Installation von SnapCenter Server

SnapCenter Software 4.6

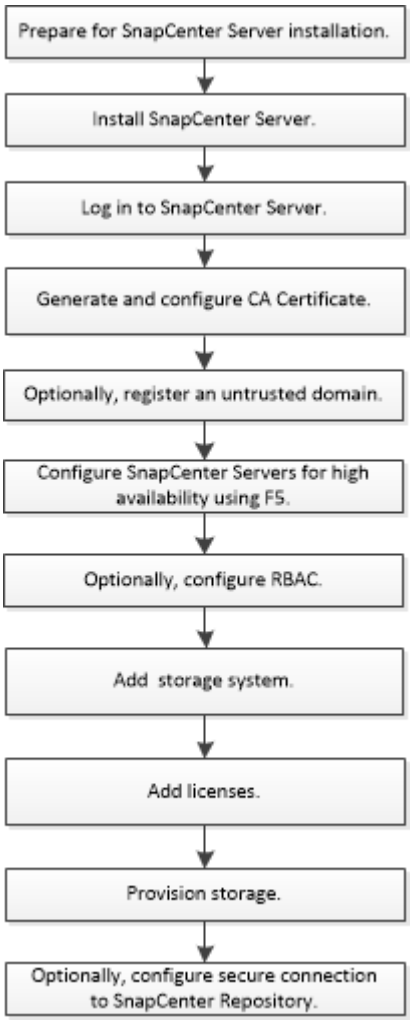
NetApp
September 29, 2025

Inhalt

Installation von SnapCenter Server

Installations-Workflow

Der Workflow zeigt die verschiedenen Aufgaben, die für die Installation und Konfiguration des SnapCenter-Servers erforderlich sind.



Bereiten Sie sich auf die Installation des SnapCenter-Servers vor

Anforderungen an Domäne und Arbeitsgruppe

Der SnapCenter-Server kann auf Systemen installiert werden, die sich entweder in einer Domäne oder in einer Arbeitsgruppe befinden. Der für die Installation verwendete Benutzer muss bei Arbeitsgruppen und Domänen über Administratorrechte auf dem Computer verfügen.

Für die Installation von SnapCenter Server und SnapCenter Plug-ins auf Windows Hosts sollten Sie einen der folgenden Schritte verwenden:

- **Active Directory-Domäne**

  Sie müssen einen Domänenbenutzer 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

Vor der Installation des SnapCenter Servers sollten Sie mit den Platz- und Größenanforderungen vertraut sein. Sie sollten auch die verfügbaren System- und Sicherheitsupdates anwenden.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Es werden nur englische, deutsche, japanische und vereinfachte chinesische Versionen der Betriebssysteme unterstützt. Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".
Minimale CPU-Anzahl	4 Kerne
Mind. RAM	8 GB Der MySQL Server Pufferpool nutzt 20 Prozent des gesamten RAM.
Minimaler Festplattenspeicher für die SnapCenter-Serversoftware und Protokolle	4 GB Wenn sich das SnapCenter-Repository auf demselben Laufwerk befindet, auf dem SnapCenter-Server installiert ist, wird empfohlen, 10 GB zu verwenden.

Element	Anforderungen
Minimaler Festplattenspeicher für das SnapCenter-Repository	6 GB HINWEIS: Wenn der SnapCenter-Server auf demselben Laufwerk installiert ist, auf dem das SnapCenter-Repository installiert ist, wird empfohlen, 10 GB zu verwenden.
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.5.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

SAN-Host-Anforderungen

Wenn Ihr SnapCenter Host Teil einer FC-/iSCSI-Umgebung ist, müssen Sie möglicherweise zusätzliche Software auf dem System installieren, um den Zugriff auf ONTAP Storage zu ermöglichen.

SnapCenter umfasst keine Host Utilities oder DSM. Wenn Ihr SnapCenter Host Teil einer SAN-Umgebung ist, müssen Sie eventuell die folgende Software installieren und konfigurieren:

- Host Utilities

  Die Host Utilities unterstützen FC und iSCSI, und es ermöglicht Ihnen die Verwendung von MPIO auf Ihren Windows Servern. Weitere Informationen finden Sie unter "Host Utilities-Dokumentation".

- Microsoft DSM für Windows MPIO

  Diese Software arbeitet mit Windows MPIO-Treibern für das Management mehrerer Pfade zwischen NetApp und Windows Host-Computern zusammen.

  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".

Unterstützte Storage-Systeme und Applikationen

Sie sollten die unterstützten Storage-Systeme, Applikationen und Datenbanken kennen.

- SnapCenter unterstützt ONTAP 8.3.0 und neuere Versionen für den Schutz Ihrer Daten.
- SnapCenter unterstützt Amazon FSX für NetApp ONTAP, um Ihre Daten vor der SnapCenter Software 4.5

P1-Patch-Veröffentlichung zu schützen.

Wenn Sie Amazon FSX für NetApp ONTAP verwenden, stellen Sie sicher, dass die SnapCenter Server Host-Plug-ins auf 4.5 P1 oder höher aktualisiert werden, um Datensicherungsprozesse zu auszuführen.

Informationen zu Amazon FSX für NetApp ONTAP finden Sie unter "Dokumentation zu Amazon FSX für NetApp ONTAP".

- SnapCenter unterstützt den Schutz verschiedener Applikationen und Datenbanken.

  Ausführliche Informationen zu den unterstützten Anwendungen und Datenbanken finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Unterstützte Browser

SnapCenter-Software kann auf mehreren Browsern verwendet werden.

- Chrom

  Wenn sie v66 verwenden, kann das SnapCenter GUI möglicherweise nicht gestartet werden.

- Internet Explorer

  Die SnapCenter UI wird nicht richtig geladen, wenn Sie IE 10 oder frühere Versionen verwenden. Sie sollten ein Upgrade auf IE 11 durchführen.

  - Es wird nur die Standardsicherheit unterstützt.

    Wenn Sie Änderungen an den Sicherheitseinstellungen von Internet Explorer vornehmen, treten erhebliche Probleme bei der Anzeige des Browsers auf.

  - Die Kompatibilitätsansicht für Internet Explorer muss deaktiviert sein.

- Microsoft Edge

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Verbindungs- und Portanforderungen

Stellen Sie sicher, dass die Verbindungs- und Ports-Anforderungen erfüllt sind, bevor Sie die SnapCenter Server- und Applikations- oder Datenbank-Plug-ins installieren.

- Anwendungen können einen Port nicht gemeinsam nutzen.

  Jeder Port muss der entsprechenden Applikation zugeordnet sein.

- Bei anpassbaren Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.

  Sie können einen Plug-in-Port nach der Installation mithilfe des Assistenten zum Ändern von Hosts ändern.

- 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.

Typ des Ports	Standardport
SnapCenter-Port	8146 (HTTPS), bidirektional, anpassbar, wie unter der URL *https://server:8146* Wird für die Kommunikation zwischen dem SnapCenter-Client (dem SnapCenter-Benutzer) und dem SnapCenter-Server verwendet. Wird auch zur Kommunikation von den Plug-in-Hosts mit dem SnapCenter-Server verwendet. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
SnapCenter SMCore-Kommunikations-Port	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen dem SnapCenter-Server und den Hosts verwendet, auf denen die SnapCenter-Plug-ins installiert sind. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
MySQL-Anschluss	3306 (HTTPS), bidirektional Der Port wird für die Kommunikation zwischen SnapCenter und der MySQL Repository Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter-Server zum MySQL-Server erstellen. "Weitere Informationen ."

Typ des Ports	Standardport
Windows Plug-in-Hosts	135, 445 (TCP) Neben den Ports 135 und 445 sollte auch der von Microsoft festgelegte dynamische Portbereich geöffnet sein. Remote-Installationsvorgänge verwenden den Windows Management Instrumentation (WMI)-Dienst, der diesen Portbereich dynamisch durchsucht. Informationen zum unterstützten dynamischen Portbereich finden Sie unter "Serviceübersicht und Netzwerkanschlussanforderungen für Windows" Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Um Plug-in-Binärdateien auf Windows-Plug-in-Hosts zu übertragen, müssen die Ports nur auf dem Plug-in-Host geöffnet sein, und sie können nach der Installation geschlossen werden.
Linux- oder AIX-Plug-in-Hosts	22 (SSH) Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Die Ports werden von SnapCenter verwendet, um Plug-in-Paketbinärdateien auf Linux- oder AIX-Plug-in-Hosts zu kopieren. Sie sollten von der Firewall oder von iptables geöffnet oder ausgeschlossen sein.
SnapCenter-Plug-ins-Paket für Windows, SnapCenter-Plug-ins-Paket für Linux oder SnapCenter-Plug-ins-Paket für AIX	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-ins-Paket installiert ist. Der Kommunikationspfad muss auch zwischen der SVM-Management-LIF und dem SnapCenter-Server offen sein. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows" Oder "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."

Typ des Ports	Standardport
SnapCenter Plug-in für Oracle Database	27216, anpassbar Der Standard-JDBC-Port wird vom Plug-in für Oracle für die Verbindung mit der Oracle-Datenbank verwendet. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."
Benutzerdefinierte Plug-ins für SnapCenter	9090 (HTTPS), fest Dies ist ein interner Port, der nur auf dem benutzerdefinierten Plug-in-Host verwendet wird. Es ist keine Firewall-Ausnahme erforderlich. Die Kommunikation zwischen dem SnapCenter-Server und benutzerdefinierten Plug-ins wird über Port 8145 geleitet.
ONTAP-Cluster oder SVM-Kommunikations-Port	443 (HTTPS), bidirectional80 (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.
SnapCenter-Plug-in für SAP HANA-Datenbank vCode Zauber-Checkerports	3instance_number13 or 3instance_number15, HTTP oder HTTPS, bidirektional und anpassbar 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. Beispielsweise ist 32013 die Portnummer für die Instanz 20 und 31015 die Portnummer für Instanz 10. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."

Typ des Ports	Standardport
Kommunikations-Port des Domänencontrollers	In der Microsoft-Dokumentation finden Sie Informationen zu den Ports, die in der Firewall auf einem Domänencontroller geöffnet werden sollen, damit die Authentifizierung ordnungsgemäß funktioniert. Es ist erforderlich, die erforderlichen Microsoft-Ports auf dem Domänen-Controller zu öffnen, damit der SnapCenter-Server, Plug-in-Hosts oder andere Windows-Client die Benutzer authentifizieren kann.

Informationen zum Ändern der Portdetails finden Sie unter "Ändern Sie die Plug-in-Hosts".

SnapCenter-Lizenzen

Für die Datensicherung von Applikationen, Datenbanken, Filesystemen und Virtual Machines benötigt SnapCenter mehrere Lizenzen. Die Art der installierten SnapCenter Lizenzen hängt von Ihrer Storage-Umgebung und den gewünschten Funktionen ab.

Lizenz	Bei Bedarf
SnapCenter Standard Controller-basiert	Erforderlich für FAS und AFF Bei der SnapCenter Standard Lizenz handelt es sich um eine Controller-basierte Lizenz und ist im Rahmen des Premium Bundle enthalten. Wenn Sie die Lizenz für die SnapManager Suite besitzen, erhalten Sie auch die Standardlizenz von SnapCenter. Wenn Sie SnapCenter auf Testbasis mit FAS oder AFF Storage installieren möchten, wenden Sie sich an den Vertriebsmitarbeiter, um eine Evaluierungslizenz für das Premium Bundle zu erhalten. SnapCenter ist auch als Teil des Datensicherungs-Bundles verfügbar. Wenn Sie A400 oder höher erworben haben, sollten Sie ein Datensicherungs-Bundle erwerben.

Lizenz	Bei Bedarf
Kapazitätsbasierte SnapCenter Lösung	Erforderlich für ONTAP Select und Cloud Volumes ONTAP Als Cloud Volumes ONTAP- oder ONTAP Select-Kunde müssen Sie eine kapazitätsbasierte Lizenz pro TB erwerben, die auf den von SnapCenter gemanagten Daten basiert. Standardmäßig liefert SnapCenter eine integrierte kapazitätsbasierte SnapCenter-Testlizenz mit 90 TB und 100 Tagen im Umfang von TB aus. Weitere Informationen erhalten Sie von dem Vertriebsmitarbeiter.
SnapMirror oder SnapVault	ONTAP Wenn die Replizierung in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault Lizenz erforderlich.
SnapRestore	Für die Wiederherstellung und Überprüfung von Backups erforderlich. Auf primären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen. • Erforderlich auf SnapMirror Zielsystemen für die Remote-Verifizierung
FlexClone	Die für das Klonen von Datenbanken und Verifizierungsvorgängen erforderlich sind. Auf primären und sekundären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um Klone aus dem sekundären Vault Backup zu erstellen. • Erforderlich auf SnapMirror Zielsystemen, um Klone aus dem sekundären SnapMirror Backup zu erstellen.

Lizenz	Bei Bedarf
Protokolle	• ISCSI- oder FC-Lizenz für LUNs • CIFS-Lizenz für SMB-Freigaben • NFS-Lizenz für NFS-Typ VMDKs • ISCSI- oder FC-Lizenz für VMFS-VMDKs des Typs VMDK Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.
SnapCenter-Standardlizenzen (optional)	Sekundäre Ziele Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen nicht für sekundäre Ziele aktiviert sind, können Sie nach einem Failover-Vorgang SnapCenter nicht für ein Backup von Ressourcen auf dem sekundären Ziel verwenden. Allerdings ist eine FlexClone Lizenz für sekundäre Ziele erforderlich, um Klon- und Verifizierungsvorgänge durchzuführen.

Lizenzen für SnapCenter Advanced- und SnapCenter-NAS-Fileservices sind veraltet und sind nicht mehr verfügbar.

Sie sollten eine oder mehrere SnapCenter Lizenzen installieren. Informationen zum Hinzufügen von Lizenzen finden Sie unter "Controller-basierte SnapCenter Standard-Lizenzen hinzufügen" Oder "Hinzufügen von kapazitätsbasierten SnapCenter Standard-Lizenzen".

Single Mailbox Recovery-Lizenzen (SMBR

Wenn Sie für das Management von Microsoft Exchange Server Datenbanken und Single Mailbox Recovery (SMBR) mit dem SnapCenter Plug-in für Exchange arbeiten, benötigen Sie eine zusätzliche Lizenz für SMBR, die separat in Abhängigkeit von der Benutzer-Mailbox erworben werden muss.

Die Einstellung der Verfügbarkeit für NetApp Single Mailbox Recovery (EOA) steht am 12. Mai 2023 fest. Weitere Informationen finden Sie unter "CPC-00507". NetApp unterstützt Kunden, die für den Zeitraum der Support-Berechtigung Mailbox-Kapazität, Wartung und Support erworben haben, weiterhin über die am 24. Juni 2020 eingeführten Marketing-Teilenummern.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. OnTrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können von Ontrack (bis licensingteam@ontrack.com) neue Ontrack PowerControls Softwarelizenzen und Ontrack PowerControls Wartungs- und Supportverlängerungen für eine granulare Mailbox-Recovery nach dem EOA-Datum vom 12. Mai 2023 beziehen.

Authentifizierungsmethoden für Ihre Anmeldedaten

Je nach Anwendung oder Umgebung verwenden Anmeldeinformationen unterschiedliche Authentifizierungsmethoden. Anmeldedaten authentifizieren Benutzer, sodass sie SnapCenter-Vorgänge ausführen können. Zum Installieren von Plug-ins und einem anderen Satz für Datensicherungsvorgänge sollten Sie einen Satz von Anmeldeinformationen erstellen.

Windows Authentifizierung

Die Windows-Authentifizierungsmethode authentifiziert sich gegen Active Directory. Für die Windows-Authentifizierung wird Active Directory außerhalb von SnapCenter eingerichtet. SnapCenter authentifiziert sich ohne zusätzliche Konfiguration. Sie benötigen Windows-Anmeldedaten, um Aufgaben wie das Hinzufügen von Hosts, die Installation von Plug-in-Paketen und die Planung von Jobs auszuführen.

Nicht vertrauenswürdige Domänenauthentifizierung

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen unter Verwendung von Benutzern und Gruppen, die zu nicht vertrauenswürdigen Domänen gehören. Damit die Authentifizierung erfolgreich ist, sollten Sie die nicht vertrauenswürdigen Domains bei SnapCenter registrieren.

Authentifizierung für lokale Arbeitsgruppen

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen für Benutzer und Gruppen lokaler Arbeitsgruppen. Die Windows-Authentifizierung für Benutzer und Gruppen lokaler Arbeitsgruppen findet zum Zeitpunkt der Erstellung von Windows-Anmeldeinformationen nicht statt, wird jedoch verschoben, bis die Hostregistrierung und andere Hostvorgänge durchgeführt werden.

SQL Server-Authentifizierung

Die SQL-Authentifizierungsmethode authentifiziert sich anhand einer SQL Server-Instanz. Das bedeutet, dass eine SQL Server-Instanz in SnapCenter erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-in-Pakete installieren und Ressourcen aktualisieren. Sie benötigen die SQL Server-Authentifizierung für Vorgänge wie die Planung auf SQL Server oder die Ermittlung von Ressourcen.

Linux-Authentifizierung

Die Linux-Authentifizierungsmethode authentifiziert sich bei einem Linux-Host. Sie benötigen die Linux-Authentifizierung während des ersten Schritts des Hinzufügens des Linux-Hosts und der Remote-Installation des SnapCenter-Plug-ins-Pakets für Linux über die SnapCenter-Benutzeroberfläche.

AIX Authentifizierung

Die AIX-Authentifizierungsmethode authentifiziert sich gegen einen AIX-Host. Sie benötigen eine AIX-Authentifizierung während des ersten Schritts, in dem Sie den AIX-Host hinzufügen und das SnapCenter Plug-ins Paket für AIX Remote von der SnapCenter-Benutzeroberfläche aus installieren.

Oracle-Datenbankauthentifizierung

Die Oracle-Datenbankauthentifizierung authentifiziert sich anhand einer Oracle-Datenbank. Sie benötigen eine Oracle-Datenbankauthentifizierung, um Vorgänge in der Oracle-Datenbank auszuführen, wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist. Daher sollten Sie vor dem Hinzufügen

von Oracle-Datenbankberechtigungen einen Oracle-Benutzer in der Oracle-Datenbank mit sysdba-Berechtigungen erstellen.

Oracle ASM Authentifizierung

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich anhand einer Oracle Automatic Storage Management (ASM)-Instanz. Wenn Sie auf die Oracle ASM-Instanz zugreifen müssen und wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist, benötigen Sie eine Oracle ASM-Authentifizierung. Daher sollten Sie vor dem Hinzufügen einer Oracle ASM-Berechtigung einen Oracle-Benutzer mit sysasm-Berechtigungen in der ASM-Instanz erstellen.

RMAN-Katalogauthentifizierung

Die Authentifizierungsmethode des RMAN-Katalogs authentifiziert sich mit der Oracle Recovery Manager (RMAN)-Katalogdatenbank. Wenn Sie einen externen Katalogmechanismus konfiguriert und Ihre Datenbank in der Katalogdatenbank registriert haben, müssen Sie die RMAN-Katalogauthentifizierung hinzufügen.

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).

- **Anmeldeinformationen**

  - 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.

Installieren Sie den SnapCenter-Server

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.

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

Was Sie brauchen

- 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:\"`

Melden Sie sich 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.

Was Sie brauchen

- 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.

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. Der "SnapCenter Software Cmdlet Referenzhandbuch" Enthält 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.

Ergebnisse

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 ."

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 Sie das CA-Zertifikat

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.

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**.
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**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
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, *.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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$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**.

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.

Was Sie brauchen

- 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 auf die verweisen "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.

- Zeigt 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.

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.

Was Sie brauchen

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 Auf + 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**.

Für dieses Feld…	Tun Sie das…
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**.
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 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.

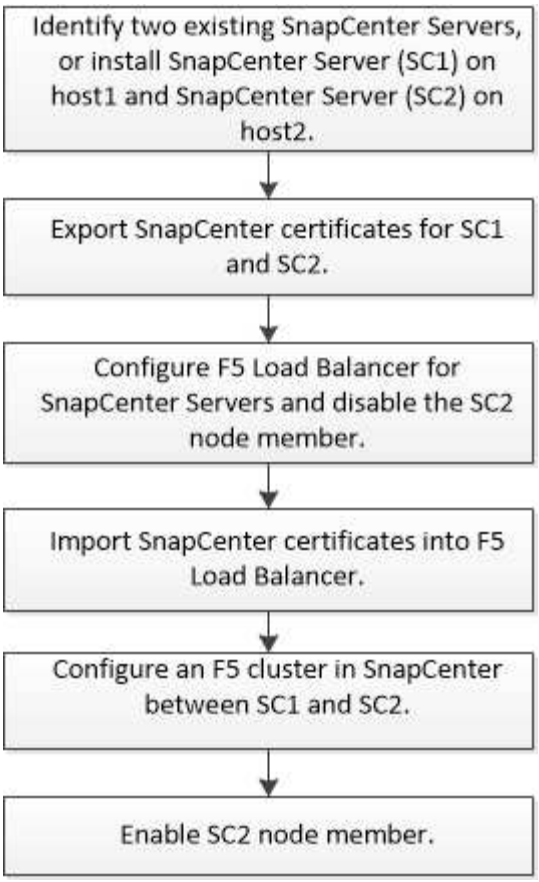
Konfiguration Der Hochverfügbarkeit

Konfiguration von SnapCenter-Servern für Hochverfügbarkeit mit F5

Zur Unterstützung von Hochverfügbarkeit (High Availability, HA) in SnapCenter kann der F5 Load Balancer installiert werden. 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.

Wenn Sie von SnapCenter 4.2.x aktualisiert haben und zuvor den Netzwerklastausgleich (NLB) verwendet haben, können Sie diese Konfiguration weiterhin verwenden oder zu F5 wechseln.

Das Workflow-Image führt die Schritte für die Konfiguration von SnapCenter-Servern für hohe Verfügbarkeit mit F5 Load Balancer auf. Detaillierte Anweisungen 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".

Zusätzliche F5 Konfigurationsinformationen

- 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 Node hinzufügen, der teilweise vom NLB- oder F5-Knoten aufgelöst wird, und wenn der SnapCenter-Knoten nicht auf diesen Node zugreifen kann, wechselt die SnapCenter-Host-Seite häufig zwischen Hosts aus und dem laufenden Status. Um dieses Problem zu beheben, sollten Sie sicherstellen, dass beide SnapCenter-Knoten den Host in NLB oder F5-Knoten lösen können.

Konfigurieren Sie den Microsoft Network Load Balancer manuell

Sie können Microsoft Network Load Balancing (NLB) für die Einrichtung der SnapCenter-

Hochverfügbarkeit konfigurieren. Ab SnapCenter 4.2 sollten Sie NLB manuell außerhalb der SnapCenter-Installation konfigurieren, um eine hohe Verfügbarkeit zu gewährleisten.

Weitere Informationen zum Konfigurieren des Netzwerklastverteilung (Network Load Balancing, NLB) mit SnapCenter finden Sie unter "So konfigurieren Sie NLB mit SnapCenter".

SnapCenter 4.1.1 oder eine frühere Version unterstützte die Konfiguration des Network Load Balancing (NLB) bei der Installation von SnapCenter.

Für hohe Verfügbarkeit von NLB auf F5 umschalten

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 verweisen "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 verweisen "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".

Exportieren von SnapCenter-Zertifikaten

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**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
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.

Ergebnisse

Zertifikate werden im .pfx-Format exportiert.

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

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.

Was Sie brauchen

- 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.

  Ab SnapCenter 4.5 können Sie nur die folgenden Sonderzeichen in Benutzernamen und Gruppennamen enthalten: Leerzeichen ( ), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:). Wenn Sie eine Rolle verwenden möchten, die Sie in einer früheren Version von SnapCenter mit diesen Sonderzeichen erstellt haben, können Sie die Validierung des Rollennamens deaktivieren, indem Sie in der Datei Web.config, in der die SnapCenter WebApp installiert ist, den Wert des Parameters 'ableSQLInjectionValidation' auf true ändern. Nachdem Sie den Wert geändert haben, müssen Sie den Dienst nicht neu starten.

- 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 Snapshot Kopien replizieren möchten, müssen Sie dem Benutzer, der den Vorgang durchführt, die Storage-Verbindung für das Quell- und 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.

Für dieses Feld…	Tun Sie das…
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.

Erstellen Sie eine Rolle

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

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

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 auf der Seite Rolle hinzufügen einen Namen und eine Beschreibung für die neue Rolle an.

   Ab SnapCenter 4.5 können Sie nur die folgenden Sonderzeichen in Benutzernamen und Gruppennamen enthalten: Leerzeichen ( ), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:). Wenn Sie eine Rolle verwenden möchten, die Sie in einer früheren Version von SnapCenter mit diesen Sonderzeichen erstellt haben, können Sie die Validierung des Rollennamens deaktivieren, indem Sie in der Datei Web.config, in der die SnapCenter WebApp installiert ist, den Wert des Parameters 'ableSQLInjectionValidation' auf true ändern. Nachdem Sie den Wert geändert haben, müssen Sie den Dienst nicht neu starten.

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 ONTAP RBAC-Rolle hinzu

Sie können mit den Sicherheits-Login-Befehlen eine ONTAP RBAC-Rolle hinzufügen, wenn auf Ihren Storage-Systemen Clustered ONTAP ausgeführt wird.

Was Sie brauchen

- Bevor Sie eine ONTAP RBAC-Rolle für Storage-Systeme mit Clustered ONTAP erstellen, müssen Sie Folgendes angeben:
  - Die Aufgabe (oder Aufgaben), die Sie ausführen möchten
  - Die zum Ausführen dieser Aufgaben erforderlichen Berechtigungen
- Zum Konfigurieren einer RBAC-Rolle müssen Sie die folgenden Aktionen durchführen:
  - 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.
  - Sie können Ihre Konfiguration abhängig davon, ob Ihre SnapCenter Plug-ins für das gesamte Cluster mit der Cluster Administrator-IP verbunden oder direkt mit einer SVM im Cluster verbunden sind.

Über diese Aufgabe

Um die Konfiguration dieser Rollen auf Storage-Systemen zu vereinfachen, können Sie das RBAC Benutzer Creator für Data ONTAP Tool verwenden, das im NetApp Communities Forum verfügbar ist.

Dieses Tool verarbeitet automatisch die korrekte Einrichtung der ONTAP-Berechtigungen. Beispielsweise fügt das Tool RBAC Benutzer Creator für Data ONTAP automatisch die Berechtigungen in der richtigen Reihenfolge ein, sodass zuerst die Berechtigungen für alle Zugriffe 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 zu einem späteren Zeitpunkt ein Upgrade von SnapCenter oder ONTAP durchführen, sollten Sie das Tool RBAC User Creator für Data ONTAP 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".

Aus Konsistenzgründen bezieht sich die SnapCenter-Dokumentation auf die Rollen als Verwenden von Berechtigungen. Die OnCommand System Manager GUI verwendet den Begriff „`attribut`“ anstatt „`` Privilege“. Beim Einrichten von ONTAP RBAC-Rollen bedeuten beide Begriffe dasselbe.

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

"lun igroup add" -access all

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

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

"volume qtree show" -access all

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

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`

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 -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 stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun move-in-volume" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all

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

"volume file clone create" -access all

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

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

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.

Storage-Systeme hinzufügen

Sie sollten das Storage-System einrichten, mit dem SnapCenter Zugriff auf ONTAP Storage oder Amazon FSX für NetApp ONTAP erhalten, um Datensicherungs- und Bereitstellungsvorgänge durchzuführen.

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.

Was Sie brauchen

- 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.

- Falls Sie Snapshot Kopien zu einem SnapMirror Ziel oder einem SnapVault Ziel replizieren möchten, müssen Sie Storage-Systemverbindungen für die Ziel-SVM oder das Ziel-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. Speichersystemnamen, die nicht den Domainnamen enthalten, müssen 15 oder weniger Zeichen haben, und die Namen müssen resolable sein. 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.

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

      Der Standardport 443 funktioniert in der Regel.

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

      Der Standardwert ist 60 Sekunden.

   e. 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.
   f. Klicken Sie Auf **Speichern**.
5. Klicken Sie Auf **Absenden**.

Ergebnisse

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
enable -noteto enable
```

Der SVM-Administrator hat keinen Zugriff auf AutoSupport.

Controller-basierte SnapCenter Standard-Lizenzen hinzufügen

Wenn Sie FAS oder AFF Storage Controller verwenden, ist eine Controller-basierte SnapCenter Standard-Lizenz 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 aktiviert, indem sie direkt zum FAS oder AFF Storage Controller hinzugefügt wird. Dazu wird entweder der ONTAP System Manager oder die Storage-Cluster-Befehlszeile verwendet

  Sie geben keine Lizenzinformationen in der SnapCenter GUI für die Controller-basierten SnapCenter Lizenzen ein.

- Gesperrt an die Seriennummer des Controllers

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

Voraussetzungen für das Hinzufügen einer Controller-basierten Lizenz

Bevor Sie eine Controller-basierte Lizenz hinzufügen, sollten Sie überprüfen, ob die SnapManager Suite-Lizenz installiert ist, die auf dem Controller installierten Lizenzen identifizieren, die Seriennummer des Controllers abrufen und die Seriennummer der Controller-basierten Lizenz abrufen.

Überprüfen Sie, ob die SnapManager Suite-Lizenz installiert ist

Mit der SnapCenter GUI können Sie anzeigen, ob eine Lizenz der SnapManager Suite auf primären FAS oder AFF Storage-Systemen installiert ist, und ermitteln, welche Storage-Systeme möglicherweise Lizenzen der SnapManager Suite benötigen. Lizenzen der SnapManager Suite gelten nur für FAS und AFF SVMs oder Cluster auf primären Storage-Systemen.

Wenn Sie auf Ihrem Controller bereits eine Lizenz für die SnapManager Suite besitzen, wird die Controller-basierte SnapCenter Standard-Lizenzberechtigung automatisch bereitgestellt. Die Namen SnapManagerSuite Lizenz und SnapCenter Standard Controller-basierte Lizenz werden austauschbar verwendet, aber sie beziehen sich auf dieselbe Lizenz.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
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 auf den Cluster-Namen klicken, werden im Abschnitt Storage Virtual Machines alle SVMs, die Teil des Clusters sind, 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 Lizenz der SnapManager Suite auf einem primären FAS oder AFF Speichersystem installiert ist.
   - Zeigt an, dass keine SnapManager Suite-Lizenz auf einem primären FAS oder AFF-Speichersystem installiert ist.
   - Nicht zutreffend. Dies zeigt an, dass keine Lizenz für die SnapManager Suite gilt, da der Speicher-Controller auf Cloud Volumes ONTAP-, ONTAP Select- oder sekundären Speicherplattformen ausgeführt wird.

Identifizieren Sie die auf dem Controller installierten Lizenzen

Mit der ONTAP-Befehlszeile können Sie alle auf dem Controller installierten Lizenzen anzeigen. Sie sollten ein Cluster-Administrator auf dem FAS oder AFF System sein.

Die Controller-basierte SnapCenter Standard-Lizenz wird auf dem Controller als SnapManagerSuite-Lizenz angezeigt.

Schritte

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

```
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.

Rufen Sie die Seriennummer des Controllers ab

Sie benötigen die Controller-Seriennummer zum Abrufen der Seriennummer Ihrer Controller-basierten Lizenz. Sie können die Seriennummer des Controllers über die ONTAP-Befehlszeile abrufen. Sie sollten ein Cluster-Administrator auf dem FAS oder AFF System sein.

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.

```
cluster1::> system show -instance

Node: fas8080-41-42-01
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.

Rufen Sie die Seriennummer der Controller-basierten Lizenz ab

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

Was Sie brauchen

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

  Wenn Sie keine gültigen Anmeldedaten eingeben, werden keine Informationen für Ihre Suche zurückgegeben.

- Sie sollten die Controller-Seriennummer angeben.

Schritte

1. Loggen Sie sich auf der NetApp Support Site unter ein "mysupport.netapp.com".
2. Navigieren Sie zu **Systems** > **Softwarelizenzen**.
3. Stellen Sie im Bereich „Selection Criteria“ (Auswahlkriterien) sicher, dass die Seriennummer (auf der Rückseite des Geräts) ausgewählt ist, geben Sie die Seriennummer des Controllers ein und klicken Sie dann auf **Go!**.

   Eine Liste der Lizenzen für den angegebenen Controller wird angezeigt.

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

Hinzufügen einer Controller-basierten Lizenz

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

Was Sie brauchen

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

Über diese Aufgabe

Wenn Sie SnapCenter als Testlizenz mit FAS oder AFF Storage installieren möchten, können Sie eine Evaluierungslizenz für das Premium Bundle erhalten, 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
```

Entfernen Sie die Testlizenz

Wenn Sie eine Controller-basierte SnapCenter Standard-Lizenz verwenden und die kapazitätsbasierte Testlizenz entfernen müssen (Seriennummer mit „50“ endet), 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. Wenn Sie eine kapazitätsbasierte SnapCenter-Standardlizenz erworben und in die SnapCenter-Benutzeroberfläche hinzugefügt haben, wird die Testlizenz automatisch überschrieben.

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 Verbindungssitzung mit dem SnapCenter-Server für ein SnapCenterAdmin-Konto zu initiieren.
   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';
```

Hinzufügen von kapazitätsbasierten SnapCenter Standard-Lizenzen

Sie verwenden eine SnapCenter Standardkapazitätslizenz zum Schutz von Daten auf ONTAP Select und Cloud Volumes ONTAP Plattformen.

Die Lizenz weist folgende Merkmale auf:

- Bestehend aus einer neunstelligen Seriennummer im Format 51xxxxxxx

  Sie verwenden die Lizenzseriennummer und gültige Anmeldedaten für die NetApp Support Site, um die Lizenz mithilfe der SnapCenter GUI zu aktivieren.

- Die Lösung ist als separate, unbefristete Lizenz verfügbar, wobei die Kosten entweder auf Basis der verwendeten Storage-Kapazität oder der Größe der zu sichernden Daten, je nachdem, welcher Wert

niedriger ist und die Daten von SnapCenter gemanagt werden

- Verfügbar pro Terabyte

  Sie erhalten beispielsweise eine kapazitätsbasierte Lizenz für 1 TB, 2 TB, 4 TB usw.

- Verfügbar als 90-Tage-Testlizenz mit 100 TB Kapazitätsberechtigung

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

Voraussetzungen für das Hinzufügen kapazitätsbasierter Lizenz

Bevor Sie eine kapazitätsbasierte Lizenz hinzufügen, sollten Sie die Kapazitätsanforderungen berechnen, die Seriennummer der kapazitätsbasierten Lizenz abrufen und optional eine Lizenzdatei generieren.

Berechnen der Kapazitätsanforderungen

Bevor Sie eine kapazitätsbasierte SnapCenter Lizenz erhalten, sollten Sie die Kapazitätsmenge auf einem Host berechnen, der von SnapCenter gemanagt werden soll.

Sie sollten ein Cluster-Administrator auf dem Cloud Volumes ONTAP oder ONTAP Select System sein.

Über diese Aufgabe

SnapCenter berechnet die tatsächlich genutzte Kapazität. Wenn die Größe des Dateisystems oder der Datenbank 1 TB beträgt, aber nur 500 GB Speicherplatz verwendet wird, berechnet SnapCenter 500 GB der verwendeten Kapazität. Die Volume-Kapazität wird nach der Deduplizierung und Komprimierung berechnet und basiert auf der gesamten verwendeten Kapazität des Volume.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim NetApp Controller ein.
2. Um die verwendete Volume-Kapazität anzuzeigen, geben Sie den Befehl ein.

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

2   entries were displayed.
```

   Die insgesamt verwendete Kapazität für die beiden Volumes beträgt weniger als 5 TB. Wenn Sie also alle 5 TB Daten sichern möchten, benötigen Sie die SnapCenter-Mindestlizenz 5, die auf Kapazität basiert.

   Wenn Sie jedoch nur 2 TB der insgesamt genutzten Kapazität von 5 TB schützen möchten, können Sie eine kapazitätsbasierte Lizenz von 2 TB erwerben.

Rufen Sie die Seriennummer der kapazitätsbasierten Lizenz ab

Ihre SnapCenter kapazitätsbasierte Lizenz-Seriennummer steht Ihnen in der Bestellbestätigung oder im Dokumentationspaket zur Verfügung. Wenn Sie diese Seriennummer nicht haben, können Sie sie jedoch von

der NetApp Support Website abrufen.

Sie sollten gültige Anmeldedaten für die NetApp Support Site haben.

Schritte

1. Loggen Sie sich auf der NetApp Support Site unter ein "mysupport.netapp.com".
2. Navigieren Sie zu **Systems** > **Softwarelizenzen**.
3. Wählen Sie im Auswahlkriterienbereich im Dropdown-Menü „Show Me All: Serial Numbers and Licenses“ die Option **SC_STANDARD** aus.

4. Geben Sie Ihren Firmennamen ein und klicken Sie dann auf **Go!**.

   Die neunstellige Seriennummer der SnapCenter-Lizenz im Format 51xxxxxxx wird angezeigt.

5. Notieren Sie die Seriennummer.

Generieren einer NetApp Lizenzdatei

Wenn Sie Ihre Anmeldedaten für die NetApp Support Site und die Seriennummer der SnapCenter-Lizenz in der SnapCenter GUI nicht eingeben möchten oder wenn Sie über SnapCenter keinen Internetzugang auf die NetApp Support Site haben, können Sie eine NetApp Lizenzdatei generieren. Anschließend kann die Datei heruntergeladen und an einem Speicherort gespeichert werden, auf den über den SnapCenter-Host zugegriffen werden kann.

Was Sie brauchen

- Sie sollten SnapCenter mit ONTAP Select oder Cloud Volumes ONTAP verwenden.
- Sie sollten über gültige Anmeldedaten für die NetApp Support Site verfügen.
- Sie sollten Ihre neunstellige Seriennummer der Lizenz im Format 51xxxxxxx haben.

Schritte

1. Navigieren Sie zum "NetApp Lizenzdatei-Generator".
2. Geben Sie die erforderlichen Informationen ein.
3. Wählen Sie im Feld Produktlinie im Pulldown-Menü die Option **SnapCenter Standard (kapazitätsbasiert)** aus.
4. Geben Sie im Feld Seriennummer des Produkts die Seriennummer für die SnapCenter-Lizenz ein
5. Lesen und akzeptieren Sie die NetApp Datenschutzrichtlinie, und klicken Sie dann auf **Absenden**.

6. Speichern Sie die Lizenzdatei, und notieren Sie anschließend den Speicherort der Datei.

Kapazitätsbasierte Lizenz hinzufügen

Wenn Sie SnapCenter mit ONTAP Select- oder Cloud Volumes ONTAP-Plattformen verwenden, sollten Sie eine oder mehrere kapazitätsbasierte SnapCenter Lizenzen installieren.

Was Sie brauchen

- Sie sollten sich als SnapCenter Admin-Benutzer einloggen.
- Sie sollten über gültige Anmeldedaten für die NetApp Support Site verfügen.
- Sie sollten Ihre neunstellige Seriennummer der Lizenz im Format 51xxxxxxx haben.

  Wenn Sie zum Hinzufügen Ihrer Lizenz eine NetApp Lizenzdatei (NetApp License File, NLF) verwenden, sollten Sie den Speicherort der Lizenzdatei kennen.

Über diese Aufgabe

Auf der Seite Einstellungen können Sie die folgenden Aufgaben ausführen:

- Fügen Sie eine Lizenz hinzu.
- Zeigen Sie Lizenzdetails an, um schnell Informationen zu jeder Lizenz zu finden.
- Ändern Sie eine Lizenz, wenn Sie die vorhandene Lizenz ersetzen möchten, z. B. um die Lizenzkapazität zu aktualisieren oder die Einstellungen für die Schwellenwertbenachrichtigung zu ändern.
- Löschen Sie eine Lizenz, wenn Sie eine vorhandene Lizenz ersetzen möchten oder wenn die Lizenz nicht mehr benötigt wird.

Die Testlizenz (Seriennummer, die mit 50 endet) kann nicht mit dem GUI von SnapCenter gelöscht werden. Die Testlizenz wird automatisch überschrieben, wenn Sie eine erworbene SnapCenter Standard kapazitätsbasierte Lizenz hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Software**.
3. Klicken Sie im Abschnitt Lizenz der Software-Seite auf **Hinzufügen** (+).
4. Wählen Sie im Assistenten zum Hinzufügen von SnapCenter-Lizenzen eine der folgenden Methoden aus, um die Lizenz zu erhalten, die Sie hinzufügen möchten:

Für dieses Feld…	Tun Sie das…
Geben Sie Ihre Zugangsdaten für die NetApp Support Site (NSS) ein, um Lizenzen zu importieren	a. Geben Sie Ihren NSS-Benutzernamen ein. b. Geben Sie Ihr NSS-Passwort ein. c. Geben Sie die Seriennummer der Controller-basierten Lizenz ein.

Für dieses Feld…	Tun Sie das…
NetApp Lizenzdatei	a. Navigieren Sie zum Speicherort der Lizenzdatei, und wählen Sie sie aus. b. Klicken Sie Auf **Offen**.

5. Geben Sie auf der Seite Benachrichtigungen den Kapazitätsschwellenwert ein, bei dem SnapCenter E-Mail-, EMS- und AutoSupport-Benachrichtigungen sendet.

   Der Standardwert ist 90 Prozent.

6. Um den SMTP-Server für E-Mail-Benachrichtigungen zu konfigurieren, klicken Sie auf **Einstellungen** > **Globale Einstellungen** > **Benachrichtigungsserver-Einstellungen** und geben Sie die folgenden Details ein:

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie entweder **immer** oder **nie**.
Geben Sie E-Mail-Einstellungen an	Wenn Sie **immer** wählen, geben Sie Folgendes an: • E-Mail-Adresse des Absenders • E-Mail-Adresse des Empfängers • Optional: Bearbeiten Sie die Standard-Betreffzeile Das Standardfach lautet wie folgt: "SnapCenter-Lizenzbenachrichtigung".

7. Wenn Event Management System (EMS)-Meldungen an das Storage-System-Syslog gesendet werden sollen oder AutoSupport-Meldungen für fehlgeschlagene Vorgänge an das Storage-System gesendet werden sollen, aktivieren Sie die entsprechenden Kontrollkästchen.

   Best Practice: Die Aktivierung von AutoSupport wird empfohlen, um Probleme zu beheben, die möglicherweise auftreten.

8. Klicken Sie Auf **Weiter**.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Berechnung der Kapazitätsauslastung durch SnapCenter

SnapCenter berechnet automatisch die Kapazitätsauslastung einmal täglich um Mitternacht auf dem verwalteten ONTAP Select und Cloud Volumes ONTAP Storage. Um sicherzustellen, dass Sie SnapCenter korrekt konfiguriert haben, sollten Sie beachten, wie SnapCenter die Kapazität berechnet.

Bei Verwendung einer Standard-Kapazitätslizenz berechnet SnapCenter die nicht genutzte Kapazität, indem die genutzte Kapazität für alle Volumes aus der insgesamt lizenzierten Kapazität abgeleitet wird. Wenn die genutzte Kapazität die lizenzierte Kapazität überschreitet, wird auf dem SnapCenter Dashboard eine Warnmeldung zur Übernutzung angezeigt. Wenn Sie in SnapCenter Kapazitätsschwellenwerte und -Benachrichtigungen konfiguriert haben, wird eine E-Mail gesendet, wenn die verwendete Kapazität den von

Ihnen angegebenen Schwellenwert erreicht.

Bereitstellung Ihres Storage-Systems

Bereitstellen von Storage auf Windows Hosts

Konfigurieren des LUN-Speichers

Mit SnapCenter können Sie eine FC-verbundene oder iSCSI-verbundene LUN konfigurieren. Sie können auch SnapCenter verwenden, um eine vorhandene LUN mit einem Windows-Host zu verbinden.

LUNs sind die grundlegende Storage-Einheit in einer SAN-Konfiguration. Der Windows-Host sieht LUNs auf Ihrem System als virtuelle Festplatten. Weitere Informationen finden Sie unter "ONTAP 9 SAN Configuration Guide".

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.

Trennen Sie eine iSCSI-Sitzung

Gelegentlich müssen Sie eine iSCSI-Sitzung von einem Ziel trennen, mit dem Sie mehrere Sitzungen 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. Wählen Sie aus der Liste der iSCSI-Sitzungen die Sitzung aus, die Sie trennen möchten, und klicken Sie auf **Sitzung trennen**.
6. Klicken Sie im Dialogfeld Sitzung trennen auf **OK**.

   SnapCenter trennt die iSCSI-Sitzung.

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.

Erstellen und Verwalten von Festplatten

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.

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.

Was Sie brauchen

- 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.
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**.

Auswählen…	Wenn…
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.
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.

Eigenschaft	Beschreibung
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, eine Snapshot Kopie zu erstellen, bevor Sie die Größe einer LUN ändern.
- Wenn Sie eine LUN aus einer Snapshot Kopie wiederherstellen müssen, die vor der Größe der LUN erstellt wurde, wird die LUN automatisch von SnapCenter neu in die Größe der Snapshot Kopie angepasst.

  Nach dem Wiederherstellungsvorgang müssen die Daten, die der LUN nach der Größe hinzugefügt wurden, aus einer Snapshot Kopie wiederhergestellt werden, die nach der Größe der LUN erstellt 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.

Was Sie brauchen

- 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.

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.
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.

Eigenschaft	Beschreibung
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.

Was Sie brauchen

- 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.

In diesem Feld…	Tun Sie das…
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.

Was Sie brauchen

- 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 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 verweisen "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

Mit dem SnapCenter Plug-in für Microsoft Windows in VMware Umgebungen können LUNs erstellt und gemanagt und Snapshot Kopien gemanagt werden.

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.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

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".

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 MySQLProtocol-Schlüssels in der Datei Web.config.

   Das folgende Beispiel zeigt den Wert des in der Datei Web.config aktualisierten MySQLProtocol-Schlüssels.

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

7. Aktualisieren Sie die Datei Web.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. Den Wert des MySQLProtocol-Schlüssels in der Datei Web.config für beide HA-Knoten aktualisieren.

   Das folgende Beispiel zeigt den Wert des in der Datei Web.config aktualisierten MySQLProtocol-Schlüssels.

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

8. Aktualisieren Sie die Datei Web.config mit den Pfaden, die Sie im Abschnitt [Client] der Datei my.ini für beide HA-Knoten 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.

Während der Installation auf Ihrem Windows-Host aktivierte Funktionen

Das SnapCenter-Serverinstallationsprogramm aktiviert die Windows-Funktionen und -Rollen auf Ihrem Windows-Host während der Installation. Diese sind möglicherweise für die Fehlerbehebung und die Wartung des Host-Systems interessant.

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 4.5 ◦ Server-Seitige Umfasst ◦ WebSocket-Protokoll • Management Tools IIS-Verwaltungskonsole

Kategorie	Merkmal
IIS-Verwaltungsskripte und -Tools	• IIS-Verwaltungsdienst • Web-Management-Tools
.NET Framework 4.5.2 – Funktionen	• .NET Framework 4.5.2 • ASP.NET 4.5.2 • Windows Communication Foundation (WCF) HTTP Activation45 ◦ TCP-Aktivierung ◦ HTTP-Aktivierung ◦ Aktivierung von Message Queuing (MSMQ)
Message Queuing	• Message Queuing Services Stellen Sie sicher, dass keine anderen Anwendungen den MSMQ-Dienst verwenden, den SnapCenter erstellt und verwaltet. • MSMQ-Server
Windows-Prozess-Aktivierungsdienst	• Prozessmodell
Konfigurations-APIs	Alle