Installa e configura SnapCenter Server

SnapCenter software

NetApp
November 06, 2025

Sommario

Installa e configura SnapCenter Server

Prepararsi all'installazione di SnapCenter Server

Requisiti per installare SnapCenter Server

Prima di installare SnapCenter Server su un host Windows o Linux, è necessario verificare e assicurarsi che tutti i requisiti per l'ambiente siano soddisfatti.

Requisiti di dominio e gruppo di lavoro per l'host Windows

SnapCenter Server può essere installato su un host Windows appartenente a un dominio o a un gruppo di lavoro.

L'utente con privilegi di amministratore è autorizzato a installare il server SnapCenter .

- Dominio Active Directory: è necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente del 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 multidominio e trust tra domini, i domini tra foreste non sono supportati. Per ulteriori informazioni, consultare la documentazione Microsoft sui domini e i trust di Active Directory.

Dopo aver installato SnapCenter Server, non modificare il dominio in cui si trova l'host SnapCenter . Se si rimuove l'host di SnapCenter Server dal dominio in cui si trovava al momento dell'installazione di SnapCenter Server e poi si tenta di disinstallare SnapCenter Server, l'operazione di disinstallazione non riesce.

Requisiti di spazio e dimensioni

Dovresti conoscere i requisiti di spazio e dimensioni.

Articolo	Requisiti host Windows	Requisiti host Linux
Sistemi operativi	Microsoft Windows Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi. Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .

Articolo	Requisiti host Windows	Requisiti host Linux
Numero minimo di CPU	4 core	4 core
RAM minima	8 GB Il buffer pool di MySQL Server utilizza il 20 percento della RAM totale.	8 GB
Spazio minimo sul disco rigido per il software e i registri di SnapCenter Server	7 GB Se il repository SnapCenter si trova nella stessa unità in cui è installato SnapCenter Server, si consiglia di disporre di 15 GB.	15 GB
Spazio minimo su disco rigido per il repository SnapCenter	8 GB NOTA: se SnapCenter Server si trova nella stessa unità in cui è installato il repository SnapCenter , si consiglia di disporre di 15 GB.	Non applicabile

Articolo	Requisiti host Windows	Requisiti host Linux
Pacchetti software richiesti	• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) • PowerShell 7.4.2 o versione successiva Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet" .	• .NET Framework 8.0.12 (e tutte le successive patch 8.0.x) • PowerShell 7.4.2 o versione successiva • Nginx è un server web che può essere utilizzato come proxy inverso • Pam-devel PAM (Pluggable Authentication Modules) è uno strumento di sicurezza del sistema che consente agli amministratori di sistema di impostare criteri di autenticazione senza dover ricompilare i programmi che eseguono l'autenticazione.

ASP.NET Core necessita di IIS_IUSRS per accedere al file system temporaneo in SnapCenter Server su Windows.

Requisiti dell'host SAN

SnapCenter non include utilità host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN (FC/iSCSI), potrebbe essere necessario installare e configurare software aggiuntivo sull'host SnapCenter Server.

- Utilità host: le utilità host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. "Saperne di più" .
- Microsoft DSM per Windows MPIO: questo software funziona con i driver Windows MPIO per gestire più percorsi tra NetApp e computer host Windows. Per le configurazioni ad alta disponibilità è necessario un DSM.

Se utilizzavi ONTAP DSM, dovresti migrare a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM" .

Requisiti del browser

Il SnapCenter software supporta Chrome 125 e versioni successive e Microsoft Edge 110.0.1587.17 e versioni successive.

Requisiti portuali

Il SnapCenter software richiede porte diverse per la comunicazione tra i diversi componenti.

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

- Per le porte fisse, dovresti 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 durante l'installazione SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per quella porta per SnapCenter Plug-in Loader.

Nella tabella seguente sono elencate le diverse porte e i relativi valori predefiniti.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Porta web SnapCenter	8146	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra il client SnapCenter (l'utente SnapCenter) e il server SnapCenter e viene utilizzata anche per la comunicazione dagli host del plug-in al server SnapCenter . È possibile personalizzare il numero di porta.
Porta di comunicazione SnapCenter SMCore	8145	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e gli host in cui sono installati i plug-in SnapCenter . È possibile personalizzare il numero di porta.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Porta del servizio di pianificazione	8154	HTTPS		Questa porta viene utilizzata per orchestrare in modo centralizzato i flussi di lavoro dello scheduler di SnapCenter per tutti i plug-in gestiti all'interno dell'host del server SnapCenter . È possibile personalizzare il numero di porta.
Porta RabbitMQ	5672	TCP		Questa è la porta predefinita su cui RabbitMQ è in ascolto e viene utilizzata per la comunicazione del modello publisher-subscriber tra il servizio Scheduler e SnapCenter.
Porta MySQL	3306	HTTPS		La porta viene utilizzata per comunicare con il database del repository SnapCenter . È possibile creare connessioni protette dal server SnapCenter al server MySQL."Saperne di più"

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Host plug-in di Windows	135, 445	TCP		Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host su cui viene installato il plug-in. Dovrebbe essere aperto anche un intervallo di porte dinamiche aggiuntivo specificato da Microsoft.
Host plug-in Linux o AIX	22	SSH	Unidirezionale	Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host, avviata dal server all'host client.
Pacchetto di plug-in SnapCenter per Windows, Linux o AIX	8145	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Personalizzabile. È possibile personalizzare il numero di porta.
Plug-in SnapCenter per Oracle Database	27216			La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle.
Plug-in SnapCenter per database Exchange	909			La porta NET.TCP predefinita viene utilizzata dal plug-in per Windows per la connessione ai callback di Exchange VSS.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Plug-in supportati da NetApp per SnapCenter	9090	HTTPS		Si tratta di una porta interna utilizzata solo sull'host del plug-in; non è richiesta alcuna eccezione del firewall. La comunicazione tra SnapCenter Server e i plug-in avviene tramite la porta 8145.
Cluster ONTAP o porta di comunicazione SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirezionale	La porta viene utilizzata dal SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue SnapCenter Server e SVM. Attualmente la porta è utilizzata anche dal SAL sugli host del plug-in SnapCenter per Windows per la comunicazione tra l'host del plug-in SnapCenter e SVM.
Plug-in SnapCenter per database SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirezionale	Per un contenitore di database multi-tenant (MDC) con un solo tenant, il numero di porta termina con 13; per un contenitore non MDC, il numero di porta termina con 15. È possibile personalizzare il numero di porta.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Plug-in SnapCenter per PostgreSQL	5432			Questa porta è la porta PostgreSQL predefinita utilizzata per la comunicazione tra il plug-in per PostgreSQL e il cluster PostgreSQL. È possibile personalizzare il numero di porta.

Registrati per accedere al SnapCenter software

Se non hai familiarità con Amazon FSx for NetApp ONTAP o Azure NetApp Files e non hai un account NetApp esistente, devi registrarti per accedere al SnapCenter software.

Prima di iniziare

- Dovresti avere accesso all'ID e-mail aziendale.
- Se si utilizza Azure NetApp Files, è necessario disporre dell'ID di sottoscrizione di Azure.
- Se si utilizza Amazon FSx for NetApp ONTAP, è necessario disporre dell'ID del file system FSx per ONTAP .

Informazioni su questo compito

La registrazione è soggetta a convalida delle informazioni e potrebbe volerci fino a un giorno per confermare e aggiornare il nuovo account NetApp Support Site (NSS) dall'accesso **ospite** all'accesso **completo**.

Passi

1. Clic https://mysupport.netapp.com/site/user/registration per la registrazione.
2. Inserisci il tuo ID e-mail aziendale, completa il captcha, accetta l'informativa sulla privacy di NetApp e fai clic su **Invia**.
3. Autentica la registrazione inserendo l'OTP inviato al tuo indirizzo e-mail e clicca su **Continua**.
4. Nella pagina di completamento della registrazione, inserisci i seguenti dati per completare la registrazione.
   a. Seleziona **Cliente NetApp /Utente finale**.
   b. Nel campo NUMERO DI SERIE, immettere l'ID della sottoscrizione di Azure se si utilizza Azure NetApp Files oppure l'ID del file system se si utilizza Amazon FSx for NetApp ONTAP.

Puoi sollevare un biglietto a https://mysupport.netapp.com/site/help se riscontri problemi durante la registrazione o per conoscerne lo stato.

Autenticazione a più fattori (MFA)

Gestire l'autenticazione a più fattori (MFA)

È possibile gestire la funzionalità di autenticazione a più fattori (MFA) nel server Active

Directory Federation Service (AD FS) e nel server SnapCenter .

Abilita l'autenticazione a più fattori (MFA)

È possibile abilitare la funzionalità MFA per SnapCenter Server utilizzando i comandi di PowerShell.

Informazioni su questo compito

- 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 AD FS.
- Le informazioni riguardanti i parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name` . In alternativa, puoi anche vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

Prima di iniziare

- Windows Active Directory Federation Service (AD FS) deve essere attivo e funzionante nel rispettivo dominio.
- Dovresti disporre di un servizio di autenticazione a più fattori supportato da AD FS, come Azure MFA, Cisco Duo e così via.
- Il timestamp SnapCenter e del server AD FS deve essere lo stesso, indipendentemente dal fuso orario.
- Ottenere e configurare il certificato CA autorizzato per SnapCenter Server.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non vengano interrotte perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l'aggiornamento, la riparazione o il ripristino di emergenza (DR) in una configurazione autonoma o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce le risoluzioni IP-FQDN.

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

Passi

1. Connettersi all'host Active Directory Federation Services (AD FS).
2. Scarica il file dei metadati della federazione AD FS da"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato su SnapCenter Server per abilitare la funzionalità MFA.
4. Accedere a SnapCenter Server come utente amministratore SnapCenter tramite PowerShell.
5. Utilizzando la sessione di PowerShell, generare il file di metadati SnapCenter MFA utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   Il parametro path specifica il percorso in cui 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. Abilita MFA per SnapCenter Server utilizzando `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) Controllare lo stato e le impostazioni della configurazione MFA utilizzando `Get-SmMultiFactorAuthentication` cmdlet.

9. Accedere alla console di gestione Microsoft (MMC) ed eseguire i seguenti passaggi:
    a. Fare clic su **File** > **Aggiungi/Rimuovi snap-in**.
    b. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
    c. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
    d. Fare clic su **Console Root** > **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 per le autorizzazioni, eseguire i seguenti passaggi:
        i. Fare clic su **Aggiungi**.
        ii. Fare clic su **Posizioni** e selezionare l'host interessato (in cima alla gerarchia).
        iii. Fare clic su **OK** nella finestra pop-up **Posizioni**.
        iv. Nel campo del nome dell'oggetto, immettere 'IIS_IUSRS' e fare clic su **Controlla nomi**, quindi 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 AD FS ed eseguire i seguenti passaggi:
    a. Fare clic con il pulsante destro del mouse su **Trust della parte affidabile** > **Aggiungi trust della parte affidabile** > **Avvia**.
    b. Selezionare la seconda opzione, sfogliare il file dei metadati SnapCenter MFA e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Selezionare una policy di controllo degli accessi in base alle proprie esigenze e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **Fine**.

        SnapCenter viene ora visualizzato come relying party con il nome visualizzato fornito.

11. Selezionare il nome ed eseguire i seguenti passaggi:
    a. Fare clic su **Modifica politica di emissione reclami**.
    b. Fare clic su **Aggiungi regola** e quindi su **Avanti**.
    c. Specificare un nome per la regola di rivendicazione.
    d. Selezionare **Active Directory** come archivio attributi.
    e. Selezionare l'attributo come **User-Principal-Name** e il tipo di claim 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. Per confermare che i metadati siano stati importati correttamente, procedere come segue.

a. Fare clic con il pulsante destro del mouse sul trust della parte affidabile e selezionare **Proprietà**.

b. Assicurarsi che i campi Endpoint, Identificatori e Firma siano compilati.

14. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

La funzionalità SnapCenter MFA può essere abilitata anche tramite API REST.

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

Aggiorna i metadati AD FS MFA

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

Passi

1. Scarica il file dei metadati della federazione AD FS da"https://<host Nome di dominio completo>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiare il file scaricato su SnapCenter Server per aggiornare la configurazione MFA.
3. Aggiornare i metadati 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 il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

Aggiorna i metadati SnapCenter MFA

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

Passi

1. Nell'host AD FS, aprire la procedura guidata di gestione AD FS ed eseguire i seguenti passaggi:
   a. Selezionare **Trust della parte affidante**.
   b. Fare clic con il pulsante destro del mouse sul trust della relying party creato per SnapCenter e selezionare **Elimina**.

      Verrà visualizzato il nome definito dall'utente del trust della parte affidabile.

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

      Vedere "Abilita l'autenticazione a più fattori" .
2. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

Disabilitare l'autenticazione a più fattori (MFA)

Passi

1. Disabilitare MFA e pulire i file di configurazione creati quando MFA è stato abilitato utilizzando `Set-`

`SmMultiFactorAuthentication` cmdlet.

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

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

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. L'MFA è supportato tramite un gestore di identità AD FS. È possibile abilitare MFA, disabilitare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

Imposta AD FS come OAuth/OIDC

Configurare AD FS utilizzando la procedura guidata GUI di Windows

1. Passare a **Dashboard di Server Manager** > **Strumenti** > **Gestione ADFS**.
2. Passare a **ADFS** > **Gruppi di applicazioni**.
   a. Fare clic con il tasto destro del mouse su **Gruppi di applicazioni**.
   b. Selezionare **Aggiungi gruppo di applicazioni** e immettere **Nome applicazione**.
   c. Selezionare **Applicazione server**.
   d. Fare clic su **Avanti**.
3. Copia **Identificatore cliente**.

   Questo è l'ID cliente. .. Aggiungere l'URL di callback (URL del server SnapCenter) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Seleziona **Genera segreto condiviso**.

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

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.
   a. Nella pagina **Completa**, fare clic su **Chiudi**.
6. Fare clic con il pulsante destro del mouse sul **Gruppo applicazioni** appena aggiunto e selezionare **Proprietà**.
7. Selezionare **Aggiungi applicazione** da Proprietà app.
8. Fare clic su **Aggiungi applicazione**.

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

9. Nella pagina Configura API Web, immettere l'URL del server SnapCenter e l'identificatore client creati nel passaggio precedente nella sezione Identificatore.
   a. Fare clic su **Aggiungi**.
   b. Fare clic su **Avanti**.
10. Nella pagina **Scegli criterio di controllo degli accessi**, seleziona il criterio di controllo in base alle tue esigenze (ad esempio, Consenti a tutti e richiedi MFA) e fai clic su **Avanti**.
11. Nella pagina **Configura autorizzazione applicazione**, per impostazione predefinita openid è selezionato come ambito, fare clic su **Avanti**.
12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

Nella pagina **Completa**, fare clic su **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 a essere utilizzato dalla risorsa.

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

15. Modifica la WebAPI selezionata e verifica che l'URL di callback (URL del server SnapCenter) e l'identificatore client siano stati aggiunti correttamente.

    Configurare OpenID Connect per fornire un nome utente come claim.

16. Aprire lo strumento **Gestione AD FS** che si trova nel menu **Strumenti** in alto a destra di Server Manager.
    a. Selezionare la cartella **Gruppi di applicazioni** dalla barra laterale sinistra.
    b. Selezionare l'API Web e fare clic su **MODIFICA**.
    c. Vai alla scheda Regole di trasformazione dell'emissione
17. Fare clic su **Aggiungi regola**.
    a. Selezionare **Invia attributi LDAP come claim** nel menu a discesa Modello regola claim.
    b. Fare clic su **Avanti**.
18. Inserisci il nome della **Regola di rivendicazione**.
    a. Selezionare **Active Directory** nel menu a discesa Archivio attributi.
    b. Selezionare **User-Principal-Name** nel menu a discesa **LDAP Attribute** e **UPN** nel menu a discesa O*outgoing Claim Type*.
    c. Fare clic su **Fine**.

Creare un gruppo di applicazioni utilizzando i comandi di PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi di PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per maggiori informazioni vedere <link all'articolo della Knowledge Base>.

1. Creare il nuovo gruppo di applicazioni in AD FS utilizzando il seguente comando.

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

   `ClientRoleIdentifier`nome del tuo gruppo di applicazioni

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

2. Creare l'applicazione server AD FS e generare il segreto client.

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

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

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

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

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

4. Ottieni l'ID client e il segreto client dall'output dei seguenti comandi perché vengono mostrati solo una 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. Scrivere il file delle regole di trasformazione.

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

7. Assegna un nome all'applicazione Web API e definisci le sue regole di trasformazione del rilascio utilizzando un file esterno.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Aggiorna il tempo di scadenza del token di accesso

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

Informazioni su questo compito

- 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 loro scadenza.
- Per impostazione predefinita, il tempo di scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e proporzionato. È necessario fornire un valore sufficiente per evitare lavori critici per l'azienda in corso.

Fare un passo

Per aggiornare la 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>"`

Ottieni il token portatore da AD FS

Dovresti compilare i parametri menzionati di seguito in qualsiasi client REST (come Postman) e ti verrà chiesto di inserire le credenziali utente. Inoltre, dovresti inserire l'autenticazione a due fattori (qualcosa che hai e qualcosa che sei) per ottenere il token portatore.

+ La validità del token portatore è configurabile dal server AD FS per applicazione e il periodo di validità predefinito è di 60 minuti.

Campo	Valore
Tipo di sovvenzione	Codice di autorizzazione
URL di richiamata	Se non si dispone di un URL di callback, immettere l'URL di base dell'applicazione.
URL di autorizzazione	[nome-dominio-adfs]/adfs/oauth2/authorize
URL del token di accesso	[nome-dominio-adfs]/adfs/oauth2/token
ID cliente	Inserisci l'ID client AD FS
Segreto del cliente	Inserisci il segreto del client AD FS
Ambito	OpenID
Autenticazione del client	Invia come intestazione AUTH di base
Risorsa	Nella scheda **Opzioni avanzate**, aggiungi il campo Risorsa con lo stesso valore dell'URL di callback, che viene fornito come valore "aud" nel token JWT.

Configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API

È possibile configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API.

Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) è esteso con un ulteriore campo denominato "AccessToken" per utilizzare il token di connessione per autenticare l'utente.

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

Dopo l'esecuzione del cmdlet sopra indicato, viene creata una sessione per consentire all'utente interessato di eseguire ulteriori cmdlet SnapCenter .

Autenticazione API REST MFA SnapCenter

Utilizzare il token del portatore nel formato *Authorization=Bearer <token di accesso>* nel client REST API (come Postman o Swagger) e menzionare l'utente RoleName nell'intestazione per ottenere una risposta positiva da SnapCenter.

Flusso di lavoro dell'API REST MFA

Quando MFA è configurato con AD FS, è necessario autenticarsi utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter tramite qualsiasi API REST.

Informazioni su questo compito

- Puoi utilizzare qualsiasi client REST come Postman, Swagger UI o FireCamp.
- Ottieni un token di accesso e utilizzalo per autenticare le richieste successive (SnapCenter Rest API) per eseguire qualsiasi operazione.

Passi

Per autenticarsi tramite AD FS MFA

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

   Quando fai clic sul pulsante per ottenere un token di accesso per un'applicazione, verrai reindirizzato alla pagina AD FS SSO, dove dovrai fornire le tue credenziali AD ed eseguire l'autenticazione con MFA. 1. Nella pagina AD FS SSO, digita il tuo nome utente o indirizzo email nella casella di testo Nome utente.

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

2. Nella casella di testo Password, digita la tua password.
3. Fare clic su **Accedi**.
4. Dalla sezione **Opzioni di accesso**, seleziona un'opzione di autenticazione ed esegui l'autenticazione (a seconda della configurazione).
   - Push: approva la notifica push inviata al tuo telefono.
   - Codice QR: usa l'app mobile AUTH Point per scansionare il codice QR, quindi digita il codice di verifica mostrato nell'app

◦ Password monouso: digita la password monouso per il tuo token.

5. Dopo l'autenticazione avvenuta con successo, si aprirà una finestra popup contenente il token di accesso, l'ID e il token di aggiornamento.

   Copia il token di accesso e utilizzalo nell'API Rest SnapCenter per eseguire l'operazione.

6. Nell'API REST, dovresti 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 del ruolo, SnapCenter autentica l'utente per l'esecuzione dell'API.

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

Abilita o disabilita la funzionalità SnapCenter MFA per REST API, CLI e GUI

Interfaccia grafica

Passi

1. Accedi al server SnapCenter come amministratore SnapCenter .
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni di autenticazione a più fattori (MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per abilitare o disabilitare l'accesso MFA.

Interfaccia PowerShell

Passi

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 dei metadati AD FS MFA.

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

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

Interfaccia SCCLI

Passi

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	Inviare
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	Ottenere
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

Installa SnapCenter Server sull'host Windows

È possibile eseguire il file eseguibile di installazione di SnapCenter Server per installare SnapCenter Server.

Facoltativamente, è possibile eseguire diverse procedure di installazione e configurazione utilizzando i cmdlet di PowerShell. Dovresti utilizzare PowerShell 7.4.2 o versione successiva.

L'installazione silenziosa di SnapCenter Server dalla riga di comando non è supportata.

Prima di iniziare

- L'host del server SnapCenter deve essere aggiornato con gli aggiornamenti di Windows e non deve esserci alcun riavvio del sistema in sospeso.
- Dovresti assicurarti che MySQL Server non sia installato sull'host in cui intendi installare SnapCenter Server.
- Avresti dovuto abilitare il debug di Windows Installer.

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

  Non installare SnapCenter Server su un host che dispone di Microsoft Exchange Server, Active Directory o Domain Name Server.

Passi

1. Scarica il pacchetto di installazione di SnapCenter Server da "Sito di supporto NetApp" .
2. Avviare l'installazione di SnapCenter Server 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 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. Rivedere i valori precompilati richiesti per l'installazione di SnapCenter Server e modificarli se necessario.

   Non è necessario specificare la password per il database del repository di MySQL Server. Durante l'installazione SnapCenter Server 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 fallisce.

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

   Se sono stati specificati valori non validi, verranno visualizzati i messaggi di errore appropriati. Dovresti reinserire i valori e poi avviare l'installazione.

   Facendo clic sul pulsante **Annulla**, il passaggio in esecuzione verrà completato e verrà avviata l'operazione di rollback. Il server SnapCenter verrà completamente rimosso dall'host.

   Tuttavia, se si fa clic su **Annulla** quando sono in corso le operazioni "Riavvio del sito di SnapCenter Server" o "In attesa dell'avvio di SnapCenter Server", l'installazione procederà senza annullare l'operazione.

   I file di registro vengono sempre elencati (dal più vecchio) nella cartella %temp% dell'utente amministratore. Se si desidera reindirizzare le posizioni dei registri, avviare l'installazione di SnapCenter Server dal prompt dei comandi eseguendo:`C:\installer_location\installer_name.exe /log"C:\"`

Funzionalità abilitate sull'host Windows durante l'installazione

Il programma di installazione di SnapCenter Server abilita le funzionalità e i ruoli di Windows sull'host Windows durante l'installazione. Potrebbero essere utili per la risoluzione dei problemi e la manutenzione del sistema host.

Categoria	Caratteristica
Server Web	• Servizi di informazione Internet • Servizi del World Wide Web • Funzionalità HTTP comuni ◦ Documento predefinito ◦ Esplorazione delle directory ◦ Errori HTTP ◦ Reindirizzamento HTTP ◦ Contenuto statico ◦ Pubblicazione WebDAV • Salute e diagnostica ◦ Registrazione personalizzata ◦ Registrazione HTTP ◦ Strumenti di registrazione ◦ Monitor delle richieste ◦ Tracciamento • Caratteristiche delle prestazioni ◦ Compressione dei contenuti statici • Sicurezza ◦ Sicurezza IP ◦ Autenticazione di base ◦ Supporto centralizzato per certificati SSL ◦ Autenticazione del mapping del certificato client ◦ Autenticazione del mapping dei certificati client IIS ◦ Restrizioni IP e dominio ◦ Filtraggio delle richieste ◦ Autorizzazione URL ◦ Autenticazione di Windows • Funzionalità di sviluppo delle applicazioni ◦ Estensibilità .NET 4.5 ◦ Inizializzazione dell’applicazione ◦ Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) ◦ Inclusioni lato server ◦ Protocollo WebSocket • Strumenti di gestione Console di gestione IIS

Categoria	Caratteristica
Script e strumenti di gestione IIS	• Servizio di gestione IIS • Strumenti di gestione web
.NET Framework 8.0.12 Funzionalità	• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) • Attivazione HTTP di Windows Communication Foundation (WCF)45 ◦ Attivazione TCP ◦ Attivazione HTTP Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet" .
Servizio di attivazione dei processi di Windows	Modello di processo
API di configurazione	Tutto

Installa SnapCenter Server sull'host Linux

È possibile eseguire il file eseguibile di installazione di SnapCenter Server per installare SnapCenter Server.

Prima di iniziare

- Se si desidera installare SnapCenter Server utilizzando un utente non root che non dispone di privilegi sufficienti per installare SnapCenter, ottenere il file di checksum sudoers dal sito di supporto NetApp . Dovresti usare un file di checksum appropriato in base alla versione di Linux.
- Se il pacchetto sudo non è disponibile in SUSE Linux, installarlo per evitare errori di autenticazione.
- Per SUSE Linux, configurare il nome host per evitare errori di installazione.
- Controlla lo stato sicuro di Linux eseguendo il comando `sestatus` . Se lo stato *SELinux* è "abilitato" e la *modalità corrente* è "enforcing", procedere come segue:
  - Eseguire il comando: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    Il valore predefinito di *WEBAPP_EXTERNAL_PORT* è 8146
  - Se il firewall blocca la porta, eseguire `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    Il valore predefinito di *WEBAPP_EXTERNAL_PORT* è 8146
  - Esegui i seguenti comandi dalla directory in cui hai i permessi di lettura e scrittura:
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Se il comando restituisce "niente da fare", eseguire nuovamente il comando dopo aver installato SnapCenter Server.

- Se il comando crea *my-nginx.pp*, eseguire il comando per rendere attivo il pacchetto di policy: `sudo semodule -i my-nginx.pp`

◦ Il percorso utilizzato per la directory PID di MySQL è */var/opt/mysqld*. Eseguire i seguenti comandi per impostare le autorizzazioni per l'installazione di MySQL.

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

◦ Il percorso utilizzato per la directory dei dati MySQL è */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Eseguire i seguenti comandi per impostare le autorizzazioni per la directory dei dati MySQL.

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

Informazioni su questo compito

- Quando SnapCenter Server viene installato sull'host Linux, vengono installati servizi di terze parti come MySQL, RabbitMq, Errlang. Non dovresti disinstallarli.
- Il server SnapCenter installato sull'host Linux non supporta:
  - Alta disponibilità
  - Plug-in di Windows
  - Active Directory (supporta solo gli utenti locali, sia root che non root con credenziali)
  - Autenticazione basata su chiave per accedere a SnapCenter
- Durante l'installazione del runtime .NET, se l'installazione non riesce a risolvere le dipendenze della libreria *libicu*, installare *libicu* eseguendo il comando: `yum install -y libicu`
- Se l'installazione di SnapCenter Server non riesce a causa della non disponibilità di *Perl*, installare *Perl* eseguendo il comando: `yum install -y perl`

Passi

1. Scarica quanto segue da "Sito di supporto NetApp" nella directory */home*.
   - Pacchetto di installazione di SnapCenter Server - **snapcenter-linux-server-(el8/el9/sles15).bin**
   - File della chiave pubblica - **snapcenter_public_key.pub**
   - File di firma rispettivo - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Convalidare il file della firma. `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Per l'installazione da parte di utenti non root, aggiungere il contenuto visudo specificato in **snapcenter_server_checksum_(el8/el9/sles15).txt** disponibile insieme al programma di installazione .bin.
4. Assegnare l'autorizzazione di esecuzione per il programma di installazione .bin. `chmod +x`

`snapcenter-linux-server-(el8/el9/sles15).bin`

5. Eseguire una delle azioni per installare SnapCenter Server.

Se vuoi esibirti…	Fai questo…
Installazione interattiva	`./snapcenter-linux-server-(el8/el9/sles15).bin` Ti verrà chiesto di inserire i seguenti dettagli: • Porta esterna dell'applicazione web utilizzata per accedere a SnapCenter Server al di fuori dell'host Linux. Il valore predefinito è 8146. • L'utente di SnapCenter Server che installerà SnapCenter Server. • La directory di installazione in cui verranno installati i pacchetti.

Se vuoi esibirti…	Fai questo…
Installazione non interattiva	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` Esempio: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log I registri verranno archiviati in */var/opt/snapcenter/logs*. Parametri da passare per l'installazione di SnapCenter Server: • DWEBAPP_EXTERNAL_PORT: porta esterna dell'applicazione Web utilizzata per accedere a SnapCenter Server al di fuori dell'host Linux. Il valore predefinito è 8146. • DWEBAPP_INTERNAL_PORT: porta interna della Webapp utilizzata per accedere a SnapCenter Server nell'host Linux. Il valore predefinito è 8147. • DSMCORE_PORT: porta SMCore su cui sono in esecuzione i servizi smcore. Il valore predefinito è 8145. • DSCHEDULER_PORT: Porta dello scheduler su cui sono in esecuzione i servizi dello scheduler. Il valore predefinito è 8154. • DSNAPCENTER_SERVER_USER: utente di SnapCenter Server che installerà SnapCenter Server. Per *DSNAPCENTER_SERVER_USER*, l'impostazione predefinita è l'utente che esegue il programma di installazione. • DUSER_INSTALL_DIR: Directory di installazione in cui verranno installati i pacchetti. Per *DUSER_INSTALL_DIR*, la directory di installazione predefinita è */opt*. • DINSTALL_LOG_NAME: Nome del file di registro in cui verranno archiviati i registri di installazione. Questo è un parametro facoltativo e se specificato non verrà visualizzato alcun registro sulla console. Se non si specifica questo parametro, i registri verranno visualizzati sulla console e archiviati anche nel file di registro predefinito.

Cosa succederà ora?

- Se lo stato *SELinux* è "abilitato" e la *modalità corrente* è "enforcing", il servizio **nginx** non riesce ad avviarsi. Dovresti eseguire i seguenti comandi:
  a. Vai alla directory home.
  b. Eseguire il comando: `journalctl -x|grep nginx`.
  c. Se la porta interna della Webapp (8147) non è autorizzata all'accesso, eseguire i seguenti comandi:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Correre `setsebool -P httpd_can_network_connect on`
- DSELINUX: se lo *stato SELinux* è "abilitato", la *modalità corrente* è "enforcing" e sono stati eseguiti i comandi menzionati nella sezione Prima di iniziare, è necessario specificare questo parametro e assegnare il valore 1. Il valore predefinito è 0.
- DUPGRADE: Il valore predefinito è 0. Specificare questo parametro e il suo valore come un numero intero diverso da 0 per aggiornare SnapCenter Server.

Funzionalità abilitate sull'host Linux durante l'installazione

SnapCenter Server installa i seguenti pacchetti software che possono aiutare nella risoluzione dei problemi e nella manutenzione del sistema host.

- Rabbitmq
- Erlang

Registra SnapCenter

Se non hai familiarità con i prodotti NetApp e non hai un account NetApp esistente, dovresti registrare SnapCenter per abilitare il supporto.

Passi

1. Dopo aver installato SnapCenter, vai su **Aiuto > Informazioni**.
2. Nella finestra di dialogo *Informazioni su SnapCenter*, prendere nota dell'istanza SnapCenter , un numero di 20 cifre che inizia con 971.
3. Clic https://register.netapp.com .
4. Fare clic su **Non sono un cliente NetApp registrato**.
5. Specifica i tuoi dati per registrarti.
6. Lasciare vuoto il campo NetApp Reference SN.
7. Selezionare * SnapCenter* dal menu a discesa Linea di prodotti.
8. Selezionare il fornitore di fatturazione.
9. Immettere l'ID istanza SnapCenter di 20 cifre.
10. Fare clic su **Invia**.

Accedi a SnapCenter utilizzando l'autorizzazione RBAC

SnapCenter supporta il controllo degli accessi basato sui ruoli (RBAC). L'amministratore SnapCenter assegna ruoli e risorse tramite SnapCenter RBAC a un utente nel gruppo di lavoro o in Active Directory oppure a gruppi in Active Directory. L'utente RBAC può ora accedere a SnapCenter con i ruoli assegnati.

Prima di iniziare

- Dovresti abilitare il servizio Attivazione processo Windows (WAS) in Windows Server Manager.
- Se si desidera utilizzare Internet Explorer come browser per accedere a SnapCenter Server, è necessario assicurarsi che la modalità protetta in Internet Explorer sia disattivata.
- Se SnapCenter Server è installato su un host Linux, è necessario effettuare l'accesso utilizzando l'account utente utilizzato per installare SnapCenter Server.

Informazioni su questo compito

Durante l'installazione, la procedura guidata di installazione di SnapCenter Server 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 accedere da un sistema remoto.

Se hai più schede aperte nel tuo browser web, chiudendo solo la scheda del browser SnapCenter non verrai disconnesso da SnapCenter. Per terminare la connessione con SnapCenter, è necessario uscire da SnapCenter cliccando sul pulsante **Esci** oppure chiudendo l'intero browser web.

Migliore pratica: per motivi di sicurezza, si consiglia di non abilitare il browser per salvare la password SnapCenter .

L'URL GUI predefinito è una connessione sicura alla porta predefinita 8146 sul server su cui è installato SnapCenter Server (*https://server:8146*). Se durante l'installazione SnapCenter è stata specificata una porta server diversa, verrà utilizzata quella porta.

Per la distribuzione ad alta disponibilità (HA), è necessario accedere a SnapCenter utilizzando l'IP del cluster virtuale *https://Virtual_Cluster_IP_or_FQDN:8146*. Se non vedi l'interfaccia utente SnapCenter quando accedi a *https://Virtual_Cluster_IP_or_FQDN:8146* in Internet Explorer (IE), devi aggiungere l'indirizzo IP o FQDN del Virtual Cluster come sito attendibile in IE su ciascun host del plug-in oppure devi disattivare IE Enhanced Security su ciascun host del plug-in. Per ulteriori informazioni, vedere "Impossibile accedere all'indirizzo IP del cluster dalla rete esterna" .

Oltre a utilizzare l'interfaccia utente grafica SnapCenter , è possibile utilizzare i cmdlet di PowerShell per creare script per eseguire operazioni di configurazione, backup e ripristino. Alcuni cmdlet potrebbero essere cambiati con ogni versione SnapCenter . IL "Guida di riferimento ai cmdlet del software SnapCenter" ha i dettagli.

Se accedi a SnapCenter per la prima volta, devi effettuare l'accesso utilizzando le credenziali fornite durante il processo di installazione.

Passi

1. Avvia SnapCenter dal collegamento presente sul desktop dell'host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore SnapCenter .
2. Inserisci le credenziali utente.

Per specificare quanto segue…	Utilizza uno di questi formati…
Amministratore di dominio	• NetBIOS\Nome utente • Suffisso UserName@UPN Ad esempio, username@netapp.com • Nome FQDN del dominio\Nome utente
amministratore locale	Nome utente

3. Se ti è stato assegnato più di un ruolo, dalla casella Ruolo seleziona il ruolo che desideri utilizzare per questa sessione di accesso.

   Dopo aver effettuato l'accesso, l'utente corrente e il ruolo associato vengono visualizzati in alto a destra in SnapCenter .

Risultato

Viene visualizzata la pagina Dashboard.

Se la registrazione fallisce e viene visualizzato l'errore che il sito non è raggiungibile, è necessario mappare il certificato SSL su SnapCenter. "Saperne di più"

Dopo aver finito

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

Se si dispone di domini Active Directory non attendibili che si desidera vengano supportati SnapCenter , è necessario registrare tali domini con SnapCenter prima di configurare i ruoli per gli utenti sui domini non attendibili. "Saperne di più" .

Se si desidera aggiungere l'host del plug-in in SnapCenter in esecuzione su un host Linux, è necessario ottenere il file di checksum dal percorso: */opt/ NetApp/snapcenter/SnapManagerWeb/Repository*.

A partire dalla versione 6.0, sul desktop viene creato un collegamento per SnapCenter PowerShell. È possibile accedere direttamente ai cmdlet di SnapCenter PowerShell utilizzando il collegamento.

Accedi a SnapCenter utilizzando l'autenticazione a più fattori (MFA)

SnapCenter Server supporta l'autenticazione MFA per gli account di dominio, che fanno parte di Active Directory.

Prima di iniziare

Avresti dovuto abilitare MFA. Per informazioni su come abilitare MFA, vedere"Abilita l'autenticazione a più fattori"

Informazioni su questo compito

- È supportato solo FQDN
- Gli utenti di gruppi di lavoro e di domini multipli non possono accedere tramite MFA

Passi

1. Avvia SnapCenter dal collegamento presente sul desktop dell'host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore SnapCenter .
2. Nella pagina di accesso di AD FS, immettere nome utente e password.

   Quando nella pagina AD FS viene visualizzato il messaggio di errore "nome utente o password non validi", è necessario verificare quanto segue:

   - Se il nome utente o la password sono validi

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

   - Se hai superato il numero massimo di tentativi consentiti impostato in AD
   - Se AD e AD FS sono attivi e funzionanti

Modifica il timeout della sessione GUI predefinita di SnapCenter

È possibile modificare il periodo di timeout della sessione dell'interfaccia utente grafica SnapCenter per renderlo inferiore o superiore al periodo di timeout predefinito di 20 minuti.

Come misura di sicurezza, dopo un periodo predefinito di 15 minuti di inattività, SnapCenter avvisa che la sessione GUI verrà disconnessa entro 5 minuti. Per impostazione predefinita, SnapCenter disconnette l'utente dalla sessione GUI dopo 20 minuti di inattività, dopodiché sarà necessario effettuare nuovamente l'accesso.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni** > **Impostazioni globali**.
2. Nella pagina Impostazioni globali, fare clic su **Impostazioni di configurazione**.
3. Nel campo Timeout sessione, immettere il nuovo timeout della sessione in minuti, quindi fare clic su **Salva**.

Proteggi il server web SnapCenter disabilitando SSL 3.0

Per motivi di sicurezza, dovresti disattivare il protocollo Secure Socket Layer (SSL) 3.0 in Microsoft IIS se è abilitato sul tuo server web SnapCenter .

Il protocollo SSL 3.0 presenta delle falle che un aggressore può sfruttare per causare errori di connessione o per eseguire attacchi man-in-the-middle e osservare il traffico di crittografia tra il tuo sito web e i suoi visitatori.

Passi

1. Per avviare l'Editor del Registro di sistema sull'host del server web SnapCenter , fare clic su **Start** > **Esegui**, quindi immettere regedit.
2. Nell'editor del Registro di sistema, vai a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Se la chiave del server esiste già:
     i. Selezionare il valore DWORD abilitato, quindi fare clic su **Modifica** > **Modifica**.
     ii. Modificare il valore su 0, quindi fare clic su **OK**.
   - Se la chiave del server non esiste:

i. Fare clic su **Modifica** > **Nuovo** > **Chiave**, quindi assegnare alla chiave il nome Server.

ii. Dopo aver selezionato la nuova chiave del server, fare clic su **Modifica** > **Nuovo** > **DWORD**.

iii. Assegnare al nuovo DWORD il nome Enabled, quindi immettere 0 come valore.

3. Chiudere l'editor del Registro di sistema.

Configurare il server SnapCenter

Aggiungere e predisporre il sistema di archiviazione

Aggiungere sistemi di archiviazione

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

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

Prima di iniziare

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

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

- I nomi dei sistemi di archiviazione devono essere univoci.

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

Informazioni su questo compito

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

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

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

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

Passi

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

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

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

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

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

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

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

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

      In genere funziona la porta predefinita 443.

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

      Il valore predefinito è 60 secondi.

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

Risultato

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

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

  Se hai aggiunto SVM FSx, questi vengono elencati qui.

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

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

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

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

Dopo aver finito

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

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

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

Connessioni di archiviazione e credenziali

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

Connessioni di archiviazione

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

Credenziali

- Amministratore di dominio o qualsiasi membro del gruppo di amministratori

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

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

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

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

- Credenziali per singoli gruppi di risorse

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

Fornire spazio di archiviazione su host Windows

Creare e gestire igroup

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

Crea un igroup

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

Passi

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

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

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

   SnapCenter crea l'igroup sul sistema di archiviazione.

Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

Passi

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

Modificare un igroup

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

Passi

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

Elimina un igroup

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

Passi

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

   SnapCenter elimina l'igroup.

Creare e gestire dischi

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

- SnapCenter supporta solo dischi di base. I dischi dinamici non sono supportati.
- Per GPT è consentita solo una partizione dati e per MBR è consentita solo una partizione primaria con un volume formattato con NTFS o CSVFS e un percorso di montaggio.

- Stili di partizione supportati: GPT, MBR; in una VM VMware UEFI, sono supportati solo i dischi iSCSI

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

Visualizza i dischi su un host

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

Passi

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

   I dischi sono elencati.

Visualizza i dischi in cluster

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

Passi

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

   I dischi sono elencati.

Stabilire una sessione iSCSI

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

Prima di iniziare

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

Informazioni su questo compito

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

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

Se si modifica il nome di un iniziatore iSCSI, l'accesso alle destinazioni iSCSI ne risente. Dopo aver modificato il nome, potrebbe essere necessario riconfigurare i target a cui accede l'iniziatore in modo che possano riconoscere il nuovo nome. Dopo aver modificato il nome di un iniziatore iSCSI, è necessario assicurarsi di riavviare l'host.

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

Passi

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

   Viene visualizzata la procedura guidata Crea sessione.

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

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

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

   SnapCenter stabilisce la sessione iSCSI.

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

Creare LUN o dischi connessi tramite FC o tramite iSCSI

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

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

Prima di iniziare

- È necessario aver creato un volume per la LUN sul sistema di archiviazione.

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

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

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

Informazioni su questo compito

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

Passi

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

   Si apre la procedura guidata Crea disco.

5. Nella pagina Nome LUN, identificare la LUN:

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

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

Selezionare…	Se…
Disco dedicato	L'accesso alla LUN è consentito solo a un host. Ignora il campo **Gruppo di risorse**.
Disco condiviso	Il LUN è condiviso dagli host in un cluster di failover di Windows Server. Immettere il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. È necessario creare il disco su un solo host nel cluster di failover.
Volume condiviso del cluster (CSV)	Il LUN è condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV. Immettere il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. Assicurarsi che l'host su cui si sta creando il disco sia il proprietario del gruppo cluster.

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

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

Proprietà	Descrizione
Utilizzare il thin provisioning per il volume che ospita questa LUN	Fornire una disposizione sottile della LUN. Il thin provisioning alloca solo lo spazio di archiviazione necessario in un dato momento, consentendo alla LUN di crescere in modo efficiente fino alla massima capacità disponibile. Assicurati che ci sia abbastanza spazio disponibile sul volume per contenere tutto lo spazio di archiviazione LUN che ritieni necessario.
Scegli il tipo di partizione	Selezionare la partizione GPT per una tabella delle partizioni GUID o la partizione MBR per un Master Boot Record. Le partizioni MBR potrebbero causare problemi di disallineamento nei cluster di failover di Windows Server. I dischi di partizione UEFI (Unified Extensible Firmware Interface) non sono supportati.

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

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

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

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

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

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

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

Ridimensionare un disco

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

Informazioni su questo compito

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

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

Passi

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

   I dischi sono elencati.

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

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

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

   SnapCenter ridimensiona il disco.

Collegare un disco

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

Prima di iniziare

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

Passi

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

   Si apre la procedura guidata Connetti disco.

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

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

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

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

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

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

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

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

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

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

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

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

Disconnettere un disco

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

Prima di iniziare

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

Informazioni su questo compito

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

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

Passi

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

   I dischi sono elencati.

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

   SnapCenter disconnette il disco.

Elimina un disco

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

Passi

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

   I dischi sono elencati.

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

   SnapCenter elimina il disco.

Creare e gestire condivisioni SMB

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

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

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

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

Crea una condivisione SMB

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

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

Passi

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

   Si apre la finestra di dialogo Nuova condivisione.

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

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

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

   SnapCenter crea la condivisione SMB sulla SVM.

Elimina una condivisione SMB

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

Passi

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

   SnapCenter elimina la condivisione SMB dall'SVM.

Recuperare spazio sul sistema di archiviazione

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

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

Prima di iniziare

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

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

Informazioni su questo compito

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

  Ciò potrebbe rallentare il processo di bonifica.

Fare un passo

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

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

drive_path è il percorso dell'unità mappato al LUN.

Fornire l'archiviazione utilizzando i cmdlet di PowerShell

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

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

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

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

Fornire storage in ambienti VMware

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

Piattaforme di sistemi operativi guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni del cluster Microsoft

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

- LUN RDM

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

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

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

Limitazioni relative al server VMware ESXi

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

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

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

Privilegi minimi vCenter richiesti per le operazioni SnapCenter RDM

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

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

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

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

Gestire le LUN FC RDM in un cluster Microsoft

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

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

Requisiti

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

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

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

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

  Non è possibile utilizzare dischi virtuali per l'archiviazione condivisa.

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

compatibilità fisica:

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

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

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

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

  L'igroup contenente gli iniziatori di tutti gli host ESXi deve essere creato sul controller di archiviazione prima di creare i LUN RDM che verranno utilizzati come dischi del cluster condivisi.

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

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

Limitazioni

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

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

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

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

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

Creare un LUN FC RDM condiviso

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

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

Aggiungi licenze basate sul controller SnapCenter Standard

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

La licenza basata sul controller presenta le seguenti caratteristiche:

- Diritto a SnapCenter Standard incluso con l'acquisto di Premium o Flash Bundle (non con il pacchetto base)
- Utilizzo illimitato dello spazio di archiviazione
- Aggiunto direttamente al controller di archiviazione FAS, AFF o ASA tramite ONTAP System Manager o ONTAP CLI.

> Per le licenze basate sul controller SnapCenter non è necessario immettere alcuna informazione sulla licenza nell'interfaccia utente SnapCenter .

- Bloccato sul numero di serie del controller

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

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

È possibile utilizzare l'interfaccia utente SnapCenter per verificare se una licenza SnapManager Suite è installata sui sistemi di archiviazione primari FAS, AFF o ASA e identificare quali sistemi necessitano di licenze. Le licenze di SnapManager Suite si applicano solo a SVM o cluster FAS, AFF e ASA su sistemi di storage primari.

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

Passi

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

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

   La colonna Licenza controller visualizza il seguente stato:

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

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

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

Passaggio 2: identificare le licenze installate sul controller

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

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

Passi

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

Esempio di output

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

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

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

Nell'esempio, è installata la licenza SnapManagerSuite, pertanto non è richiesta alcuna ulteriore azione di

licenza SnapCenter .

Passaggio 3: recuperare il numero di serie del controller

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

Passi

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

Esempio di output

```
cluster1::> system show -instance

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

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

3. Annotare i numeri di serie.

Passaggio 4: recuperare il numero di serie della licenza basata sul controller

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

Prima di iniziare

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

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

- Dovresti avere il numero di serie del controller.

Passi

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

   Viene visualizzato un elenco delle licenze per il controller specificato.

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

Passaggio 5: aggiungere la licenza basata sul controller

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

Prima di iniziare

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

Informazioni su questo compito

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

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

Passi

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

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

   Questo comando è disponibile a livello di privilegio amministratore.

3. Verificare che la licenza SnapManagerSuite sia installata:

   ```
   license show
   ```

Passaggio 6: rimuovere la licenza di prova

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

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

Passi

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

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

   MySQL ti chiederà la password. Inserisci le credenziali fornite durante la reimpostazione della password.
3. Rimuovere la licenza di prova dal database:

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

Configurare l’alta disponibilità

Configurare i server SnapCenter per l’alta disponibilità

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

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

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

Configurare l'alta disponibilità utilizzando F5

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

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

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

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

Informazioni aggiuntive

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

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

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

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

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

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

Passi

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

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

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

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

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

Passi

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

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

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

Passi

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

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

Elevata disponibilità per il repository MySQL SnapCenter

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

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

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

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

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

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

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

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

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

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

  Se il failover avviene perché MySQL Server o SnapCenter Server non è attivo, tutti i processi in esecuzione potrebbero non riuscire. Dopo il failover sul secondo nodo, tutti i processi successivi vengono eseguiti correttamente.

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

Configurare il controllo degli accessi basato sui ruoli (RBAC)

Crea un ruolo

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

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

Passi

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

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

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

5. Selezionare **Tutti i membri di questo ruolo possono vedere gli oggetti degli altri membri** per consentire agli altri membri del ruolo di vedere risorse quali volumi e host dopo aver aggiornato l'elenco delle risorse.

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

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

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

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

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

Prima di iniziare

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

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

  È sempre necessario assegnare prima i privilegi di accesso completo.

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

Informazioni su questo compito

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

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP . Ad esempio, lo strumento RBAC User Creator per NetApp ONTAP aggiunge automaticamente i privilegi nell'ordine corretto, in modo che i privilegi di accesso completo vengano visualizzati per primi. Se si aggiungono prima i privilegi di sola lettura e poi i privilegi di accesso completo, ONTAP contrassegna i privilegi di accesso completo come duplicati e li ignora.

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

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

Passi

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

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

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

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

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

2. Crea un nome utente immettendo il seguente comando:

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

   - user_name è il nome dell'utente che stai creando.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà una.
   - svm_name è il nome dell'SVM.

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

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

   - <user_name> è il nome dell'utente creato nel passaggio 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome dell'SVM.
   - <role_name> è il nome del ruolo creato nel passaggio 1.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà una.

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

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

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

Creare ruoli SVM con privilegi minimi

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

Passi

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

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

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

Esistono diversi comandi ONTAP CLI che dovresti eseguire per creare ruoli SVM e assegnare autorizzazioni.

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

"lun igroup add" -access all

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

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

"volume qtree modify" -access all

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

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

Creare ruoli SVM per i sistemi ASA r2

Per creare un ruolo per un nuovo utente SVM nei sistemi ASA r2, è necessario eseguire

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

Passi

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

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

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

Esistono diversi comandi ONTAP CLI che dovresti eseguire per creare ruoli SVM e assegnare autorizzazioni.

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

"lun igroup delete" -access all

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

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

"volume restrict" -access all

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

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

"volume delete" -access all

- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

Creare ruoli cluster ONTAP con privilegi minimi

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

Passi

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

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

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

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

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

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

"lun offline" -access all

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

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

"system node modify" -access all

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

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

"vserver cifs show" -access all

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

Creare ruoli cluster ONTAP per sistemi ASA r2

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

Passi

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

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

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

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

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

"lun igroup rename" -access all

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

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

"snapmirror show" -access all

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

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

"vserver" -access all

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

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

Aggiungi un utente o un gruppo e assegna ruoli e risorse

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

Prima di iniziare

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

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

- SnapCenter include diversi ruoli predefiniti.

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

- Gli utenti AD e i gruppi AD aggiunti a SnapCenter RBAC devono disporre dell'autorizzazione READ sul contenitore Users e sul contenitore Computer in Active Directory.
- Dopo aver assegnato un ruolo a un utente o a un gruppo che contiene le autorizzazioni appropriate, è necessario assegnare all'utente l'accesso alle risorse SnapCenter , come host e connessioni di archiviazione.

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

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

Operazione	Assegnazione dei beni
Proteggere le risorse	ospite, politica
Backup	host, gruppo di risorse, policy

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

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

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

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

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

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

Passi

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

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

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

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

c. Ripetere questa procedura per tutte le risorse richieste.

d. Fare clic su **Salva**.

5. Fare clic su **Invia**.

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

Configurare le impostazioni del registro di controllo

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

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

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

Informazioni su questo compito

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

  Le unità condivise o montate in rete non sono supportate.

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

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

Passi

1. Nella pagina **Impostazioni**, vai a **Impostazioni** > **Impostazioni globali** > **Impostazioni registro di**

controllo.

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

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

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

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

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

Configurare connessioni MySQL protette con SnapCenter Server

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

Configurare connessioni MySQL protette per configurazioni di SnapCenter Server autonome

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

Vengono generati i seguenti certificati:

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

Passi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato nel file SnapManager.Web.UI.dll.config.

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

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

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

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

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

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

8. Avviare l'applicazione Web SnapCenter Server in IIS.

Configurare connessioni MySQL protette per configurazioni HA

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

Vengono generati i seguenti certificati:

- Certificato CA

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

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

Passi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Per il secondo nodo HA, copiare il certificato CA e generare il certificato pubblico del server, i file della chiave privata del server, il certificato pubblico del client e i file della chiave privata del client. Eseguire i seguenti passaggi:

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

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

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

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

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

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

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

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

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

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

      È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave

privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

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

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

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

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

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

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

+

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

+

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

5. Arrestare l'applicazione Web SnapCenter Server in Internet Information Server (IIS) su entrambi i nodi HA.
6. Riavviare il servizio MySQL su entrambi i nodi HA.
7. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config per entrambi i nodi HA.

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato nel file SnapManager.Web.UI.dll.config.

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

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

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

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

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

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

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

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

Configurare l'autenticazione basata su certificato

L'autenticazione basata su certificato aumenta la sicurezza verificando l'identità sia del server SnapCenter che degli host dei plug-in, garantendo comunicazioni sicure e crittografate.

Abilita l'autenticazione basata sul certificato

Per abilitare l'autenticazione basata su certificato per SnapCenter Server e gli host plug-in di Windows, eseguire il seguente cmdlet di PowerShell. Per gli host plug-in Linux, l'autenticazione basata su certificato verrà abilitata quando si abilita l'SSL bidirezionale.

- Per abilitare l'autenticazione basata sul certificato client:

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

- Per disabilitare l'autenticazione basata sul certificato client:

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

Esportare i certificati dell'autorità di certificazione (CA) da SnapCenter Server

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

Prima di iniziare

Dovresti aver configurato l'SSL bidirezionale.

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra Snap-in Certificati, selezionare l'opzione **Account computer**, 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 ottenuto, utilizzato per SnapCenter Server, quindi selezionare **Tutte le attività** > **Esporta** per avviare la procedura guidata di esportazione.
6. Eseguire le seguenti azioni nella procedura guidata.

Per questa opzione…	Procedi come segue…
Esporta chiave privata	Selezionare **No, non esportare la chiave privata**, quindi fare clic su **Avanti**.
Formato file di esportazione	Fare clic su **Avanti**.
Nome del file	Fare clic su **Sfoglia** e specificare il percorso del file in cui salvare il certificato, quindi fare clic su **Avanti**.
Completamento della procedura guidata di esportazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'esportazione.

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

Importa il certificato CA negli host dei plug-in di Windows

Per utilizzare il certificato CA di SnapCenter Server esportato, è necessario importare il certificato correlato negli host del plug-in Windows SnapCenter tramite la console di gestione Microsoft (MMC).

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra Snap-in Certificati, selezionare l'opzione **Account computer**, 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 "Personale", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Eseguire le seguenti azioni nella procedura guidata.

Per questa opzione…	Procedi come segue…
Posizione del negozio	Fare clic su **Avanti**.

Per questa opzione…	Procedi come segue…
File da importare	Selezionare il certificato SnapCenter Server che termina con l'estensione .cer.
Archivio certificati	Fare clic su **Avanti**.
Completamento della procedura guidata di esportazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione.

Importa il certificato CA negli host del plug-in UNIX

Dovresti importare il certificato CA negli host del plug-in UNIX.

Informazioni su questo compito

- È possibile gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmata dalla CA in uso.
- La password per il keystore SPL e per tutte le password alias associate alla chiave privata devono essere le stesse.

Passi

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL. È il valore corrispondente alla chiave `SPL_KEYSTORE_PASS` .
2. Cambia la password del keystore: `$ 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 il keystore: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS in `spl.properties` file.
5. Riavviare il servizio dopo aver modificato la password.

Configurare i certificati radice o intermedi per l'archivio attendibile SPL

È necessario configurare i certificati radice o intermedi su SPL trust-store. Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Passi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc` .
2. Individuare il file `keystore.jks` .
3. Elenca i certificati aggiunti nel keystore: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungi un certificato radice o intermedio: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi su SPL trust-store.

Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL

È necessario configurare la coppia di chiavi firmata dalla CA su SPL trust-store.

Passi

1. Passare alla cartella contenente il keystore dell'SPL `/var/opt/snapcenter/spl/etc` .
2. Individuare il file `keystore.jks` .
3. Elenca i certificati aggiunti nel keystore: `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere il certificato CA con chiave sia privata che pubblica. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Elenca 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 con la password del keystore.

   La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS in `spl.properties` file.

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

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

Esportare i certificati SnapCenter

Dovresti esportare i certificati SnapCenter in formato .pfx.

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, seleziona l'opzione **Il mio account utente**, quindi fai clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati - Utente corrente** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato con il nome descrittivo SnapCenter , quindi selezionare **Tutte le attività** > **Esporta** per avviare la procedura guidata di esportazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Procedi come segue…
Esporta chiave privata	Selezionare l'opzione **Sì, esporta 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 file per il certificato esportato (è necessario utilizzare .pfx), quindi fare clic su **Avanti**.
Completamento della procedura guidata di esportazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'esportazione.

Configurare il certificato CA per l'host Windows

Genera 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 sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene 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 un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.

2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Procedi come segue…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato 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 della procedura guidata di importazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione.

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

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

Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

Passi

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. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale 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: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

Get-ChildItem -Percorso Cert:\LocalMachine\My

b. Copia l'impronta digitale.

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

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

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

Passi

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>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   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"
   ```

   Per 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.

Passi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter .
2. Nel riquadro di navigazione a sinistra, fare clic su **Connessioni**.
3. Espandi il nome del server e **Siti**.

4. Seleziona il sito web SnapCenter su cui desideri installare il certificato SSL.
5. Vai su **Azioni** > **Modifica sito**, fai clic su **Associazioni**.
6. Nella pagina Binding, seleziona **binding per https**.
7. Fare clic su **Modifica**.
8. Dall'elenco a discesa Certificato SSL, seleziona il Certificato SSL importato di recente.
9. Fare clic su **OK**.

Il sito SnapCenter Scheduler (porta predefinita: 8154, HTTPS) è configurato con certificato autofirmato. Questa porta comunica all'interno dell'host del server SnapCenter e non è obbligatorio configurarla con un certificato CA. Tuttavia, se l'ambiente richiede l'utilizzo di un certificato CA, ripetere i passaggi da 5 a 9 utilizzando il sito SnapCenter Scheduler.

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

Assicurarsi che il certificato venga aggiunto utilizzando il seguente percorso: **Console Root > Certificati – Computer locale > Autorità di certificazione radice attendibili > Certificati**.

Abilita i certificati CA per SnapCenter

È necessario configurare i certificati CA e abilitare la convalida dei certificati CA per SnapCenter Server.

Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet Set-SmCertificateSettings.
- È possibile visualizzare lo stato del certificato per SnapCenter Server 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, è possibile fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Passi

1. Nella pagina Impostazioni, vai su **Impostazioni** > **Impostazioni globali** > **Impostazioni certificato CA**.
2. Selezionare **Abilita convalida certificato**.
3. Fare clic su **Applica**.

Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che non è abilitato 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 è stato 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 sono state completate correttamente.

Configurare il certificato CA per l'host Linux

Dopo aver installato SnapCenter Server su Linux, il programma di installazione crea il certificato autofirmato. Se si desidera utilizzare il certificato CA, è necessario configurare i certificati per il proxy inverso nginx, la registrazione degli audit e i servizi SnapCenter .

Configurare il certificato nginx

Passi

1. Vai a */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Aprire **snapcenter.conf** utilizzando vi o un qualsiasi editor di testo.
3. Passare alla sezione server nel file di configurazione.
4. Modificare i percorsi di *ssl_certificate* e *ssl_certificate_key* in modo che puntino al certificato CA.
5. Salvare e chiudere il file.
6. Ricarica nginx: `$nginx -s reload`

Configurare il certificato del registro di controllo

Passi

1. Aprire *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* utilizzando vi o un qualsiasi editor di testo.

   Il valore predefinito di *INSTALL_DIR* è */opt*.

2. Modificare le chiavi **AUDILOG_CERTIFICATE_PATH** e **AUDILOG_CERTIFICATE_PASSWORD** per includere rispettivamente il percorso del certificato CA e la password.

   Per il certificato del registro di controllo è supportato solo il formato *.pfx*.

3. Salvare e chiudere il file.
4. Riavviare il servizio **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

Configurare il certificato dei servizi SnapCenter

Passi

1. Aprire i seguenti file di configurazione utilizzando vi o un qualsiasi editor di testo.
   - *DIR_INSTALL/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config*

     Il valore predefinito di *INSTALL_DIR* è */opt*.

2. Modificare le chiavi **SERVICE_CERTIFICATE_PATH** e **SERVICE_CERTIFICATE_PASSWORD** per includere rispettivamente il percorso del certificato CA e la password.

   Per il certificato dei servizi SnapCenter è supportato solo il formato *.pfx*.

3. Salvare e chiudere i file.
4. Riavviare tutti i servizi.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Configurare e abilitare la comunicazione SSL bidirezionale sull'host Windows

Configurare la comunicazione SSL bidirezionale sull'host Windows

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Windows e i plug-in.

Prima di iniziare

- Dovresti aver generato il file CSR del certificato CA con la lunghezza minima supportata della chiave pari a 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- Dovresti avere un certificato CA con chiave privata e dettagli dell'impronta digitale.
- Avresti dovuto abilitare la configurazione SSL unidirezionale.

  Per maggiori dettagli, vedere "Configurare la sezione del certificato CA."

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

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

Passi

1. Per associare la porta, eseguire i seguenti passaggi sull'host del server SnapCenter per la porta 8146 (predefinita) del server Web SnapCenter IIS e ancora una volta per la porta 8145 (predefinita) di SMCore utilizzando i comandi di PowerShell.

   a. Rimuovere l'associazione 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>
      ```

      Per 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 ottenuto 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>
```

Per 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 i passaggi seguenti per accedere al certificato CA appena ottenuto.
   a. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
   b. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
   c. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
   d. Fare clic su **Console Root** > **Certificati – Computer locale** > **Personale** > **Certificati**.
   e. Selezionare il certificato SnapCenter .
   f. Per avviare la procedura guidata Aggiungi utente/autorizzazione, 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 del computer locale (il più in alto nella gerarchia)
   h. Aggiungere l'utente IIS AppPool\ SnapCenter e concedere autorizzazioni di controllo complete.
3. Per **l'autorizzazione IIS del certificato CA**, aggiungere la nuova voce delle chiavi di registro DWORD in SnapCenter Server dal seguente percorso:

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

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

4. Crea una nuova voce di chiave di registro DWORD nel contesto della configurazione del registro SCHANNEL.

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

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

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

Prima di iniziare

Assicurarsi che l'impronta digitale del certificato CA sia disponibile.

Passi

1. Per associare la porta, eseguire le seguenti azioni sull'host plug-in Windows per la porta SMCore 8145 (predefinita).

   a. Rimuovere l'associazione della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

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

   Per esempio,

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

   b. Associare il certificato CA appena ottenuto 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>
   ```

   Per 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
```

Abilita la comunicazione SSL bidirezionale sull'host Windows

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Windows e i plug-in utilizzando i comandi di PowerShell.

Prima di iniziare

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

Passi

1. Per abilitare 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
```

Disabilita la comunicazione SSL bidirezionale

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

Informazioni su questo compito

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

Passi

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi su SnapCenter Server per tutti gli host del plug-in e per 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 e abilitare la comunicazione SSL bidirezionale sull'host Linux

Configurare la comunicazione SSL bidirezionale sull'host Linux

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Linux e i plug-in.

Prima di iniziare

- Dovresti aver configurato il certificato CA per l'host Linux.
- È necessario abilitare la comunicazione SSL bidirezionale su tutti gli host del plug-in e sul server SnapCenter .

Passi

1. Copia **certificate.pem** in */etc/pki/ca-trust/source/anchors/*.
2. Aggiungi i certificati all'elenco di attendibilità del tuo host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Verificare se i certificati sono stati aggiunti all'elenco di attendibilità. `trust list | grep "<CN of your certificate>"`
4. Aggiornare **ssl_certificate** e **ssl_certificate_key** nel file **nginx** SnapCenter e riavviare.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Aggiorna il collegamento all'interfaccia utente grafica di SnapCenter Server.
6. Aggiornare i valori delle seguenti chiavi in * SnapManager.Web.UI.dll.config* situato in _ /<percorso di installazione>/ NetApp/snapcenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** situato in */<percorso di installazione>/ NetApp/snapcenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<percorso del certificato.pfx>" />
   - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>
7. Riavviare i seguenti servizi.
   - `systemctl restart smcore.service`

- `systemctl restart snapmanagerweb.service`

8. Verificare che il certificato sia collegato alla porta web SnapManager . `openssl s_client -connect localhost:8146 -brief`
9. Verificare che il certificato sia collegato alla porta smcore. `openssl s_client -connect localhost:8145 -brief`
10. Gestisci la password per l'archivio chiavi e l'alias SPL.
    a. Recupera la password predefinita del keystore SPL assegnata alla chiave **SPL_KEYSTORE_PASS** nel file delle proprietà SPL.
    b. Cambia la password del keystore. `keytool -storepasswd -keystore keystore.jks`
    c. Cambia la password per tutti gli alias delle voci della chiave privata. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Aggiornare la stessa password per la chiave **SPL_KEYSTORE_PASS** in *spl.properties*.
    e. Riavviare il servizio.
11. Sull'host Linux del plug-in, aggiungere i certificati radice e intermedi nel keystore del plug-in SPL.
    - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
    - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
      i. Controllare le voci in keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
      ii. Se necessario, rinominare qualsiasi alias. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Aggiornare il valore di **SPL_CERTIFICATE_ALIAS** nel file *spl.properties* con l'alias di **certificate.pfx** memorizzato in *keystore.jks* e riavviare il servizio SPL: `systemctl restart spl`
13. Verificare che il certificato sia collegato alla porta smcore. `openssl s_client -connect localhost:8145 -brief`

Abilita la comunicazione SSL sull'host Linux

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Linux e i plug-in utilizzando i comandi di PowerShell.

Fare un passo

1. Per abilitare la comunicazione SSL unidirezionale, procedere come segue.
    a. Accedi all'interfaccia grafica utente SnapCenter .
    b. Fare clic su **Impostazioni** > **Impostazioni globali** e selezionare **Abilita convalida certificato su SnapCenter Server**.
    c. Fare clic su **Host** > **Host gestiti** e selezionare l'host del plug-in per il quale si desidera abilitare SSL unidirezionale.

d. Clic icona, quindi fare clic su **Abilita convalida certificato**.

2. Abilita la comunicazione SSL bidirezionale dall'host Linux di SnapCenter Server.
   - `Open-SmConnection`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
   - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
   - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

Configurare Active Directory, LDAP e LDAPS

Registra domini Active Directory non attendibili

È necessario registrare Active Directory con SnapCenter Server per gestire host, utenti e gruppi da 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.
- Dovresti aver abilitato la comunicazione bidirezionale tra gli host del plug-in e il server SnapCenter .
- La risoluzione DNS deve essere impostata dal server SnapCenter agli host del plug-in e viceversa.

Protocollo LDAP

- Il nome di dominio completo (FQDN) dovrebbe essere risolvibile da SnapCenter Server.

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

Protocollo LDAPS

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

  "Configurare il certificato client CA per LDAPS"

- I nomi host del controller di dominio (DCHostName) devono essere raggiungibili da SnapCenter Server.

Informazioni su questo compito

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

Passi

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

2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Impostazioni globali, fare clic su **Impostazioni dominio**.
4. Clic + per registrare un nuovo dominio.
5. Nella pagina Registra nuovo dominio, seleziona **LDAP** o **LDAPS**.
   a. Se si seleziona **LDAP**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAP:

Per questo campo…	Fai questo…
Nome di dominio	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare il nome di dominio completo (FQDN) e fare clic su **Risolvi**.
Indirizzi IP del controller di dominio	Se il nome di dominio completo (FQDN) 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 selezioni **LDAPS**, specifica le informazioni necessarie per registrare il dominio non attendibile per LDAPS:

Per questo campo…	Fai questo…
Nome di dominio	Specificare il nome NetBIOS per il dominio.
FQDN del dominio	Specificare il nome di dominio completo (FQDN).
Nomi dei controller di dominio	Specificare uno o più nomi di controller di dominio e fare clic su **Risolvi**.
Indirizzi IP del controller di dominio	Se i nomi dei controller di dominio non sono risolvibili da SnapCenter Server, è necessario correggere le risoluzioni DNS.

6. Fare clic su **OK**.

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 Application Pool personalizzato quando è necessario abilitare le autorizzazioni di lettura di Active Directory per SnapCenter.

Passi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter .
2. Nel riquadro di navigazione a sinistra, fare clic su **Pool di applicazioni**.
3. Selezionare SnapCenter nell'elenco Pool di applicazioni, quindi fare clic su **Impostazioni avanzate** nel riquadro Azioni.
4. Selezionare Identità, quindi fare clic su **…** per modificare l'identità del pool di applicazioni SnapCenter .
5. Nel campo Account personalizzato, immettere il nome di un account utente di dominio o di un amministratore di dominio con autorizzazione di lettura di Active Directory.
6. Fare clic su OK.

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

Configurare il certificato client CA per LDAPS

È necessario configurare il certificato client CA per LDAPS sul server SnapCenter quando Windows Active Directory LDAPS è configurato con i certificati CA.

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Procedi come segue…
Nella seconda pagina della procedura guidata	Fare clic su **Sfoglia**, selezionare il *Certificato radice* e fare clic su **Avanti**.
Completamento della procedura guidata di importazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione.

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

Informazioni sul copyright

Informazioni sul marchio commerciale