzo e-mail del mittente • Indirizzo e-mail del destinatario • Facoltativo: Consente di modificare la riga dell'oggetto predefinita Il soggetto predefinito è il seguente: "Notifica della capacità della licenza SnapCenter".

7. Se si desidera che i messaggi del sistema di gestione degli eventi (EMS) vengano inviati al sistema di storage syslog o che i messaggi AutoSupport vengano inviati al sistema di storage per le operazioni non riuscite, selezionare le caselle di controllo appropriate. Si consiglia di attivare AutoSupport per risolvere eventuali problemi.
8. Selezionare **Avanti**.
9. Esaminare il riepilogo, quindi selezionare **fine**.

Eseguire il provisioning del sistema storage

Eseguire il provisioning dello storage su host Windows

Configurare lo storage LUN

È possibile utilizzare SnapCenter per configurare un LUN connesso a FC o a iSCSI. È inoltre possibile utilizzare SnapCenter per connettere un LUN esistente a un host Windows.

I LUN sono l'unità di storage di base in una configurazione SAN. L'host Windows vede le LUN del sistema come dischi virtuali. Per ulteriori informazioni, vedere "Guida alla configurazione SAN di ONTAP 9".

Stabilire una sessione iSCSI

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

Prima di iniziare

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

A proposito di questa attività

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

È possibile utilizzare un indirizzo IPv6 link-local per la gestione della sessione iSCSI e per la comunicazione

tra un host e una destinazione solo quando entrambi si trovano nella stessa subnet.

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

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

Fasi

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

   Viene visualizzata la procedura guidata per stabilire la sessione.

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

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

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

   SnapCenter stabilisce la sessione iSCSI.

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

Disconnettere una sessione iSCSI

A volte, potrebbe essere necessario disconnettere una sessione iSCSI da una destinazione con cui si hanno più sessioni.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.

2. Nella pagina host, fare clic su **iSCSI Session** (sessione iSCSI).
3. Dall'elenco a discesa **Storage Virtual Machine** (macchina virtuale di storage), selezionare la macchina virtuale di storage (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **host**, selezionare l'host per la sessione.
5. Dall'elenco delle sessioni iSCSI, selezionare la sessione che si desidera disconnettere e fare clic su **Disconnetti sessione**.
6. Nella finestra di dialogo Disconnetti sessione, fare clic su **OK**.

   SnapCenter disconnette la sessione iSCSI.

Creare e gestire igroups

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

Creare un igroup

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

Fasi

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

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

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

   SnapCenter crea l'igroup sul sistema storage.

Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

Fasi

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

Modificare un igroup

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

Fasi

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

Eliminare un igroup

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

Fasi

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

   SnapCenter elimina l'igroup.

Creare e gestire i dischi

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

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

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

Visualizzare i dischi su un host

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

Fasi

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

   I dischi sono elencati.

Visualizzare i dischi in cluster

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

Fasi

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

   I dischi sono elencati.

Creazione di LUN o dischi connessi a FC o iSCSI

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

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

Prima di iniziare

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

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

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

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

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

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

Proprietà	Descrizione
Utilizzare il thin provisioning per il volume che ospita questo LUN	Eseguire il thin provisioning del LUN. Il thin provisioning alloca solo lo spazio di storage necessario alla volta, consentendo al LUN di crescere in modo efficiente fino alla massima capacità disponibile. Assicurarsi che sul volume sia disponibile spazio sufficiente per ospitare tutto lo storage LUN che si ritiene necessario.
Scegliere il tipo di partizione	Selezionare la partizione GPT per una tabella di partizione GUID o la partizione MBR per un record di avvio principale. Le partizioni MBR potrebbero causare problemi di disallineamento nei cluster di failover di Windows Server. I dischi di partizione UEFI (Unified Extensible firmware Interface) non sono supportati.

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

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

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

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

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

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

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

Ridimensionare un disco

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

A proposito di questa attività

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

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

Fasi

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

   I dischi sono elencati.

4. Selezionare il disco che si desidera ridimensionare, quindi fare clic su **Ridimensiona**.
5. Nella finestra di dialogo Ridimensiona disco, utilizzare lo strumento a scorrimento per specificare le nuove dimensioni del disco oppure inserire le nuove dimensioni nel campo dimensione.

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

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

   SnapCenter ridimensiona il disco.

Collegare un disco

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

Prima di iniziare

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

Fasi

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

   Viene visualizzata la procedura guidata Connect Disk.

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

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

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

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

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

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

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

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

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

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

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

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

Scollegare un disco

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

Prima di iniziare

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

A proposito di questa attività

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

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

Fasi

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

   I dischi sono elencati.

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

   SnapCenter disconnette il disco.

Eliminare un disco

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

Fasi

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

   I dischi sono elencati.

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

   SnapCenter elimina il disco.

Creare e gestire le condivisioni SMB

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

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

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

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

Creare una condivisione SMB

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

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

Fasi

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

   Viene visualizzata la finestra di dialogo Nuova condivisione.

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

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

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

   SnapCenter crea la condivisione SMB sulla SVM.

Eliminare una condivisione SMB

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

Fasi

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

   SnapCenter elimina la condivisione SMB dalla SVM.

Recuperare spazio sul sistema storage

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

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

Prima di iniziare

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

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

A proposito di questa attività

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

  In questo modo, il processo di recupero può rallentare.

Passo

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

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

Drive_path è il percorso del disco mappato al LUN.

Eseguire il provisioning dello storage utilizzando i cmdlet PowerShell

Se non si desidera utilizzare l'interfaccia grafica di SnapCenter per eseguire il provisioning host e i processi di recupero dello spazio, è possibile utilizzare i cmdlet PowerShell forniti dal plug-in SnapCenter per Microsoft Windows. È possibile utilizzare i cmdlet direttamente o aggiungerli agli script.

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

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

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

Eseguire il provisioning dello storage in ambienti VMware

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

Piattaforme del sistema operativo guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni cluster Microsoft

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

- LUN RDM

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

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

Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Limitazioni relative al server VMware ESXi

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

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

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

Privilegi minimi vCenter richiesti per le operazioni RDM di SnapCenter

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

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

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

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

Gestire LUN RDM FC in un cluster Microsoft

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

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

Requisiti

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

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

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

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

  Non è possibile utilizzare dischi virtuali per lo storage condiviso.

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

compatibilità fisica:

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

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

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

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

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

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

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

Limitazioni

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

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

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

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

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

Creare un LUN FC RDM condiviso

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

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

Configura connessioni MySQL protette con il server SnapCenter

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

Configurare connessioni MySQL protette per configurazioni standalone del server SnapCenter

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

Vengono generati i seguenti certificati:

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

Fasi

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

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

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

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

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

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

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

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

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

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

L'esempio seguente mostra i certificati e i file 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 del server SnapCenter nel server di informazioni Internet (IIS).
5. Riavviare il servizio MySQL.
6. Aggiornare il valore della chiave MySQLProtocol nel file web.config.

   Nell'esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file web.config.

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

7. Aggiornare il file web.config con i percorsi forniti nella sezione [client] del file my.ini.

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

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

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

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

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

Configurare connessioni MySQL protette per le configurazioni ha

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

Vengono generati i seguenti certificati:

- Certificato CA

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

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

Fasi

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

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

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

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

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

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

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

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è C:

ProgramData/NetApp/SnapCenter/MySQL Data/my.ini.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

   Nell'esempio seguente viene illustrato il valore della chiave MySQLProtocol aggiornata nel file web.config.

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

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

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

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

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

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

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

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

Funzionalità abilitate sull'host Windows durante l'installazione

Il programma di installazione del server SnapCenter abilita le funzionalità e i ruoli di Windows sull'host durante l'installazione. Questi potrebbero essere di interesse per la risoluzione dei problemi e la manutenzione del sistema host.

Categoria	Funzione
Server Web	• Internet Information Services • World Wide Web Services • Funzionalità HTTP comuni ◦ Documento predefinito ◦ Navigazione nelle directory ◦ Errori HTTP ◦ Reindirizzamento HTTP ◦ Contenuto statico ◦ Pubblicazione WebDAV • Salute e diagnostica ◦ Registrazione personalizzata ◦ Registrazione HTTP ◦ Strumenti di logging ◦ Richiedi Monitor ◦ Tracciamento • Caratteristiche delle performance ◦ Compressione del contenuto statico • Sicurezza ◦ Sicurezza IP ◦ Autenticazione di base ◦ Supporto centralizzato dei certificati SSL ◦ Autenticazione del mapping dei certificati client ◦ Autenticazione mapping certificati client IIS ◦ Limitazioni di dominio e IP ◦ Filtraggio delle richieste ◦ Autorizzazione URL ◦ Autenticazione di Windows • Funzionalità di sviluppo delle applicazioni ◦ Estendibilità di .NET 4.5 ◦ Inizializzazione dell’applicazione ◦ ASP.NET 4.7.2 ◦ Include lato server ◦ Protocollo WebSocket • Strumenti di gestione ◦ Console di gestione IIS

Categoria	Funzione
Script e strumenti di gestione IIS	• Servizio di gestione IIS • Strumenti di gestione Web
.funzionalità di NET Framework 4.7.2	• .NET Framework 4.7.2 • ASP.NET 4.7.2 • Attivazione HTTP di Windows Communication Foundation (WCF) 45 ◦ Attivazione TCP ◦ Attivazione HTTP ◦ Attivazione di message Queuing (MSMQ) Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet".
Accodamento messaggi	• Servizi di Accodamento messaggi Assicurarsi che nessun'altra applicazione utilizzi il servizio MSMQ creato e gestito da SnapCenter. • Server MSMQ
Servizio di attivazione del processo di Windows	• Modello di processo
API di configurazione	Tutto

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.