Konfigurieren des SnapCenter-Servers

SnapCenter software

NetApp
January 09, 2026

Inhalt

Konfigurieren des SnapCenter-Servers . . . 1
Hinzufügen und Bereitstellen des Speichersystems . . . 1
Storage-Systeme hinzufügen . . . 1
Storage-Verbindungen und Anmeldedaten . . . 4
Bereitstellen von Storage auf Windows Hosts . . . 5
Bereitstellung von Storage in VMware Umgebungen . . . 20
Controller-basierte SnapCenter Standard-Lizenzen hinzufügen . . . 22
Schritt 1: Überprüfen Sie, ob die SnapManager Suite-Lizenz installiert ist . . . 23
Schritt 2: Identifizieren Sie die auf dem Controller installierten Lizenzen . . . 24
Schritt 3: Rufen Sie die Seriennummer des Controllers ab . . . 24
Schritt 4: Rufen Sie die Seriennummer der Controller-basierten Lizenz ab . . . 25
Schritt 5: Controller-basierte Lizenz hinzufügen . . . 26
Schritt 6: Entfernen Sie die Testlizenz . . . 27
Konfiguration Der Hochverfügbarkeit . . . 27
Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit . . . 27
Hochverfügbarkeit für das SnapCenter MySQL Repository . . . 32
Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) . . . 32
Erstellen Sie eine Rolle . . . 32
Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine RBAC-Rolle für NetApp ONTAP hinzu . . . 33
Erstellen Sie SVM-Rollen mit minimalen Berechtigungen . . . 35
Erstellung von SVM-Rollen für ASA r2 Systeme . . . 40
Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen . . . 45
Erstellen von ONTAP Clusterrollen für ASA r2-Systeme . . . 51
Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu . . . 58
Konfigurieren Sie die Einstellungen für das Prüfprotokoll . . . 61
Konfigurieren Sie gesicherte MySQL-Verbindungen mit SnapCenter-Server . . . 63
Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter-Server-Konfigurationen . . . 63
Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen . . . 65

Konfigurieren des SnapCenter-Servers

Hinzufügen und Bereitstellen des Speichersystems

Storage-Systeme hinzufügen

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

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

Bevor Sie beginnen

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

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

- Speichersystemnamen sollten eindeutig sein.

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

      Der Standardport 443 funktioniert in der Regel.

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

      Der Standardwert ist 60 Sekunden.

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

Ergebnis

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

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

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

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

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

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

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

Nach Ihrer Beendigung

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

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

Der SVM-Administrator hat keinen Zugriff auf AutoSupport.

Storage-Verbindungen und Anmeldedaten

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

Speicherverbindungen

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

Anmeldedaten

- Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

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

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

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

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

- Anmeldedaten für einzelne Ressourcengruppen

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

Bereitstellen von Storage auf Windows Hosts

Erstellen und Verwalten von Initiatorgruppen

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

Erstellen einer Initiatorgruppe

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

Schritte

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

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

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

   SnapCenter erstellt die Initiatorgruppe auf dem Storage-System.

Benennen Sie eine Initiatorgruppe um

Sie können eine vorhandene Initiatorgruppe mit SnapCenter umbenennen.

Schritte

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

Ändern einer Initiatorgruppe

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

Schritte

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

Löschen einer Initiatorgruppe

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

Schritte

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

   SnapCenter löscht die Initiatorgruppe.

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.

Richten Sie eine iSCSI-Sitzung ein

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

Schritte

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

   Der Assistent „Sitzung einrichten“ wird angezeigt.

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

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

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

   SnapCenter richtet die iSCSI-Sitzung ein.

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

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

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

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

Bevor Sie beginnen

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

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

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

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

Über diese Aufgabe

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

Schritte

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

   Der Assistent Datenträger erstellen wird geöffnet.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ändern der Größe einer Festplatte

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

Über diese Aufgabe

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

Größe angezeigt.

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

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

Schritte

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

   Die Festplatten werden aufgelistet.

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

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

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

   SnapCenter Größe der Festplatte neu.

Schließen Sie eine Festplatte an

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

Bevor Sie beginnen

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

Schritte

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

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

   Der Assistent zum Verbinden von Festplatten wird geöffnet.

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

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

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

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

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

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

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

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

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

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

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

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

Trennen Sie eine Festplatte

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

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

   Die Festplatten werden aufgelistet.

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

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

   SnapCenter trennt die Verbindung der Festplatte.

Löschen Sie eine Festplatte

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

Schritte

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

   Die Festplatten werden aufgelistet.

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

   SnapCenter löscht die Festplatte.

SMB-Freigaben erstellen und managen

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

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

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

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

Erstellen Sie eine SMB-Freigabe

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

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

Schritte

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

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

   Das Dialogfeld Neue Freigabe wird geöffnet.

5. Definieren Sie im Dialogfeld Neue Freigabe die Freigabe:

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

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

   SnapCenter erstellt die SMB-Freigabe auf der SVM.

Löschen einer SMB-Freigabe

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

Schritte

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

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

   SnapCenter löscht die SMB-Freigabe von der SVM.

Rückgewinnung von Speicherplatz im Storage-System

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

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

  Dadurch kann der Rückgewinnungsprozess verlangsamt werden.

Schritt

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

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

Drive_Path ist der der der LUN zugeordnete Laufwerkpfad.

Stellen Sie Storage mit PowerShell cmdlets bereit

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

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

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

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

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

Bereitstellung von Storage in VMware Umgebungen

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

Unterstützte VMware Gastbetriebssystemplattformen

- Unterstützte Versionen von Windows Server
- Microsoft Cluster-Konfigurationen

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

- RDM-LUNs

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

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

Serverbezogene Einschränkungen bei VMware ESXi

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

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

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

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

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

- Datastore: Datei Entfernen

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

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

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

Verwalten Sie FC RDM LUNs in einem Microsoft Cluster

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

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

Anforderungen

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

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

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

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

  Sie können virtuelle Laufwerke nicht für gemeinsamen Speicher verwenden.

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

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

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

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

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

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

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

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

Einschränkungen

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

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

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

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

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

Erstellen Sie eine gemeinsame FC RDM LUN

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

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

Controller-basierte SnapCenter Standard-Lizenzen hinzufügen

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

Die Controller-basierte Lizenz weist folgende Merkmale auf:

- SnapCenter Standard-Nutzungsberechtigung ist beim Kauf von Premium oder Flash Bundle enthalten (nicht im Basispaket).
- Unbegrenzte Storage-Nutzung
- Wird mithilfe des ONTAP System Manager oder der ONTAP CLI direkt zum FAS, AFF oder ASA -Speichercontroller hinzugefügt.

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

- Gesperrt an die Seriennummer des Controllers

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

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

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

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

Schritte

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

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

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

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

Schritt 2: Identifizieren Sie die auf dem Controller installierten Lizenzen

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

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

Schritte

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

Beispielausgabe

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

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

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description             Expiration
----------------- -------- ---------------------   ---------------
NFS               license  NFS License             -
CIFS              license  CIFS License            -
iSCSI             license  iSCSI License           -
FCP               license  FCP License             -
SnapRestore       license  SnapRestore License     -
SnapMirror        license  SnapMirror License      -
FlexClone         license  FlexClone License       -
SnapVault         license  SnapVault License       -
SnapManagerSuite  license  SnapManagerSuite License -
```

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

Schritt 3: Rufen Sie die Seriennummer des Controllers ab

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

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim Controller ein.
2. Geben Sie den Befehl „System show -instance“ ein, und überprüfen Sie die Ausgabe, um die Controller-Seriennummer zu finden.

   Beispielausgabe

```
cluster1::> system show -instance

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

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

3. Notieren Sie die Seriennummern.

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

Wenn Sie FAS, ASA oder AFF -Speicher verwenden, können Sie die Controller-basierte Lizenz für SnapCenter

von der NetApp -Support-Site abrufen, bevor Sie sie über die ONTAP -Befehlszeile installieren.

Bevor Sie beginnen

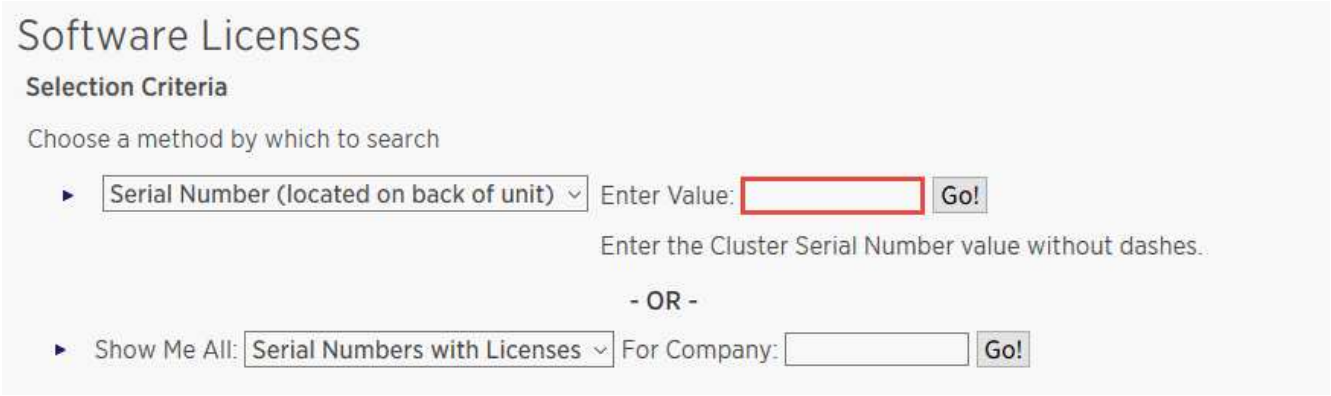
- Sie sollten über gültige Anmeldedaten für die NetApp Support Site verfügen.

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

- Sie sollten die Controller-Seriennummer angeben.

Schritte

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



   Eine Liste der Lizenzen für den angegebenen Controller wird angezeigt.

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

Schritt 5: Controller-basierte Lizenz hinzufügen

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

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

2. Fügen Sie den Lizenzschlüssel für die SnapManagerSuite hinzu:

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

   Dieser Befehl ist auf der Administrator-Berechtigungsebene verfügbar.

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

   ```
   license show
   ```

Schritt 6: Entfernen Sie die Testlizenz

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

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

Schritte

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

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

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

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

3. Entfernen Sie die Testlizenz aus der Datenbank:

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

Konfiguration Der Hochverfügbarkeit

Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit

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

Sie können auch den Netzwerklastenausgleich (NLB) konfigurieren, um die hohe Verfügbarkeit von

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

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

Konfigurieren Sie Hochverfügbarkeit mit F5

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

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

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

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

Weitere Informationen

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

Konfigurieren von Hochverfügbarkeit mit Network Load Balancing (NLB)

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

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

Hochverfügbarkeit mit AWS Elastic Load Balancing (ELB) konfigurieren

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

Schritte

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

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

e. Testen Sie die vollständige Funktion.

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

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

Konfigurieren Sie Hochverfügbarkeit mit dem Azure Load Balancer

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

Schritte

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

== Wechsel von NLB zu F5 für hohe Verfügbarkeit

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

Schritte

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

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

Hochverfügbarkeit für das SnapCenter MySQL Repository

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

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

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

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

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

Beachten Sie die Einschränkungen für die MySQL HA-Funktion:

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

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

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

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

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

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

Erstellen Sie eine Rolle

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

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

Schritte

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

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

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

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

Über diese Aufgabe

Um die Konfiguration dieser Rollen auf Speichersystemen zu vereinfachen, können Sie das Tool „RBAC User

Creator für NetApp ONTAP“ verwenden, das im NetApp Communities Forum veröffentlicht wird.

Dieses Tool verarbeitet automatisch die korrekte Einrichtung der ONTAP-Berechtigungen. Das Tool RBAC User Creator for NetApp ONTAP fügt beispielsweise die Privileges automatisch in der richtigen Reihenfolge hinzu, sodass die Privileges mit allen Zugriffsrechten zuerst angezeigt werden. Wenn Sie zuerst die schreibgeschützten Berechtigungen hinzufügen und dann die All-Access-Berechtigungen hinzufügen, markiert ONTAP die All-Access-Berechtigungen als Duplikate und ignoriert sie.

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

   - <user_Name> ist der Name des Benutzers, den Sie in Schritt 2 erstellt haben. Mit diesem Befehl

können Sie den Benutzer so ändern, dass er der Rolle zugeordnet wird.

- <svm_Name> ist der Name der SVM.
- <Role_Name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.
- <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.

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

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

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

Erstellen Sie SVM-Rollen mit minimalen Berechtigungen

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

Schritte

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

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

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

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

3. Entsperren Sie den Benutzer.

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

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

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

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

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun serial" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all

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

"vserver cifs share delete" -access all

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

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

Erstellung von SVM-Rollen für ASA r2 Systeme

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

Schritte

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

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

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

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

3. Entsperren Sie den Benutzer.

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

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

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

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

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all

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

"vserver cifs share show" -access all

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

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen

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

Schritte

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

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

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

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

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

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

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

"nvme subsystem modify" -access all

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

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

"volume snapshot modify-snaplock-expiry-time" -access all

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

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

Erstellen von ONTAP Clusterrollen für ASA r2-Systeme

Sie sollten eine ONTAP-Cluster-Rolle mit minimalen Berechtigungen erstellen, damit Sie

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

Schritte

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

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

   Sie sollten diesen Befehl für jede Berechtigung wiederholen.

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

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

3. Entsperren Sie den Benutzer.

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

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

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

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

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun serial" -access all

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

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

"volume clone create" -access all

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

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

"vserver export-policy rule create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

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

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

Bevor Sie beginnen

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

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

- SnapCenter umfasst mehrere vordefinierte Rollen.

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

- AD-Benutzer und AD-Gruppen, die SnapCenter RBAC hinzugefügt werden, müssen über DIE LESEBERECHTIGUNG auf dem Benutzer-Container und dem Computer-Container im Active Directory

verfügen.

- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle zugewiesen haben, die die entsprechenden Berechtigungen enthält, müssen Sie den Benutzerzugriff auf SnapCenter-Ressourcen wie Hosts und Speicherverbindungen zuweisen.

  Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

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

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

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

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

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

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

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

Schritte

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

Für dieses Feld…	Tun Sie das…
Zugriffstyp	Wählen Sie entweder Domäne oder Arbeitsgruppe aus Für den Authentifizierungstyp Domäne müssen Sie den Domänennamen des Benutzers oder der Gruppe angeben, dem Sie den Benutzer zu einer Rolle hinzufügen möchten. Standardmäßig wird er mit dem angemeldeten Domänennamen ausgefüllt. Sie müssen die nicht vertrauenswürdige Domäne auf der Seite **Einstellungen** > **Globale Einstellungen** > **Domain-Einstellungen** registrieren.
Typ	Wählen Sie entweder Benutzer oder Gruppe aus SnapCenter unterstützt nur Sicherheitsgruppen, nicht die Vertriebsgruppe.

Für dieses Feld…	Tun Sie das…
Benutzername	a. Geben Sie den teilweisen Benutzernamen ein, und klicken Sie dann auf **Hinzufügen**. Bei Benutzername wird die Groß-/Kleinschreibung berücksichtigt. b. Wählen Sie den Benutzernamen aus der Suchliste aus. Wenn Sie Benutzer aus einer anderen Domäne oder einer nicht vertrauenswürdigen Domäne hinzufügen, sollten Sie den Benutzernamen vollständig eingeben, da keine Suchliste für domänenübergreifende Benutzer vorhanden ist. Wiederholen Sie diesen Schritt, um der ausgewählten Rolle weitere Benutzer oder Gruppen hinzuzufügen.
Rollen	Wählen Sie die Rolle aus, der Sie den Benutzer hinzufügen möchten.

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

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

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

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

Konfigurieren Sie die Einstellungen für das Prüfprotokoll

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

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

die Integrität des Inhalts zu gewährleisten.

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

Über diese Aufgabe

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

  Freigegebene oder netzwerkbasierte Laufwerke werden nicht unterstützt.

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

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

Schritte

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

   Sie können auch den Befehl **Start-SmAuditIntegritätCheck** ausführen, um die Integritätsprüfung bei Bedarf zu starten.

6. (Optional) Aktivieren Sie die Weiterleitung von Audit-Protokollen an Remote-Syslog-Server und geben Sie

die Details des Syslog-Servers ein.

Sie sollten das Zertifikat vom Syslog-Server in den 'Trusted Root' für das TLS 1.2-Protokoll importieren.

a. Geben Sie Syslog Server Host Ein
b. Geben Sie Den Syslog-Server-Port Ein
c. Geben Sie Syslog Server Protocol Ein
d. RFC-Format eingeben

7. Klicken Sie Auf **Speichern**.
8. Durch Klicken auf **Monitor** > **Jobs** können Sie die Integritätsprüfungen und die Überprüfung des Festplattenspeichers einsehen.

Konfigurieren Sie gesicherte MySQL-Verbindungen mit SnapCenter-Server

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

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

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

Folgende Zertifikate werden generiert:

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

Schritte

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

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

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

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

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

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

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

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

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

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

   Das folgende Beispiel zeigt die Zertifikate und Schlüsseldateien, die in den Abschnitt [mysqld] der Datei my.ini im Standardordner kopiert wurden `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Starten Sie die Webanwendung des SnapCenter-Servers im IIS.

Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen

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

Folgende Zertifikate werden generiert:

- CA-Zertifikat

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

+

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

+

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

5. Beenden Sie die Webanwendung des SnapCenter-Servers im Internet Information Server (IIS) auf beiden HA-Knoten.
6. Starten Sie den MySQL Service auf beiden HA-Nodes neu.
7. Aktualisieren Sie den Wert des Schlüssels MySQLProtocol in der Datei SnapManager.Web.UI.dll.config für beide HA-Knoten.

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

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

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

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

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

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

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

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

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