Installieren und Konfigurieren von SnapCenter Server

SnapCenter software

NetApp
January 09, 2026

Inhalt

Installieren und Konfigurieren von SnapCenter Server

Bereiten Sie sich auf die Installation des SnapCenter-Servers vor

Voraussetzungen für die Installation des SnapCenter-Servers

Bevor Sie SnapCenter Server entweder auf Windows- oder Linux-Hosts installieren, sollten Sie überprüfen und sicherstellen, dass alle Anforderungen für Ihre Umgebung erfüllt sind.

Domänen- und Arbeitsgruppenanforderungen für Windows-Host

Der SnapCenter-Server kann auf einem Windows-Host installiert werden, der sich entweder in einer Domäne oder in einer Arbeitsgruppe befindet.

Der Benutzer mit Admin-Privileges darf den SnapCenter-Server installieren.

- Active Directory-Domäne: Sie müssen einen Domain-Benutzer mit lokalen Administratorrechten verwenden. Der Domänenbenutzer muss Mitglied der lokalen Administratorgruppe auf dem Windows-Host sein.
- Arbeitsgruppen: Sie müssen ein lokales Konto mit lokalen Administratorrechten verwenden.

Obwohl Domänen-Trusts, Multi-Domain-Wälder und domänenübergreifende Trusts unterstützt werden, werden forstübergreifende Domänen nicht unterstützt. Die Microsoft-Dokumentation zu Active Directory-Domänen und Trusts enthält weitere Informationen.

> Nach der Installation des SnapCenter-Servers sollten Sie nicht die Domäne ändern, in der sich der SnapCenter-Host befindet. Wenn Sie den SnapCenter-Server-Host aus der Domäne entfernen, in der sich der SnapCenter-Server installiert hatte, und dann versuchen Sie, SnapCenter-Server zu deinstallieren, schlägt der Deinstallationsvorgang fehl.

Platz- und Größenanforderungen

Sie sollten mit den Platz- und Größenanforderungen vertraut sein.

Element	Windows-Host-Anforderungen	Anforderungen an Linux-Hosts
Betriebssysteme	Microsoft Windows Es werden nur englische, deutsche, japanische und vereinfachte chinesische Versionen der Betriebssysteme unterstützt. Die aktuellsten Informationen zu den unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool"Die	• Red hat Enterprise Linux (RHEL) 8 und 9 • SUSE Linux Enterprise Server (SLES) 15 Die aktuellsten Informationen zu den unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool"Die
Minimale CPU-Anzahl	4 Kerne	4 Kerne
Mind. RAM	8 GB Der MySQL Server Pufferpool nutzt 20 Prozent des gesamten RAM.	8 GB
Minimaler Festplattenspeicher für die SnapCenter-Serversoftware und Protokolle	7 GB Wenn sich das SnapCenter-Repository auf demselben Laufwerk befindet, auf dem SnapCenter-Server installiert ist, wird empfohlen, 15 GB zu verwenden.	15 GB
Minimaler Festplattenspeicher für das SnapCenter-Repository	8 GB HINWEIS: Wenn der SnapCenter-Server auf demselben Laufwerk installiert ist, auf dem das SnapCenter-Repository installiert ist, wird empfohlen, 15 GB zu verwenden.	Keine Angabe

Element	Windows-Host-Anforderungen	Anforderungen an Linux-Hosts
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting Bundle • PowerShell 7.4.2 oder höher Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".	• .NET Framework 8.0.12 (und alle nachfolgenden 8.0.x-Patches) • PowerShell 7.4.2 oder höher • Nginx ist ein Webserver, der als Reverse Proxy verwendet werden kann • PAM-Entwicklung PAM (Pluggable Authentication Modules) ist ein Systemsicherheitstool, mit dem Systemadministratoren Authentifizierungsrichtlinien festlegen können, ohne Programme neu kompilieren zu müssen, die die Authentifizierung durchführen.

ASP.NET Core benötigt IIS_IUSRS für den Zugriff auf das temporäre Dateisystem im SnapCenter-Server unter Windows.

SAN-Host-Anforderungen

SnapCenter umfasst keine Host Utilities oder DSM. Wenn der SnapCenter-Host Teil einer SAN-Umgebung (FC/iSCSI) ist, müssen Sie möglicherweise zusätzliche Software auf dem SnapCenter-Server-Host installieren und konfigurieren.

- Host Utilities: Die Host Utilities unterstützen FC und iSCSI. Sie können MPIO auf Ihren Windows Servern verwenden. "Weitere Informationen".
- Microsoft DSM für Windows MPIO: Diese Software arbeitet mit Windows MPIO-Treibern zusammen, um mehrere Pfade zwischen NetApp- und Windows-Hostcomputern zu verwalten. DSM ist für Hochverfügbarkeitskonfigurationen erforderlich.

Wenn Sie ONTAP DSM verwenden, sollten Sie zu Microsoft DSM migrieren. Weitere Informationen finden Sie unter "So migrieren Sie von ONTAP DSM zu Microsoft DSM".

Browser-Anforderungen

SnapCenter Software unterstützt Chrome 125 und höher und Microsoft Edge 110.0.1587.17 und höher.

Port-Anforderungen

Die SnapCenter-Software erfordert verschiedene Ports für die Kommunikation zwischen verschiedenen Komponenten.

- Anwendungen können einen Port nicht gemeinsam nutzen.

- Bei anpassbaren Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.
- Für feste Ports sollten Sie die Standard-Port-Nummer akzeptieren.
- Firewalls
  - Firewalls, Proxys oder andere Netzwerkgeräte sollten keine Verbindung stören.
  - Wenn Sie bei der Installation von SnapCenter einen benutzerdefinierten Port angeben, sollten Sie auf dem Plug-in-Host eine Firewall-Regel für diesen Port für den SnapCenter-Plug-in-Loader hinzufügen.

In der folgenden Tabelle werden die verschiedenen Ports und ihre Standardwerte aufgeführt.

Port-Name	Port-Nummern	Protokoll	Richtung	Beschreibung
SnapCenter -Webport	8146	HTTPS	Bidirektional	Dieser Port wird für die Kommunikation zwischen dem SnapCenter-Client (dem SnapCenter-Benutzer) und dem SnapCenter-Server verwendet und wird auch für die Kommunikation zwischen den Plug-in-Hosts und dem SnapCenter-Server verwendet. Sie können die Portnummer anpassen.
SnapCenter SMCore-Kommunikations-Port	8145	HTTPS	Bidirektional	Dieser Port wird für die Kommunikation zwischen dem SnapCenter-Server und den Hosts verwendet, auf denen die SnapCenter-Plug-ins installiert sind. Sie können die Portnummer anpassen.

Port-Name	Port-Nummern	Protokoll	Richtung	Beschreibung
Scheduler-Service-Port	8154	HTTPS		Über diesen Port werden die SnapCenter-Scheduler-Workflows für alle gemanagten Plug-ins im SnapCenter Server Host zentral orchestriert. Sie können die Portnummer anpassen.
RabbitMQ-Anschluss	5672	TCP		Dies ist der Standardport, den RabbitMQ abhört und der für die Kommunikation zwischen dem Scheduler-Dienst und dem SnapCenter zwischen dem Publisher-Subscriber-Modell verwendet wird.
MySQL-Anschluss	3306	HTTPS		Der Port wird für die Kommunikation mit der SnapCenter-Repository-Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter-Server zum MySQL-Server erstellen. "Weitere Informationen ."

Port-Name	Port-Nummern	Protokoll	Richtung	Beschreibung
Windows Plug-in-Hosts	135, 445	TCP		Dieser Port wird für die Kommunikation zwischen dem SnapCenter-Server und dem Host verwendet, auf dem das Plug-in installiert wird. Der von Microsoft angegebene zusätzliche dynamische Portbereich sollte ebenfalls offen sein.
Linux- oder AIX-Plug-in-Hosts	22	SSH	Unidirektional	Dieser Port wird für die Kommunikation zwischen dem SnapCenter-Server und dem Host verwendet, der vom Server zum Client-Host initiiert wird.
SnapCenter Plug-ins-Paket für Windows, Linux oder AIX	8145	HTTPS	Bidirektional	Dieser Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-ins-Paket installiert ist. Anpassbar. Sie können die Portnummer anpassen.
SnapCenter Plug-in für Oracle Database	27216			Der Standard-JDBC-Port wird vom Plug-in für Oracle für die Verbindung mit der Oracle-Datenbank verwendet.

Port-Name	Port-Nummern	Protokoll	Richtung	Beschreibung
SnapCenter Plug-in für Exchange Datenbank	909			Das Standard-NET. Der TCP-Port wird vom Plug-in für Windows für die Verbindung mit Exchange VSS-Rückrufen verwendet.
Von NetApp unterstützte Plug-ins für SnapCenter	9090	HTTPS		Dies ist ein interner Port, der nur auf dem Plug-In-Host verwendet wird; es ist keine Firewall-Ausnahme erforderlich. Die Kommunikation zwischen dem SnapCenter-Server und den Plug-Ins wird über Port 8145 geleitet.
ONTAP-Cluster oder SVM-Kommunikations-Port	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirektional	Der Port wird von der SAL (Storage Abstraction Layer) für die Kommunikation zwischen dem Host verwendet, auf dem SnapCenter-Server und SVM ausgeführt wird. Der Port wird zur Kommunikation zwischen dem SnapCenter Plug-in-Host und der SVM derzeit auch von der SAL on SnapCenter für Windows Plug-in-Hosts verwendet.

Port-Name	Port-Nummern	Protokoll	Richtung	Beschreibung
SnapCenter-Plug-in für SAP HANA Database	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirektional	Bei einem einzelnen Mandanten mit mandantenfähigen Datenbank-Containern (MDC) endet die Port-Nummer mit 13. Für einen nicht-MDC-Server endet die Port-Nummer mit 15. Sie können die Portnummer anpassen.
SnapCenter Plug-in für PostgreSQL	5432			Dieser Port ist der Standard-PostgreSQL-Port, der für die Kommunikation des Plug-ins für PostgreSQL mit dem PostgreSQL-Cluster verwendet wird. Sie können die Portnummer anpassen.

Registrieren Sie sich, um auf die SnapCenter Software zuzugreifen

Sie sollten sich registrieren, um auf die SnapCenter Software zuzugreifen, wenn Sie zum ersten mal Amazon FSX for NetApp ONTAP oder Azure NetApp Files kennen und noch kein NetApp-Konto besitzen.

Bevor Sie beginnen

- Sie sollten Zugriff auf die Unternehmens-E-Mail-ID haben.
- Wenn Sie Azure NetApp Files verwenden, sollten Sie über die Azure-Abonnement-ID verfügen.
- Wenn Sie Amazon FSX für NetApp ONTAP verwenden, sollten Sie die Dateisystem-ID Ihres FSX für ONTAP-Dateisystems haben.

Über diese Aufgabe

Ihre Registrierung unterliegt der Informationsvalidierung und kann bis zu einem Tag dauern, bis Sie ein neues Konto auf der NetApp Support-Website (NSS) bestätigen und upgraden können, um vom **Guest**-Zugang **vollen** Zugriff zu erhalten.

Schritte

1. Klicken Sie hier, https://mysupport.netapp.com/site/user/registration um sich zu registrieren.
2. Geben Sie Ihre Unternehmens-E-Mail-ID ein, füllen Sie das Captcha aus, akzeptieren Sie die Datenschutzerklärung von NetApp und klicken Sie auf **Senden**.
3. Authentifizieren Sie die Registrierung, indem Sie das an Ihre E-Mail-ID gesendete OTP eingeben und auf **Weiter** klicken.
4. Geben Sie auf der Seite zum Abschluss der Registrierung die folgenden Details ein, um die Registrierung abzuschließen.
   a. Wählen Sie **NetApp-Kunde/Endbenutzer** aus.
   b. Geben Sie im Feld SERIENNUMMER entweder die Azure-Abonnement-ID ein, wenn Sie Azure NetApp Files verwenden, oder die Dateisystemkennung, wenn Sie Amazon FSX für NetApp ONTAP verwenden.

Sie können ein Ticket https://mysupport.netapp.com/site/help erstellen, wenn Sie während der Registrierung Probleme haben oder den Status kennen.

Multi-Faktor-Authentifizierung (MFA)

Multi-Faktor-Authentifizierung (MFA) managen

Sie können die Multi-Faktor-Authentifizierung (MFA)-Funktion im Active Directory-Verbunddienst (AD FS) und im SnapCenter-Server verwalten.

Multi-Faktor-Authentifizierung (MFA) aktivieren

Sie können die MFA-Funktionalität für SnapCenter-Server mithilfe von PowerShell-Befehlen aktivieren.

Über diese Aufgabe

- SnapCenter unterstützt SSO-basierte Anmeldungen, wenn andere Applikationen mit demselben AD FS konfiguriert werden. In bestimmten AD FS-Konfigurationen erfordert SnapCenter möglicherweise aus Sicherheitsgründen die Benutzerauthentifizierung in Abhängigkeit von der Persistenz der AD FS-Session.
- Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können und deren Beschreibungen können durch Ausführen abgerufen werden `Get-Help command_name`. Alternativ können Sie auch sehen "SnapCenter Software Cmdlet Referenzhandbuch".

Bevor Sie beginnen

- Der Windows Active Directory Federation Service (AD FS) sollte in der jeweiligen Domäne ausgeführt werden.
- Sie sollten über einen AD FS-unterstützten Multi-Faktor-Authentifizierungsservice wie Azure MFA, Cisco Duo usw. verfügen.
- Der SnapCenter- und AD-FS-Server-Zeitstempel sollte unabhängig von der Zeitzone gleich sein.
- Beschaffung und Konfiguration des autorisierten CA-Zertifikats für den SnapCenter-Server.

  CA-Zertifikat ist aus folgenden Gründen obligatorisch:

  - Stellt sicher, dass die ADFS-F5-Kommunikation nicht unterbrochen wird, da die selbstsignierten Zertifikate auf Knotenebene eindeutig sind.
  - Stellt sicher, dass bei Upgrade, Reparatur oder Disaster Recovery (DR) in einer Standalone- oder Hochverfügbarkeitskonfiguration das selbstsignierte Zertifikat nicht wiederhergestellt wird, wodurch

MFA neu konfiguriert werden kann.

- Stellt IP-FQDN-Auflösungen sicher.

  Informationen zum CA-Zertifikat finden Sie unter "ZertifikatCSR-Datei erstellen".

Schritte

1. Stellen Sie eine Verbindung zum Active Directory Federation Services (AD FS)-Host her.
2. Laden Sie die AD FS Federation-Metadatendatei von herunter "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.XML“.
3. Kopieren Sie die heruntergeladene Datei auf SnapCenter-Server, um die MFA-Funktion zu aktivieren.
4. Melden Sie sich bei SnapCenter Server als SnapCenter-Administrator-Benutzer über PowerShell an.
5. Generieren Sie mithilfe der PowerShell-Sitzung die SnapCenter MFA-Metadatendatei mit dem Cmdlet *New-SmMultifactorAuthenticationMetadata -Path*.

   Der Parameter Path gibt den Pfad an, in dem die MFA-Metadatendatei im SnapCenter-Server-Host gespeichert werden soll.

6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Client-Einheit zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter-Server mithilfe von `Set-SmMultiFactorAuthentication` Cmdlet:
8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit `Get-SmMultiFactorAuthentication` Cmdlet:
9. Gehen Sie zur Microsoft Management Console (MMC), und führen Sie die folgenden Schritte aus:
   a. Klicken Sie Auf **Datei** > **Snapin Hinzufügen/Entfernen**.
   b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
   c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
   d. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
   e. Klicken Sie mit der rechten Maustaste auf das CA-Zertifikat, das an SnapCenter gebunden ist, und wählen Sie dann **Alle Aufgaben** > **Privater Schlüssel verwalten** aus.
   f. Führen Sie auf dem Berechtigungsassistenten die folgenden Schritte aus:
      i. Klicken Sie Auf **Hinzufügen**.
      ii. Klicken Sie auf **Standorte** und wählen Sie den betreffenden Host (oben in der Hierarchie) aus.
      iii. Klicken Sie im Popup-Fenster **Locations** auf **OK**.
      iv. Geben Sie im Feld Objektname ‘IIS_IUSRS’ ein, und klicken Sie auf **Namen überprüfen** und klicken Sie auf **OK**.

      Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.

10. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie mit der rechten Maustaste auf **vertraut auf Partei** > **Vertrauensbeschuss hinzufügen** > **Start**.
    b. Wählen Sie die zweite Option aus, und durchsuchen Sie die SnapCenter MFA-Metadatendatei und klicken Sie auf **Weiter**.

c. Geben Sie einen Anzeigenamen an und klicken Sie auf **Weiter**.

d. Wählen Sie eine Zugangskontrollrichtlinie nach Bedarf aus und klicken Sie auf **Weiter**.

e. Wählen Sie die Einstellungen auf der nächsten Registerkarte standardmäßig aus.

f. Klicken Sie Auf **Fertig Stellen**.

SnapCenter wird jetzt als vertrauensanzeige-Partei mit dem angegebenen Anzeigenamen dargestellt.

11. Wählen Sie den Namen aus, und führen Sie die folgenden Schritte aus:

a. Klicken Sie Auf **Richtlinie Zur Bearbeitung Von Forderungen**.

b. Klicken Sie auf **Regel hinzufügen** und klicken Sie auf **Weiter**.

c. Geben Sie einen Namen für die Antragsregel an.

d. Wählen Sie **Active Directory** als Attributspeicher aus.

e. Wählen Sie das Attribut als **Benutzer-Principal-Name** und den ausgehenden Antragsart als **Name-ID** aus.

f. Klicken Sie Auf **Fertig Stellen**.

12. Führen Sie die folgenden PowerShell-Befehle auf dem ADFS-Server aus.

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

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

13. Führen Sie die folgenden Schritte durch, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.

a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensbesteller und wählen Sie **Eigenschaften**.

b. Stellen Sie sicher, dass die Felder Endpoints, Identifikatoren und Signatur ausgefüllt sind.

14. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Session-Cookies zu löschen, und melden Sie sich erneut an.

Die SnapCenter MFA-Funktion kann auch über REST-APIs aktiviert werden.

Informationen zur Fehlerbehebung finden Sie unter "Gleichzeitige Anmeldeversuche auf mehreren Registerkarten zeigen MFA-Fehler an".

AD FS MFA-Metadaten aktualisieren

Sie sollten die AD FS MFA-Metadaten in SnapCenter aktualisieren, sobald es Änderungen im AD FS-Server gibt, wie z. B. Upgrade, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Laden Sie die AD FS Federation-Metadatendatei von herunter "https://<host FQDN>/FederationMetadaten/2007-06/FederationMetadata.XML“
2. Kopieren Sie die heruntergeladene Datei auf SnapCenter-Server, um die MFA-Konfiguration zu aktualisieren.
3. Aktualisieren Sie die AD FS Metadaten in SnapCenter, indem Sie das folgende Cmdlet ausführen:

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

4. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Session-Cookies zu löschen, und melden Sie sich erneut an.

SnapCenter MFA-Metadaten aktualisieren

Sie sollten die SnapCenter MFA-Metadaten in AD FS immer dann aktualisieren, wenn es Änderungen am ADFS-Server gibt, wie Reparatur, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Treuhandfonds Der Vertrauenlichen Partei** Aus.
   b. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung, die für SnapCenter erstellt wurde, und wählen Sie **Löschen** aus.

      Der benutzerdefinierte Name des Vertrauensverhältnisses wird angezeigt.

   c. Multi-Faktor-Authentifizierung (MFA) aktivieren.

      Siehe "Multi-Faktor-Authentifizierung aktivieren".

2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Session-Cookies zu löschen, und melden Sie sich erneut an.

Multi-Faktor-Authentifizierung (MFA) deaktivieren

Schritte

1. Deaktivieren Sie MFA, und bereinigen Sie die Konfigurationsdateien, die bei der Aktivierung von MFA mithilfe des erstellt wurden `Set-SmMultiFactorAuthentication` Cmdlet:
2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Session-Cookies zu löschen, und melden Sie sich erneut an.

Multi-Faktor-Authentifizierung (MFA) mit Rest-API, PowerShell und SCCLI managen

Die MFA-Anmeldung wird von Browser, REST-API, PowerShell und SCCLI unterstützt. MFA wird durch einen AD FS-Identitätsmanager unterstützt. Sie können MFA aktivieren, MFA deaktivieren und MFA über GUI, REST API, PowerShell und SCCLI konfigurieren.

Richten Sie AD FS als OAuth/OIDC ein

Konfigurieren Sie AD FS mit dem Windows GUI Wizard

1. Navigieren Sie zu **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Navigieren Sie zu **ADFS** > **Anwendungsgruppen**.
   a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
   b. Wählen Sie **Add Application Group** und geben Sie **Application Name** ein.
   c. Wählen Sie **Server-Anwendung**.
   d. Klicken Sie Auf **Weiter**.

3. Kopieren Sie Die Client-Kennung*.

   Dies ist die Client-ID. .. RückrufURL (SnapCenter-Server-URL) in Umleitung URL hinzufügen. .. Klicken Sie Auf **Weiter**.

4. Wählen Sie **gemeinsam genutzten Schlüssel generieren**.

   Kopieren Sie den geheimen Wert. Das ist das Geheimnis des Kunden. .. Klicken Sie Auf **Weiter**.

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.
   a. Klicken Sie auf der Seite **complete** auf **Close**.
6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Application Group** und wählen Sie **Properties**.
7. Wählen Sie aus den Anwendungseigenschaften **Anwendung hinzufügen**.
8. Klicken Sie auf **Anwendung hinzufügen**.

   Wählen Sie Web API und klicken Sie auf **Weiter**.

9. Geben Sie auf der Seite WebAPI konfigurieren die im vorherigen Schritt erstellte SnapCenter-Server-URL und die Clientkennung in den Abschnitt Kennung ein.
   a. Klicken Sie Auf **Hinzufügen**.
   b. Klicken Sie Auf **Weiter**.
10. Wählen Sie auf der Seite **Select Access Control Policy** die Kontrollrichtlinie entsprechend Ihrer Anforderung aus (z. B. „Permit everyone“ und „Require MFA“) und klicken Sie auf **Next**.
11. Auf der Seite **Configure Application permission** wird openid standardmäßig als Bereich ausgewählt, klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

    Klicken Sie auf der Seite **complete** auf **Close**.

13. Klicken Sie auf der Seite **Beispielanwendungseigenschaften** auf **OK**.
14. JWT-Token, das von einem Autorisierungsserver (AD FS) ausgegeben und von der Ressource verwendet werden soll.

    Der „aud“- oder Zielgruppenanspruch dieses Tokens muss mit der Kennung der Ressource oder der Web-API übereinstimmen.

15. Bearbeiten Sie die ausgewählte WebAPI, und überprüfen Sie, ob die RückrufURL (SnapCenter-Server-URL) und die Client-Kennung korrekt hinzugefügt wurden.

    Konfigurieren Sie OpenID Connect so, dass ein Benutzername als Schadensfälle angegeben wird.

16. Öffnen Sie das Tool **AD FS Management** im Menü **Tools** oben rechts im Server Manager.
    a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.
    b. Wählen Sie die Web-API aus und klicken Sie auf **EDIT**.
    c. Wechseln Sie zur Registerkarte „Emissionsumform“
17. Klicken Sie Auf **Regel Hinzufügen**.
    a. Wählen Sie in der Dropdown-Liste „Antragsregel“ die Option **LDAP-Attribute als Schadensfall**

senden aus.

b. Klicken Sie Auf **Weiter**.

18. Geben Sie den Namen **Claim rule** ein.
    a. Wählen Sie **Active Directory** in der Dropdown-Liste Attributspeicher aus.
    b. Wählen Sie **User-Principal-Name** in der Dropdown-Liste **LDAP Attribute** und **UPN** in der Dropdown-Liste O*utgoing Claim Type* aus.
    c. Klicken Sie Auf **Fertig Stellen**.

Erstellen Sie eine Anwendungsgruppe mit PowerShell Befehlen

Sie können die Anwendungsgruppe und die Web-API erstellen und den Umfang und die Ansprüche mit PowerShell Befehlen hinzufügen. Diese Befehle sind im automatisierten Skriptformat verfügbar. Weitere Informationen finden Sie im <link to KB article>.

1. Erstellen Sie die neue Anwendungsgruppe in AD FS mit der folgenden Kombination.

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

   `ClientRoleIdentifier` Name Ihrer Applikationsgruppe

   `redirectURL` Gültige URL für Umleitung nach Autorisierung

2. Erstellen Sie die AD FS Server-Anwendung und generieren Sie den Client-Schlüssel.

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

3. Erstellen Sie die ADFS-Web-API-Anwendung und konfigurieren Sie den Richtliniennamen, den sie verwenden soll.

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

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

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

4. Holen Sie sich die Client-ID und den Client-Schlüssel aus der Ausgabe der folgenden Befehle, da sie nur einmal angezeigt wird.

   ```
   "client_id = $identifier"

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

5. Erteilen Sie der AD FS-Anwendung die allattallatallaims und openid-Berechtigungen.

   ```
   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. Schreiben Sie die Transformer-Regeldatei aus.

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

7. Benennen Sie die Web-API-Anwendung und definieren Sie die zugehörigen Regeln für die Emissionstransformation mithilfe einer externen Datei.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Ablaufdatum des Zugriffstoken aktualisieren

Sie können die Ablaufzeit des Zugriffstoken mit dem PowerShell Befehl aktualisieren.

Über diese Aufgabe

- Ein Zugriffstoken kann nur für eine bestimmte Kombination von Benutzer, Client und Ressource verwendet werden. Zugriffstoken können nicht widerrufen werden und sind bis zu ihrem Ablauf gültig.
- Standardmäßig beträgt die Gültigkeitsdauer eines Zugriffstoken 60 Minuten. Diese minimale Verfallszeit ist ausreichend und skaliert. Sie müssen ausreichend Wert bieten, um fortlaufende geschäftskritische Aufgaben zu vermeiden.

Schritt

Verwenden Sie den folgenden Befehl im AD FS-Server, um die Ablaufzeit des Zugriffstoken für eine Anwendungsgruppe WebAPI zu aktualisieren.

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

Holen Sie sich das Inhabertoken von AD FS

Sie sollten die unten genannten Parameter in jedem REST-Client (wie Postman) ausfüllen und Sie werden aufgefordert, die Benutzeranmeldeinformationen einzugeben. Zusätzlich sollten Sie die zweite-Faktor-Authentifizierung eingeben (etwas, das Sie haben und etwas, das Sie sind), um den Träger-Token zu erhalten.

+ Die Gültigkeit des Inhabertoken kann vom AD FS-Server pro Anwendung konfiguriert werden, und die Standardgültigkeitsdauer beträgt 60 Minuten.

Feld	Wert
Zuteilungsart	Autorisierungscode
Rückruf-URL	Geben Sie die Basis-URL Ihrer Anwendung ein, wenn Sie keine Rückruf-URL haben.
Authentifizs-URL	[adfs-Domain-Name]/adfs/oauth2/Autorisieren
Zugriff auf Token-URL	[adfs-Domain-Name]/adfs/oauth2/Token
Client-ID	Geben Sie die AD FS-Client-ID ein
Kundengeheimnis	Geben Sie den AD FS-Client-Schlüssel ein
Umfang	OpenID
Clientauthentifizierung	Als Basis-AUTH-Kopfzeile senden
Ressource	Fügen Sie auf der Registerkarte **Advance Options** das Ressourcenfeld mit dem gleichen Wert wie die Callback-URL hinzu, das als „aud“-Wert im JWT-Token erscheint.

Konfigurieren Sie MFA in SnapCenter-Server mit PowerShell, SCCLI und REST-API

Sie können MFA in SnapCenter-Server mit PowerShell, SCCLI und REST-API konfigurieren.

SnapCenter MFA CLI-Authentifizierung

In PowerShell und SCCLI wird das vorhandene Cmdlet (Open-SmConnection) um ein weiteres Feld namens "AccessToken" erweitert, um das Trägertoken zur Authentifizierung des Benutzers zu verwenden.

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

Nach Ausführung des oben genannten Cmdlet wird eine Sitzung erstellt, damit der jeweilige Benutzer weitere SnapCenter Cmdlets ausführen kann.

SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Trägertoken im Format *Authorization=Bearer <access token>* im REST-API-Client (wie Postman oder swagger) und geben Sie den Benutzer RoleName in der Kopfzeile an, um eine erfolgreiche Antwort von SnapCenter zu erhalten.

MFA-Rest-API-Workflow

Wenn MFA mit AD FS konfiguriert ist, sollten Sie sich mit einem Zugriffstoken (Träger) authentifizieren, um über eine beliebige Rest-API auf die SnapCenter-Anwendung zuzugreifen.

Über diese Aufgabe

- Sie können jeden REST-Client wie Postman, Swagger UI oder FireCamp verwenden.
- Holen Sie sich ein Zugriffstoken und authentifizieren Sie es für nachfolgende Anfragen (SnapCenter Rest API), um einen Vorgang auszuführen.

Schritte

Zur Authentifizierung über AD FS MFA

1. Konfigurieren Sie den REST-Client so, dass er den AD FS-Endpunkt aufruft, um das Zugriffstoken zu erhalten.

   Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS SSO-Seite weitergeleitet, auf der Sie Ihre AD-Anmeldeinformationen angeben und sich bei MFA authentifizieren müssen. 1. Geben Sie auf der AD FS SSO-Seite Ihren Benutzernamen oder Ihre E-Mail-Adresse in das Textfeld Benutzername ein.

   + Benutzernamen müssen als Benutzer@Domäne oder Domäne\Benutzer formatiert sein.

2. Geben Sie im Textfeld Kennwort Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie im Abschnitt **Anmeldeoptionen** eine Authentifizierungsoption aus und authentifizieren Sie sich (je nach Konfiguration).
   - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
   - QR-Code: Verwenden Sie die mobile App AUTH Point, um den QR-Code zu scannen, und geben Sie dann den in der App angezeigten Verifizierungscode ein
   - Einmalpasswort: Geben Sie das Einmalpasswort für Ihr Token ein.
5. Nach erfolgreicher Authentifizierung wird ein Popup-Fenster geöffnet, das die Token Zugriff, ID und Aktualisieren enthält.

   Kopieren Sie das Zugriffstoken und verwenden Sie es in der SnapCenter-Rest-API, um den Vorgang durchzuführen.

6. In der Rest-API sollten Sie das Zugriffstoken und den Rollennamen in der Kopfzeile übergeben.
7. SnapCenter validiert dieses Zugriffstoken aus AD FS.

   Wenn es sich um ein gültiges Token handelt, dekodiert SnapCenter es und ruft den Benutzernamen ab.

8. Mit dem Benutzernamen und Rollennamen authentifiziert SnapCenter den Benutzer für eine API-Ausführung.

Wenn die Authentifizierung erfolgreich ist, gibt SnapCenter das Ergebnis zurück, sonst wird eine Fehlermeldung angezeigt.

Aktivieren oder Deaktivieren der SnapCenter-MFA-Funktion für Rest-API, CLI und GUI

GUI

Schritte

1. Melden Sie sich beim SnapCenter-Server als SnapCenter-Administrator an.
2. Klicken Sie auf **Einstellungen** > **Globale Einstellungen** > **MultiFactorAuthentication(MFA) Settings**
3. Wählen Sie die Schnittstelle (GUI/RST API/CLI) aus, um die MFA-Anmeldung zu aktivieren oder zu deaktivieren.

PowerShell-Schnittstelle

Schritte

1. Führen Sie die PowerShell- oder CLI-Befehle zur Aktivierung von MFA für GUI, Rest API, PowerShell und SCCLI aus.

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

   Der Pfadparameter gibt den Speicherort der AD FS MFA-Metadaten-XML-Datei an.

   Aktiviert MFA für SnapCenter-GUI, Rest-API, PowerShell und SCCLI, konfiguriert mit angegebenem AD FS-Metadatendateipfad.

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe des `Get-SmMultiFactorAuthentication` Cmdlet:

SCCLI-Schnittstelle

Schritte

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

REST-APIs

1. Führen Sie die folgende Post-API zur Aktivierung von MFA für GUI, Rest-API, PowerShell und SCCLI aus.

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Post

Text Anfordern	{ „IsGuiMFAEnabled“: Falsch, „IsRestApiMFAEnabled“: Wahr, „IsCliMFAEnabled“: False, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“ }
Antwortkörper	{ „MFAConfiguration“: { „IsGuiMFAEnabled“: Falsch, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“, „SCConfigFilePath“: Null, „IsRestApiMFAEnabled“: Wahr, „IsCliMFAEnabled“: False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe der folgenden API.

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Verstehen
Antwortkörper	{ „MFAConfiguration“: { „IsGuiMFAEnabled“: Falsch, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“, „SCConfigFilePath“: Null, „IsRestApiMFAEnabled“: Wahr, „IsCliMFAEnabled“: False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }

Installieren Sie den SnapCenter-Server

Installieren Sie den SnapCenter-Server auf dem Windows-Host

Sie können die ausführbare Datei für das SnapCenter-Server-Installationsprogramm ausführen, um den SnapCenter-Server zu installieren.

Optional können Sie mithilfe von PowerShell Cmdlets mehrere Installations- und Konfigurationsverfahren durchführen. Sie sollten PowerShell 7.4.2 oder höher verwenden.

Die automatische Installation des SnapCenter-Servers über die Befehlszeile wird nicht unterstützt.

Bevor Sie beginnen

- Der SnapCenter-Server-Host muss mit Windows-Updates auf dem neuesten Stand sein, ohne dass das System neu gestartet werden muss.
- Sie sollten sicherstellen, dass MySQL Server nicht auf dem Host installiert ist, auf dem Sie den SnapCenter-Server installieren möchten.
- Sie sollten das Debuggen von Windows-Installateurs aktiviert haben.

  Informationen zur Aktivierung finden Sie auf der Microsoft-Website "Windows Installer-Protokollierung".

Sie sollten den SnapCenter-Server nicht auf einem Host mit Microsoft Exchange Server, Active Directory oder Domain Name Servern installieren.

Schritte

1. Laden Sie das Installationspaket für den SnapCenter Server von herunter "NetApp Support Website".
2. Starten Sie die Installation des SnapCenter-Servers, indem Sie auf die heruntergeladene .exe-Datei doppelklicken.

   Nach Beginn der Installation werden alle Vorabprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Sie können die Warnmeldungen ignorieren und mit der Installation fortfahren. Fehler sollten jedoch behoben werden.

3. Überprüfen Sie die für die SnapCenter Server-Installation erforderlichen vordefinierten Werte, und ändern Sie sie, falls erforderlich.

   Sie müssen das Kennwort für die MySQL Server Repository-Datenbank nicht angeben. Während der Installation des SnapCenter Servers wird das Passwort automatisch generiert.

   Das Sonderzeichen “%” is not supported in the custom path for the repository database. If you include "`%`“ im Pfad schlägt die Installation fehl.

4. Klicken Sie Auf **Jetzt Installieren**.

   Wenn Sie ungültige Werte angegeben haben, werden entsprechende Fehlermeldungen angezeigt. Sie sollten die Werte erneut eingeben und dann die Installation starten.

   Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wird der ausgeführte Schritt abgeschlossen und der Rollback-Vorgang gestartet. Der SnapCenter-Server wird vollständig vom Host entfernt.

   Wenn Sie jedoch **Abbrechen** klicken, wenn die Vorgänge „Neustart des SnapCenter-Servers“ oder „Warten auf Start des SnapCenter-Servers“ ausgeführt werden, wird die Installation ohne Abbrechen des Vorgangs fortgesetzt.

   Protokolldateien werden immer im Ordner %temp% des Admin-Benutzers aufgeführt (älteste zuerst). Wenn Sie die Protokollstandorte umleiten möchten, initiieren Sie die Installation des SnapCenter-Servers über die Eingabeaufforderung, indem Sie Folgendes ausführen:`C:\installer_location\installer_name.exe /log"C:\"`

Während der Installation auf dem Windows-Host aktivierte Funktionen

Das SnapCenter-Serverinstallationsprogramm aktiviert die Windows-Funktionen und -Rollen auf Ihrem Windows-Host während der Installation. Diese könnten für die Fehlerbehebung und Wartung des Hostsystems von Interesse sein.

Kategorie	Merkmal
Web-Server	• Internet Information Services • World Wide Web Services • Allgemeine HTTP-Funktionen ◦ Standarddokument ◦ Verzeichnisbrowsing ◦ HTTP-Fehler ◦ HTTP-Umleitung ◦ Statischer Inhalt ◦ WebDAV-Publishing • Systemzustand und Diagnose ◦ Benutzerdefinierte Protokollierung ◦ HTTP-Protokollierung ◦ Protokollierungs-Tools ◦ Monitor Anfordern ◦ Nachzeichnen • Performance-Funktionen ◦ Statische Inhaltskomprimierung • Sicherheit ◦ IP-Sicherheit ◦ Grundlegende Authentifizierung ◦ Zentralisierte Unterstützung von SSL-Zertifikaten ◦ Authentifizierung Für Die Clientzertifikatzuordnung ◦ Authentifizierung für die IIS-Clientzertifikatzuordnung ◦ IP- und Domänenbeschränkungen ◦ Anforderungsfilterung ◦ URL-Autorisierung ◦ Windows Authentifizierung • Funktionen Zur Applikationsentwicklung ◦ .NET Extensibility 4.5 ◦ Initialisierung Der Applikation ◦ ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting Bundle ◦ Server-Seitige Umfasst ◦ WebSocket-Protokoll Management Tools IIS-Verwaltungskonsole

Kategorie	Merkmal
IIS-Verwaltungsskripte und -Tools	• IIS-Verwaltungsdienst • Web-Management-Tools
.NET Framework 8.0.12 Features	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting Bundle • Windows Communication Foundation (WCF) HTTP Activation45 ◦ TCP-Aktivierung ◦ HTTP-Aktivierung Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".
Windows-Prozess-Aktivierungsdienst	Prozessmodell
Konfigurations-APIs	Alle

Installieren Sie den SnapCenter-Server auf dem Linux-Host

Sie können die ausführbare Datei für das SnapCenter-Server-Installationsprogramm ausführen, um den SnapCenter-Server zu installieren.

Bevor Sie beginnen

- Wenn Sie den SnapCenter-Server unter Verwendung eines nicht-root-Benutzers installieren möchten, der nicht über ausreichende Berechtigungen zum Installieren von SnapCenter verfügt, rufen Sie die sudoers-Prüfsummendatei von der NetApp-Support-Website ab. Sie sollten die entsprechende Prüfsummendatei verwenden, die auf der Linux-Version basiert.
- Wenn das sudo-Paket in SUSE Linux nicht verfügbar ist, installieren Sie das sudo-Paket, um Authentifizierungsfehler zu vermeiden.
- Konfigurieren Sie für SUSE Linux den Hostnamen, um einen Installationsfehler zu vermeiden.
- Überprüfen Sie den sicheren Linux-Status, indem Sie den Befehl ausführen `sestatus`. Wenn der *SELinux Status* „aktiviert“ ist und der *Current Mode* „erzwingt“ ist, führen Sie folgende Schritte aus:
  - Führen Sie den Befehl aus: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    Der Standardwert von *WEBAPP_EXTERNAL_PORT* ist 8146
  - Wenn die Firewall den Port blockiert, führen Sie aus `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    Der Standardwert von *WEBAPP_EXTERNAL_PORT* ist 8146
  - Führen Sie die folgenden Befehle aus dem Verzeichnis aus, in dem Sie Lese- und

Schreibberechtigungen haben:

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

  Wenn der Befehl „nichts zu tun“ zurückgibt, führen Sie den Befehl nach der Installation des SnapCenter-Servers erneut aus.

- Wenn der Befehl *my-nginx.pp* erstellt, führen Sie den Befehl aus, um das Richtlinienpaket zu aktivieren: `sudo semodule -i my-nginx.pp`

◦ Der für das MySQL PID-Verzeichnis verwendete Pfad ist */var/opt/mysqld*. Führen Sie die folgenden Befehle aus, um die Berechtigungen für die MySQL-Installation festzulegen.

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

◦ Der für das MySQL-Datenverzeichnis verwendete Pfad lautet */INSTALL_dir/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Führen Sie die folgenden Befehle aus, um die Berechtigungen für das MySQL-Datenverzeichnis festzulegen.

- `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`

Über diese Aufgabe

- Wenn SnapCenter-Server auf dem Linux-Host installiert ist, werden Dienste von Drittanbietern wie MySQL, RabbitMQ und Errlang installiert. Sie sollten sie nicht deinstallieren.
- Der auf dem Linux-Host installierte SnapCenter-Server unterstützt Folgendes nicht:
  - Hochverfügbarkeit
  - Windows Plug-ins
  - Active Directory (unterstützt nur lokale Benutzer, sowohl Root- als auch nicht-Root-Benutzer mit Creds)
  - Schlüsselbasierte Authentifizierung zur Anmeldung bei SnapCenter
- Während der Installation von . NET Runtime, wenn die Installation die Abhängigkeiten der *libicu*-Bibliothek nicht auflöst, installieren Sie *libicu*, indem Sie den folgenden Befehl ausführen: `yum install -y libicu`
- Wenn die Installation von SnapCenter Server aufgrund der Nichtverfügbarkeit von *Perl* fehlschlägt, installieren Sie *Perl*, indem Sie den Befehl ausführen: `yum install -y perl`

Schritte

1. Laden Sie Folgendes von */Home Directory* herunter "NetApp Support Website" .
   - SnapCenter-Server-Installationspaket - **snapcenter-linux-Server-(el8/el9/sles15).bin**
   - Öffentliche Schlüsseldatei - **snapcenter_public_key.Pub**
   - Entsprechende Signaturdatei - **snapcenter-linux-Server-(el8/el9/sles15).bin.sig**
2. Validieren Sie die Signaturdatei. `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin`

`file>`

3. Für die Installation eines nicht-root-Benutzers fügen Sie den in **snapcenter_Server_checksum_(el8/el9/sles15).txt** angegebenen visudo-Inhalt hinzu, der zusammen mit dem .bin-Installationsprogramm verfügbar ist.
4. Weisen Sie die Ausführungsberechtigung für das .bin-Installationsprogramm zu. `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Führen Sie eine der Aktionen zur Installation des SnapCenter-Servers durch.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Interaktive Installation	`./snapcenter-linux-server-(el8/el9/sles15).bin` Sie werden aufgefordert, die folgenden Details einzugeben: • Der externe Webapp-Port, der für den Zugriff auf SnapCenter-Server außerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8146. • Der SnapCenter-Server-Benutzer, der den SnapCenter-Server installieren wird. • Das Installationsverzeichnis, in dem Pakete installiert werden.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Nicht interaktive Installation	`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>` Beispiel: Sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_dir=/opt -DINSTALL_LOG_NAME=InstallerLog.log Protokolle werden unter */var/opt/snapcenter/logs* gespeichert. Zu übergebene Parameter für die Installation des SnapCenter-Servers: • DWEBAPP_EXTERNAL_PORT: Externer Webapp-PORT, der verwendet wird, um außerhalb des Linux-Hosts auf den SnapCenter-Server zuzugreifen. Der Standardwert ist 8146. • DWEBAPP_INTERNAL_PORT: Interner Webapp-PORT, der für den Zugriff auf den SnapCenter-Server innerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8147. • DSMCORE_PORT: SMCore-Port, auf dem die smcore-Dienste ausgeführt werden. Der Standardwert ist 8145. • DSCHEDULER_PORT: Scheduler-Port, auf dem die Scheduler-Dienste ausgeführt werden. Der Standardwert ist 8154. • DSNAPCENTER_SERVER_USER: SnapCenter-SERVER-Benutzer, der den SnapCenter-Server installieren wird. Bei *DSNAPCENTER_SERVER_USER* ist der Standard der Benutzer, der das Installationsprogramm ausführt. • DUSER_INSTALL_dir: Installationsverzeichnis, in dem Pakete installiert werden. Für *DUSER_INSTALL_dir* lautet das Standardinstallationsverzeichnis */opt*. • DINSTALL_LOG_NAME: NAME der Protokolldatei, in der die Installationsprotokolle gespeichert werden. Dies ist ein optionaler Parameter, und wenn angegeben, werden keine Protokolle auf der Konsole angezeigt. Wenn Sie diesen Parameter nicht angeben, werden

Was kommt als Nächstes?

- Wenn der *SELinux Status* "aktiviert" ist und der *Current Mode* "erzwingt" ist, startet der **nginx**-Dienst nicht. Sie sollten die folgenden Befehle ausführen:
  a. Gehen Sie zum Home Directory.
  b. Führen Sie den Befehl aus: `journalctl -x|grep nginx`.
  c. Wenn der interne Webapp-Port (8147) nicht hören darf, führen Sie die folgenden Befehle aus:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Lauf `setsebool -P httpd_can_network_connect` die

Protokolle auf der Konsole angezeigt und auch in der Standardprotokolldatei gespeichert.

- DSELINUX: Wenn *SELinux Status* "aktiviert" ist, ist der *Current Mode* "Enforcing" und Sie haben die Befehle ausgeführt, die im Abschnitt vor dem Start erwähnt wurden, sollten Sie diesen Parameter angeben und den Wert als 1 zuweisen. Der Standardwert ist 0.
- DUPGRADE: Der Standardwert ist 0. Geben Sie diesen Parameter und seinen Wert als eine ganze Zahl außer 0 an, um den SnapCenter-Server zu aktualisieren.

Funktionen, die während der Installation auf dem Linux-Host aktiviert wurden

Der SnapCenter-Server installiert die folgenden Softwarepakete, die bei der Fehlerbehebung und Wartung des Hostsystems helfen können.

- Rabbitmq
- Erlang

Registrieren Sie SnapCenter

Wenn Sie neue NetApp Produkte nutzen und noch keinen NetApp Account haben, sollten Sie SnapCenter registrieren, um den Support zu aktivieren.

Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld *Info zu SnapCenter* die SnapCenter-Instanz, eine 20-stellige Zahl, die mit 971 beginnt.
3. Klicken Sie Auf https://register.netapp.com.
4. Klicken Sie auf **Ich bin kein registrierter NetApp-Kunde**.
5. Geben Sie Ihre Daten an, um sich zu registrieren.
6. Lassen Sie das Feld NetApp Referenz SN leer.
7. Wählen Sie in der Dropdown-Liste Produktreihe **SnapCenter** aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter-Instanz-ID ein.
10. Klicken Sie Auf **Absenden**.

Melden Sie sich über die RBAC-Autorisierung bei SnapCenter an

SnapCenter unterstützt die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC). Der SnapCenter Administrator weist über die SnapCenter RBAC Rollen und Ressourcen entweder einem Benutzer in der Arbeitsgruppe oder im aktiven Verzeichnis oder Gruppen im aktiven Verzeichnis zu. Der RBAC-Benutzer kann sich nun mit den zugewiesenen Rollen bei SnapCenter anmelden.

Bevor Sie beginnen

- Sie sollten den Windows Process Activation Service (WAR) in Windows Server Manager aktivieren.
- Wenn Sie Internet Explorer als Browser verwenden möchten, um sich beim SnapCenter-Server anzumelden, sollten Sie sicherstellen, dass der geschützte Modus in Internet Explorer deaktiviert ist.
- Wenn SnapCenter-Server auf Linux-Host installiert ist, sollten Sie sich mit dem Benutzerkonto anmelden, das zur Installation des SnapCenter-Servers verwendet wurde.

Über diese Aufgabe

Während der Installation erstellt der Installationsassistent für SnapCenter-Server eine Verknüpfung und legt sie auf dem Desktop und im Startmenü des Hosts ab, auf dem SnapCenter installiert ist. Außerdem zeigt der Installationsassistent am Ende der Installation die SnapCenter-URL basierend auf den Informationen an, die Sie während der Installation angegeben haben. Diese können Sie kopieren, wenn Sie sich von einem Remote-System aus anmelden möchten.

Wenn in Ihrem Webbrowser mehrere Registerkarten geöffnet sind, meldet Sie sich beim Schließen der Registerkarte „SnapCenter-Browser“ nicht von SnapCenter ab. Um Ihre Verbindung mit SnapCenter zu beenden, müssen Sie sich von SnapCenter entweder durch Klicken auf den **Abmelden**-Button oder durch Schließen des gesamten Webbrowsers abmelden.

Best Practice: aus Sicherheitsgründen wird empfohlen, dass Sie Ihren Browser nicht aktivieren, um Ihr SnapCenter-Passwort zu speichern.

Die Standard-GUI-URL ist eine sichere Verbindung zum Standardport 8146 auf dem Server, auf dem der SnapCenter-Server installiert ist (*https://server:8146*). Wenn Sie während der SnapCenter-Installation einen anderen Server-Port bereitgestellt haben, wird dieser Port verwendet.

Für die Implementierung von Hochverfügbarkeit (High Availability, HA) müssen Sie über die virtuelle Cluster-IP *https://Virtual_Cluster_IP_or_FQDN:8146* auf SnapCenter zugreifen können. Wenn Sie die SnapCenter-Benutzeroberfläche nicht sehen, wenn Sie im Internet Explorer (IE) zu *https://Virtual_Cluster_IP_or_FQDN:8146* navigieren, müssen Sie die IP-Adresse des virtuellen Clusters oder den FQDN als vertrauenswürdige Site in IE auf jedem Plug-in-Host hinzufügen, oder Sie müssen die erweiterte Sicherheit des IE auf jedem Plug-in-Host deaktivieren. Weitere Informationen finden Sie unter "Der Zugriff auf die Cluster-IP-Adresse kann nicht vom externen Netzwerk aus erfolgen".

Über die SnapCenter GUI hinaus können Sie mit PowerShell Cmdlets Skripte erstellen, um Konfigurations-, Backup- und Restore-Vorgänge durchzuführen. Einige Cmdlets haben sich möglicherweise bei jeder SnapCenter Version geändert. Das "SnapCenter Software Cmdlet Referenzhandbuch" hat die Details.

Wenn Sie sich zum ersten Mal bei SnapCenter anmelden, müssen Sie sich mit den Anmeldeinformationen anmelden, die Sie während des Installationsvorgangs angegeben haben.

Schritte

1. Starten Sie SnapCenter über die Verknüpfung auf Ihrem lokalen Hostdesktop, über die am Ende der Installation angegebene URL oder über die vom SnapCenter-Administrator bereitgestellte URL.
2. Geben Sie die Anmeldedaten des Benutzers ein.

So geben Sie Folgendes an:	Verwenden Sie eines dieser Formate…
Domain-Administrator	• NetBIOS\Benutzername • Benutzername@UPN-Suffix Beispiel: username@netapp.com • Domain FQDN\Benutzername
Lokaler Administrator	Benutzername

3. Wenn Ihnen mehr als eine Rolle zugewiesen ist, wählen Sie im Feld Rolle die Rolle aus, die Sie für diese Anmeldesitzung verwenden möchten.

   Ihre aktuellen Benutzer und die zugehörige Rolle werden nach der Anmeldung oben rechts von SnapCenter angezeigt.

Ergebnis

Die Seite Dashboard wird angezeigt.

Wenn die Protokollierung fehlschlägt und der Fehler aufgetreten ist, dass die Site nicht erreicht werden kann, sollten Sie das SSL-Zertifikat SnapCenter zuordnen. "Weitere Informationen ."

Nach Ihrer Beendigung

Nachdem Sie sich zum ersten Mal bei SnapCenter Server als RBAC-Benutzer angemeldet haben, aktualisieren Sie die Ressourcenliste.

Wenn Sie nicht vertrauenswürdige Active Directory-Domänen haben, die von SnapCenter unterstützt werden sollen, müssen Sie diese Domänen bei SnapCenter registrieren, bevor Sie die Rollen für die Benutzer in nicht vertrauenswürdigen Domänen konfigurieren. "Weitere Informationen .".

Wenn Sie den Plug-in-Host in SnapCenter unter Linux Host hinzufügen möchten, sollten Sie die Prüfsummendatei vom Speicherort abrufen: */opt/NetApp/snapManagerWeb/Repository*.

Ab Version 6.0 wird eine Verknüpfung für SnapCenter PowerShell auf dem Desktop erstellt. Sie können direkt auf die SnapCenter PowerShell-Cmdlets zugreifen, indem Sie die Verknüpfung verwenden.

Melden Sie sich mit Multi-Faktor-Authentifizierung (MFA) bei SnapCenter an.

SnapCenter Server unterstützt MFA für Domain-Konto, das Teil des Active Directory ist.

Bevor Sie beginnen

Sie sollten MFA aktiviert haben. Informationen zum Aktivieren von MFA finden Sie unter "Multi-Faktor-Authentifizierung aktivieren"

Über diese Aufgabe

- Nur FQDN wird unterstützt
- Workgroup- und domänenübergreifende Benutzer können sich nicht mit MFA anmelden

Schritte

1. Starten Sie SnapCenter über die Verknüpfung auf Ihrem lokalen Hostdesktop, über die am Ende der Installation angegebene URL oder über die vom SnapCenter-Administrator bereitgestellte URL.
2. Geben Sie auf der Anmeldeseite AD FS Benutzernamen und Kennwort ein.

   Wenn die Fehlermeldung „Benutzername“ oder „Kennwort ungültig“ auf der Seite „AD FS“ angezeigt wird, sollten Sie Folgendes überprüfen:

   - Gibt an, ob Benutzername oder Passwort gültig ist

     Das Benutzerkonto sollte im Active Directory (AD) vorhanden sein.

   - Ob Sie die maximal zulässigen Versuche überschritten haben, die in AD festgelegt wurden
   - Gibt an, ob AD und AD FS verfügbar ist und ausgeführt wird

Ändern Sie das Zeitlimit für die SnapCenter-StandardGUI-Sitzung

Sie können den Zeitlimits für die SnapCenter-GUI-Sitzung ändern, damit sie kürzer als oder größer als der Standardzeitraum von 20 Minuten ist.

Als Sicherheitsfunktion warnt Sie SnapCenter nach einer Standardlaufzeit von 15 Minuten Inaktivität, dass Sie in 5 Minuten von der GUI-Sitzung abgemeldet werden. Standardmäßig meldet SnapCenter Sie nach 20 Minuten Inaktivität von der GUI-Sitzung ab, und Sie müssen sich erneut anmelden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen** > **Globale Einstellungen**.
2. Klicken Sie auf der Seite Globale Einstellungen auf **Konfigurationseinstellungen**.
3. Geben Sie im Feld Session-Timeout die neue Sitzungszeitüberschreitung in Minuten ein und klicken Sie dann auf **Speichern**.

Sichern Sie den SnapCenter Webserver durch Deaktivieren von SSL 3.0

Aus Sicherheitsgründen sollten Sie das SSL-3.0-Protokoll (Secure Socket Layer) in Microsoft IIS deaktivieren, wenn es auf Ihrem SnapCenter-Webserver aktiviert ist.

Das SSL 3.0-Protokoll enthält Mängel, mit denen ein Angreifer Verbindungsfehler verursachen kann oder man-in-the-Middle-Angriffe ausführen und den Verschlüsselungsverkehr zwischen Ihrer Website und ihren Besuchern beobachten kann.

Schritte

1. Um den Registrierungs-Editor auf dem SnapCenter-Webserver-Host zu starten, klicken Sie auf **Start** > **Ausführen** und geben dann regedit ein.
2. Navigieren Sie im Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Falls der Server-Schlüssel bereits vorhanden ist:
     i. Wählen Sie das aktivierte DWORD aus, und klicken Sie dann auf **Bearbeiten** > **Ändern**.
     ii. Ändern Sie den Wert auf 0, und klicken Sie dann auf **OK**.

- Wenn der Server-Schlüssel nicht vorhanden ist:
  i. Klicken Sie auf **Bearbeiten** > **Neu** > **Schlüssel** und benennen Sie den Schlüssel Server.
  ii. Wenn der neue Serverschlüssel ausgewählt ist, klicken Sie auf **Bearbeiten** > **Neu** > **DWORD**.
  iii. Benennen Sie die neue DWORD aktiviert, und geben Sie dann 0 als Wert ein.

3. Schließen Sie Den Registrierungs-Editor.

Konfigurieren des SnapCenter-Servers

Hinzufügen und Bereitstellen des Speichersystems

Storage-Systeme hinzufügen

Sie sollten das Storage-System einrichten, das SnapCenter-Zugriff auf ONTAP Storage, ASA r2 Systeme oder Amazon FSX for NetApp ONTAP bietet, um Datensicherungs- und Bereitstellungsvorgänge auszuführen.

Sie können entweder eine eigenständige SVM oder ein Cluster aus mehreren SVMs hinzufügen. Wenn Sie Amazon FSX für NetApp ONTAP verwenden, können Sie entweder FSX Admin LIF aus mehreren SVMs mit fsxadmin-Konto hinzufügen oder FSX SVM in SnapCenter hinzufügen.

Bevor Sie beginnen

- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Über diese Aufgabe

- Wenn Sie Speichersysteme konfigurieren, können Sie auch die Funktionen für das Ereignismanagement (EMS) & AutoSupport aktivieren. Das AutoSupport Tool erfasst Daten zum Systemzustand des Systems und sendet die Daten automatisch an den technischen Support von NetApp. Damit können sie Fehler im System Ihres Systems beheben.

  Wenn Sie diese Funktionen aktivieren, sendet SnapCenter AutoSupport-Informationen an das Storage-System und EMS-Meldungen an das Syslog-System, wenn eine Ressource geschützt ist, eine Wiederherstellung oder ein Klonvorgang erfolgreich abgeschlossen wird oder ein Vorgang ausfällt.

- Wenn Sie planen, Snapshots auf ein SnapMirror Ziel oder ein SnapVault Ziel zu replizieren, müssen Sie Storage-Systemverbindungen für die Ziel-SVM oder das Cluster sowie die Quell-SVM oder das Cluster einrichten.

Wenn Sie das Kennwort des Speichersystems ändern, können geplante Jobs, Backup-Vorgänge bei Bedarf und Wiederherstellungsvorgänge fehlschlagen. Nach dem Ändern des Kennworts des Speichersystems können Sie das Passwort aktualisieren, indem Sie auf der Registerkarte Speicher auf **Ändern** klicken.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Klicken Sie auf der Seite Speichersysteme auf **Neu**.
3. Geben Sie auf der Seite Add Storage System die folgenden Informationen ein:

Für dieses Feld…	Tun Sie das…
Storage-System	Geben Sie den Namen des Storage-Systems oder die IP-Adresse ein. Die Namen des Speichersystems, ohne den Domänennamen zu enthalten, müssen 15 oder weniger Zeichen enthalten und die Namen müssen aufgelöst werden können. Um Verbindungen zu Speichersystemen mit Namen zu erstellen, die mehr als 15 Zeichen enthalten, können Sie das Cmdlet "Add-SmStorageConnectionPowerShell" verwenden. Bei Storage-Systemen mit MetroCluster-Konfiguration (MCC) wird sowohl lokale als auch Peer-Cluster registrieren, um unterbrechungsfreien Betrieb zu gewährleisten. SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss über einen eindeutigen Namen verfügen. Nachdem Sie die Storage-Verbindung zu SnapCenter hinzugefügt haben, sollten Sie die SVM oder den Cluster nicht mithilfe von ONTAP umbenennen. Wenn eine SVM mit einem kurzen Namen oder einem FQDN hinzugefügt wird, muss sie sowohl aus dem SnapCenter als auch dem Plug-in-Host resolable sein.
Benutzername/Passwort	Geben Sie die Anmeldedaten des Speicherbenutzers ein, der über die erforderlichen Berechtigungen für den Zugriff auf das Speichersystem verfügt.

Für dieses Feld…	Tun Sie das…
Einstellungen für Ereignismanagement-System (EMS) und AutoSupport	Wenn Sie EMS-Meldungen an das Syslog-Speichersystem senden möchten oder wenn Sie AutoSupport-Meldungen für den angewendeten Schutz, abgeschlossene Wiederherstellungsvorgänge oder fehlgeschlagene Vorgänge an das Speichersystem senden möchten, aktivieren Sie das entsprechende Kontrollkästchen. Wenn Sie das Kontrollkästchen **AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden** aktivieren, ist das Kontrollkästchen * SnapCenter-Ereignisse in syslog* aktiviert, da EMS-Nachrichten zur Aktivierung von AutoSupport-Benachrichtigungen erforderlich sind.

4. Klicken Sie auf **Mehr Optionen**, wenn Sie die Standardwerte ändern möchten, die Plattform, Protokoll, Port und Timeout zugewiesen sind.

   a. Wählen Sie unter Plattform eine der Optionen aus der Dropdown-Liste aus.

      Wenn die SVM das sekundäre Storage-System in einer Backup-Beziehung ist, aktivieren Sie das Kontrollkästchen **sekundär**. Wenn die Option **Sekundär** ausgewählt ist, führt SnapCenter keine Lizenzprüfung sofort durch.

   Wenn Sie eine SVM in SnapCenter hinzugefügt haben, muss der Benutzer den Plattformtyp manuell aus der Dropdown-Liste auswählen.

   a. Wählen Sie im Protokoll das Protokoll aus, das während der SVM- oder Cluster-Einrichtung, normalerweise HTTPS, konfiguriert wurde.
   b. Geben Sie den Port ein, den das Speichersystem akzeptiert.

      Der Standardport 443 funktioniert in der Regel.

   c. Geben Sie die Zeit in Sekunden ein, die verstreichen soll, bevor die Kommunikationsversuche angehalten werden.

      Der Standardwert ist 60 Sekunden.

   d. Wenn die SVM über mehrere Managementschnittstellen verfügt, aktivieren Sie das Kontrollkästchen **bevorzugte IP** und geben Sie dann die bevorzugte IP-Adresse für SVM-Verbindungen ein.
   e. Klicken Sie Auf **Speichern**.
5. Klicken Sie Auf **Absenden**.

Ergebnis

Führen Sie auf der Seite Storage Systems aus dem Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

- Wählen Sie **ONTAP SVMs** aus, wenn Sie alle hinzugefügten SVMs anzeigen möchten.

  Falls Sie FSX SVMs hinzugefügt haben, finden Sie hier die FSX SVMs.

- Wählen Sie **ONTAP Cluster** aus, wenn Sie alle hinzugefügten Cluster anzeigen möchten.

  Wenn Sie FSX-Cluster mit fsxadmin hinzugefügt haben, werden die FSX-Cluster hier aufgelistet.

  Wenn Sie auf den Cluster-Namen klicken, werden im Abschnitt Storage Virtual Machines alle SVMs, die Teil des Clusters sind, angezeigt.

  Wenn dem ONTAP Cluster über die ONTAP-Benutzeroberfläche eine neue SVM hinzugefügt wird, klicken Sie auf **Neu entdecken**, um die neu hinzugefügte SVM anzuzeigen.

Nach Ihrer Beendigung

Ein Cluster-Administrator muss AutoSupport auf jedem Node des Storage-Systems aktivieren, um E-Mail-Benachrichtigungen von allen Storage-Systemen zu senden, auf die SnapCenter Zugriff hat, indem der folgende Befehl über die Befehlszeile des Storage-Systems ausgeführt wird:

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

Der SVM-Administrator hat keinen Zugriff auf AutoSupport.

Storage-Verbindungen und Anmeldedaten

Vor Durchführung von Datensicherungsvorgängen sollten Sie die Speicherverbindungen einrichten und die Zugangsdaten hinzufügen, die der SnapCenter-Server und die SnapCenter-Plug-ins verwenden werden.

Speicherverbindungen

Über die Speicherverbindungen können SnapCenter-Server und SnapCenter-Plug-ins auf den ONTAP-Speicher zugreifen. Zum Einrichten dieser Verbindungen gehört auch die Konfiguration von Funktionen für das AutoSupport- und Ereignismanagement-System (EMS).

Anmeldedaten

- Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

  Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind:

  - *NetBIOS\Benutzername*
  - *Domain FQDN\Benutzername*
  - *Benutzername@upn*
- Lokaler Administrator (nur für Arbeitsgruppen)

  Geben Sie bei Systemen, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist.

  Das zulässige Format für das Feld Benutzername lautet: *Username*

- Anmeldedaten für einzelne Ressourcengruppen

  Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Bereitstellen von Storage auf Windows Hosts

Erstellen und Verwalten von Initiatorgruppen

Sie erstellen Initiatorgruppen, um anzugeben, welche Hosts auf eine bestimmte LUN im Storage-System zugreifen können. Sie können SnapCenter eine Initiatorgruppe auf einem Windows Host erstellen, umbenennen, ändern oder löschen.

Erstellen einer Initiatorgruppe

Sie können SnapCenter zum Erstellen einer Initiatorgruppe auf einem Windows Host verwenden. Die Initiatorgruppe ist im Assistenten „Festplatte erstellen“ oder „Festplatte verbinden“ verfügbar, wenn Sie eine LUN zuordnen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iGroup**.
3. Klicken Sie auf der Seite Initiatorgruppen auf **Neu**.
4. Definieren Sie im Dialogfeld Initiatorgruppe erstellen die Initiatorgruppe:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus, die Sie der Initiatorgruppe zuordnen möchten.
Host	Wählen Sie den Host aus, auf dem Sie die Initiatorgruppe erstellen möchten.
Initiatorgruppe	Geben Sie den Namen der Initiatorgruppe ein.
Initiatoren	Wählen Sie den Initiator aus.
Typ	Wählen Sie den Initiatortyp, die iSCSI, FCP oder die Kombination aus (FCP und iSCSI) aus.

5. Wenn Sie mit Ihren Einträgen zufrieden sind, klicken Sie auf **OK**.

   SnapCenter erstellt die Initiatorgruppe auf dem Storage-System.

Benennen Sie eine Initiatorgruppe um

Sie können eine vorhandene Initiatorgruppe mit SnapCenter umbenennen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iGroup**.
3. Klicken Sie auf der Seite Initiatorgruppen im Feld **Storage Virtual Machine** auf, um eine Liste der verfügbaren SVMs anzuzeigen, und wählen Sie dann die SVM für die Initiatorgruppe aus, die Sie umbenennen möchten.
4. Wählen Sie in der Liste der Initiatorgruppen für die SVM die Initiatorgruppe aus, die Sie umbenennen möchten, und klicken Sie auf **Umbenennen**.
5. Geben Sie im Dialogfeld Initiatorgruppe umbenennen den neuen Namen für die Initiatorgruppe ein und klicken Sie auf **Umbenennen**.

Ändern einer Initiatorgruppe

Sie können mit SnapCenter Initiatoren zu einer vorhandenen Initiatorgruppe hinzufügen. Beim Erstellen einer Initiatorgruppe können Sie nur einen Host hinzufügen. Wenn Sie eine Initiatorgruppe für ein Cluster erstellen möchten, können Sie die Initiatorgruppe ändern, um dieser Initiatorgruppe weitere Nodes hinzuzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iGroup**.
3. Klicken Sie auf der Seite Initiatorgruppen im Feld **Storage Virtual Machine** auf, um eine Dropdown-Liste der verfügbaren SVMs anzuzeigen. Wählen Sie dann die SVM für die Initiatorgruppe aus, die Sie ändern möchten.
4. Wählen Sie in der Liste der Initiatorgruppen eine Initiatorgruppe aus und klicken Sie auf **Initiator zur Initiatorgruppe hinzufügen**.
5. Wählen Sie einen Host aus.
6. Wählen Sie die Initiatoren aus und klicken Sie auf **OK**.

Löschen einer Initiatorgruppe

Sie können eine Initiatorgruppe mit SnapCenter löschen, wenn Sie sie nicht mehr benötigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iGroup**.
3. Klicken Sie auf der Seite Initiatorgruppen im Feld **Storage Virtual Machine** auf, um eine Dropdown-Liste der verfügbaren SVMs anzuzeigen. Wählen Sie dann die SVM für die Initiatorgruppe aus, die Sie löschen möchten.
4. Wählen Sie in der Liste der Initiatorgruppen für die SVM die Initiatorgruppe aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
5. Klicken Sie im Dialogfeld Initiatorgruppe löschen auf **OK**.

   SnapCenter löscht die Initiatorgruppe.

Der Windows-Host sieht LUNs auf Ihrem Storage-System als virtuelle Festplatten. Sie können SnapCenter verwenden, um eine FC-verbundene oder iSCSI-verbundene LUN zu erstellen und zu konfigurieren.

- SnapCenter unterstützt nur grundlegende Festplatten. Die dynamischen Festplatten werden nicht unterstützt.
- Für GPT ist nur eine Datenpartition und für MBR eine primäre Partition zulässig, die ein Volume mit NTFS oder CSVFS formatiert hat und einen Bereitstellungspfad hat.
- Unterstützte Partitionsstile: GPT, MBR; in einer VMware UEFI VM werden nur iSCSI-Laufwerke unterstützt

SnapCenter unterstützt das Umbenennen einer Festplatte nicht. Wenn eine von SnapCenter gemanagte Festplatte umbenannt wird, ist der SnapCenter-Betrieb nicht erfolgreich.

Zeigen Sie die Festplatten auf einem Host an

Sie können die Festplatten auf jedem Windows Host, den Sie mit SnapCenter verwalten, anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

   Die Festplatten werden aufgelistet.

Anzeige geclusterter Festplatten

Sie können Cluster-Festplatten auf dem Cluster anzeigen, den Sie mit SnapCenter verwalten. Die Cluster-Laufwerke werden nur angezeigt, wenn Sie das Cluster aus dem Dropdown-Menü Hosts auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Cluster aus der Dropdown-Liste **Host** aus.

   Die Festplatten werden aufgelistet.

Richten Sie eine iSCSI-Sitzung ein

Wenn Sie iSCSI zum Herstellen einer Verbindung zu einer LUN verwenden, müssen Sie eine iSCSI-Sitzung starten, bevor Sie die LUN erstellen, um die Kommunikation zu ermöglichen.

Bevor Sie beginnen

- Sie müssen den Knoten des Speichersystems als iSCSI-Ziel definiert haben.
- Sie müssen den iSCSI-Service auf dem Speichersystem gestartet haben. "Weitere Informationen ."

Über diese Aufgabe

Sie können eine iSCSI-Sitzung nur zwischen denselben IP-Versionen einrichten, entweder von IPv6 zu IPv6 oder von IPv4 zu IPv4.

Sie können eine Link-lokale IPv6-Adresse für das iSCSI-Sitzungsmanagement und für die Kommunikation zwischen einem Host und einem Ziel nur verwenden, wenn beide sich im selben Subnetz befinden.

Wenn Sie den Namen eines iSCSI-Initiators ändern, ist der Zugriff auf iSCSI-Ziele beeinträchtigt. Nach Ändern des Namens müssen Sie eventuell die Ziele, auf die der Initiator Zugriff hat, neu konfigurieren, damit sie den neuen Namen erkennen können. Sie müssen sicherstellen, dass der Host nach Ändern des Namens eines iSCSI-Initiators neu gestartet wird.

Wenn Ihr Host über mehrere iSCSI-Schnittstellen verfügt, können Sie eine iSCSI-Sitzung mit einer IP-Adresse in der ersten Schnittstelle nicht von einer anderen Schnittstelle mit einer anderen IP-Adresse aus starten, wenn Sie eine iSCSI-Sitzung für SnapCenter eingerichtet haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iSCSI-Sitzung**.
3. Wählen Sie aus der Dropdown-Liste **Storage Virtual Machine** die Storage Virtual Machine (SVM) für das iSCSI-Ziel aus.
4. Wählen Sie aus der Dropdown-Liste **Host** den Host für die Sitzung aus.
5. Klicken Sie Auf **Sitzung Erstellen**.

   Der Assistent „Sitzung einrichten“ wird angezeigt.

6. Geben Sie im Assistenten zum Erstellen von Sitzungen das Ziel an:

In diesem Feld…	Eingeben…
Name des Ziel-Nodes	Der Knotenname des iSCSI-Ziels Wenn ein vorhandener Zielknotenname vorhanden ist, wird der Name im schreibgeschützten Format angezeigt.
Zielportaladresse	Die IP-Adresse des Zielnetzwerkportals
Zielportalport	Der TCP-Port des Zielnetzwerkportals
Adresse des Initiator-Portals	Die IP-Adresse des Initiator-Netzwerkportals

7. Wenn Sie mit Ihren Einträgen zufrieden sind, klicken Sie auf **Verbinden**.

   SnapCenter richtet die iSCSI-Sitzung ein.

8. Wiederholen Sie diesen Vorgang, um für jedes Ziel eine Sitzung einzurichten.

Erstellen Sie mit FC verbundene oder mit iSCSI verbundene LUNs oder Festplatten

Der Windows-Host sieht die LUNs auf Ihrem Storage-System als virtuelle Festplatten. Sie können SnapCenter verwenden, um eine FC-verbundene oder iSCSI-verbundene LUN zu erstellen und zu konfigurieren.

Wenn Sie Festplatten außerhalb von SnapCenter erstellen und formatieren möchten, werden nur NTFS- und CSVFS-Dateisysteme unterstützt.

Bevor Sie beginnen

- Sie müssen ein Volume für die LUN auf Ihrem Speichersystem erstellt haben.

  Das Volume sollte nur LUNs enthalten und nur LUNs, die mit SnapCenter erstellt wurden.

  Sie können auf einem mit SnapCenter erstellten Klon-Volume keine LUN erstellen, es sei denn, der Klon wurde bereits aufgeteilt.

- Sie müssen den FC- oder iSCSI-Service auf dem Storage-System gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem eingerichtet haben.
- Das SnapCenter-Plug-ins-Paket für Windows muss nur auf dem Host installiert sein, auf dem Sie den Datenträger erstellen.

Über diese Aufgabe

- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt.
- Wenn eine LUN von Hosts in einem Windows Server Failover Cluster freigegeben wird, die CSV (Cluster Shared Volumes) verwenden, müssen Sie die Festplatte auf dem Host erstellen, der die Cluster-Gruppe besitzt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.
4. Klicken Sie Auf **Neu**.

   Der Assistent Datenträger erstellen wird geöffnet.

5. Geben Sie auf der Seite LUN-Name die LUN an:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus.
Der LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Ordners auszuwählen, der die LUN enthält.
Der LUN-Name	Geben Sie den Namen der LUN ein.

In diesem Feld…	Tun Sie das…
Clustergröße	Wählen Sie die Block-Zuweisungsgröße der LUN für das Cluster aus. Die Cluster-Größe hängt vom Betriebssystem und den Applikationen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite Festplattentyp den Festplattentyp aus:

Auswählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host zugegriffen werden. Ignorieren Sie das Feld **Ressourcengruppe**.
Freigegebenes Laufwerk	Die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt. Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld **Ressourcengruppe** ein. Sie müssen die Festplatte auf nur einem Host im Failover-Cluster erstellen.
Gemeinsam genutztes Cluster-Volume (CSV)	Die LUN wird von Hosts in einem Windows Server Failover Cluster, das CSV verwendet, gemeinsam verwendet. Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld **Ressourcengruppe** ein. Stellen Sie sicher, dass der Host, auf dem Sie die Festplatte erstellen, der Besitzer der Cluster-Gruppe ist.

7. Geben Sie auf der Seite Laufwerkeigenschaften die Laufwerkeigenschaften an:

Eigenschaft	Beschreibung
Automatisches Zuweisen des Bereitstellungspunkts	SnapCenter weist auf der Grundlage des Systemlaufwerks automatisch einen Volume-Mount-Punkt zu. Beispiel: Wenn Ihr Systemlaufwerk C: Ist, erstellt Auto assign einen Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnpt\). Die automatische Zuweisung wird für freigegebene Festplatten nicht unterstützt.

Eigenschaft	Beschreibung
Weisen Sie einen Laufwerkbuchstaben zu	Befestigen Sie die Festplatte an dem Laufwerk, das Sie in der Dropdown-Liste neben ausgewählt haben.
Verwenden Sie den Volume-Bereitstellungspunkt	Befestigen Sie die Festplatte an dem im Feld nebenan angegebenen Laufwerkspfad. Das Root des Volume-Bereitstellungspunkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weisen Sie keinen Laufwerksbuchstaben oder einen Volume-Bereitstellungspunkt zu	Wählen Sie diese Option, wenn Sie die Festplatte manuell in Windows mounten möchten.
Die LUN-Größe	Geben Sie die LUN-Größe an; Minimum 150 MB. Wählen Sie MB, GB oder TB in der angrenzenden Dropdown-Liste aus.
Verwenden Sie Thin Provisioning für das Volume, das diese LUN hostet	Thin Provisioning für die LUN Thin Provisioning weist nur so viel Speicherplatz zu, wie gleichzeitig benötigt wird. Dies ermöglicht es der LUN, die maximale verfügbare Kapazität effizient zu erweitern. Stellen Sie sicher, dass auf dem Volume genügend Speicherplatz verfügbar ist, um allen LUN-Storage, den Sie glauben, dass Sie benötigen werden, gerecht zu werden.
Wählen Sie Partitionstyp	Wählen Sie GPT-Partition für eine GUID-Partitionstabelle oder MBR-Partition für einen Master Boot Record aus. MBR-Partitionen können falsche Ausrichtung in Windows Server Failover Clustern verursachen. Partitionsfestplatten der Unified Extensible Firmware Interface (UEFI) werden nicht unterstützt.

8. Wählen Sie auf der Seite LUN zuordnen den iSCSI- oder FC-Initiator auf dem Host aus:

In diesem Feld…	Tun Sie das…
Host	Doppelklicken Sie auf den Cluster-Gruppennamen, um eine Dropdown-Liste anzuzeigen, in der die Hosts angezeigt werden, die zum Cluster gehören, und wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird.
Wählen Sie Host Initiator aus	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host aus. Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit Multipath I/O (MPIO) verwenden.

9. Geben Sie auf der Seite Gruppentyp an, ob Sie eine vorhandene Initiatorgruppe der LUN zuordnen möchten, oder erstellen Sie eine neue Initiatorgruppe:

Auswählen…	Wenn…
Erstellen einer neuen Initiatorgruppe für ausgewählte Initiatoren	Sie möchten eine neue Initiatorgruppe für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Initiatorgruppe aus, oder geben Sie eine neue Initiatorgruppe für ausgewählte Initiatoren an	Sie möchten eine vorhandene Initiatorgruppe für die ausgewählten Initiatoren angeben oder eine neue Initiatorgruppe mit dem angegebenen Namen erstellen. Geben Sie den Initiatorgruppennamen in das Feld * igroup Name* ein. Geben Sie die ersten Buchstaben des bestehenden Initiatorgruppennamens ein, um das Feld automatisch abzuschließen.

10. Überprüfen Sie auf der Zusammenfassungsseite Ihre Auswahl und klicken Sie dann auf **Fertig stellen**.

    SnapCenter erstellt die LUN und verbindet sie mit dem angegebenen Laufwerk oder dem angegebenen Laufwerkpfad auf dem Host.

Ändern der Größe einer Festplatte

Sie können die Größe einer Festplatte bei sich ändernden Anforderungen Ihres Storage-Systems erhöhen oder reduzieren.

Über diese Aufgabe

- Bei einer LUN, die über Thin Provisioning bereitgestellt wurde, wird die Größe der ONTAP-lun-Geometrie als maximale Größe angezeigt.
- Bei LUNs mit Thick Provisioning wird die erweiterbare Größe (verfügbare Größe im Volume) als maximale

Größe angezeigt.

- LUNs mit Partitionen im MBR-Stil haben eine Größenbeschränkung von 2 TB.
- LUNs mit GPT-Partitionen haben eine Speichersystemgröße von maximal 16 TB.
- Es ist eine gute Idee, einen Snapshot vor der Größenänderung einer LUN zu erstellen.
- Wenn Sie eine LUN aus einem vor der Größe der LUN erstellten Snapshot wiederherstellen müssen, passt SnapCenter die LUN automatisch an die Größe des Snapshots an.

  Nach dem Restore müssen Daten, die der LUN nach der Größe der Größe hinzugefügt wurden, aus einem Snapshot wiederhergestellt werden, nachdem die Größe geändert wurde.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste Host aus.

   Die Festplatten werden aufgelistet.

4. Wählen Sie die Festplatte aus, die Sie ändern möchten, und klicken Sie dann auf **Größe**.
5. Verwenden Sie im Dialogfeld „Festplatte ändern“ das Schieberegler-Werkzeug, um die neue Größe der Festplatte festzulegen, oder geben Sie die neue Größe in das Feld Größe ein.

   Wenn Sie die Größe manuell eingeben, müssen Sie außerhalb des Felds Größe klicken, bevor die Schaltfläche verkleinern oder erweitern entsprechend aktiviert ist. Außerdem müssen Sie auf MB, GB oder TB klicken, um die Maßeinheit anzugeben.

6. Wenn Sie mit Ihren Einträgen zufrieden sind, klicken Sie ggf. auf **verkleinern** oder **erweitern**.

   SnapCenter Größe der Festplatte neu.

Schließen Sie eine Festplatte an

Sie können den Assistenten zum Verbinden von Festplatten verwenden, um eine vorhandene LUN mit einem Host zu verbinden, oder um eine getrennte LUN erneut zu verbinden.

Bevor Sie beginnen

- Sie müssen den FC- oder iSCSI-Service auf dem Storage-System gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem eingerichtet haben.
- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt.
- Wenn die LUN von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host verbinden, der die Cluster-Gruppe besitzt.
- Das Plug-in für Windows muss nur auf dem Host installiert sein, auf dem Sie die Festplatte anschließen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.

2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.
4. Klicken Sie Auf **Verbinden**.

   Der Assistent zum Verbinden von Festplatten wird geöffnet.

5. Geben Sie auf der Seite LUN-Name die zu verbindende LUN an:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus.
Der LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Volumes auszuwählen, das die LUN enthält.
Der LUN-Name	Geben Sie den Namen der LUN ein.
Clustergröße	Wählen Sie die Block-Zuweisungsgröße der LUN für das Cluster aus. Die Cluster-Größe hängt vom Betriebssystem und den Applikationen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite Festplattentyp den Festplattentyp aus:

Auswählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host zugegriffen werden.
Freigegebenes Laufwerk	Die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt. Sie müssen die Festplatte nur mit einem Host im Failover-Cluster verbinden.
Gemeinsam genutztes Cluster-Volume (CSV)	Die LUN wird von Hosts in einem Windows Server Failover Cluster, das CSV verwendet, gemeinsam verwendet. Stellen Sie sicher, dass der Host, auf dem Sie eine Verbindung zur Festplatte herstellen, der Besitzer der Cluster-Gruppe ist.

7. Geben Sie auf der Seite Laufwerkeigenschaften die Laufwerkeigenschaften an:

Eigenschaft	Beschreibung
Automatische Zuweisung	Lassen Sie SnapCenter automatisch einen Volume Mount-Punkt basierend auf dem Systemlaufwerk zuweisen. Beispiel: Wenn Ihr Systemlaufwerk C: Ist, erstellt die Eigenschaft Auto assign einen Volume Mount Point unter Ihrem Laufwerk C: (C:\scmnpt\). Die Eigenschaft „Automatische Zuweisung“ wird für freigegebene Festplatten nicht unterstützt.
Weisen Sie einen Laufwerkbuchstaben zu	Legen Sie den Datenträger in die entsprechende Dropdown-Liste ein.
Verwenden Sie den Volume-Bereitstellungspunkt	Mounten Sie die Festplatte an den im Feld angrenzend angegebenen Laufwerkspfad. Das Root des Volume-Bereitstellungspunkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weisen Sie keinen Laufwerksbuchstaben oder einen Volume-Bereitstellungspunkt zu	Wählen Sie diese Option, wenn Sie die Festplatte manuell in Windows mounten möchten.

8. Wählen Sie auf der Seite LUN zuordnen den iSCSI- oder FC-Initiator auf dem Host aus:

In diesem Feld…	Tun Sie das…
Host	Doppelklicken Sie auf den Cluster-Gruppennamen, um eine Dropdown-Liste anzuzeigen, in der die Hosts angezeigt werden, die zum Cluster gehören, und wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird.
Wählen Sie Host Initiator aus	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host aus. Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit MPIO verwenden.

9. Geben Sie auf der Seite Gruppentyp an, ob Sie eine vorhandene Initiatorgruppe der LUN zuordnen oder eine neue Initiatorgruppe erstellen möchten:

Auswählen…	Wenn…
Erstellen einer neuen Initiatorgruppe für ausgewählte Initiatoren	Sie möchten eine neue Initiatorgruppe für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Initiatorgruppe aus, oder geben Sie eine neue Initiatorgruppe für ausgewählte Initiatoren an	Sie möchten eine vorhandene Initiatorgruppe für die ausgewählten Initiatoren angeben oder eine neue Initiatorgruppe mit dem angegebenen Namen erstellen. Geben Sie den Initiatorgruppennamen in das Feld * igroup Name* ein. Geben Sie die ersten Buchstaben des bestehenden Initiatorgruppennamens ein, um das Feld automatisch abzuschließen.

10. Überprüfen Sie auf der Seite Zusammenfassung Ihre Auswahl und klicken Sie auf **Fertig stellen**.

    SnapCenter verbindet die LUN mit dem angegebenen Laufwerk- oder Laufwerkspfad am Host.

Trennen Sie eine Festplatte

Sie können eine LUN ohne Auswirkungen auf den Inhalt der LUN von einem Host trennen, mit einer Ausnahme: Wenn Sie einen Klon vor dessen Trennung trennen, verlieren Sie den Inhalt des Klons.

Bevor Sie beginnen

- Stellen Sie sicher, dass die LUN nicht von einer Applikation verwendet wird.
- Stellen Sie sicher, dass die LUN nicht mit Monitoring-Software überwacht wird.
- Wenn die LUN gemeinsam genutzt wird, entfernen Sie die Abhängigkeiten der Cluster-Ressourcen aus der LUN, und überprüfen Sie, ob alle Nodes im Cluster eingeschaltet sind, ordnungsgemäß funktionieren und SnapCenter zur Verfügung stehen.

Über diese Aufgabe

Wenn Sie eine LUN in einem FlexClone Volume trennen, das SnapCenter erstellt hat, und keine anderen LUNs auf dem Volume sind verbunden, löscht SnapCenter das Volume. Vor dem Trennen der LUN zeigt SnapCenter eine Meldung an, dass das FlexClone Volume möglicherweise gelöscht wird.

Um das automatische Löschen des FlexClone Volume zu vermeiden, sollten Sie das Volume umbenennen, bevor Sie die letzte LUN trennen. Wenn Sie das Volume umbenennen, stellen Sie sicher, dass Sie mehrere Zeichen als nur das letzte Zeichen im Namen ändern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

   Die Festplatten werden aufgelistet.

4. Wählen Sie das Laufwerk aus, das Sie trennen möchten, und klicken Sie dann auf **Trennen**.

5. Klicken Sie im Dialogfeld Disconnect Disk auf **OK**.

   SnapCenter trennt die Verbindung der Festplatte.

Löschen Sie eine Festplatte

Sie können einen Datenträger löschen, wenn Sie ihn nicht mehr benötigen. Nach dem Löschen eines Datenträgers können Sie das Löschen nicht rückgängig machen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

   Die Festplatten werden aufgelistet.

4. Wählen Sie den Datenträger aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie im Dialogfeld Datenträger löschen auf **OK**.

   SnapCenter löscht die Festplatte.

SMB-Freigaben erstellen und managen

Um eine SMB3-Freigabe auf einer Storage Virtual Machine (SVM) zu konfigurieren, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets verwenden.

Best Practice: die Verwendung der Cmdlets wird empfohlen, da es Ihnen ermöglicht, die Vorteile von Vorlagen mit SnapCenter zur Automatisierung der Share-Konfiguration zu nutzen.

Die Vorlagen kapseln die Best Practices für die Volume- und Share-Konfiguration. Die Vorlagen finden Sie im Ordner Vorlagen im Installationsordner für das SnapCenter-Plug-ins-Paket für Windows.

Wenn Sie sich damit wohlfühlen, können Sie Ihre eigenen Vorlagen nach den bereitgestellten Modellen erstellen. Sie sollten die Parameter in der Cmdlet-Dokumentation überprüfen, bevor Sie eine benutzerdefinierte Vorlage erstellen.

Erstellen Sie eine SMB-Freigabe

Auf der Seite „SnapCenter Shares“ können Sie eine SMB3-Freigabe auf einer Storage Virtual Machine (SVM) erstellen.

Datenbanken auf SMB-Freigaben können nicht mit SnapCenter gesichert werden. SMB-Support ist auf die reine Provisionierung beschränkt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Shares**.

3. Wählen Sie die SVM aus der Dropdown-Liste **Storage Virtual Machine** aus.
4. Klicken Sie Auf **Neu**.

   Das Dialogfeld Neue Freigabe wird geöffnet.

5. Definieren Sie im Dialogfeld Neue Freigabe die Freigabe:

In diesem Feld…	Tun Sie das…
Beschreibung	Geben Sie einen beschreibenden Text für die Freigabe ein.
Freigabename	Geben Sie den Freigabenamen ein, z. B. „Test_share“. Der Name, den Sie für die Freigabe eingeben, wird auch als Volume-Name verwendet. Der Share-Name: • Muss eine UTF-8-Zeichenfolge sein. • Darf folgende Zeichen nicht enthalten: Steuerzeichen von 0x00 bis 0x1F (beide inklusiv), 0x22 (doppelte Anführungszeichen) und die Sonderzeichen `\ / [ ] : (vertical bar) < > + = ; , ?`
Freigabepfad	• Klicken Sie in das Feld, um einen neuen Dateisystempfad einzugeben, z. B. /. • Doppelklicken Sie in das Feld, um eine Liste der vorhandenen Dateisystempfade auszuwählen.

6. Wenn Sie mit Ihren Einträgen zufrieden sind, klicken Sie auf **OK**.

   SnapCenter erstellt die SMB-Freigabe auf der SVM.

Löschen einer SMB-Freigabe

Sie können eine SMB-Freigabe löschen, wenn Sie sie nicht mehr benötigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Shares**.
3. Klicken Sie auf der Seite Freigaben im Feld **Storage Virtual Machine** auf, um ein Dropdown-Menü mit einer Liste der verfügbaren Storage Virtual Machines (SVMs) anzuzeigen. Wählen Sie dann die SVM für die Freigabe aus, die Sie löschen möchten.
4. Wählen Sie aus der Liste der Freigaben auf der SVM die Freigabe aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

5. Klicken Sie im Dialogfeld Freigabe löschen auf **OK**.

   SnapCenter löscht die SMB-Freigabe von der SVM.

Rückgewinnung von Speicherplatz im Storage-System

Obwohl NTFS den verfügbaren Speicherplatz auf einer LUN verfolgt, wenn Dateien gelöscht oder geändert werden, werden die neuen Informationen nicht dem Storage-System gemeldet. Sie können das PowerShell Cmdlet zur Speicherplatzrückgewinnung auf dem Plug-in für Windows Host ausführen, um sicherzustellen, dass neu freigegebene Blöcke im Storage als verfügbar markiert werden.

Wenn Sie das Cmdlet auf einem Remote Plug-in-Host ausführen, müssen Sie das Cmdlet "SnapCenterOpen-SMConnection" ausführen, um eine Verbindung zum SnapCenter Server zu öffnen.

Bevor Sie beginnen

- Sie müssen sicherstellen, dass der Prozess zur Rückgewinnung von Speicherplatz abgeschlossen wurde, bevor Sie eine Wiederherstellung durchführen.
- Wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird, müssen Sie Speicherplatz auf dem Host, der die Cluster-Gruppe besitzt, freigeben.
- Um eine optimale Storage-Performance zu erzielen, sollten Sie so oft wie möglich eine Platzreklamation durchführen.

  Stellen Sie sicher, dass das gesamte NTFS-Dateisystem gescannt wurde.

Über diese Aufgabe

- Die Rückgewinnung von Speicherplatz ist zeitaufwändig und CPU-intensiv. Daher ist es normalerweise am besten, wenn die Auslastung des Storage-Systems und des Windows-Hosts niedrig ist.
- Die Speicherplatzrückgewinnung beansprucht fast allen verfügbaren Speicherplatz, nicht aber 100 Prozent.
- Sie sollten die Festplattendefragmentierung nicht gleichzeitig ausführen, da Sie Speicherplatz einsparen.

  Dadurch kann der Rückgewinnungsprozess verlangsamt werden.

Schritt

Geben Sie an der PowerShell-Eingabeaufforderung des Anwendungsservers den folgenden Befehl ein:

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

Drive_Path ist der der der LUN zugeordnete Laufwerkpfad.

Stellen Sie Storage mit PowerShell cmdlets bereit

Wenn Sie die SnapCenter-GUI nicht zum Durchführen von Hostbereitstellungs- und Speicherplatzrückgewinnungsaufträgen verwenden möchten, können Sie die PowerShell-Cmdlets verwenden. Sie können Cmdlets direkt verwenden oder zu Skripten hinzufügen.

Wenn Sie die Cmdlets auf einem Remote-Plug-in-Host ausführen, müssen Sie das Cmdlet SnapCenter Open-

SMConnection ausführen, um eine Verbindung zum SnapCenter Server zu öffnen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Wenn SnapCenter PowerShell Cmdlets aufgrund der Entfernung von SnapDrive für Windows vom Server beschädigt sind, lesen Sie "SnapCenter cmdlets defekt, wenn SnapDrive für Windows deinstalliert wird".

Bereitstellung von Storage in VMware Umgebungen

Sie können das SnapCenter-Plug-in für Microsoft Windows in VMware-Umgebungen verwenden, um LUNs zu erstellen und zu verwalten und Snapshots zu verwalten.

Unterstützte VMware Gastbetriebssystemplattformen

- Unterstützte Versionen von Windows Server
- Microsoft Cluster-Konfigurationen

  Unterstützung von maximal 16 Knoten auf VMware bei Verwendung des Microsoft iSCSI Software-Initiators oder bis zu zwei Knoten mit FC

- RDM-LUNs

  Unterstützung von maximal 56 RDM LUNs mit vier LSI Logic SCSI Controllern für normalen RDMS oder 42 RDM LUNs mit drei LSI Logic SCSI Controllern auf einem VMware VM MSC Box-to-Box Plug-in für Windows Konfiguration

  Unterstützt VMware Paravirtuellen SCSI-Controller 256 Festplatten können auf RDM-Festplatten unterstützt werden.

Serverbezogene Einschränkungen bei VMware ESXi

- Das Installieren des Plug-ins für Windows auf einem Microsoft-Cluster auf virtuellen Maschinen mit ESXi-Anmeldedaten wird nicht unterstützt.

  Sie sollten Ihre vCenter-Anmeldedaten verwenden, wenn Sie das Plug-in für Windows auf geclusterten virtuellen Maschinen installieren.

- Alle Cluster-Knoten müssen dieselbe Ziel-ID (auf dem virtuellen SCSI-Adapter) für dieselbe geclusterte Festplatte verwenden.
- Wenn Sie eine RDM-LUN außerhalb des Plug-in für Windows erstellen, müssen Sie den Plug-in-Service neu starten, damit die neu erstellte Festplatte erkannt werden kann.
- Auf einem VMware Gastbetriebssystem können Sie keine iSCSI- und FC-Initiatoren gleichzeitig verwenden.

Minimale vCenter-Berechtigungen, die für SnapCenter RDM-Vorgänge erforderlich sind

Sie sollten die folgenden vCenter-Rechte auf dem Host haben, um RDM-Vorgänge in einem Gastbetriebssystem durchzuführen:

- Datastore: Datei Entfernen

- Host: Konfiguration > Speicherpartition Konfiguration
- Virtual Machine: Konfiguration

Sie müssen diese Berechtigungen einer Rolle auf Virtual Center-Server-Ebene zuweisen. Die Rolle, der Sie diese Berechtigungen zuweisen, kann keinem Benutzer ohne Root-Berechtigungen zugewiesen werden.

Nachdem Sie diese Berechtigungen zugewiesen haben, können Sie das Plug-in für Windows auf dem Gastbetriebssystem installieren.

Verwalten Sie FC RDM LUNs in einem Microsoft Cluster

Sie können das Plug-in für Windows verwenden, um einen Microsoft Cluster mithilfe von FC RDM LUNs zu verwalten. Sie müssen jedoch zuerst das gemeinsame RDM Quorum und den gemeinsam genutzten Speicher außerhalb des Plug-ins erstellen und dann die Festplatten den virtuellen Maschinen im Cluster hinzufügen.

Ab ESXi 5.5 können Sie auch ESX iSCSI und FCoE Hardware verwenden, um einen Microsoft-Cluster zu managen. Das Plug-in für Windows bietet Out-of-Box-Unterstützung für Microsoft Cluster.

Anforderungen

Das Plug-in für Windows unterstützt Microsoft Cluster mithilfe von FC RDM LUNs auf zwei verschiedenen Virtual Machines, die zu zwei verschiedenen ESX- oder ESXi-Servern gehören, auch „Cluster Across“ genannt, wenn Sie die spezifischen Konfigurationsanforderungen erfüllen.

- Die Virtual Machines (VMs) müssen dieselbe Windows Serverversion ausführen.
- ESX oder ESXi Serverversionen müssen für jeden übergeordneten VMware Host die gleichen sein.
- Jeder übergeordnete Host muss mindestens zwei Netzwerkadapter haben.
- Es muss mindestens ein VMware Virtual Machine File System (VMFS) Datastore vorhanden sein, der von den beiden ESX- oder ESXi-Servern gemeinsam genutzt wird.
- VMware empfiehlt, den gemeinsam genutzten Datenspeicher auf einem FC SAN zu erstellen.

  Bei Bedarf kann auch der gemeinsam genutzte Datenspeicher über iSCSI erstellt werden.

- Die gemeinsam genutzte RDM LUN muss sich im physischen Kompatibilitätsmodus befinden.
- Die gemeinsame RDM LUN muss außerhalb des Plug-in für Windows manuell erstellt werden.

  Sie können virtuelle Laufwerke nicht für gemeinsamen Speicher verwenden.

- Ein SCSI-Controller muss für jede Virtual Machine im Cluster im physischen Kompatibilitätsmodus konfiguriert sein:

  Für Windows Server 2008 R2 müssen Sie den LSI Logic SAS SCSI-Controller auf jeder virtuellen Maschine konfigurieren. Freigegebene LUNs können den vorhandenen LSI Logic SAS-Controller nicht verwenden, wenn nur einer seiner Typen vorhanden ist und dieser bereits mit dem Laufwerk C: Verbunden ist.

  SCSI-Controller vom Typ paravirtuell werden auf VMware Microsoft Clustern nicht unterstützt.

> Wenn Sie einer gemeinsam genutzten LUN auf einer virtuellen Maschine im physischen Kompatibilitätsmodus einen SCSI-Controller hinzufügen, müssen Sie im VMware Infrastructure Client die Option **Raw Device Mapping** (RDM) und nicht die Option **Create a New Disk** auswählen.

- Die Cluster der Microsoft Virtual Machine können nicht Teil eines VMware Clusters sein.
- Sie müssen vCenter-Anmeldeinformationen und keine ESX- oder ESXi-Anmeldeinformationen verwenden, wenn Sie das Plug-in für Windows auf virtuellen Maschinen installieren, die zu einem Microsoft-Cluster gehören.
- Das Plug-in für Windows kann keine einzelne Initiatorgruppe mit Initiatoren aus mehreren Hosts erstellen.

  Die Initiatorgruppe, die die Initiatoren aller ESXi Hosts enthält, muss auf dem Storage Controller erstellt werden, bevor die RDM-LUNs erstellt werden, die als gemeinsam genutzte Cluster-Festplatten verwendet werden.

- Stellen Sie sicher, dass Sie eine RDM LUN unter ESXi 5.0 mit einem FC-Initiator erstellen.

  Wenn Sie eine RDM-LUN erstellen, wird eine Initiatorgruppe mit ALUA erstellt.

Einschränkungen

Das Windows-Plug-in unterstützt Microsoft Cluster mit FC/iSCSI RDM LUNs auf verschiedenen Virtual Machines, die zu verschiedenen ESX- oder ESXi-Servern gehören.

Diese Funktion wird in Versionen vor ESX 5.5i nicht unterstützt.

- Das Plug-in für Windows unterstützt keine Cluster auf ESX iSCSI und NFS-Datenspeichern.
- Das Plug-in für Windows unterstützt keine gemischten Initiatoren in einer Cluster-Umgebung.

  Der Initiator muss entweder FC oder Microsoft iSCSI sein, aber nicht beides.

- ESX iSCSI-Initiatoren und HBAs werden von freigegebenen Laufwerken in einem Microsoft-Cluster nicht unterstützt.
- Das Plug-in für Windows unterstützt keine Migration von Virtual Machines mit vMotion, wenn die Virtual Machine Teil eines Microsoft Clusters ist.
- Das Plug-in für Windows unterstützt MPIO nicht auf virtuellen Maschinen in einem Microsoft-Cluster.

Erstellen Sie eine gemeinsame FC RDM LUN

Bevor Sie in einem Microsoft Cluster Speicher zwischen den Knoten mit FC RDM LUNs teilen können, müssen Sie zuerst die gemeinsame Quorum-Festplatte und die freigegebene Speicherplatte erstellen und diese dann beiden virtuellen Maschinen im Cluster hinzufügen.

Das freigegebene Laufwerk wird mit dem Plug-in für Windows nicht erstellt. Sie sollten die gemeinsame LUN erstellen und dann jeder virtuellen Maschine im Cluster hinzufügen. Weitere Informationen finden Sie unter "Clustern Von Virtual Machines Über Physische Hosts Hinweg".

Controller-basierte SnapCenter Standard-Lizenzen hinzufügen

Wenn Sie FAS, AFF oder ASA Storage Controller verwenden, ist eine Controller-basierte Lizenz für SnapCenter Standard erforderlich.

Die Controller-basierte Lizenz weist folgende Merkmale auf:

- SnapCenter Standard-Nutzungsberechtigung ist beim Kauf von Premium oder Flash Bundle enthalten (nicht im Basispaket).

- Unbegrenzte Storage-Nutzung
- Wird mithilfe des ONTAP System Manager oder der ONTAP CLI direkt zum FAS, AFF oder ASA -Speichercontroller hinzugefügt.

  Für die Controller-basierten Lizenzen von SnapCenter geben Sie in der SnapCenter -Benutzeroberfläche keine Lizenzinformationen ein.

- Gesperrt an die Seriennummer des Controllers

Informationen zu den erforderlichen Lizenzen finden Sie unter "SnapCenter-Lizenzen".

Schritt 1: Überprüfen Sie, ob die SnapManager Suite-Lizenz installiert ist

Sie können die SnapCenter Benutzeroberfläche verwenden, um zu überprüfen, ob eine SnapManager Suite-Lizenz auf FAS, AFF oder ASA Primärspeichersystemen installiert ist, und um festzustellen, welche Systeme Lizenzen benötigen. SnapManager Suite-Lizenzen gelten nur für FAS, AFF und ASA -SVMs oder Cluster auf primären Speichersystemen.

Wenn Sie bereits über eine SnapManager Suite-Lizenz auf Ihrem Controller verfügen, stellt SnapCenter automatisch die Berechtigung für die Standard-Controller-basierte Lizenz bereit. Die Bezeichnungen SnapManagerSuite-Lizenz und Controller-basierte SnapCenter Standard-Lizenz werden synonym verwendet, beziehen sich jedoch auf dieselbe Lizenz.

Schritte

1. Wählen Sie im linken Navigationsbereich **Storage Systems** aus.
2. Wählen Sie auf der Seite Storage Systems im Dropdown-Menü **Typ** aus, ob alle hinzugefügten SVMs oder Cluster angezeigt werden sollen:
   - Um alle hinzugefügten SVMs anzuzeigen, wählen Sie **ONTAP SVMs**.
   - Um alle hinzugefügten Cluster anzuzeigen, wählen Sie **ONTAP Cluster**.

     Wenn Sie den Cluster-Namen auswählen, werden alle SVMs, die Teil des Clusters sind, im Abschnitt Storage Virtual Machines angezeigt.
3. Suchen Sie in der Liste Speicherverbindungen die Spalte Controller-Lizenz.

   In der Spalte „Controller License“ wird der folgende Status angezeigt:

   - Zeigt an, dass eine SnapManager Suite-Lizenz auf einem primären Speichersystem von FAS, AFF oder ASA installiert ist.
   - Zeigt an, dass keine SnapManager Suite-Lizenz auf einem primären Speichersystem von FAS, AFF oder ASA installiert ist.
   - Nicht zutreffend bedeutet, dass eine SnapManager Suite-Lizenz nicht anwendbar ist, da sich der Storage Controller auf Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select oder sekundären Speicherplattformen befindet.

Schritt 2: Identifizieren Sie die auf dem Controller installierten Lizenzen

Mit der ONTAP-Befehlszeile können Sie alle auf dem Controller installierten Lizenzen anzeigen. Sie sollten

Cluster-Administrator auf dem FAS-, AFF- oder ASA-System sein.

> Der Controller zeigt die Controller-basierte Lizenz von SnapCenter Standard als SnapManagerSuite-Lizenz an.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim NetApp Controller ein.
2. Geben Sie den Befehl „license show“ ein und sehen Sie sich dann die Ausgabe an, um zu sehen, ob die SnapManagerSuite-Lizenz installiert ist.

   Beispielausgabe

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

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

Serial Number: 1-81-00000000000000000000000xx
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 -
```

   Da hier beispielsweise die SnapManagerSuite Lizenz installiert ist, ist keine zusätzliche SnapCenter Lizenzmaßnahme erforderlich.

Schritt 3: Rufen Sie die Seriennummer des Controllers ab

Rufen Sie die Seriennummer des Controllers mithilfe der ONTAP -Befehlszeile ab. Sie müssen Clusteradministrator auf dem FAS, AFF oder ASA -System sein, um Ihre Controller-basierte Lizenzseriennummer zu erhalten.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim Controller ein.

2. Geben Sie den Befehl „System show -instance“ ein, und überprüfen Sie die Ausgabe, um die Controller-Seriennummer zu finden.

   Beispielausgabe

```
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. Notieren Sie die Seriennummern.

Schritt 4: Rufen Sie die Seriennummer der Controller-basierten Lizenz ab

Wenn Sie FAS, ASA oder AFF -Speicher verwenden, können Sie die Controller-basierte Lizenz für SnapCenter von der NetApp -Support-Site abrufen, bevor Sie sie über die ONTAP -Befehlszeile installieren.

Bevor Sie beginnen

- Sie sollten über gültige Anmeldedaten für die NetApp Support Site verfügen.

  Wenn Sie keine gültigen Anmeldeinformationen eingeben, gibt das System keine Informationen zu Ihrer Suche zurück.

- Sie sollten die Controller-Seriennummer angeben.

Schritte

1. Melden Sie sich bei an "NetApp Support Website".
2. Navigieren Sie zu **Systems** > **Softwarelizenzen**.
3. Stellen Sie im Bereich Auswahlkriterien sicher, dass die Seriennummer (auf der Rückseite des Geräts) ausgewählt ist, geben Sie die Seriennummer des Controllers ein und wählen Sie dann **Go!**.

   Eine Liste der Lizenzen für den angegebenen Controller wird angezeigt.

4. Suchen und notieren Sie die SnapCenter Standard- oder SnapManagerSuite-Lizenz.

Schritt 5: Controller-basierte Lizenz hinzufügen

Sie können die ONTAP Befehlszeile verwenden, um eine SnapCenter Controller-basierte Lizenz hinzuzufügen, wenn Sie FAS-, AFF- oder ASA-Systeme verwenden und über eine SnapCenter Standard- oder SnapManagerSuite-Lizenz verfügen.

Bevor Sie beginnen

- Sie sollten Cluster-Administrator auf dem FAS-, AFF- oder ASA-System sein.
- Sie sollten über die Lizenz für SnapCenter Standard oder SnapManagerSuite verfügen.

Über diese Aufgabe

Wenn Sie SnapCenter Testversionen mit FAS, AFF oder ASA Storage installieren möchten, erhalten Sie eine Evaluierungslizenz für das Premium Bundle, die auf Ihrem Controller installiert wird.

Wenn Sie SnapCenter auf Testbasis installieren möchten, sollten Sie sich an Ihren Ansprechpartner wenden, um eine Evaluierungslizenz für das Premium Bundle zu erhalten, die auf Ihrem Controller installiert wird.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim NetApp Cluster ein.
2. Fügen Sie den Lizenzschlüssel für die SnapManagerSuite hinzu:

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

Dieser Befehl ist auf der Administrator-Berechtigungsebene verfügbar.

3. Überprüfen Sie, ob die SnapManagerSuite-Lizenz installiert ist:

```
license show
```

Schritt 6: Entfernen Sie die Testlizenz

Wenn Sie eine Controller-basierte SnapCenter Standard-Lizenz verwenden und die kapazitätsbasierte Testlizenz (Seriennummer endet mit „50“) entfernen müssen, sollten Sie MySQL-Befehle verwenden, um die Testlizenz manuell zu entfernen. Die Testlizenz kann nicht über die SnapCenter Benutzeroberfläche gelöscht werden.

Das manuelle Entfernen einer Testlizenz ist nur erforderlich, wenn Sie eine Controller-basierte SnapCenter Standard-Lizenz verwenden.

Schritte

1. Öffnen Sie auf dem SnapCenter-Server ein PowerShell-Fenster, um das MySQL-Passwort zurückzusetzen.
   a. Führen Sie das Cmdlet Open-SmConnection aus, um eine Verbindung mit dem SnapCenter -Server für ein SnapCenterAdmin-Konto herzustellen.
   b. Führen Sie das Set-RepositRepositRepositSmoryPassword aus, um das MySQL-Passwort zurückzusetzen.

      Informationen zu den Cmdlets finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch" .

2. Öffnen Sie die Eingabeaufforderung und führen Sie mysql -U root -p aus, um sich bei MySQL anzumelden.

   MySQL fordert Sie zur Eingabe des Passworts auf. Geben Sie die Anmeldeinformationen ein, die Sie beim Zurücksetzen des Passworts angegeben haben.

3. Entfernen Sie die Testlizenz aus der Datenbank:

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

Konfiguration Der Hochverfügbarkeit

Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit

Um Hochverfügbarkeit (HA) in SnapCenter zu unterstützen, die entweder unter Windows oder unter Linux ausgeführt werden, können Sie den F5 Load Balancer installieren. Mit F5 kann der SnapCenter Server aktiv/Passiv-Konfigurationen in bis zu zwei Hosts an demselben Standort unterstützen. Um F5 Load Balancer in SnapCenter zu verwenden, sollten Sie die SnapCenter-Server konfigurieren und F5 Load Balancer konfigurieren.

Sie können auch den Netzwerklastenausgleich (NLB) konfigurieren, um die hohe Verfügbarkeit von SnapCenter einzurichten. Sie sollten NLB außerhalb der SnapCenter-Installation manuell konfigurieren, um eine hohe Verfügbarkeit zu gewährleisten.

Für Cloud-Umgebungen können Sie Hochverfügbarkeit entweder mit Amazon Web Services (AWS) Elastic Load Balancing (ELB) und Azure Load Balancer konfigurieren.

Konfigurieren Sie Hochverfügbarkeit mit F5

Anweisungen zum Konfigurieren von SnapCenter -Servern für hohe Verfügbarkeit mit F5 Load Balancer finden Sie unter "Konfigurieren von SnapCenter-Servern für Hochverfügbarkeit mit F5 Load Balancer" .

Sie müssen Mitglied der Gruppe Lokale Administratoren auf den SnapCenter-Servern sein (zusätzlich zur SnapCenterAdmin-Rolle zugewiesen), um die folgenden Cmdlets zum Hinzufügen und Entfernen von F5-Clustern zu verwenden:

- Add-SmServerCluster
- Add-SmServer
- Entfernen Sie-SmServerCluster

  Weitere Informationen finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch".

Weitere Informationen

- Nachdem Sie SnapCenter für Hochverfügbarkeit installiert und konfiguriert haben, bearbeiten Sie die SnapCenter Desktop-Verknüpfung, um auf die F5 Cluster-IP zu verweisen.
- Wenn ein Failover zwischen SnapCenter-Servern auftritt und es auch eine SnapCenter-Sitzung gibt, müssen Sie den Browser schließen und sich erneut bei SnapCenter anmelden.
- Wenn Sie im Load Balancer Setup (NLB oder F5) einen Host hinzufügen, der teilweise vom NLB- oder F5-Host aufgelöst wurde, und wenn der SnapCenter-Host nicht in der Lage ist, auf diesen Host zuzugreifen, schaltet die SnapCenter-Hostseite häufig zwischen Hosts aus und wird ausgeführt. Um dieses Problem zu beheben, sollten Sie sicherstellen, dass beide SnapCenter-Hosts den Host im NLB- oder F5-Host lösen können.
- SnapCenter-Befehle für MFA-Einstellungen sollten auf allen Hosts ausgeführt werden. Die Konfiguration von Drittanbieterkonfigurationen sollte auf dem Active Directory Federation Services (AD FS)-Server unter Verwendung von F5-Clusterdetails erfolgen. Der Zugriff auf die SnapCenter-Benutzeroberfläche auf Hostebene wird blockiert, nachdem MFA aktiviert wurde.
- Während des Failovers werden die Einstellungen des Überwachungsprotokolls nicht auf dem zweiten Host wiedergegeben. Daher sollten Sie die Einstellungen des Überwachungsprotokolls auf dem passiven F5-Host manuell wiederholen, wenn er aktiv wird.

Konfigurieren von Hochverfügbarkeit mit Network Load Balancing (NLB)

Sie können den Netzwerklastenausgleich (NLB) konfigurieren, um die hohe Verfügbarkeit von SnapCenter einzurichten. Sie sollten NLB außerhalb der SnapCenter-Installation manuell konfigurieren, um eine hohe Verfügbarkeit zu gewährleisten.

Informationen zum Konfigurieren des Netzwerklastausgleichs (NLB) mit SnapCenter finden Sie unter "So konfigurieren Sie NLB mit SnapCenter".

Hochverfügbarkeit mit AWS Elastic Load Balancing (ELB) konfigurieren

Um eine hochverfügbare SnapCenter-Umgebung in Amazon Web Services (AWS) zu konfigurieren, lassen sich zwei SnapCenter-Server in separaten Verfügbarkeitszonen einrichten und für automatisches Failover konfigurieren. Die Architektur umfasst virtuelle private IP-Adressen, Routing-Tabellen und Synchronisierung zwischen aktiven und Standby-MySQL-Datenbanken.

Schritte

1. Konfigurieren Sie die virtuelle private Overlay-IP in AWS. Weitere Informationen finden Sie unter "Konfigurieren Sie die virtuelle private Overlay-IP".

2. Bereiten Sie Ihren Windows-Host vor
    a. IPv4-Priorität über IPv6 erzwingen:
        - Standort: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameter
        - Schlüssel: DisabledComponents
        - Geben Sie „REG_DWORD“ ein
        - Wert: 0x20
    b. Stellen Sie sicher, dass die vollständig qualifizierten Domänennamen per DNS oder über die lokale Hostkonfiguration an die IPv4-Adressen aufgelöst werden können.
    c. Stellen Sie sicher, dass kein System-Proxy konfiguriert ist.
    d. Stellen Sie sicher, dass das Administratorkennwort auf dem Windows-Server identisch ist, wenn Sie ein Setup ohne Active Directory verwenden und sich die Server nicht in einer Domäne befinden.
    e. Fügen Sie virtuelle IP auf beiden Windows-Servern hinzu.
3. Erstellen Sie den SnapCenter-Cluster.
    a. Starten Sie PowerShell und stellen Sie eine Verbindung mit SnapCenter her. `Open-SmConnection`
    b. Erstellen Sie den Cluster. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
    c. Fügen Sie den sekundären Server hinzu. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
    d. Erfahren Sie mehr zur Hochverfügbarkeit. `Get-SmServerConfig`
4. Erstellen Sie die Lamda-Funktion, um die Routing-Tabelle anzupassen, falls der virtuelle private IP-Endpunkt nicht mehr verfügbar ist und von AWS CloudWatch überwacht wird. Weitere Informationen finden Sie unter "Lambda-Funktion erstellen".
5. Erstellen Sie einen Monitor in CloudWatch, um die Verfügbarkeit des SnapCenter-Endpunkts zu überwachen. Ein Alarm ist so konfiguriert, dass er eine Lambda-Funktion auslöst, wenn der Endpunkt nicht erreichbar ist. Die Lambda-Funktion passt die Routingtabelle an, um den Datenverkehr auf den aktiven SnapCenter-Server umzuleiten. Weitere Informationen finden Sie unter "Erstellen Sie synthetische Kanaren".
6. Implementieren Sie einen Workflow mit einer Step-Funktion als Alternative zur CloudWatch-Überwachung und profitieren Sie von geringeren Failover-Zeiten. Der Workflow beinhaltet eine Lambda-Sondenfunktion zum Testen der SnapCenter-URL, eine DynamoDB-Tabelle zum Speichern der Fehleranzahl und die Step-Funktion selbst.
    a. Verwenden Sie eine Lambda-Funktion zum Sondieren der SnapCenter-URL. Weitere Informationen finden Sie unter "Lambda-Funktion erzeugen".
    b. Erstellen Sie eine DynamoDB-Tabelle zum Speichern der Fehleranzahl zwischen zwei-Schritt-Funktions-Iterationen. Weitere Informationen finden Sie unter "Erste Schritte mit der DynamoDB-Tabelle".
    c. Erstellen Sie die Step-Funktion. Weitere Informationen finden Sie unter "Dokumentation der Step-Funktion".
    d. Testen Sie einen einzelnen Schritt.

e. Testen Sie die vollständige Funktion.

f. IAM-Rolle erstellen und Berechtigungen anpassen, um die Lambda-Funktion ausführen zu dürfen.

g. Erstellen Sie einen Zeitplan, um die Schrittfunktion auszulösen. Weitere Informationen finden Sie unter "Verwenden des Amazon EventBridge Scheduler zum Starten von Schrittfunktionen".

Konfigurieren Sie Hochverfügbarkeit mit dem Azure Load Balancer

Sie können die SnapCenter-Umgebung mit Hochverfügbarkeit mit dem Azure Load Balancer konfigurieren.

Schritte

1. Erstellen Sie mit dem Azure-Portal Virtual Machines in einem Scale-Set. Mit dem Scale-Set für virtuelle Azure-Maschinen können Sie eine Gruppe von Virtual Machines mit Lastausgleich erstellen und managen. Die Anzahl der virtuellen Maschineninstanzen kann sich automatisch auf die Nachfrage oder einen definierten Zeitplan erhöhen oder verringern. Weitere Informationen finden Sie unter "Erstellen Sie mit dem Azure-Portal Virtual Machines in einem Scale-Set".
2. Melden Sie sich nach dem Konfigurieren der virtuellen Maschinen bei jeder virtuellen Maschine im VM-Set an, und installieren Sie SnapCenter-Server in beiden Knoten.
3. Erstellen Sie den Cluster in Host 1. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. Fügen Sie den sekundären Server hinzu. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. Sehen Sie sich die Details zur Hochverfügbarkeit an. `Get-SmServerConfig`
6. Falls erforderlich, erstellen Sie den sekundären Host neu. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Failover auf den zweiten Host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Wechsel von NLB zu F5 für hohe Verfügbarkeit

Sie können Ihre SnapCenter HA-Konfiguration von Network Load Balancing (NLB) auf F5 Load Balancer ändern.

Schritte

1. Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit mit F5. "Weitere Informationen .".
2. Starten Sie PowerShell auf dem Host des SnapCenter Servers.
3. Starten Sie eine Sitzung mit dem Cmdlet "Open-SmConnection", und geben Sie dann Ihre Anmeldeinformationen ein.
4. Aktualisieren Sie den SnapCenter-Server, um mit dem Cmdlet "Update-SmServerCluster" auf die F5-Cluster-IP-Adresse zu verweisen.

   Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Hochverfügbarkeit für das SnapCenter MySQL Repository

MySQL-Replikation ist eine Funktion von MySQL Server, mit der Sie Daten von einem MySQL-Datenbankserver (Master) auf einen anderen MySQL-Datenbankserver (Slave) replizieren können. SnapCenter unterstützt die MySQL-Replikation für Hochverfügbarkeit nur auf zwei NLB-fähigen (Network Load Balancing-enabled) Knoten.

SnapCenter führt Lese- oder Schreibvorgänge im Master-Repository durch und leitet die Verbindung zum Slave-Repository weiter, wenn ein Fehler im Master-Repository auftritt. Das Slave-Repository wird dann zum Master-Repository. SnapCenter unterstützt außerdem die umgekehrte Replizierung, die nur während des Failover aktiviert ist.

Wenn Sie die MySQL High Availability (HA)-Funktion verwenden möchten, müssen Sie den Network Load Balancer (NLB) auf dem ersten Knoten konfigurieren. Das MySQL-Repository ist auf diesem Knoten als Teil der Installation installiert. Bei der Installation von SnapCenter auf dem zweiten Knoten müssen Sie sich mit F5 des ersten Knotens verbinden und auf dem zweiten Knoten eine Kopie des MySQL-Repository erstellen.

SnapCenter bietet die *get-SmRepositoryConfig* und *set-SmRepositoryConfig* PowerShell Commandlets zur Verwaltung der MySQL Replikation.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Beachten Sie die Einschränkungen für die MySQL HA-Funktion:

- NLB und MySQL HA werden nicht über zwei Knoten hinaus unterstützt.
- Ein Wechsel von einer eigenständigen SnapCenter-Installation zu einer NLB-Installation oder umgekehrt und das Umschalten von einer MySQL-Standalone-Konfiguration auf MySQL HA wird nicht unterstützt.
- Automatisches Failover wird nicht unterstützt, wenn die Slave-Repository-Daten nicht mit den Master-Repository-Daten synchronisiert werden.

  Sie können ein erzwungenes Failover initiieren, indem Sie das Cmdlet *set-SmoryConfig* verwenden.

- Wenn ein Failover initiiert wird, können Jobs, die ausgeführt werden, fehlschlagen.

  Wenn ein Failover aufgrund eines MySQL Servers oder SnapCenter Servers ausfällt, können alle ausgeführten Jobs fehlschlagen. Nach dem Failover zum zweiten Node werden alle nachfolgenden Jobs erfolgreich ausgeführt.

Informationen zur Konfiguration der Hochverfügbarkeit finden Sie unter "So konfigurieren Sie NLB und ARR mit SnapCenter".

Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)

Erstellen Sie eine Rolle

Zusätzlich zur Nutzung vorhandener SnapCenter-Rollen können Sie eigene Rollen erstellen und die Berechtigungen anpassen.

Um eigene Rollen zu erstellen, ist eine Anmeldung mit der Rolle „SnapCenterAdmin“ erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Rollen**.
3. Klicken Sie Auf .
4. Geben Sie einen Namen und eine Beschreibung für die neue Rolle an.

   In Benutzernamen und Gruppennamen dürfen nur die folgenden Sonderzeichen verwendet werden: Leerzeichen ( ), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:).

5. Wählen Sie **Alle Mitglieder dieser Rolle können Objekte anderer Mitglieder** sehen, damit andere Mitglieder der Rolle nach der Aktualisierung der Ressourcenliste Ressourcen wie Volumes und Hosts sehen können.

   Sie sollten diese Option deaktivieren, wenn Sie nicht möchten, dass Mitglieder dieser Rolle Objekte sehen, denen andere Mitglieder zugewiesen sind.

   Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

6. Wählen Sie auf der Seite Berechtigungen die Berechtigungen aus, die Sie der Rolle zuweisen möchten, oder klicken Sie auf **Alle auswählen**, um der Rolle alle Berechtigungen zu gewähren.
7. Klicken Sie Auf **Absenden**.

Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine RBAC-Rolle für NetApp ONTAP hinzu

Sie können die Sicherheitskontinbefehle verwenden, um eine RBAC-Rolle für NetApp ONTAP hinzuzufügen, wenn auf Ihren Storage-Systemen Clustered ONTAP ausgeführt wird.

Bevor Sie beginnen

- Identifizieren Sie die Aufgabe (oder Aufgaben), die Sie ausführen möchten, und die Berechtigungen, die zum Ausführen dieser Aufgaben erforderlich sind.
- Gewähren Sie Berechtigungen für Befehle und/oder Befehlsverzeichnisse.

  Für jedes Befehlsverzeichnis gibt es zwei Zugriffsebenen: All-Access und Read-Only.

  Sie müssen immer zuerst die All-Access-Berechtigungen zuweisen.

- Rollen Benutzern zuweisen.
- Identifizieren Sie Ihre Konfiguration, je nachdem, ob Ihre SnapCenter-Plug-Ins mit der Cluster-Administrator-IP für den gesamten Cluster oder direkt mit einer SVM innerhalb des Clusters verbunden sind.

Über diese Aufgabe

Um die Konfiguration dieser Rollen auf Speichersystemen zu vereinfachen, können Sie das Tool „RBAC User Creator für NetApp ONTAP“ verwenden, das im NetApp Communities Forum veröffentlicht wird.

Dieses Tool verarbeitet automatisch die korrekte Einrichtung der ONTAP-Berechtigungen. Das Tool RBAC User Creator for NetApp ONTAP fügt beispielsweise die Privileges automatisch in der richtigen Reihenfolge

hinzu, sodass die Privileges mit allen Zugriffsrechten zuerst angezeigt werden. Wenn Sie zuerst die schreibgeschützten Berechtigungen hinzufügen und dann die All-Access-Berechtigungen hinzufügen, markiert ONTAP die All-Access-Berechtigungen als Duplikate und ignoriert sie.

> Wenn Sie später SnapCenter oder ONTAP aktualisieren, sollten Sie das RBAC-Benutzerersteller für NetApp ONTAP-Tool erneut ausführen, um die zuvor erstellten Benutzerrollen zu aktualisieren. Benutzerrollen, die für eine frühere Version von SnapCenter oder ONTAP erstellt wurden, funktionieren nicht ordnungsgemäß mit aktualisierten Versionen. Wenn Sie das Tool erneut ausführen, übernimmt es automatisch die Aktualisierung. Sie müssen die Rollen nicht neu erstellen.

Weitere Informationen zum Einrichten von ONTAP RBAC-Rollen finden Sie im "ONTAP 9 Administratorauthentifizierung und RBAC-Energiehandbuch".

Schritte

1. Erstellen Sie auf dem Storage-System eine neue Rolle, indem Sie den folgenden Befehl eingeben:

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

   - svm_Name ist der Name der SVM. Wenn Sie dieses Feld leer lassen, werden standardmäßig Cluster-Administratoren verwendet.
   - Role_Name ist der Name, den Sie für die Rolle angeben.
   - Befehl ist die ONTAP Funktion.

   > Sie müssen diesen Befehl für jede Berechtigung wiederholen. Beachten Sie, dass vor schreibgeschützten Befehlen All-Access-Befehle aufgelistet werden müssen.

   Informationen zur Liste der Berechtigungen finden Sie unter "ONTAP CLI-Befehle zum Erstellen von Rollen und Zuweisen von Berechtigungen".

2. Erstellen Sie einen Benutzernamen durch Eingabe des folgenden Befehls:

   ```
   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 ist der Name des von Ihnen erstellten Benutzers.
   - <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.
   - svm_Name ist der Name der SVM.

3. Weisen Sie dem Benutzer die Rolle durch Eingabe des folgenden Befehls zu:

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

   - <user_Name> ist der Name des Benutzers, den Sie in Schritt 2 erstellt haben. Mit diesem Befehl können Sie den Benutzer so ändern, dass er der Rolle zugeordnet wird.
   - <svm_Name> ist der Name der SVM.
   - <Role_Name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.

◦ <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.

4. Überprüfen Sie, ob der Benutzer ordnungsgemäß erstellt wurde, indem Sie den folgenden Befehl eingeben:

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

   User_Name ist der Name des Benutzers, den Sie in Schritt 3 erstellt haben.

Erstellen Sie SVM-Rollen mit minimalen Berechtigungen

Beim Erstellen einer Rolle für einen neuen SVM-Benutzer in ONTAP müssen Sie verschiedene ONTAP-CLI-Befehle ausführen. Diese Rolle ist erforderlich, wenn Sie SVMs in ONTAP für die Verwendung mit SnapCenter konfigurieren und Sie nicht die vsadmin-Rolle verwenden möchten.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `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`

Erstellung von SVM-Rollen für ASA r2 Systeme

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen müssen, um eine Rolle für einen neuen SVM-Benutzer in ASA r2-Systemen zu erstellen. Diese Rolle ist erforderlich, wenn Sie SVMs in ASA r2-Systemen für die Verwendung mit SnapCenter konfigurieren und die Rolle „vsadmin“ nicht verwenden möchten.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `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`

Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen

Sie sollten eine ONTAP-Cluster-Rolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP-Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP CLI-Befehle ausführen, um die ONTAP-Cluster-Rolle zu erstellen und minimale Berechtigungen zuzuweisen.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um Cluster-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `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

Erstellen von ONTAP Clusterrollen für ASA r2-Systeme

Sie sollten eine ONTAP-Cluster-Rolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP-Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP CLI-Befehle ausführen, um die ONTAP-Cluster-Rolle zu erstellen und minimale Berechtigungen zuzuweisen.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um Cluster-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `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

Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu

Um die rollenbasierte Zugriffssteuerung für SnapCenter-Benutzer zu konfigurieren, können Sie Benutzer oder Gruppen hinzufügen und Rollen zuweisen. Die Rolle legt die Optionen fest, auf die SnapCenter-Benutzer zugreifen können.

Bevor Sie beginnen

- Sie müssen sich als „SnapCenterAdmin“-Rolle angemeldet haben.
- Sie müssen die Benutzer- oder Gruppenkonten in Active Directory im Betriebssystem oder in der Datenbank erstellt haben. Sie können SnapCenter nicht zum Erstellen dieser Konten verwenden.

  In Benutzernamen und Gruppennamen können nur die folgenden Sonderzeichen eingefügt werden: Leerzeichen ( ), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:).

- SnapCenter umfasst mehrere vordefinierte Rollen.

  Sie können diese Rollen entweder dem Benutzer zuweisen oder neue Rollen erstellen.

- AD-Benutzer und AD-Gruppen, die SnapCenter RBAC hinzugefügt werden, müssen über DIE LESEBERECHTIGUNG auf dem Benutzer-Container und dem Computer-Container im Active Directory verfügen.
- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle zugewiesen haben, die die entsprechenden Berechtigungen enthält, müssen Sie den Benutzerzugriff auf SnapCenter-Ressourcen wie Hosts und Speicherverbindungen zuweisen.

  Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen

zugewiesenen Assets verfügen.

- Sie sollten dem Benutzer oder der Gruppe irgendwann eine Rolle zuweisen, um die RBAC-Berechtigungen und Effizienzfunktionen zu nutzen.
- Sie können Assets wie Host, Ressourcengruppen, Richtlinien, Storage-Verbindungen, Plug-in, Und Anmeldeinformationen für den Benutzer beim Erstellen des Benutzers oder der Gruppe.
- Die Mindestwerte, die Sie einem Benutzer zur Durchführung bestimmter Vorgänge zuweisen sollten, sind:

Betrieb	Zuweisung von Assets
Ressourcen schützen	Host, Richtlinie
Backup	Host, Ressourcengruppe und Richtlinie
Wiederherstellen	Host, Ressourcengruppe
Klon	Host, Ressourcengruppe und Richtlinie
Lebenszyklus von Klonen	Host
Erstellen Sie eine Ressourcengruppe	Host

- Wenn ein neuer Knoten zu einem Windows Cluster oder einer DAG (Exchange Server Database Availability Group)-Ressource hinzugefügt wird und wenn dieser neue Knoten einem Benutzer zugewiesen ist, müssen Sie das Element dem Benutzer oder der Gruppe neu zuweisen, um den neuen Knoten dem Benutzer oder der Gruppe hinzuzufügen.

  Sie sollten den RBAC-Benutzer oder die Gruppe dem Cluster oder der DAG neu zuweisen, um den neuen Node auch dem RBAC-Benutzer oder der Gruppe einzuschließen. Sie verfügen beispielsweise über ein Cluster mit zwei Nodes und haben dem Cluster einen RBAC-Benutzer oder eine Gruppe zugewiesen. Wenn Sie dem Cluster einen weiteren Node hinzufügen, sollten Sie den RBAC-Benutzer oder die Gruppe dem Cluster neu zuweisen, um den neuen Node für den Benutzer oder die Gruppe der RBAC einzubeziehen.

- Wenn Sie planen, Snapshots zu replizieren, müssen Sie dem Benutzer, der den Vorgang durchführt, die Speicherverbindung für das Quell- und das Ziel-Volume zuweisen.

  Sie sollten Assets hinzufügen, bevor Sie den Benutzern Zugriff zuweisen.

Wenn Sie zum Schutz von VMs, VMDKs oder Datastores das SnapCenter Plug-in für VMware vSphere verwenden, sollten Sie ein vCenter Benutzer zu einem SnapCenter Plug-in für VMware vSphere hinzufügen. Weitere Informationen zu VMware vSphere-Rollen finden Sie unter "Vordefinierte Rollen in Paketen mit SnapCenter Plug-in für VMware vSphere".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Benutzer und Zugriff** > .
3. Auf der Seite Benutzer/Gruppen aus Active Directory oder Workgroup hinzufügen:

Für dieses Feld…	Tun Sie das…
Zugriffstyp	Wählen Sie entweder Domäne oder Arbeitsgruppe aus Für den Authentifizierungstyp Domäne müssen Sie den Domänennamen des Benutzers oder der Gruppe angeben, dem Sie den Benutzer zu einer Rolle hinzufügen möchten. Standardmäßig wird er mit dem angemeldeten Domänennamen ausgefüllt. Sie müssen die nicht vertrauenswürdige Domäne auf der Seite **Einstellungen** > **Globale Einstellungen** > **Domain-Einstellungen** registrieren.
Typ	Wählen Sie entweder Benutzer oder Gruppe aus SnapCenter unterstützt nur Sicherheitsgruppen, nicht die Vertriebsgruppe.
Benutzername	a. Geben Sie den teilweisen Benutzernamen ein, und klicken Sie dann auf **Hinzufügen**. Bei Benutzername wird die Groß-/Kleinschreibung berücksichtigt. b. Wählen Sie den Benutzernamen aus der Suchliste aus. Wenn Sie Benutzer aus einer anderen Domäne oder einer nicht vertrauenswürdigen Domäne hinzufügen, sollten Sie den Benutzernamen vollständig eingeben, da keine Suchliste für domänenübergreifende Benutzer vorhanden ist. Wiederholen Sie diesen Schritt, um der ausgewählten Rolle weitere Benutzer oder Gruppen hinzuzufügen.
Rollen	Wählen Sie die Rolle aus, der Sie den Benutzer hinzufügen möchten.

4. Klicken Sie auf **Zuweisen** und dann auf der Seite „Assets zuweisen“ auf:
   a. Wählen Sie den Typ des Assets aus der Dropdown-Liste **Asset** aus.
   b. Wählen Sie in der Asset-Tabelle das Asset aus.

      Die Assets werden nur aufgeführt, wenn der Benutzer die Assets zu SnapCenter hinzugefügt hat.

   c. Wiederholen Sie diesen Vorgang für alle erforderlichen Assets.
   d. Klicken Sie Auf **Speichern**.
5. Klicken Sie Auf **Absenden**.

   Nachdem Sie Benutzer oder Gruppen hinzugefügt und Rollen zugewiesen haben, aktualisieren Sie die Ressourcenliste.

Konfigurieren Sie die Einstellungen für das Prüfprotokoll

Für jede Aktivität des SnapCenter Servers werden Audit-Protokolle erstellt. Standardmäßig sind Audit-Protokolle am installierten Standardspeicherort gesichert *C:\Program Files\NetApp\SnapCenter WebApp\Audit*.

Prüfprotokolle werden durch die Generierung von Digital Signed Digest für jedes einzelne Audit-Ereignis gesichert, um es vor nicht autorisierten Änderungen zu schützen. Die generierten Digest-Dateien werden in der separaten Prüfsumme-Prüfdatei aufbewahrt und werden regelmäßig Integritätsprüfungen unterzogen, um die Integrität des Inhalts zu gewährleisten.

Sie sollten sich als „SnapCenterAdmin“-Rolle angemeldet haben.

Über diese Aufgabe

- Warnmeldungen werden in den folgenden Szenarien gesendet:
  - Der Zeitplan für die Integritätsprüfung des Überwachungsprotokolls oder der Syslog-Server ist aktiviert oder deaktiviert
  - Prüfung der Integritätsprüfung der Protokolle, Audit-Protokoll oder Ausfall des Syslog-Serverprotokolls
  - Nur wenig Speicherplatz
- E-Mails werden nur gesendet, wenn die Integritätsprüfung fehlschlägt.
- Sie sollten sowohl das Verzeichnis des Prüfprotokolls als auch die Verzeichnispfade für das Prüfsumme-Protokoll gemeinsam ändern. Es ist nicht möglich, nur eine dieser Änderungen vorzunehmen.
- Wenn das Verzeichnis des Prüfprotokolls und die Verzeichnispfade der Prüfsumme geändert werden, kann die Integritätsprüfung nicht für die am früheren Speicherort vorhandenen Prüfprotokolle durchgeführt werden.
- Verzeichnis für Prüfsumme und Prüfsumme für Prüfprotokolle sollten sich auf dem lokalen Laufwerk des SnapCenter Servers befinden.

  Freigegebene oder netzwerkbasierte Laufwerke werden nicht unterstützt.

- Wenn das UDP-Protokoll in den Einstellungen des Syslog-Servers verwendet wird, sind Fehler aufgrund des Ports ausgefallen oder nicht verfügbar. Es kann weder als Fehler noch als Warnung in SnapCenter erfasst werden.
- Sie können Set-SmAuditSettings und Get-SmAuditSettings Befehle verwenden, um die Prüfprotokolle zu konfigurieren.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von Get-Help Command_Name abgerufen werden. Alternativ können Sie auch die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Navigieren Sie auf der Seite **Einstellungen** zu **Einstellungen** > **Globale Einstellungen** > **Prüfprotokoll-Einstellungen**.
2. Geben Sie im Abschnitt Prüfprotokoll die Details ein.
3. Geben Sie das Logverzeichnis **Audit** und das Verzeichnis **Prüfsumme-Prüfsumme-Protokoll** ein
   a. Geben Sie die maximale Dateigröße ein
   b. Geben Sie die maximale Anzahl von Protokolldateien ein
   c. Geben Sie den Prozentsatz der Speicherplatznutzung ein, um eine Meldung zu senden
4. (Optional) Aktivieren Sie **UTC-Uhrzeit protokollieren**.
5. (Optional) Aktivieren Sie **Auditprotokoll Integritätsprüfung Zeitplan** und klicken Sie auf **Integritätsprüfung starten**, um die Integritätsprüfung nach Bedarf zu prüfen.

   Sie können auch den Befehl **Start-SmAuditIntegritätCheck** ausführen, um die Integritätsprüfung bei Bedarf zu starten.
6. (Optional) Aktivieren Sie die Weiterleitung von Audit-Protokollen an Remote-Syslog-Server und geben Sie die Details des Syslog-Servers ein.

   Sie sollten das Zertifikat vom Syslog-Server in den 'Trusted Root' für das TLS 1.2-Protokoll importieren.
   a. Geben Sie Syslog Server Host Ein
   b. Geben Sie Den Syslog-Server-Port Ein
   c. Geben Sie Syslog Server Protocol Ein
   d. RFC-Format eingeben
7. Klicken Sie Auf **Speichern**.
8. Durch Klicken auf **Monitor** > **Jobs** können Sie die Integritätsprüfungen und die Überprüfung des Festplattenspeichers einsehen.

Konfigurieren Sie gesicherte MySQL-Verbindungen mit SnapCenter-Server

Sie können SSL-Zertifikate (Secure Sockets Layer) und Schlüsseldateien generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Server in Standalone-Konfigurationen oder NLB-Konfigurationen (Network Load Balancing) sichern möchten.

Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter-Server-Konfigurationen

Sie können SSL-Zertifikate (Secure Sockets Layer) und Schlüsseldateien generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Server sichern möchten. Sie müssen die Zertifikate und Schlüsseldateien im MySQL-Server und im SnapCenter-Server konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat
- Öffentliches Serverzertifikat und private Schlüsseldatei
- Öffentliches Zertifikat des Clients und Datei des privaten Schlüssels

Schritte

1. Richten Sie die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mithilfe des openssl-Befehls ein.

   Weitere Informationen finden Sie unter "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

   > Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

   Best Practice: der Server Fully Qualified Domain Name (FQDN) sollte als allgemeiner Name für das Serverzertifikat verwendet werden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

   Der standardmäßige Ordnerpfad für MySQL Data ist `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Die standardmäßige MySQL Server-Konfigurationsdatei (my.ini) ist `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Server-Schlüsselpfade im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

   Sie müssen im Abschnitt [Client] der MySQL-Serverkonfigurationsdatei (my.ini) das CA-Zertifikat, das öffentliche Clientzertifikat und die privaten Schlüsselpfade des Clients angeben.

   Das folgende Beispiel zeigt die Zertifikate und Schlüsseldateien, die in den Abschnitt [mysqld] der Datei my.ini im Standardordner kopiert wurden `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"
```

Das folgende Beispiel zeigt die im Abschnitt [Client] der Datei my.ini aktualisierten Pfade.

```
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. Beenden Sie die Webanwendung des SnapCenter-Servers im Internetinformationsserver (IIS).
5. Starten Sie den MySQL-Dienst neu.
6. Aktualisieren Sie den Wert des Schlüssels MySQLProtocol in der Datei SnapManager.Web.UI.dll.config.

   Das folgende Beispiel zeigt den Wert des Schlüssels MySQLProtocol, der in der Datei SnapManager.Web.UI.dll.config aktualisiert wurde.

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

7. Aktualisieren Sie die Datei SnapManager.Web.UI.dll.config mit den Pfaden, die im Abschnitt [Client] der Datei my.ini bereitgestellt wurden.

   Das folgende Beispiel zeigt die im Abschnitt [Client] der Datei my.ini aktualisierten Pfade.

```
<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. Starten Sie die Webanwendung des SnapCenter-Servers im IIS.

Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen

Sie können SSL-Zertifikate (Secure Sockets Layer) und Schlüsseldateien sowohl für die HA-Knoten (High Availability) generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Servern sichern möchten. Sie müssen die Zertifikate und Schlüsseldateien auf den MySQL-Servern und auf den HA-Knoten konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat

  Auf einem der HA-Nodes wird ein CA-Zertifikat generiert, und dieses CA-Zertifikat wird auf den anderen HA-Node kopiert.

- Öffentliche Zertifikate des Servers und private Schlüsseldateien des Servers für beide HA-Nodes
- Öffentliche Client-Zertifikate und private Schlüsseldateien von Clients für beide HA-Nodes

Schritte

1. Richten Sie beim ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL Server und Clients unter Windows mithilfe des openssl-Befehls ein.

   Weitere Informationen finden Sie unter "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

   > Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

   Best Practice: der Server Fully Qualified Domain Name (FQDN) sollte als allgemeiner Name für das Serverzertifikat verwendet werden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

   Der standardmäßige Ordner MySQL Data ist C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Die standardmäßige MySQL Server-Konfigurationsdatei (my.ini) lautet C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.in

   > Sie müssen im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) CA-Zertifikat, öffentliches Serverzertifikat und private Server-Schlüsselpfade angeben.

   Sie müssen im Abschnitt [Client] der MySQL-Server-Konfigurationsdatei (my.ini) im Abschnitt [Client] CA-Zertifikat, öffentliches Clientzertifikat und private Schlüsselpfade des Clients angeben.

   Im folgenden Beispiel werden die Zertifikate und Schlüsseldateien im Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data kopiert.

```
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"
```

Das folgende Beispiel zeigt die im Abschnitt [Client] der Datei my.ini aktualisierten Pfade.

```
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. Kopieren Sie für den zweiten HA-Node das CA-Zertifikat, und generieren Sie öffentliche Serverzertifikate, Dateien mit privaten Schlüsseln des Servers, öffentliches Client-Zertifikat und private Schlüsseldateien des Clients. Führen Sie folgende Schritte aus:

   a. Kopieren Sie das auf dem ersten HA-Knoten generierte CA-Zertifikat in den Ordner MySQL Data des zweiten NLB-Knotens.

      Der standardmäßige Ordner MySQL Data ist C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

      > Sie dürfen kein CA-Zertifikat erneut erstellen. Sie sollten nur das öffentliche Serverzertifikat, das öffentliche Zertifikat des Clients, die Datei des privaten Schlüssels und die Datei des privaten Clientschlüssels erstellen.

   b. Richten Sie beim ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL Server und Clients unter Windows mithilfe des openssl-Befehls ein.

      "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

      > Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

Es wird empfohlen, den Server-FQDN als gemeinsamen Namen für das Serverzertifikat zu verwenden.

c. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

d. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

> Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Server-Schlüsselpfade im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Sie müssen im Abschnitt [Client] der MySQL-Serverkonfigurationsdatei (my.ini) das CA-Zertifikat, das öffentliche Clientzertifikat und die privaten Schlüsselpfade des Clients angeben.

Im folgenden Beispiel werden die Zertifikate und Schlüsseldateien im Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data kopiert.

```
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"
```

Das folgende Beispiel zeigt die im Abschnitt [Client] der Datei my.ini aktualisierten Pfade.

```
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. Beenden Sie die Webanwendung des SnapCenter-Servers im Internet Information Server (IIS) auf beiden HA-Knoten.
6. Starten Sie den MySQL Service auf beiden HA-Nodes neu.

7. Aktualisieren Sie den Wert des Schlüssels MySQLProtocol in der Datei SnapManager.Web.UI.dll.config für beide HA-Knoten.

   Das folgende Beispiel zeigt den Wert des Schlüssels MySQLProtocol, der in der Datei SnapManager.Web.UI.dll.config aktualisiert wurde.

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

8. Aktualisieren Sie die Datei SnapManager.Web.UI.dll.config mit den Pfaden, die Sie im Abschnitt [Client] der Datei my.ini für beide HA-Nodes angegeben haben.

   Das folgende Beispiel zeigt die im Abschnitt [Client] der my.ini Dateien aktualisierten Pfade.

   ```
   <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. Starten Sie die Webanwendung des SnapCenter Servers im IIS auf beiden HA-Knoten.
10. Verwenden Sie das Cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell mit der Option -Force auf einem der HA-Knoten, um eine gesicherte MySQL-Replikation auf beiden HA-Knoten einzurichten.

    Selbst wenn der Replikationsstatus ordnungsgemäß ist, können Sie mit der Option -Force das Slave-Repository wiederherstellen.

Konfigurieren Sie die zertifikatbasierte Authentifizierung

Die zertifikatbasierte Authentifizierung erhöht die Sicherheit durch die Überprüfung der Identität des SnapCenter-Servers und der Plug-in-Hosts und gewährleistet so eine sichere und verschlüsselte Kommunikation.

Aktivieren Sie die zertifikatbasierte Authentifizierung

Führen Sie das folgende PowerShell-Cmdlet aus, um die zertifikatbasierte Authentifizierung für SnapCenter Server und die Windows Plug-in-Hosts zu aktivieren. Bei Linux-Plug-in-Hosts wird die zertifikatbasierte Authentifizierung aktiviert, wenn Sie die bidirektionale SSL-Funktion aktivieren.

- So aktivieren Sie die clientzertifikatbasierte Authentifizierung:

  ```
  Set-SmConfigSettings -Agent –configSettings
  ```

```
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- So deaktivieren Sie die clientzertifikatbasierte Authentifizierung:

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

Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter-Server

Sie sollten die CA-Zertifikate über die Microsoft Management Console (MMC) vom SnapCenter-Server auf die Plug-in-Hosts exportieren.

Bevor Sie beginnen

Sie sollten die bidirektionale SSL-Konfiguration vorgenommen haben.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster Zertifikate Snap-in die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenstamm** > **Zertifikate - Lokaler Computer** > **Persönlich** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das beschaffte CA-Zertifikat, das für den SnapCenter-Server verwendet wird, und wählen Sie dann **Alle Aufgaben** > **Export** aus, um den Export-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Privaten Schlüssel Exportieren	Wählen Sie **Nein, exportieren Sie den privaten Schlüssel nicht**, und klicken Sie dann auf **Weiter**.
Dateiformat Exportieren	Klicken Sie Auf **Weiter**.
Dateiname	Klicken Sie auf **Browse** und geben Sie den Dateipfad an, um das Zertifikat zu speichern, und klicken Sie auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Export zu starten.

Die zertifikatbasierte Authentifizierung wird für SnapCenter HA-Konfigurationen und das SnapCenter Plug-in für VMware vSphere nicht unterstützt.

Importieren Sie das CA-Zertifikat auf die Windows-Plug-in-Hosts

Um das exportierte SnapCenter-Server-CA-Zertifikat zu verwenden, sollten Sie das zugehörige Zertifikat über die Microsoft-Managementkonsole (MMC) auf die SnapCenter-Windows-Plug-in-Hosts importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster Zertifikate Snap-in die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenstamm** > **Zertifikate - Lokaler Computer** > **Persönlich** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Personal“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Import-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Speicherort Des Geschäfts	Klicken Sie Auf **Weiter**.
Zu importierende Datei	Wählen Sie das SnapCenter-Serverzertifikat aus, das mit der Erweiterung .cer endet.
Zertifikatspeicher	Klicken Sie Auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Importieren Sie das CA-Zertifikat auf die UNIX-Plug-in-Hosts

Sie sollten das CA-Zertifikat auf die UNIX-Plug-in-Hosts importieren.

Über diese Aufgabe

- Sie können das Kennwort für den SPL-Keystore und den Alias des CA-Schlüsselpaars verwalten, das gerade verwendet wird.
- Das Passwort für den SPL-Keystore und für das zugehörige Alias-Passwort des privaten Schlüssels muss identisch sein.

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen. Es ist der Wert, der dem Schlüssel entspricht `SPL_KEYSTORE_PASS`.
2. Ändern Sie das Schlüsselspeicher-Passwort: `$ keytool -storepasswd -keystore keystore.jks`
3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe

Kennwort, das für den Schlüsselspeicher verwendet wird: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`

4. Aktualisieren Sie das gleiche für den Schlüssel SPL_KEYSTORE_PASS in `spl.properties` Datei:
5. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate für den SPL-Vertrauensspeicher konfigurieren. Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore enthält: `/var/opt/snapcenter/spl/etc`.
2. Suchen Sie die Datei `keystore.jks`.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher: `$ keytool -list -v -keystore keystore.jks`
4. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.

Konfigurieren Sie das CA-signierte Schlüsselpaar für SPL Trust-Store

Sie sollten das CA-Schlüsselpaar für den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore enthält `/var/opt/snapcenter/spl/etc`.
2. Suchen Sie die Datei `keystore.jks`.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher: `$ keytool -list -v -keystore keystore.jks`
4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen Schlüssel hinzu. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf. `$ keytool -list -v -keystore keystore.jks`
6. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Standard-SPL-Keystore-Kennwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in `spl.properties` Datei:

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

8. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen einfachen Namen: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in `spl.properties` Datei: Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.
10. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Exportieren von SnapCenter-Zertifikaten

Sie sollten die SnapCenter-Zertifikate im PFX-Format exportieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snap-in hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Mein Benutzerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate - Aktueller Benutzer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit dem SnapCenter Friendly Name, und wählen Sie dann **Alle Aufgaben** > **Exportieren** aus, um den Exportassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Exportieren	Wählen Sie die Option **Ja, exportieren Sie den privaten Schlüssel** und klicken Sie dann auf **Weiter**.
Dateiformat Exportieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Zu exportierende Datei	Geben Sie einen Dateinamen für das exportierte Zertifikat an (Sie müssen .pfx verwenden), und klicken Sie dann auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Export zu starten.

Konfigurieren Sie das CA-Zertifikat für den Windows-Host

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „persönlich“.

Abrufen des Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld Zertifikat auf die Registerkarte **Details**.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter-Server und allen Plug-in-Hosts durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

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

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows Host Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

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

   Beispiel:

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

Konfigurieren Sie ein CA-Zertifikat mit SnapCenter Site

Sie sollten das CA-Zertifikat mit der SnapCenter-Site auf einem Windows-Host konfigurieren.

Schritte

1. Öffnen Sie den IIS-Manager auf dem Windows-Server, auf dem SnapCenter installiert ist.
2. Klicken Sie im linken Navigationsbereich auf **Verbindungen**.
3. Erweitern Sie den Namen des Servers und **Sites**.
4. Wählen Sie die SnapCenter-Website aus, auf der Sie das SSL-Zertifikat installieren möchten.
5. Navigieren Sie zu **Aktionen** > **Website bearbeiten** und klicken Sie auf **Bindungen**.
6. Wählen Sie auf der Seite Bindungen die Option **Bindung für https** aus.
7. Klicken Sie Auf **Bearbeiten**.
8. Wählen Sie aus der Dropdown-Liste SSL-Zertifikat das kürzlich importierte SSL-Zertifikat aus.

9. Klicken Sie auf **OK**.

Die SnapCenter-Scheduler-Site (Standardport: 8154, HTTPS) ist mit einem selbstsignierten Zertifikat konfiguriert. Dieser Port kommuniziert innerhalb des SnapCenter-Serverhosts, und es ist nicht zwingend erforderlich, mit einem CA-Zertifikat zu konfigurieren. Wenn Sie in Ihrer Umgebung jedoch die Verwendung eines CA-Zertifikats vorschreibt, wiederholen Sie die Schritte 5 bis 9 mithilfe des SnapCenter-Planerstandorts.

Wenn das kürzlich bereitgestellte CA-Zertifikat nicht im Dropdown-Menü aufgeführt ist, überprüfen Sie, ob das CA-Zertifikat mit dem privaten Schlüssel verknüpft ist.

Stellen Sie sicher, dass das Zertifikat über den folgenden Pfad hinzugefügt wird: **Konsolenstamm > Zertifikate – lokaler Computer > vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

Aktivieren Sie CA-Zertifikate für SnapCenter

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikatvalidierung für den SnapCenter-Server aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Set-SmCertificateSettings" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für den SnapCenter-Server mit dem Cmdlet Get-SmCertificateSettings anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **CA Zertifikateinstellungen**.
2. Wählen Sie **Zertifikatvalidierung Aktivieren**.
3. Klicken Sie Auf **Anwenden**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass kein CA-Zertifikat aktiviert oder dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Konfigurieren Sie das CA-Zertifikat für den Linux-Host

Nach der Installation des SnapCenter -Servers unter Linux erstellt das Installationsprogramm das selbstsignierte Zertifikat. Wenn Sie das CA-Zertifikat verwenden möchten, sollten Sie die Zertifikate für den Nginx-Reverse-Proxy, die Audit-Protokollierung und SnapCenter konfigurieren.

Konfigurieren Sie das nginx-Zertifikat

Schritte

1. Navigieren Sie zu */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Öffnen Sie **snapcenter.conf** mit vi oder einem beliebigen Texteditor.
3. Navigieren Sie zum Abschnitt Server in der Konfigurationsdatei.
4. Ändern Sie die Pfade von *ssl_Certificate* und *ssl_Certificate_Key*, um auf das CA-Zertifikat zu verweisen.
5. Speichern und schließen Sie die Datei.
6. Nginx neu laden: `$nginx -s reload`

Konfigurieren Sie das Audit-Protokoll-Zertifikat

Schritte

1. Öffnen Sie *INSTALL_dir/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config* mithilfe von vi oder einem beliebigen Texteditor.

   Der Standardwert von *INSTALL_dir* ist */opt*.

2. Bearbeiten Sie die Schlüssel **AUDILOG_CERTIFICATE_PATH** und **AUDILOG_CERTIFICATE_PASSWORD**, um den CA-Zertifikatspfad und das Passwort einzuschließen.

   Für das Auditprotokoll-Zertifikat wird nur das *.pfx*-Format unterstützt.

3. Speichern und schließen Sie die Datei.
4. Starten Sie den Dienst **SnapManager Web** neu: `$ systemctl restart snapmanagerweb`

Konfigurieren des SnapCenter -Zertifikats

Schritte

1. Öffnen Sie die folgenden Konfigurationsdateien mit vi oder einem beliebigen Texteditor.
   - *INSTALL_dir/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*

     Der Standardwert von *INSTALL_dir* ist */opt*.

2. Bearbeiten Sie die Schlüssel **SERVICE_CERTIFICATE_PATH** und **SERVICE_CERTIFICATE_PASSWORD**, um den CA-Zertifikatspfad und das entsprechende Passwort einzuschließen.

Für das SnapCenter -Zertifikat wird nur das *.pfx*-Format unterstützt.

3. Speichern und schließen Sie die Dateien.
4. Starten Sie alle Dienste neu.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Sie sollten die bidirektionale SSL-Kommunikation so konfigurieren, dass die gegenseitige Kommunikation zwischen SnapCenter-Server auf Windows-Host und den Plug-ins gesichert ist.

Bevor Sie beginnen

- Sie sollten die CSR-Datei des CA-Zertifikats mit der unterstützten Mindestschlüssellänge von 3072 erstellt haben.
- Das CA-Zertifikat sollte die Serverauthentifizierung und die Clientauthentifizierung unterstützen.
- Sie sollten über ein CA-Zertifikat mit privatem Schlüssel und Fingerabdruck-Details verfügen.
- Sie sollten die Einweg-SSL-Konfiguration aktiviert haben.

  Weitere Informationen finden Sie unter "Abschnitt „CA-Zertifikat konfigurieren“."

- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-in-Hosts und dem SnapCenter-Server aktiviert haben.

  Umgebungen mit einigen Hosts oder Servern, die für die bidirektionale SSL-Kommunikation nicht aktiviert sind, werden nicht unterstützt.

Schritte

1. Um den Port zu binden, führen Sie die folgenden Schritte auf dem SnapCenter-Server-Host für SnapCenter IIS-Webserver-Port 8146 (Standard) und erneut für SMCore-Port 8145 (Standard) mit PowerShell-Befehlen durch.

   a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

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

      Beispiel:

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

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

b. Binden Sie das neu beschaffte CA-Zertifikat an den SnapCenter-Server und den SMCore-Port.

```
> $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>
```

Beispiel:

```
> $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. Um auf das CA-Zertifikat zuzugreifen, fügen Sie den Standard-IIS-Webserver-Benutzer „**IIS AppPool\SnapCenter**“ von SnapCenter in die Zertifikatsberechtigungsliste ein, indem Sie die folgenden Schritte ausführen, um auf das neu beschaffte CA-Zertifikat zuzugreifen.
   a. Rufen Sie die Microsoft Management Console (MMC) auf, und klicken Sie dann auf **Datei** > **SnapIn hinzufügen/entfernen**.
   b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
   c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
   d. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
   e. Wählen Sie das SnapCenter-Zertifikat aus.
   f. Um den Assistenten zum Hinzufügen von Benutzerberechtigungen zu starten\, klicken Sie mit der rechten Maustaste auf das CA-Zertifikat und wählen **Alle Aufgaben** > **Private Schlüssel verwalten**.
   g. Klicken Sie auf **Hinzufügen**, im Assistenten Benutzer und Gruppen auswählen ändern Sie den Speicherort in den lokalen Computernamen (ganz oben in der Hierarchie)
   h. Fügen Sie den Benutzer IIS AppPool\SnapCenter hinzu, geben Sie die vollen Kontrollberechtigungen ein.
3. Fügen Sie für die IIS-Berechtigung **CA-Zertifikat** den neuen DWORD-Registrierungsschlüssel-Eintrag im SnapCenter-Server über den folgenden Pfad hinzu:

Im Windows-Registrierungs-Editor, Traverse auf den unten genannten Pfad,

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

4. Erstellen Sie einen neuen DWORD-Registrierungsschlüsseleintrag im Kontext DER SCHANNEL-Registrierungskonfiguration.

```
SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
```

Konfigurieren Sie das SnapCenter-Windows-Plug-in für die bidirektionale SSL-Kommunikation

Sie sollten das SnapCenter-Windows-Plug-in für die bidirektionale SSL-Kommunikation mithilfe von PowerShell Befehlen konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass der Fingerabdruck des CA-Zertifikats verfügbar ist.

Schritte

1. Um den Port zu binden, führen Sie die folgenden Aktionen auf dem Windows-Plug-in-Host für SMCore-Port 8145 aus (Standard).

   a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

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

   Beispiel:

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

   b. Binden Sie das neu beschaffte CA-Zertifikat an den SMCore-Port.

   ```
   > $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>
   ```

   Beispiel:

   ```
   > $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
```

Aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Sie können die bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen SnapCenter Server auf Windows-Hosts und den Plug-ins mithilfe von PowerShell-Befehlen zu sichern.

Bevor Sie beginnen

Führen Sie die Befehle für alle Plug-ins und den SMCore-Agent zuerst und dann für den Server aus.

Schritte

1. Um die bidirektionale SSL-Kommunikation zu aktivieren, führen Sie die folgenden Befehle auf dem SnapCenter-Server für die Plug-ins, den Server und für jeden Agenten aus, für den die bidirektionale SSL-Kommunikation erforderlich ist.

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

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

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

2. Führen Sie den IIS-SnapCenter-Anwendungspool-Recyclingvorgang mit dem folgenden Befehl durch. `> Restart-WebAppPool -Name "SnapCenter"`
3. Starten Sie für Windows-Plug-ins den SMCore-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

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

Deaktivieren Sie die bidirektionale SSL-Kommunikation

Sie können die bidirektionale SSL-Kommunikation mithilfe von PowerShell Befehlen deaktivieren.

Über diese Aufgabe

- Führen Sie die Befehle für alle Plug-ins und den SMCore-Agent zuerst und dann für den Server aus.
- Wenn Sie die bidirektionale SSL-Kommunikation deaktivieren, werden das CA-Zertifikat und seine Konfiguration nicht entfernt.
- Um dem SnapCenter-Server einen neuen Host hinzuzufügen, müssen Sie die bidirektionale SSL-Verbindung für alle Plug-in-Hosts deaktivieren.
- NLB und F5 werden nicht unterstützt.

Schritte

1. Um die bidirektionale SSL-Kommunikation zu deaktivieren, führen Sie die folgenden Befehle auf dem SnapCenter-Server für alle Plug-in-Hosts und den SnapCenter-Host aus.

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

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

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

2. Führen Sie den IIS-SnapCenter-Anwendungspool-Recyclingvorgang mit dem folgenden Befehl durch. `> Restart-WebAppPool -Name "SnapCenter"`
3. Starten Sie für Windows-Plug-ins den SMCore-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

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

Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

Sie sollten die bidirektionale SSL-Kommunikation konfigurieren, um die gegenseitige Kommunikation zwischen SnapCenter-Server auf Linux-Host und den Plug-ins zu sichern.

Bevor Sie beginnen

- Sie sollten das CA-Zertifikat für den Linux-Host konfiguriert haben.
- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-in-Hosts und dem SnapCenter-Server aktiviert haben.

Schritte

1. Kopieren Sie **Certificate.pem** nach */etc/pki/Ca-Trust/source/Anchors/*.
2. Fügen Sie die Zertifikate in die Vertrauensliste Ihres Linux-Hosts ein.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Überprüfen Sie, ob die Zertifikate zur Vertrauensliste hinzugefügt wurden. `trust list | grep "<CN of your certificate>"`
4. Aktualisieren Sie **ssl_Certificate** und **ssl_Certificate_key** in der SnapCenter **nginx**-Datei und starten Sie neu.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Aktualisieren Sie den GUI-Link des SnapCenter-Servers.
6. Aktualisieren Sie die Werte der folgenden Schlüssel in **SnapManager.Web.UI.dll.config** unter _ /<installation path>/NetApp/snapcenter/SnapManagerWeb_ und **SMCoreServiceHost.dll.config** unter

/<installation path>/NetApp/snapcenter/SMCore.

- <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
- <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>

7. Starten Sie die folgenden Dienste neu.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. Vergewissern Sie sich, dass das Zertifikat an den SnapManager-Webport angeschlossen ist. `openssl s_client -connect localhost:8146 -brief`
9. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist. `openssl s_client -connect localhost:8145 -brief`
10. Kennwort für SPL-Keystore und Alias verwalten.
    a. Rufen Sie das SPL-Keystore-Standardpasswort ab, das dem Schlüssel **SPL_KEYSTORE_PASS** in der SPL-Eigenschaftsdatei zugewiesen wurde.
    b. Ändern Sie das Passwort für den Keystore. `keytool -storepasswd -keystore keystore.jks`
    c. Ändern Sie das Passwort für alle Aliase von privaten Schlüsseleinträgen. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Aktualisieren Sie dasselbe Passwort für den Schlüssel **SPL_KEYSTORE_PASS** in *spl.properties*.
    e. Starten Sie den Dienst neu.
11. Fügen Sie auf dem Plug-in-Linux-Host die Root- und Zwischenzertifikate im Keystore des SPL-Plug-ins hinzu.
    - `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. Überprüfen Sie die Einträge in keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
      ii. Benennen Sie bei Bedarf alle Alias um. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Aktualisieren Sie den Wert von **SPL_CERTIFICATE_ALIAS** in der Datei *spl.properties* mit dem Alias **Certificate.pfx**, der in *keystore.jks* gespeichert ist, und starten Sie den SPL-Dienst neu: `systemctl restart spl`
13. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist. `openssl s_client -connect localhost:8145 -brief`

Aktivieren Sie die SSL-Kommunikation auf Linux-Host

Sie können bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen SnapCenter Server auf Linux-Host und den Plug-ins mithilfe von PowerShell-Befehlen zu sichern.

Schritt

1. Führen Sie die folgenden Schritte aus, um die einfache SSL-Kommunikation zu aktivieren.
   a. Melden Sie sich bei der SnapCenter GUI an.
   b. Klicken Sie auf **Einstellungen** > **Globale Einstellungen** und wählen Sie **Zertifikatvalidierung auf dem SnapCenter-Server aktivieren**.
   c. Klicken Sie auf **Hosts** > **verwaltete Hosts** und wählen Sie den Plug-in-Host aus, für den Sie One-Way-SSL aktivieren möchten.
   d. Klicken Sie auf das  Symbol, und klicken Sie dann auf **Zertifikatvalidierung aktivieren**.
2. Aktivieren Sie die bidirektionale SSL-Kommunikation vom SnapCenter-Server-Linux-Host.
   - `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"}`

Konfiguration von Active Directory, LDAP und LDAPS

Registrieren Sie nicht vertrauenswürdige Active Directory-Domänen

Sie sollten das Active Directory beim SnapCenter-Server registrieren, um Hosts, Benutzer und Gruppen aus mehreren nicht vertrauenswürdigen Active Directory-Domänen zu verwalten.

Bevor Sie beginnen

LDAP- und LDAPS-Protokolle

- Sie können die nicht vertrauenswürdigen Active Directory-Domänen entweder über das LDAP- oder LDAPS-Protokoll registrieren.
- Sie sollten die bidirektionale Kommunikation zwischen den Plug-in-Hosts und dem SnapCenter-Server aktivieren.
- Die DNS-Auflösung sollte vom SnapCenter-Server zu den Plug-in-Hosts eingerichtet und umgekehrt werden.

LDAP-Protokoll

- Der vollständig qualifizierte Domänenname (FQDN) sollte vom SnapCenter-Server resolable sein.

  Sie können eine nicht vertrauenswürdige Domäne mit dem FQDN registrieren. Wenn der FQDN nicht vom SnapCenter-Server aus lösbar ist, können Sie sich mit einer IP-Adresse des Domänencontrollers registrieren, und dieser sollte vom SnapCenter-Server aus gelöst werden können.

LDAPS-Protokoll

- CA-Zertifikate sind für LDAPS erforderlich, um während der Active Directory-Kommunikation eine End-to-End-Verschlüsselung bereitzustellen.

"Konfigurieren Sie das CA-Client-Zertifikat für LDAPS"

- Domänencontroller Host-Namen (DCHostName) sollten über den SnapCenter Server erreichbar sein.

Über diese Aufgabe

- Sie können entweder die SnapCenter Benutzeroberfläche, PowerShell Cmdlets oder DIE REST API verwenden, um eine nicht vertrauenswürdige Domäne zu registrieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Globale Einstellungen**…
3. Klicken Sie auf der Seite Globale Einstellungen auf **Domäneneinstellungen**.
4. Klicken Sie hier + , um eine neue Domain zu registrieren.
5. Wählen Sie auf der Seite Neue Domäne registrieren entweder **LDAP** oder **LDAPS** aus.
   a. Wenn Sie **LDAP** auswählen, geben Sie die Informationen an, die zur Registrierung der nicht vertrauenswürdigen Domäne für LDAP erforderlich sind:

Für dieses Feld…	Tun Sie das…
Domain-Name	Geben Sie den NetBIOS-Namen für die Domäne an.
Domain-FQDN	Geben Sie den FQDN an und klicken Sie auf **Auflösen**.
IP-Adressen des Domänencontrollers	Wenn der Domain-FQDN nicht vom SnapCenter-Server resolbar ist, geben Sie eine oder mehrere IP-Adressen für den Domänencontroller an. Weitere Informationen finden Sie unter "Fügen Sie von der GUI eine Domänen-Controller-IP für eine nicht vertrauenswürdige Domäne hinzu".

   b. Wenn Sie **LDAPS** auswählen, geben Sie die Informationen an, die zur Registrierung der nicht vertrauenswürdigen Domäne für LDAPS erforderlich sind:

Für dieses Feld…	Tun Sie das…
Domain-Name	Geben Sie den NetBIOS-Namen für die Domäne an.
Domain-FQDN	Geben Sie den FQDN an.
Domänen-Controller-Namen	Geben Sie einen oder mehrere Domänencontroller-Namen an und klicken Sie auf **Auflösen**.

Für dieses Feld…	Tun Sie das…
IP-Adressen des Domänencontrollers	Wenn die Domänencontrollernamen nicht vom SnapCenter-Server behoben werden können, sollten Sie die DNS-Auflösungen beheben.

6. Klicken Sie auf **OK**.

Konfigurieren Sie IIS-Anwendungspools, um die Leseberechtigungen von Active Directory zu aktivieren

Sie können IIS (Internet Information Services) auf Ihrem Windows-Server so konfigurieren, dass ein benutzerdefiniertes Application Pool-Konto erstellt wird, wenn Sie Active Directory-Leseberechtigungen für SnapCenter aktivieren müssen.

Schritte

1. Öffnen Sie den IIS-Manager auf dem Windows-Server, auf dem SnapCenter installiert ist.
2. Klicken Sie im linken Navigationsbereich auf **Anwendungspools**.
3. Wählen Sie in der Liste Anwendungspools SnapCenter aus, und klicken Sie dann im Bereich Aktionen auf **Erweiterte Einstellungen**.
4. Wählen Sie Identität aus, und klicken Sie dann auf **…**, um die Identität des SnapCenter-Anwendungspools zu bearbeiten.
5. Geben Sie im Feld Benutzerdefiniertes Konto einen Domänenbenutzer oder Domänenadministratornamen mit der Berechtigung Active Directory Lesen ein.
6. Klicken Sie auf OK.

   Das benutzerdefinierte Konto ersetzt das integrierte ApplicationPoolIdentity-Konto für den SnapCenter-Anwendungspool.

Konfigurieren Sie das CA-Client-Zertifikat für LDAPS

Sie sollten das CA-Clientzertifikat für LDAPS auf dem SnapCenter-Server konfigurieren, wenn die Windows Active Directory-LDAPS mit den CA-Zertifikaten konfiguriert ist.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.

6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Auf der zweiten Seite des Assistenten	Klicken Sie auf **Durchsuchen**, wählen Sie das *Root-Zertifikat* und klicken Sie auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

7. Wiederholen Sie die Schritte 5 und 6 für die Zwischenzertifikate.