Konfigurieren des SnapCenter -Servers

SnapCenter software

NetApp
November 06, 2025

Inhalt

Konfigurieren des SnapCenter -Servers

Hinzufügen und Bereitstellen des Speichersystems

Speichersysteme hinzufügen

Sie sollten das Speichersystem einrichten, das SnapCenter Zugriff auf ONTAP -Speicher, ASA r2-Systeme oder Amazon FSx for NetApp ONTAP gewährt, um Datenschutz- und Bereitstellungsvorgänge durchzuführen.

Sie können entweder eine eigenständige SVM oder einen Cluster aus mehreren SVMs hinzufügen. Wenn Sie Amazon FSx for NetApp ONTAP verwenden, können Sie entweder FSx-Admin-LIF hinzufügen, das aus mehreren SVMs besteht, indem Sie das fsxadmin-Konto verwenden, oder FSx-SVM in SnapCenter hinzufügen.

Bevor Sie beginnen

- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

  Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

Über diese Aufgabe

- Wenn Sie Speichersysteme konfigurieren, können Sie auch die Funktionen Event Management System (EMS) und AutoSupport aktivieren. Das AutoSupport Tool sammelt Daten zum Zustand Ihres Systems und sendet die Daten automatisch an den technischen Support von NetApp , damit dieser Fehler an Ihrem System beheben kann.

  Wenn Sie diese Funktionen aktivieren, sendet SnapCenter AutoSupport Informationen an das Speichersystem und EMS-Nachrichten an das Syslog des Speichersystems, wenn eine Ressource geschützt ist, ein Wiederherstellungs- oder Klonvorgang erfolgreich abgeschlossen wird oder ein Vorgang fehlschlägt.

- Wenn Sie Snapshots auf ein SnapMirror oder SnapVault -Ziel replizieren möchten, müssen Sie Speichersystemverbindungen für die Ziel-SVM oder den Ziel-Cluster sowie die Quell-SVM oder den Quell-Cluster einrichten.

Wenn Sie das Kennwort des Speichersystems ändern, können geplante Jobs, On-Demand-Sicherungs- und Wiederherstellungsvorgänge fehlschlagen. Nachdem Sie das Kennwort des Speichersystems geändert haben, können Sie das Kennwort 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 „Speichersystem hinzufügen“ die folgenden Informationen ein:

Für dieses Feld…	Machen Sie Folgendes…
Speichersystem	Geben Sie den Namen oder die IP-Adresse des Speichersystems ein. Speichersystemnamen dürfen (ohne Domänennamen) höchstens 15 Zeichen lang sein und müssen auflösbar sein. Um Speichersystemverbindungen mit Namen zu erstellen, die mehr als 15 Zeichen haben, können Sie das Cmdlet Add-SmStorageConnectionPowerShell verwenden. Für Speichersysteme mit MetroCluster -Konfiguration (MCC) wird empfohlen, sowohl lokale als auch Peer-Cluster für unterbrechungsfreie Vorgänge zu registrieren. SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss einen eindeutigen Namen haben. Nachdem Sie die Speicherverbindung zu SnapCenter hinzugefügt haben, sollten Sie die SVM oder den Cluster nicht mit ONTAP umbenennen. Wenn SVM mit einem Kurznamen oder FQDN hinzugefügt wird, muss es sowohl vom SnapCenter als auch vom Plug-In-Host auflösbar sein.
Benutzername/Passwort	Geben Sie die Anmeldeinformationen des Speicherbenutzers ein, der über die erforderlichen Berechtigungen für den Zugriff auf das Speichersystem verfügt.

Für dieses Feld…	Machen Sie Folgendes…
Event Management System (EMS) und AutoSupport -Einstellungen	Wenn Sie EMS-Nachrichten an das Syslog des Speichersystems senden möchten oder wenn Sie möchten, dass AutoSupport Nachrichten zum angewendeten Schutz, zu abgeschlossenen Wiederherstellungsvorgängen oder zu fehlgeschlagenen Vorgängen an das Speichersystem gesendet werden, aktivieren Sie das entsprechende Kontrollkästchen. Wenn Sie das Kontrollkästchen * AutoSupport -Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden* aktivieren, wird auch das Kontrollkästchen * SnapCenter -Server -Ereignisse in Syslog protokollieren* aktiviert, da EMS-Messaging erforderlich ist, um AutoSupport Benachrichtigungen zu aktivieren.

4. Klicken Sie auf **Weitere Optionen**, wenn Sie die der Plattform, dem Protokoll, dem Port und dem Timeout zugewiesenen Standardwerte ändern möchten.

   a. Wählen Sie unter „Plattform“ eine der Optionen aus der Dropdownliste aus.

      Wenn es sich bei der SVM um das sekundäre Speichersystem in einer Sicherungsbeziehung handelt, aktivieren Sie das Kontrollkästchen **Sekundär**. Wenn die Option **Sekundär** ausgewählt ist, führt SnapCenter nicht sofort eine Lizenzprüfung durch.

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

   a. Wählen Sie unter „Protokoll“ das Protokoll aus, das während der SVM- oder Cluster-Einrichtung konfiguriert wurde, normalerweise HTTPS.

   b. Geben Sie den Port ein, den das Speichersystem akzeptiert.

      Normalerweise funktioniert der Standardport 443.

   c. Geben Sie die Zeit in Sekunden ein, die vergehen soll, bevor Kommunikationsversuche abgebrochen werden.

      Der Standardwert beträgt 60 Sekunden.

   d. Wenn die SVM über mehrere Verwaltungsschnittstellen 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 **Senden**.

Ergebnis

Führen Sie auf der Seite „Speichersysteme“ im Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

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

Wenn Sie FSx SVMs hinzugefügt haben, werden die FSx SVMs hier aufgelistet.

- 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 Clusternamen klicken, werden alle SVMs, die Teil des Clusters sind, im Abschnitt „Storage Virtual Machines“ angezeigt.

  Wenn dem ONTAP Cluster mithilfe der ONTAP GUI ein neues SVM hinzugefügt wird, klicken Sie auf **Neu erkennen**, um das neu hinzugefügte SVM anzuzeigen.

Nachdem Sie fertig sind

Ein Clusteradministrator muss AutoSupport auf jedem Speichersystemknoten aktivieren, um E-Mail-Benachrichtigungen von allen Speichersystemen zu senden, auf die SnapCenter Zugriff hat, indem er den folgenden Befehl von der Befehlszeile des Speichersystems aus ausführt:

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

Der Administrator der Storage Virtual Machine (SVM) hat keinen Zugriff auf AutoSupport.

Speicherverbindungen und Anmeldeinformationen

Bevor Sie Datenschutzvorgänge durchführen, sollten Sie die Speicherverbindungen einrichten und die Anmeldeinformationen hinzufügen, die der SnapCenter Server und die SnapCenter Plug-Ins verwenden werden.

Speicherverbindungen

Die Speicherverbindungen ermöglichen dem SnapCenter Server und den SnapCenter -Plug-Ins den Zugriff auf den ONTAP -Speicher. Zum Einrichten dieser Verbindungen gehört auch die Konfiguration der Funktionen von AutoSupport und Event Management System (EMS).

Anmeldeinformationen

- Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

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

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

  Geben Sie für Systeme, 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 Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist.

Das gültige Format für das Feld „Benutzername“ ist: *Benutzername*

- Anmeldeinformationen für einzelne Ressourcengruppen

  Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

Bereitstellen von Speicher auf Windows-Hosts

Erstellen und Verwalten von igroups

Sie erstellen Initiatorgruppen (igroups), um anzugeben, welche Hosts auf eine bestimmte LUN im Speichersystem zugreifen können. Sie können SnapCenter verwenden, um eine igroup auf einem Windows-Host zu erstellen, umzubenennen, zu ändern oder zu löschen.

Erstellen einer igroup

Sie können SnapCenter verwenden, um eine igroup auf einem Windows-Host zu erstellen. Die igroup ist im Assistenten „Datenträger erstellen“ oder „Datenträger verbinden“ verfügbar, wenn Sie die igroup einer LUN zuordnen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Igroup**.
3. Klicken Sie auf der Seite „Initiatorgruppen“ auf **Neu**.
4. Definieren Sie im Dialogfeld „Igroup erstellen“ die Igroup:

In diesem Bereich…	Machen Sie Folgendes…
Speichersystem	Wählen Sie die SVM für die LUN aus, die Sie der igroup zuordnen möchten.
Gastgeber	Wählen Sie den Host aus, auf dem Sie die igroup erstellen möchten.
Igroup-Name	Geben Sie den Namen der Igroup ein.
Initiatoren	Wählen Sie den Initiator aus.
Typ	Wählen Sie den Initiatortyp: iSCSI, FCP oder gemischt (FCP und iSCSI).

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

   SnapCenter erstellt die igroup auf dem Speichersystem.

Umbenennen einer igroup

Sie können SnapCenter verwenden, um eine vorhandene igroup umzubenennen.

Schritte

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

Ändern einer igroup

Sie können SnapCenter verwenden, um einer vorhandenen Igroup Igroup-Initiatoren hinzuzufügen. Beim Erstellen einer igroup können Sie nur einen Host hinzufügen. Wenn Sie eine Igroup für einen Cluster erstellen möchten, können Sie die Igroup ändern, um dieser Igroup weitere Knoten hinzuzufügen.

Schritte

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

Löschen einer igroup

Sie können SnapCenter verwenden, um eine Igroup zu löschen, wenn Sie sie nicht mehr benötigen.

Schritte

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

   SnapCenter löscht die igroup.

Erstellen und Verwalten von Datenträgern

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

- SnapCenter unterstützt nur Basisdatenträger. Die dynamischen Datenträger werden nicht unterstützt.
- Für GPT ist nur eine Datenpartition und für MBR eine primäre Partition zulässig, die über ein mit NTFS oder CSVFS formatiertes Volume und einen Mount-Pfad verfügt.
- Unterstützte Partitionsstile: GPT, MBR; in einer VMware UEFI VM werden nur iSCSI-Festplatten unterstützt

SnapCenter unterstützt das Umbenennen einer Festplatte nicht. Wenn eine von SnapCenter verwaltete Festplatte umbenannt wird, sind SnapCenter -Vorgänge nicht erfolgreich.

Anzeigen der Festplatten auf einem Host

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

Schritte

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

   Die Datenträger werden aufgelistet.

Anzeigen von Clusterdatenträgern

Sie können Cluster-Datenträger auf dem Cluster anzeigen, den Sie mit SnapCenter verwalten. Die gruppierten Datenträger werden nur angezeigt, wenn Sie den Cluster aus der Dropdown-Liste „Hosts“ auswählen.

Schritte

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

   Die Datenträger werden aufgelistet.

Richten Sie eine iSCSI-Sitzung ein

Wenn Sie iSCSI zum Herstellen einer Verbindung mit einer LUN verwenden, müssen Sie vor dem Erstellen der LUN eine iSCSI-Sitzung einrichten, um die Kommunikation zu ermöglichen.

Bevor Sie beginnen

- Sie müssen den Speichersystemknoten als iSCSI-Ziel definiert haben.
- Sie müssen den iSCSI-Dienst auf dem Speichersystem gestartet haben. "Mehr erfahren"

Über diese Aufgabe

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

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

Wenn Sie den Namen eines iSCSI-Initiators ändern, wirkt sich dies auf den Zugriff auf iSCSI-Ziele aus. Nach der Namensänderung müssen Sie möglicherweise die vom Initiator aufgerufenen Ziele neu konfigurieren, damit sie den neuen Namen erkennen können. Sie müssen sicherstellen, dass der Host neu gestartet wird, nachdem Sie den Namen eines iSCSI-Initiators geändert haben.

Wenn Ihr Host über mehr als eine iSCSI-Schnittstelle verfügt, können Sie, nachdem Sie eine iSCSI-Sitzung zu SnapCenter mithilfe einer IP-Adresse auf der ersten Schnittstelle hergestellt haben, keine iSCSI-Sitzung von einer anderen Schnittstelle mit einer anderen IP-Adresse herstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ 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 herstellen**.

   Der Assistent zum Einrichten einer Sitzung wird angezeigt.

6. Identifizieren Sie im Assistenten „Sitzung einrichten“ das Ziel:

In diesem Bereich…	Eingeben…
Zielknotenname	Der Knotenname des iSCSI-Ziels Wenn ein Zielknotenname vorhanden ist, wird der Name im schreibgeschützten Format angezeigt.
Zielportaladresse	Die IP-Adresse des Zielnetzwerkportals
Zielportal-Port	Der TCP-Port des Zielnetzwerkportals
Adresse des Initiatorportals	Die IP-Adresse des Initiator-Netzwerkportals

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

   SnapCenter stellt die iSCSI-Sitzung her.

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

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

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

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

Bevor Sie beginnen

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

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

  Sie können auf einem von SnapCenter erstellten Klonvolume keine LUN erstellen, es sei denn, der Klon wurde bereits aufgeteilt.

- Sie müssen den FC- oder iSCSI-Dienst auf dem Speichersystem gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem hergestellt haben.
- Das SnapCenter Plug-Ins-Paket für Windows darf nur auf dem Host installiert werden, auf dem Sie die Festplatte 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-Failovercluster gemeinsam genutzt.
- Wenn eine LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host erstellen, dem die Clustergruppe gehört.

Schritte

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

   Der Assistent zum Erstellen von Datenträgern wird geöffnet.

5. Identifizieren Sie auf der Seite „LUN-Name“ die LUN:

In diesem Bereich…	Machen Sie Folgendes…
Speichersystem	Wählen Sie die SVM für die LUN aus.
LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Ordners auszuwählen, der die LUN enthält.
LUN-Name	Geben Sie den Namen der LUN ein.

In diesem Bereich…	Machen Sie Folgendes…
Clustergröße	Wählen Sie die LUN-Blockzuweisungsgröße für den Cluster aus. Die Clustergröße hängt vom Betriebssystem und den Anwendungen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite „Datenträgertyp“ den Datenträgertyp aus:

Wählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host aus zugegriffen werden. Ignorieren Sie das Feld **Ressourcengruppe**.
Gemeinsam genutzte Festplatte	Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt. Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld **Ressourcengruppe** ein. Sie müssen die Festplatte nur auf einem Host im Failovercluster erstellen.
Gemeinsam genutztes Clustervolume (CSV)	Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt, der CSV 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 Eigentümer der Clustergruppe ist.

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

Eigentum	Beschreibung
Einhängepunkt automatisch zuweisen	SnapCenter weist basierend auf dem Systemlaufwerk automatisch einen Volume-Mount-Punkt zu. Wenn Ihr Systemlaufwerk beispielsweise C: ist, erstellt die automatische Zuweisung einen Volume-Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnpt\). Die automatische Zuweisung wird für gemeinsam genutzte Datenträger nicht unterstützt.

Eigentum	Beschreibung
Laufwerksbuchstaben zuweisen	Hängen Sie die Festplatte in das Laufwerk ein, das Sie in der angrenzenden Dropdown-Liste auswählen.
Volume-Mount-Punkt verwenden	Hängen Sie die Festplatte in den Laufwerkspfad ein, den Sie im angrenzenden Feld angeben. Das Stammverzeichnis des Volume-Mount-Punkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weder Laufwerksbuchstaben noch Volume-Mount-Punkte zuweisen	Wählen Sie diese Option, wenn Sie die Festplatte lieber manuell in Windows mounten möchten.
LUN-Größe	Geben Sie die LUN-Größe an; mindestens 150 MB. Wählen Sie in der angrenzenden Dropdown-Liste MB, GB oder TB aus.
Verwenden Sie Thin Provisioning für das Volume, das diese LUN hostet	Führen Sie eine Thin-Provisioning-Bereitstellung für die LUN durch. Thin Provisioning weist nur so viel Speicherplatz zu, wie jeweils benötigt wird, sodass die LUN effizient auf die maximal verfügbare Kapazität anwachsen kann. Stellen Sie sicher, dass auf dem Volume genügend Speicherplatz für den gesamten LUN-Speicher verfügbar ist, den Sie voraussichtlich benötigen.
Partitionstyp auswählen	Wählen Sie eine GPT-Partition für eine GUID-Partitionstabelle oder eine MBR-Partition für einen Master Boot Record. MBR-Partitionen können in Windows Server-Failoverclustern zu Ausrichtungsproblemen führen. UEFI-Partitionsdatenträger (Unified Extensible Firmware Interface) werden nicht unterstützt.

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

In diesem Bereich…	Machen Sie Folgendes…
Gastgeber	Doppelklicken Sie auf den Clustergruppennamen, um eine Dropdownliste mit den zum Cluster gehörenden Hosts anzuzeigen, und wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird.
Host-Initiator auswählen	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host. 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 der LUN eine vorhandene Igroup zuordnen oder eine neue Igroup erstellen möchten:

Wählen…	Wenn…
Neue igroup für ausgewählte Initiatoren erstellen	Sie möchten eine neue Igroup für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Igroup oder geben Sie eine neue Igroup für ausgewählte Initiatoren an	Sie möchten eine vorhandene Igroup für die ausgewählten Initiatoren angeben oder eine neue Igroup mit dem von Ihnen angegebenen Namen erstellen. Geben Sie den Igroup-Namen in das Feld **Igroup-Name** ein. Geben Sie die ersten Buchstaben des vorhandenen igroup-Namens ein, um das Feld automatisch zu vervollständigen.

10. Überprüfen Sie auf der Seite „Zusammenfassung“ Ihre Auswahl und klicken Sie dann auf **Fertig**.

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

Ändern der Größe einer Festplatte

Sie können die Größe einer Festplatte vergrößern oder verkleinern, wenn sich die Anforderungen Ihres Speichersystems ändern.

Über diese Aufgabe

- Für Thin Provisioning LUN wird die ONTAP LUN-Geometriegröße als maximale Größe angezeigt.
- Bei Thick Provisioning LUN 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 Partitionen im GPT-Stil haben eine Speichersystemgrößenbeschränkung von 16 TB.
- Es ist eine gute Idee, vor der Größenänderung einer LUN einen Snapshot zu erstellen.
- Wenn Sie eine LUN aus einem Snapshot wiederherstellen müssen, der vor der Größenänderung der LUN erstellt wurde, passt SnapCenter die Größe der LUN automatisch an die Größe des Snapshots an.

  Nach dem Wiederherstellungsvorgang müssen Daten, die der LUN nach der Größenänderung hinzugefügt wurden, aus einem Snapshot wiederhergestellt werden, der nach der Größenänderung erstellt wurde.

Schritte

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

   Die Datenträger werden aufgelistet.

4. Wählen Sie die Festplatte aus, deren Größe Sie ändern möchten, und klicken Sie dann auf **Größe ändern**.
5. Verwenden Sie im Dialogfeld „Datenträgergröße ändern“ den Schieberegler, um die neue Größe des Datenträgers 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 wird. Außerdem müssen Sie auf MB, GB oder TB klicken, um die Maßeinheit anzugeben.

6. Wenn Sie mit Ihren Eingaben zufrieden sind, klicken Sie je nach Bedarf auf **Verkleinern** oder **Erweitern**.

   SnapCenter ändert die Größe der Festplatte.

Verbinden einer Festplatte

Mit dem Assistenten „Datenträger verbinden“ können Sie eine vorhandene LUN mit einem Host verbinden oder eine getrennte LUN erneut verbinden.

Bevor Sie beginnen

- Sie müssen den FC- oder iSCSI-Dienst auf dem Speichersystem gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem hergestellt haben.
- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt.
- Wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host verbinden, dem die Clustergruppe gehört.
- Das Plug-in für Windows muss nur auf dem Host installiert werden, an den Sie die Festplatte anschließen.

Schritte

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

4. Klicken Sie auf **Verbinden**.

   Der Assistent „Datenträger verbinden“ wird geöffnet.

5. Identifizieren Sie auf der Seite „LUN-Name“ die LUN, mit der eine Verbindung hergestellt werden soll:

In diesem Bereich…	Machen Sie Folgendes…
Speichersystem	Wählen Sie die SVM für die LUN aus.
LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Volumes auszuwählen, das die LUN enthält.
LUN-Name	Geben Sie den Namen der LUN ein.
Clustergröße	Wählen Sie die LUN-Blockzuweisungsgröße für den Cluster aus. Die Clustergröße hängt vom Betriebssystem und den Anwendungen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite „Datenträgertyp“ den Datenträgertyp aus:

Wählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host aus zugegriffen werden.
Gemeinsam genutzte Festplatte	Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt. Sie müssen die Festplatte nur mit einem Host im Failovercluster verbinden.
Gemeinsam genutztes Clustervolume (CSV)	Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt, der CSV verwendet. Stellen Sie sicher, dass der Host, auf dem Sie eine Verbindung zur Festplatte herstellen, der Eigentümer der Clustergruppe ist.

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

Eigentum	Beschreibung
Automatische Zuweisung	Lassen Sie SnapCenter automatisch einen Volume-Mount-Punkt basierend auf dem Systemlaufwerk zuweisen. Wenn Ihr Systemlaufwerk beispielsweise C: ist, erstellt die automatische Zuweisungseigenschaft einen Volume-Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnpt\). Die Eigenschaft „Automatische Zuweisung“ wird für gemeinsam genutzte Datenträger nicht unterstützt.
Laufwerksbuchstaben zuweisen	Hängen Sie die Festplatte in das Laufwerk ein, das Sie in der angrenzenden Dropdown-Liste auswählen.
Volume-Mount-Punkt verwenden	Hängen Sie die Festplatte in den Laufwerkspfad ein, den Sie im angrenzenden Feld angeben. Das Stammverzeichnis des Volume-Mount-Punkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weder Laufwerksbuchstaben noch Volume-Mount-Punkte zuweisen	Wählen Sie diese Option, wenn Sie die Festplatte lieber manuell in Windows mounten möchten.

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

In diesem Bereich…	Machen Sie Folgendes…
Gastgeber	Doppelklicken Sie auf den Clustergruppennamen, um eine Dropdown-Liste mit den zum Cluster gehörenden Hosts anzuzeigen. Wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird.
Host-Initiator auswählen	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host. Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit MPIO verwenden.

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

Wählen…	Wenn…
Neue igroup für ausgewählte Initiatoren erstellen	Sie möchten eine neue Igroup für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Igroup oder geben Sie eine neue Igroup für ausgewählte Initiatoren an	Sie möchten eine vorhandene Igroup für die ausgewählten Initiatoren angeben oder eine neue Igroup mit dem von Ihnen angegebenen Namen erstellen. Geben Sie den Igroup-Namen in das Feld **Igroup-Name** ein. Geben Sie die ersten Buchstaben des vorhandenen igroup-Namens ein, um das Feld automatisch auszufüllen.

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 auf dem Host.

Trennen einer Festplatte

Sie können eine LUN von einem Host trennen, ohne den Inhalt der LUN zu beeinträchtigen, mit einer Ausnahme: Wenn Sie einen Klon trennen, bevor er abgespalten wurde, verlieren Sie den Inhalt des Klons.

Bevor Sie beginnen

- Stellen Sie sicher, dass die LUN von keiner Anwendung verwendet wird.
- Stellen Sie sicher, dass die LUN nicht mit einer Überwachungssoftware überwacht wird.
- Wenn die LUN gemeinsam genutzt wird, stellen Sie sicher, dass Sie die Cluster-Ressourcenabhängigkeiten von der LUN entfernen und überprüfen, ob alle Knoten im Cluster eingeschaltet sind, ordnungsgemäß funktionieren und für SnapCenter verfügbar sind.

Über diese Aufgabe

Wenn Sie eine LUN in einem von SnapCenter erstellten FlexClone -Volume trennen und keine anderen LUNs auf dem Volume verbunden sind, löscht SnapCenter das Volume. Bevor die LUN getrennt wird, zeigt SnapCenter eine Warnmeldung an, dass das FlexClone Volume möglicherweise gelöscht wird.

Um das automatische Löschen des FlexClone -Volumes zu vermeiden, sollten Sie das Volume umbenennen, bevor Sie die letzte LUN trennen. Achten Sie beim Umbenennen des Datenträgers darauf, dass Sie mehrere Zeichen ändern und nicht nur das letzte Zeichen im Namen.

Schritte

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

   Die Datenträger werden aufgelistet.

4. Wählen Sie die Festplatte aus, die Sie trennen möchten, und klicken Sie dann auf **Trennen**.
5. Klicken Sie im Dialogfeld „Datenträger trennen“ auf **OK**.

SnapCenter trennt die Verbindung zur Festplatte.

Löschen eines Datenträgers

Sie können eine Festplatte löschen, wenn Sie sie nicht mehr benötigen. Nachdem Sie eine Festplatte gelöscht haben, können Sie sie nicht wiederherstellen.

Schritte

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

   Die Datenträger werden aufgelistet.

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

   SnapCenter löscht die Festplatte.

Erstellen und Verwalten von SMB-Freigaben

Zum Konfigurieren einer SMB3-Freigabe auf einer Storage Virtual Machine (SVM) können Sie entweder die SnapCenter -Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

Best Practice: Die Verwendung der Cmdlets wird empfohlen, da Sie so die mit SnapCenter bereitgestellten Vorlagen nutzen können, um die Freigabekonfiguration zu automatisieren.

Die Vorlagen umfassen bewährte Methoden für die Volume- und Freigabekonfiguration. Sie finden die Vorlagen im Ordner „Templates“ im Installationsordner des SnapCenter Plug-ins-Pakets für Windows.

Wenn Sie sich dabei sicher fühlen, können Sie anhand der bereitgestellten Modelle Ihre eigenen Vorlagen erstellen. Sie sollten die Parameter in der Cmdlet-Dokumentation überprüfen, bevor Sie eine benutzerdefinierte Vorlage erstellen.

Erstellen einer SMB-Freigabe

Sie können die SnapCenter Freigabenseite verwenden, um eine SMB3-Freigabe auf einer virtuellen Speichermaschine (SVM) zu erstellen.

Sie können SnapCenter nicht zum Sichern von Datenbanken auf SMB-Freigaben verwenden. Der SMB-Support ist nur auf die Bereitstellung beschränkt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Freigaben**.
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 Bereich…	Machen Sie Folgendes…
Beschreibung	Geben Sie einen beschreibenden Text für die Freigabe ein.
Freigabename	Geben Sie den Freigabenamen ein, beispielsweise „test_share“. Der Name, den Sie für die Freigabe eingeben, wird auch als Volumename verwendet. Der Freigabename: • Muss eine UTF-8-Zeichenfolge sein. • Darf die folgenden Zeichen nicht enthalten: Steuerzeichen von 0x00 bis 0x1F (beide inklusive), 0x22 (doppelte Anführungszeichen) und die Sonderzeichen `\ / [ ] : (vertical bar) < > + = ; , ?`
Pfad teilen	• Klicken Sie in das Feld, um einen neuen Dateisystempfad einzugeben, beispielsweise /. • Doppelklicken Sie in das Feld, um aus einer Liste vorhandener Dateisystempfade auszuwählen.

6. Wenn Sie mit Ihren Eingaben 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 Seite „Hosts“ auf **Freigaben**.
3. Klicken Sie auf der Seite „Freigaben“ in das Feld **Storage Virtual Machine**, 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 aus der SVM.

Speicherplatz auf dem Speichersystem freigeben

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

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

Bevor Sie beginnen

- Sie müssen sicherstellen, dass der Prozess zur Speicherplatzrückgewinnung abgeschlossen ist, bevor Sie einen Wiederherstellungsvorgang durchführen.
- Wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, müssen Sie die Speicherplatzrückgewinnung auf dem Host durchführen, dem die Clustergruppe gehört.
- Für eine optimale Speicherleistung sollten Sie die Speicherplatzrückgewinnung so oft wie möglich durchführen.

  Sie sollten sicherstellen, dass das gesamte NTFS-Dateisystem gescannt wurde.

Über diese Aufgabe

- Die Speicherplatzrückgewinnung ist zeitaufwändig und CPU-intensiv. Daher ist es normalerweise am besten, den Vorgang auszuführen, wenn die Auslastung des Speichersystems und des Windows-Hosts gering ist.
- Durch die Speicherplatzrückgewinnung wird fast der gesamte verfügbare Speicherplatz zurückgewonnen, jedoch nicht 100 Prozent.
- Sie sollten die Festplattendefragmentierung nicht gleichzeitig mit der Speicherplatzrückgewinnung ausführen.

  Dies kann den Wiederherstellungsprozess verlangsamen.

Schritt

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

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

drive_path ist der Laufwerkspfad, der der LUN zugeordnet ist.

Bereitstellen von Speicher mithilfe von PowerShell-Cmdlets

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

Wenn Sie die Cmdlets auf einem Remote-Plug-In-Host ausführen, müssen Sie das SnapCenter Open-SMConnection-Cmdlet ausführen, um eine Verbindung zum SnapCenter -Server zu öffnen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Wenn SnapCenter PowerShell-Cmdlets aufgrund der Entfernung von SnapDrive für Windows vom Server beschädigt sind, lesen Sie "SnapCenter -Cmdlets funktionieren nicht mehr, wenn SnapDrive für Windows deinstalliert wird" .

Bereitstellen von Speicher 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-Clusterkonfigurationen

  Unterstützung für bis zu maximal 16 Knoten auf VMware bei Verwendung des Microsoft iSCSI Software Initiator oder bis zu zwei Knoten bei Verwendung von FC

- RDM-LUNs

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

  Unterstützt VMware ParaVirtual SCSI Controller. Auf RDM-Festplatten können 256 Festplatten unterstützt werden.

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

Einschränkungen im Zusammenhang mit VMware ESXi-Servern

- Die Installation des Plug-ins für Windows auf einem Microsoft-Cluster auf virtuellen Maschinen mit ESXi-Anmeldeinformationen wird nicht unterstützt.

  Sie sollten Ihre vCenter-Anmeldeinformationen verwenden, wenn Sie das Plug-in für Windows auf virtuellen Maschinen im Cluster installieren.

- Alle Clusterknoten müssen dieselbe Ziel-ID (auf dem virtuellen SCSI-Adapter) für dieselbe Clusterfestplatte verwenden.
- Wenn Sie eine RDM-LUN außerhalb des Plug-ins für Windows erstellen, müssen Sie den Plug-in-Dienst neu starten, damit er die neu erstellte Festplatte erkennt.
- Sie können iSCSI- und FC-Initiatoren nicht gleichzeitig auf einem VMware-Gastbetriebssystem verwenden.

Für SnapCenter RDM-Vorgänge erforderliche Mindestberechtigungen für vCenter

Sie sollten über die folgenden vCenter-Berechtigungen auf dem Host verfügen, um RDM-Vorgänge in einem Gastbetriebssystem durchzuführen:

- Datenspeicher: Datei entfernen
- Host: Konfiguration > Speicherpartitionskonfiguration
- Virtuelle Maschine: Konfiguration

Sie müssen diese Berechtigungen einer Rolle auf der 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 von 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 gemeinsam genutzte RDM-Quorum und den gemeinsam genutzten Speicher außerhalb des Plug-ins erstellen und dann die Festplatten zu den virtuellen Maschinen im Cluster hinzufügen.

Ab ESXi 5.5 können Sie auch ESX iSCSI- und FCoE-Hardware zur Verwaltung eines Microsoft-Clusters verwenden. Das Plug-in für Windows umfasst sofort einsatzbereite Unterstützung für Microsoft-Cluster.

Anforderungen

Das Plug-in für Windows bietet Unterstützung für Microsoft-Cluster mithilfe von FC RDM LUNs auf zwei verschiedenen virtuellen Maschinen, die zu zwei verschiedenen ESX- oder ESXi-Servern gehören (auch als Cluster über Boxen bezeichnet), wenn Sie bestimmte Konfigurationsanforderungen erfüllen.

- Auf den virtuellen Maschinen (VMs) muss dieselbe Windows Server-Version ausgeführt werden.
- Die ESX- oder ESXi-Serverversionen müssen für jeden übergeordneten VMware-Host identisch sein.
- Jeder übergeordnete Host muss über mindestens zwei Netzwerkadapter verfügen.
- Es muss mindestens ein von den beiden ESX- oder ESXi-Servern gemeinsam genutzter VMware Virtual Machine File System (VMFS)-Datenspeicher vorhanden sein.
- VMware empfiehlt, den gemeinsam genutzten Datenspeicher auf einem FC-SAN zu erstellen.

  Bei Bedarf kann der gemeinsame Datenspeicher auch über iSCSI erstellt werden.

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

  Sie können virtuelle Datenträger nicht für gemeinsam genutzten Speicher verwenden.

- Auf jeder virtuellen Maschine im Cluster muss im physischen Kompatibilitätsmodus ein SCSI-Controller konfiguriert werden:

  Windows Server 2008 R2 erfordert, dass Sie den LSI Logic SAS SCSI-Controller auf jeder virtuellen Maschine konfigurieren. Gemeinsam genutzte LUNs können den vorhandenen LSI Logic SAS-Controller nicht verwenden, wenn nur einer seines Typs vorhanden ist und dieser bereits an das Laufwerk C: angeschlossen ist.

  SCSI-Controller vom Typ „Paravirtual“ werden auf VMware Microsoft-Clustern nicht unterstützt.

Wenn Sie einen SCSI-Controller zu einer freigegebenen LUN auf einer virtuellen Maschine im physischen Kompatibilitätsmodus hinzufügen, müssen Sie im VMware Infrastructure Client die Option **Raw Device Mappings** (RDM) und nicht die Option **Neue Festplatte erstellen** auswählen.

- Microsoft-Cluster virtueller Maschinen 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 igroup mit Initiatoren von mehreren Hosts erstellen.

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

- Stellen Sie sicher, dass Sie mithilfe eines FC-Initiators eine RDM-LUN auf ESXi 5.0 erstellen.

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

Einschränkungen

Das Plug-in für Windows unterstützt Microsoft-Cluster mithilfe von FC/iSCSI RDM LUNs auf verschiedenen virtuellen Maschinen, 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 Clusterumgebung.

  Initiatoren müssen entweder FC oder Microsoft iSCSI sein, aber nicht beides.

- ESX iSCSI-Initiatoren und HBAs werden auf gemeinsam genutzten Datenträgern in einem Microsoft-Cluster nicht unterstützt.
- Das Plug-in für Windows unterstützt keine Migration virtueller Maschinen mit vMotion, wenn die virtuelle Maschine Teil eines Microsoft-Clusters ist.
- Das Plug-in für Windows unterstützt MPIO auf virtuellen Maschinen in einem Microsoft-Cluster nicht.

Erstellen einer freigegebenen FC RDM LUN

Bevor Sie FC RDM LUNs verwenden können, um Speicher zwischen Knoten in einem Microsoft-Cluster gemeinsam zu nutzen, müssen Sie zunächst die gemeinsam genutzte Quorum-Festplatte und die gemeinsam genutzte Speicherfestplatte erstellen und sie dann zu beiden virtuellen Maschinen im Cluster hinzufügen.

Die freigegebene Festplatte wird nicht mit dem Plug-in für Windows erstellt. Sie sollten die gemeinsam genutzte LUN erstellen und dann zu jeder virtuellen Maschine im Cluster hinzufügen. Weitere Informationen finden Sie unter "Clustern virtueller Maschinen über physische Hosts" .

Hinzufügen von Controller-basierten Lizenzen für SnapCenter Standard

Wenn Sie FAS, AFF oder ASA Speichercontroller verwenden, ist eine Controller-basierte

Lizenz für SnapCenter Standard erforderlich.

Die Controller-basierte Lizenz weist die folgenden Merkmale auf:

- SnapCenter Standard-Berechtigung im Kauf von Premium oder Flash Bundle enthalten (nicht im Basispaket)
- Unbegrenzte Speichernutzung
- 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.

- An die Seriennummer des Controllers gebunden

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 **Speichersysteme** aus.
2. Wählen Sie auf der Seite „Speichersysteme“ 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 Clusternamen 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-Lizenz“ wird der folgende Status angezeigt:

   - zeigt an, dass eine SnapManager Suite-Lizenz auf einem FAS, AFF oder ASA Primärspeichersystem installiert ist.
   - zeigt an, dass auf einem FAS, AFF oder ASA Primärspeichersystem keine SnapManager Suite-Lizenz installiert ist.

- Nicht anwendbar bedeutet, dass eine SnapManager Suite-Lizenz nicht anwendbar ist, da sich der Speichercontroller auf Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select oder sekundäre Speicherplattformen befindet.

Schritt 2: Identifizieren der auf dem Controller installierten Lizenzen

Sie können die ONTAP -Befehlszeile verwenden, um alle auf Ihrem Controller installierten Lizenzen anzuzeigen. Sie sollten Clusteradministrator auf dem FAS, AFF oder ASA System sein.

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

Schritte

1. Melden Sie sich über die ONTAP -Befehlszeile beim NetApp -Controller an.
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: 1-81-0000000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

Im Beispiel ist die SnapManagerSuite-Lizenz installiert, daher ist keine zusätzliche SnapCenter -Lizenzierungsaktion 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. Melden Sie sich über die ONTAP -Befehlszeile beim Controller an.
2. Geben Sie den Befehl „system show -instance“ ein und überprüfen Sie dann die Ausgabe, um die Seriennummer des Controllers 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: Seriennummer der Controller-basierten Lizenz abrufen

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

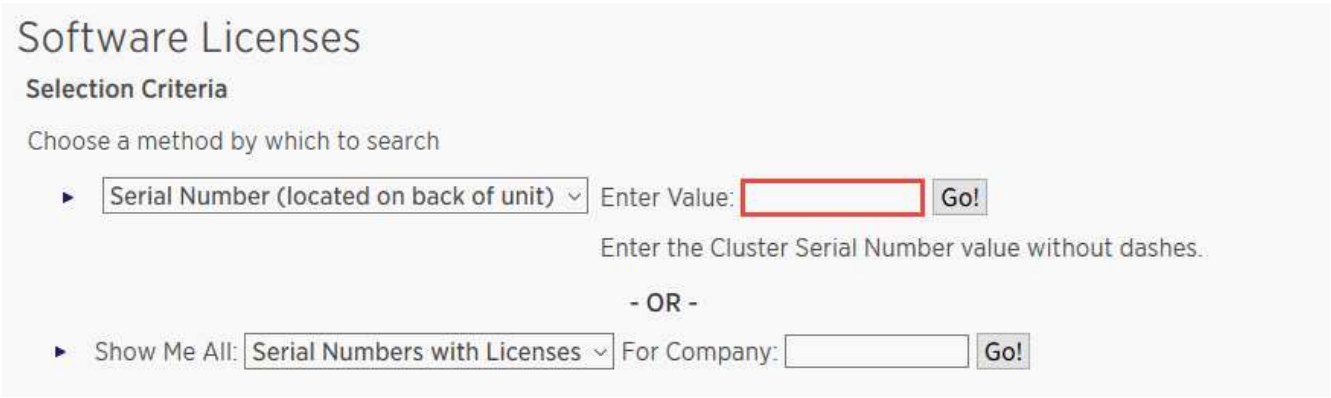
- Sie sollten über gültige Anmeldeinformationen für die NetApp -Support-Site verfügen.

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

- Sie sollten die Seriennummer des Controllers haben.

Schritte

1. Melden Sie sich an bei "NetApp Support Site" .
2. Navigieren Sie zu **Systeme** > **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 **Los!**.



   Es wird eine Liste der Lizenzen für den angegebenen Controller angezeigt.

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

Schritt 5: Controllerbasierte Lizenz hinzufügen

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn Sie SnapCenter auf Testbasis mit FAS, AFF oder ASA -Speicher installieren möchten, können Sie eine Evaluierungslizenz für das Premium Bundle erwerben und auf Ihrem Controller installieren.

Wenn Sie SnapCenter testweise installieren möchten, sollten Sie sich an Ihren Vertriebsmitarbeiter wenden,

um eine Evaluierungslizenz für das Premium Bundle zur Installation auf Ihrem Controller zu erhalten.

Schritte

1. Melden Sie sich über die ONTAP -Befehlszeile beim NetApp -Cluster an.
2. Fügen Sie den SnapManagerSuite-Lizenzschlüssel hinzu:

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

   Dieser Befehl ist auf der Administratorberechtigungsebene verfügbar.

3. Stellen Sie sicher, dass 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 Lizenz für SnapCenter Standard verwenden.

Schritte

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

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

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

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

3. Entfernen Sie die Testlizenz aus der Datenbank:

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

Konfigurieren der Hochverfügbarkeit

Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit

Um Hochverfügbarkeit (HA) in SnapCenter unter Windows oder Linux zu unterstützen, können Sie den F5-Lastenausgleich installieren. F5 ermöglicht dem SnapCenter Server die Unterstützung von Aktiv-Passiv-Konfigurationen auf bis zu zwei Hosts am selben

Standort. Um den F5 Load Balancer in SnapCenter zu verwenden, sollten Sie die SnapCenter -Server und den F5 Load Balancer konfigurieren.

Sie können auch Network Load Balancing (NLB) konfigurieren, um SnapCenter High Availability einzurichten. Für eine hohe Verfügbarkeit sollten Sie NLB außerhalb der SnapCenter -Installation manuell konfigurieren.

Für Cloudumgebungen können Sie Hochverfügbarkeit entweder mit Amazon Web Services (AWS) Elastic Load Balancing (ELB) oder Azure Load Balancer konfigurieren.

Konfigurieren der Hochverfügbarkeit mit F5

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

Sie müssen Mitglied der lokalen Administratorgruppe auf den SnapCenter -Servern sein (und Ihnen muss zusätzlich die Rolle „SnapCenterAdmin“ zugewiesen sein), um die folgenden Cmdlets zum Hinzufügen und Entfernen von F5-Clustern verwenden zu können:

- Add-SmServerCluster
- SmServer hinzufügen
- Entfernen-SmServerCluster

  Weitere Informationen finden Sie unter "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Weitere Informationen

- Nachdem Sie SnapCenter für hohe Verfügbarkeit installiert und konfiguriert haben, bearbeiten Sie die SnapCenter Desktopverknüpfung so, dass sie auf die IP des F5-Clusters verweist.
- Wenn ein Failover zwischen SnapCenter -Servern auftritt und auch eine SnapCenter -Sitzung vorhanden ist, müssen Sie den Browser schließen und sich erneut bei SnapCenter anmelden.
- Wenn Sie beim Einrichten des Lastenausgleichs (NLB oder F5) einen Host hinzufügen, der teilweise vom NLB- oder F5-Host aufgelöst wird, und der SnapCenter Host diesen Host nicht erreichen kann, wechselt die SnapCenter Hostseite häufig zwischen dem Status „Hosts ausgefallen“ und „Hosts ausgeführt“. Um dieses Problem zu beheben, sollten Sie sicherstellen, dass beide SnapCenter -Hosts den Host im NLB- oder F5-Host auflösen können.
- SnapCenter -Befehle für MFA-Einstellungen sollten auf allen Hosts ausgeführt werden. Die Konfiguration der vertrauenden Seite sollte auf dem Active Directory Federation Services (AD FS)-Server mithilfe der F5-Clusterdetails erfolgen. Der Zugriff auf die SnapCenter Benutzeroberfläche auf Hostebene wird blockiert, nachdem MFA aktiviert wurde.
- Während des Failovers werden die Audit-Protokolleinstellungen nicht auf dem zweiten Host angezeigt. Daher sollten Sie die Audit-Protokolleinstellungen auf dem passiven F5-Host manuell wiederholen, wenn dieser aktiv wird.

Konfigurieren Sie Hochverfügbarkeit mithilfe des Netzwerklastenausgleichs (NLB).

Sie können den Netzwerklastenausgleich (NLB) konfigurieren, um SnapCenter High Availability einzurichten. Für eine hohe Verfügbarkeit sollten Sie NLB außerhalb der SnapCenter -Installation manuell konfigurieren.

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

Konfigurieren Sie Hochverfügbarkeit mit AWS Elastic Load Balancing (ELB).

Sie können eine SnapCenter -Umgebung mit hoher Verfügbarkeit in Amazon Web Services (AWS) konfigurieren, indem Sie zwei SnapCenter -Server in separaten Verfügbarkeitszonen (AZs) einrichten und sie 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 der virtuellen privaten Overlay-IP" .

2. Vorbereiten Ihres Windows-Hosts
    a. Erzwingen, dass IPv4 gegenüber IPv6 priorisiert wird:
        - Speicherort: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
        - Schlüssel: DisabledComponents
        - Typ: REG_DWORD
        - Wert: 0x20
    b. Stellen Sie sicher, dass die vollqualifizierten Domänennamen über DNS oder über die lokale Hostkonfiguration in die IPv4-Adressen aufgelöst werden können.
    c. Stellen Sie sicher, dass Sie keinen Systemproxy konfiguriert haben.
    d. Stellen Sie sicher, dass das Administratorkennwort auf beiden Windows-Servern identisch ist, wenn Sie ein Setup ohne Active Directory verwenden und sich die Server nicht in derselben Domäne befinden.
    e. Fügen Sie auf beiden Windows-Servern eine virtuelle IP hinzu.
3. Erstellen Sie den SnapCenter Cluster.
    a. Starten Sie Powershell und stellen Sie eine Verbindung zu 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. Holen Sie sich die Details zur Hochverfügbarkeit. `Get-SmServerConfig`
4. Erstellen Sie die Lambda-Funktion, um die Routing-Tabelle anzupassen, falls der virtuelle private IP-Endpunkt nicht verfügbar ist, überwacht von AWS CloudWatch. Weitere Informationen finden Sie unter "Erstellen einer Lambda-Funktion" .
5. Erstellen Sie einen Monitor in CloudWatch, um die Verfügbarkeit des SnapCenter -Endpunkts zu überwachen. Ein Alarm wird so konfiguriert, dass er eine Lambda-Funktion auslöst, wenn der Endpunkt nicht erreichbar ist. Die Lambda-Funktion passt die Routing-Tabelle an, um den Datenverkehr zum aktiven SnapCenter -Server umzuleiten. Weitere Informationen finden Sie unter "Erstellen Sie synthetische Kanarienvögel" .
6. Implementieren Sie einen Workflow mithilfe einer Schrittfunktion als Alternative zur CloudWatch-Überwachung, um kürzere Failover-Zeiten zu ermöglichen. Der Workflow umfasst eine Lambda-Testfunktion zum Testen der SnapCenter -URL, eine DynamoDB-Tabelle zum Speichern der Fehleranzahl und die Step-Funktion selbst.
    a. Verwenden Sie eine Lambda-Funktion zum Prüfen der SnapCenter -URL. Weitere Informationen finden Sie unter "Erstellen einer Lambda-Funktion" .
    b. Erstellen Sie eine DynamoDB-Tabelle zum Speichern der Fehleranzahl zwischen zwei Step Function-Iterationen. Weitere Informationen finden Sie unter "Erste Schritte mit DynamoDB-Tabellen" .
    c. Erstellen Sie die Schrittfunktion. Weitere Informationen finden Sie unter "Step Function-Dokumentation" .
    d. Testen Sie einen einzelnen Schritt.

e. Testen Sie die komplette Funktion.

f. Erstellen Sie eine IAM-Rolle und passen Sie die Berechtigungen an, um die Lambda-Funktion ausführen zu dürfen.

g. Erstellen Sie einen Zeitplan zum Auslösen der Step-Funktion. Weitere Informationen finden Sie unter "Verwenden des Amazon EventBridge Scheduler zum Starten einer Step Function" .

Konfigurieren der Hochverfügbarkeit mit Azure Load Balancer

Sie können eine SnapCenter Umgebung mit hoher Verfügbarkeit mithilfe des Azure Load Balancers konfigurieren.

Schritte

1. Erstellen Sie mithilfe des Azure-Portals virtuelle Computer in einer Skalierungsgruppe. Mit dem Azure-VM-Skalierungssatz können Sie eine Gruppe von virtuellen Maschinen mit Lastenausgleich erstellen und verwalten. Die Anzahl der Instanzen virtueller Maschinen kann je nach Bedarf oder nach einem festgelegten Zeitplan automatisch erhöht oder verringert werden. Weitere Informationen finden Sie unter "Erstellen virtueller Computer in einer Skalierungsgruppe mithilfe des Azure-Portals" .
2. Melden Sie sich nach der Konfiguration der virtuellen Maschinen bei jeder virtuellen Maschine im VM-Set an und installieren Sie SnapCenter Server auf beiden Knoten.
3. Erstellen Sie den Cluster auf 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. Erhalten Sie die Details zur Hochverfügbarkeit. `Get-SmServerConfig`
6. Erstellen Sie bei Bedarf den sekundären Host neu. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. Failover zum zweiten Host. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== Wechseln Sie von NLB zu F5 für hohe Verfügbarkeit

Sie können Ihre SnapCenter HA-Konfiguration von Network Load Balancing (NLB) ändern, um F5 Load Balancer zu verwenden.

Schritte

1. Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit mit F5. "Mehr erfahren" .
2. Starten Sie PowerShell auf dem SnapCenter Server-Host.
3. Starten Sie eine Sitzung mit dem Cmdlet „Open-SmConnection“ und geben Sie dann Ihre Anmeldeinformationen ein.
4. Aktualisieren Sie den SnapCenter -Server mithilfe des Cmdlets „Update-SmServerCluster“, sodass er auf die IP-Adresse des F5-Clusters verweist.

   Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Hohe Verfügbarkeit für das SnapCenter MySQL-Repository

Die MySQL-Replikation ist eine Funktion des MySQL-Servers, mit der Sie Daten von einem MySQL-Datenbankserver (Master) auf einen anderen MySQL-Datenbankserver (Slave) replizieren können. SnapCenter unterstützt die MySQL-Replikation für hohe Verfügbarkeit nur auf zwei Knoten mit aktiviertem Netzwerklastenausgleich (NLB).

SnapCenter führt Lese- oder Schreibvorgänge am Master-Repository aus und leitet seine Verbindung zum Slave-Repository um, wenn im Master-Repository ein Fehler auftritt. Das Slave-Repository wird dann zum Master-Repository. SnapCenter unterstützt auch die umgekehrte Replikation, die nur während eines Failovers aktiviert wird.

Wenn Sie die MySQL-Hochverfügbarkeitsfunktion (HA) verwenden möchten, müssen Sie Network Load Balancer (NLB) auf dem ersten Knoten konfigurieren. Das MySQL-Repository wird im Rahmen der Installation auf diesem Knoten installiert. Während Sie SnapCenter auf dem zweiten Knoten installieren, müssen Sie sich mit F5 des ersten Knotens verbinden und eine Kopie des MySQL-Repositorys auf dem zweiten Knoten erstellen.

SnapCenter bietet die PowerShell-Cmdlets *Get-SmRepositoryConfig* und *Set-SmRepositoryConfig* zur Verwaltung der MySQL-Replikation.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Sie müssen sich der Einschränkungen im Zusammenhang mit der MySQL HA-Funktion bewusst sein:

- NLB und MySQL HA werden über zwei Knoten hinaus nicht unterstützt.
- Der Wechsel von einer eigenständigen SnapCenter -Installation zu einer NLB-Installation oder umgekehrt sowie der Wechsel von einem eigenständigen MySQL-Setup zu MySQL HA werden nicht unterstützt.
- Automatisches Failover wird nicht unterstützt, wenn die Daten des Slave-Repositorys nicht mit den Daten des Master-Repositorys synchronisiert sind.

  Sie können ein erzwungenes Failover mithilfe des Cmdlets *Set-SmRepositoryConfig* initiieren.

- Wenn ein Failover eingeleitet wird, können laufende Jobs fehlschlagen.

  Wenn ein Failover auftritt, weil der MySQL-Server oder der SnapCenter Server ausgefallen ist, können alle ausgeführten Jobs fehlschlagen. Nach dem Failover auf den zweiten Knoten werden alle nachfolgenden Jobs erfolgreich ausgeführt.

Informationen zum Konfigurieren von Hochverfügbarkeit finden Sie unter "So konfigurieren Sie NLB und ARR mit SnapCenter" .

Konfigurieren der rollenbasierten Zugriffssteuerung (RBAC)

Erstellen einer Rolle

Zusätzlich zur Verwendung der vorhandenen SnapCenter -Rollen können Sie Ihre eigenen 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 + .
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 die Objekte anderer Mitglieder sehen** aus, um anderen Mitgliedern der Rolle das Anzeigen von Ressourcen wie Volumes und Hosts zu ermöglichen, nachdem sie die Ressourcenliste aktualisiert haben.

   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 die 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 erteilen.
7. Klicken Sie auf **Senden**.

Hinzufügen einer NetApp ONTAP RBAC-Rolle mithilfe von Sicherheitsanmeldebefehlen

Sie können die Sicherheitsanmeldebefehle verwenden, um eine NetApp ONTAP RBAC-Rolle hinzuzufügen, wenn auf Ihren Speichersystemen 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.
- Erteilen Sie Berechtigungen für Befehle und/oder Befehlsverzeichnisse.

  Für jeden Befehl/jedes Befehlsverzeichnis gibt es zwei Zugriffsebenen: Vollzugriff und schreibgeschützt.

  Sie müssen immer zuerst die Vollzugriffsrechte zuweisen.

- Weisen Sie Benutzern Rollen zu.
- 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.

Informationen zu diesem Vorgang

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 kümmert sich automatisch um die korrekte Einrichtung der ONTAP Berechtigungen. Beispielsweise fügt das Tool RBAC User Creator für NetApp ONTAP die Berechtigungen automatisch in der richtigen Reihenfolge hinzu, sodass die Berechtigungen für den uneingeschränkten Zugriff zuerst angezeigt werden. Wenn Sie zuerst die Nur-Lese-Berechtigungen und dann die Vollzugriffsberechtigungen hinzufügen, markiert ONTAP die Vollzugriffsberechtigungen als Duplikate und ignoriert sie.

> Wenn Sie SnapCenter oder ONTAP später aktualisieren, sollten Sie das Tool RBAC User Creator für NetApp ONTAP erneut ausführen, um die zuvor erstellten Benutzerrollen zu aktualisieren. Für eine frühere Version von SnapCenter oder ONTAP erstellte Benutzerrollen funktionieren mit aktualisierten Versionen nicht ordnungsgemäß. Wenn Sie das Tool erneut ausführen, wird das Upgrade automatisch durchgeführt. Sie müssen die Rollen nicht neu erstellen.

Weitere Informationen zum Einrichten von ONTAP RBAC-Rollen finden Sie im "ONTAP 9 Administrator-Authentifizierung und RBAC Power Guide" .

Schritte

1. Erstellen Sie auf dem Speichersystem 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, wird standardmäßig der Clusteradministrator verwendet.
   - role_name ist der Name, den Sie für die Rolle angeben.
   - Befehl ist die ONTAP Fähigkeit.

   > Sie müssen diesen Befehl für jede Berechtigung wiederholen. Denken Sie daran, dass Befehle mit vollem Zugriff vor schreibgeschützten Befehlen aufgeführt 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, indem Sie den folgenden Befehl eingeben:

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

   - Benutzername ist der Name des Benutzers, den Sie erstellen.
   - <Passwort> ist Ihr Passwort. Wenn Sie kein Kennwort angeben, werden Sie vom System zur Eingabe eines Kennworts aufgefordert.
   - svm_name ist der Name der SVM.

3. Weisen Sie dem Benutzer die Rolle zu, indem Sie den folgenden Befehl eingeben:

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

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

können Sie den Benutzer ändern, um ihn der Rolle zuzuordnen.

- <svm_name> ist der Name der SVM.
- <role_name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.
- <Passwort> ist Ihr Passwort. Wenn Sie kein Kennwort angeben, werden Sie vom System zur Eingabe eines Kennworts aufgefordert.

4. Überprüfen Sie, ob der Benutzer korrekt 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

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen müssen, wenn Sie eine Rolle für einen neuen SVM-Benutzer in ONTAP erstellen. Diese Rolle ist erforderlich, wenn Sie SVMs in ONTAP 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 diesem Benutzer die Rolle 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 mehrere 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

Erstellen Sie 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 diesem Benutzer die Rolle 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 mehrere 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 Clusterrollen mit minimalen Berechtigungen

Sie sollten eine ONTAP Clusterrolle 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 Clusterrolle zu erstellen und Mindestberechtigungen 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 diesem Benutzer die Rolle 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 mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um Clusterrollen 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 Sie ONTAP Clusterrollen für ASA R2-Systeme

Sie sollten eine ONTAP Clusterrolle 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 Clusterrolle zu erstellen und Mindestberechtigungen 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 diesem Benutzer die Rolle 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 mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um Clusterrollen 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 Zugriffskontrolle für SnapCenter -Benutzer zu konfigurieren, können Sie Benutzer oder Gruppen hinzufügen und Rollen zuweisen. Die Rolle bestimmt die Optionen, auf die SnapCenter -Benutzer zugreifen können.

Bevor Sie beginnen

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

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

- SnapCenter umfasst mehrere vordefinierte Rollen.

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

- AD-Benutzer und AD-Gruppen, die zu SnapCenter RBAC hinzugefügt werden, müssen über die Leseberechtigung für den Benutzercontainer und den Computercontainer im Active Directory verfügen.
- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle mit den entsprechenden Berechtigungen zugewiesen haben, müssen Sie dem Benutzer Zugriff auf SnapCenter -Assets wie Hosts und Speicherverbindungen zuweisen.

Dadurch 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 Vorteile der RBAC-Berechtigungen und -Effizienz zu nutzen.
- Sie können dem Benutzer beim Erstellen des Benutzers oder der Gruppe Assets wie Host, Ressourcengruppen, Richtlinien, Speicherverbindungen, Plug-Ins und Anmeldeinformationen zuweisen.
- Die Mindestressourcen, die Sie einem Benutzer zum Ausführen bestimmter Vorgänge zuweisen sollten, sind wie folgt:

Betrieb	Vermögenszuordnung
Ressourcen schützen	Gastgeber, Politik
Sicherung	Host, Ressourcengruppe, Richtlinie
Wiederherstellen	Host, Ressourcengruppe
Klonen	Host, Ressourcengruppe, Richtlinie
Lebenszyklus des Klons	Gastgeber
Erstellen einer Ressourcengruppe	Gastgeber

- Wenn einem Windows-Cluster oder einem DAG-Asset (Exchange Server Database Availability Group) ein neuer Knoten hinzugefügt wird und dieser neue Knoten einem Benutzer zugewiesen wird, müssen Sie das Asset dem Benutzer oder der Gruppe neu zuweisen, um den neuen Knoten in den Benutzer oder die Gruppe aufzunehmen.

  Sie sollten den RBAC-Benutzer oder die RBAC-Gruppe dem Cluster oder DAG neu zuweisen, um den neuen Knoten in den RBAC-Benutzer oder die RBAC-Gruppe aufzunehmen. Sie verfügen beispielsweise über einen Cluster mit zwei Knoten und haben dem Cluster einen RBAC-Benutzer oder eine RBAC-Gruppe zugewiesen. Wenn Sie dem Cluster einen weiteren Knoten hinzufügen, sollten Sie den RBAC-Benutzer oder die RBAC-Gruppe dem Cluster neu zuweisen, um den neuen Knoten für den RBAC-Benutzer oder die RBAC-Gruppe einzuschließen.

- Wenn Sie Snapshots replizieren möchten, müssen Sie die Speicherverbindung sowohl für das Quell- als auch für das Zielvolume dem Benutzer zuweisen, der den Vorgang durchführt.

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

Wenn Sie die Funktionen des SnapCenter Plug-in for VMware vSphere zum Schutz von VMs, VMDKs oder Datenspeichern verwenden, sollten Sie die VMware vSphere-GUI verwenden, um einen vCenter-Benutzer zu einer SnapCenter Plug-in for VMware vSphere hinzuzufügen. Informationen zu VMware vSphere-Rollen finden Sie unter "Vordefinierte Rollen im SnapCenter Plug-in for 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 Arbeitsgruppe hinzufügen“:

Für dieses Feld…	Machen Sie Folgendes…
Zugriffstyp	Wählen Sie entweder Domäne oder Arbeitsgruppe aus Beim Domänenauthentifizierungstyp sollten Sie den Domänennamen des Benutzers oder der Gruppe angeben, der Sie den Benutzer zu einer Rolle hinzufügen möchten. Standardmäßig ist es bereits mit dem angemeldeten Domänennamen ausgefüllt. Sie müssen die nicht vertrauenswürdige Domäne auf der Seite **Einstellungen** > **Globale Einstellungen** > **Domäneneinstellungen** registrieren.
Typ	Wählen Sie entweder „Benutzer“ oder „Gruppe“ aus. SnapCenter unterstützt nur Sicherheitsgruppen und nicht die Verteilergruppe.

Für dieses Feld…	Machen Sie Folgendes…
Benutzername	a. Geben Sie den Teil des Benutzernamens ein und klicken Sie dann auf **Hinzufügen**. Beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden. b. Wählen Sie den Benutzernamen aus der Suchliste aus. Wenn Sie Benutzer aus einer anderen oder 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, zu der Sie den Benutzer hinzufügen möchten.

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

      Die Assets werden nur aufgelistet, 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 **Senden**.

   Aktualisieren Sie die Ressourcenliste, nachdem Sie Benutzer oder Gruppen hinzugefügt und Rollen zugewiesen haben.

Konfigurieren der Überwachungsprotokolleinstellungen

Für jede einzelne Aktivität des SnapCenter -Servers werden Prüfprotokolle generiert. Standardmäßig werden Überwachungsprotokolle am standardmäßigen Installationsort *C:\Programme\ NetApp\ SnapCenter WebApp\audit* gesichert.

Prüfprotokolle werden durch die Generierung digital signierter Zusammenfassungen für jedes einzelne Prüfereignis gesichert, um sie vor unbefugten Änderungen zu schützen. Die generierten Digests werden in

einer separaten Prüfsummendatei gespeichert und regelmäßigen Integritätsprüfungen unterzogen, um die Integrität des Inhalts sicherzustellen.

Sie sollten sich mit der Rolle „SnapCenterAdmin“ angemeldet haben.

Informationen zu diesem Vorgang

- In den folgenden Szenarien werden Warnungen gesendet:
  - Zeitplan für die Integritätsprüfung des Audit-Protokolls oder Syslog-Server ist aktiviert oder deaktiviert
  - Integritätsprüfung des Überwachungsprotokolls, Überwachungsprotokoll oder Syslog-Serverprotokollfehler
  - Wenig Speicherplatz
- Eine E-Mail wird nur gesendet, wenn die Integritätsprüfung fehlschlägt.
- Sie sollten die Verzeichnispfade für das Überwachungsprotokoll und das Überwachungsprüfsummenprotokoll gemeinsam ändern. Sie können nicht nur einen davon ändern.
- Wenn die Verzeichnispfade für das Prüfprotokoll und das Prüfsummenprotokoll geändert werden, kann die Integritätsprüfung für die am früheren Speicherort vorhandenen Prüfprotokolle nicht durchgeführt werden.
- Die Verzeichnispfade für das Überwachungsprotokoll und das Überwachungsprüfsummenprotokoll sollten sich auf dem lokalen Laufwerk des SnapCenter -Servers befinden.

  Gemeinsam genutzte oder im Netzwerk bereitgestellte Laufwerke werden nicht unterstützt.
- Wenn in den Syslog-Servereinstellungen das UDP-Protokoll verwendet wird, können Fehler aufgrund eines ausgefallenen oder nicht verfügbaren Ports in SnapCenter weder als Fehler noch als Warnung erfasst werden.
- Sie können die Überwachungsprotokolle mit den Befehlen „Set-SmAuditSettings“ und „Get-SmAuditSettings“ konfigurieren.

  Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help command_name. Alternativ können Sie auch die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Navigieren Sie auf der Seite **Einstellungen** zu **Einstellungen** > **Globale Einstellungen** > **Einstellungen für Überwachungsprotokoll**.
2. Geben Sie im Abschnitt „Überwachungsprotokoll“ die Details ein.
3. Geben Sie das **Audit-Protokollverzeichnis** und das **Audit-Prüfsummenprotokollverzeichnis** ein
   a. Geben Sie die maximale Dateigröße ein
   b. Geben Sie die maximale Anzahl an Protokolldateien ein
   c. Geben Sie den Prozentsatz der Speicherplatznutzung ein, um eine Warnung zu senden
4. (Optional) Aktivieren Sie **UTC-Zeit protokollieren**.
5. (Optional) Aktivieren Sie **Zeitplan für Integritätsprüfung des Audit-Protokolls** und klicken Sie auf **Integritätsprüfung starten**, um die Integritätsprüfung bei Bedarf durchzuführen.

   Sie können auch den Befehl **Start-SmAuditIntegrityCheck** ausführen, um die Integritätsprüfung bei Bedarf zu starten.
6. (Optional) Aktivieren Sie „Überwachungsprotokolle an Remote-Syslog-Server weiterleiten“ und geben Sie

die Syslog-Serverdetails ein.

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

a. Geben Sie den Syslog-Server-Host ein
b. Geben Sie den Syslog-Server-Port ein
c. Geben Sie das Syslog-Serverprotokoll ein
d. RFC-Format eingeben

7. Klicken Sie auf **Speichern**.
8. Sie können Audit-Integritätsprüfungen und Festplattenspeicherprüfungen anzeigen, indem Sie auf **Überwachen** > **Jobs** klicken.

Konfigurieren Sie sichere MySQL-Verbindungen mit SnapCenter Server

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

Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter -Serverkonfigurationen

Sie können Secure Sockets Layer (SSL)-Zertifikate 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 SnapCenter -Server konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat
- Öffentliches Serverzertifikat und private Schlüsseldatei
- Öffentliches Client-Zertifikat und private Schlüsseldatei

Schritte

1. Richten Sie die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

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

   Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

Best Practice: Sie sollten den vollqualifizierten Domänennamen (FQDN) des Servers als allgemeinen Namen für das Serverzertifikat verwenden.

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

   Der Standardpfad des MySQL-Datenordners lautet `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Der Standardpfad der MySQL-Serverkonfigurationsdatei (my.ini) lautet `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

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

   Sie müssen das CA-Zertifikat, das öffentliche Client-Zertifikat und die privaten Schlüsselpfade des Clients im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) 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. Stoppen Sie die SnapCenter Server-Webanwendung im Internet Information Server (IIS).
5. Starten Sie den MySQL-Dienst neu.
6. Aktualisieren Sie den Wert des MySQLProtocol-Schlüssels in der SnapManager Datei .Web.UI.dll.config.

   Das folgende Beispiel zeigt den Wert des MySQLProtocol-Schlüssels, der in der SnapManager Datei .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 angegeben 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 SnapCenter Server-Webanwendung im IIS.

Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen

Sie können Secure Sockets Layer (SSL)-Zertifikate und Schlüsseldateien für beide High Availability (HA)-Knoten 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-Knoten wird ein CA-Zertifikat generiert und dieses CA-Zertifikat wird auf den anderen HA-Knoten kopiert.

- Öffentliches Serverzertifikat und private Serverschlüsseldateien für beide HA-Knoten

- Öffentliches Client-Zertifikat und private Client-Schlüsseldateien für beide HA-Knoten

Schritte

1. Richten Sie für den ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

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

   > Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

   Best Practice: Sie sollten den vollqualifizierten Domänennamen (FQDN) des Servers als allgemeinen Namen für das Serverzertifikat verwenden.

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

   Der Standardpfad des MySQL-Datenordners lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Der Standardpfad der MySQL-Serverkonfigurationsdatei (my.ini) lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.

   > Sie müssen die Pfade für das CA-Zertifikat, das öffentliche Serverzertifikat und den privaten Schlüssel des Servers im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

   Sie müssen die Pfade des CA-Zertifikats, des öffentlichen Client-Zertifikats und des privaten Client-Schlüssels im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

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

   ```
   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-Knoten das CA-Zertifikat und generieren Sie ein öffentliches Serverzertifikat, private Serverschlüsseldateien, ein öffentliches Clientzertifikat und private Clientschlüsseldateien. Führen Sie die folgenden Schritte aus:

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

      Der Standardpfad des MySQL-Datenordners lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

      > Sie müssen kein CA-Zertifikat erneut erstellen. Sie sollten nur das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, die private Schlüsseldatei des Servers und die private Schlüsseldatei des Clients erstellen.

   b. Richten Sie für den ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

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

      > Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

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

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

   d. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

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

      Sie müssen das CA-Zertifikat, das öffentliche Client-Zertifikat und die privaten Schlüsselpfade des

Clients im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

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

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

   Das folgende Beispiel zeigt den Wert des MySQLProtocol-Schlüssels, 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-Knoten angegeben haben.

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

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

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

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

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

    Auch wenn der Replikationsstatus fehlerfrei ist, können Sie mit der Option -Force das Slave-Repository neu erstellen.